

# Curves, Cryptosystems, and Quantum Computing

Karl-Heinz Zimmermann

TUHH

July 4, 2019



©K.-H. Zimmermann

Prof. Dr. Karl-Heinz Zimmermann  
Hamburg University of Technology  
21071 Hamburg  
Germany

This monograph is listed in the GBV database and the TUHH library.

All rights reserved  
©2019, by Karl-Heinz Zimmermann, author

<https://doi.org/10.15480/882.2319>  
<http://hdl.handle.net/11420/2890>  
<urn:nbn:de:gbv:830-882.037832>

## Preface

Today, data security is a huge asset of our society. Cryptography is a field that provides methods and techniques for the security and authenticity of data. It's a fantastic detective drama series about lovely Alice, crooked Bob, evil Eve and the like. Modern cryptography is heavily based on mathematics and computer science.

The slides at hand are a development of class notes of a four-hour lecture held for first-year Master students of Computer Science, Electrical Engineering, and Technomathematics at the Hamburg University of Technology in hot and dry summer 2018.

The ultimate goal of the course was to present the beautiful mathematics of elliptic curves and their use in cryptography. However, alarmed by recent announcements of leading computer companies that quantum computers with about 70 qubits are at the gates, I decided to include a short introduction to the intriguing quantum mechanics and the shrugging quantum algorithms of Grover and Shor which could render the current cryptographic protocols nearly useless in the future.

## Preface (Cont'd)

I must apologize for giving this course fully based on slides and not by chalk and blackboard. This is an unexcusable mistake for a course which should be attributed to pure mathematics. However, the slides contain all the necessary steps to understand the arguments and I would have never come this far when writing on the board. Needless to say it would have cost me another made-to-measure suit.

\*Starred material can be safely skipping on a first reading without loss of continuity. Note that literature is mentioned at several places in the document and an index will be separately available.

I would like to thank my collaborator Robert Leppert for useful comments and to help out when required. Finally, I would like to thank my students for their attention, their stimulating questions, and their dedicated work.

Hamburg, July 2019

*Karl-Heinz Zimmermann*

## Dedication

To my family  
for sempiternal  
support.

## Contents

- Basic cryptography
- Theory of algebraic and elliptic curves
- Elliptic curve cryptography
- Quantum computing with emphasis on cryptography

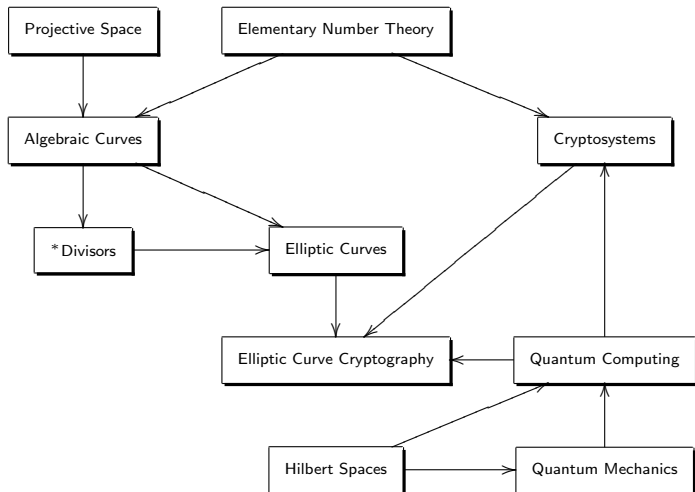
## Contents - Chapters

- 1 Introduction to cryptosystems
- 2 Projective space
- 3 Algebraic curves
- 4 Introduction to elliptic curves
- 5 Theory of elliptic curves
- 6 Elliptic curves over finite fields
- 7 Elliptic curve cryptography
- 8 Quantum computing

## Appendix

- 9 Elementary number theory
- 10 Hilbert space
- 11 Introduction to quantum mechanics

## Contents – Road Map



## Oral Exam (25 min.)

### Topics:

- Algebraic and elliptic curves in projective space
- Elliptic curves over finite fields
- Elliptic curve cryptography
- Quantum computing.

\*No starred material, no Singular.

## Formalities

- *Schedule:*
  - Wednesday, 12:30-2:00 pm, H0.03,
  - Friday, 8:00-9:30 am, H0.05.
- *Classroom:* transparencies
- *StudIP:* documents, appointments
- *Exam:* oral (25 min)

## Literature

- F.L. Bauer, *Decrypted Secrets*, Springer, Berlin, 2000.
- Gert-Martin Greuel, Gerhard Pfister, *A Singular Introduction to Commutative Algebra*, Springer, Berlin, 2008.
- David J. Griffiths, Darrell F. Schroeter, *Introduction to Quantum Mechanics*, Cambridge Univ. Press, Cambridge, UK, 2018.
- Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer, Berlin, 1994.
- Anthony Knapp, *Elliptic Curves*, Princeton Univ. Press, New York, 1992.
- Rene L. Schilling, *Measures, Integrals and Martingales*, Cambridge Univ. Press, Cambridge, UK, 2017.
- Joseph Silverman, *The Arithmetic of Elliptic Curves*, Springer, Berlin, 2009.
- Lawrence Washington, *Elliptic Curves - Number Theory and Cryptography*, Chapman & Hall, Boca Raton, 2008.
- Annette Werner, *Elliptische Kurven*, Springer, 2013.

## Notation

$\mathbb{Z}$	ring of integers
$\mathbb{Z}_n$	ring of integers modulo $n$
$\mathbb{Z}_n^*$	unit group of integers modulo $n$
$\mathbb{Q}$	field of rational numbers
$\mathbb{R}$	field of real numbers
$\mathbb{C}$	field of complex numbers
$i$	imaginary unit
$\mathbb{K}$	field
$\bar{\mathbb{K}}$	algebraic closure of field $\mathbb{K}$
$\mathbb{F}_q$	finite field of order $q$
$\mathbb{K}^*$	unit group of field
$\mathbb{A}^n$	affine $n$ -space
$\mathbb{P}^n$	projective $n$ -space
$f^{(k)}$	degree $k$ -part of homogenous polynomial $f$
$f^h$	homogenization of polynomial $f$
$f^a$	dehomogenization of homogeneous polynomial $f$

## Notation (cont'd)

$\ell$	linear homogeneous polynomial
$\mathcal{L}(\ell)$	projective line
$\mathcal{L}(\alpha, \beta, \gamma)$	projective line
$\mathcal{C}$	algebraic curve
$\mathcal{E}$	elliptic curve
$i(P, \mathcal{L}, \mathcal{C})$	intersection multiplicity
$(a, b)$	gcd of $a$ and $b$
$a \equiv b \pmod{n}$	congruence modulo $n$
$a \equiv b \pmod{n}$	congruence modulo $n$ , symmetric case
$\phi(n)$	Euler's totient function
$\varphi$	golden ratio
$[a_0, \dots, a_n]$	Euler bracket
$\left(\frac{a}{n}\right)$	Jacobi symbol

# Part I

# Cryptosystems

# Cryptosystems

Curves,  
Cryptosystems,  
and Quantum  
Computing

K.-H.  
Zimmermann

Contents

History

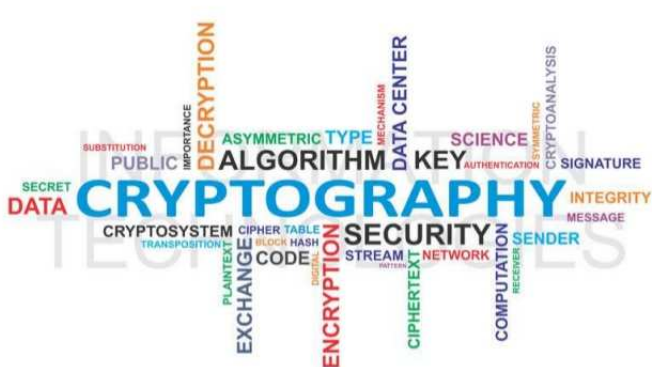
RSA

Discrete Log

\* Attacking  
Discrete Log

\* Pseudoprimes

\* Factoring



## Cryptosystems

Nearly every inventor of a cipher system has been convinced of the unsolvability of his brainchild.

David Kahn, 1967

## Cryptosystems

- Historical Account
- RSA
- Discrete logarithm
- \*Attacking discrete logarithm
- \*Pseudoprimality
- \*Factorization

## Early History of Cryptosystems

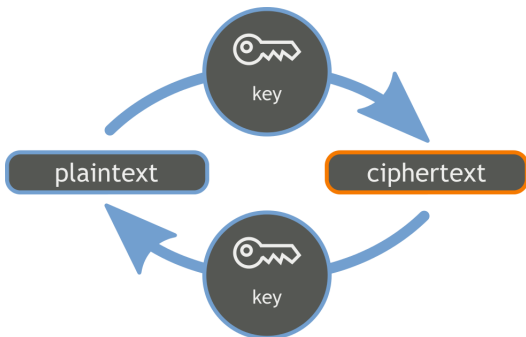
A substitution with a CAESAR encryption step was introduced in 1915 in the Russian army after it turned out to be impossible to expect the staffs to use anything more complicated.

F.L. Bauer, 2000

## Historical Account

- Symmetric cryptosystems
- Simple and polygraphic substitutions
- Transpositions
- Rotor crypto machines – Enigma
- Data encryption standard (DES)
- Asymmetric cryptosystems
- One-way and trapdoor functions
- Blockchain
- Cryptology

## Symmetric Cryptosystems



## Symmetric Cryptosystems

- The key agreed upon by two partners determines both the encryption and decryption.
- Cryptanalytic security depends on the secrecy of the key.
- Authentication is guaranteed as long as the secrecy of the key is guaranteed.

## Symmetric Cryptosystems

### Disadvantages:

- Sender of a message cannot prove to his partner that she sent the message (lack of judicial protection).
- The key has to be communicated or negotiated on a cryptanalytically secure channel.
- For a large number of partners wanting secure communication, the number of two-way channels and keys becomes quite large.
- A network with  $n$  partners requires  $\binom{n}{2} = \frac{n(n-1)}{2}$  self-reciprocal keys or  $n(n-1)$  symmetric keys.

## Simple Substitutions

- Monocyclic permutation:

abcdefghijklmnopqrstuvwxy  
z  
bcdefghijklmnopqrstuvwxyza

- The 3rd power was used by Julius Caesar:

abcdefghijklmnopqrstuvwxy  
z  
defghijklmnopqrstuvwxyzabc

Key: number 3

- Non-selfreciprocal and non-cyclic permutation:

abcdefghijklmnopqrstuvwxy  
z  
securityabdfghijklmnopqvwz

Key: security

## Cipher Disk

Leon Battista Alberti (1466)



## Polygraphic Substitutions

### Playfair cipher (1854)

- From a password, a permuted alphabet  $\mathbb{Z}_{25}$  (say omitting 'J') is inscribed into a  $5 \times 5$  square (thought as a closed torus):

S	E	C	U	R
A	B	D	F	G
H	I	K	L	M
N	O	P	Q	T
V	W	X	Y	Z

- If the letters of a bigram stand in the same line or column, each is replaced by the subsequent letter,

SH  $\mapsto$  AN,    CR  $\mapsto$  US.

## Polygraphic Substitutions

### Kurzsignalheft of Kriegsmarine (since 1941):

AAAA Beabsichtige gemeldete Feindstreitkräfte anzugreifen  
AAEE Beabsichtige Durchführung Unternehmung wie vorgesehen  
AAFF Beabsichtige Durchführung Unternehmung mit vollem Einsatz  
AAGG Beabsichtige gemeldete Feindstreitkräfte unter Vermeidung vollen Einsatzes

...

Four-letter code with position data and sender information encrypted by Enigma.

## Transpositions

The plaintext is written in rows of chosen length  $k$ , the columns are reordered according to a permutation  $\pi$  of length  $k$ , and the ciphertext is read out column-wise.

- Plain text

the transposition method gives a nice mess

- Matrices

thetrans	snarteht
position	noitisop
methodgi	igdohtem
vesanice	ecinasev
messxxxx	xxxxssem

- Key  $\pi = (8, 7, 6, 5, 4, 3, 2, 1)$  is called *Losung*.

- Cipher text

sniexnogcxaidixrtonxtihasestsshoeetpvmv

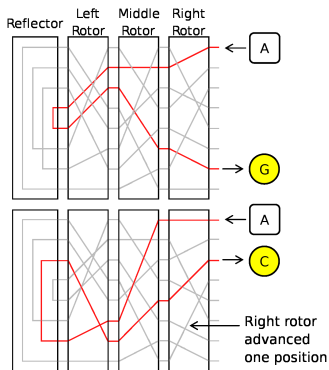
## Rotor Crypto Machines

### Enigma machine (Wehrmacht, World War II)



## Rotor Crypto Machines

## Enigma encryption



## Rotor Crypto Machines

- Encryption in Enigma C is an involution:

$$E = PR_1R_2R_3UR_3^{-1}R_2^{-1}R_1^{-1}P^{-1}$$

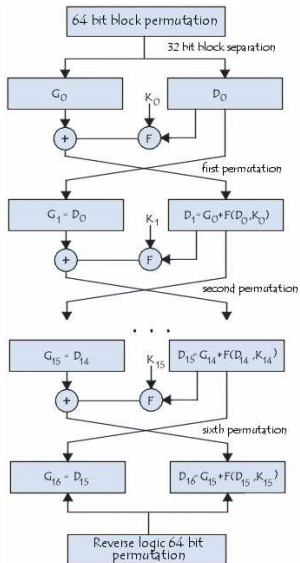
with plugboard transformation  $P$ , rotors  $R_1, R_2, R_3$ , and reflector  $U$ .

- If the rotor  $R_i$  is moves  $j$  positions, the transformation is  $\rho^j R_i \rho^{-j}$  with standard transformation  $\rho = (a, b, c, \dots, z)$ .
- The transformation becomes

$$E = P(\rho^i R_1 \rho^{-i})(\rho^j R_2 \rho^{-j})(\rho^k R_3 \rho^{-k})U \\ (\rho^k R_3^{-1} \rho^{-k})(\rho^j R_2^{-1} \rho^{-j})(\rho^i R_1^{-1} \rho^{-i})P^{-1}.$$

- Encryption and decryption work in the same way.
- Breaking the Enigma by the Polish and the British mainly due to problems with key negotiation and key administration.

# Data Encryption Standard (DES)



Curves,  
Cryptosystems,  
and Quantum  
Computing

K.-H.  
Zimmermann

Contents

History

Symmetric Systems  
Simple Substitutions

Polygraphic  
Substitutions

Transpositions

Enigma

DES

Asymmetric Systems

One-Way, Trapdoor

Blockchain

Cryptology

RSA

Discrete Log

\* Attacking

Discrete Log

\* Pseudoprimes

\* Factoring

## DES Encryption

- The 8-byte plaintext block is subjected to a (key-independent) initial transposition  $\pi$  and then split into two 4-byte blocks  $L_0$  and  $R_0$ .

- Next are 16 rounds,  $1 \leq i \leq 16$ ,

$$L_i = R_{i-1} \quad \text{and} \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

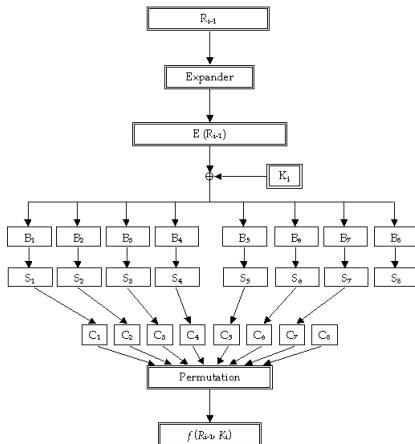
where  $\oplus$  is addition modulo 2 and  $K_i$  is a 48-bit key generated from the given key  $K$ .

- Final transposition  $\pi^{-1}$  ends encryption step.

## DES Encryption

The function  $f$  is the central part of DES:

- The 32-bit block  $R_{i-1}$  is expanded into 48-bit block  $E(R_{i-1})$  by duplication of certain bit positions and added modulo 2 to  $K_i$ .
- The 48-bit block is split into eight 6-bit groups as input of the eight substitution modules  $S_1, \dots, S_8$ , called *S-boxes*.

Encryption Function  $f$ 

## S-Boxes

$$S_1$$

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$$S_2$$

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

$$S_3$$

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

$$S_4$$

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

## S-Boxes

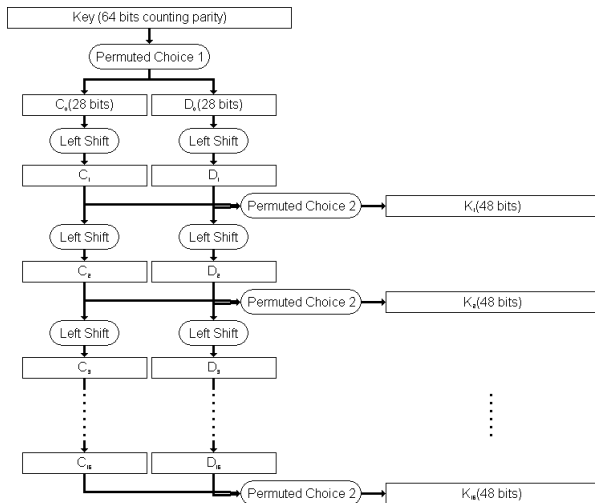
- Bit 1 and 6 of the 6-bit group, interpreted as binary numbers, determine the row.
- Bits 2 to 5 of the 6-bit group determine the column.
- In S-box  $S_1$ , the input 110010 gives row 2 (10) and column 9 (1001); the output is 1010 (10).

## DES Subkey Generation

Generation of the subkeys:

- The parity bits of the input key  $K$  are removed giving a 56-bit word.
- The 56-bit word is transposed w.r.t. fixed prescription and split in two 28-bit blocks.
- These blocks are cyclically left-shifted in each round.
- From these blocks a 48-bit subkey  $K_i$  is generated.

## DES Subkey Generation



## DES Specification

- The rounds of encryption can be described by processing

$$h_i : (L, R) \mapsto (R, L \oplus f(R, K_i))$$

and swapping

$$g : (R, L) \mapsto (L, R).$$

- Both mappings are involutions

$$g(g(R, L)) = g(L, R) = (R, L)$$

and

$$\begin{aligned} h_i(h_i(R, L)) &= h_i(R, L \oplus f(R, K_i)) \\ &= (R, L \oplus f(R, K_i) \oplus f(R, K_i)) \\ &= (R, L). \end{aligned}$$

## DES Encryption and Decryption

### ■ Encryption

$$E = \pi^{-1} \circ h_{16} \circ g \circ h_{15} \circ \dots \circ h_2 \circ g \circ h_1 \circ \pi.$$

### ■ Decryption by reversing the order of the subkeys,

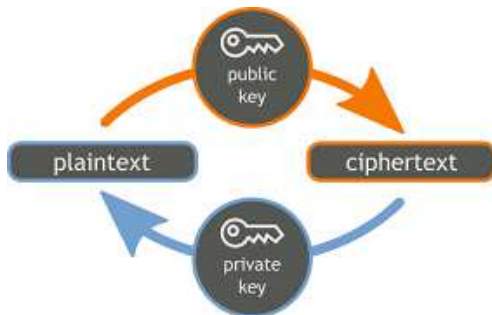
$$D = \pi^{-1} \circ h_1 \circ g \circ h_2 \circ \dots \circ h_{15} \circ g \circ h_{16} \circ \pi.$$

- Since all mappings are self-reciprocal, the composition of  $E$  and  $D$  yields the identity.

## DES Security

- *Avalanche effect*: After a few rounds, each bit of the intermediate result depends on each bit of the plaintext and the key.
- Main points of attack:
  - Design criteria of S-boxes not disclosed (trapdoor?).
  - Key length too small:  $2^{56} \approx 72 \cdot 10^{15}$  different keys.
  - In the ECB mode (streaming cipher), the key is kept fixed for quite a while.
- First successful brute force attack in 1998.
- Today, Advanced Encryption Standard (AES) is used (three key lengths: 128, 192, and 256 bits).

## Asymmetric Cryptosystems



## Asymmetric Cryptosystems

- Each partner has an open (public) key and a private key.
- No negotiation of keys is necessary.
- For a large number of partners, the total number of keys is much less than in symmetric cryptography.
- Public keys of all participants can be stored in an open directory.
- The concept of an open encryption key system was first published by Diffie and Hellman (1976).
- First implementation of open encryption key system by RSA (1998).

## Asymmetric Key Structure

- Let  $K_i$  and  $P_i$  be the public and private key of  $i$ -th partner, resp.
- $K_i$  and  $P_i$  determine encryption  $E_i$  and decryption  $D_i$  methods.
- Both  $E_i$  and  $D_i$  have efficient implementations.
- $(K_i)_i$  is a public directory and  $P_i$  is only known to  $i$ -th partner.
- Deriving  $P_i$  from  $K_i$  is practically impossible (intractable).

## Asymmetric Encryption

- Suppose the *asymmetric encryption property serving secrecy* holds:

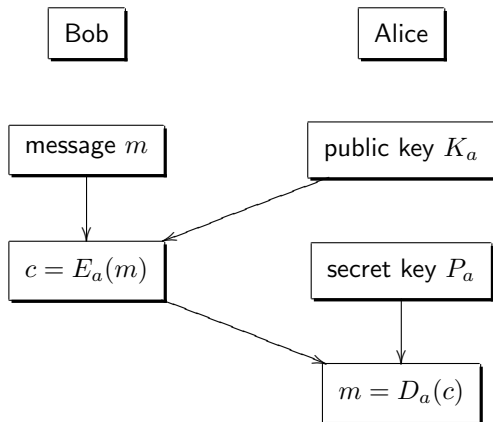
$$D_i(E_i(m)) = m$$

for each message  $m$ .

- Bob wants to send message  $m$  to Alice:
  - Bob takes the public key  $K_a$  of Alice and sends  $c = E_a(m)$  to Alice.
  - Alice can recover message  $m$  by computing

$$D_a(c) = D_a(E_a(m)) = m.$$

## Asymmetric Encryption



## Asymmetric Signature Method

- Suppose the *asymmetric signature method serving authentication* holds:

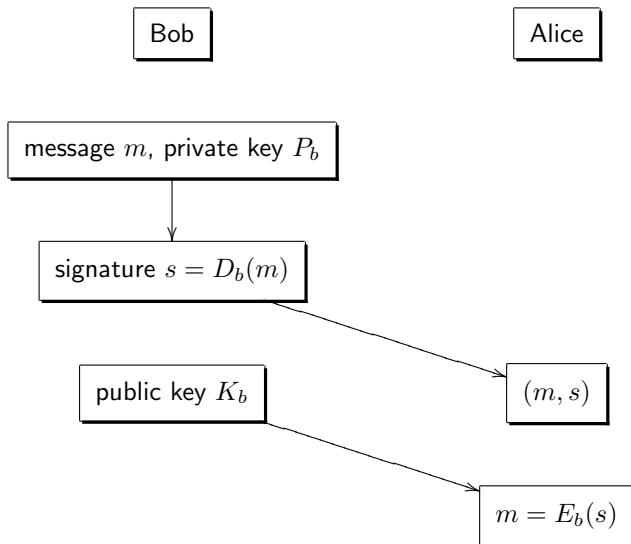
$$E_i(D_i(c)) = c$$

for each cipher  $c$ .

- Bob wants to send message  $m$  signed by his signature "bOb" to Alice.
  - Bob takes his private key  $P_b$ , computes the signature of the message  $s = D_b(m)$  and sends  $(m, s)$  to Alice.
  - Alice takes Bob's public key  $K_b$  to verify the signature by computing

$$E_b(s) = E_b(D_b(m)) = m.$$

## Asymmetric Signature Method



## Asymmetric Signature Method

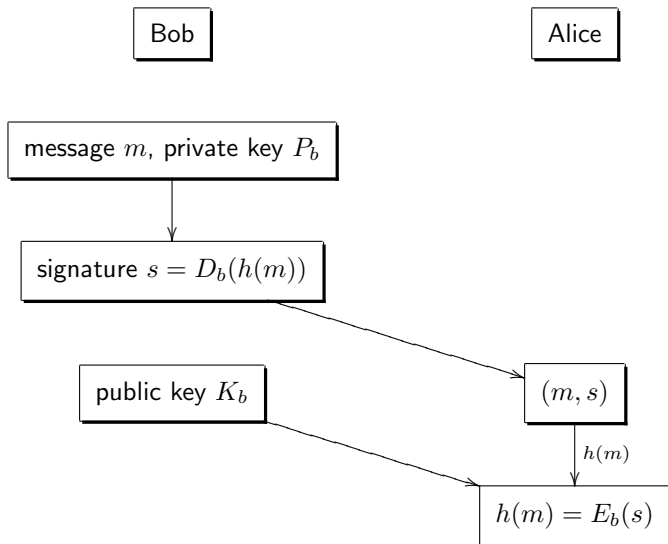
- Suppose the *asymmetric signature method serving authentication* holds:

$$E_i(D_i(c)) = c$$

for each cipher  $c$ .

- A hash function  $h$  is used to map message  $m$  of arbitrary size to fixed-length message  $h(m)$  before enciphering.
- Bob wants to send message  $m$  signed by his signature "bOb" to Alice.
  - Bob takes his private key  $P_b$ , computes the signature of the *fingerprinted* message  $s = D_b(h(m))$  and sends  $(m, s)$  to Alice.
  - Alice takes Bob's public key  $K_b$  to verify the signature by computing  $h(m)$  and comparing it with

$$E_b(s) = E_b(D_b(h(m))) = h(m).$$

Asymmetric Signature Method – Common Hash Function  $h$ 

## Hash Functions

A *hash function*  $h$  has the following properties:

- Applicable to messages of each size.
- Produces fixed-length output.
- For any message  $m$ ,  $h(m)$  is easy to compute.
- Given  $c$ , it is computationally infeasible to find  $m$  with  $h(m) = c$  (one-way property).
- Given  $x$ , it is computationally infeasible to find  $y$  with  $h(x) = h(y)$  (weak collision).

Today, hash functions in use are SHA-1 and MD5.

## One-Way Functions

An injective function  $f : X \rightarrow Y$  is a *one-way function* if the following holds:

- There is an efficient method to calculate  $f(x)$  for given  $x \in X$ .
- There is no efficient method to compute the inverse  $x \in X$  from given  $y \in \text{ran}(f)$ .

## One-Way Functions – Example

For a letter  $L$ , *some* name starting with  $L$  is looked up in the telephone dictionary of a large city, and a 7-digit telephone number listed under this name is the cryptotext.

Encryption of "kindergarten":

$k$	Koch	8202310	$g$	Greith	2730661
$i$	Ivanisevic	8119896	$a$	Aranyi	2603760
$n$	Nadler	6926286	$r$	Rexroth	5328563
$d$	Dicklberger	5702035	$t$	Tecins	6703008
$e$	Esau	8348578	$e$	Eisenhauer	7913174
$r$	Remy	7256575	$n$	Neunzig	3002123

Encryption is a sequence of twelve 7-digit codegroups:

8202310	8119896	6926286	5702035	8348578	7256575
2730661	2603760	5328565	6703008	7913174	3002123

Trapdoor is the (legally established) inverse dictionary.

## One-Way Functions

- One-way functions cannot be used in a reasonable way for encryption of messages followed up by decryption.
- One-way functions can be used for authentication.
  - A password is encrypted by a one-way function and stored in this form.
  - Any time access is required the password presented is encrypted and compared with the stored cryptotext (UNIX<sup>TM</sup> operating system).

## Trapdoor Functions

An injective function  $f : X \rightarrow Y$  is a *trapdoor function* if the following holds:

- There is an efficient method to compute  $f(x)$  for given  $x \in X$ .
- There is no efficient method to calculate the inverse  $x \in X$  from given  $y \in \text{ran}(f)$ , unless an additional secret information (trapdoor) is available.

## One-Way Function – Example

A one-way function without trapdoor: multiplication of primes.

Let  $X = \{(x_1, x_2) \mid x_1, x_2 \text{ prime}, K \leq x_1 \leq x_2\}$  for sufficiently large  $K$ . The injective function

$$f : X \rightarrow \mathbb{N} : (x_1, x_2) \mapsto x_1 \cdot x_2$$

is one-way (multiplication of large numbers takes only seconds).  
No trapdoors (factorization) are known.

## One-Way Function – Example

A one-way function without trapdoor: exponentiation in  $\mathbb{Z}_p$ .

Let  $p$  be a prime. For a fixed element  $a \in \mathbb{Z}_p^*$  define the  $a$ -exponential function

$$f_a : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^* : n \mapsto a^n \pmod{p}$$

for sufficiently large  $p$  and  $a$ .

The function  $f_a$  is one-way (fast modular exponentiation). No trapdoors (discrete logarithm) are known.

## Trapdoor One-Way Function – Example

Let  $e, n$  be positive integers.

- The exponentiation (RSA encryption)

$$f(m) = m^e \pmod n$$

is one-way (fast modular exponentiation).

- Given  $y = f(m) = m^e \pmod n$ . Trapdoor is the inverse of  $e \pmod{\phi(n)}$ , i.e.,

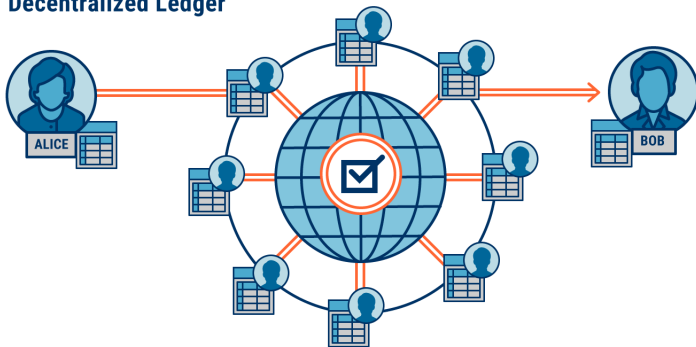
$$ed \equiv 1 \pmod{\phi(n)}.$$

Then

$$y^d = m^{ed} \equiv m \pmod n.$$

# Blockchain

## Decentralized Ledger

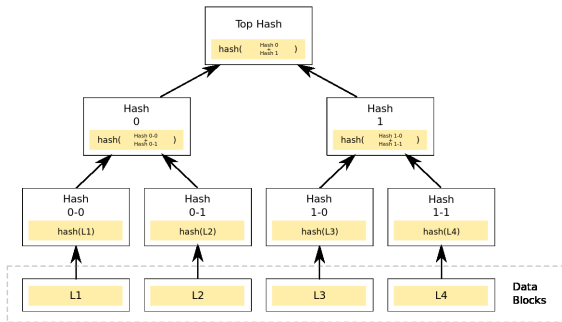


CBINSIGHTS

## Blockchain – Technology

- Continually extendable list of data records (blocks) linked using cryptography.
- Each block contains cryptographic hash of previous block, time stamp, and transaction data (represented by Merkle tree).
- Blockchain implements distributed ledger technology (consensus of replicated, shared and synchronized digital data geographically spread across multiple sites without central administration).
- First application: Bitcoin (Satoshi Nakamoto, 2008)

## Merkle Tree – Binary Hash Tree (1979)



- Hashes 0-0 and 0-1 are hash values of data blocks L1 and L2, resp.
- Hash 0 is the hash of the concatenation of the hashes 0-0 and 0-1, and so on.

## Blockchain – Properties

- Consensus mechanism: New blocks are added by decentral consensus (replaces trustworthy third party).
- Concatenation principle: Addition of new blocks via linked list.
- Decentral storage: Participants can store their own copy.
- Security against manipulation: Data in a block cannot be altered retroactively (requires consensus of network majority).
- Transparency: Blocks are visible to the participants, but content can be encrypted.
- Authentication: Blocks can use digital signatures.

## Cryptography – Breaking a Cryptosystem

Two types of information required:

- System structure (often leaks out over a period of time).
- Enciphering key (by frequency analysis of intercepted encrypted messages).

Deciphering is in my opinion one of the most fascinating of arts, and I fear I have wasted upon it more time than it deserves.

Charles Babbage, 1864

## Cryptography Axioms

- One should not underrate the adversary.
- Only the cryptanalyst, if anybody, can judge the security of a cryptosystem.
- A cryptosystem should be secure even if everything about the system except the key is public knowledge (Augustine Kerckhoff, 19th century). Equivalently, the enemy knows the system being used (Claude Shannon, 1949).
- Superficial complications can be illusory (e.g., Umkehrwalze in the Enigma).
- Cryptographic faults should be taken into account in judging the encryption security (e.g., probable words and phrases like "by order of the Führer", repetition of encrypted message in plain).

## Cryptography – Efficiency Boundary

- Technological progress shifts the border line between "intractable" and "efficient".
- Roughly, every two years the computer speed doubles and every 15 months the computer costs halve.
- Cryptologists counteract this by suitably increasing some of the encryption parameters.
- See the Wikipedia page "Integer factorization records".

# RSA

In cryptography, no rule is absolute.

Étienne Bazeris, 1901



Contents

History

RSA

Key Generation

Message  
Transmission

Correctness

Parameters

Attacks

Discrete Log

\* Attacking  
Discrete Log

\* Pseudoprimes

\* Factoring

## RSA

- RSA key generation
- Confidential message transmission
- RSA correctness
- RSA parameters
- Attacks against plain RSA

## RSA

- Inventors Ron Rivest, Adi Shamir, Leonard Adleman (1978)
- One of the first public-key cryptosystems
- Security relies on mathematical problems
- Usage in passing shared keys for symmetric key cryptography and digital signature

## Key Generation

Each user  $U$  generates a public/private key pair:

- Select two large primes at random,  $p$  and  $q$
- Compute the Eulerian totient value  $\phi(pq) = (p-1)(q-1)$
- Compute the system modulus  $n = p \cdot q$
- Select at random the encryption key  $e$ ,

$$1 < e < \phi(n) \quad \text{and} \quad (e, \phi(n)) = 1$$

- Calculate the decryption key  $d$ ,

$$0 \leq d \leq n \quad \text{and} \quad ed \equiv 1 \pmod{\phi(n)}.$$

Public encryption key  $U_P = (e, n)$  and secret decryption key  $U_R = \{d\}$ .

## Exercise (RSA)

- Choose randomly two primes  $p$  and  $q$  with arity  $\geq 100$ .
- Compute  $\phi(pq)$ .
- Choose randomly a prime  $e$  with arity  $\geq 20$ .
- Compute the inverse  $d$  of  $e$  in  $\mathbb{Z}_{\phi(pq)}$ .

## Exercise (RSA) – Solution

```
> with(numtheory):  
> r1 := rand(10^100..10^101):  
> a := r1():  
> p := nextprime(a):  
> b := r1():  
> q := nextprime(b):  
> pq_phi := (p-1)*(q-1):  
> r2 := rand(10^20..10^21):  
> c := r2():  
> e := nextprime(c):  
> igcdex(pq_phi,e,'r','s'):  
> d := modp(s,pq_phi):
```

## Exercise (RSA) – Toy Example

```
> with(numtheory):  
> r1 := rand(100..1000):  
> p := nextprime(r1());  
> q := nextprime(r1());
```

$$p = 163, \quad q = 439$$

```
> pq_phi := (p-1)*(q-1);
```

$$70956$$

```
> r2 := rand(10..100):  
> e := nextprime(r2());
```

$$e = 13$$

```
> igcdex(pq_phi, e, 'r', 's'):  
> d := modp(s, pq_phi);
```

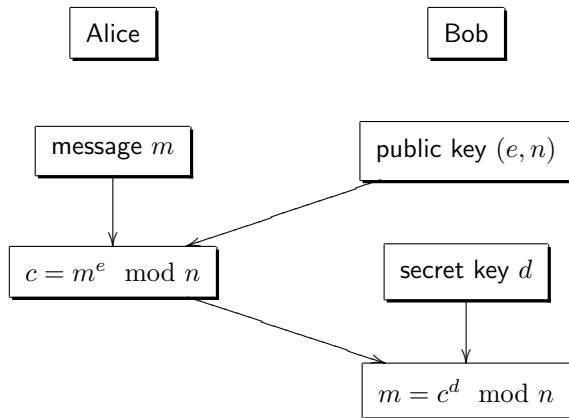
$$d = 32749$$

## RSA – Confidential Message Transmission

Alice has message  $m$  she wants to send to Bob.

- Alice encrypts the message  $m$ :
  - Alice obtains the public key of Bob:  $B_P = (e, n)$
  - Alice computes the ciphertext  $c = m^e \pmod n$ , where  $0 \leq m < n$
  - Alice sends the ciphertext  $c$  to Bob.
- Bob decrypts the ciphertext  $c$ :
  - Bob takes his private key  $B_R = \{d\}$ .
  - Bob computes  $m = c^d \pmod n$ .

## RSA – Confidential Message Transmission



## RSA – Correctness

For each  $m \in \mathbb{Z}_n$ ,

$$m^{ed} \equiv m \pmod{n}. \quad (1)$$

### Proof.

Since  $ed \equiv 1 \pmod{\phi(n)}$ ,  $ed = 1 + k\phi(n)$  for some integer  $k$ .

- Let  $(m, n) = 1$ . Then by Euler's theorem,

$$m^{ed} = m^{1+k\phi(n)} = m \left( m^{\phi(n)} \right)^k = m \cdot 1^k = m.$$

- Let  $(m, n) \neq 1$ . Then  $p|m$  or  $q|m$ . Take the ring isomorphism

$$\psi : \mathbb{Z}_n \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q : m \mapsto (m \pmod{p}, m \pmod{q}).$$

Suppose  $p|m$ ,  $q \nmid m$ . Then  $\psi(m^{ed}) = (0, m^{ed} \pmod{q}) = (0, m \pmod{q}) = (m \pmod{p}, m \pmod{q}) = \psi(m)$  as in the first case and so  $m^{ed} \equiv m \pmod{n}$ .  $\square$

## RSA – Parameters

Let  $n$  be the product of two primes. Then knowing  $\phi(n)$  is sufficient to recover both primes.

### Proof.

Let  $n = pq$  with primes  $p$  and  $q$ . Then

$$n - \phi(n) + 1 = n - (p-1)(q-1) + 1 = n - pq + p + q - 1 + 1 = p + q.$$

Suppose  $p > q$ . Then

$$p - q = \sqrt{(p-q)^2} = \sqrt{(p+q)^2 - 4n}.$$

Thus  $p + q$  and  $p - q$  are known and so

$$\begin{aligned} p &= \frac{1}{2}[(p+q) + (p-q)], \\ q &= \frac{1}{2}[(p+q) - (p-q)]. \end{aligned}$$



## RSA – Parameters

- The numbers  $p - 1$  and  $q - 1$  should have only very small common factors, besides the necessary 2.

Indeed, any common factors of  $p - 1$  and  $q - 1$  are present in the factorization of  $n - 1$ , since

$$n - 1 = pq - 1 = (p - 1)(q - 1) + (p - 1) + (q - 1).$$

- Use of small value for  $e$  with small number of binary digits, such as the Fermat prime

$$2^{2^4} + 1 = 65537,$$

speeds up the encryption process.

Indeed, exponentiation can be computed by the Horner scheme.

## Security of RSA

The security of RSA cryptosystem is based on two mathematical problems:

- Factorization of large numbers.
- Computation of discrete logarithm (RSA problem).

No efficient algorithms exist for solving them.

Practical RSA implementations prepare message  $m$  by using structured randomized padding before encryption.

## Attacks against plain RSA

- Small exponents (e.g.,  $e = 3$ ) and small values of  $m$  (e.g.,  $m < n^{1/e}$ ) give  $m^e < n$ . Decryption of  $c$  may be possible by taking its  $e$ -th root.
- Send the same encryption of  $m$  to  $\geq e$  users with same encryption key  $e$  but different  $p, q$  and therefore  $n$ . The Chinese Remainder theorem may be used for decryption.
- Encrypt likely plaintexts under the public key and test if they are equal to the ciphertext (chosen plaintext attack).

Avoid plain RSA attacks by using a padding scheme such as the standard PKCS#1.

## Discrete Log

Even in cryptology, silence is golden.

Laurence D. Smith

## Discrete Log

- Definition of discrete logarithm
- Diffie-Hellman key exchange
- Massey-Omura cryptosystem
- ElGamal cryptosystem

## Discrete Log

- Given finite group  $G$ ,  $g \in G$ , and  $y \in G$  which is a power of  $g$ . The *discrete logarithm* of  $y$  to base  $g$  is any integer  $x$  such that

$$g^x = y.$$

Write  $x = \log_g y$  for the minimum integer  $x \geq 0$ .

- Special case:* Given finite cyclic group  $G$ , a generator  $g$  of  $G$  and  $y \in G$ . The *discrete logarithm* of  $y$  to base  $g$  is any integer  $x$  such that

$$g^x = y.$$

Write  $x = \log_g y$  for the minimum integer  $x \geq 0$ .

*Example:* The multiplicative group of each finite field  $\mathbb{F}_q$  is cyclic:  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ .

## Example

The cyclic group  $G = \mathbb{F}_{19}^* = \mathbb{Z}_{19}^*$  is generated by  $b = 2$ ,

$$\begin{array}{ll} 2^1 = 2, & 2^2 = 4, \\ 2^3 = 8, & 2^4 = 16, \\ 2^5 = 13, & 2^6 = 7, \\ 2^7 = 14, & 2^8 = 9, \\ 2^9 = 18, & 2^{10} = 17, \\ 2^{11} = 15, & 2^{12} = 11, \\ 2^{13} = 3, & 2^{14} = 6, \\ 2^{15} = 12, & 2^{16} = 5, \\ 2^{17} = 10, & 2^{18} = 1. \end{array}$$

Thus  $\log_2 7 = 6$ .

## Example

Take the cyclic group  $G = \mathbb{F}_8^*$  generated by the root  $\alpha$  of  $X^3 + X + 1 \in \mathbb{F}_2[X]$ . Since  $\alpha^3 + \alpha + 1 = 0$ , i.e.,  $\alpha^3 = \alpha + 1$ , the elements of  $G$  are

$$\begin{aligned}\alpha^0 &= 1 \\ \alpha^1 &= \alpha \\ \alpha^2 &= \alpha^2 \\ \alpha^3 &= \alpha + 1 \\ \alpha^4 &= \alpha^2 + \alpha \\ \alpha^5 &= \alpha^2 + \alpha + 1 \\ \alpha^6 &= \alpha^2 + 1 \\ \alpha^7 &= 1.\end{aligned}$$

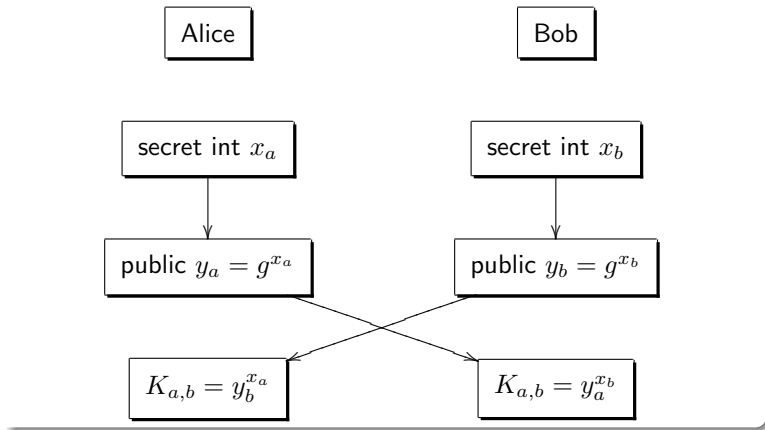
Thus  $\log_{\alpha}(\alpha^2 + \alpha) = 4$ .

## Diffie-Hellman Key Exchange (1976)

- Alice and Bob agree on large finite group  $G$  and element  $g \in G$  of order  $n$  (public).
- Alice takes secret integer  $x_a$  with  $1 \leq x_a \leq n - 1$  and computes public  $y_a = g^{x_a} \in G$ .
- Bob takes secret integer  $x_b$  with  $1 \leq x_b \leq n - 1$  and computes public  $y_b = g^{x_b} \in G$ .
- Alice and Bob establish common secret key:
  - Alice computes  $y_b^{x_a}$ .
  - Bob computes  $y_a^{x_b}$ .
  - Common secret key  $K_{a,b} = g^{x_a x_b}$ .
- Correctness:

$$y_b^{x_a} = (g^{x_b})^{x_a} = K_{a,b} = (g^{x_a})^{x_b} = y_a^{x_b}.$$

## Diffie-Hellman Key Exchange



## Diffie-Hellman Key Exchange

- *Diffie-Hellman assumption*: It is computationally infeasible to compute  $K_{a,b} = g^{x_a x_b}$  when the eavesdropper only knows the transmitted messages

$$y_a = g^{x_a} \quad \text{and} \quad y_b = g^{x_b}.$$

- Discrete logarithms:

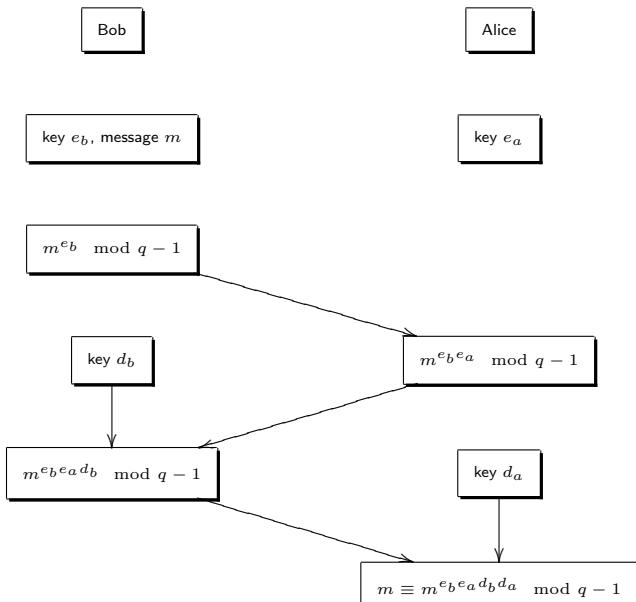
$$x_a = \log_g y_a \quad \text{and} \quad x_b = \log_g y_b.$$

If discrete logarithms are computable, the Diffie-Hellman assumption will fail.

## Massey-Omura Cryptosystem (1993)

- Public data: large prime power  $q$ .
- Each user takes secret random integer  $e$ ,  $1 \leq e \leq q - 1$ , with  $(e, q - 1) = 1$  and computes its inverse  $d = e^{-1} \pmod{q - 1}$ ; i.e.,  $ed \equiv 1 \pmod{q - 1}$ .
- Bob has message  $m$ ,  $0 \leq m < q$ , and communicates with Alice:
  - Bob sends  $m^{e_b} \pmod{q - 1}$  to Alice.
  - Alice sends  $m^{e_b e_a} \pmod{q - 1}$  back.
  - Bob sends  $m^{e_b e_a d_b} = m^{e_a} \pmod{q - 1}$  back.
  - Alice computes  $m^{e_a d_a} \equiv m \pmod{q - 1}$ .
- Correctness follows from (1).
- Security is based on computing discrete logarithms.
- Method is rarely used in practice.

# Massey-Omura Cryptosystem



## ElGamal Cryptosystem (1985)

- Public data: large prime power  $q$  and generator  $g \in \mathbb{F}_q^*$ .
- Each user takes random private key  $x_u$  with  $1 \leq x_u \leq q - 1$  and computes public key  $y_u = g^{x_u}$ .
- Bob wants to send message  $m$ ,  $0 \leq m < q$ , to Alice:
  - Bob chooses random number  $r$  with  $1 \leq r \leq q - 1$  and sends  $(g^r, m \cdot y_a^r)$  to Alice.
  - Alice computes  $s = (g^r)^{x_a} = g^{rx_a}$ .
  - Alice recovers message:

$$(m \cdot y_a^r) \cdot s^{-1} = m \cdot (g^{x_a r}) \cdot (g^{rx_a})^{-1} = m.$$

Direct computation of inverses:

$$(g^a)^{-1} = g^{q-1-a}, \quad 1 \leq a \leq q - 1.$$

- Security is based on computing discrete logarithms.

## ElGamal Cryptosystem

Bob

Alice

private  $x_b$ , public  $y_b = g^{x_b}$ message  $m$ , random  $r$ private  $x_a$ , public  $y_a = g^{x_a}$  $(g^r, m \cdot y_a^r)$  $s = (g^r)^{x_a}, m = (m \cdot y_a^r) \cdot s^{-1}$

## Attacking Discrete Logarithm

Deciphering is an affair of time,  
ingenuity, and patience.

Charles Babbage, 1864

## Attacking Discrete Logarithm

- Complete enumeration
- Baby-step giant-step algorithm
- Pohlig-Hellman algorithm
- Pollard's rho method

## Complete Enumeration

The simplest attacking method is complete enumeration.

**Require:** Given cyclic group  $G$  of order  $n$ , generator  $g$  and group element  $y$ .

**Ensure:** Integer  $x$  with  $y = g^x$ .

```
for  $x \leftarrow 1$  to  $n$  do
```

```
  if  $y = g^x$  then
```

```
    return  $x$ 
```

```
  end if
```

```
end for
```

This attack is extremely time-consuming. The other attacks here are much quicker.

## Baby-Step Giant-Step Algorithm (1978)

Meet-in-the-middle algorithm for computing the discrete logarithm.

- Given cyclic group  $G$  of order  $n$ , generator  $g$  and group element  $y$ . Find an integer  $x$  with  $y = g^x$ .
- The BSGS algorithm is based on rewriting  $x$  as  $x = qm + r$  with  $m = \lceil \sqrt{n} \rceil$  and  $0 \leq r \leq m - 1$ .
- *Baby steps*: compute list of pairs  $(y \cdot g^{-r}, r)$ ,  $0 \leq r \leq m - 1$ , in table; for fast retrieval use hash table or binary search in sorted array.
- *Giant steps*: compute  $g^{qm}$  for  $1 \leq q \leq m - 1$ .
- Time complexity  $O(\sqrt{n})$ .

## Baby-Step Giant-Step Algorithm

**Require:** Cyclic group  $G$  of order  $n$  with generator  $g$ , group element  $y$ .

**Ensure:** Integer  $x$  with  $g^x = y$ .

$$m \leftarrow \lceil \sqrt{n} \rceil$$

**for**  $r \leftarrow 0$  to  $m - 1$  **do**

    store pairs  $(y \cdot g^{-r}, r)$  in table

**end for**

**if**  $y \cdot g^{-r} = 1$  for some  $r$  **then**

**return**  $x \leftarrow r$

**end if**

**for**  $q \leftarrow 1$  to  $m - 1$  **do**

**if**  $g^{qm}$  equals the first element  $y \cdot g^{-r}$  in list **then**

**return**  $x \leftarrow qm + r$

**end if**

**end for**

## Baby-Step Giant-Step Algorithm – Example

```
> n:=19: g:=2: y:=15: m:=4:  
> for r from 0 to m-1 do print(modp(y/g^r,n)) end do;  
15  
17  
18  
9  
> for q from 1 to m do print(modp(g^(q*m),n)) end do;  
16  
9  
11  
5  
> q:=2: r:= 3: x:=q*m+r; modp(g^x,n);  
11  
15
```

## Pohlig-Hellman Algorithm (1978)

Computation of discrete logarithms in finite abelian group whose order is a smooth integer.

- A *smooth integer* is an integer that factors completely into small prime numbers.
- Special algorithm for cyclic groups with prime-power order.
- General algorithm for cyclic groups using the Chinese Remainder theorem.

## Pohlig-Hellman Algorithm

Given cyclic group  $G$  of order  $n = p^e$  with generator  $g$ , group element  $y$  with  $y = g^x$  and  $x$ ,  $0 \leq x \leq n - 1$ , unknown.

- Put  $h = g^{n/p} = g^{p^{e-1}}$  and  $y_0 = y^{n/p}$ .
- Then  $y_0 = (g^x)^{n/p} = h^x$  and  $h$  has order  $p$ , i.e.,  $h^p = 1$ .
- If the discrete log problem is solvable in  $\langle h \rangle$ , there is  $x_0$ ,  $0 \leq x_0 \leq p - 1$ , with

$$y_0 = h^{x_0}.$$

## Pohlig-Hellman Algorithm

- Consider the  $p$ -adic expansion of  $x$ ,  $0 \leq x \leq p^e - 1$ ,

$$x = x_0 + x_1p + \dots + x_{e-1}p^{e-1}$$

with  $0 \leq x_0, \dots, x_{e-1} \leq p - 1$ .

- Use  $y = g^{x_0 + x_1p + \dots + x_{e-1}p^{e-1}}$  to compute

$$\begin{aligned} y_j &= \left( y \cdot g^{-(x_0 + \dots + x_{j-1}p^{j-1})} \right)^{n/p^{j+1}} \\ &= \left( g^{x_j p^j + \dots + x_{e-1} p^{e-1}} \right)^{n/p^{j+1}} \\ &= (g^{x_j})^{n/p} = h^{x_j}, \end{aligned}$$

where  $h = g^{n/p}$  has order  $p$ .

- If the discrete log problem is solvable in  $\langle h \rangle$ , there is  $x_j$ ,  $0 \leq x_j \leq p - 1$ , with  $y_j = h^{x_j}$ .

## Pohlig-Hellman Algorithm (PH I)

**Require:** Cyclic group  $G$  of order  $n = p^e$  with generator  $g$ , group element  $y$ .

**Ensure:** Unique integer  $x$ ,  $0 \leq x \leq n - 1$ , with  $g^x = y$ .

$$y_0 \leftarrow y^{n/p}$$

$$h \leftarrow g^{n/p}$$

Use BSGS algorithm to compute  $x_0$ ,  $0 \leq x_0 \leq p - 1$ , with

$$h^{x_0} = y_0$$

$$x \leftarrow x_0$$

**for**  $j \leftarrow 1$  to  $e - 1$  **do**

$$y_j \leftarrow \left( y \cdot g^{-(x_0 + \dots + x_{j-1} p^{j-1})} \right)^{n/p^{j+1}}$$

$$h \leftarrow g^{n/p}$$

Use BSGS algorithm to compute  $x_j$ ,  $0 \leq x_j \leq p - 1$ , with

$$h^{x_j} = y_j$$

$$x \leftarrow x + p^j x_j$$

**end for**

**return**  $x$

## Pohlig-Hellman Algorithm (PH II)

**Require:** Cyclic group  $G$  of order  $n$  with generator  $g$ , group element  $y$ , and factorization  $n = \prod_{i=1}^r p_i^{e_i}$ .

**Ensure:** Unique integer  $x$ ,  $0 \leq x \leq n - 1$ , with  $g^x = y$ .

**for**  $i \leftarrow 1$  to  $r$  **do**

$g_i \leftarrow g^{n/p_i^{e_i}}$  { $g_i$  has order  $p_i^{e_i}$ }

$y_i \leftarrow y^{n/p_i^{e_i}}$  { $y_i \in \langle g_i \rangle$ }

Use algorithm PH I in  $H_i = \langle h_i \rangle$  to compute  $x_i$  with  $h_i^{x_i} = y_i$

**end for**

Solve the simultaneous congruences  $x \equiv x_i \pmod{p_i^{e_i}}$  for

$1 \leq i \leq r$  {The CRT gives a unique solution  $x$  with

$0 \leq x \leq n - 1$ .}

**return**  $x$

## Pollard's rho Method (1975)

Computation of discrete logarithms in finite abelian group.

- Special algorithm for cyclic groups with prime-power order.
- General algorithm for cyclic groups similar to Pohlig-Hellman.
- Time complexity  $O(\sqrt{n})$  but needs less space than BSGS.

## Pollard's rho Method

Given cyclic group  $G$  of order  $n = p^e$  with generator  $g$ , group element  $y$  with  $y = g^x$ ,  $0 \leq x \leq n - 1$ , unknown.

- Compute elements

$$h_i = g^{a_i} \cdot y^{b_i}, \quad 1 \leq i \leq s,$$

where  $a_i, b_i$  are random integers.

- Take surjective function  $f : G \rightarrow \{1, \dots, s\}$  partitioning  $G$  into disjoint subsets

$$G_i = f^{-1}(\{i\}), \quad 1 \leq i \leq s.$$

- Use starting point

$$z_0 = g^{u_0} \cdot y^{v_0}$$

to define the sequence

$$z_{l+1} = z_l \cdot h_{f(z_l)}, \quad l \geq 0.$$

## Pollard's rho Method

- Each element  $z_l$  has the form

$$z_l = g^{u_l} \cdot y^{v_l}, \quad l \geq 0.$$

- Since  $G$  is finite, there are indices  $l < m$  with  $z_l = z_m$ . Then

$$g^{u_l - u_m} = y^{v_m - v_l} = g^{(v_m - v_l)x}.$$

Thus

$$u_l - u_m \equiv (v_m - v_l)x \pmod{n}.$$

- If  $(v_m - v_l, n) = 1$ , then  $v_m - v_l$  is invertible in  $\mathbb{Z}_n$  and so

$$x = (u_l - u_m) \cdot (v_m - v_l)^{-1}.$$

## Pollard's rho Method

- If  $d = (v_m - v_l, n) > 1$ , then  $(v_m - v_l)/d$  is invertible in  $\mathbb{Z}_n$  and so for some integer  $v'$ ,  $v'(v_m - v_l) \equiv d \pmod n$ .
- Since  $u_l - u_m \equiv (v_m - v_l)x \pmod n$  and  $v_m - v_l$  is multiple of  $d$ ,  $u_l - u_m$  is a multiple of  $d$ , i.e.,  $u_l - u_m = du'$  for some integer  $u'$ .
- Thus  $du'v' \equiv dx \pmod n$  and hence

$$x \equiv u'v' + k\frac{n}{d} \pmod n$$

for some  $k = 0, \frac{n}{d}, \dots, (d-1)\frac{n}{d}$ .

- If  $d$  is too large, take new starting point.
- The (smallest) equality  $z_l = z_m$  can be expected after  $O(\sqrt{n})$  steps.

## Pseudoprimes

Today, the Department of Computer Science at the University of Washington announced that  $2^{58,111,625,031} + 8$  is even. This is the largest non-prime yet reported.

Bathroom graffiti, University of Washington

The largest known prime number is  $2^{77,232,916} - 1$ , a Mersenne number with 23,249,425 digits.

January, 2018

## Pseudoprimes

- Trial division
- Pseudoprimes
- Carmichael numbers
- Strong pseudoprimes
- Rabin-Miller test

## Trial Division

The simplest primality test is trial division.

**Require:** Odd positive integer  $n$ .

**Ensure:** Return 1 if  $n$  is prime, otherwise 0.

```
for  $m = 3$  to  $\lfloor \sqrt{n} \rfloor$  by 2 do
  if  $m$  divides  $n$  then
    return 0
  end if
end for
return 1
```

This test is extremely time-consuming. The other tests here are much quicker.

## Pseudoprimes

Given odd composite number  $n$  and integer  $b$ . Then  $n$  is a *pseudoprime to base  $b$*  if  $(n, b) = 1$  and

$$b^{n-1} \equiv 1 \pmod{n}. \quad (2)$$

If  $n$  is not prime, (2) is not very likely.

## Fermat's Little Theorem

If  $n$  is prime, then for each integer  $b$  with  $(n, b) = 1$ ,

$$b^{n-1} \equiv 1 \pmod{n}. \quad (3)$$

## Example

- $n = 91$  is a pseudoprime to base 3, since  $3^{90} \equiv 1 \pmod{91}$ .
- $n = 91$  is not a pseudoprime to base 2, since  $2^{90} \equiv 64 \pmod{91}$ .

## Pseudoprimes

Let  $n$  be an odd composite integer.

- If  $n$  is a pseudoprime to base  $b$ , then  $b \in \mathbb{Z}_n^*$  and the order of  $b$  in  $\mathbb{Z}_n^*$  divides  $n - 1$ .
- If  $n$  is a pseudoprime to bases  $b_1$  and  $b_2$ , then  $n$  is a pseudoprime to base  $b_1 b_2$  and also to base  $b_1^{-1}$ .
- If  $n$  fails the test (2) for some base  $b \in \mathbb{Z}_n^*$ , then  $n$  fails for at least half of the possible bases in  $\mathbb{Z}_n^*$ .

## Proof (Part 3).

- Let  $\{b_1, \dots, b_s\}$  be the set of bases for which  $n$  is a pseudoprime.
- Let  $b$  be an integer for which  $n$  is not a pseudoprime.
- Then  $n$  cannot be a pseudoprime for any of the bases

$$bb_1, \dots, bb_s.$$

If  $n$  were a pseudoprime for  $bb_i$ , then (by part 2)  $n$  would be a pseudoprime for base  $b \equiv (bb_i)b_i^{-1} \pmod{n}$ .

- So there are at least as many bases in  $\mathbb{Z}_n^*$  for which  $n$  fails to be a pseudoprime as there are bases for which (2) holds.



## \*Carmichael Numbers (1910)

A *Carmichael number* is a composite integer  $n$  such that

$$b^{n-1} \equiv 1 \pmod{n} \quad (4)$$

holds for each  $b \in \mathbb{Z}_n^*$ .

- If  $n$  is a square-free odd composite integer, then  $n$  is a Carmichael number iff  $p - 1 \mid n - 1$  for each prime dividing  $n$ .
- Each Carmichael number is the product of at least three distinct primes.
- $n = 561 = 3 \cdot 11 \cdot 17$  is the (smallest) Carmichael number, since 560 is divisible by  $3 - 1$ ,  $11 - 1$ , and  $17 - 1$ .
- There are infinitely many Carmichael numbers.
- No Carmichael number is a strong pseudoprime and so a strong probable prime test could prove that a Carmichael number is composite.

## Strong Pseudoprimes

Given odd composite integer  $n$  with

$$n - 1 = 2^s t, \quad t \text{ odd.} \quad (5)$$

Let  $b \in \mathbb{Z}_n^*$ . Then  $n$  is a *strong pseudoprime to base  $b$*  if either

$$b^t \equiv 1 \pmod{n} \quad (6)$$

or there exists  $r$ ,  $0 \leq r < s$ , with

$$b^{2^r t} \equiv -1 \pmod{n}. \quad (7)$$

## Strong Pseudoprimes – Example

- $n = 2047$  is a strong pseudoprime to base 2, since  $2046 = 2 \cdot 1023$  and  $2^{1023} \equiv 1 \pmod{2047}$ .
- $n = 121$  is a strong pseudoprime to base 3, since  $120 = 2^3 \cdot 15$  and  $3^{15} \equiv 1 \pmod{121}$ .
- Let  $n = 91$ ,  $90 = 2 \cdot 45$ . Here  $n$  is a strong pseudoprime for the bases  
9, 16, 22, 53, 74, 79, 81.

## Miller-Rabin Primality Test

Decide whether a large odd integer  $n > 0$  is prime or composite.

- Consider the sequence modulo  $n$ ,

$$(b^t, b^{2t}, \dots, b^{2^{s-1}t}, b^{2^s t}).$$

- If  $n$  is prime, then by Euler's theorem,

$$b^{2^s t} = b^{n-1} \equiv 1 \pmod{n}$$

and the sequence ends with 1.

- If  $n$  is prime,  $x^2 \equiv 1 \pmod{n}$  iff  $x \equiv \pm 1 \pmod{n}$  and so the penultimate sequence position is  $\pm 1$ .
- Test if the sequence begins with 1 or has  $\pm 1$  at least at the penultimate position. If so,  $n$  is prime or a strong pseudoprime to base  $b$ .

## Miller-Rabin Primality Test

- If  $n$  is an odd composite, then  $n$  is a strong pseudoprime to base  $b$  for at most 25% of all  $0 < b < n$ ; i.e., the probability that  $n$  passes the test is  $< \frac{1}{4}$ .
- Repeating the test for  $k$  independently chosen numbers  $b$  with  $0 < b < n$ , the probability that  $n$  passes the test is  $< \frac{1}{4^k}$ .
- For many odd composite numbers, the fraction of bases passing the test is much smaller than  $\frac{1}{4}$ .

## Factoring

The work of the professional cryptologist is thankless; he is not allowed to celebrate his success in public ... Such restrictions usually persist even after active duty.

F.L. Bauer, 2000

## Factoring

- Fermat factoring
- Factor bases
- Continued fractions
- Quadratic sieve

## Fermat Factoring

Let  $n$  be a positive odd integer. There is a 1-to-1 correspondence between factorizations of  $n = pq$ , where  $p \geq q > 0$ , and representations of  $n$  in the form  $u^2 - v^2$ , where  $u, v$  are non-negative integers.

The correspondence is given by

$$u = \frac{p+q}{2}, \quad v = \frac{p-q}{2}, \quad p = u+v, \quad q = u-v. \quad (8)$$

Note that if  $p$  and  $q$  are close together, then  $v = (p-q)/2$  is small and so  $u$  is only slightly larger than  $\sqrt{n}$ .

### Example

$n = 200819$  factors into  $n = 491 \cdot 409$  and has the representation  $n = 450^2 - 41^2$ .

## Fermat Factoring – Algorithm

Fermat's factoring works well if  $n$  is a product of two primes close to each other.

**Require:** Odd positive integer  $n$  with  $n = pq$  and  $p, q$  primes close together.

**Ensure:** Values  $p, q$

$$u \leftarrow \lfloor \sqrt{n} \rfloor + 1$$

**repeat**

$$u \leftarrow u + 1$$

**until**  $u^2 - n$  is a perfect square

$$v \leftarrow \sqrt{u^2 - n}$$

$$p \leftarrow u + v$$

$$q \leftarrow u - v$$

**return**  $p, q$

## Fermat Factoring – Example

Let  $n = 200819$ .

- Take  $u = \lfloor \sqrt{200819} \rfloor + 1 = 449$ . Then  $449^2 - 200819 = 782 = 2 \cdot 17 \cdot 23$ , not perfect square.
- Take  $u = 449 + 1 = 450$ . Then  $450^2 - 200819 = 1681 = 41^2$ , perfect square. Thus

$$u = 450, \quad v = 41, \quad p = 491, \quad q = 409.$$

## Factor Bases (1974)

- A *factor basis* is a set  $B = \{p_1, \dots, p_h\}$  of distinct primes, except  $p_1 = -1$ .
- Let  $n \geq 2$  (modulus). A square of an integer  $b$  is a *B-number* for  $n$  if the least absolute residue  $b^2 \bmod n$  can be written as a product of numbers from  $B$ .
- The *least absolute residue* of a number  $a$  modulo  $n$  is the integer from the interval  $-n/2$  to  $n/2$  to which  $a$  is congruent, written  $a \bmod n$ .

## Example

Let  $n = 4633$  and  $B = \{-1, 2, 3\}$ . The squares of 67, 68, and 69 are *B-numbers* for  $n$ , since  $67^2 \equiv -144 \bmod 4633$ ,  $68^2 \equiv -9 \bmod 4633$ , and  $69^2 \equiv 128 \bmod 4633$ , with  $-144 = (-1)2^4 3^2$ ,  $-9 = (-1)3^2$ , and  $128 = 2^7$ .

## Factor Bases

Given  $n$  and factor basis  $B = \{p_1, \dots, p_h\}$ .

- Write each  $B$ -number  $a = b^2 \pmod n$  as

$$a = \prod_{j=1}^h p_j^{\alpha_j}, \quad \alpha_j \geq 0. \quad (9)$$

- For  $B$ -number  $a = b^2 \pmod n$  define  $\epsilon_b = (\epsilon_{b1}, \dots, \epsilon_{bh}) \in \mathbb{F}_2^h$  as

$$\epsilon_{bj} = \begin{cases} 0 & \text{if } \alpha_j \text{ in } b^2 \text{ is even,} \\ 1 & \text{otherwise.} \end{cases} \quad (10)$$

## Factor Bases – Example

Let  $n = 4633$  and  $B = \{-1, 2, 3\}$ .

- For 67,  $-144 = (-1) \cdot 2^4 \cdot 3^2$  and so  $\epsilon_{67} = (1, 0, 0)$ .
- For 68,  $-9 = (-1) \cdot 3^2$  and so  $\epsilon_{68} = (1, 0, 0)$ .
- For 69,  $128 = 2^7$  and so  $\epsilon_{69} = (0, 1, 0)$ .

## Factor Bases

Given  $n$  and factor basis  $B = \{p_1, \dots, p_h\}$ .

- If  $b_1^2 \bmod n$  and  $b_2^2 \bmod n$  are  $B$ -numbers, then  $(b_1 b_2)^2 \bmod n$  is a  $B$ -number.
- The set of all  $B$ -numbers forms an additive subgroup of  $\mathbb{F}_2^h$ , since multiplying  $B$ -numbers means adding the corresponding binary vectors (in the exponents).

## Factor Bases

Given  $n$  and factor basis  $B = \{p_1, \dots, p_h\}$ .

Suppose the squares of the numbers  $b_1, \dots, b_s$  are  $B$ -numbers for  $n$ , where

$$a_i = b_i^2 \bmod n = \prod_{j=1}^h p_j^{\alpha_{ij}}. \quad (11)$$

Table:

	$p_1$	$\dots$	$p_j$	$\dots$	$p_h$
$b_1^2 \bmod n$	$\alpha_{11}$	$\dots$	$\alpha_{1j}$	$\dots$	$\alpha_{1h}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$b_i^2 \bmod n$	$\alpha_{i1}$	$\dots$	$\alpha_{ij}$	$\dots$	$\alpha_{ih}$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$b_s^2 \bmod n$	$\alpha_{s1}$	$\dots$	$\alpha_{sj}$	$\dots$	$\alpha_{sh}$

## Factor Bases

Take  $B$ -numbers for  $n$ ,

$$a_{i_1} = b_{i_1}^2 \bmod n, \dots, a_{i_k} = b_{i_k}^2 \bmod n, \quad (12)$$

whose corresponding binary vectors add up to the zero vector in the space  $\mathbb{F}_2^h$ . Write  $a_{i_l} = \prod_{j=1}^h p_j^{\alpha_{i_l j}}$ ,  $1 \leq l \leq k$ . Then

$$\prod_{l=1}^k a_{i_l} = \prod_{j=1}^h p_j^{\sum_{l=1}^k \alpha_{i_l j}} \quad (13)$$

and each sum  $\sum_l \alpha_{i_l j}$  is even.

## Factor Bases

Write

$$b = b_{i_1} \dots b_{i_l} \pmod n \quad (14)$$

and

$$c = \prod_{j=1}^h p_j^{\sum_{l=1}^k \alpha_{i_l j} / 2} \pmod n. \quad (15)$$

Then by (13),

$$b^2 \equiv c^2 \pmod n. \quad (16)$$

## Factor Bases

Let  $b^2 \equiv c^2 \pmod n$ .

- If  $b \not\equiv \pm c \pmod n$ , we find a factor of  $n$  by computing  $(b + c, n)$  or  $(b - c, n)$ .

Indeed,  $n$  divides  $b^2 - c^2 = (b + c)(b - c)$ . But by hypothesis,  $n$  does not divide  $b + c$  or  $b - c$ . Thus  $(b + c, n)$  or  $(b - c, n)$  must be a proper factor of  $n$ .

- If  $b \equiv \pm c \pmod n$ , there is no further information.

## Factor Bases – Example

Let  $n = 4633$ .

- Take  $B = \{-1, 2, 3\}$ .
- The squares of 67, 68 and 69 are  $B$ -numbers for  $n$ ; these numbers are close to  $\sqrt{4633} = 68.067$ .
- The squares of 67, 68 and 69 are  $B$ -numbers for  $n$ , since

$$67^2 \equiv -144 \pmod{4633},$$

$$68^2 \equiv -9 \pmod{4633},$$

$$69^2 \equiv 128 \pmod{4633}.$$

- Table:

	-1	2	3	$\epsilon$
-144	1	4	2	(1, 0, 0)
-9	1	2	0	(1, 0, 0)
128	0	7	0	(0, 1, 0)

## Factor Bases – Example (cont'd)

- The first two binary vectors are both  $(1, 0, 0)$  and add up to the zero vector.
- Compute  $b = 67 \cdot 68 \bmod 4633 = -77$ .
- Compute  $c = 2^{4/2}3^{4/2} = 36$ , where  $(-144) \cdot (-9) = 2^43^4$ .

- Then

$$-77^2 \equiv 36^2 \bmod 4633.$$

- We have  $-77 \not\equiv \pm 36 \bmod 4633$  and so

$$(-77 + 36, 4633) = 41$$

gives a factor of 4633.

## Factor Bases – Example

Let  $n = 1829$ .

- Take as  $b_i$  the integers of the form  $\lfloor \sqrt{1829 \cdot k} \rfloor$  and  $\lfloor \sqrt{1829 \cdot k} \rfloor + 1$  for  $k = 1, 2, 3, 4$  such that  $b_i^2 \bmod n$  is a product of primes  $\leq 19$ .
- Write  $b_i^2 \bmod n = \prod_j p_j^{\alpha_{ij}}$  and tabulate the  $\alpha_{ij}$ :

	-1	2	3	5	7	11	13	19
42	1			1			1	
43		2		1				
61			2		1			
74	1					1		
85	1				1		1	
86		4		1				

## Factor Bases – Example (cont'd)

Let  $n = 1829$ .

- The 2nd and 6th row sum to the even row  $-6 - 2 - \dots$ .
- Thus  $b = b_2 \cdot b_6 \pmod n$  and  $c = 2^{6/2} 5^{2/2} \pmod n$  and hence

$$(43 \cdot 86)^2 \equiv 40^2 \pmod{1829}.$$

- Since  $43 \cdot 86 \equiv 40 \pmod{1829}$ , resume with another even row sum.

## Factor Bases – Example (cont'd)

Let  $n = 1829$ .

- The 1st, 2nd, 3rd, and 5th row sum up to  $22222 - 2$ .

- Thus

$$(42 \cdot 42 \cdot 61 \cdot 85)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)^2 \pmod{1829},$$

i.e.,  $1459^2 \equiv 901^2 \pmod{1829}$ .

- Since  $1459 \not\equiv \pm 901 \pmod{1829}$ ,

$$(1459 + 901, 1829) = 59$$

is a factor of 1829.

## Factor Bases – Algorithm

**Require:** Odd positive composite 50-decimal-digit integer  $n$

**Ensure:** Divisor of  $n$

**repeat**

    Choose a random integer  $y$  with 5 decimal digits

    Let  $B$  consist of  $-1$  and all primes  $\leq y$

    Choose a large number of random  $b_i$  such that  $b_i^2 \bmod n$  can be expressed as a product of primes in  $B$

    Compute the corresponding set of binary vectors  $\epsilon_{b_i}$

    Find a subset of the  $b_i$  whose associated sum of binary vectors is zero

$b \leftarrow \prod_i b_i \bmod n$

$c \leftarrow \prod_j p_j^{\gamma_j} \bmod n$

**if**  $b \not\equiv \pm c \bmod n$  **then**

**return**  $(b + c, n)$

**end if**

**until** time elapsed

Factoring an  $r$ -bit integer  $n$  requires  $O(e^{C\sqrt{r \log r}})$  bit operations, where  $C$  is a constant; e.g.,  $\exp(\sqrt{50 \cdot \log(50)}) = 1185586.456$ .

## Continued Fraction Method (1983)

Given an odd composite integer  $n$ .

- The factor-base method works best if there are many integers  $b$ ,  $1 < b < n$ , such that  $b^2 \bmod n$  is a product of small primes; this is most likely if  $|b^2 \bmod n|$  is small.
- The continued fraction method gives integers  $b$  with  $|b^2 \bmod n| < 2\sqrt{n}$ .

## Continued Fractions

Let  $x$  be an irrational number. Construct its continued fraction expansion as follows:

- Write

$$x_0 = x = a_0 + 1/x_1,$$

where  $a_0 = \lfloor x_0 \rfloor$  and  $x_1 > 1$ .

- For  $n \geq 1$ , write

$$x_n = a_n + 1/x_{n+1},$$

where  $a_n = \lfloor x_n \rfloor$  and  $x_{n+1} > 1$ .

- The process never stops, since each  $x_n$  is irrational.

## Continued Fractions

Combining these equations gives

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n + x_{n+1}}}} \quad (17)$$

or shorter

$$x = a_0 + \frac{1}{a_1 +} \frac{1}{a_2 +} \dots \frac{1}{a_n +} \frac{1}{x_{n+1}} \quad (18)$$

or shorter

$$x = [a_0, a_1, a_2, \dots, a_n, x_{n+1}], \quad (19)$$

where  $a_1, \dots, a_n \in \mathbb{N}$  and  $a_0 \in \mathbb{Z}$ .

## Continued Fractions – Example

```

> X := sqrt(3):
> n := 6:
> seq(x[i],i=1..n): seq(a[i],i=1..n):
> a[0] := floor(X): x[0] := evalf(X-a[0]):
> print(0,x[0],1/x[0],a[0]);
> for i from 1 to n do
    a[i] := floor(1/x[i-1]);
    x[i] := evalf(1/x[i-1]}-a[i]);
    print(i,x[i],1/x[i],a[i])
> end:
0, 0.732050808, 1.366025403, 1
1, 0.366025403, 1.366025394, 1
2, 0.732050808, 2.732050881, 2
3, 0.366025403, 1.366025267, 1
4, 0.732050808, 2.732051829, 2
5, 0.366025403, 1.365998859, 1
6, 0.732050808, 2.732065033, 2

```

## Continued Fractions – Example (cont'd)

- We have

$$\sqrt{3} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \dots}}}}$$

Conjecture that the  $a_i$ 's alternate between 1 and 2.

- Let  $x$  be the infinite continued fraction with alternating 1's and 2's. Then

$$x = 1 + \frac{1}{1 + \frac{1}{1+x}}$$

Its expansion gives  $x^2 - 3 = 0$  and so  $x = \sqrt{3}$  ( $> 0$  in our setting).

## Continued Fractions

For any irrational number  $x$ , the  $n$ -th convergent of  $x$  in (17) is the rational number

$$\frac{b_n}{c_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}. \quad (20)$$

The convergents  $(b_n/c_n)$  form an infinite sequence of rational numbers.

## Continued Fractions – Example

Convergents of  $x = \sqrt{3}$ :

```
> cf := cfrac(sqrt(3));  
> for n from 1 to 6 do  
>   nthconver(cf, n)  
> end;
```

Output

$$2, \frac{5}{3}, \frac{7}{4}, \frac{19}{11}, \frac{26}{15}, \frac{71}{41}.$$

## Continued Fractions

By Euler's rule,

$$\begin{aligned}x &= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots \frac{1}{a_{n-1} + \frac{1}{x_{n+1}}}}} \\ &= \frac{[a_0, a_1, \dots, a_n, x_{n+1}]}{[a_1, a_2, \dots, a_n, x_{n+1}]}.\end{aligned}\tag{21}$$

## Continued Fractions

### Recurrence relation

$$\begin{aligned} [a_0, \dots, a_n, x_{n+1}] &= x_{n+1}[a_0, \dots, a_n] + [a_0, \dots, a_{n-1}] \\ &= x_{n+1}b_n + b_{n-1}, \end{aligned} \quad (22)$$

and

$$\begin{aligned} [a_1, \dots, a_n, x_{n+1}] &= x_{n+1}[a_1, \dots, a_n] + [a_1, \dots, a_{n-1}] \\ &= x_{n+1}c_n + c_{n-1}. \end{aligned} \quad (23)$$

Hence,

$$x = \frac{x_{n+1}b_n + b_{n-1}}{x_{n+1}c_n + c_{n-1}}. \quad (24)$$

## Continued Fractions

Given a purely periodic continued fraction

$$x = a_0 + \frac{1}{a_1 + \dots + \frac{1}{a_n + x}}. \quad (25)$$

Then

$$x = \frac{b_n x + b_{n-1}}{c_n x + c_{n-1}}. \quad (26)$$

Define the continued fraction  $y$  by reversing the period,

$$y = a_n + \frac{1}{a_{n-1} + \dots + \frac{1}{a_0 + y}}. \quad (27)$$

Then

$$y = \frac{b_n y + c_n}{b_{n-1} y + c_{n-1}}. \quad (28)$$

The numbers  $x$  and  $-1/y$  are conjugate to each other (Galois, 1828)

## Continued Fractions – Example

- Consider the purely periodic continued fraction

$$x = 4 + \frac{1}{1 + \frac{1}{3 + \frac{1}{x}}}.$$

Then  $4x^2 - 18x - 5 = 0$  with solutions  $\frac{9}{4} \pm \frac{1}{4}\sqrt{101}$ .

- Take the continued fraction by reversing the period,

$$y = 3 + \frac{1}{1 + \frac{1}{4 + \frac{1}{y}}}.$$

Then  $5y^2 - 18y - 4 = 0$  with solutions  $\frac{9}{5} \pm \frac{1}{5}\sqrt{101}$ .

- Both equations are related by the setting  $x = -1/y$ :

$$-1/\left(\frac{9}{4} + \frac{1}{4}\sqrt{101}\right) = \frac{9}{5} - \frac{1}{5}\sqrt{101},$$

$$-1/\left(\frac{9}{4} - \frac{1}{4}\sqrt{101}\right) = \frac{9}{5} + \frac{1}{5}\sqrt{101}.$$

## Continued Fractions (Example)

Some purely periodic continued fractions:

$$\sqrt{\varphi} = [1; \overline{1}, \dots],$$

$$\sqrt{2} = [1; \overline{2}, \dots],$$

$$\sqrt{3} = [1; \overline{1, 2}, \dots],$$

$$\sqrt{5} = [2; \overline{4}, \dots],$$

$$\sqrt{6} = [2; \overline{2, 4}, \dots],$$

$$\sqrt{7} = [2; \overline{1, 1, 4}, \dots],$$

$$\sqrt{8} = [2; \overline{1, 4}, \dots].$$

Contents

History

RSA

Discrete Log

\* Attacking  
Discrete Log

\* Pseudoprimes

\* Factoring

Fermat Factoring

Factor Bases

Continued Fractions

Quadratic Sieve

## Continued Fractions

For each real number  $x > 1$  with convergents  $(b_n/c_n)$ ,

$$\left| x - \frac{b_n}{c_n} \right| < \frac{1}{c_n c_{n+1}}. \quad (29)$$

**Proof.**

We have

$$\begin{aligned} x - \frac{b_n}{c_n} &= \frac{x_{n+1}b_n + b_{n-1}}{x_{n+1}c_n + c_{n-1}} - \frac{b_n}{c_n} \\ &= \frac{b_{n-1}c_n - c_{n-1}b_n}{c_n(x_{n+1}c_n + c_{n-1})} \\ &= \frac{\pm 1}{c_n(x_{n+1}c_n + c_{n-1})}. \end{aligned}$$

But  $x_{n+1} > a_{n+1}$  and  $c_{n+1} = a_{n+1}c_n + c_{n-1}$  and so the result follows. □

## Continued Fractions

For each real number  $x > 1$  with convergents  $(b_n/c_n)$ ,

$$|b_n^2 - x^2 c_n^2| < 2x. \quad (30)$$

### Corollary

Let  $n > 1$  be an integer which is not a perfect square and let  $(b_m/c_m)$  be the convergents of  $\sqrt{n}$ . Then for each  $m \geq 1$ ,

$$|b_m^2 \bmod n| < 2\sqrt{n}. \quad (31)$$

### Proof.

Take  $x = \sqrt{n}$ . Then  $b_m^2 \equiv b_m^2 - nc_m^2 \bmod n$  and so by (30), the latter is less than  $2\sqrt{n}$  in absolute value.  $\square$

## Continued Fractions – Maple

```

> n := 9073:
> k := 6:
> seq(x[i],i=0..k):
> seq(a[i],i=0..k):
> seq(b[i],i=-1..k):
> seq(c[i],i=-1..k):
> b[-1] := 1: c[-1] := 0: a[0] := floor(sqrt(n)):
> b[0] := a[0]: c[0] := 1: x[0] := evalf(sqrt(n)-a[0]):
> print(0,x[0],a[0],b[0],c[0],mods(b[0]^2,n));
> for i from 0 to k do
    a[i] := floor(1/x[i-1]);
    x[i] := evalf(1/x[i-1]-a[i]);
    b[i] := a[i]*b[i-1]+b[i-2];
    c[i] := a[i]*c[i-1]+c[i-2];
    print(i,x[i],a[i],b[i],c[i],mods(b[i]^2,n))
end:

```

## Continued Fractions – Maple Output

$$\sqrt{9073} = 95 + \frac{1}{3 + \frac{1}{1 + \frac{1}{26 + \frac{1}{2 + \frac{1}{6 + \frac{1}{1 + \dots}}}}}}$$

$i$	0	1	2	3	4	5	6
$a_i$	95	3	1	26	2	6	1
$b_i$	95	286	381	1119	2619	7760	1306
$c_i$	1	3	4	107	218	1415	1633
$b_i^2 \bmod n$	-48	139	-7	87	-27	99	-88

Contents

History

RSA

Discrete Log

\* Attacking  
Discrete Log

\* Pseudoprimes

\* Factoring

Fermat Factoring

Factor Bases

Continued Fractions

Quadratic Sieve

## Continued Fractions – Example (cont'd)

- Choose the factor basis  $B = \{-1, 2, 3, 7\}$ .

- Then

$$b_i^2 \bmod 9073 = -48, -7, -27$$

are  $B$ -numbers for  $i = 0, 2, 4$  with vectors

$$(1, 4, 1, 0), (1, 0, 0, 1), (1, 0, 3, 0).$$

- The sum of the first and third is  $(2, 4, 4, 0)$  and so 0 modulo 2.
- Then  $b = b_0 b_4 = 95 \cdot 2619 \equiv 3834 \bmod 9073$  and  $c = 2^{4/2} \cdot 3^{4/2} = 36$ .
- Thus  $3834^2 \equiv 36^2 \bmod 9073$ .
- But  $3834 \not\equiv \pm 36 \bmod 9073$  and so a nontrivial factor is  $(3834 + 36, 9073) = 43$ . Indeed,  $9073 = 43 \cdot 211$ .

## Quadratic Sieve Method (1981)

- Fastest for integers under 100 decimal digits.
- General running time  $O(e^{\sqrt{\log n \log \log n}})$ .
- Second fastest method known (after number field sieve).
- Number field sieve (1994) has general running time  $e^{O((\log n)^{1/3}(\log \log n)^{2/3})}$ , useful for larger integers ( $> 100$  digits).

## Quadratic Sieve Algorithm

Given odd composite number  $n$ .

- Choose bounds  $P$  and  $A$  of order  $L(n) = e^{\sqrt{\log n \log \log n}}$  with  $P < A < P^2$ . If  $n \approx 10^6$ , then  $L(n) \approx 400$ .
- Factor base  $B$  consists of 2 and all odd primes  $p < P$  for which  $n$  is a quadratic residue modulo  $p$ .
- Define  $|A| \times |B|$  matrix with rows labelled by  $t = \lfloor \sqrt{n} \rfloor + 1, \dots, \lfloor \sqrt{n} \rfloor + A$  and columns labelled by  $p \in B$ .
- The  $(t, p)$  matrix entry is the maximal  $i \geq 0$  such that  $p^i$  divides  $t^2 - n$ .
- Delete all rows numbered  $t$  for which  $t^2 - n$  is not a  $B$ -number.
- Use factor basis  $B$  to factor  $n$  if possible; otherwise, restart.

## Example

Factorize  $n = 1042387$ .

- Take bounds  $P = 50$  and  $A = 500$ .
- Factor basis  $B = \{2, 3, 11, 17, 19, 23, 43, 47\}$  with  $n$  quadratic residue.
- $\lfloor \sqrt{n} \rfloor = 1020$ .
- Take  $500 \times 8$  array with rows numbered by  $t = 1021, \dots, 1520$  and columns numbered by  $p \in B$ .
- Delete all rows numbered by  $t$  for which  $t^2 - n$  is not a  $B$ -number.
- Apply the factor-basis algorithm to the resulting  $11 \times 8$  table.

## Example (cont'd)

$t$	$t^2 - n$	2	3	11	17	19	23	43	47
1021	54	1	3						
1027	12342	1	1	2	1				
1030	18513		2	2	1				
1061	83334	1	1		1	1		1	
1112	194157		5		1				1
1129	232254	1	3	1	1		1		1
1148	275517		2	3			1		
1157	338238	1	2			1	1	1	
1217	438702	1	1	1	2		1		
1390	889713		2	2		1		1	
1520	1268013		1		1		2		1

## Example (cont'd)

- The first three rows sum to an even number in each column giving twice the row

$$1 \ 3 \ 2 \ 1 \ - \ - \ - \ -.$$

- The corresponding congruence is

$$(1021 \cdot 1027 \cdot 1030)^2 \equiv (2 \cdot 3^3 \cdot 11^2 \cdot 17)^2 \pmod{1042387}.$$

- Both numbers are  $\equiv 111078 \pmod{1042387}$  providing the trivial factorization.

## Example (cont'd)

- The fifth and the last row sum to an even number with corresponding congruence

$$(1112 \cdot 1520)^2 \equiv (3^2 \cdot 17 \cdot 23 \cdot 47)^2 \pmod{1042387}.$$

$$\text{Thus } 647853^2 \equiv 496179^2 \pmod{1042387}.$$

- But  $647853 \not\equiv \pm 496179 \pmod{1042387}$  and so a nontrivial factor is

$$(647853 - 496179, 1042387) = 1487.$$

## Part II

# Projective Space

## Contents

Projective  
 $n$ -Space

Projective Line

Projective Plane

Homogeneous  
PolynomialsLines in  
Projective Plane\* Projective  
Transformations

## Projective Space

- Projective  $n$ -space
- Projective line
- Projective plane
- Homogeneous polynomials
- Lines in projective plane
- \*Projective transformations

## Projective $n$ -Space

The idea of projective space relates to perspective, more precisely to the way an eye or a camera projects a 3D scene to a 2D image.

Wikipedia, 2018

## Affine $n$ -Space

Let  $\mathbb{K}$  be a field. Put  $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ .

- The *affine  $n$ -space* over  $\mathbb{K}$ ,

$$\mathbb{A}^n(\mathbb{K}) = \mathbb{K}^n = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in \mathbb{K}\}. \quad (32)$$

- The *projective  $n$ -space*  $\mathbb{P}^n(\mathbb{K})$  over  $\mathbb{K}$  is the set of all lines in  $\mathbb{K}^{n+1}$  passing through the origin  $0$ ; i.e., the set of all one-dimensional subspaces of  $\mathbb{K}^{n+1}$ .

## Projective $n$ -Space

- Define an equivalence relation  $\sim$  on  $\mathbb{K}^{n+1} \setminus \{0\}$ ,

$$(p_0, \dots, p_n) \sim (q_0, \dots, q_n) \Leftrightarrow (p_0, \dots, p_n) = \kappa(q_0, \dots, q_n) \quad (33)$$

for some  $\kappa \in \mathbb{K}^*$ , where

$$\kappa(q_0, \dots, q_n) = (\kappa q_0, \dots, \kappa q_n). \quad (34)$$

- Two points  $P$  and  $Q$  in  $\mathbb{K}^{n+1}$  are equivalent iff they lie on the same line.
- The *projective  $n$ -space*  $\mathbb{P}^n(\mathbb{K})$  is the quotient space of  $\mathbb{K}^{n+1}$  given by the set of equivalence classes of the nonzero points in  $\mathbb{K}^{n+1}$ .

## Homogeneous Coordinates

- A point  $P$  in  $\mathbb{P}^n(\mathbb{K})$  is determined by the equivalence class of an  $n + 1$ -tuple  $(p_0, \dots, p_n) \in \mathbb{K}^{n+1}$ , written

$$P = (p_0 : \dots : p_n).$$

Each  $(n + 1)$ -tuple belonging to this equivalence class is referred to as *homogeneous coordinates* of  $P$ .

- Each point in  $\mathbb{P}^n(\mathbb{K})$  has many homogeneous coordinates; e.g.,

$$(0 : i : \sqrt{2}) = (0 : -\sqrt{2} : 2i)$$

are the same point in  $\mathbb{P}^2(\mathbb{C})$ , since for  $\kappa = i\sqrt{2}$ ,

$$i\sqrt{2} \cdot (0, i, \sqrt{2}) = (0, -\sqrt{2}, 2i).$$

## Decomposition of Projective $n$ -Space

For each  $n \geq 2$ , the projective  $n$ -space decomposes as

$$\mathbb{P}^n(\mathbb{K}) = \mathbb{A}^n(\mathbb{K}) \cup \mathbb{P}^{n-1}(\mathbb{K}). \quad (35)$$

### Proof.

Let  $P = (p_0 : p_1 : \dots : p_n)$  in  $\mathbb{P}^n(\mathbb{K})$ .

- If  $p_n \neq 0$ , then  $P = (p'_0 : \dots : p'_{n-1} : 1)$  with  $p'_i = p_i/p_n$ ,  $0 \leq i \leq n$ . We have

$$\begin{aligned} (p_0 : \dots : p_{n-1} : 1) &= (q_0 : \dots : q_{n-1} : 1) & (36) \\ \iff (p_0, \dots, p_{n-1}) &= (q_0, \dots, q_{n-1}). \end{aligned}$$

Thus the points  $P$  with  $p_n \neq 0$  form the affine  $n$ -space.

- If  $p_n = 0$ , then  $P = (p_0 : \dots : p_{n-1} : 0)$ , where the  $p_i$  are defined only up to a common scalar. Thus the points  $P$  with  $p_n = 0$  form the projective  $n - 1$ -space, called *points at infinity*. □

## Affine Subspaces of Projective $n$ -Space

For each  $0 \leq i \leq n$ , define the subset of  $\mathbb{P}^n(\mathbb{K})$ ,

$$\begin{aligned} U_i &= \{(p_0 : \dots : p_i : \dots : p_n) \in \mathbb{P}^n(\mathbb{K}) \mid p_i \neq 0\} \\ &= \{(p_0 : \dots : p_{i-1} : 1 : p_{i+1} : \dots : p_n) \in \mathbb{P}^n(\mathbb{K}) \mid p_i = 1\}. \end{aligned} \quad (37)$$

- $U_i$  is an open subset of  $\mathbb{P}^n(\mathbb{K})$  ( $\rightarrow$  Algebraic Geometry).
- The mapping  $\phi : \mathbb{K}^n \rightarrow U_i$  given by

$$\begin{aligned} \phi(p_0, \dots, p_{i-1}, p_{i+1}, \dots : p_n) \\ = (p_0, \dots : p_{i-1} : 1 : p_{i+1} : \dots : p_n) \end{aligned} \quad (38)$$

is a bijection.

## Affine Covering of Projective $n$ -Space

The projective  $n$ -space  $\mathbb{P}^n(\mathbb{K})$  has the following properties:

- For each  $0 \leq i \leq n$ , there is a bijection between  $U_i$  and  $\mathbb{K}^n$ .
- For each  $0 \leq i \leq n$ , the complement  $\mathbb{P}^n(\mathbb{K}) \setminus U_i$  can be identified with  $\mathbb{P}^{n-1}(\mathbb{K})$ .
- The projective  $n$ -space  $\mathbb{P}^n(\mathbb{K})$  has an open covering of  $n + 1$  affine  $n$ -spaces

$$\mathbb{P}^n(\mathbb{K}) = \bigcup_{i=0}^n U_i. \quad (39)$$

## Order of Finite Projective $n$ -Space

Let  $\mathbb{F}_q$  be the Galois field with  $q$  elements. Then

$$|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1} - 1}{q - 1}. \quad (40)$$

**Proof.**

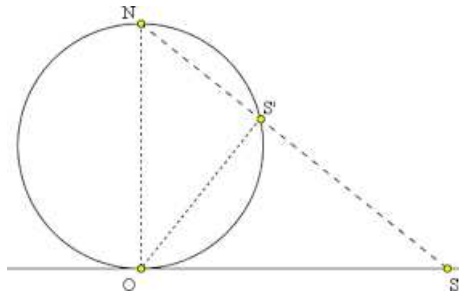
For the projective line,

$$|\mathbb{P}^1(\mathbb{F}_q)| = q + 1 = \frac{q^2 - 1}{q - 1}.$$

For the projective  $n + 1$ -space,

$$\begin{aligned} |\mathbb{P}^{n+1}(\mathbb{F}_q)| &= |\mathbb{A}^{n+1}(\mathbb{F}_q)| + |\mathbb{P}^n(\mathbb{F}_q)| \\ &= q^{n+1} + \frac{q^{n+1} - 1}{q - 1} \\ &= \frac{q^{n+2} - 1}{q - 1}. \end{aligned}$$

## Projective Line



Stereographic projection of real projective line.

## Decomposition of Projective Line

The *projective line* over  $\mathbb{K}$  decomposes as

$$\mathbb{P}^1(\mathbb{K}) = \mathbb{A}^1(\mathbb{K}) \cup \{(1 : 0)\}, \quad (41)$$

where

$$\mathbb{A}^1(\mathbb{K}) = \{(p : 1) \mid p \in \mathbb{K}\} \quad (42)$$

is the *affine line*.

### Proof.

Let  $P = (p_0 : p_1)$  in  $\mathbb{P}^1(\mathbb{K})$ .

- If  $p_1 \neq 0$ , then  $P = (p : 1)$  with  $p = p_0/p_1$ . We have

$$(p : 1) = (q : 1) \iff p = q. \quad (43)$$

Thus the points  $P$  with  $p_1 \neq 0$  form the affine line.

- If  $p_1 = 0$ , then  $p_0 \neq 0$  and so  $P = (1 : 0)$ , called *point at infinity*. □

## Projective Line over $\mathbb{F}_4$

- The Galois field  $\mathbb{F}_4 = \mathbb{Z}_2[x]/\langle X^2 + X + 1 \rangle$  has the elements

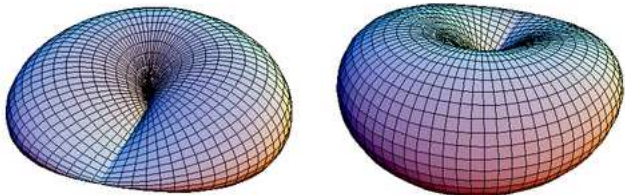
$$0, 1, \alpha, \alpha^2,$$

where  $\alpha$  is a zero of  $X^2 + X + 1$  over  $\mathbb{Z}_2$ ; i.e.,  $\alpha^2 + \alpha + 1 = 0$  or  $\alpha^2 = \alpha + 1$ .

- The projective line over  $\mathbb{F}_4$  has the elements

$$(0 : 1), (1 : 1), (\alpha : 1), (\alpha^2 : 1), \text{ and } (1 : 0).$$

## Projective Plane



## Real projective plane

Contents

Projective  
 $n$ -Space

Projective Line

Projective Plane

Homogeneous  
PolynomialsLines in  
Projective Plane\* Projective  
Transformations

## Decomposition of Projective Plane

The *projective plane*  $\mathbb{P}^2(\mathbb{K})$  decomposes as

$$\mathbb{P}^2(\mathbb{K}) = \mathbb{A}^2(\mathbb{K}) \cup \mathbb{L}(\mathbb{K}) \cup \{(1 : 0 : 0)\}, \quad (44)$$

where  $\mathbb{A}^2(\mathbb{K})$  is the *affine plane*,

$$\mathbb{A}^2(\mathbb{K}) = \{(a : b : 1) \mid a, b \in \mathbb{K}\}, \quad (45)$$

and  $\mathbb{L}(\mathbb{K})$  is an affine line,

$$\mathbb{L}(\mathbb{K}) = \{(a : 1 : 0) \mid a \in \mathbb{K}\}. \quad (46)$$

The points  $(a : b : c)$  with  $c = 0$  are the *points at infinity*.

Projective Plane over  $\mathbb{F}_4$ 

- The Galois field  $\mathbb{F}_4 = \mathbb{Z}_2[x]/\langle X^2 + X + 1 \rangle$  has the elements

$$0, 1, \alpha, \alpha^2,$$

where  $\alpha$  is a zero of  $X^2 + X + 1$  over  $\mathbb{Z}_2$ , i.e.,  $\alpha^2 + \alpha + 1 = 0$ .

- The projective plane over  $\mathbb{F}_4$  decomposes into

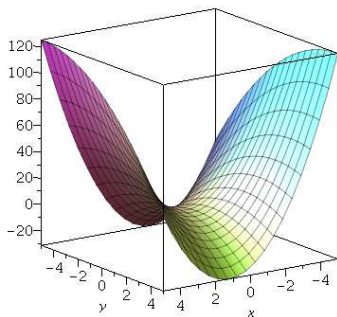
$$\mathbb{P}^2(\mathbb{F}_4) = \mathbb{A}^2(\mathbb{F}_4) \cup \mathbb{L}(\mathbb{F}_4) \cup \{(1 : 0 : 0)\}$$

with

$$\mathbb{A}^2(\mathbb{F}_4) = \{(a : b : 1) \mid a, b \in \mathbb{F}_4\},$$

$$\mathbb{L}(\mathbb{F}_4) = \{(a : 1 : 0) \mid a \in \mathbb{F}_4\}.$$

## Homogeneous Polynomials



```
> with(plots):
> plot3d(4*x^2-2*x*y-y^2,x=-5..5,y=-5..5,grid=[20,20]);
```

## Zeros of Homogeneous Polynomial

If  $f \in \mathbb{K}[X_0, \dots, X_n]$  is a homogeneous polynomial of total degree  $d$  that vanishes on some homogeneous coordinates of a point  $P \in \mathbb{P}^n(\mathbb{K})$ , then  $f$  vanishes on all homogeneous coordinates of  $P$ .

### Proof.

Let  $P = (p_0 : \dots : p_n) \in \mathbb{P}^n(\mathbb{K})$ . Then by homogeneity,

$$f(\kappa p_0, \dots, \kappa p_n) = \kappa^d f(p_0, \dots, p_n) \quad (47)$$

for each  $\kappa \in \mathbb{K}^*$ . Thus

$$f(p_0, \dots, p_n) = 0 \iff f(\kappa p_0, \dots, \kappa p_n) = 0, \quad (48)$$

since  $\kappa^d \in \mathbb{K}^*$ . □

## Zeros of Homogeneous Polynomial

Let

$$f = XY - Y^2 + XZ \in \mathbb{K}[X, Y, Z]$$

and  $P = (1 : 1 : 0) \in \mathbb{P}^2(\mathbb{K})$ .

Then  $f(P) = 0$  and for each  $Q = \kappa P = (\kappa : \kappa : 0)$  with  $\kappa \neq 0$ ,

$$f(Q) = \kappa^2 f(P) = 0.$$

For a homogeneous polynomial  $f$ , an equation of the form

$$f = a$$

with  $a \in \mathbb{K}$  makes only sense for  $a = 0$ .

## Homogenization

Given a polynomial  $f \in \mathbb{K}[X_1, \dots, X_n]$  of degree  $d$  and its expansion as a sum of homogeneous components,

$$f = \sum_{k=0}^d f^{(k)}, \quad (49)$$

where  $f^{(k)}$  is the degree- $k$  part. Then

$$f^h(X_0, \dots, X_n) = \sum_{k=0}^d X_0^{d-k} f^{(k)}(X_1, \dots, X_n) \quad (50)$$

is a homogeneous polynomial in  $\mathbb{K}[X_0, X_1, \dots, X_n]$  of total degree  $d$ , called *homogenization* of  $f$ .

## Homogenization – Example

The polynomial

$$f = X^2Y + X^2 + XY + Y + 2 \in \mathbb{K}[X, Y]$$

of degree 3 has the homogeneous components

$$f^{(0)} = 2, f^{(1)} = Y, f^{(2)} = X^2 + XY, f^{(3)} = X^2Y.$$

Homogenization yields the homogeneous polynomial

$$f^h = X^2Y + X^2Z + XYZ + YZ^2 + 2Z^3 \in \mathbb{K}[X, Y, Z].$$

## Dehomogenization

Let  $f \in \mathbb{K}[X_0, \dots, X_n]$  be a homogeneous polynomial of total degree  $d$ . Then

$$f^a(X_1, \dots, X_n) = f(1, X_1, \dots, X_n) \quad (51)$$

is a polynomial in  $\mathbb{K}[X_1, \dots, X_n]$  obtained by the substitution  $X_0 = 1$ , called *dehomogenization* of  $f$ .

## Dehomogenization – Example

The homogeneous polynomial

$$f = X^2Y + X^2Z + XYZ + YZ^2 + 2Z^3 \in \mathbb{K}[X, Y, Z]$$

is dehomogenized by setting  $Z = 1$ ,

$$f^a = X^2Y + X^2 + XY + Y + 2 \in \mathbb{K}[X, Y].$$

## Homogenization and Dehomogenization

- If  $f$  is a polynomial in  $\mathbb{K}[X_1, \dots, X_n]$  of degree  $d$ , then the homogenization of  $f$  satisfies

$$f^h = X_0^d \cdot f\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right), \quad (52)$$

where the right-hand side is evaluated as rational function.

- If  $f$  is a polynomial in  $\mathbb{K}[X_1, \dots, X_n]$ , then

$$(f^h)^a = f. \quad (53)$$

- If  $f$  is a homogeneous polynomial in  $\mathbb{K}[X_0, \dots, X_n]$  and  $X_0^{e_0}$  is the highest power of  $X_0$  dividing  $f$ , then

$$f = X_0^{e_0} \cdot (f^a)^h. \quad (54)$$

## Homogenization and Dehomogenization – Example

Let

$$f = X^2Y + X^2 + Y + 2 \in \mathbb{K}[X, Y].$$

Then

$$\begin{aligned} f^h &= Z^3 f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \\ &= Z^3 \left[ \left(\frac{X}{Z}\right)^2 \left(\frac{Y}{Z}\right) + \left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right) + 2 \right] \\ &= X^2Y + X^2Z + YZ^2 + 2Z^3 \in \mathbb{K}[X, Y, Z]. \end{aligned}$$

Moreover,

$$\begin{aligned} (f^h)^a &= (X^2Y + X^2Z + YZ^2 + 2Z^3)^a \\ &= X^2Y + X^2 + Y + 2 = f. \end{aligned}$$

## Homogenization and Dehomogenization – Example

Let

$$f = X_0^3 + X_0X_1X_2 \in \mathbb{K}[X_0, X_1, X_2].$$

The highest power  $X_0^{e_0}$  of  $X_0$  dividing  $f$  is  $X_0^1$ , so  $e_0 = 1$ .

Then

$$\begin{aligned} X_0^{e_0} \cdot (f^a)^h &= X_0 \cdot (1 + X_1X_2)^h \\ &= X_0 \cdot (X_0^2 + X_1X_2) \\ &= X_0^3 + X_0X_1X_2 = f. \end{aligned}$$

## Homogeneous Polynomials in Singular

```

> ring r = 0, (x,y,z), dp;
> poly f = x3y3 + x7y+ 2xy;
> poly fh = homog(f,z); // homogenization of f
> fh;
x7y+x3y3z2 + x7y+ 2xyz6;
> homog(f); // test for homogeneity
0
> homog(fh); // test for homogeneity
1

```

## Lines in Projective Plane



Contents

Projective  
 $n$ -Space

Projective Line

Projective Plane

Homogeneous  
Polynomials**Lines in  
Projective Plane**\* Projective  
Transformations

## Projective Lines

- Given homogeneous polynomial  $\ell \in \mathbb{K}[X, Y, Z]$  of total degree 1. Then

$$\ell = \alpha X + \beta Y + \gamma Z, \quad (55)$$

where  $\alpha, \beta, \gamma \in \mathbb{K}$  with  $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ .

- The corresponding zero locus

$$\mathcal{L}(\ell) = \{(a : b : c) \in \mathbb{P}^2(\mathbb{K}) \mid \ell(a, b, c) = 0\} \quad (56)$$

over  $\mathbb{K}$  is called *projective line* over  $\mathbb{K}$ , also written  $\mathcal{L}_{\mathbb{K}}(\alpha, \beta, \gamma)$  or simpler  $\mathcal{L}(\alpha, \beta, \gamma)$ .

## Nonsingularity of Lines

A projective line  $\mathcal{L}(\alpha, \beta, \gamma)$  is always non-singular.

### Proof.

For each point  $P$  on the line,

$$\frac{\partial \ell}{\partial X}(P) = \alpha, \quad \frac{\partial \ell}{\partial Y}(P) = \beta, \quad \frac{\partial \ell}{\partial Z}(P) = \gamma. \quad (57)$$

These partial derivatives do not vanish altogether, since  $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ . □

## Lines and Dehomogenization

Given the projective line  $\mathcal{L}_{\mathbb{K}}(\ell)$  by the linear polynomial

$$\ell = \alpha X + \beta Y + \gamma Z \in \mathbb{K}[X, Y, Z].$$

Dehomogenization yields the dehomogenized polynomial

$$\ell^a = \alpha X + \beta Y + \gamma \in \mathbb{K}[X, Y]$$

with zero locus

$$\mathcal{L}(\ell^a) = \{(a, b) \in \mathbb{K}^2 \mid \ell^a(a, b) = 0\}.$$

## Affine and Projective Lines – Summary

## ■ Affine line

$$\ell_1 : Y = mX + b, \quad m \neq 0,$$

projective line

$$\ell_1^h : Y = mX + bZ,$$

zero locus

$$\mathcal{L}(\ell_1^h) = \{(x : mx + b : 1) \mid x \in \mathbb{K}\} \cup \left\{ \left( \frac{1}{m} : 1 : 0 \right) \right\}.$$

## ■ Affine line

$$\ell_2 : X = a,$$

projective line

$$\ell_2^h : X = aZ,$$

zero locus

$$\mathcal{L}(\ell_2^h) = \{(a : y : 1) \mid y \in \mathbb{K}\} \cup \{(0 : 1 : 0)\}.$$

## Line Through Two Points

Two distinct points in  $\mathbb{P}^2(\mathbb{K})$  lie on a unique projective line.

### Proof.

Given distinct points  $P_1 = (a_1 : b_1 : c_1)$ ,  $P_2 = (a_2 : b_2 : c_2)$  in  $\mathbb{P}^2(\mathbb{K})$ . A line  $\mathcal{L}(\alpha, \beta, \gamma)$  over  $\mathbb{K}$  with  $(\alpha, \beta, \gamma) \neq (0, 0, 0)$  between  $P_1, P_2$  satisfies

$$\alpha a_1 + \beta b_1 + \gamma c_1 = \alpha a_2 + \beta b_2 + \gamma c_2.$$

Equivalently, there is a solution of the homogeneous linear system of equations with coefficient matrix

$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}.$$

Since the points are distinct, one row is not the scalar multiple of the other and thus the rows of  $A$  are linearly independent. Thus  $A$  has rank 2 and hence its kernel is one-dimensional giving a unique line  $\mathcal{L}(\alpha, \beta, \gamma)$  between the points up to a scalar multiple.  $\square$

## Line Through Two Points – Example

Given the points  $P_1 = (0 : 1 : 0)$  and  $P_2 = (1 : 1 : 0)$  in  $\mathbb{P}^2(\mathbb{K})$ .  
The matrix

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

has rank 2 and its kernel is generated by the vector  $(0, 0, 1)$ . Thus the homogeneous polynomial  $\ell = Z$  gives the unique projective line  $\mathcal{L}(0, 0, 1)$  between these points.

## Intersection of Two Lines

Two distinct projective lines in  $\mathbb{P}^2(\mathbb{K})$  meet in exactly one point.

### Proof.

Let  $\mathcal{L}(\alpha_1, \beta_1, \gamma_1)$  and  $\mathcal{L}(\alpha_2, \beta_2, \gamma_2)$  be distinct projective lines in  $\mathbb{P}^2(\mathbb{K})$ . Then the matrix

$$A = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{pmatrix}$$

has rank 2 and the kernel of the matrix is one-dimensional providing a unique vector  $(a, b, c)$  up to a scalar multiple. This is the unique point  $P = (a : b : c)$  lying on both projective lines.  $\square$

## Intersection of Two Lines – Example

Given the projective lines  $\mathcal{L}(0, 1, 0)$  and  $\mathcal{L}(1, 1, 0)$  in  $\mathbb{P}^2(\mathbb{K})$ . The matrix

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

has rank 2 and its kernel is generated by the vector  $(0, 0, 1)$ . Thus the unique point lying on both projective lines is  $P = (0 : 0 : 1)$ .

## Intersection of Two Lines – Example

Consider the parallel affine lines over  $\mathbb{K}$  given by

$$l_0 = Y - X \quad \text{and} \quad l_1 = Y - X - 1.$$

- The affine loci are

$$\mathcal{L}(l_0) = \{(a, a) \mid a \in \mathbb{K}\},$$

$$\mathcal{L}(l_1) = \{(a, a + 1) \mid a \in \mathbb{K}\}.$$

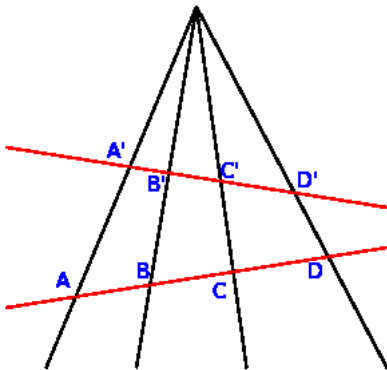
These lines are parallel in  $\mathbb{A}^2(\mathbb{K})$ :  $\mathcal{L}(l_0) \cap \mathcal{L}(l_1) = \emptyset$ .

- By homogenization,

$$l_0^h = Y - X \quad \text{and} \quad l_1^h = Y - X - Z.$$

These lines meet at  $P = (1 : 1 : 0)$ :  $\mathcal{L}(l_0^h) \cap \mathcal{L}(l_1^h) = \{P\}$ .

# \*Projective Transformations



- Contents
- Projective  $n$ -Space
- Projective Line
- Projective Plane
- Homogeneous Polynomials
- Lines in Projective Plane
- \* Projective Transformations

## Affine Transformations

An *affine transformation*  $T$  of the affine space  $\mathbb{A}^2(\mathbb{K})$  is given by an invertible linear mapping followed by a translation, i.e.,

$$T : \mathbb{A}^2(\mathbb{K}) \rightarrow \mathbb{A}^2(\mathbb{K}) : (x, y) \mapsto (x', y'), \quad (58)$$

where

$$x' = ax + by + c, \quad y' = dx + ey + f, \quad ad - bc \neq 0. \quad (59)$$

The affine transformations of  $\mathbb{A}^2(\mathbb{K})$  form a group under the composition of maps.

## Projective Transformations

An invertible  $3 \times 3$  matrix  $A = (a_{ij})$  over  $\mathbb{K}$  acts on the projective plane  $\mathbb{P}^2(\mathbb{K})$  via

$$A \cdot (x : y : z) = (x' : y' : z'), \quad (60)$$

where

$$(x', y', z') = (x, y, z) \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}. \quad (61)$$

This mapping is well-defined, since

$$\begin{aligned} A \cdot (\lambda x : \lambda y : \lambda z) &= \lambda(x, y, z)A = \lambda(x', y', z') \\ &= (\lambda x' : \lambda y' : \lambda z'), \quad \lambda \in \mathbb{K}^*. \end{aligned} \quad (62)$$

## Projective Transformations – Example

Let

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

We have

$$\mathbb{P}^2(\mathbb{K}) = \mathbb{A}^2(\mathbb{K}) \cup L(\mathbb{K}) \cup \{(1 : 0 : 0)\}.$$

Then

$$A \cdot (a : b : 1) = (a + b + 1 : b + 1 : 1),$$

$$A \cdot (a : 1 : 0) = (a + 1 : 1 : 0),$$

$$A \cdot (1 : 0 : 0) = (1 : 0 : 0).$$

## Projective Transformations

- The diagonal matrix  $\text{diag}(\lambda, \lambda, \lambda)$ ,  $\lambda \in \mathbb{K}^*$ , fixes each element  $(x : y : z) \in \mathbb{P}^2(\mathbb{K})$ .
- The group of all diagonal matrices  $\text{diag}(\lambda, \lambda, \lambda)$ ,  $\lambda \in \mathbb{K}^*$ , is isomorph to  $\mathbb{K}^*$ .
- The *general linear group*  $\text{GL}_3(\mathbb{K})$  is the group of all invertible  $3 \times 3$  matrices over  $\mathbb{K}$ .

- The *projective linear group*  $\text{PGL}_3(\mathbb{K})$  is the quotient group

$$\text{PGL}_3(\mathbb{K}) = \text{GL}_3(\mathbb{K})/\mathbb{K}^*.$$

The elements of  $\text{PGL}_3(\mathbb{K})$  are called *projective transformations*.

- Two projective transformations  $A, B$  are equal iff  $B = \lambda A$  for some  $\lambda \in \mathbb{K}^*$ .

## Projective Transformations

Let  $A = (a_{ij}) \in \text{PGL}_3(\mathbb{K})$  be a projective transformation. The following are equivalent:

- 1 The restriction of  $A$  to  $\mathbb{A}^2(\mathbb{K}) = \{(x : y : 1) \mid x, y \in \mathbb{K}\}$  is an affine transformation.
- 2  $a_{13} = a_{23} = 0$ .
- 3  $A$  fixes the projective line given by  $\ell = Z$ .

## Projective Transformations – Proof

- $1 \Rightarrow 2$ : We have  $A \cdot (x : y : 1) = (x' : y' : z')$  with  $z' = a_{13}x + a_{23}y + a_{33}$ . If  $A$  induces an affine transformation, then  $z' \neq 0$  for all  $x, y \in \mathbb{K}$ . Thus  $a_{13} = a_{23} = 0$  and as  $\det A \neq 0$  (by rescaling)  $a_{33} = 1$ .
- $2 \Rightarrow 1$ : If  $a_{13} = a_{23} = 0$  and  $a_{33} = 1$ , then  $A \cdot (x : y : 1) = (x' : y' : 1)$ , where  $x' = a_{11}x + a_{21}y + a_{31}$  and  $y' = a_{12}x + a_{22}y + a_{32}$ . This is an affine transformation.

## Projective Transformations – Proof (cont'd)

- $2 \Rightarrow 3$ : If  $a_{13} = a_{23} = 0$  and  $a_{33} = 1$ , then  $A \cdot (x : y : 0) = (x' : y' : 0)$  and so the line  $\mathcal{L}(0, 0, 1)$  is preserved.
- $3 \Rightarrow 2$ : If  $A \cdot (x : y : 0) = (x' : y' : 0)$  for all  $x, y \in \mathbb{K}$ , then  $a_{13} = a_{23} = 0$ .



## Projective Transformations

The group  $\mathrm{PGL}_3(\mathbb{K})$  acts on the set of projective cubic curves  $\mathcal{C}(f)$  over  $\mathbb{K}$  in the sense that

$$f^A = A \cdot f = f((X, Y, Z)A^{-1}), \quad (63)$$

where  $A \in \mathrm{PGL}_3(\mathbb{K})$  and  $f \in \mathbb{K}[X, Y, Z]$  is a homogeneous polynomial of degree 3.

We have

$$I \cdot f = f \quad \text{and} \quad (AB) \cdot f = A \cdot (B \cdot f) \quad (64)$$

where  $A, B \in \mathrm{PGL}_3(\mathbb{K})$  and  $I$  is the unit  $3 \times 3$  matrix over  $\mathbb{K}$ .

## Proof.

We have

$$(I \cdot f)(X, Y, Z) = f((X, Y, Z)I) = f(X, Y, Z)$$

and

$$\begin{aligned} (AB \cdot f)(X, Y, Z) &= f((X, Y, Z)(AB)^{-1}) \\ &= f((X, Y, Z)B^{-1}A^{-1}) \\ &= A \cdot (f((X, Y, Z)B^{-1})) \\ &= (A \cdot (B \cdot f))(X, Y, Z). \end{aligned}$$



## Projective Transformations – Example

Let

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix},$$

and

$$f = X^2Y + XZ^2 - Z^3.$$

Then

$$\begin{aligned} f^A &= A \cdot f = f((X, Y, Z)A^{-1}) \\ &= f(X - Y, Y - Z, Z) \\ &= (X - Y)^2(Y - Z) + (X - Y)Z^2 - Z^3 \\ &= X^2Y - X^2Z - 2XY^2 + 2XYZ + XZ^2 + Y^3 \\ &\quad - Y^2Z - YZ^2 - Z^3. \end{aligned}$$

# Part III

## Algebraic Curves

## Algebraic Curves

- Plane curves
- Singularities
- Rational mappings and birationality
- Tangents
- Intersection multiplicities
- Weierstrass equation

## Plane Curves

Curves,  
Cryptosystems,  
and Quantum  
Computing

K.-H.  
Zimmermann

Contents

Plane Curves

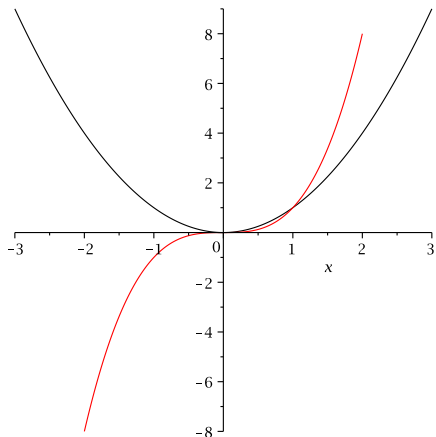
Singularities

Rational  
Mappings

Tangents

Intersection  
Multiplicities

Weierstrass Form



```
> with(plots):
> plots[multiple](plot, [x^2, x=-3..3, color=black],
                   [y^3, y=-2..2, color=red]);
```

## Plane Projective Curves

- A *plane projective curve of degree  $d \geq 1$  over  $\mathbb{K}$*  is the zero locus of a homogeneous polynomial  $f \in \mathbb{K}[X, Y, Z]$  of degree  $d$ ,

$$\mathcal{C}_{\mathbb{K}}(f) = \{(a : b : c) \in \mathbb{P}^2(\mathbb{K}) \mid f(a, b, c) = 0\}. \quad (65)$$

If  $\mathbb{L}$  is a field extension of  $\mathbb{K}$ , then  $\mathcal{C}_{\mathbb{K}}(f)$  is a subset of  $\mathcal{C}_{\mathbb{L}}(f)$

- Examples:
  - Unit circle  $f = X^2 + Y^2 - Z^2$ ,
  - Parabola  $g = X^2 - YZ$ ,
  - Elliptic curve  $h = Y^2Z - X^3 - XZ^2$ .

## Plane Affine Curves

- The dehomogenization of a homogeneous polynomial  $f \in \mathbb{K}[X, Y, Z]$  obtained by setting  $Z = 1$  gives a polynomial  $f^a$  in  $\mathbb{K}[X, Y]$  and the corresponding zero locus is a *plane affine curve*,

$$\mathcal{C}_{\mathbb{K}}(f^a) = \{(a, b) \in \mathbb{A}^2(\mathbb{K}) \mid f^a(a, b) = 0\}. \quad (66)$$

- Examples:

- Unit circle  $f^a = X^2 + Y^2 - 1$ ,
- Parabola  $g^a = X^2 - Y$ ,
- Elliptic curve  $h^a = Y^2 - X^3 - X$ .

## Projective Lines and Conics

- A projective curve of degree 1 is a *projective line* defined as zero locus of the linear homogeneous polynomial

$$f = aX + bY + cZ, \quad (67)$$

where  $a, b, c \in \mathbb{K}$  with  $(a, b, c) \neq (0, 0, 0)$ .

- A projective curve of degree 2 is a *conic* defined as zero locus of the quadratic homogeneous polynomial

$$f = a_1X^2 + a_2XY + a_3XZ + a_4Y^2 + a_5YZ + a_6Z^2 \quad (68)$$

where  $a_1, \dots, a_6 \in \mathbb{K}$ .

- Examples:
  - Unit circle  $f^a = X^2 + Y^2 - Z^2$ ,
  - Parabola  $g^a = X^2 - YZ$ .

## Unit Parabola – Example

The affine unit parabola is the zero locus of the polynomial  $f = X^2 - Y \in \mathbb{R}[X, Y]$ ,

$$\mathcal{C}_{\mathbb{R}}(f) = \{(a, a^2) \mid a \in \mathbb{R}\}.$$

The projective unit parabola is the zero locus of the homogeneous polynomial  $f^h = X^2 - YZ \in \mathbb{R}[X, Y, Z]$ ,

$$\mathcal{C}_{\mathbb{R}}(f^h) = \{(a : a^2 : 1) \mid a \in \mathbb{R}\} \cup \{(0 : 1 : 0)\}.$$

## Cubics

- A projective curve of degree 3 is a *cubic* defined as zero locus of the cubic homogeneous polynomial

$$\begin{aligned}
 f = & a_1X^3 + a_2X^2Y + a_3X^2Z + a_4XY^2 \\
 & + a_5XZ^2 + a_6XYZ + a_7Y^3 + a_8Y^2Z \quad (69) \\
 & + a_9YZ^2 + a_{10}Z^3,
 \end{aligned}$$

where  $a_1, \dots, a_{10} \in \mathbb{K}$ .

- Example: elliptic curve in Weierstrass form

$$f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

## Unit Cubic – Example

The affine unit cubic is the zero locus of the polynomial  $f = X^3 - Y \in \mathbb{R}[X, Y]$ ,

$$\mathcal{C}_{\mathbb{R}}(f) = \{(a, a^3) \mid a \in \mathbb{R}\}.$$

The projective unit cubic is the zero locus of the homogeneous polynomial  $f^h = X^3 - YZ^2 \in \mathbb{R}[X, Y, Z]$ ,

$$\mathcal{C}_{\mathbb{R}}(f^h) = \{(a : a^3 : 1) \mid a \in \mathbb{R}\} \cup \{(0 : 1 : 0)\}.$$

## Homogenization

Let  $f$  be a nonzero polynomial in  $\mathbb{K}[X, Y]$  of degree  $d$ . The homogenization of  $f$  is the homogeneous polynomial  $f^h$  of degree  $d$  in  $\mathbb{K}[X, Y, Z]$  such that

$$f^h(a, b, 1) = f(a, b) \text{ for all } (a, b) \in \mathbb{A}^2(\mathbb{K}), \quad (70)$$

i.e.,

$$\mathcal{C}_{\mathbb{K}}(f^h) \cap \mathbb{A}^2(\mathbb{K}) = \mathcal{C}_{\mathbb{K}}(f). \quad (71)$$

## Dehomogenization

Let  $f$  be a nonzero homogeneous polynomial in  $\mathbb{K}[X, Y, Z]$  of degree  $d$ . The dehomogenization of  $f$  is the polynomial  $f^a$  of degree at most  $d$  in  $\mathbb{K}[X, Y]$  such that

$$f^a(a, b) = f(a, b, 1) \text{ for all } (a, b) \in \mathbb{A}^2(\mathbb{K}), \quad (72)$$

i.e.,

$$\mathcal{C}_{\mathbb{K}}(f^a) = \mathcal{C}_{\mathbb{K}}(f) \cap \mathbb{A}^2(\mathbb{K}). \quad (73)$$

## Homogenization and Dehomogenization – Example

- The polynomial  $f = X^3 - Y$  corresponds to the homogeneous polynomial  $f^h = X^3 - YZ^2$  with

$$\mathcal{C}_{\mathbb{R}}(f^h) \cap \mathbb{A}^2(\mathbb{R}) = \mathcal{C}_{\mathbb{R}}(f) = \{(a, a^3) \mid a \in \mathbb{R}\}.$$

- The homogeneous polynomial  $f = X^3 - YZ^2$  corresponds to the dehomogenized polynomial  $f^a = X^3 - Y$  with

$$\mathcal{C}_{\mathbb{R}}(f) \cap \mathbb{A}^2(\mathbb{R}) = \mathcal{C}_{\mathbb{R}}(f^a) = \{(a, a^3) \mid a \in \mathbb{R}\}.$$

## \*Projective Transformations

Given plane projective curve  $\mathcal{C}_{\mathbb{K}}(f)$  with  $f \in \mathbb{K}[X, Y, Z]$  and projective transformation  $A \in \text{PGL}_3(\mathbb{K})$ . Then

$$\mathcal{C}(f^A) = \{A \cdot P \mid P \in \mathcal{C}(f)\}. \quad (74)$$

## Proof.

- Let  $(x : y : z) \in \mathcal{C}(f)$  and  $(x' : y' : z') = A \cdot (x : y : z)$ ; i.e.,  $(x', y', z') = (x, y, z)A$ . Then

$$f^A(x', y', z') = f((x', y', z')A^{-1}) = f(x, y, z) = 0.$$

- Let  $(x' : y' : z') \in \mathcal{C}(f^A)$  and  $(x : y : z) = A^{-1} \cdot (x' : y' : z')$ ; i.e.,  $(x, y, z) = (x', y', z')A^{-1}$  and so  $(x, y, z)A = (x', y', z')$  or  $A \cdot (x : y : z) = (x' : y' : z')$ . Then

$$f(x, y, z) = f((x', y', z')A^{-1}) = f^A(x', y', z') = 0.$$



## \*Projective Transformations – Example

Take the unit parabola  $\mathcal{C}(f)$  given by  $f = X^2 - YZ$  and the projective transformation  $A$  given by

$$(x' : y' : z') = A \cdot (x : y : z) = (x + y : y : z),$$

where

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (75)$$

Then

$$\begin{aligned} f^A(X, Y, Z) &= f((X, Y, Z)A^{-1}) = f(X - Y, Y, Z) \\ &= (X - Y)^2 - YZ. \end{aligned}$$

## \*Projective Transformations

Projective transformations preserve the degree of curves.

## Proof.

Given plane projective curve  $\mathcal{C}(f)$  and projective transformation  $A$  of  $\mathbb{P}^2(\mathbb{K})$ . Consider the plane projective curve  $\mathcal{C}(f^A)$  given by

$$f^A(X, Y, Z) = f((X, Y, Z)A^{-1}).$$

Write  $A^{-1} = (b_{ij})$ . A monomial  $X^i Y^j Z^{d-i-j}$  of degree  $d$  involved in  $f$  is mapped to

$$(b_{11}X + b_{21}Y + b_{31}Z)^i (b_{12}X + b_{22}Y + b_{32}Z)^j (b_{13}X + b_{23}Y + b_{33}Z)^{d-i-j},$$

which is a homogeneous polynomial of degree  $d$ . Since  $f^A$  is a linear combination of such polynomials, it is itself homogeneous of degree  $d$ . □

## \*Factors of Homogeneous Polynomials

Let  $f \in \mathbb{K}[X, Y, Z]$  be a homogeneous polynomial of degree  $d \geq 1$ , and let  $f = gh$ , where  $g$  and  $h$  are non-constant polynomials in  $\mathbb{K}[X, Y, Z]$ . Then  $g$  and  $h$  are homogeneous polynomials, too.

### Proof.

Consider the rational function field  $\mathbb{L} = \mathbb{K}(X, Y, Z)$  and take a new variable  $T$ . We have

$$f(TX, TY, TZ) = f(X, Y, Z) \cdot T^d \in \mathbb{L}[T],$$

$$g(TX, TY, TZ) = \sum_i g_i(X, Y, Z) \cdot T^i \in \mathbb{L}[T],$$

$$h(TX, TY, TZ) = \sum_j h_j(X, Y, Z) \cdot T^j \in \mathbb{L}[T],$$

where the  $g_i$  and  $h_j$  are the homogeneous components of  $g$  and  $h$ , respectively.

\*Proof (cont'd).

Since  $f = gh$ , comparing coefficients gives

$$T^d = \left( \sum_i \frac{g_i(X, Y, Z)}{f(X, Y, Z)} T^i \right) \left( \sum_j \frac{h_j(X, Y, Z)}{f(X, Y, Z)} T^j \right) \in \mathbb{L}[T].$$

It follows that the first factor corresponds to  $T^k$  for some  $k \geq 0$  and the second factor corresponds to  $T^l$  for some  $l \geq 0$  with  $d = k + l$ . Thus all the homogeneous components  $g_i$  except for  $g_k$  are zero and all the homogeneous components  $h_j$  except for  $h_l$  are zero. Hence, the polynomials  $g = g_k$  and  $h = h_l$  are homogeneous.  $\square$

## \*Zero Loci of Homogeneous Polynomials

Let  $f \in \mathbb{K}[X, Y, Z]$  be a homogeneous polynomial of degree  $d \geq 1$ . Given the decomposition of  $f$  as a product of powers of irreducible factors in  $\bar{\mathbb{K}}[X, Y, Z]$ ,

$$f = \prod_{i=1}^s f_i^{e_i}, \quad e_i \geq 1. \quad (76)$$

Then all polynomials  $f_i$  are homogeneous (as shown) and we have

$$\mathcal{C}_{\bar{\mathbb{K}}}(f) = \bigcup_{i=1}^s \mathcal{C}_{\bar{\mathbb{K}}}(f_i). \quad (77)$$

The zero loci  $\mathcal{C}_{\bar{\mathbb{K}}}(f_i)$  are the irreducible components of the curve  $\mathcal{C}_{\bar{\mathbb{K}}}(f)$  and  $e_i$  is the multiplicity of the component  $\mathcal{C}_{\bar{\mathbb{K}}}(f_i)$ ,  $1 \leq i \leq s$ .

## Singularities

Curves,  
Cryptosystems,  
and Quantum  
ComputingK.-H.  
Zimmermann

Contents

Plane Curves

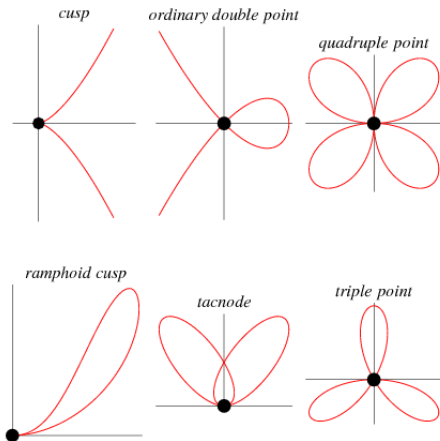
Singularities

Rational  
Mappings

Tangents

Intersection  
Multiplicities

Weierstrass Form



## Definition of Singularity

Let  $f$  be a homogeneous polynomial in  $\mathbb{K}[X, Y, Z]$  of degree  $d$ .

- The projective curve  $\mathcal{C} = \mathcal{C}(f)$  over  $\mathbb{K}$  is *singular* at the point  $P = (a : b : c) \in \mathcal{C}$  if the first partial derivatives of  $f$  at  $P$  vanish,

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f}{\partial Y}(P) = \frac{\partial f}{\partial Z}(P) = 0. \quad (78)$$

Then  $P$  is a *singular point* of  $\mathcal{C}$ . Every other point in  $\mathcal{C}$  is *non-singular*.

Well-definedness:  $f$  is homogeneous and so the partial derivatives are also homogeneous.

## Definition of Singularity

Let  $f$  be a homogeneous polynomial in  $\mathbb{K}[X, Y, Z]$  of degree  $d$ .

- A projective curve  $\mathcal{C} = \mathcal{C}(f)$  is *non-singular* or *smooth* if it has no singular point.

The vanishing of all three derivatives of  $f$  in  $P = (a : b : c)$  is independent of the homogeneous coordinates of  $P$ .

## Example

The homogeneous polynomial  $\ell = \alpha X + \beta Y + \gamma Z \in \mathbb{K}[X, Y, Z]$  of degree 1 gives rise to the projective line

$$\mathcal{L}(\alpha, \beta, \gamma) = \mathcal{L}(\ell) = \{(a : b : c) \in \mathbb{P}^2(\mathbb{K}) \mid \ell(a, b, c) = 0\}. \quad (79)$$

The line  $\mathcal{L}(\ell)$  is non-singular, since for each point  $P$  on the line

$$\frac{\partial \ell}{\partial X}(P) = \alpha, \quad \frac{\partial \ell}{\partial Y}(P) = \beta, \quad \frac{\partial \ell}{\partial Z}(P) = \gamma \quad (80)$$

and  $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ .

## Example

Consider the projective conic given by  $f = X^2 + Y^2 \in \mathbb{K}[X, Y, Z]$ .  
Then

$$\frac{\partial f}{\partial X} = 2X, \quad \frac{\partial f}{\partial Y} = 2Y, \quad \frac{\partial f}{\partial Z} = 0.$$

The point  $P = (0 : 0 : 1)$  is singular.

If  $\text{char}(\mathbb{K}) = 2$ , then every point is singular and so  $\mathcal{C}(f)$  is singular.

## Example

Consider the projective cubic given by  
 $f = X^3 + Y^3 + Z^3 \in \mathbb{K}[X, Y, Z]$ . Then

$$\frac{\partial f}{\partial X} = 3X, \quad \frac{\partial f}{\partial Y} = 3Y, \quad \frac{\partial f}{\partial Z} = 3Z.$$

If  $\text{char}(\mathbb{K}) \neq 3$ , this cubic is smooth.

If  $\text{char}(\mathbb{K}) = 3$ , then  $f = (X + Y + Z)^3$  and so

$$\frac{\partial f}{\partial X} = \frac{\partial f}{\partial Y} = \frac{\partial f}{\partial Z} = 3(X + Y + Z)^2 = 0,$$

i.e., all points are singular and so  $\mathcal{C}(f)$  is singular.

## Example

Consider the twisted cubic given by  $f = X^2Y - Z^3 \in \mathbb{K}[X, Y, Z]$ .  
Then

$$\frac{\partial f}{\partial X} = 2XY, \quad \frac{\partial f}{\partial Y} = X^2, \quad \frac{\partial f}{\partial Z} = -3Z^2.$$

It has one singularity at  $P = (0 : 1 : 0)$ , since

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f}{\partial Y}(P) = \frac{\partial f}{\partial Z}(P) = 0.$$

All other points are non-singular. For this, consider the points  $(a : b : 1)$ ,  $(a : 1 : 0)$  with  $a \neq 0$ , and  $(1 : 0 : 0)$ .

## Intersection of Plane Curves

Let  $\mathcal{C}_1 = \mathcal{C}(f_1)$  and  $\mathcal{C}_2 = \mathcal{C}(f_2)$  be plane projective curves over  $\mathbb{K}$ , and let  $P$  be a point of the intersection  $\mathcal{C}_1 \cap \mathcal{C}_2$ . Then  $P$  is a singular point of  $\mathcal{C}(f_1 f_2)$ .

### Proof.

By the product rule,

$$\frac{\partial f_1 f_2}{\partial X}(P) = \frac{\partial f_1}{\partial X}(P) f_2(P) + f_1(P) \frac{\partial f_2}{\partial X}(P) = 0,$$

since  $f_1(P) = 0 = f_2(P)$ . The same holds for the other variables  $Y$  and  $Z$ . □

## Affine vs. Projective Singularities

Let  $f$  be a homogeneous polynomial in  $\mathbb{K}[X, Y, Z]$  of degree  $d$  and let  $f^a$  denote the corresponding dehomogenized polynomial in  $\mathbb{K}[X, Y]$ .

The plane projective curve  $\mathcal{C}(f)$  is singular at  $P = (a : b : 1)$  iff the plane affine curve  $\mathcal{C}(f^a)$  is singular at  $Q = (a, b)$ .

### Proof.

The point  $P = (a : b : 1)$  lies in  $\mathcal{C}(f)$  iff the point  $Q = (a, b)$  belongs to  $\mathcal{C}(f^a)$ . Write

$$f = \sum_{\substack{i, j \geq 0 \\ i+j \leq d}} a_{ij} X^i Y^j Z^{d-i-j}.$$

Then

$$f^a = \sum_{\substack{i, j \geq 0 \\ i+j \leq d}} a_{ij} X^i Y^j.$$

## Proof (cont'd).

We have

$$\frac{\partial f}{\partial X} = \sum_{\substack{i>0, j \geq 0 \\ i+j \leq d}} i a_{ij} X^{i-1} Y^j Z^{d-i-j}$$

and

$$\frac{\partial f^a}{\partial X} = \sum_{\substack{i>0, j \geq 0 \\ i+j \leq d}} i a_{ij} X^{i-1} Y^j.$$

Thus

$$\frac{\partial f}{\partial X}(P) = \frac{\partial f^a}{\partial X}(Q).$$

Similarly,

$$\frac{\partial f}{\partial Y}(P) = \frac{\partial f^a}{\partial Y}(Q).$$

## Proof (cont'd).

Moreover,

$$\frac{\partial f}{\partial Z} = \sum_{\substack{i,j \geq 0 \\ i+j < d}} (d-i-j)a_{ij}X^iY^jZ^{d-i-j-1}.$$

Thus

$$\begin{aligned} \frac{\partial f}{\partial Z}(P) &= \sum_{\substack{i,j \geq 0 \\ i+j \leq d}} (d-i-j)a_{ij}a^ib^j \\ &= d \cdot f^a(Q) - a \cdot \frac{\partial f^a}{\partial X}(Q) - b \cdot \frac{\partial f^a}{\partial Y}(Q). \end{aligned}$$

In the next to the last sum, we can allow  $i+j \leq d$  since the term with  $d=i+j$  vanishes in the derivative. From these equations the result follows.  $\square$

## Example

- The projective conic given by  $f = X^2 + Y^2 \in \mathbb{K}[X, Y, Z]$  is singular at  $P = (0 : 0 : 1)$ , since the partial derivatives are

$$\frac{\partial f}{\partial X} = 2X, \quad \frac{\partial f}{\partial Y} = 2Y, \quad \frac{\partial f}{\partial Z} = 0.$$

If  $\text{char}(\mathbb{K}) = 2$ , each point is singular.

- The affine conic given by  $f^a = X^2 + Y^2 \in \mathbb{K}[X, Y]$  is singular at  $Q = (0, 0)$ , since the partial derivatives are

$$\frac{\partial f^a}{\partial X} = 2X, \quad \frac{\partial f^a}{\partial Y} = 2Y.$$

If  $\text{char}(\mathbb{K}) = 2$ , each point is singular.

## Example

- The projective conic given by  $f = XZ + YZ \in \mathbb{K}[X, Y, Z]$  is non-singular at  $P = (a : -a : 1)$ , since the partial derivatives are

$$\frac{\partial f}{\partial X} = Z, \quad \frac{\partial f}{\partial Y} = Z, \quad \frac{\partial f}{\partial Z} = X + Y$$

with

$$\frac{\partial f}{\partial X}(P) = 1, \quad \frac{\partial f}{\partial Y}(P) = 1, \quad \frac{\partial f}{\partial Z}(P) = 0.$$

- The affine line given by  $f^a = X + Y \in \mathbb{K}[X, Y]$  is non-singular at  $Q = (a, -a)$ , since the partial derivatives are

$$\frac{\partial f^a}{\partial X} = 1, \quad \frac{\partial f^a}{\partial Y} = 1.$$

## \*Projective Transformations

Projective transformations preserve singularities.

## Proof.

Given plane projective curve  $\mathcal{C}(f)$  and projective transformation  $A$  of  $\mathbb{P}^2(\mathbb{K})$ . Consider the plane projective curve  $\mathcal{C}(f^A)$  given by

$$f^A(X, Y, Z) = f((X, Y, Z)A^{-1}).$$

By the chain rule,

$$\left( \frac{\partial f}{\partial X}, \frac{\partial f}{\partial Y}, \frac{\partial f}{\partial Z} \right) = \left( \frac{\partial f^A}{\partial X}, \frac{\partial f^A}{\partial Y}, \frac{\partial f^A}{\partial Z} \right) \cdot A. \quad (81)$$

Since  $A$  is invertible,  $\mathcal{C}(f)$  is non-singular iff  $\mathcal{C}(f^A)$  is non-singular. □

## Rational Mappings

A curve is *rational* if it is birationally equivalent to a line.



Contents

Plane Curves

Singularities

**Rational  
Mappings**

Tangents

Intersection  
Multiplicities

Weierstrass Form

## Rational Mappings

Given two plane projective curves  $\mathcal{C}_1$  and  $\mathcal{C}_2$  over  $\mathbb{K}$  and homogeneous polynomials  $g_0, g_1, g_2, h_0, h_1, h_2 \in \mathbb{K}[X, Y, Z]$ .

A mapping  $\phi : \mathcal{C}_1 \rightarrow \mathcal{C}_2$  is *rational* over  $\mathbb{K}$  if for almost all points  $(x : y : z) \in \mathcal{C}_1(\overline{\mathbb{K}})$ , the expression

$$\phi(x : y : z) = \left( \frac{g_0(x, y, z)}{h_0(x, y, z)} : \frac{g_1(x, y, z)}{h_1(x, y, z)} : \frac{g_2(x, y, z)}{h_2(x, y, z)} \right) \quad (82)$$

is defined and lies in  $\mathcal{C}_2(\overline{\mathbb{K}})$ .

## Example

Take the line  $f_1 = Z$  and the conic  $f_2 = Y^2 - XZ$  in  $\mathbb{K}[X, Y, Z]$ .

- The zero loci are

$$\mathcal{C}(f_1) = \{(x : 1 : 0) \mid x \in \bar{\mathbb{K}}\} \cup \{(1 : 0 : 0)\}$$

and

$$\mathcal{C}(f_2) = \{(x^2 : x : 1) \mid x \in \bar{\mathbb{K}}\} \cup \{(1 : 0 : 0)\}.$$

- The polynomials  $g_0 = X^2$ ,  $g_1 = XY$ , and  $g_2 = Y^2$  provide a rational mapping

$$\phi : \mathcal{C}(f_1) \rightarrow \mathcal{C}(f_2) : (x : y : z) \mapsto (x^2 : xy : y^2)$$

with  $\phi(x : 1 : 0) = (x^2 : x : 1)$  and  $\phi(1 : 0 : 0) = (1 : 0 : 0)$ .

## Birational Mappings

Given two plane projective curves  $\mathcal{C}_1$  and  $\mathcal{C}_2$  over  $\mathbb{K}$ .

- A rational mapping  $\phi : \mathcal{C}_1 \rightarrow \mathcal{C}_2$  defined over  $\mathbb{K}$  is *birational* if there is a rational mapping  $\psi : \mathcal{C}_2 \rightarrow \mathcal{C}_1$  defined over  $\mathbb{K}$  such that for almost all points of  $\mathcal{C}_1(\overline{\mathbb{K}})$  and  $\mathcal{C}_2(\overline{\mathbb{K}})$ , the mappings  $\phi \circ \psi$  and  $\psi \circ \phi$  are defined and are equal to the identity; i.e., a birational mapping is bijective almost everywhere.
- Two plane projective curves  $\mathcal{C}_1$  and  $\mathcal{C}_2$  over  $\mathbb{K}$  are *birationally equivalent over  $\mathbb{K}$*  if there is a birational mapping  $\phi : \mathcal{C}_1 \rightarrow \mathcal{C}_2$  defined over  $\mathbb{K}$ .

## Example

The zero loci of the line  $f_1 = Z$  and the conic  $f_2 = Y^2 - XZ$  in  $\mathbb{K}[X, Y, Z]$  are birationally equivalent over  $\mathbb{K}$  by the rational mappings

$$\phi(x : y : z) = (x^2 : xy : y^2)$$

and

$$\psi(x : y : z) = (y : z : 0),$$

since

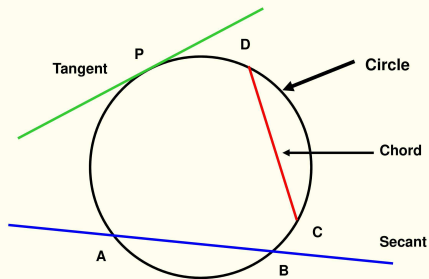
$$\phi(x : 1 : 0) = (x^2 : x : 1), \quad \phi(1 : 0 : 0) = (1 : 0 : 0)$$

and

$$\psi(x^2 : x : 1) = (x : 1 : 0), \quad \psi(1 : 0 : 0) \text{ undefined.}$$

## Tangents

## Formation of tangent



## Tangents

Let  $\mathcal{C} = \mathcal{C}(f)$  be a plane projective curve in  $\mathbb{P}^2(\mathbb{K})$  and let  $P$  be a non-singular point on  $\mathcal{C}$  defined over  $\mathbb{K}$ .

The projective line

$$\mathcal{L} = \mathcal{L} \left( \frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial Y}(P), \frac{\partial f}{\partial Z}(P) \right) \quad (83)$$

is the *tangent line* to  $\mathcal{C}$  at  $P$  (see (79)).

The tangent line  $\mathcal{L}$  is well-defined, since  $P$  is non-singular and so the partial derivatives do not vanish altogether at  $P$ .

## Example

The cubic  $\mathcal{C}(f)$  given by

$$f = Y^2Z - X^3 - XZ^2 \in \mathbb{R}[X, Y, Z]$$

is non-singular with partial derivatives

$$\frac{\partial f}{\partial X} = -3X^2 - Z^2,$$

$$\frac{\partial f}{\partial Y} = 2YZ,$$

$$\frac{\partial f}{\partial Z} = Y^2 - 2XZ.$$

The tangent line to  $\mathcal{C}$  at  $P = (0 : 1 : 0)$  is

$$\mathcal{L}([-3X^2 - Z^2](P), [2YZ](P), [Y^2 - 2XZ](P)) = \mathcal{L}(0, 0, 1),$$

given by the homogeneous polynomial  $\ell = Z$ .

## \*Example

- The projective unit parabola  $\mathcal{C} = \mathcal{C}(f)$  with  $f = X^2 - YZ \in \mathbb{R}[X, Y, Z]$  is non-singular with partial derivatives

$$\frac{\partial f}{\partial X} = 2X, \quad \frac{\partial f}{\partial Y} = -Z, \quad \frac{\partial f}{\partial Z} = -Y.$$

The point  $P = (1 : 1 : 1) \in \mathcal{C}$  has tangent line  $\mathcal{L}(2, -1, -1)$ .

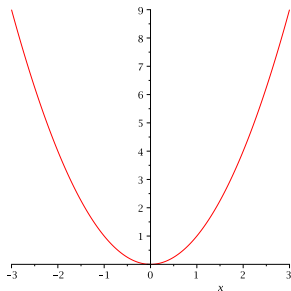
- In view of the projective transformation  $A$  in (75), the cubic  $\mathcal{C}^A = \mathcal{C}(f^A)$  with  $f^A(X, Y, Z) = (X - Y)^2 - YZ$  is non-singular with partial derivatives

$$\frac{\partial f^A}{\partial X} = 2(X - Y), \quad \frac{\partial f^A}{\partial Y} = -2(X - Y) - Z, \quad \frac{\partial f^A}{\partial Z} = -Y.$$

The point  $P' = A \cdot P = (2 : 1 : 1) \in \mathcal{C}^A$  has tangent line  $\mathcal{L}(2, -3, -1)$ .

## Intersection Multiplicities

Intersection of  $X$ -axis with parabola  $Y = X^2$  has degree 2.



## Intersection Multiplicities

Given plane projective curve  $\mathcal{C} = \mathcal{C}(f)$  in  $\mathbb{P}^2(\mathbb{K})$  and projective line  $\mathcal{L}$  in  $\mathbb{P}^2(\mathbb{K})$ .

- Fix a point  $P = (a : b : c) \in \mathcal{L}$  and an auxiliary point  $P' = (a' : b' : c') \in \mathcal{L}$ .
- The *intersection multiplicity* of  $\mathcal{L}$  and  $\mathcal{C}$  at  $P$ , denoted  $i(P, \mathcal{L}, \mathcal{C})$ , is the order of zero of the polynomial

$$\phi(t) = f(a + ta', b + tb', c + tc') \in \mathbb{K}[t]. \quad (84)$$

## Order of Zero

- The *order of zero* of a polynomial

$$\phi(t) = \alpha_0 + \alpha_1 t + \dots + \alpha_m t^m \in \mathbb{K}[t]$$

is the smallest index  $j \geq 0$  such that

$$\alpha_0 = 0, \alpha_1 = 0, \dots, \alpha_{j-1} = 0, \text{ and } \alpha_j \neq 0.$$

- Equivalently, the order of zero of  $\phi(t)$  is the smallest index  $j \geq 0$  such that the derivatives of  $\phi(t)$  satisfy

$$\phi(0) = 0, \phi'(0) = 0, \dots, \phi^{(j-1)}(0) = 0, \text{ and } \phi^{(j)}(0) \neq 0.$$

- Example: The polynomials  $2t + t^2$  and  $t^3 - t^5$  in  $\mathbb{K}[t]$  have order of zero 1 and 3, respectively.

## Basic Facts

- The definition of intersection multiplicity is independent of the choice of auxiliary point  $P'$ .
- The constant term of polynomial  $\phi(t)$  is  $f(a, b, c)$  and thus the point  $P = (a : b : c)$  lies on the curve  $\mathcal{C}$  iff  $\phi(0) = 0$ , i.e.,  $i(P, \mathcal{L}, \mathcal{C}) \geq 1$ .
- Thus for each point  $P$  on the line  $\mathcal{L}$ , which does not belong to the curve  $\mathcal{C}$ , we have  $\phi(0) \neq 0$ , i.e.,  $i(P, \mathcal{L}, \mathcal{C}) = 0$ .
- Define  $i(P, \mathcal{L}, \mathcal{C}) = 0$  if the point  $P$  does not belong to the line  $\mathcal{L}$ .
- If  $\mathcal{C}(f)$  is a plane projective curve of degree  $d \geq 1$ , then

$$i(P, \mathcal{L}, \mathcal{C}) \leq d, \quad (85)$$

since the arguments of  $f$  as polynomials in  $t$  are linear and so  $\phi(t)$  has degree  $\leq d$ .

## Basic Facts – Explanation

Take the homogeneous polynomial of degree  $d$ ,

$$f = \sum_{\alpha} a_{\alpha} X^{\alpha} \in \mathbb{K}[X_0, X_1, X_2],$$

where  $a_{\alpha} \in \mathbb{K}$ ,  $\alpha_0 + \alpha_1 + \alpha_2 = d$ , and  $X^{\alpha} = X_0^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2}$ . Then

$$\begin{aligned} \phi(t) &= f(a + ta', b + tb', c + tc') \\ &= \sum_{\alpha} a_{\alpha} (a + ta')^{\alpha_0} (b + tb')^{\alpha_1} (c + tc')^{\alpha_2} \\ &= f(a, b, c)t^0 + u_1 t^1 + \dots + u_d t^d, \end{aligned}$$

where  $u_1, \dots, u_d \in \mathbb{K}$ .

## Example

- Consider the conic  $\mathcal{C} = \mathcal{C}(f)$  given by  $f = X^2 - YZ$  in  $\mathbb{R}[X, Y, Z]$ .
- Take the projective line  $\mathcal{L} = \mathcal{L}(1, -1, 0)$ .
- The point  $P = (0 : 0 : 1)$  lies in the intersection  $\mathcal{C} \cap \mathcal{L}$ .
- Fix the auxiliary point  $P' = (1 : 1 : 1) \in \mathcal{L}$ .
- Then

$$\begin{aligned}\phi(t) &= f(0 + 1 \cdot t, 0 + 1 \cdot t, 1 + 1 \cdot t) \\ &= f(t, t, 1 + t) = t^2 - t(1 + t) = -t\end{aligned}$$

and so  $i(P, \mathcal{L}, \mathcal{C}) = 1$ .

## Example

- Consider the cubic  $\mathcal{C} = \mathcal{C}(f)$  given by  $f = Y^2Z - X^3 - XZ^2$  in  $\mathbb{R}[X, Y, Z]$ .
- Take the projective line  $\mathcal{L} = \mathcal{L}(1, 0, 1)$ .
- The point  $P = (0 : 1 : 0)$  lies in the intersection  $\mathcal{C} \cap \mathcal{L}$ .
- Fix the auxiliary point  $P' = (1 : 0 : -1) \in \mathcal{L}$ .
- Then

$$\begin{aligned}\phi(t) &= f(0 + 1 \cdot t, 1 + 0 \cdot t, 0 + (-1) \cdot t) \\ &= f(t, 1, -t) = (-t) - t^3 - t(-t)^2 = -t - 2t^3\end{aligned}$$

and so  $i(P, \mathcal{L}, \mathcal{C}) = 1$ .

## Intersection Multiplicities – Tangents

Let  $\mathcal{L} = \mathcal{L}(\alpha, \beta, \gamma)$  be a tangent line to plane projective curve  $\mathcal{C} = \mathcal{C}(f)$  at non-singular point  $P = (a : b : c) \in \mathcal{C}$  defined over  $\mathbb{K}$ . Then

$$i(P, \mathcal{L}, \mathcal{E}) \geq 2. \quad (86)$$

## Proof.

Since  $P$  lies on the curve  $\mathcal{C}$ ,  $\phi(0) = f(a, b, c) = 0$ . Moreover, since  $\mathcal{L} = \mathcal{L}(\alpha, \beta, \gamma)$  is the tangent line to  $\mathcal{C}$  at  $P$ ,

$$\alpha = \frac{\partial f}{\partial X}(a, b, c), \quad \beta = \frac{\partial f}{\partial Y}(a, b, c), \quad \gamma = \frac{\partial f}{\partial Z}(a, b, c).$$

By taking another point  $P' = (a' : b' : c') \in \mathcal{L}$ , the chain rule gives

$$\begin{aligned} \phi'(0) &= \frac{\partial f}{\partial X}(a, b, c) \cdot a' + \frac{\partial f}{\partial Y}(a, b, c) \cdot b' + \frac{\partial f}{\partial Z}(a, b, c) \cdot c' \\ &= \alpha a' + \beta b' + \gamma c' \end{aligned}$$

which equals 0 since  $P' \in \mathcal{L}$ . Hence,  $i(P, \mathcal{L}, \mathcal{E}) \geq 2$ . □

## Example

- Consider the conic  $\mathcal{C} = \mathcal{C}(f)$  given by  $f = X^2 - YZ$ .
- Take the point  $P = (0 : 0 : 1) \in \mathcal{C}$ .
- The corresponding tangent at  $P$  is  $\mathcal{L} = \mathcal{L}(0, -1, 0)$ , since

$$\frac{\partial f}{\partial X}(P) = 0, \quad \frac{\partial f}{\partial Y}(P) = -1, \quad \frac{\partial f}{\partial Z}(P) = 0.$$

- Take the auxiliary point  $P' = (1 : 0 : 1) \in \mathcal{L}$ .
- Then

$$\phi(t) = f(0 + 1 \cdot t, 0 + 0 \cdot t, 1 + 1 \cdot t) = f(t, 0, 1 + t) = t^2$$

and so  $i(P, \mathcal{L}, \mathcal{C}) = 2$ .

## Example

- The cubic  $\mathcal{C}(f)$  given by  $f = Y^2Z - X^3 - XZ^2$  is non-singular at the point  $P = (0 : 1 : 0)$ .
- The corresponding tangent line is  $\mathcal{L} = \mathcal{L}(0, 0, 1)$ , since

$$\frac{\partial f}{\partial X}(P) = 0, \quad \frac{\partial f}{\partial Y}(P) = 0, \quad \frac{\partial f}{\partial Z}(P) = 1.$$

- Take the auxiliary point  $P' = (1 : 1 : 0) \in \mathcal{L}$ .
- Then

$$\phi(t) = f(0 + 1 \cdot t, 1 + 1 \cdot t, 0 + 0 \cdot t) = f(t, 1 + t, 0) = -t^3$$

and so  $i(P, \mathcal{L}, \mathcal{C}) = 3$ ; i.e.,  $P$  is a *flex* of  $\mathcal{C}$ .

## Example – Circle

Consider the complex conic  $\mathcal{C} = \mathcal{C}(f)$  given by

$$f = X^2 + Y^2 - Z^2 \in \mathbb{C}[X, Y, Z].$$

- The conic consists of the affine points

$$\left( \frac{a}{\sqrt{a^2 + b^2}} : \frac{b}{\sqrt{a^2 + b^2}} : 1 \right), \quad (a, b) \neq (0, 0),$$

and the point at infinity  $(i : 1 : 0)$ .

- The conic is smooth, since the partial derivatives do not vanish altogether,

$$\frac{\partial f}{\partial X} = 2X, \quad \frac{\partial f}{\partial Y} = 2Y, \quad \frac{\partial f}{\partial Z} = -2Z.$$

## Example (cont'd)

- The affine point  $P = \left( \frac{a}{\sqrt{a^2+b^2}} : \frac{b}{\sqrt{a^2+b^2}} : 1 \right) \in \mathcal{C}$  has tangent line

$$\begin{aligned} & \mathcal{L}(2X(P), 2Y(P), -2Z(P)) \\ &= \mathcal{L}\left(\frac{a}{\sqrt{a^2+b^2}}, \frac{b}{\sqrt{a^2+b^2}}, -1\right). \end{aligned}$$

Taking the auxiliary point  $P' = (-b : a : 0) \in \mathcal{L}$  gives

$$\begin{aligned} \phi(t) &= f\left(\frac{a}{\sqrt{a^2+b^2}} + (-b)t, \frac{b}{\sqrt{a^2+b^2}} + at, 1\right) \\ &= (a^2 + b^2)t^2 \end{aligned}$$

and so  $i(P, \mathcal{L}, \mathcal{C}) = 2$ .

## Example (cont'd)

- The point at infinity  $Q = (i : 1 : 0) \in \mathcal{C}$  has tangent line

$$\mathcal{L}(2X(Q), 2Y(Q), -2Z(Q)) = \mathcal{L}(i : 1 : 0).$$

Taking the auxiliary point  $Q' = (0 : 0 : 1) \in \mathcal{L}$  gives

$$\phi(t) = f(i, 1, t) = i^2 + 1^2 - t^2 = -t^2$$

and so  $i(Q, \mathcal{L}, \mathcal{C}) = 2$ .

## \*Projective Transformations

Projective transformations preserve multiplicities.

## Proof.

Given plane projective curve  $\mathcal{C}(f)$  and projective transformation  $A$  of  $\mathbb{P}^2(\mathbb{K})$ . Consider the plane projective curve  $\mathcal{C}(f^A)$  given by

$$f^A(X, Y, Z) = f((X, Y, Z)A^{-1}).$$

It is easy to check that the intersection multiplicities  $i(P, \mathcal{L}, \mathcal{C}(f))$  and  $i(A^{-1}P, \mathcal{L}^A, \mathcal{C}(f^A))$  coincide, where  $\mathcal{L} = \mathcal{L}(\ell)$  and  $\mathcal{L}^A = \mathcal{L}(\ell^A)$  with  $\ell^A(X, Y, Z) = \ell((X, Y, Z)A^{-1})$ . □

## Weierstrass Form



Karl Weierstrass (1815-1897)

## General Cubics

A general cubic over  $\mathbb{K}$  has the form

$$\begin{aligned} f = & a_{yyy}Y^3 + a_{xyy}XY^2 + a_{xxy}X^2Y + a_{yyz}Y^2Z \\ & + a_{xyz}XYZ + a_{yzz}YZ^2 + a_{xxx}X^3 + a_{xxz}X^2Z \\ & + a_{xzz}XZ^2 + a_{zzz}Z^3. \end{aligned} \tag{87}$$

## Geometric Condition on Cubics I

The cubic (87) is to pass through the point at infinity  $O = (0 : 1 : 0)$ . Then

$$a_{yyy} = 0. \quad (88)$$

### Proof.

We have  $f(O) = a_{yyy}$  and so  $a_{yyy} = 0$ . □

## Geometric Condition on Cubics II

Let  $a_{yyy} = 0$ .

The cubic (87) is to have  $O = (0 : 1 : 0)$  as non-singular point.

Then

$$a_{xyy} \neq 0 \text{ or } a_{yyz} \neq 0. \quad (89)$$

**Proof.**

We have

$$\frac{\partial f}{\partial X}(O) = a_{xyy}, \quad \frac{\partial f}{\partial Y}(O) = 3a_{yyy} = 0, \quad \frac{\partial f}{\partial Z}(O) = a_{yyz}.$$

Thus  $a_{xyy} \neq 0$  or  $a_{yyz} \neq 0$ . □

## Geometric Condition on Cubics III

Let  $a_{yyy} = 0$ , and  $a_{xyy} \neq 0$  or  $a_{yyz} \neq 0$ .

The cubic (87) is to have  $\mathcal{L} = \mathcal{L}(0, 0, 1)$  as tangent line at  $O = (0 : 1 : 0)$ . Then

$$a_{xyy} = 0 \text{ and so } a_{yyz} \neq 0. \quad (90)$$

### Proof.

We have

$$\frac{\partial f}{\partial X}(O) = a_{xyy}, \quad \frac{\partial f}{\partial Y}(O) = 3a_{yyy} = 0, \quad \frac{\partial f}{\partial Z}(O) = a_{yyz}.$$

Thus the tangent line is  $\mathcal{L} = \mathcal{L}(a_{xyy}, 0, a_{yyz})$ . By hypothesis,  $\mathcal{L} = \mathcal{L}(0, 0, 1)$  and so  $a_{xyy} = 0$  and  $a_{yyz} \neq 0$ . □

## Geometric Condition on Cubics IV

Let  $a_{yyy} = 0$ ,  $a_{xyy} = 0$  and  $a_{yyz} \neq 0$ .

The tangent line  $\mathcal{L} = \mathcal{L}(0, 0, 1)$  to the cubic (87) at  $O = (0 : 1 : 0)$  is to be a flex; i.e.,  $i(O, \mathcal{L}, \mathcal{C}) = 3$ . Then

$$a_{xxy} = 0 \text{ and } a_{xxx} \neq 0. \quad (91)$$

### Proof.

Taking the auxiliary point  $P' = (1 : 1 : 0) \in \mathcal{L}$  gives

$$\begin{aligned} \phi(t) &= f(0 + 1 \cdot t, 1 + 1 \cdot t, 0 + 0 \cdot t) \\ &= f(t, 1 + t, 0) \\ &= a_{yyy}(1+t)^3 + a_{xyy}t(1+t)^2 + a_{xxy}t^2(1+t) + a_{xxx}t^3 \\ &= a_{xxy}t^2(1+t) + a_{xxx}t^3 \\ &= a_{xxy}t^2 + (a_{xxy} + a_{xxx})t^3. \end{aligned}$$

By hypothesis,  $O$  is a flex and so  $a_{xxy} = 0$  and  $a_{xxx} \neq 0$ . □

## Weierstrass Form

When the conditions I-IV are met, i.e.,

$$a_{yyy} = 0, a_{xyy} = 0, a_{xxy} = 0, a_{yyz} \neq 0, a_{xxx} \neq 0, \quad (92)$$

the cubic (87) becomes

$$\begin{aligned} f = & a_{yyz}Y^2Z + a_{xyz}XYZ + a_{yzz}YZ^2 \\ & + a_{xxx}X^3 + a_{xxz}X^2Z + a_{xzz}XZ^2 + a_{zzz}Z^3 \end{aligned} \quad (93)$$

with  $a_{yyz} \neq 0$  and  $a_{xxx} \neq 0$ .

By a projective transformation, the cubic becomes

$$\begin{aligned} f = & Y^2Z + a_1XYZ + a_3YZ^2 \\ & - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3. \end{aligned} \quad (94)$$

This cubic is in *Weierstrass form*.

## Weierstrass Form

There is a projective transformation that transforms the cubic (93) to the cubic (94).

### Proof.

Let  $t \in \mathbb{K}^*$ . Put  $A = \text{diag}(t^{-1}, t^{-1}, 1)$ . Then

$$\begin{aligned} f^A(X, Y, Z) &= f((X, Y, Z)A^{-1}) \\ &= f(tX, tY, Z) \\ &= a_{yyz}(t^2Y^2Z) + \dots + a_{xxx}(t^3X^3) + \dots \end{aligned}$$

Putting  $t = -a_{yyz}/a_{xxx}$  shows that the coefficients of  $Y^2Z$  and  $X^3$  have the same value and different sign. This gives the required transformation.  $\square$

## \*Cubic Case of Fermat's Last Theorem

Consider the projective cubic given by

$$X^3 + Y^3 = Z^3. \quad (95)$$

- Fermat showed that the only  $\mathbb{Q}$ -rational solutions are the trivial ones:  $(1 : 0 : 1)$ ,  $(0 : 1 : 1)$  and  $(1 : -1 : 0)$ .
- If  $(x : y : 1)$  satisfies  $X^2 + Y^2 = 1$  and  $(x' : y' : 1)$  satisfies  $Y^2 - 9Y = X^3 - 27$ , the relationships are

$$\begin{aligned} x' &= \frac{3x}{1-y}, & x &= \frac{3x'}{y'}, \\ y' &= \frac{9}{1-y}, & y &= \frac{y'-9}{y'}. \end{aligned}$$

This gives a projective transformation between the affine points that leads to the affine cubic

$$Y^2 - 9Y = X^3 - 27 \quad (96)$$

with corresponding solutions  $(3 : 9 : 1)$ ,  $(0 : 1 : 0)$ ,  $(3 : 0 : 1)$ .

# Part IV

## Introduction to Elliptic Curves

## Elliptic Curves

- Weierstrass form
- Discriminant
- \*j-Invariant
- Singular points
- Intersection multiplicities
- Group law
- Group law in coordinates
- Use of Singular

## Weierstrass Form



Karl Weierstrass (1815-1897)

## Weierstrass Polynomials and Equations

Let  $\mathbb{K}$  be a field.

- The polynomial

$$f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \quad (97)$$

in  $\mathbb{K}[X, Y, Z]$  is called *Weierstrass polynomial* over  $\mathbb{K}$ .

- The equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (98)$$

is called *Weierstrass equation* over  $\mathbb{K}$ .

## Basic Facts

Consider the decomposition of the projective plane

$$\mathbb{P}^2(\mathbb{K}) = \mathbb{A}^2(\mathbb{K}) \cup \mathbb{L}(\mathbb{K}) \cup \{(1 : 0 : 0)\}. \quad (99)$$

- For each point  $P = (a : 1 : 0) \in \mathcal{E}(f) \cap \mathbb{L}(\mathbb{K})$  on the line,  $f(a, 1, 0) = -a^3 = 0$  and so  $a = 0$ .
- The point  $O = (0 : 1 : 0)$  lies in  $\mathcal{E}(f)$  called *base point*.
- The point  $(1 : 0 : 0)$  does not lie in  $\mathcal{E}(f)$ , since  $f(1, 0, 0) = -1$ .
- The base point  $O$  is the only point at infinity in  $\mathcal{E}(f)$ ; i.e., the only point on the curve not in the affine plane  $\mathbb{A}^2(\mathbb{K})$ .
- The base point  $O$  is non-singular:

$$\frac{\partial f}{\partial Z}(O) = \quad (100)$$

$$[Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4X - 3a_6Z^2](O) = 1.$$

## Elliptic Curves

- An *elliptic curve*  $\mathcal{E}(f)$  over  $\mathbb{K}$  is a non-singular cubic over  $\mathbb{K}$  which is in Weierstrass form  $f$ .
- A curve in Weierstrass form can be tested for non-singularity by testing only the affine points  $(a : b : 1) \in \mathbb{A}^2(\mathbb{K})$ ; the base point  $O$  is always non-singular.
- Simplification of Weierstrass form depends on the characteristic of  $\mathbb{K}$ .

## Characteristic of a Field

---

## Simplification of Weierstrass Form

If  $\text{char}(\mathbb{K}) \neq 2$ , the elliptic curve  $\mathcal{E}(f)$  is birationally equivalent to the elliptic curve  $\mathcal{E}(h_1)$ , where

$$h_1 = Y^2Z - X^3 - \frac{1}{4}b_2X^2Z - \frac{1}{2}b_4XZ^2 - \frac{1}{4}b_6Z^3 \quad (101)$$

and

$$b_2 = a_1^2 + 4a_2, \quad (102)$$

$$b_4 = 2a_4 + a_1a_3, \quad (103)$$

$$b_6 = a_3^2 + 4a_6. \quad (104)$$

## Proof.

By a projective transformation, the mapping

$$\phi_1 : \mathbb{P}^2 \rightarrow \mathbb{P}^2 : (a : b : c) \mapsto \left( a : b + \frac{a_1}{2}a + \frac{a_3}{2}c : c \right)$$

is bijective and its inverse is

$$\phi_1^{-1} : \mathbb{P}^2 \rightarrow \mathbb{P}^2 : (a : b : c) \mapsto \left( a : b - \frac{a_1}{2}a - \frac{a_3}{2}c : c \right).$$

Note that the denominators are nonzero in  $\mathbb{K}$ .

We have

$$h_1(X, Y, Z) = f \left( X, Y - \frac{a_1}{2}X - \frac{a_3}{2}Z, Z \right).$$



## Simplification of Weierstrass Form in Maple

Implementation of rational mapping:

```

> f := Y^2*Z + a_1*X*Y*Z + a_3*Y*Z^2 - X^3
      - a_2*X^2*Z - a_4*X*Z^2 - a_6*Z^3;
> subs( { Y = Y - a_1/2 * X - a_3/2 * Z }, f);
> simplify(%);
> h_1 := collect(%, [X,Y,Z]);

```

## Simplification of Weierstrass Form

If  $\text{char}(\mathbb{K}) \neq 2, 3$ , the elliptic curve  $\mathcal{E}(f)$  is birationally equivalent to the elliptic curve  $\mathcal{E}(h_2)$ , where

$$h_2 = Y^2Z - X^3 + 27c_4XZ^2 + 54c_6Z^3 \quad (105)$$

and

$$c_4 = b_2^2 - 24b_4, \quad (106)$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \quad (107)$$

## Proof.

By a projective transformation, the mapping

$$\phi_2 : \mathbb{P}^2 \rightarrow \mathbb{P}^2 : (a : b : c) \mapsto (36a + 3b_2c : 216b : c)$$

is bijective and its inverse is

$$\phi_2^{-1} : \mathbb{P}^2 \rightarrow \mathbb{P}^2 : (a : b : c) \mapsto \left( \frac{1}{36}a - \frac{b_2}{12}c : \frac{1}{216}b : c \right).$$

Note that the denominators are nonzero in  $\mathbb{K}$ , since  $36 = 2^2 3^2$ ,  $12 = 2^2 3$ , and  $216 = 2^3 3^3$ .

We have

$$h_2(X, Y, Z) = 2^6 3^6 h_1 \left( \frac{1}{36}X - \frac{b_2}{12}Z, \frac{1}{216}Y, Z \right).$$



## Simplification of Weierstrass Form

If  $\text{char}(\mathbb{K}) = 2$  and  $a_1 \neq 0$ , the elliptic curve  $\mathcal{E}(f)$  is birationally equivalent to the elliptic curve  $\mathcal{E}(h_3)$ , where

$$h_3 = Y^2Z + XYZ - X^3 - a'_2X^2Z - a'_6Z^3 \quad (108)$$

and

$$a'_2 = \frac{a_3 + a_1a_2}{a_1^3}, \quad (109)$$

$$a'_6 = \frac{a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_1^3a_3^3 + a_3^4}{a_1^{12}}. \quad (110)$$

## Proof.

By a projective transformation, the mapping

$$\phi_3 : \mathbb{P}^2 \rightarrow \mathbb{P}^2 : (a : b : c) \mapsto \left( \frac{1}{a_1^2}a - \frac{a_3}{a_1^3}c : \frac{1}{a_1^3}b - \frac{a_1^2 a_4 + a_3^2}{a_1^6}c : c \right)$$

is bijective and its inverse is

$$\phi_3^{-1} : \mathbb{P}^2 \rightarrow \mathbb{P}^2 : (a : b : c) \mapsto \left( a_1^2 a + \frac{a_3}{a_1}c : a_1^3 b + \frac{a_1^2 a_4 + a_3^2}{a_1^3}c : c \right).$$

Note that the denominators are by assumption nonzero in  $\mathbb{K}$ .

We have

$$a_1^6 h_3(X, Y, Z) = f \left( a_1^2 X + \frac{a_3}{a_1} Z, a_1^3 Y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} Z, Z \right).$$



## Affine Weierstrass Equations

- $\text{char}(\mathbb{K}) \neq 2$ :

$$Y^2 = X^3 + \frac{1}{4}b_2X^2 + \frac{1}{2}b_4X + \frac{1}{4}b_6. \quad (111)$$

- $\text{char}(\mathbb{K}) \neq 2, 3$ :

$$Y^2 = X^3 - 27c_4X - 54c_6. \quad (112)$$

- $\text{char}(\mathbb{K}) = 2, a_1 \neq 0$ :

$$Y^2 + XY = X^3 + a'_2X^2 + a'_6. \quad (113)$$

## Computation of Points

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{Q}$  given by the affine Weierstrass polynomial

$$f^a = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6.$$

For each  $x \in \mathbb{Q}$ , find the points  $P = (x : y : 1) \in \mathcal{E}(f)$ .

Substitute  $X = x$ ,

$$Y^2 + (a_1x + a_3)Y = x^3 + a_2x^2 + a_4x + a_6$$

Put  $c = a_1x + a_3$  and  $d = x^3 + a_2x^2 + a_4x + a_6$ . By completing the square,

$$\left(Y + \frac{c}{2}\right)^2 = d + \frac{c^2}{4}$$

Put  $e = d + \frac{c^2}{4}$ . Then

$$y_{1,2} = -\frac{c}{2} \pm \sqrt{e} \in \mathbb{Q}(\sqrt{e}) = \{a + b\sqrt{e} \mid a, b \in \mathbb{Q}\}.$$

## Example

Given the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{Q}$  by

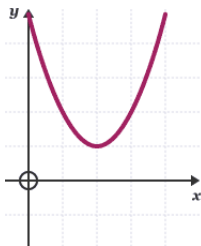
$$Y^2 + Y = X^3 - X.$$

```
> solveE := proc(x)
    local y; solve( y^2+y = x^3-x, y): print(x, %);
end:
> for x from 1 to 7 do solveE(x) end;
```

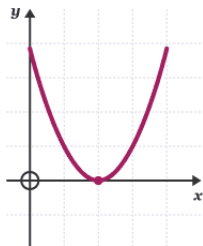
Output:

input $x$	output $y$
1	0, -1
2	2, -3
3	$-\frac{1}{2} \pm \frac{1}{2}\sqrt{97}$ ,
4	$-\frac{1}{2} \pm \frac{1}{2}\sqrt{241}$ ,
5	$-\frac{1}{2} \pm \frac{1}{2}\sqrt{481}$ ,
6	14, -15
7	$-\frac{1}{2} \pm \frac{1}{2}\sqrt{1345}$

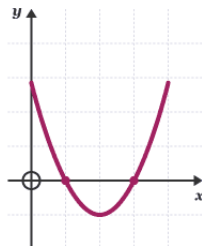
## Discriminant



$b^2 - 4ac < 0$   
there are no  
real roots



$b^2 - 4ac = 0$   
the roots are real  
and equal



$b^2 - 4ac > 0$   
the roots are real  
and unequal

Contents

Weierstrass Form

Discriminant

\*j-Invariant

Singular Points

Intersection  
Multiplicities

The Group Law

Using Coordinates

Using Singular

## Cubic Polynomials

Given a monic cubic polynomial in  $\mathbb{K}[X]$ ,

$$\begin{aligned} f(X) &= X^3 - aX^2 + bX - c \\ &= (X - r_1)(X - r_2)(X - r_3). \end{aligned} \quad (114)$$

The coefficients are elementary symmetric polynomials in the roots  $r_1, r_2, r_3 \in \overline{\mathbb{K}}$ ,

$$a = r_1 + r_2 + r_3, \quad (115)$$

$$b = r_1r_2 + r_1r_3 + r_2r_3, \quad (116)$$

$$c = r_1r_2r_3. \quad (117)$$

The *discriminant* of the polynomial  $f$  is defined as

$$D(f) = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2. \quad (118)$$

## Cubic Polynomials

We have

$$\det \begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} = (r_3 - r_2)(r_3 - r_1)(r_2 - r_1) \quad (119)$$

and

$$\begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} \begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} = \begin{pmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix}, \quad (120)$$

where each  $s^i$  is a power sum in  $r_1, r_2, r_3$ ,

$$s_i = r_1^i + r_2^i + r_3^i, \quad 1 \leq i \leq 4. \quad (121)$$

## Cubic Polynomials

We have

$$D(f) = \det \begin{pmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix}, \quad (122)$$

where

$$s_1 = a, \quad (123)$$

$$s_2 = a^2 - 2b, \quad (124)$$

$$s_3 = a^3 - 3ab + 3c, \quad (125)$$

$$s_4 = a^4 - 4a^2b + 2b^2 + 4ac. \quad (126)$$

## Example

The cubic polynomial  $f = X^3 + pX + q$  has discriminant

$$D(f) = -4p^3 - 27q^2. \quad (127)$$

## Proof.

Here  $a = 0$ ,  $b = p$ ,  $c = -q$ . Thus

$$\begin{aligned} D(f) &= \det \begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix} \\ &= -4p^3 - 27q^2. \end{aligned}$$



## Basic Facts

- For a general cubic  $f$ ,  $D(f) = 0$  iff  $f$  has at least two equal roots.
- For a cubic  $f \in \mathbb{R}[X]$ ,  $D(f) = 0$  iff  $f$  has repeated roots.
  - If all roots of  $f \in \mathbb{R}[X]$  are real, then  $D(f) \geq 0$ .
  - Otherwise,  $f \in \mathbb{R}[X]$  has one real root  $r_1$  and two complex conjugate roots  $r_2, r_3 = \bar{r}_2$ , since complex conjugation

$$z = a + ib \mapsto \bar{z} = a - ib \quad (128)$$

is an automorphism of  $\mathbb{C}$ . Indeed, if  $z \in \mathbb{C}$  is a zero of a polynomial  $f \in \mathbb{R}[X]$ , then

$$f(\bar{z}) = \overline{f(z)} = \bar{0} = 0. \quad (129)$$

Then  $(r_1 - r_2)(r_1 - \bar{r}_2)$  is real and  $(r_2 - \bar{r}_2)$  is imaginary. Since  $D(f)$  is the square,  $D(f) \leq 0$ .

## Discriminants vs. Singularities

Let  $\text{char}(\mathbb{K}) \neq 2$ . The affine curve over  $\mathbb{K}$  given by

$$f = Y^2 - (X^3 - aX^2 + bX - c), \quad (130)$$

is non-singular iff the polynomial

$$g = X^3 - aX^2 + bX - c \quad (131)$$

has distinct roots in  $\overline{\mathbb{K}}$ .

## Proof.

The affine curve given by  $f$  is singular iff there is a  $\overline{\mathbb{K}}$ -rational point  $(x_0 : y_0 : 1)$  on the curve such that

$$\begin{aligned} f(x_0, y_0) &= y_0^2 - (x_0^3 - ax_0^2 + bx_0 - c) = 0, \\ \frac{\partial f}{\partial X}(x_0, y_0) &= 3x_0^2 - 2ax_0 + b = 0, \\ \frac{\partial f}{\partial Y}(x_0, y_0) &= 2y_0 = 0. \end{aligned}$$

Equivalently,  $y_0 = 0$  and  $g(x_0) = g'(x_0) = 0$ .

- Candidates for singular points over  $\overline{\mathbb{K}}$  are only  $(x_0 : 0 : 1)$ , where  $x_0$  is a root of  $g$ .
- The point  $(x_0 : 0 : 1)$  is singular iff  $x_0$  is multiple root of  $g$ , i.e., the first derivative of  $g$  at  $x_0$  also vanishes.

Note that if  $\text{char}(\mathbb{K}) = 2$ , then  $2y_0 = 0$  with  $y_0$  arbitrary. □

## Discriminant of Cubic

Given the Weierstrass polynomial over  $\mathbb{K}$ ,

$$f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

The *discriminant* of the curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  is defined as

$$\Delta(\mathcal{E}) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad (132)$$

where

$$b_2 = a_1^2 + 4a_2, \quad (133)$$

$$b_4 = 2a_4 + a_1a_3, \quad (134)$$

$$b_6 = a_3^2 + 4a_6, \quad (135)$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \quad (136)$$

## Discriminant – Criterion

Given the Weierstrass polynomial over  $\mathbb{K}$ ,

$$f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

The curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  is non-singular iff the discriminant  $\Delta(\mathcal{E})$  is nonzero.

## Proof.

The point at infinity  $O = (0 : 1 : 0)$  is not singular. Thus the curve  $\mathcal{E}(f)$  is non-singular iff the affine curve  $\mathcal{E}(f^a)$  is non-singular,<sup>a</sup> where

$$f^a = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6.$$

The zero locus  $\mathcal{E}(f^a)$  contains a singular point  $(x_0, y_0) \in \overline{\mathbb{K}}$  iff the following holds,

$$\begin{aligned} f^a(x_0, y_0) &= y_0^2 + a_1x_0y_0 + a_3y_0 - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0, \\ \frac{\partial f^a}{\partial X}(x_0, y_0) &= a_1y_0 - 3x_0^2 - 2a_2x_0 - a_4 = 0, \\ \frac{\partial f^a}{\partial Y}(x_0, y_0) &= 2y_0 + a_1x_0 + a_3 = 0. \end{aligned}$$

Consider several cases depending on the characteristic of  $\mathbb{K}$ .

---

<sup>a</sup>See Singularities in Algebraic Curves

## Proof (cont'd).

Let  $\text{char}(\mathbb{K}) \neq 2, 3$ . The elliptic curve  $\mathcal{E}(f)$  corresponds to  $\mathcal{E}(h_2)$ , where

$$h_2 = Y^2Z - X^3 + 27c_4XZ^2 + 54c_6Z^3.$$

The discriminant of the curve  $\mathcal{E}(h_2)$  is

$$\Delta = 2^6 3^9 (c_4^3 - c_6^2). \quad (137)$$

Indeed, the coefficients

$$a_1 = a_2 = a_3 = 0, \quad a_4 = -27c_4, \quad a_6 = -54c_6$$

give

$$b_2 = 0, \quad b_4 = -54c_4, \quad b_6 = -216c_6, \quad b_8 = -27^2 c_4^2$$

and thus

$$\Delta = 2^6 3^9 (c_4^3 - c_6^2). \quad (138)$$

## Proof (cont'd).

The curve  $\mathcal{E}(h_2)$  over  $\overline{\mathbb{K}}$  has a singular point iff the polynomial

$$h_2^a = X^3 - 27c_4X - 54c_6$$

has a repeated root in  $\overline{\mathbb{K}}$  (see (131)). By (127), the discriminant of  $h_2^a$  is

$$D(h_2^a) = -4(-27c_4)^3 - 27(-54c_6)^2 = 2^23^9(c_4^3 - c_6^2).$$

Thus  $D(h_2^a) = 0$  iff  $c_4^3 - c_6^2 = 0$  iff  $\Delta = 0$ . □

## Discriminant

Let  $\text{char}(\mathbb{K}) \neq 2, 3$ . The affine cubic  $\mathcal{E}$  over  $\mathbb{K}$  given by the Weierstrass equation

$$Y^2 = X^3 + pX + q \quad (139)$$

has the discriminant

$$\Delta = -2^4(4p^3 + 27q^2). \quad (140)$$

### Proof.

By (112),  $p = -27c_4$  and  $q = -54c_6$ . Thus by (138),

$$\begin{aligned} \Delta &= 2^6 3^9 (c_4^3 - c_6^2) \\ &= 2^6 3^9 ((-3^{-3}p)^3 - (2^{-1}3^{-3}q)^2) \\ &= -2^4(4p^3 + 27q^2). \end{aligned}$$

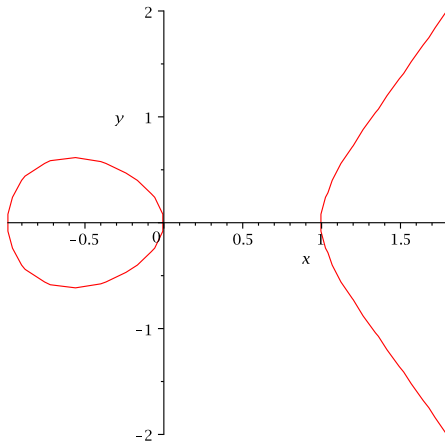


## Discriminants in Maple

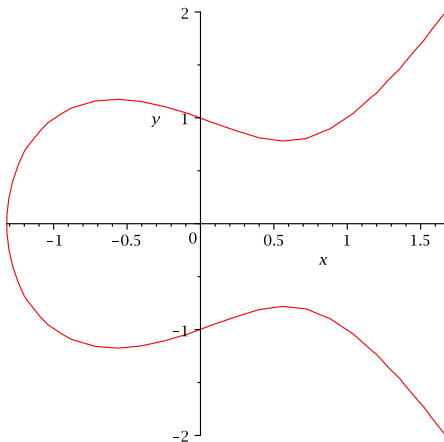
Discriminant of cubic given by  $Y^2 = X^3 + pX + q$  in Maple:

```
> discrEllipt := proc(f)
    local p, q, D;
    p := coeff( f(x),x,1);
    q := coeff( f(x),x,0);
    D := -2^4*(4*p^3+27*q^2);
    RETURN( D )
end:
> f := x -> x^3+x: discrEllipt(f);
-64
> f := x -> x^3-2*x+1: discrEllipt(f);
80
```

## Example

Elliptic curve  $Y^2 = X^3 - X$  with discriminant  $\Delta = 64$ .

## Example

Elliptic curve  $Y^2 = X^3 - X - 1$  with discriminant  $\Delta = -368$ .

## Fermat's Last Theorem

The *Frey curve* is the elliptic curve

$$f = Y^2 Z - X(X - a^p Z)(X + b^p Z) \quad (141)$$

associated with a (hypothetical) solution of Fermat's equation

$$a^p + b^p = c^p, \quad abc \neq 0, \quad (142)$$

where  $a, b, c$  are positive integers and  $p$  is an odd prime.

The affine Weierstrass form

$$f^a = Y^2 - X(X - a^p)(X + b^p) \quad (143)$$

shows that the discriminant (zeros  $0, a^p, -b^p$ ) is

$$\Delta = -a^{2p} b^{2p} (a^p + b^p)^2 \stackrel{!}{=} -a^{2p} b^{2p} c^{2p}. \quad (144)$$

## Negative Discriminants

Some elliptic curves over  $\mathbb{Q}$  with small negative discriminant:

Elliptic curve	$\Delta$	$c_4$	$c_6$
$Y^2 + Y = X^3 - X^2$	-11	16	-152
$Y^2 + XY = X^3 - 2X^2 + X$	-15	1	-161
$Y^2 + Y = X^3 + X^2 + X$	-19	-32	8
$Y^2 + XY + Y = X^3$	-26	-23	-181
$Y^2 + Y = X^3$	-27	0	-216
$Y^2 + XY - Y = X^3$	-28	25	-253
$Y^2 + Y = X^3 + X^2 - X$	-35	64	-568
$Y^2 + XY = X^3 + X^2 + X$	-39	-2	235
$Y^2 + Y = X^3 + X^2$	-43	16	-280
$Y^2 = X^3 - X^2 + X$	-48	-32	-224

## Positive Discriminants

Some elliptic curves over  $\mathbb{Q}$  with small positive discriminant:

Elliptic curve	$\Delta$	$c_4$	$c_6$
$Y^2 + 7XY + 2Y = X^3 + 4X^2 + X$	15	3841	-238049
$Y^2 + 3XY = X^3 + X$	17	33	-81
$Y^2 + Y = X^3 - X$	37	48	-216
$Y^2 + 2XY - 3Y = X^3 - 1$	37	160	-2008
$Y^2 + XY = X^3 - X^2 + X$	57	73	539
$Y^2 + 9XY - 9Y = X^3 + 9X^2 - 5X - 3$	62	15873	-1999809
$Y^2 = X^3 - X$	64	48	0
$Y^2 + XY = X^3 - X$	65	49	-73
$Y^2 + XY = X^3 - X^2 - X$	73	49	243
$Y^2 + 3XY - Y = X^3 - X^2$	79	97	-881

## Example

Compute the integral solutions of the equation

$$\binom{n}{2} = \binom{m}{3},$$

i.e.,

$$\frac{n(n-1)}{2} = \frac{m(m-1)(m-2)}{6}.$$

Clearing denominators and multiplying with  $3^3 = 27$  gives

$$81n^2 - 81n = 27m^3 - 81m^2 + 54m.$$

Setting  $n = (Y - 5)/9$  and  $m = (X - 3)/3$  gives the Weierstrass equation

$$Y^2 + Y = X^3 - 9X + 20,$$

which defines an elliptic curve over  $\mathbb{Q}$  with discriminant  $\Delta = -130491$ .

## Siegel's Theorem (1929)

A smooth algebraic curve  $\mathcal{C}$  of genus  $g > 0$  over a number field  $\mathbb{K}$  has only finitely many points on  $\mathcal{C}$  with coordinates in the ring of integers  $\mathcal{O}$  of  $\mathbb{K}$ . Example:  $\mathbb{K} = \mathbb{Q}$  and  $\mathcal{O} = \mathbb{Z}$ .

## Example (cont'd)

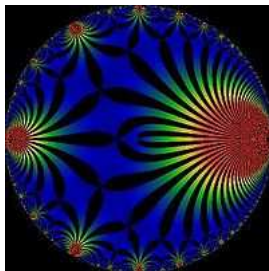
The integral points of the elliptic curve are

$$(-3, 4), (-2, 5), (0, 4), (1, 3), (3, 4), (6, 13), (10, 30), \\ (12, 40), (27, 139), (63, 499), (105, 1075).$$

Only one of each pair  $\pm P$  is listed. For more information see [www.Imfdb.org/EllipticCurve/Q/1611/a/1](http://www.Imfdb.org/EllipticCurve/Q/1611/a/1).

Backtransformation  $Y = 9n - 5$  and  $X = 3m - 3$  shows that the initial equation has only finitely many solutions.

## The j-Invariant



Contents

Weierstrass Form

Discriminant

**\*j-Invariant**

Singular Points

Intersection  
Multiplicities

The Group Law

Using Coordinates

Using Singular

## Definition of j-Invariant

For an elliptic curve  $\mathcal{E}$  with discriminant  $\Delta$ , the quantity

$$j = \frac{c_4^3}{\Delta} \quad (145)$$

is the *j-invariant* of  $\mathcal{E}$ ; well-defined since  $\Delta \neq 0$ .

## j-Invariant

Let  $\text{char}(\mathbb{K}) \neq 2, 3$ . Consider the elliptic curve  $\mathcal{E}(f)$  over  $\mathbb{K}$  given by

$$f = Y^2Z - X^3 - pXZ^2 - qZ^3.$$

Then

$$a_1 = a_2 = a_3 = 0, \quad a_4 = p, \quad a_6 = q$$

and so

$$b_2 = 0, \quad b_4 = 2p, \quad b_6 = 4q.$$

Thus

$$\Delta = -8b_4^3 - 27b_6^2 = -2^4(4p^3 + 27q^2)$$

and so

$$j = \frac{c_4^3}{\Delta} = 2^6 3^3 \frac{4p^3}{4p^3 + 27q^2}, \quad (146)$$

where  $c_4 = b_2^2 - 24b_4 = -48p = -2^4 3p$ .

## Examples

- Each elliptic curve  $\mathcal{E}(f)$  over  $\mathbb{K}$  given by

$$f = Y^2Z - X^3 - pXZ^2 \quad (147)$$

with  $q = 0$  has j-invariant  $j = 2^6 3^3 = 1728$ .

- Each elliptic curve  $\mathcal{E}(f)$  over  $\mathbb{K}$  given by

$$f = Y^2Z - X^3 - qZ^3 \quad (148)$$

with  $p = 0$  has j-invariant  $j = 0$ .

## j-Invariants in Maple

The j-invariant of cubic given by  $Y^2 = X^3 + pX + q$  in Maple:

```
> discrEllipt := proc(f)
  local p, q, c4, D;
  p := coeff( f(x),x,1);
  q := coeff( f(x),x,0);
  c4 := -48*p;
  D := -2^4*(4*p^3+27*q^2);
  if (D = 0) then RETURN(D)
  else RETURN(D, c4^3/D)
  end if
end:
> f := x -> x^3+x: discrEllipt(f);
-64, 1728
> f := x -> x^3-2*x+1: discrEllipt(f);
80, 55296/5
```

## Structure of j-Invariants

Let  $\text{char}(\mathbb{K}) \neq 2, 3$ . For each  $j_0 \in \mathbb{K}$ , there is an elliptic curve over  $\mathbb{K}$  with j-invariant  $j_0$ .

### Proof.

- The cases  $j_0 = 0$  and  $j_0 = 1728$  have appeared in (147) and (148).
- For the other values, consider the Weierstrass form

$$f = Y^2 Z - X^3 + \frac{27}{4} \frac{j_0}{j_0 - 1728} X Z^2 + \frac{27}{4} \frac{j_0}{j_0 - 1728} Z^3,$$

where

$$p = q = -\frac{27}{4} \frac{j_0}{j_0 - 1728}.$$

Then by (146),

$$j = 1728 \frac{4p^3}{4p^3 + 27q^2} \stackrel{!}{=} j_0.$$

## Admissible Change of Variables

An *admissible change of variables* in a Weierstrass form

$$f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

over  $\mathbb{K}$  is the projective transformation

$$f^A(X, Y, Z) = f((X, Y, Z)A^{-1}) \quad (149)$$

where

$$A = \begin{pmatrix} \frac{1}{u^2} & -\frac{s}{u^3} & 0 \\ 0 & \frac{1}{u^3} & 0 \\ -\frac{r}{u^2} & \frac{rs-t}{u^3} & 1 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} u^2 & su^2 & 0 \\ 0 & u^3 & 0 \\ r & t & 1 \end{pmatrix} \quad (150)$$

with  $u, r, s, t \in \mathbb{K}$  and  $u \neq 0$ .

## Admissible Change of Variables in Maple

```
> f := Y^2-X^3-pX-q:
> subs( {X=u^2*x+r, Y=u^3*y+s*u^3*x+t}, f):
> g := collect(simplify(%), [x,y]);
```

Resulting polynomial:

$$g = u^6 y^2 + 2u^5 sxy + 2u^3 ty - u^6 x^3 + (s^2 u^4 - 3u^4 r)x^2 + (-pu^2 + 2su^2 t - 3u^2 r^2)x + (t^2 - pr - q - r^3).$$

Under normalization (multiplication with  $u^{-6}$ ), the coefficients of  $y^2$  and  $x^3$  become 1 and  $-1$ , resp.

## Basic Facts I

- Under an admissible change of variables and the normalization (multiplication with  $u^{-6}$ ), a cubic  $\mathcal{E}(f)$  in Weierstrass form is mapped to cubic  $\mathcal{E}(g)$  in Weierstrass form.
- An admissible change of variables fixes  $O = (0 : 1 : 0)$ , since  $A \cdot (0 : 1 : 0) = (0 : \frac{1}{u^3} : 0)$  and  $u^3 \neq 0$ .
- Two elliptic curves are called *isomorphic* if they are related by an admissible change of variables.

## Basic Facts II

- The assignment  $f \mapsto f^A$  maps the coefficients of  $f$ ,

$$a_1, a_2, \dots, b_2, \dots, c_4, c_6,$$

to new coefficients of  $f^A$ ,

$$a'_1, a'_2, \dots, b'_2, \dots, c'_4, c'_6.$$

Each primed coefficient is  $u^{-i}$  times an expression in  $r, s, t, a_1, \dots, c_6$  not involving  $u$ . The coefficient is then said to have *weight*  $i$ .

In particular,  $c'_4 = u^{-4}c_4$  and  $c'_6 = u^{-6}c_6$  with  $r, s, t$  not involved.

## Structure of j-Invariants

Let  $\text{char}(\mathbb{K}) \neq 2, 3$ . If two elliptic curves are related by an admissible change of variables, they have the same j-invariant.

### Proof.

We have  $c'_4 = u^{-4}c_4$  and  $c'_6 = u^{-6}c_6$  with  $r, s, t$  not involved. By (137),  $\Delta(f) = 2^6 3^9 (c_4^3 - c_6^2)$  and so

$$\Delta(f^A) = 2^6 3^9 (c_4'^3 - c_6'^2) = 2^6 3^9 u^{-12} (c_4^3 - c_6^2) = u^{-12} \Delta(f).$$

Thus

$$j = \frac{c_4^3}{\Delta(f)} = \frac{u^{-12} c_4^3}{u^{-12} \Delta(f)} = \frac{c_4'^3}{\Delta(f^A)}.$$



## Admissible Change of Variables in Maple

```

> f := Y^2-X^3-pX-q:
> subs( {X=u^2*x, Y=u^3*y}, f):
> g := collect(simplify(%), [x,y]);

```

Resulting polynomial:

$$g = u^6 y^2 - u^6 x^3 - pu^2 x - q.$$

Under normalization (multiplication with  $u^{-6}$ ), we obtain

$$f^A = y^2 - x^3 - pu^{-4}x - qu^{-6}. \quad (151)$$

## Structure of j-Invariants

Let  $\text{char}(\mathbb{K}) \neq 2, 3$ . If two elliptic curves over  $\overline{\mathbb{K}}$  have the same j-invariant, they are related by an admissible change of variables.

### Proof.

Take two elliptic curves defined by  $f = Y^2 - X^3 - pX - q$  and  $g = Y^2 - X^3 - p'X - q'$  which have equal j-invariants

$$\frac{4p^3}{4p^3 + 27q^2} = \frac{4p'^3}{4p'^3 + 27q'^2}.$$

Equivalently,

$$p^3 q'^2 = p'^3 q^2.$$

Find  $u \neq 0$  such that  $p' = pu^{-4}$  and  $q' = qu^{-6}$ . Then by (151), the curves are related by an admissible change of variables.

## Proof (cont'd).

Find  $u \neq 0$  such that

$$p' = pu^{-4} \quad \text{and} \quad q' = qu^{-6}. \quad (152)$$

Three cases:

- Let  $p' = 0$ . Then  $q' \neq 0$  by non-singularity, and so  $p = 0$ . Put  $u = (q/q')^{1/6}$ . Then (152) holds.
- Let  $q' = 0$ . Then  $p' \neq 0$  by non-singularity, and so  $q = 0$ . Put  $u = (p/p')^{1/4}$ . Then (152) holds.
- Let  $p'q' \neq 0$ . Put  $u = (p/p')^{1/4}$ . Then  $p' = pu^{-4}$  and so  $q^2 = (p/p')^3 q'^2 = u^{12} q'^2$ . Thus  $q = u^6 q'$  or  $q = -u^6 q'$ .
  - If  $q = u^6 q'$ , then (152) holds.
  - If  $q = -u^6 q'$ , replace  $u$  by  $iu$ , where  $i = \sqrt{-1}$ , so that  $q = u^6 q'$ . Then (152) holds.

□

## Example

- The elliptic curves over  $\mathbb{R}$  given by the cubics

$$Y^2 = X^3 - 2X + 1 \quad \text{and} \quad Y^2 = X^3 - 2X - 1$$

have the same j-invariant  $j = \frac{2^{11}3^3}{59}$ .

- By (151), the admissible change of variables

$$X \mapsto u^2X \quad \text{and} \quad Y \mapsto u^3Y$$

leads from

$$Y^2 - X^3 - pX - q \quad \text{to} \quad Y^2 - X^3 - pu^{-4}X - qu^{-6}.$$

- Choosing  $u = i$  (primitive 4th root of unity) shows that

$$Y^2 = X^3 - 2X + 1 \quad \text{and} \quad Y^2 = X^3 - 2X - 1$$

are related by admissible change of variables.

## Singular Points

K.-H.  
Zimmermann

Contents

Weierstrass Form

Discriminant

\*j-Invariant

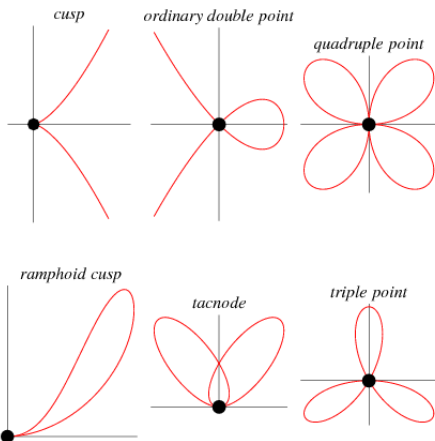
Singular Points

Intersection  
Multiplicities

The Group Law

Using Coordinates

Using Singular



## Singular Points - Projective Transformation I

Let  $\mathcal{E}(f)$  be a singular Weierstrass curve over  $\mathbb{K}$  with

$$f = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

- The base point  $O = (0 : 1 : 0)$  is non-singular.
- Given singular point  $P = (a : b : 1)$  on  $\mathcal{E}(f)$ .
- Translate  $P$  to  $(0 : 0 : 1)$  by the projective transformation  $A$  with

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -a & -b & 1 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{pmatrix},$$

i.e.,  $A \cdot P = PA = (0 : 0 : 1)$  and

$$f^A(X, Y, Z) = f((X, Y, Z)A^{-1}) = f(X + aZ, Y + bZ, Z).$$

Projective transformations preserve singularity by (81).

## Singular Points - Projective Transformation II

Let

$$f^A(X, Y, Z) = f(X + aZ, Y + bZ, Z).$$

Then

- $f^A(0, 0, 1) = [a_6Z^3 + \dots](0, 0, 1) = 0$  gives  $a_6 = 0$ .
- $\frac{\partial f^A}{\partial X}(0, 0, 1) = [a_4Z^2 + \dots](0, 0, 1) = 0$  gives  $a_4 = 0$ .
- $\frac{\partial f^A}{\partial Y}(0, 0, 1) = [a_3Z^2 + \dots](0, 0, 1) = 0$  gives  $a_3 = 0$ .

Thus the (affine) curve has the form

$$(f^A)^a = Y^2 + a_1XY - X^3 - a_2X^2.$$

## Cusps and Nodes

Consider the (affine) curve given by

$$Y^2 + a_1XY = X^3 + a_2X^2. \quad (153)$$

- Factorization of  $Y^2 + a_1XY - a_2X^2$  over  $\overline{\mathbb{K}}$  gives

$$(Y - \alpha X)(Y - \beta X) = X^3, \quad \alpha, \beta \in \overline{\mathbb{K}}. \quad (154)$$

- The singular point  $(0 : 0 : 1)$  is a *cuspid* if  $\alpha = \beta$ , and a *node* (*double point*) if  $\alpha \neq \beta$ .

## Unique Singularity

Each singular curve  $\mathcal{E}(f)$  over  $\mathbb{K}$  with Weierstrass polynomial  $f$  has a unique singular point  $P = (a : b : 1) \in \mathbb{A}^2(\mathbb{K})$ .

The point  $P$  is a cusp if  $c_4 = 0$  and a node if  $c_4 \neq 0$ .

## Proof.

Let  $\text{char}(\mathbb{K}) \neq 2$ . By (111), each (affine) curve over  $\mathbb{K}$  is given by

$$Y^2 = X^3 - aX^2 + bX - c, \quad a, b, c \in \mathbb{K}.$$

This curve is singular iff  $g = X^3 - aX^2 + bX - c$  has repeated roots (see (131)). In the latter case,  $g$  and  $g'$  have gcd  $h$  over  $\mathbb{K}$  with degree  $\geq 1$ .

- The singular points are  $(x_0 : 0 : 1)$  where  $x_0$  ranges over the roots of  $h$ .
- If  $h$  has degree 1, its unique root is  $x_0 \in \mathbb{K}$  and  $(x_0 : 0 : 1)$  is the unique singular point.
- If  $h$  has degree 2, its roots  $x_0, x'_0$  are equal since otherwise  $x_0, x'_0$  would each have multiplicity  $\geq 2$  (with total multiplicity  $\geq 4$ ) of a cubic (degree 3).

It follows that  $(x_0 : 0 : 1)$  is the *unique* singular point.

## Proof (cont'd).

Let  $\text{char}(\mathbb{K}) \neq 2$ .

- Under the projective transformation  $A$  that moves  $(a : b : 1)$  to  $(0 : 0 : 1)$ , we obtain (with  $a_3 = a_4 = a_6 = 0$ )

$$c_4 = (a_1^2 + 4a_2)^2.$$

- By comparing coefficients between (153) and (154),

$$a_1 = -(\alpha + \beta) \quad \text{and} \quad a_2 = -\alpha\beta \quad (155)$$

and

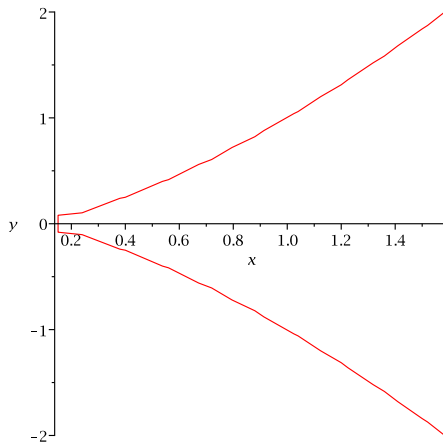
$$\alpha = -a_1 - \gamma \quad \text{and} \quad \beta = \gamma, \quad (156)$$

where  $\gamma = \text{RootOf}(Z^2 + a_1Z - a_2)$ .

- Thus  $c_4 = 0$  iff  $0 = a_1^2 + 4a_2 = (\alpha - \beta)^2$  iff  $\alpha = \beta$  (cusp case). □

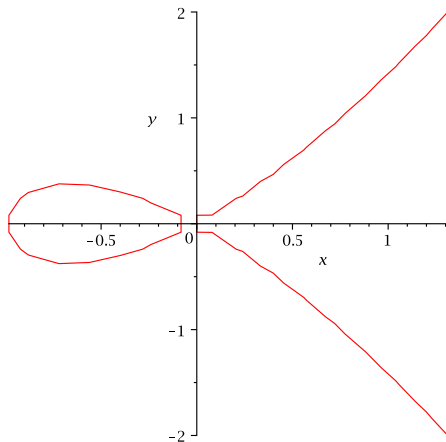
## Example

Plane projective curve  $Y^2 = X^3$  ( $a_1 = a_2 = 0, c_4 = 0$ ) with discriminant  $\Delta = 0$  and a cusp ( $\alpha = \beta = 0$ ).

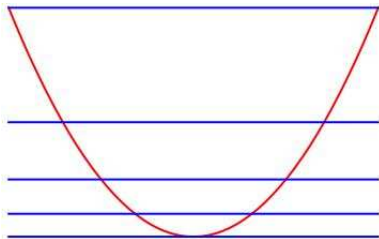


## Example

Plane projective curve  $Y^2 = X^3 + X^2$  ( $a_1 = 0, a_2 = 1, c_4 = 16$ )  
with discriminant  $\Delta = 0$  and a node ( $\alpha = 1, \beta = -1$ ).



## Intersection Multiplicities



## Structure of Intersections

Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve over  $\mathbb{K}$  and  $\mathcal{L} = \mathcal{L}(\alpha, \beta, \gamma)$  be a projective line. Then

$$\sum_{P \in \mathbb{P}^2(\mathbb{K})} i(P, \mathcal{L}, \mathcal{E}) \in \{0, 1, 3\}; \quad (157)$$

i.e., a projective line and an elliptic curve intersect in 0, 1, or 3 points.

## Proof.

Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve given by the Weierstrass polynomial  $f$ .

- The points in  $\mathcal{E}$  are (affine) points of the form  $(a : b : 1)$  and the base point  $O = (0 : 1 : 0)$ .
- $i(P, \mathcal{L}, \mathcal{E}) = 0$  for all points  $P$  in the projective plane not in  $\mathcal{L} \cap \mathcal{E}$ .
- For each point  $P \in \mathcal{L} \cap \mathcal{E}$  the intersection multiplicity satisfies  $i(P, \mathcal{L}, \mathcal{E}) \leq 3$ , since the polynomial

$$\phi(t) = f(a + ta', b + tb', c + tc') \in \mathbb{K}[t]$$

has degree at most 3, see (85).

Three cases occur for  $\mathcal{L} = \mathcal{L}(\alpha, \beta, \gamma)$ .

## Proof (cont'd).

- 1 Let  $\alpha = \beta = 0$ . Then  $\mathcal{L} = \mathcal{L}(0, 0, 1)$  and the only point in  $\mathcal{L} \cap \mathcal{E}$  is  $O = (0 : 1 : 0)$ . Take the auxiliary point  $P' = (1 : 0 : 0) \in \mathcal{L}$ . Then

$$\phi(t) = f(0 + 1 \cdot t, 1 + 0 \cdot t, 0 + 0 \cdot t) = f(t, 1, 0) = -t^3$$

and so

$$i(O, \mathcal{L}, \mathcal{E}) = 3.$$

## Proof (cont'd).

2 Let  $\alpha \neq 0$ ,  $\beta = 0$ : Then  $\mathcal{L} = (\alpha, 0, \gamma)$  for some  $\gamma \in \mathbb{K}$ .

First, the only point at infinity that lies in  $\mathcal{L} \cap \mathcal{E}$  is

$O = (0 : 1 : 0)$ . Take the auxiliary point  $P' = (-\gamma : 0 : \alpha) \in \mathcal{L}$ .

Then

$$\begin{aligned}\phi(t) &= f(0 - \gamma \cdot t, 1 + 0 \cdot t, 0 + \alpha \cdot t) \\ &= f(-\gamma t, 1, \alpha t) \\ &= \alpha t + \text{terms of higher order in } t\end{aligned}$$

and so  $i(O, \mathcal{L}, \mathcal{E}) = 1$ .

## Proof (cont'd).

- 2 Second, an affine point  $P = (x : y : 1)$  lies in  $\mathcal{L} \cap \mathcal{E}$  iff  $x = -\frac{\gamma}{\alpha}$  and  $y$  is a root of the polynomial

$$h(Y) = f\left(-\frac{\gamma}{\alpha}, Y, 1\right) \in \mathbb{K}[Y].$$

Since  $h$  has degree 2 and coefficient 1 in  $Y^2$ , there are  $r_1, r_2 \in \overline{\mathbb{K}}$  with

$$h(Y) = (Y - r_1)(Y - r_2).$$

If none of  $r_1, r_2$  lies in  $\mathbb{K}$ , then

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = i(O, \mathcal{L}, \mathcal{E}) = 1.$$

Otherwise, both  $r_1, r_2$  lie in  $\mathbb{K}$  and so with  $y_{1,2} = r_1, r_2$ ,

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = 3.$$

## Roots of Quadratic Polynomials

Let  $f = X^2 - aX + b \in \mathbb{K}[X]$ .

- If  $r_1, r_2 \in \overline{\mathbb{K}}$  are the roots of  $f$ , then

$$f = (X - r_1)(X - r_2) = X^2 - (r_1 + r_2)X + r_1r_2.$$

- By comparing coefficients,

$$a = r_1 + r_2 \in \mathbb{K}.$$

- Thus either both roots lie in  $\mathbb{K}$  or none of them.

## Proof (cont'd).

3 Let  $\beta \neq 0$ . Then  $O = (0 : 1 : 0) \notin \mathcal{L}$ .

An affine point  $P = (x : y : 1)$  lies in  $\mathcal{L} \cap \mathcal{E}$  iff

$$y = -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}x$$

and  $x$  is a root of the polynomial

$$h(X) = f\left(X, -\frac{\gamma}{\beta} - \frac{\alpha}{\beta}X, 1\right) \in \mathbb{K}[X].$$

Since  $h$  has degree 3 and coefficient  $-1$  in  $X^3$ , there are  $r_1, r_2, r_3 \in \overline{\mathbb{K}}$  with

$$h(X) = -(X - r_1)(X - r_2)(X - r_3) \in \mathbb{K}[X].$$

## Proof (cont'd).

3 If none of  $r_1, r_2, r_3 \in \mathbb{K}$ , then

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = 0.$$

If exactly one of  $r_1, r_2, r_3 \in \mathbb{K}$ , then for some  $x = r_i$ ,

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = 1.$$

If two of  $r_1, r_2, r_3 \in \mathbb{K}$ , then all three lie in  $\mathbb{K}$  and so with  $x_{1,2,3} = r_1, r_2, r_3$ ,

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = 3.$$



## Roots of Cubic Polynomials

Let  $f = X^3 - aX^2 + bX - c \in \mathbb{K}[X]$ .

- If  $r_1, r_2, r_3 \in \overline{\mathbb{K}}$  are the roots of  $f$ , then

$$\begin{aligned} f &= (X - r_1)(X - r_2)(X - r_3) \\ &= X^3 - (r_1 + r_2 + r_3)X^2 + (r_1r_2 + r_1r_3 + r_2r_3)X \\ &\quad - r_1r_2r_3. \end{aligned}$$

- By comparing coefficients,

$$a = r_1 + r_2 + r_3 \in \mathbb{K}.$$

- Thus it cannot happen that two of the roots lie in  $\mathbb{K}$  and the third one does not.

## Example

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  given by

$$f = Y^2 - X^3 - X$$

and the line  $\mathcal{L} = \mathcal{L}(\alpha, \beta, \gamma)$ .

1 Let  $\alpha = \beta = 0$ : Then  $\mathcal{L} = \mathcal{L}(0, 0, 1)$ .

- The only point in the intersection  $\mathcal{L} \cap \mathcal{E}$  is the base point  $O = (0 : 1 : 0)$ .
- The intersection multiplicity of  $O$  with  $\mathcal{L}$  and  $\mathcal{C}$  is 3 (flex point).
- Thus

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = i(O, \mathcal{L}, \mathcal{E}) = 3.$$

## Example (cont'd)

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  with  $\mathbb{Q} \subseteq \mathbb{K}$  given by

$$f = Y^2 - X^3 - X$$

and the line  $\mathcal{L} = \mathcal{L}(\alpha, \beta, \gamma)$ .

2 Let  $\alpha \neq 0$  and  $\beta = 0$ . Take  $\mathcal{L} = \mathcal{L}(1, 0, 1)$ .

- The point  $O$  lies in  $\mathcal{L} \cap \mathcal{E}$  with  $i(O, \mathcal{L}, \mathcal{E}) = 1$ .
- The point  $P = (x : y : 1)$  lies in  $\mathcal{L} \cap \mathcal{E}$  iff  $x = -1$  and  $y$  is a root of

$$h(Y) = Y^2 - x^3 - x = Y^2 + 2 = (Y - \sqrt{-2})(Y + \sqrt{-2}).$$

The roots of  $h(Y)$  are  $\pm i\sqrt{2}$ .

- Thus

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = \begin{cases} 3 & \text{if } i\sqrt{2} \in \mathbb{K}, \\ 1 & \text{otherwise.} \end{cases}$$

## Example (cont'd)

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  with  $\mathbb{Q} \subseteq \mathbb{K}$  given by

$$f = Y^2 - X^3 - X$$

and the line  $\mathcal{L} = \mathcal{L}(\alpha, \beta, \gamma)$ .

3 Let  $\beta \neq 0$ . Take  $\mathcal{L} = \mathcal{L}(0, 1, 0)$ .

- The point  $O$  does not lie in  $\mathcal{L} \cap \mathcal{E}$ , so  $i(O, \mathcal{L}, \mathcal{E}) = 0$ .
- The point  $P = (x : y : 1)$  lies in  $\mathcal{L} \cap \mathcal{E}$  iff  $y = 0$  and  $x$  is a root of

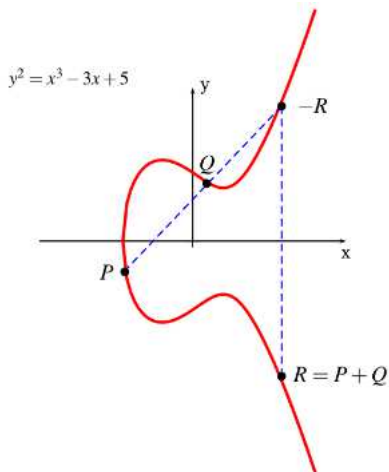
$$h(X) = -X^3 - X = -X(X^2 + 1) = -X(X - i)(X + i).$$

The roots of  $h(X)$  are 0 and  $\pm i$ .

- Thus

$$\sum_P i(P, \mathcal{L}, \mathcal{E}) = \begin{cases} 3 & \text{if } i \in \mathbb{K}, \\ 1 & \text{if } i \notin \mathbb{K}. \end{cases}$$

## The Group Law



## Secant-Tangent Composition Law

Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve over  $\mathbb{K}$ .

- *Secant case:* Let  $P$  and  $Q$  be distinct points in  $\mathcal{E}$  and let  $\mathcal{L}$  be the projective line connecting these points. Then by (157) there is a third point  $R \in \mathcal{L} \cap \mathcal{E}$  if multiplicities are counted. The third point may coincide with  $P$  or  $Q$ .
- *Tangent case:* Let  $\mathcal{L}$  be the tangent line to  $\mathcal{E}$  at  $P$ . Then by (86),  $i(P, \mathcal{L}, \mathcal{E}) \geq 2$  and so by (157) there is a third point  $R \in \mathcal{L} \cap \mathcal{E}$  if multiplicities are counted. The third point will be  $R = P$  if  $P$  is flex point of  $\mathcal{E}$ .

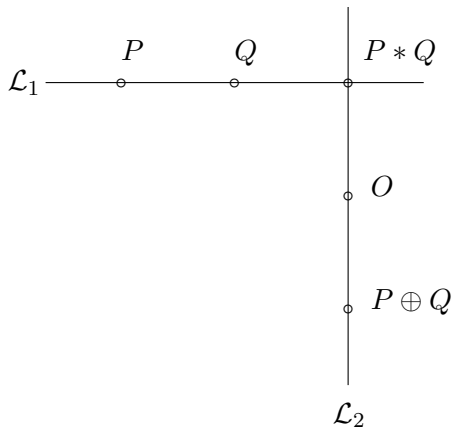
## Secant Case

Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve over  $\mathbb{K}$ .

For two distinct  $\mathbb{K}$ -rational points  $P, Q$  on  $\mathcal{E}$  define the  $\mathbb{K}$ -rational point  $P \oplus Q$ :

- Take the unique projective line  $\mathcal{L}_1$  through the points  $P$  and  $Q$ . The line  $\mathcal{L}_1$  intersects the curve  $\mathcal{E}$  in another point  $P * Q$ .
- Take the unique projective line  $\mathcal{L}_2$  through the point  $P * Q$  and the base point  $O$ . If  $P * Q = O$ , take the tangent line at  $\mathcal{E}$  in  $O$ . The line  $\mathcal{L}_2$  intersects the curve  $\mathcal{E}$  in another point  $P \oplus Q$ .

## Secant Case



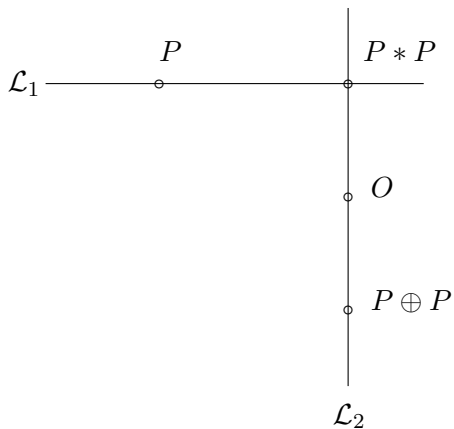
## Tangent Case

Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve over  $\mathbb{K}$ .

For a  $\mathbb{K}$ -rational point  $P$  on  $\mathcal{E}$  define the  $\mathbb{K}$ -rational point  $P \oplus P$ :

- Let  $\mathcal{L}_1$  be the tangent line at  $\mathcal{E}$  in the point  $P$ . The line  $\mathcal{L}_1$  intersects the curve  $\mathcal{E}$  in another point  $P * P$ .
- Take the unique projective line  $\mathcal{L}_2$  through the point  $P * P$  and the base point  $O$ . If  $P * P = O$ , take the tangent line at  $\mathcal{E}$  in  $O$ . The line  $\mathcal{L}_2$  intersects the curve  $\mathcal{E}$  in another point  $P \oplus P$ .

## Tangent Case



## Unit Element

Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve over  $\mathbb{K}$ . Each  $\mathbb{K}$ -rational point  $P$  on  $\mathcal{E}$  satisfies

$$P \oplus O = P. \quad (158)$$

### Proof.

- Let  $P = O$ . The tangent line  $\mathcal{L}_1$  at  $\mathcal{E}$  in  $O$  is  $\mathcal{L}_1 = \mathcal{L}(0, 0, 1)$ , since the Weierstrass polynomial  $f$  shows that

$$\frac{\partial f}{\partial X}(0, 1, 0) = 0, \quad \frac{\partial f}{\partial Y}(0, 1, 0) = 0, \quad \frac{\partial f}{\partial Z}(0, 1, 0) = 1.$$

By the discussion of intersection multiplicities (case 1),  $i(O, \mathcal{L}_1, \mathcal{E}) = 3$ . Thus the third intersection point is  $O$  and hence  $O * O = O$ .

Moreover, the line  $\mathcal{L}_2$  is the tangent line at  $\mathcal{E}$  in  $O$  and thus  $\mathcal{L}_2 = \mathcal{L}(0, 0, 1)$ . But  $O$  is a flex point and so the third intersection point is also  $O$ . Hence,  $O \oplus O = O$ .

## Proof (cont'd).

- Let  $P \neq O$ . Take the line  $\mathcal{L}_1$  through  $P$  and  $O$  which intersects the curve in a third point  $P * O$ .

Moreover, the line  $\mathcal{L}_2$  intersects  $O$  and  $P * O$ . But there is a unique projective line between any two points and so  $\mathcal{L}_1 = \mathcal{L}_2$ . Thus the third intersection point of  $\mathcal{L}_2$  with  $\mathcal{E}$  is  $P$  and hence  $P \oplus O = P$ .



## Collinearity

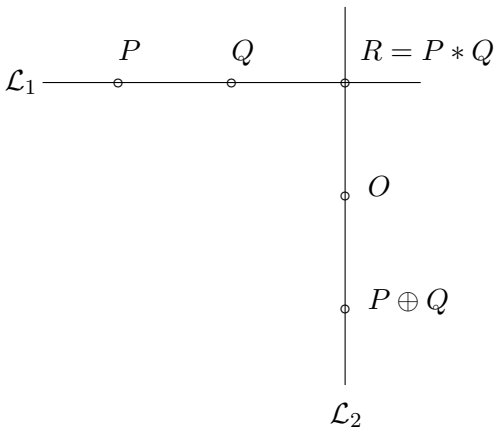
Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve over  $\mathbb{K}$ . Let  $P$ ,  $Q$ , and  $R$  be distinct  $\mathbb{K}$ -rational points of  $\mathcal{E}$  which lie on a projective line  $\mathcal{L}$  over  $\mathbb{K}$ . Then

$$(P \oplus Q) \oplus R = O. \quad (159)$$

### Proof.

- Add the points  $P$  and  $Q$ : Take the line  $\mathcal{L}_1$  through the points  $P$  and  $Q$ . By uniqueness,  $\mathcal{L}_1 = \mathcal{L}$  and by the intersection multiplicities,  $R = P * Q$  is the third point on the line. Moreover, take the line  $\mathcal{L}_2$  through  $R$  and  $O$ . The third point on the line  $\mathcal{L}_2$  is  $P \oplus Q$ .

## Proof (cont'd).

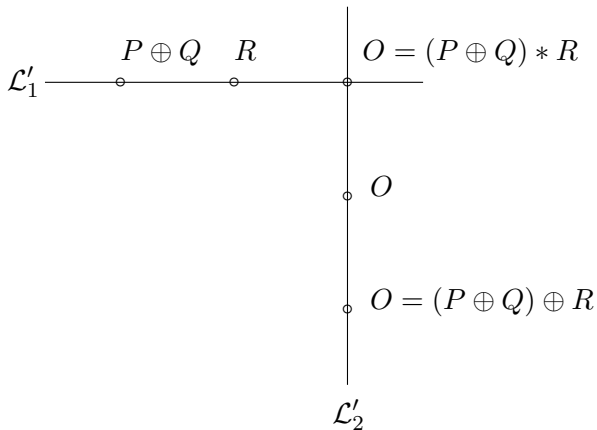


## Proof (cont'd).

- Add the points  $P \oplus Q$  and  $R$ : Take the line  $\mathcal{L}'_1$  through the points  $P \oplus Q$  and  $R$ . By uniqueness,  $\mathcal{L}'_1 = \mathcal{L}_2$  and the third intersection point is  $O$ .

Moreover, the tangent line  $\mathcal{L}'_2$  at  $\mathcal{E}$  in  $O$  has intersection multiplicity 3 and so the third intersection point is  $O$  giving  $(P \oplus Q) \oplus R = O$ .

## Proof (cont'd).



## Group Structure

An elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  forms together with the operation

$$\oplus : \mathcal{E} \times \mathcal{E} \rightarrow \mathcal{E} : (P, Q) \mapsto P \oplus Q \quad (160)$$

an abelian group with unit element  $O$ .

### Proof.

- The operation is well-defined thanks to the secant-tangent composition law.
- The operation is commutative, since the construction of the point  $P \oplus Q$  is independent of the order of the given points  $P$  and  $Q$ .
- The base point  $O$  is the unit element by (158).

## Proof (cont'd).

- Each  $\mathbb{K}$ -rational point  $P$  on  $\mathcal{E}$  has a  $\mathbb{K}$ -rational inverse point  $P'$  on  $\mathcal{E}$ , i.e.,

$$P \oplus P' = O. \quad (161)$$

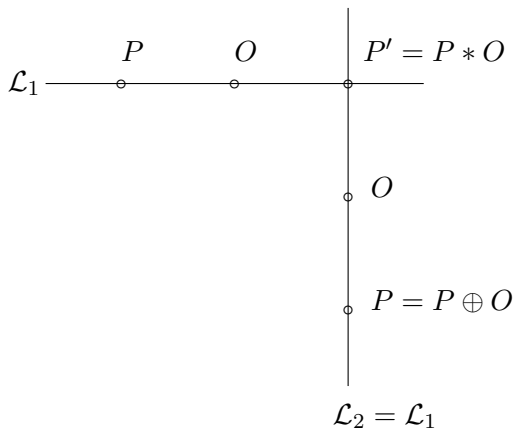
To see this, assume that  $P \neq O$ .

Take the line  $\mathcal{L}_1$  through  $P$  and  $O$ . By the intersection multiplicities (case 2),  $O$  has multiplicity  $i(O, \mathcal{L}, \mathcal{E}) = 1$ . Thus there is a third intersection point  $P' = P * O$  on the line. Then by collinearity (159) and (158),

$$O = (P \oplus O) \oplus P' = P \oplus P'.$$

- The operation is associative. This can be proved by using explicit coordinates or the famous Nine point lemma.

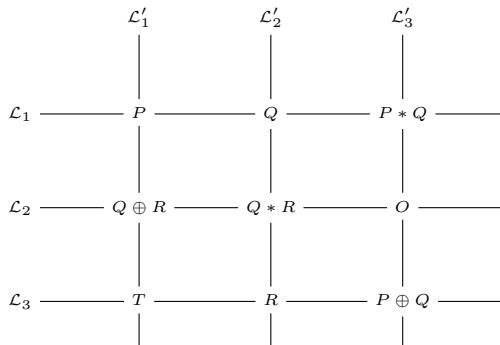
## Proof (cont'd).



## Proof (cont'd).

- Nine point lemma:** Suppose the eight  $\mathbb{K}$ -rational points  $O$ ,  $P$ ,  $Q$ ,  $R$ ,  $P * Q$ ,  $Q * R$ ,  $P \oplus Q$ , and  $Q \oplus R$  in  $\mathbb{P}^2(\mathbb{K})$  are pairwise distinct and are different from the  $\mathbb{K}$ -rational points  $P * (Q \oplus R)$  and  $(P \oplus Q) * R$ . Then there is a unique  $\mathbb{K}$ -rational point  $T$  (below) which equals

$$P * (Q \oplus R) = (P \oplus Q) * R.$$



## Notation

- Define  $P + Q$  as  $P \oplus Q$ .
- Denote the inverse of  $P$  as  $-P$ .
- For each integer  $l$ , the  $l$ -fold of a point  $P \in \mathcal{E}$  is

$$0P = O,$$

$$lP = (l-1)P + P \text{ for } l \geq 1,$$

$$lP = (-l)(-P) \text{ for } l \leq -1.$$

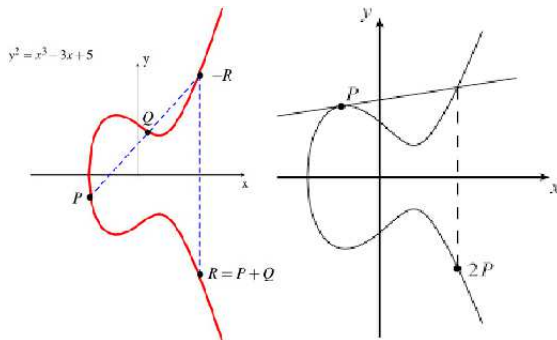
Thus for each integer  $l \geq 1$ ,

$$lP = P + \dots + P, \quad l\text{-times,}$$

and

$$(-l)P = (-P) + \dots + (-P) \quad l\text{-times.}$$

## Group Law in Coordinates



## Inverse Point

Let  $P = (x : y : 1)$  be a  $\mathbb{K}$ -rational point on an elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  with Weierstrass polynomial  $f$ . The inverse of  $P$  is the  $\mathbb{K}$ -rational point

$$-P = (x : -y - a_1x - a_3 : 1). \quad (162)$$

### Proof.

The line through  $P$  and  $O$  is  $\mathcal{L}(1, 0, -x)$ . The third intersection point on the line is  $P * O = (x : -y - a_1x - a_3 : 1)$ , which is the inverse of  $P$ , see (161). This can be shown by the following Maple code:

```
> f := Y^2+a1*X*Y+a3*Y; // part of f involving Y
> subs({X=x, Y=-y-a1*x-a3}, f): simplify(%);
```

The output is  $y^2 + a_1xy + a_3y$ . □

## Inverse Point – Special Case

Let  $P = (x : y : 1)$  be a  $\mathbb{K}$ -rational point on an elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  with affine Weierstrass polynomial

$$f = Y^2 - X^3 - pX - q \in \mathbb{K}[X].$$

The inverse of  $P$  is the  $\mathbb{K}$ -rational point

$$-P = (x : -y : 1), \quad (163)$$

since  $a_1 = a_3 = 0$ ; i.e.,  $-P$  is obtained from  $P$  by reflection at the  $x$ -axis.

## Line Through Two Points

Let  $P_1 = (x_1 : y_1 : 1)$  and  $P_2 = (x_2 : y_2 : 1)$  be  $\mathbb{K}$ -rational points on an elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  with  $P_2 \neq -P_1$ . The line through  $P_1$  and  $P_2$  is given by

$$Y = mX + bZ = \begin{cases} \text{line through } P_1, P_2 & \text{if } P_1 \neq P_2 \text{ (secant case),} \\ \text{tangent line at } P_1 & \text{if } P_1 = P_2 \text{ (tangent case),} \end{cases}$$

where

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{in secant case,} \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{in tangent case,} \end{cases} \quad (164)$$

and

$$b = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{in secant case,} \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{in tangent case.} \end{cases} \quad (165)$$

## Proof.

*Secant case:* The system of equations

$$y_1 = mx_1 + b \quad \text{and} \quad y_2 = mx_2 + b$$

yields

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

and

$$b = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

## Proof (cont'd).

*Tangent case:* Take the affine Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

By implicit differentiation,<sup>a</sup>

$$2YY' + a_1XY' + a_1Y + a_3Y' = 3X^2 + 2a_2X + a_4.$$

Putting  $Y' = m$  and  $(X, Y) = (x_1, y_1)$  gives

$$2y_1m + a_1x_1m + a_1y_1 + a_3m = 3x_1^2 + 2a_2x_1 + a_4.$$

Thus

$$m = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

---

<sup>a</sup>For a real-valued implicit function  $f(X, Y) = 0$ , the derivative is given by the chain rule  $\frac{\partial f}{\partial X} + \frac{\partial f}{\partial Y} \frac{dY}{dX} = 0$ .

## Proof (cont'd).

*Tangent case:* Moreover, since  $b = y_1 - mx_1$ , we obtain

$$b = \frac{2y_1^2 + a_1x_1y_1 + a_3y_1 - 3x_1^3 - 2a_2x_1^2 - a_4x_1 + a_1x_1y_1}{2y_1 + a_1x_1 + a_3}.$$

Substituting  $y_1^2 = -a_1x_1y_1 - a_3y_1 + x_1^3 + a_2x_1^2 + a_4x_1 + a_6$  gives

$$b = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$



## Example – Secant Case

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{Q}$  given by

$$f = Y^2 - X^3 + 36X,$$

where  $a_1 = a_2 = a_3 = a_6 = 0$  and  $a_4 = -36$ .

- $P_1 = (-3, 9)$  and  $P_2 = (-2, 8)$  lie on  $\mathcal{E}$ .
- The line through  $P_1$  and  $P_2$  is

$$Y = -X + 6,$$

since

$$m = \frac{y_2 - y_1}{x_2 - x_1} = -1 \quad \text{and} \quad b = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} = 6.$$

## Example – Tangent Case

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{Q}$  given by

$$f = Y^2 - X^3 + 36X,$$

where  $a_1 = a_2 = a_3 = a_6 = 0$  and  $a_4 = -36$ .

- $P_1 = (-3, 9)$  lies on  $\mathcal{E}$ .
- The tangent line of  $\mathcal{E}$  at  $P_1$  is

$$Y = -\frac{1}{2}X + \frac{15}{2},$$

since

$$m = \frac{3x_1^2 - 36}{2y_1} = -0.5 \quad \text{and} \quad b = \frac{-x_1^3 - 36x_1}{2y_1} = 7.5.$$

Alternatively, calculate tangent line from homogenized polynomial  $f^h = Y^2Z - X^3 + 36XZ^2$ , see (78).

## Point Addition

Let  $P_1 = (x_1 : y_1 : 1)$  and  $P_2 = (x_2 : y_2 : 1)$  be distinct  $\mathbb{K}$ -rational points on elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$  with  $P_2 \neq -P_1$ .

Then  $P_3 = P_1 + P_2$  is a  $\mathbb{K}$ -rational point  $P_3 = (x_3 : y_3 : 1)$  with

$$x_3 = m^2 + a_1 m - a_2 - x_1 - x_2, \quad (166)$$

$$y_3 = -(m + a_1)x_3 - b - a_3. \quad (167)$$

## Proof.

Take the affine Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

- Let  $F(X, Y)$  denote the difference between the right-hand side and the left-hand side of the Weierstrass equation.

Along the line  $Y = mX + b$ , this expression becomes  $F(X, mX + b)$  which is a monic cubic polynomial in  $X$  over  $\mathbb{K}$ .

- The points  $P_1$ ,  $P_2$ , and  $P_1 * P_2$  lie on the line  $Y = mX + b$ . By (162),  $x_3$  equals the  $x$ -coordinate of  $P_1 * P_2$ . Since  $x_1$ ,  $x_2$ , and  $x_3$  are roots of  $F(X, mX + b)$ , we have

$$F(X, mX + b) = (X - x_1)(X - x_2)(X - x_3).$$

## Proof (cont'd).

- Substituting  $Y = mX + b$  into the Weierstrass equation gives

$$\begin{aligned} X^3 + a_2X^2 + a_4X + a_6 - (mX + b)^2 - a_1X(mX + b) - a_3(mX + b) \\ = X^3 - (x_1 + x_2 + x_3)X^2 + \text{terms of lower order in } X. \end{aligned}$$

Comparing the coefficients of  $X^2$  gives

$$a_2 - m^2 - a_1m = -(x_1 + x_2 + x_3)$$

and so

$$x_3 = m^2 + a_1m - a_2 - x_1 - x_2.$$

For the point  $P_1 * P_2 = (x_3 : y'_3 : 1)$ ,  $y'_3 = mx_3 + b$  and so by (162),

$$y_3 = -y'_3 - a_1x_3 - a_3 = -(m + a_1)x_3 - b - a_3.$$



## Example – Point Addition

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{Q}$  given by

$$f = Y^2 - X^3 + 36X,$$

where  $a_1 = a_2 = a_3 = a_6 = 0$  and  $a_4 = -36$ .

- $P_1 = (-3, 9)$  and  $P_2 = (-2, 8)$  lie on  $\mathcal{E}$ .
- The line through  $P_1$  and  $P_2$  is

$$Y = -X + 6.$$

- Point addition gives  $P_3 = P_1 + P_2 = (6, 0)$ , since

$$x_3 = m^2 - x_1 - x_2 = 6 \quad \text{and} \quad y_3 = -mx_3 - b = 0.$$

## Point Addition – Maple

Given elliptic curve  $\mathcal{E}$  over  $\mathbb{Q}$  by Weierstrass form

$$Y^2 = X^3 + pX + q$$

with  $\mathbb{Q}$ -rational points  $P_1 = (x_1 : y_1 : 1)$  and  $P_2 = (x_2 : y_2 : 1)$  on  $\mathcal{E}$ .

```
> pointAdditionEllipt := proc( x1,y1, x2,y2, f)
    p := coeff( f(x),x,1);
    q := coeff( f(x),x,0);
    m := (y2-y1)/(x2-x1);
    b := (y1*x2-y2*x1)/(x2-x1);
    x3 := m^2-x1-x2;
    y3 := -m*x3-b;
    print(m, b, x3, y3);
end:
> f := x -> x^3-36*x;
> pointAdditionEllipt( -3,9, -2,8, f);
-1, 6, 6, 0
```

## Point Doubling

Let  $P = (x_1 : y_1 : 1)$  be a  $\mathbb{K}$ -rational point on elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{K}$ .

Then  $2P = P \oplus P$  is a  $\mathbb{K}$ -rational point  $2P = (x_3 : y_3 : 1)$  with

$$x_3 = \frac{x_1^4 - b_4x_1^2 - 2b_6x_1 - b_8}{4x_1^3 + b_2x_1^2 + 2b_4x_1 + b_6}, \quad (168)$$

$$y_3 = -(m + a_1)x_3 - b - a_3. \quad (169)$$

## Proof.

A special case of (166) and (167) is that  $P_1 = P_2$  so that we are in the tangent case. Substituting  $m$  in the tangent case (164) into (166) yields the formula

$$x_3 = \frac{x_1^4 - b_4x_1^2 - 2b_6x_1 - b_8}{4x_1^3 + b_2x_1^2 + 2b_4x_1 + b_6},$$

where  $b_2, b_4, b_6, b_8$  are as in (133), (134), (135), (136), respectively. The coordinate  $y_3$  depends only on  $x_3$  and so is as in (167).  $\square$

## Example – Point Doubling

Consider the elliptic curve  $\mathcal{E} = \mathcal{E}(f)$  over  $\mathbb{Q}$  given by

$$f = Y^2 - X^3 + 36X,$$

where  $a_1 = a_2 = a_3 = a_6 = 0$  and  $a_4 = -36$ .

- $P_1 = (-3, 9)$  lies on  $\mathcal{E}$ .
- The tangent line of  $\mathcal{E}$  at  $P_1$  is

$$Y = -\frac{1}{2}X + \frac{15}{2}.$$

- Point doubling gives  $2P_1 = \left(\frac{25}{4}, -\frac{35}{8}\right)$ , since  $a_4 = -36$ ,  $b_2 = 0$ ,  $b_4 = 2a_4$ ,  $b_6 = 0$ ,  $b_8 = -a_4^2$  and so

$$x_3 = \frac{x_1^4 - b_4x_1^2 - b_8}{4x_1^3 + 2b_4x_1} = \frac{25}{4} \quad \text{and} \quad y_3 = -mx_3 - b = -\frac{35}{8}.$$

## Point Doubling – Maple

Given elliptic curve  $\mathcal{E}$  over  $\mathbb{Q}$  by Weierstrass form

$$Y^2 = X^3 + pX + q \text{ and a } \mathbb{Q}\text{-rational point } P = (x_1 : y_1 : 1) \in \mathcal{E}.$$

```

> pointDoublingEllipt := proc( x1, y1, f )
    local, p, q, b4, b6, b8, m, b, x3, y3;
        p := coeff( f(x),x,1);
        q := coeff( f(x),x,0);
        b4 := 2*p; b6 := 4*q; b8 := -p^2;
        m := (3*x1^2+p)/(2*y1);
        b := (-x1^3+p*x1+2*q)/(2*y1);
        x3 := m^2-2*x1;
        y3 := -m*x3-b;
        print(m, b, x3, y3);
    end:
> f := x -> x^3 - 36*x;
> pointDoublingEllipt( -3, 9, f);
-1/2, 15/2, 25/4, -35/8

```

## Fast Point Doubling

**Require:** Point  $P$  on elliptic curve  $\mathcal{E}$ , positive integer  $k$

**Ensure:** Point  $kP$  on elliptic curve  $\mathcal{E}$

$a \leftarrow k, B \leftarrow O, C \leftarrow P$

**while**  $a > 0$  **do**

**if**  $a$  is even **then**

$a \leftarrow a/2, B \leftarrow B, C \leftarrow 2C$

**else**

$a \leftarrow a - 1, B \leftarrow B + C, C \leftarrow C$

**end if**

**end while**

**return**  $B$

Time complexity  $O(\log_2 k)$ .

## Fast Point Doubling

Trace for the computation of the point  $B = 19P$ :

$a$	$B$	$C$
19	$O$	$P$
18	$P$	$P$
9	$P$	$2P$
8	$P + 2P$	$2P$
4	$P + 2P$	$4P$
2	$P + 2P$	$8P$
1	$P + 2P$	$16P$
0	$P + 2P + 16P$	$16P$

The computation makes use of the Horner scheme.

## Summary - Special Case

Let  $\text{char}(\mathbb{K}) \neq 2, 3$ . Let  $\mathcal{E} = \mathcal{E}(f)$  be an elliptic curve over  $\mathbb{K}$  given by

$$f = Y^2Z - X^3 - pXZ^2 - qZ^3.$$

- Let  $P = (x : y : 1)$  be a  $\mathbb{K}$ -rational point of  $\mathcal{E}$ . Then  $-P$  is the  $\mathbb{K}$ -rational point  $-P = (x : -y : 1)$  of  $\mathcal{E}$ .
- Let  $P_1 = (x_1 : y_1 : 1)$  and  $P_2 = (x_2 : y_2 : 1)$  be  $\mathbb{K}$ -rational points of  $\mathcal{E}$  with  $P_1 \neq -P_2$ . Then  $P_3 = P_1 + P_2$  is a  $\mathbb{K}$ -rational point  $P_3 = (x_3 : y_3 : 1)$  of  $\mathcal{E}$ , where

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = -mx_3 - b \quad (170)$$

with

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \\ \frac{3x_1^2 + p}{2y_1}, \end{cases} \quad b = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{if } P_1 \neq P_2, \\ \frac{-3x_1^3 + px_1 + 2q}{2y_1} & \text{if } P_1 = P_2. \end{cases} \quad (171)$$

## Elliptic Curves in Singular



Contents

Weierstrass Form

Discriminant

\*  $j$ -Invariant

Singular Points

Intersection  
Multiplicities

The Group Law

Using Coordinates

Using Singular

## Generation of Random Elliptic Curve

Generation of random elliptic curve over ring  $\mathbb{Z}_N$ .

```
> LIB "crypto.lib";
> ring r = 0,z,dp;
> ellipticRandomCurve(11); // N=11
[1]:
    5                               // a
[2]:
    8                               // b
[3]:
    1                               // discriminant
```

Returned is a list of two random numbers  $a, b$  and  $\Delta = 4a^3 + 27b^2 \pmod N$ .

The curve is given by the equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

## Test for Point Membership

Test whether a point lies on a curve:

```
> isOnCurve(11, 5, 8, list(0,1,0));  
1 // on curve  
> isOnCurve(11, 5, 8, list(5,5,1));  
0 // not on curve
```

## Generation of Random Point

Generate a random point on an elliptic curve:

```
> ellipticRandomPoint(11, 5, 8);  
[1]:  
    6  
[2]:  
    1  
[3]:  
    1
```

## Number of Points

Provide the number of points on a curve:

```
> countPoints(11, 5, 8);  
15
```

## List of Points

List of all points of an elliptic curve:

```
> list L = ellipticAllPoints(11, 5, 8);  
> size(L);  
15  
> L[1];  
[1]:  
  0  
[2]:  
  1  
[3]:  
  0
```

## Point Addition

Addition of two points on an elliptic curve:

```
> list P,Q;  
> P[1]=1;  
> P[2]=5;  
> P[3]=1;  
> Q[1]=1;  
> Q[2]=6;  
> Q[3]=1;  
> ellipticAdd(11, 5, 8, P, Q); // P+Q  
[1]:  
  0  
[2]:  
  1  
[3]:  
  0
```

## Point Multiple

Multiple of a point on an elliptic curve:

```
> list P;  
> P[1]=1;  
> P[2]=5;  
> P[3]=1;  
> ellipticMult(11, 5, 8, P, 6); // 6*P  
[1]:  
    6  
[2]:  
    1  
[3]:  
    1
```

## Addition Table

The elliptic curve  $\mathcal{C}$  over  $\mathbb{Z}_7$  given by  
 $f = Y^2Z - X^3 - 3XZ^2 - 5Z^3$  has the points

$$P_1 = O = [0 : 1 : 0], \quad P_2 = [1 : 4 : 1], \quad P_3 = [1 : 3 : 1],$$

$$P_4 = [4 : 2 : 1], \quad P_5 = [4 : 5 : 1],$$

$$P_6 = [6 : 1 : 1], \quad P_7 = [6 : 6 : 1].$$

The addition table is as follows:

+	$O$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$
$O$	$O$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$
$P_2$		$P_6$	$O$	$P_5$	$P_7$	$P_4$	$P_3$
$P_3$			$P_7$	$P_6$	$P_4$	$P_2$	$P_5$
$P_4$				$P_3$	$O$	$P_7$	$P_2$
$P_5$					$P_2$	$P_3$	$P_6$
$P_6$						$P_5$	$O$
$P_7$							$P_4$

## Division Polynomials

```

> LIB "crypto.lib";
> ring r = 0, (x,y), dp;
> ellipticRandomCurve(11);
[1]:
    4
[2]:
    9
[3]:
    1
> generateG(4,9,2);
2x
> generateG(4,9,3);
3y4+24y2+108y-16

```

# Part V

## Theory of Elliptic Curves

## Elliptic Curves

- Endomorphisms
- Frobenius endmorphism
- Torsion subgroup
- Division polynomials
- Weil pairing
- \*Divisors
- Use of Singular

## Endomorphisms



Ferdinand Georg Frobenius (1849-1917).

## Endomorphisms

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$ .

A mapping  $\phi : \mathcal{E}(\bar{\mathbb{K}}) \rightarrow \mathcal{E}(\bar{\mathbb{K}})$  is an *endomorphism* of  $\mathcal{E}$  if

- $\phi$  is a homomorphism, i.e., for all  $P_1, P_2 \in \mathcal{E}(\bar{\mathbb{K}})$

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2), \quad (172)$$

- there are rational functions (quotients of polynomials)  $r_1(X, Y), r_2(X, Y)$  with coefficients in  $\bar{\mathbb{K}}$  such that for all  $(x, y) \in \mathcal{E}(\bar{\mathbb{K}})$  (in affine coordinates)

$$\phi(x, y) = (r_1(x, y), r_2(x, y)). \quad (173)$$

For each homomorphism  $\phi$ ,

$$\phi(O) = O. \quad (174)$$

The trivial endomorphism maps each point to the base point  $O$  and is denoted by  $0$ .

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  with  $\text{char}(\mathbb{K}) \neq 2, 3$  given by  $Y^2 = X^3 + pX + q$ .

An endomorphism of  $\mathcal{E}$  is given by the doubling operation

$$\phi : \mathcal{E}(\bar{\mathbb{K}}) \rightarrow \mathcal{E}(\bar{\mathbb{K}}) : P \mapsto 2P. \quad (175)$$

- $\phi$  is a homomorphism,

$$\begin{aligned} \phi(P_1 + P_2) &= 2(P_1 + P_2) = 2P_1 + 2P_2 \\ &= \phi(P_1) + \phi(P_2). \end{aligned} \quad (176)$$

## Example (cont'd)

- There are rational functions by (170) and (171),

$$r_1(X, Y) = \left( \frac{3X^2 + p}{2Y} \right)^2 - 2X, \quad (177)$$

$$r_2(X, Y) = \left( \frac{3X^2 + p}{2Y} \right) \left( 2X - \left( \frac{3X^2 + p}{2Y} \right)^2 \right) - \frac{-3X^3 + pX + 2q}{2Y} \quad (178)$$

such that

$$\phi(x, y) = (r_1(x, y), r_2(x, y)). \quad (179)$$

## Endomorphisms

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  given by  $Y^2 = X^3 + pX + q$ . Each endomorphism  $\phi$  of  $\mathcal{E}$  can be written as

$$\phi(X, Y) = (r_1(X), r_2(X)Y) \quad (180)$$

with rational functions  $r_1(X), r_2(X)$ .

### Proof.

Using  $Y^2 = X^3 + pX + q$  replace each power  $Y^{2m}$  by  $(X^3 + pX + q)^m$  and each power  $Y^{2m+1}$  by  $(X^3 + pX + q)^m Y$ . Thus each rational function  $r(X, Y)$  over  $\bar{\mathbb{K}}$  has the form

$$r(X, Y) = \frac{p_1(X) + p_2(X)Y}{p_3(X) + p_4(X)Y}.$$

## Proof (cont'd).

Multiplying numerator and denominator by  $p_3(X) - p_4(X)Y$  gives

$$r(X, Y) = \frac{q_1(X) + q_2(X)Y}{q_3(X)}$$

for some rational functions  $q_1(X), q_2(X), q_3(X)$ .

Take the endomorphism  $\phi$  of  $\mathcal{E}$  given by

$$\phi(X, Y) = (r_1(X, Y), r_2(X, Y)).$$

Then

$$\phi(X, -Y) = \phi(-(X, Y)),$$

since  $-(X, Y) = (X, -Y)$  is the inverse point, and

$$\phi(-(X, Y)) = -\phi(X, Y),$$

since  $\phi$  is a homomorphism.

## Proof (cont'd).

It follows that

$$\phi(X, -Y) = (r_1(X, -Y), r_2(X, -Y)) = -\phi(X, Y)$$

and so

$$r_1(X, -Y) = r_1(X, Y) \quad \text{and} \quad r_2(X, -Y) = -r_2(X, Y).$$

Write

$$r_1(X, Y) = \frac{q_1(X) + q_2(X)Y}{q_3(X)} \quad \text{and} \quad r_2(X, Y) = \frac{q'_1(X) + q'_2(X)Y}{q'_3(X)}.$$

Since  $r_1(X, -Y) = r_1(X, Y)$ ,  $q_2(X) = 0$ , and since  $r_2(X, -Y) = -r_2(X, Y)$ ,  $q'_1(X) = 0$ . Hence,  $\phi(X, Y)$  has the required form. □

## Degree

Given an endomorphism  $\phi$  of an elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  by

$$\phi(X, Y) = (r_1(X), r_2(X)Y) \quad (181)$$

with

$$r_1(X) = \frac{p(X)}{q(X)}, \quad (182)$$

where  $p(X)$  and  $q(X)$  are polynomial without common factor.  
If  $\phi$  is nontrivial, the *degree* of  $\phi$  is

$$\deg(\phi) = \max\{\deg p(X), \deg q(X)\}. \quad (183)$$

The degree of the trivial endomorphism  $\phi = 0$  is  $\deg(0) = 0$ .

## Separability

Given a nontrivial endomorphism  $\phi$  of an elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  by

$$\phi(X, Y) = (r_1(X), r_2(X)Y) \quad (184)$$

with

$$r_1(X) = \frac{p(X)}{q(X)}, \quad (185)$$

where  $p(X)$  and  $q(X)$  are polynomials without common factor.

The endomorphism  $\phi$  is *separable* if the derivative  $r_1'(X)$  is not identically zero.

- If  $\text{char}(\mathbb{K}) = 0$ , each nonconstant polynomial has nonzero derivative.
- If  $\text{char}(\mathbb{K}) = p > 0$ , the polynomials with zero derivative are of the form  $g(X^p)$ .

## Example (cont'd)

Reconsider the elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  with  $\text{char}(\mathbb{K}) \neq 2, 3$  given by  $Y^2 = X^3 + pX + q$  and endomorphism  $\phi(P) = 2P$ .

Then

$$r_1(X, Y) = \left( \frac{3X^2 + p}{2Y} \right)^2 - 2X. \quad (186)$$

Since  $Y^2 = X^3 + pX + q$ ,

$$r_1(X) = \frac{X^4 - 2pX^2 - 8qX + p^2}{4(X^3 + pX + q)}. \quad (187)$$

Thus the endomorphism  $\phi$  has degree  $\deg(\phi) = 4$ .

The derivative

$$r'_1(X) = \frac{X^6 + 5pX^4 + 20qX^3 - 5p^2X^2 - 4pqX - p^3 - 8q^2}{4(X^3 + pX + q)^2} \quad (188)$$

is not identically zero and so  $\phi$  is separable.

## Endomorphisms

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$  with endomorphism  $\phi \neq 0$ .  
The *kernel* of  $\phi$  is

$$\ker(\phi) = \{P \in \mathcal{E}(\bar{\mathbb{K}}) \mid \phi(P) = O\}. \quad (189)$$

- If  $\phi$  is separable,

$$\deg \phi = \#\ker(\phi). \quad (190)$$

- If  $\phi$  is not separable,

$$\deg \phi > \#\ker(\phi). \quad (191)$$

(See Washington, section 2.9)

## Endomorphisms

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$ . Each nonzero endomorphism  $\phi : \mathcal{E}(\bar{\mathbb{K}}) \rightarrow \mathcal{E}(\bar{\mathbb{K}})$  is surjective.

### Proof.

Let  $P \in \mathcal{E}(\bar{\mathbb{K}})$ . Since  $\phi(O) = O$ , we may assume that  $P \neq O$ . For the affine part, take  $P = (a, b)$  and write

$$\phi(X, Y) = (r(X), s(X)Y).$$

Write  $r(X) = g(X)/h(X)$ . If  $g(X) - ah(X)$  is not a constant polynomial, it has a root  $x_0 \in \bar{\mathbb{K}}$ ; i.e.,  $g(x_0) = ah(x_0)$ . As  $g(X), h(X)$  have no common root,  $h(x_0) \neq 0$ . Take  $y_0 \in \bar{\mathbb{K}}$  as a square root of  $x_0^3 + px_0 + q$ . Then  $\phi(x_0, y_0) = (a, c)$  with  $c^2 = a^3 + pa + q = b^2$  and so  $c = \pm b$ . If  $c = b$ , we are done; otherwise,  $\phi(x_0, -y_0) = (a, -c) = (a, b)$ . Thus  $\phi$  is surjective. The case where  $g - ah$  is constant is similar.  $\square$

## Endomorphisms

Let  $\phi_1, \phi_2, \phi_3$  be nonzero endomorphisms of elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  with  $\phi_1 + \phi_2 = \phi_3$ . Write

$$\phi_i(X, Y) = (r_i(X), s_i(X)Y), \quad 1 \leq i \leq 3. \quad (192)$$

If there are constants  $c_1, c_2$  with

$$\frac{r'_1(X)}{s_1(X)} = c_1 \quad \text{and} \quad \frac{r'_2(X)}{s_2(X)} = c_2, \quad (193)$$

then

$$\frac{r'_3(X)}{s_3(X)} = c_1 + c_2. \quad (194)$$

Proof uses differentials (Washington, section 2.9).

## Endomorphisms

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$  and let  $n \neq 0$  be an integer. If multiplication by  $n$  on  $\mathcal{E}$  is given by

$$[n](X, Y) = (r_n(X), s_n(X)Y), \quad (195)$$

then

$$\frac{r'_n(X)}{s_n(X)} = n. \quad (196)$$

Thus multiplication by  $n$  is separable iff  $\text{char}(\mathbb{K}) \nmid n$ .

### Proof.

The assertion holds for  $n = 1$ , since  $r_1(X) = X$  and  $s_1(X) = 1$ . If it holds for  $n \geq 1$ , then also for  $n + 1$ , which by induction hypothesis and (194) is the sum of  $c_1 = 1$  and  $c_2 = n$ .  $\square$

## Frobenius Endomorphism



Ferdinand Georg Frobenius (1849-1917).

## Frobenius Endomorphism

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F} = \mathbb{F}_q$ . The mapping

$$\phi_q : \mathcal{E}(\bar{\mathbb{F}}) \rightarrow \mathcal{E}(\bar{\mathbb{F}}) : (a : b : c) \mapsto (a^q : b^q : c^q) \quad (197)$$

is an endomorphism of  $\mathcal{E}$  of degree  $q$ , but  $\phi_q$  is not separable.  
 $\phi_q$  is called *Frobenius endomorphism* of  $\mathcal{E}$ .

## Frobenius Map

Let  $\mathbb{F}$  be a field of characteristic  $p > 0$ . The mapping

$$\phi : \mathbb{F} \rightarrow \mathbb{F} : a \mapsto a^p \quad (198)$$

is a ring endomorphism, called *Frobenius map*. We have

$$\phi(1) = 1, \quad \phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b) \quad (199)$$

and (Freshman's dream)

$$\begin{aligned} \phi(a+b) &= (a+b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} = a^p + b^p \\ &= \phi(a) + \phi(b), \end{aligned} \quad (200)$$

since in the binomial coefficient  $\binom{p}{i} = \frac{p!}{i!(p-i)!}$  with  $1 \leq i \leq p-1$ , the numerator is divisible by  $p$  but the denominator is not.

## Frobenius Map – Example

The field  $\mathbb{F}_8 = \mathbb{Z}_2[X]/\langle X^3 + X + 1 \rangle$  has the elements

$$\begin{array}{l} 0, \quad \alpha, \quad \alpha^3 = \alpha + 1, \quad \alpha^5 = \alpha^2 + \alpha + 1, \\ 1, \quad \alpha^2, \quad \alpha^4 = \alpha^2 + \alpha, \quad \alpha^6 = \alpha^2 + 1, \end{array}$$

where  $\alpha^7 = 1$  and  $\alpha$  is a zero of  $X^3 + X + 1$  in  $\mathbb{F}_8$ , i.e.,

$$\alpha^3 = \alpha + 1.$$

The Frobenius map  $\mathbb{F}_8 \rightarrow \mathbb{F}_8 : a \mapsto a^2$  gives

$$\begin{array}{ll} \phi(0) = 0, & \phi(1) = 1, \\ \phi(\alpha) = \alpha^2, & \phi(\alpha^2) = \alpha^4, \\ \phi(\alpha^3) = \alpha^6, & \phi(\alpha^4) = \alpha, \\ \phi(\alpha^5) = \alpha^3, & \phi(\alpha^6) = \alpha^5. \end{array}$$

It fixes the prime field  $\mathbb{Z}_2$ :  $0^2 = 0$  and  $1^2 = 1$ .

## Frobenius Map – Example

- The Frobenius map  $\phi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  is the identity mapping, since by Little Fermat,

$$a^p = a \text{ for each } a \in \mathbb{Z}_p. \quad (201)$$

- The Frobenius map  $\phi : \mathbb{Z}_p[X] \rightarrow \mathbb{Z}_p[X]$  fulfills by Little Fermat and Freshman's Dream

$$\left( \sum_i a_i X^i \right)^p = \sum_i a_i X^{pi}, \quad a_i \in \mathbb{Z}_p. \quad (202)$$

- The Frobenius map  $\phi : \mathbb{F}_q[X] \rightarrow \mathbb{F}_q[X]$  fulfills by (206) and Freshman's Dream

$$\left( \sum_i a_i X^i \right)^q = \sum_i a_i X^{qi}, \quad a_i \in \mathbb{F}_q. \quad (203)$$

## Frobenius Map

Let  $\mathbb{F}$  be a field of characteristic  $p > 0$ . The Frobenius map

$$\phi : \mathbb{F} \rightarrow \mathbb{F} : a \mapsto a^p \quad (204)$$

is injective.

### Proof.

If  $\phi(a) = a^p = 0$  for some  $a \in \mathbb{F}$ , then  $a$  is nilpotent. But a field has no zero divisors and so  $a = 0$ .  $\square$

A field  $\mathbb{F}$  of characteristic  $p > 0$  is *perfect* if the Frobenius map of  $\mathbb{F}$  is surjective and so an automorphism.

## Frobenius Map

Each finite field  $\mathbb{F}$  is perfect.

### Proof.

The Frobenius map  $\phi : \mathbb{F} \rightarrow \mathbb{F}$  is injective. But each injective mapping between two finite sets of the same cardinality is also surjective and so bijective.  $\square$

## Frobenius Map

The rational function field

$$\mathbb{F} = \mathbb{Z}_p(X) = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in \mathbb{Z}_p[X], g(X) \neq 0 \right\}$$

is not perfect.

**Proof.**

The unknown  $X$  does not lie in the image of the Frobenius map.

Indeed, suppose  $X = \left( \frac{f(X)}{g(X)} \right)^p$  for some  $f(X), g(X) \in \mathbb{Z}_p[X]$ ,  $g(X) \neq 0$ . Then  $g(X)^p X = f(X)^p$ .

Write  $f(X) = \sum_i a_i X^i$  and  $g(X) = \sum_i b_i X^i$ . Then

$$\sum_i b_i X^{ip+1} = \sum_i a_i X^{ip}.$$

By comparing coefficients,  $a_i = b_i = 0$  contradicting  $g(X) \neq 0$ .  $\square$

## Frobenius Map

Consider the prime field  $\mathbb{F}_p = \mathbb{Z}_p$  of characteristic  $p > 0$ .

By Little Fermat, each element  $a \in \mathbb{F}_p$  satisfies  $a^p = a$ . Thus  $a$  is a root of the polynomial

$$X^p - X \in \mathbb{F}_p[X]. \quad (205)$$

The elements of  $\mathbb{F}_p$  are therefore the roots of this polynomial, since any polynomial of degree  $p$  has not more than  $p$  roots over any extension field.

More generally, if  $\mathbb{F}$  is an algebraic extension of  $\mathbb{F}_p$  such as the algebraic closure of  $\mathbb{F}_p$ , then  $\mathbb{F}_p$  is the *fixed field* of the Frobenius map  $\mathbb{F} \rightarrow \mathbb{F} : a \mapsto a^p$ .

## Frobenius Map – Example

Consider the prime field  $\mathbb{F}_3 = \{0, 1, 2\}$  ( $p = 3$ ).

The polynomial  $g = X^2 + X + 2 \in \mathbb{F}_3[X]$  is irreducible.

The extension field  $\mathbb{F} = \mathbb{F}_9 = \mathbb{F}_3[X]/\langle g \rangle$  is given by

$$\mathbb{F}_9 = \{a\alpha + b \mid a, b \in \mathbb{F}_3\}$$

where  $\alpha^2 + \alpha + 2 = 0$ ; i.e.,  $\alpha^2 = 2\alpha + 1$ .

**Addition**

$$(a\alpha + b) + (c\alpha + d) = (a + c)\alpha + (b + d).$$

**Multiplication**

$$\begin{aligned} (a\alpha + b)(c\alpha + d) &= a c \alpha^2 + a d \alpha + b c \alpha + b d \\ &= (2ac + ad + bc)\alpha + (ac + bd). \end{aligned}$$

The automorphism  $\phi : \mathbb{F}_9 \rightarrow \mathbb{F}_9 : a \mapsto a^3$  fixes the elements of  $\mathbb{F}_3 \subseteq \mathbb{F}_9$ .

## Frobenius Map

Let  $\mathbb{F}_q$  denote the finite field with  $q = p^r$  elements.

The  $r$ -th iterate of the Frobenius automorphism has similar properties. For this, note that the elements of  $\mathbb{F}_q$  are exactly the roots of the polynomial

$$X^q - X \in \mathbb{F}_q[X]. \quad (206)$$

The elements of  $\mathbb{F}_p$  are therefore the roots of this polynomial, since any polynomial of degree  $p$ . Thus if  $\mathbb{F}$  is an algebraic extension of  $\mathbb{F}_q$ , the  $r$ -th iterate of the Frobenius map,

$$\phi : \mathbb{F} \rightarrow \mathbb{F} : a \mapsto a^q, \quad (207)$$

has the *fixed field*  $\mathbb{F}_q$ .

## Frobenius Map – Example

Consider the field  $\mathbb{F}_4 = \{0, 1, \beta, \beta^2\}$ , where  $\beta^2 = \beta + 1$  ( $q = 4$ ).

The polynomial  $g = X^2 + X + \beta \in \mathbb{F}_4[X]$  is irreducible.

The extension field  $\mathbb{F} = \mathbb{F}_{16} = \mathbb{F}_4[X]/\langle g \rangle$  is given by

$$\mathbb{F}_{16} = \{a\alpha + b \mid a, b \in \mathbb{F}_4\}$$

where  $\alpha^2 + \alpha + \beta = 0$ ; i.e.,  $\alpha^2 = \alpha + \beta$ .

**Addition**

$$(a\alpha + b) + (c\alpha + d) = (a + c)\alpha + (b + d).$$

**Multiplication**

$$\begin{aligned} (a\alpha + b)(c\alpha + d) &= aca^2 + ada + bca + bd \\ &= (ac + ad + bc)\alpha + (ac\beta + bd). \end{aligned}$$

The automorphism  $\phi : \mathbb{F}_{16} \rightarrow \mathbb{F}_{16} : a \mapsto a^4$  fixes the elements of  $\mathbb{F}_4 \subseteq \mathbb{F}_{16}$ .

## Proof (Frobenius map).

- The mapping  $\phi_q$  is well-defined. Indeed, since the Frobenius map of  $\mathbb{F}$  is injective,  $a^q = b^q = c^q = 0$  implies  $a = b = c = 0$ .
- Moreover, the mapping  $\phi_q$  preserves the equivalence classes defining the projective space  $\mathbb{P}^2(\bar{\mathbb{F}})$ .

Indeed, if  $(a, b, c)$  and  $(e, d, f)$  represent the same point in  $\mathbb{P}^2(\bar{\mathbb{F}})$ , then

$$(e, d, f) = (ta, tb, tc)$$

for some nonzero  $t \in \bar{\mathbb{F}}$ . Then

$$(e^q, d^q, f^q) = ((ta)^q, (tb)^q, (tc)^q) = (t^q a^q, t^q b^q, t^q c^q)$$

and  $(a^q, b^q, c^q)$  represent the same point as well.

## Proof (cont'd).

- Let the elliptic curve  $\mathcal{E}(\mathbb{F})$  be given by the general Weierstrass polynomial  $f \in \mathbb{F}[X, Y, Z]$ , and let  $P = (a : b : c) \in \mathcal{E}(\bar{\mathbb{F}})$ . Then  $f(a, b, c) = 0$  and thus by the Frobenius map of  $\mathbb{F}$  (see (203)),

$$0 = f(a, b, c)^q = f(a^q, b^q, c^q).$$

Hence,  $\phi_q(P) = (a^q : b^q : c^q)$  is also a point of  $\mathcal{E}(\bar{\mathbb{F}})$ .

- Claim that the mapping commutes with the group operation. Indeed, the base point  $O = (0 : 1 : 0)$  satisfies  $\phi_q(0 : 1 : 0) = (0 : 1 : 0)$ . Since  $O$  is the identity element, each point  $P$  of  $\mathcal{E}(\bar{\mathbb{F}})$  satisfies

$$\phi_q(P + O) = \phi_q(P) = \phi_q(P) + O = \phi_q(P) + \phi_q(O).$$

## Proof (cont'd).

- Let  $P_1$  and  $P_2$  be two points of  $\mathcal{E}(\bar{\mathbb{F}})$  different from the base point  $O$ . Then they lie in the affine plane and can be written as  $P_1 = (x_1, y_1)$  and  $P_2 = (x_2, y_2)$ .

First consider the point addition  $P_1 + P_2 = P_3$  with  $P_1 \neq -P_2$ . Then  $P_3 = (x_3, y_3)$ , where by (166) and (167),

$$\begin{aligned}x_3 &= m^2 + a_1m - a_2 - x_1 - x_2, \\y_3 &= -(m + a_1)x_3 - b - a_3\end{aligned}$$

where  $m, b \in \bar{\mathbb{F}}$ . By (164) and (165),

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

and

$$b = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

## Proof (cont'd).

Applying the Frobenius map of  $\mathbb{F}$  gives

$$x_3^q = (m^q)^2 + a_1 m^q - a_2 - x_1^q - x_2^q,$$

$$y_3^q = -(m^q + a_1)x_3^q - b^q - a_3,$$

since  $a_1, a_2, a_3 \in \mathbb{F}$ .

On the other hand,

$$\phi_q(P_1) + \phi_q(P_2) = (x_1^q, y_1^q) + (x_2^q, y_2^q) = (x_4, y_4),$$

where by (166) and (167),

$$x_4 = \hat{m}^2 + a_1 \hat{m} - a_2 - x_1^q - x_2^q,$$

$$y_4 = -(\hat{m} + a_1)x_4^q - \hat{b} - a_3$$

for some  $\hat{m}, \hat{b} \in \bar{\mathbb{F}}$ .

## Proof (cont'd).

By (164), (165) and Freshman's dream,

$$\hat{m} = \frac{y_2^q - y_1^q}{x_2^q - x_1^q} = m^q$$

and

$$\hat{b} = \frac{y_1^q x_2^q - y_2^q x_1^q}{x_2^q - x_1^q} = b^q.$$

Hence,

$$\begin{aligned} \phi_q(P_1) + \phi_q(P_2) &= (x_4, y_4) \\ &= (x_3^q, y_3^q) \\ &= \phi_q(P_3) \\ &= \phi_q(P_1 + P_2). \end{aligned}$$

The other cases are similar.

## Proof (cont'd).

- The discriminant  $\Delta \neq 0$  of  $\mathcal{E}$  is an element of  $\mathbb{F}_q$ . Thus  $\Delta^q = \Delta$  and hence the image of  $\mathcal{E}$  is nonsingular.
- The Frobenius endomorphism

$$\phi_q(X, Y) = (r_1(X), r_2(Y)) = (X^q, Y^q) \quad (208)$$

has degree  $\deg r_1(X) = q$ .

- Since  $q = 0$  in  $\mathbb{F}_q$ , the derivative of  $r_1(X) = X^q$  satisfies

$$r_1'(X) = qX^{q-1} = 0 \quad (209)$$

and so  $\phi_q$  is not separable.

□

## Endomorphisms

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$  with  $q = p^r$ ,  $p \neq 2$ , given by  $Y^2 = X^3 + AX + B$ , and let  $m, n$  be integers, not both 0.

The endomorphism

$$[m]\phi_q + [n], \quad (210)$$

written  $m\phi_q + n$ , is separable iff  $p \nmid n$ .

### Proof.

By (237), we can write

$$[m](X, Y) = (r_m(X), s_m(X)Y).$$

Then as  $q$  is odd,

$$\begin{aligned} & (r_{m\phi_q}(X), s_{m\phi_q}(X)Y) \\ &= \phi_q[m](X, Y) = (r_m^q(X), s_m^q(X)Y^q) \\ &= \left( r_m^q(X), Y(X^3 + AX + B)^{(q-1)/2} s_m^q(X) \right). \end{aligned}$$

## Proof (cont'd).

Thus

$$c_{m\phi_q} = r'_{m\phi_q} / s_{m\phi_q} = qr_m^{q-1} r'_m / s_{m\phi_q} = 0.$$

Moreover, by (196),

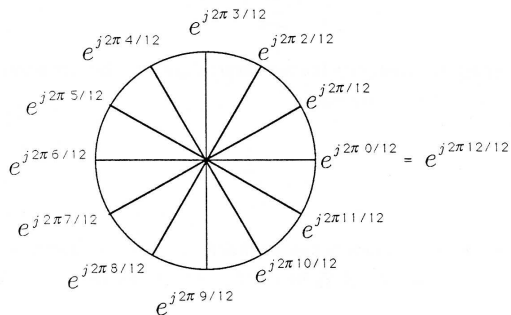
$$c_n = r'_n / s_n = n$$

and so by (194),

$$r'_{m\phi_q+n} / s_{m\phi_q+n} = c_{m\phi_q+n} = c_{m\phi_q} + c_n = 0 + n = n.$$

Hence,  $r'_{m\phi_q+n} \neq 0$  iff  $p \nmid n$ . □

## Torsion Subgroup



## Torsion Subgroup

Let  $\mathcal{E}$  be an elliptic curve over field  $\mathbb{K}$  and let  $n \geq 0$  be an integer. The mapping

$$[n] : \mathcal{E}(\bar{\mathbb{K}}) \rightarrow \mathcal{E}(\bar{\mathbb{K}}) : P \mapsto [n]P = nP \quad (211)$$

is a group homomorphism with kernel

$$\mathcal{E}[n] = \{P \in \mathcal{E}(\bar{\mathbb{K}}) \mid nP = O\} \quad (212)$$

called *n-torsion subgroup* of  $\mathcal{E}$ .

The *torsion subgroup* of  $\mathcal{E}$  is given by the points of finite order

$$\mathcal{E}_{\text{tor}} = \bigcup_{n=0}^{\infty} \mathcal{E}[n]. \quad (213)$$

The mapping  $[n]$  is an endomorphism of  $\mathcal{E}$  (see division polynomials).

## Torsion Subgroup

Let  $\mathcal{E}$  be an elliptic curve over field  $\mathbb{K}$  and let  $n \geq 2$  be an integer. If  $\text{char}(\mathbb{K}) = 0$  or  $\text{char}(\mathbb{K}) \nmid n$ , then

$$\mathcal{E}[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n. \quad (214)$$

If  $\text{char}(\mathbb{K}) = p > 0$  and  $p \mid n$ , write  $n = p^r m$  with  $p \nmid m$ , then

$$\mathcal{E}[n] \simeq \mathbb{Z}_m \oplus \mathbb{Z}_m \quad \text{or} \quad \mathcal{E}[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_m. \quad (215)$$

## Proof.

Let  $\text{char}(\mathbb{K}) = 0$  or  $\text{char}(\mathbb{K}) \nmid n$ .

- By (237), we have

$$[n](X, Y) = (r(X), s(X)Y) \quad (216)$$

for some rational functions  $r(X), s(X)$ . Then using division polynomials,

$$r(X) = \frac{X^{n^2} + \text{lower degree terms}}{n^2 X^{n^2-1} + \text{lower degree terms}}. \quad (217)$$

By hypothesis on  $\mathbb{K}$ ,  $r'(X) \neq 0$  and so the endomorphism  $[n]$  is separable.

- By (217), the endomorphism  $[n]$  has degree  $n^2$  and so by (190),  $\mathcal{E}[n] = \ker([n])$  has order  $n^2$ .

## Proof (cont'd)

- By the structure theorem for finite abelian groups,  $\mathcal{E}[n]$  is isomorphic to

$$\mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k},$$

where  $n_1, \dots, n_k$  are integers with  $n_i \mid n_{i+1}$  for all  $i$ .

- Let  $\ell$  be a prime dividing  $n_1$ . Then  $\ell \mid n_i$  for all  $i$  and so  $\mathcal{E}[\ell] \subseteq \mathcal{E}[n]$  has order  $\ell^k$ . But  $\mathcal{E}[\ell]$  has order  $\ell^2$  and so  $k = 2$ .
- We have  $\mathcal{E}[n] = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ . Since  $\mathbb{Z}_{n_2}$  is a subgroup of  $\mathcal{E}[n]$ , we have  $n_2 \mid n$ .
- We have  $n^2 = \#\mathcal{E}[n] = n_1 n_2$  and so  $n_1 = n_2 = n$  (as  $n_1, n_2$  are both divisors of  $n$ ).

The case  $\text{char}(\mathbb{K}) = p > 0$  and  $p \mid n$  is quite similar. □

## Torsion Subgroup

The direct product group  $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$  is defined by the componentwise operation

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2). \quad (218)$$

In particular, if  $(m, n) = 1$ , there exists an isomorphism

$$\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n \quad (219)$$

given by

$$a \mapsto (a \bmod m, a \bmod n). \quad (220)$$

Surjectivity is proved by the Chinese remainder theorem.

### Examples

$\mathbb{Z}_6$  and  $\mathbb{Z}_2 \oplus \mathbb{Z}_3$  are isomorphic by (219), but  $\mathbb{Z}_4$  (cyclic) and  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$  (noncyclic) are not.

## Torsion Subgroup

Suppose  $\text{char}(\mathbb{K}) = 0$  or  $\text{char}(\mathbb{K}) \nmid n$ .

- Then  $\mathcal{E}[n] = \mathbb{Z}_n \oplus \mathbb{Z}_n$  has a *basis*  $\{\beta_1, \beta_2\}$ ; i.e., each element  $\mathcal{E}[n]$  can be uniquely written in the form

$$k_1\beta_1 + k_2\beta_2 \quad (221)$$

with integers  $k_1, k_2$  (uniquely determined mod  $n$ ).

- A homomorphism  $\phi : \mathcal{E}(\bar{\mathbb{K}}) \rightarrow \mathcal{E}(\bar{\mathbb{K}})$  maps  $\mathcal{E}[n]$  into  $\mathcal{E}[n]$ .  
Indeed, if  $P \in \mathcal{E}[n]$ , then

$$n\phi(P) = \phi(nP) = \phi(O) = O$$

and so  $\phi(P) \in \mathcal{E}[n]$ .

## Torsion Subgroup (cont'd)

- There are  $a, b, c, d \in \mathbb{Z}$  such that

$$\phi(\beta_1) = a\beta_1 + c\beta_2 \quad \text{and} \quad \phi(\beta_2) = b\beta_1 + d\beta_2. \quad (222)$$

- Each homomorphism  $\phi : \mathcal{E}(\bar{\mathbb{K}}) \rightarrow \mathcal{E}(\bar{\mathbb{K}})$  is represented by an integral  $2 \times 2$  transformation matrix

$$\phi^{(n)} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \quad (223)$$

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{R}$  given by  $f = Y^2Z - X^3 + 2Z^3$  and let  $n = 2$ . Then

$$\mathcal{E}[2] = \{O, (\sqrt[3]{2} : 0 : 1), (\xi\sqrt[3]{2} : 0 : 1), (\xi^2\sqrt[3]{2} : 0 : 1)\},$$

where  $\xi = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2} \in \bar{\mathbb{R}} = \mathbb{C}$  is a primitive third root of unity.

- A basis for  $\mathcal{E}[2]$  is

$$\{\beta_1 = (\sqrt[3]{2} : 0 : 1), \beta_2 = (\xi\sqrt[3]{2} : 0 : 1)\}.$$

- We have

$$(\sqrt[3]{2} : 0 : 1) + (\xi\sqrt[3]{2} : 0 : 1) = (\xi^2\sqrt[3]{2} : 0 : 1).$$

- We have  $\mathcal{E}[2] = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

## Division Polynomials

Singular computation:

```
> LIB "crypto.lib";  
> ring r = 0, (y,x), dp;  
> generateG(4,9,2);  
2y  
> generateG(4,9,3);  
3x4+24x2+108x-16
```

## Division Polynomials

Define the division polynomials  $\psi_m \in \mathbb{Z}[X, Y, A, B]$ ,  $m \geq 0$ , as the rational functions

$$\psi_0 = 0, \quad (224)$$

$$\psi_1 = 1, \quad (225)$$

$$\psi_2 = 2Y, \quad (226)$$

$$\psi_3 = 3X^4 + 6AX^2 + 12BX - A^2, \quad (227)$$

$$\psi_4 = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3) \quad (228)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad (229)$$

$$m \geq 2,$$

$$\psi_{2m} = \frac{1}{2Y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \quad (230)$$

$$m \geq 3.$$

## Division Polynomials

- $\psi_n$  is a polynomial in  $\mathbb{Z}[X, Y^2, A, B]$  if  $n$  is odd.
- $\psi_n$  is a polynomial in  $2Y\mathbb{Z}[X, Y^2, A, B]$  if  $n$  is even.

### Proof.

The assertion holds for  $n \leq 4$ . Assume that  $2m > 4$ , so  $m > 2$ . Then  $2m > m + 2$ . Thus all polynomials appearing in the definition of  $\psi_{2m}$  fulfill the induction hypothesis.

- If  $m$  is even, then  $\psi_m, \psi_{m+2}, \psi_{m-2} \in 2Y\mathbb{Z}[X, Y^2, A, B]$  by induction hypothesis and so  $\psi_{2m} \in 2Y\mathbb{Z}[X, Y^2, A, B]$ .
- If  $m$  is odd, then  $\psi_{m+1}, \psi_{m-1} \in 2Y\mathbb{Z}[X, Y^2, A, B]$  by induction hypothesis and so  $\psi_{2m} \in 2Y\mathbb{Z}[X, Y^2, A, B]$ .

Thus the assertion holds for  $n = 2m$ . Similar for  $n = 2m + 1$ .  $\square$

## Division Polynomials

Define the rational functions

$$\phi_n = X\psi_n^2 - \psi_{n-1}\psi_{n+1}, \quad (231)$$

$$\omega_n = \frac{1}{4Y} (\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2). \quad (232)$$

We have

- $\phi_n \in \mathbb{Z}[X, Y^2, A, B]$  for all  $n$ .
- $\omega_n \in Y\mathbb{Z}[X, Y^2, A, B]$  if  $n$  is odd, and  
 $\omega_n \in \mathbb{Z}[X, Y^2, A, B]$  if  $n$  is even.

## Proof.

■ Case  $\phi_n$ :

- If  $n$  is odd, then  $\psi_{n-1}, \psi_{n+1} \in 2Y\mathbb{Z}[X, Y^2, A, B]$  and so  $\psi_{n-1} \cdot \psi_{n+1} \in \mathbb{Z}[X, Y^2, A, B]$ . Moreover,  $\psi_n \in \mathbb{Z}[X, Y^2, A, B]$  and so  $\phi_n \in \mathbb{Z}[X, Y^2, A, B]$ .
- If  $n$  is even, then  $\psi_{n-1}, \psi_{n+1} \in \mathbb{Z}[X, Y^2, A, B]$  and so  $\psi_{n-1} \cdot \psi_{n+1} \in \mathbb{Z}[X, Y^2, A, B]$ . Moreover,  $\psi_n \in 2Y\mathbb{Z}[X, Y^2, A, B]$  and so  $\phi_n \in \mathbb{Z}[X, Y^2, A, B]$ .

■ Case  $\omega_n$ :

- If  $n$  is odd, then  $\psi_{n+2}, \psi_{n-2} \in \mathbb{Z}[X, Y^2, A, B]$  and  $\psi_{n+1}, \psi_{n-1} \in 2Y\mathbb{Z}[X, Y^2, A, B]$ . Thus  $\psi_{n+2}\psi_{n-1}^2, \psi_{n-2}\psi_{n+1}^2 \in 4Y^2\mathbb{Z}[X, Y^2, A, B]$  and so  $\omega_n \in Y\mathbb{Z}[X, Y^2, A, B]$ .
- If  $n$  is even, then  $\psi_{n+2}, \psi_{n-2} \in 2Y\mathbb{Z}[X, Y^2, A, B]$  and  $\psi_{n+1}, \psi_{n-1} \in \mathbb{Z}[X, Y^2, A, B]$ . Thus  $\psi_{n+2}\psi_{n-1}^2, \psi_{n-2}\psi_{n+1}^2 \in 2Y\mathbb{Z}[X, Y^2, A, B]$  and so  $\omega_n \in \frac{1}{2}\mathbb{Z}[X, Y^2, A, B]$ .

## Proof (cont'd).

- In  $\omega_n \in \frac{1}{2}\mathbb{Z}[X, Y^2, A, B]$ , the factor  $\frac{1}{2}$  can be eliminated by observing by induction that

$$\psi_n \equiv (X^2 + A)^{(n^2-1)/4} \pmod{2}, \quad n \text{ odd},$$

and

$$\frac{1}{2Y}\psi_n \equiv \frac{n}{2}(X^2 + A)^{(n^2-4)/4} \pmod{2}, \quad n \text{ even}.$$



## Division Polynomials

Consider the elliptic curve  $\mathcal{E}$  given by the affine Weierstrass polynomial

$$Y^2 = X^3 + AX + B, \quad (233)$$

where  $A, B$  are taken as variables and by nonsingularity the discriminant is

$$4A^3 + 27B^2 \neq 0. \quad (234)$$

The polynomials in  $\mathbb{Z}[X, Y^2, A, B]$  can be regarded as polynomials in  $\mathbb{Z}[X, A, B]$  or in  $\mathbb{Z}[A, B][X]$  when  $Y^2$  is replaced by  $X^3 + AX + B$ .

## Division Polynomials

$\phi_n$  and  $\psi_n^2$  are polynomials in  $X$  with

$$\phi_n = X^{n^2} + \text{lower degree terms in } X, \quad (235)$$

$$\psi_n^2 = n^2 X^{n^2-1} + \text{lower degree terms in } X. \quad (236)$$

### Proof.

We have

- $\phi_n \in \mathbb{Z}[X, Y^2, A, B]$  for all  $n$ .
- $\psi_n \in \mathbb{Z}[X, Y^2, A, B]$  for odd  $n$  and  $\psi_n \in 2Y\mathbb{Z}[X, Y^2, A, B]$  for even  $n$ .

Replacing  $Y^2$  by  $X^3 + AX + B$  shows that  $\phi_n$  and  $\psi_n^2$  are polynomials in  $\mathbb{Z}[A, B][X]$ .

## Proof (cont'd).

The remaining assertions follow from the claim

$$\psi_n = \begin{cases} Y(nX^{(n^2-4)/2} + \dots) & \text{if } n \text{ is even,} \\ nX^{(n^2-1)/2} + \dots & \text{if } n \text{ is odd.} \end{cases}$$

To see this, consider several cases. For instance, let  $n = 2m + 1$  with  $m$  even. Then by induction, the leading term of  $\psi_{m+2}\psi_m^3$  is

$$(m+2)m^3Y^4X^{((m+2)^2-4)/2+(3m^2-12)/2}.$$

Replacing  $Y^2$  by  $X^3 + AX + B$  gives

$$(m+2)m^3X^{((2m+1)^2-1)/2}.$$

Similarly, the leading term of  $\psi_{m-1}\psi_{m+1}^3$  is

$$(m-1)(m+1)^3X^{((2m+1)^2-1)/2}.$$

By definition,  $\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$  and so the leading term is  $nX^{(n^2-1)/2}$ .  $\square$

## Point Multiplication

Let  $P = (x, y)$  be an affine point on the elliptic curve  $\mathcal{E}$  given by  $Y^2 = X^3 + AX + B$  over  $\mathbb{K}$  with  $\text{char}(\mathbb{K}) \neq 2$ , and let  $n \geq 1$  be an integer. Then

$$[n]P = \left( \frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right). \quad (237)$$

(See Washington, section 9.5)

## Corollary

Let  $\mathcal{E}$  be an elliptic curve as above. The endomorphism  $[n]$  of  $\mathcal{E}$  given by multiplication by  $n$  has degree  $n^2$ .

## Proof (Sketch).

By (237), the degree of the endomorphism  $[n]$  is

$$\max\{\phi_n(X), \psi_n^2(X)\}$$

if the quotient  $\phi_n(X)/\psi_n^2(X)$  is reduced. It can be shown that  $\phi_n(X)$  and  $\psi_n^2(X)$  have no common roots. Thus by (235) and (236) the degree is

$$\max\{\deg(X^{n^2}), \deg(n^2 X^{n^2-1})\} = n^2.$$



## Weil Pairing



André Weil (1906-1998).

## Roots of Unity

Let  $n \geq 1$  be an integer.

- An  $n$ th root of unity is a number  $z \in \mathbb{C}$  such that

$$z^n = 1. \quad (238)$$

- The  $n$ th roots of unity are

$$\exp\left(\frac{2k\pi i}{n}\right) = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad 0 \leq k \leq n-1. \quad (239)$$

The fourth roots of unity are  $\pm 1, \pm i$  with (Euler identity)

$$e^{\pi i} = -1. \quad (240)$$

- An  $n$ th root of unity  $z$  is *primitive* if

$$z^n = 1 \quad \text{and} \quad z^k \neq 1, \quad 1 \leq k \leq n-1. \quad (241)$$

## Roots of Unity

Let  $n \geq 1$  be an integer.

- The set of  $n$ th roots of unity

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} \quad (242)$$

forms a cyclic group of order  $n$ .

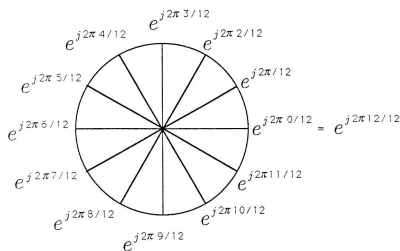
- Each primitive  $n$ th root of unity  $\xi$  is a generator of  $U_n$ ,

$$U_n = \langle \xi \rangle = \{1, \xi, \xi^2, \dots, \xi^{n-1}\}, \quad \xi^n = 1. \quad (243)$$

- If  $\xi$  is a primitive  $n$ th root of unity, then  $\xi^k$  with  $(k, n) = 1$  is also a primitive  $n$ th root of unity.

## Roots of Unity – Example

Consider the complex 12th roots of unity.



The primitive roots are  $\xi = e^{2\pi i/12}, \xi^5, \xi^7, \xi^{11}$ .

## Roots of Unity

Let  $n \geq 1$  be an integer.

- The definition of roots of unity is meaningful over any field.
- Each nonzero element in a finite field  $\mathbb{F}_q$  is a root of unity, since each nonzero element of  $\mathbb{F}_q$  satisfies by (206)

$$X^{q-1} - 1 = 0. \quad (244)$$

- For a field  $\mathbb{K}$  with  $\text{char}(\mathbb{K}) = p > 0$ , we have by Freshman's Dream

$$X^{np} - 1 = (X^n - 1)^p. \quad (245)$$

## Weil Pairing

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$  and  $n \geq 1$  with  $\text{char}(\mathbb{K}) \nmid n$ .

- The set of  $n$ -th roots of unity in  $\bar{\mathbb{K}}$ ,

$$U_n = \{x \in \bar{\mathbb{K}} \mid x^n = 1\}, \quad (246)$$

forms a cyclic group of order  $n$ , since  $\text{char}(\mathbb{K}) \nmid n$ .

- A generator  $\xi$  of  $U_n$  is a *primitive  $n$ -th root of unity*,

$$U_n = \langle \xi \rangle = \{1, \xi, \xi^2, \dots, \xi^{n-1}\}, \quad \xi^n = 1. \quad (247)$$

## Weil Pairing

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$  and  $n \geq 1$  with  $\text{char}(\mathbb{K}) \nmid n$ .  
There is a mapping

$$e_n : \mathcal{E}[n] \times \mathcal{E}[n] \rightarrow U_n, \quad (248)$$

called *Weil pairing*, such that

- $e_n$  is bilinear; i.e.,  $e_n(S + S', T) = e_n(S, T)e_n(S', T)$  and  $e_n(S, T + T') = e_n(S, T)e_n(S, T')$  for all  $S, S', T, T' \in \mathcal{E}[n]$ .
- $e_n$  is nondegenerate; i.e., if  $e_n(T, S) = 1$  for all  $S \in \mathcal{E}[n]$ , then  $T = O$ .
- $e_n(T, T) = 1$  for all  $T \in \mathcal{E}[n]$ .
- $e_n(T, S) = e_n(S, T)^{-1}$  for all  $S, T \in \mathcal{E}[n]$ .
- $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$  for all automorphisms  $\sigma$  of  $\bar{\mathbb{K}}$  which are constant on  $\mathbb{K}$ .
- $e_n(\phi(S), \phi(T)) = e_n(S, T)^{\text{deg}(\phi)}$  for all (separable or not) endomorphisms  $\phi$  of  $\mathcal{E}$ .

## Weil Pairing

If  $\{T_1, T_2\}$  is a basis of  $\mathcal{E}[n]$ , then  $e_n(T_1, T_2)$  is a primitive  $n$ -th root of unity.

### Proof.

- Let  $e_n(T_1, T_2) = \xi$  with  $\xi^d = 1$ . Then by bilinearity,  $e_n(T_1, [d]T_2) = e_n(T_1, T_2)^d = \xi^d = 1$ . Similarly,  $e_n(T_2, [d]T_2) = e_n(T_2, T_2)^d = 1$ .
- Let  $S \in \mathcal{E}[n]$ . Then by hypothesis,

$$S = aT_1 + bT_2$$

for some integers  $a, b$ . Thus by bilinearity,

$$e_n(S, [d]T_2) = e_n(T_1, [d]T_2)^a e_n(T_2, [d]T_2)^b = 1.$$

This holds for all  $S \in \mathcal{E}[n]$ . Since  $e_n$  is nondegenerate,  $[d]T_2 = O$ . But  $T_2$  has order  $n$  and so  $[d]T_2 = O$  iff  $n \mid d$ . Hence,  $\xi$  is a primitive  $n$ -th root of unity.  $\square$

## Weil Pairing

If  $\mathcal{E}[n] \subseteq \mathcal{E}(\mathbb{K})$ , then  $U_n \subset \mathbb{K}$ .

### Proof.

By definition, the points in  $\mathcal{E}[n]$  have coordinates in  $\bar{\mathbb{K}}$ . By hypothesis, these points have coordinates in  $\mathbb{K}$ .

Let  $\sigma : \bar{\mathbb{K}} \rightarrow \bar{\mathbb{K}}$  be an automorphism, which is the identity on  $\mathbb{K}$ . Let  $\{T_1, T_2\}$  be a basis of  $\mathcal{E}[n]$ . By hypothesis,  $T_1, T_2$  have coordinates in  $\mathbb{K}$  and so  $\sigma(T_1) = T_1$  and  $\sigma(T_2) = T_2$ . Thus

$$\xi = e_n(T_1, T_2) = e_n(\sigma(T_1), \sigma(T_2)) = \sigma(e_n(T_1, T_2)) = \sigma(\xi).$$

Since  $\xi$  is fixed by all automorphisms  $\sigma$ , it follows that  $\xi \in \mathbb{K}$ . Since by the previous result  $\xi$  is a primitive  $n$ -th root of unity, it generates  $U_n$  and so  $U_n \subset \mathbb{K}$ . □

## Weil Pairing

Let  $\phi$  be an endomorphism of an elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$ , and let  $n$  be a positive integer with  $\text{char}(\mathbb{K}) \nmid n$ .

- By (214),  $\mathcal{E}[n] = \mathbb{Z}_n \oplus \mathbb{Z}_n$ .
- There is a transformation matrix

$$\phi^{(n)} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_n^{2 \times 2} \quad (249)$$

describing the action of  $\phi$  on a basis  $\{T_1, T_2\}$  of  $\mathcal{E}[n]$ ; i.e.,

$$\phi(T_1) = aT_1 + cT_2 \quad \text{and} \quad \phi(T_2) = bT_1 + dT_2. \quad (250)$$

- We have

$$\det \left( \phi^{(n)} \right) \equiv \deg(\phi) \pmod{n}. \quad (251)$$

## Proof.

We have that  $\xi = e_n(T_1, T_2)$  is primitive  $n$ -th root of unity. Then by (250) and the definition of Weil pairing,

$$\begin{aligned}
 \xi^{\deg(\phi)} &= e_n(\phi(T_1), \phi(T_2)) \\
 &= e_n(aT_1 + cT_2, bT_1 + dT_2) \\
 &= e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{cd} \\
 &= e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} \\
 &= \xi^{ad-bc}.
 \end{aligned}$$

By (249), we have  $\det(\phi^{(n)}) = ad - bc$ . Since  $\xi$  is a primitive root of unity,  $\deg(\phi) \equiv \det(\phi^{(n)}) \pmod{n}$ .  $\square$

## Endomorphisms

Let  $\phi, \psi$  be endomorphisms of an elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  and let  $r, s$  be integers. The mapping  $r\phi + s\psi$  given by

$$\begin{aligned} (r\phi + s\psi)(P) &= r\phi(P) + s\psi(P) \\ &= [r](\phi(P)) + [s](\psi(P)) \end{aligned} \quad (252)$$

is an endomorphism of  $\mathcal{E}$ .

### Proof.

This mapping is a group homomorphism, since  $\phi, \psi, [r], [s]$  are group homomorphisms and the composition of group homomorphisms is a group homomorphism.

Moreover, each step of the computation (applying  $\phi, \psi$  to  $P$ , applying  $[r], [s]$ , and addition) can be described by rational functions (for  $\phi, \psi$  this holds by definition, for  $[r], [s]$  this holds by (237), and for addition this holds by the coordinate representation) and so the composition is given by rational functions. □

## Endomorphisms

Let  $\phi, \psi$  be endomorphisms of an elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  and let  $r, s$  be integers. Then

$$\begin{aligned} \deg(r\phi + s\psi) &= r^2 \deg \phi + s^2 \deg \psi & (253) \\ &+ rs[\deg(\phi + \psi) - \deg \phi - \deg \psi]. \end{aligned}$$

## Proof.

Let  $n \geq 2$  be not divisible by  $\text{char}(\mathbb{K})$ . Represent  $\phi$  and  $\psi$  by transformation matrices  $\phi^{(n)}$  and  $\psi^{(n)}$  w.r.t. some basis of  $\mathcal{E}[n]$ . Then the transformation matrix  $r\phi^{(n)} + s\psi^{(n)}$  describes the action of  $r\phi + s\psi$  on  $\mathcal{E}[n]$ .

By straightforward calculation,

$$\det(r\phi^{(n)} + s\psi^{(n)}) = r^2 \det \phi^{(n)} + s^2 \det \psi^{(n)} + rs \left[ \det(\phi^{(n)} + \psi^{(n)}) - \det \phi^{(n)} - \det \psi^{(n)} \right].$$

Thus by (251),

$$\begin{aligned} \deg(r\phi + s\psi) &\equiv r^2 \deg \phi + s^2 \deg \psi + \\ &\quad rs[\deg(\phi + \psi) - \deg \phi - \deg \psi] \pmod{n}. \end{aligned}$$

Since this holds for infinitely many  $n$ , it must be an equality (see (254)). □

## Residue Class Computation

Let  $a, b$  be integers. If

$$a \equiv b \pmod{n} \tag{254}$$

holds for infinitely many moduli  $n \geq 2$ , then  $a = b$ .

### Proof.

We have that  $n$  divides  $a - b$  for infinitely many  $n$ .

Consider the unique factorization of  $a - b$  into prime powers,

$$a - b = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

Then the number of divisors of  $a - b$  is  $n_1 n_2 \cdots n_r$  and so  $a - b = 0$ , i.e.,  $a = b$ . □

## Divisors

K.-H.  
Zimmermann

Contents

Endomorphisms

Frobenius Map

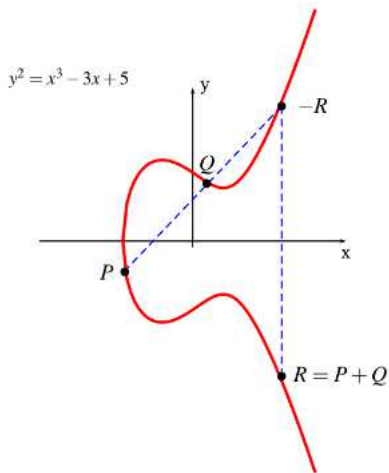
Torsion Subgroup

Division  
Polynomials

Weil Pairing

\* Divisors

Using Singular



## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$ .

- For each point  $P \in \mathcal{E}(\bar{\mathbb{K}})$  define the formal symbol  $[P]$ .
- A *divisor*  $D$  on  $\mathcal{E}$  is a finite linear combination of such symbols with integer coefficients; i.e.,

$$D = \sum_{\substack{i \\ \text{finite}}} a_i [P_i], \quad a_i \in \mathbb{Z}. \quad (255)$$

- The set of all divisors on  $\mathcal{E}$  forms a free abelian group generated by the symbols  $[P]$ , written  $\text{Div}(\mathcal{E})$ .

Definition of Weil pairing makes use of divisors.

## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$ .

- The *degree* of a divisor  $D$  is

$$\deg(D) = \deg \left( \sum_i a_i [P_i] \right) = \sum_i a_i \in \mathbb{Z}. \quad (256)$$

- The *sum* of a divisor  $D$  is

$$\text{sum}(D) = \text{sum} \left( \sum_i a_i [P_i] \right) = \sum_i a_i P_i \in \mathcal{E}(\bar{\mathbb{K}}). \quad (257)$$

## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$ .

- The mapping  $\deg : \text{Div}(\mathcal{E}) \rightarrow \mathbb{Z}$  is a surjective homomorphism with kernel

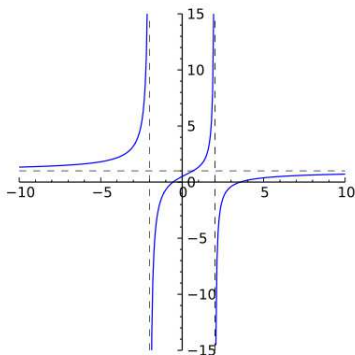
$$\text{Div}^0(\mathcal{E}) = \{D \in \text{Div}(\mathcal{E}) \mid \deg(D) = 0\}. \quad (258)$$

$\text{Div}^0(\mathcal{E})$  is a subgroup of  $\text{Div}(\mathcal{E})$ .

- The mapping  $\text{sum} : \text{Div}(\mathcal{E}) \rightarrow \mathcal{E}(\overline{\mathbb{K}})$  is a surjective homomorphism.

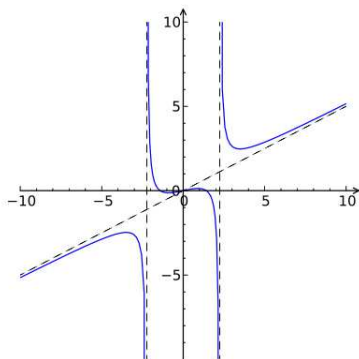
## Rational Functions

The rational function  $f(X) = \frac{X^2 - 3X - 2}{X^2 - 4}$  of degree 2 has zeros  $\frac{3}{2} \pm \frac{1}{2}\sqrt{17}$  and poles  $\pm 2$ . It is asymptotic to 1 as  $x$  approaches infinity.



## Rational Functions

The rational function  $f(X) = \frac{X^3 - 2X}{2(X^2 - 5)}$  of degree 3 has zeros  $0, \pm\sqrt{2}$  and poles  $\pm\sqrt{5}$ . It is asymptotic to  $\frac{x}{2}$  as  $x$  approaches infinity.



## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$ .

- A *function* on  $\mathcal{E}$  is a rational function

$$f(X, Y) = \frac{r(X, Y)}{s(X, Y)} \in \bar{\mathbb{K}}(X, Y) \quad (259)$$

which is defined for at least one point  $P \in \mathcal{E}(\bar{\mathbb{K}})$ .

- The rational function  $f(X, Y)$  has values in  $\bar{\mathbb{K}} \cup \{\infty\}$ .
- If  $\mathcal{E}$  is defined by  $Y^2 = X^3 + AX + B$ , the function  $1/(Y^2 - X^3 - AX - B)$  is not allowed.

## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$  and  $P \in \mathcal{E}(\bar{\mathbb{K}})$ .

- A function  $f$  has a *zero* at  $P$  if  $f(P) = 0$ .
- A function  $f$  has a *pole* at  $P$  if  $f(P) = \infty$ .
- There exists a function  $u_P$  on  $\mathcal{E}$ , called *uniformizer* at  $P$ , with  $u_P(P) = 0$  and such that each function  $f$  on  $\mathcal{E}$  with  $f(P) = 0$  has the form

$$f = u_P^r g, \quad (260)$$

where  $r \in \mathbb{Z}$  and  $g(P) \neq 0, \infty$ .

- The *order* of the function  $f$  at  $P$  is

$$\text{ord}_P(f) = r. \quad (261)$$

This number is independent of the choice of the uniformizer at  $P$ .

## Divisors – Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  given by  $Y^2 = X^3 - X$ .

- The function  $u_P = Y$  is a uniformizer at  $P = (0 : 0 : 1)$ .
- We have

$$X = Y^2 \frac{1}{X^2 - 1}$$

and  $X^2 - 1$  is nonzero and finite at  $P$ . Thus

$$\text{ord}_P(X) = 2 \quad \text{and} \quad \text{ord}_P(X/Y) = 1.$$

## Divisors

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  given by  $Y^2 = X^3 + AX + B$ .

- For each affine point  $P = (a : b : 1) \in \mathcal{E}(\bar{\mathbb{K}})$ , a uniformizer at  $P$  is

$$u_P = \begin{cases} X - a & \text{if } b \neq 0, \\ Y & \text{otherwise.} \end{cases}$$

- For the base point  $O = (0 : 1 : 0)$ , a uniformizer at  $O$  is

$$u_O = \frac{X}{Y}.$$

## Divisors – Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  given by  $Y^2 = X^3 + 72$ .

- For the point  $P = (-2 : 8 : 1) \in \mathcal{E}$ , a uniformizer is  $u_P = X + 2$ .
- The function  $f(X, Y) = X + Y - 6$  vanishes at  $P$  (but at what order?).

For this, rewrite the equation of the curve as

$$(Y + 8)(Y - 8) = (X + 2)^3 - 6(X + 2)^2 + 12(X + 2).$$

Then

$$\begin{aligned} f(X, Y) &= (X + 2) + (Y - 8) \\ &= u_P \cdot \left( 1 + \frac{(X + 2)^2 - 6(X + 2) + 12}{Y + 8} \right). \end{aligned}$$

The function in parenthesis is finite and does not vanish at  $P$ , so  $\text{ord}_P(f) = 1$ .

## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$  and  $f \neq 0$  be a function on  $\mathcal{E}$ .

- The *divisor* of  $f$  is defined as

$$\operatorname{div}(f) = \sum_{P \in \mathcal{E}(\mathbb{K})} \operatorname{ord}_P(f)[P] \in \operatorname{Div}(\mathcal{E}), \quad (262)$$

called the *principal divisor* of  $f$ .

- $f$  has only finitely many zeros and poles; this shows the well-definedness of  $\operatorname{div}(f)$ .
- $f$  has as many zeros as poles when counted with multiplicities, i.e.,

$$\deg(\operatorname{div}(f)) = 0. \quad (263)$$

- If  $f$  has no zeros or poles, then  $f$  is a constant and so  $\operatorname{div}(f) = 0$ .

(See Washington, section 11.1)

## Divisors – Example

Consider an elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$ .

- Suppose  $P_1, P_2, P_3$  are three collinear points on  $\mathcal{E}$ .
- There exists a homogeneous linear polynomial

$$\ell = \alpha X + \beta Y + \gamma Z$$

with zeros  $P_1, P_2, P_3$ .

- If  $\beta \neq 0$ , then  $\ell$  has the triple pole at  $O$  with

$$\operatorname{div}(\ell) = [P_1] + [P_2] + [P_3] - 3[O].$$

## Divisors – Example (cont'd)

- The line through  $P_3 = (a_3 : b_3 : 1)$  and  $-P_3 = (a_3 : -b_3 : 1)$  is  $X - a_3$  with divisor

$$\operatorname{div}(X - a_3) = [P_3] + [-P_3] - 2[O].$$

Thus

$$\begin{aligned} \operatorname{div}\left(\frac{\alpha X + \beta Y + \gamma Z}{X - a_3}\right) &= \operatorname{div}(\alpha X + \beta Y + \gamma Z) - \operatorname{div}(X - a_3) \\ &= [P_1] + [P_2] - [-P_3] - [O]. \end{aligned}$$

- Since  $P_1 + P_2 = -P_3$  on  $\mathcal{E}$ , we obtain

$$[P_1] + [P_2] = [P_1 + P_2] + [O] + \operatorname{div}\left(\frac{\alpha X + \beta Y + \gamma Z}{X - a_3}\right).$$

## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$  and  $D$  be a divisor on  $\mathcal{E}$  with  $\deg(D) = 0$ .

There exists a function  $f$  on  $\mathcal{E}$  such that

$$\operatorname{div}(f) = D \iff \operatorname{sum}(D) = O. \quad (264)$$

The proof provides an algorithm that finds to a divisor  $D$  (with  $\deg(D) = 0$  and  $\operatorname{sum}(D) = O$ ) a function  $f$  on  $\mathcal{E}$  with  $\operatorname{div}(f) = D$ .

## Proof.

- The above example shows that

$$[P_1] + [P_2] = [P_1 + P_2] + [O] + \text{div}(g)$$

for some function  $g$  on  $\mathcal{E}$ . Moreover,

$$\text{sum}(\text{div}(g)) = P_1 + P_2 - (P_1 + P_2) - O = O.$$

- In particular, if  $P_1 + P_2 = O$ , then

$$[P_1] + [P_2] = 2[O] + \text{div}(g)$$

for some function  $g$  on  $\mathcal{E}$ . Moreover,

$$\text{sum}(\text{div}(g)) = P_1 + P_2 - 2O = O.$$

## Proof (cont'd).

- Therefore, the sum of all terms in  $D$  with positive coefficients equals a single symbol  $[P]$  plus a multiple of  $[O]$  plus a divisor of a function. A similar result holds for the sum of the terms with negative coefficients.
- Thus there are points  $P$  and  $Q$  on  $\mathcal{E}$ , a function  $h$  on  $\mathcal{E}$ , and an integer  $n$  such that

$$D = [P] - [Q] + n[O] + \operatorname{div}(h).$$

- Since  $h$  is the product of functions  $g$  with  $\operatorname{sum}(\operatorname{div}(g)) = O$ , it follows that

$$\operatorname{sum}(\operatorname{div}(h)) = O.$$

- By (263),  $\operatorname{deg}(\operatorname{div}(h)) = 0$  and so by hypothesis

$$0 = \operatorname{deg}(D) = 1 - 1 + n + 0 = n.$$

## Proof (cont'd).

- Thus

$$D = [P] - [Q] + \operatorname{div}(h)$$

and

$$\operatorname{sum}(D) = P - Q + \operatorname{sum}(\operatorname{div}(h)) = P - Q.$$

Proof:

- Let  $\operatorname{sum}(D) = O$ . Then  $P - Q = O$  and so  $D = \operatorname{div}(h)$ .
- Let  $D = \operatorname{div}(f)$  for some function  $f$  on  $\mathcal{E}$ . Then

$$[P] - [Q] = \operatorname{div}\left(\frac{f}{h}\right).$$

The next result will show that  $P = Q$  and so  $\operatorname{sum}(D) = O$ .  $\square$

## Divisors

Let  $P, Q \in \mathcal{E}(\bar{\mathbb{K}})$ . If there exists a function  $h$  on  $\mathcal{E}$  with

$$\operatorname{div}(h) = [P] - [Q],$$

then  $P = Q$ .

(See Washington, Lemma 11.3)

## Divisors – Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{Z}_{11}$  given by  $Y^2 = X^3 + 4X$ .  
Take the divisor

$$D = [(0, 0)] + [(2, 4)] + [(4, 5)] + [(6, 3)] - 4[O].$$

We have

$$\deg(D) = 0 \quad \text{and} \quad \text{sum}(D) = O.$$

Find a function  $f$  on  $\mathcal{E}$  with  $\text{div}(f) = D$ .

## Divisors – Example (cont'd)

- 1 The line through  $(0, 0)$  and  $(2, 4)$  is  $Y = 2X$  which is tangent at  $(2, 4)$ , so

$$\operatorname{div}(Y - 2X) = [(0, 0)] + 2[(2, 4)] - 3[O].$$

The vertical line through  $(2, 4)$  is  $X = 2$  and so

$$\operatorname{div}(X - 2) = [(2, 4)] + [(2, -4)] - 2[O].$$

Thus

$$D = [(2, -4)] + \operatorname{div}\left(\frac{Y - 2X}{X - 2}\right) + [(4, 5)] + [(6, 3)] - 3[O].$$

## Divisors – Example (cont'd)

- 2 The line through  $(4, 5)$  and  $(6, 3)$  is  $Y = -X - 2$  with third point  $(2, -4)$ , so

$$\operatorname{div}(Y + X + 2) = [(4, 5)] + [(6, 3)] + [(2, -4)] - 3[O].$$

The vertical line through  $(2, -4)$  is  $X = 2$  and so

$$\operatorname{div}(X - 2) = [(2, -4)] + [(2, 4)] - 2[O].$$

Thus

$$[(4, 5)] + [(6, 3)] = [(2, 4)] + [O] + \operatorname{div}\left(\frac{Y + X + 2}{X - 2}\right).$$

## Divisors – Example (cont'd)

Thus the divisor is

$$\begin{aligned}
 D &= [(2, -4)] + \operatorname{div}\left(\frac{Y - 2X}{X - 2}\right) + [(2, 4)] + \operatorname{div}\left(\frac{Y + X + 2}{X - 2}\right) - 2[O] \\
 &= \operatorname{div}(X - 2) + \operatorname{div}\left(\frac{Y - 2X}{X - 2}\right) + \operatorname{div}\left(\frac{Y + X + 2}{X - 2}\right) \\
 &= \operatorname{div}\left(\frac{(Y - 2X)(Y + X + 2)}{X - 2}\right).
 \end{aligned}$$

Simplification using  $Y^2 = X^3 + 4X$  gives

$$\begin{aligned}
 (Y - 2X)(Y + X + 2) &= Y^2 - XY - 2X^2 + 2Y - 4X \\
 &= X^3 - XY - 2X^2 + 2Y \\
 &= (X - 2)(X^2 - Y)
 \end{aligned}$$

and so

$$D = \operatorname{div}(X^2 - Y).$$

## Divisors

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{K}$ .

- The mapping  $\text{sum} : \text{Div}^0(\mathcal{E}) \rightarrow \mathcal{E}(\bar{\mathbb{K}})$  is a surjective homomorphism.

Indeed, for any point  $P \in \mathcal{E}(\bar{\mathbb{K}})$ ,  $\deg([P] - [O]) = 0$  and  $\text{sum}([P] - [O]) = P - O = P$ .

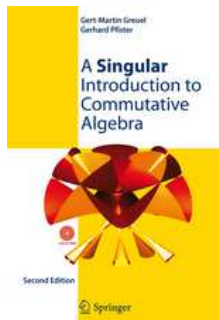
- By (264), the kernel is given by the subgroup of principal divisors  $P_0(\mathcal{E})$  of  $\mathcal{E}$ .
- By the homomorphism theorem, the induced mapping

$$\text{Div}^0(\mathcal{E})/P_0(\mathcal{E}) \rightarrow \mathcal{E}(\bar{\mathbb{K}}) : D + P_0(\mathcal{E}) \mapsto \text{sum}(D)$$

is an isomorphism of groups.

- The group law on  $\mathcal{E}(\bar{\mathbb{K}})$  corresponds to the group law on  $\text{Div}^0(\mathcal{E})$  modulo the principal divisors.

## Elliptic Curves in Singular



Contents

Endomorphisms

Frobenius Map

Torsion Subgroup

Division  
Polynomials

Weil Pairing

\* Divisors

Using Singular

## Generation of Random Elliptic Curve

Generation of random elliptic curve over ring  $\mathbb{Z}_N$ .

```
> LIB "crypto.lib";
> ring r = 0,z,dp;
> ellipticRandomCurve(11); // N=11
[1]:
    5                               // a
[2]:
    8                               // b
[3]:
    1                               // discriminant
```

Returned is a list of two random numbers  $a, b$  and  $\Delta = 4a^3 + 27b^2 \pmod N$ .

The curve is given by the equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

## Test for Point Membership

Test whether a point lies on a curve:

```
> isOnCurve(11, 5, 8, list(0,1,0));  
1 // on curve  
> isOnCurve(11, 5, 8, list(5,5,1));  
0 // not on curve
```

## Generation of Random Point

Generate a random point on an elliptic curve:

```
> ellipticRandomPoint(11, 5, 8);  
[1]:  
    6  
[2]:  
    1  
[3]:  
    1
```

## Number of Points

Provide the number of points on a curve:

```
> countPoints(11, 5, 8);  
15
```

## List of Points

List of all points on an elliptic curve:

```
> list L = ellipticAllPoints(11, 5, 8);  
> size(L);  
15  
> L[1];  
[1]:  
  0  
[2]:  
  1  
[3]:  
  0
```

## Point Addition

Addition of two points on an elliptic curve:

```
> list P,Q;
> P[1]=1;
> P[2]=5;
> P[3]=1;
> Q[1]=1;
> Q[2]=6;
> Q[3]=1;
> ellipticAdd(11, 5, 8, P, Q); // P+Q
[1]:
  0
[2]:
  1
[3]:
  0
```

## Point Multiple

Multiple of a point on an elliptic curve:

```
> list P;  
> P[1]=1;  
> P[2]=5;  
> P[3]=1;  
> ellipticMult(11, 5, 8, P, 6); // 6*P  
[1]:  
    6  
[2]:  
    1  
[3]:  
    1
```

## Point Addition

The elliptic curve  $\mathcal{E}$  over  $\mathbb{Z}_7$  given by

$$f = Y^2Z - X^3 - 3XZ^2 - 5Z^3$$

has the points

$$\begin{aligned} P_1 = O &= [0 : 1 : 0], & P_2 &= [1 : 4 : 1], & P_3 &= [1 : 3 : 1], \\ P_4 &= [4 : 2 : 1], & P_5 &= [4 : 5 : 1], \\ P_6 &= [6 : 1 : 1], & P_7 &= [6 : 6 : 1]. \end{aligned}$$

Addition table:

+	$O$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$
$O$	$O$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$
$P_2$		$P_6$	$O$	$P_5$	$P_7$	$P_4$	$P_3$
$P_3$			$P_7$	$P_6$	$P_4$	$P_2$	$P_5$
$P_4$				$P_3$	$O$	$P_7$	$P_2$
$P_5$					$P_2$	$P_3$	$P_6$
$P_6$						$P_5$	$O$
$P_7$							$P_4$

## Division Polynomials

```

> LIB "crypto.lib";
> ring r = 0, (y,x), dp;
> ellipticRandomCurve(11);
[1]:
    4
[2]:
    9
[3]:
    1
> generateG(4,9,2);
2y
> generateG(4,9,3);
3x4+24x2+108x-16

```

# Part VI

## Elliptic Curves over Finite Fields

## Elliptic Curves over Finite Fields

- Group structure
- Frobenius endomorphism
- Bounds on group order
- Group order
- \*Zeta function
- Supersingular curves
- \*Schoof's algorithm

### Contents

Group Structure

Frobenius  
Endomorphism

Bounds on Group  
Order

Group Order

Zeta Function

Supersingular  
Curves

\*Schoof's  
Algorithm

## Group Structure



Niels Henrik Abel (1802-1829)

## Group Structure

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . Then

$$\mathcal{E}(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad \text{or} \quad \mathcal{E}(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer  $n \geq 1$  or some integers  $n_1, n_2 \geq 1$  with  $n_1 \mid n_2$ .

## Proof.

- Each finite abelian group is isomorphic to a direct sum of cyclic groups

$$\mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k},$$

where  $n_1, \dots, n_k$  are integers with  $n_i \mid n_{i+1}$  for all  $i$ .

- Since  $\mathbb{Z}_{n_i}$  has  $n_i$  elements of order dividing  $n_i$ ,  $\mathcal{E}(\mathbb{F}_q)$  has  $n_1^k$  elements of order dividing  $n_1$ .
- By the result on  $\mathcal{E}[n_1]$  in (214) and (215) there are at most  $n_1^2$  such points and so  $k \leq 2$ .
- Thus  $\mathcal{E}(\mathbb{F}_q)$  is isomorphic to  $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$  with  $n_1 \mid n_2$  or by (219) isomorphic to  $\mathbb{Z}_n$ .



## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_5$  given by  $Y^2 = X^3 + X + 1$ .

The affine  $\mathbb{F}_5$ -rational points are

$x$	$x^3 + x + 1$	$y$	Points
0	1	$\pm 1$	$(0 : 1 : 1), (0 : 4 : 1)$
1	3		
2	1	$\pm 1$	$(2 : 1 : 1), (2 : 4 : 1)$
3	1	$\pm 1$	$(3 : 1 : 1), (3 : 4 : 1)$
4	4	$\pm 2$	$(4 : 2 : 1), (4 : 3 : 1)$

Note that the squares modulo 5 are 1 and 4, since  $1^2 = 1$ ,  $2^2 = 4$ ,  $3^2 = 4$ , and  $4^2 = 1$ , but 3 is not a square modulo 5.

Together with the base point  $O$ ,  $\mathcal{E}(\mathbb{F}_5)$  has order 9.

The group  $\mathcal{E}(\mathbb{F}_5)$  is cyclic with generator  $P = (0 : 1 : 1)$ , i.e.,  $\mathcal{E}(\mathbb{F}_5) \simeq \mathbb{Z}_9$ .

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_7$  given by  $Y^2 = X^3 + 2$ .

The  $\mathbb{F}_7$ -rational points are

$$\begin{aligned} & (0 : 1 : 0), \quad (0 : 3 : 1), \quad (0 : 4 : 1), \\ & (3 : 1 : 1), \quad (3 : 6 : 1), \quad (5 : 1 : 1), \\ & (5 : 6 : 1), \quad (6 : 1 : 1), \quad (6 : 6 : 1). \end{aligned}$$

All points  $P$  satisfy  $3P = O$ . Thus  $\mathcal{E}(\mathbb{F}_7) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$ .

Check via Singular:

```
> LIB "crypto.lib";
> countPoints(7,0,2);
> list L = ellipticAllPoints(7,0,2);
> ellipticMult(7,0,2,L[2],3);
```

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_2$  given by  $Y^2 + XY = X^3 + 1$ .

The  $\mathbb{F}_2$ -rational points are

$$(0 : 1 : 0), (1 : 0 : 1), (0 : 1 : 1), (1 : 1 : 1).$$

The group  $\mathcal{E}(\mathbb{F}_2)$  is cyclic of order 4, i.e.,  $\mathcal{E}(\mathbb{F}_2) \simeq \mathbb{Z}_4$ .

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_4$  given by  $Y^2 + XY = X^3 + 1$ .

Write  $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$  with  $\alpha^2 + \alpha + 1 = 0$ .

The  $\mathbb{F}_4$ -rational points are

$$\begin{array}{cccc} (0 : 1 : 0), & (0 : 1 : 1), & (1 : 0 : 1), & (1 : 1 : 1), \\ (\alpha : 0 : 1), & (\alpha : \alpha : 1), & (\alpha^2 : 0 : 1), & (\alpha^2 : \alpha^2 : 1). \end{array}$$

The group  $\mathcal{E}(\mathbb{F}_4)$  is cyclic of order 8, i.e.,  $\mathcal{E}(\mathbb{F}_4) \simeq \mathbb{Z}_8$ .

## Frobenius Endomorphism



Evariste Galois (1811-1832)

## Frobenius Endomorphism

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ .

Recall that the mapping  $\phi_q : \mathcal{E}(\overline{\mathbb{F}}_q) \rightarrow \mathcal{E}(\overline{\mathbb{F}}_q)$  given by

$$(a : b : c) \mapsto (a^q : b^q : c^q) \quad (265)$$

is a nonseparable endomorphism of degree  $q$ , called *Frobenius endomorphism*.

## Frobenius Endomorphism

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$  and let  $(x, y) \in \mathcal{E}(\bar{\mathbb{F}}_q)$ . Then

$$\phi_q(x, y) \stackrel{\text{def}}{=} (x^q, y^q) \in \mathcal{E}(\bar{\mathbb{F}}_q) \quad (266)$$

and

$$(x, y) \in \mathcal{E}(\mathbb{F}_q) \iff \phi_q(x, y) = (x, y). \quad (267)$$

**Proof.**

- Suppose the affine point  $(x, y)$  satisfies the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Applying the Frobenius map  $z \mapsto z^q$  gives

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6,$$

since  $a_1, a_2, a_3, a_5, a_6 \in \mathbb{F}_q$ . Thus  $(x^q, y^q) \in \mathcal{E}(\bar{\mathbb{F}}_q)$ .

## Proof (cont'd).

- We have

$$\begin{aligned}
 (x, y) \in \mathcal{E}(\mathbb{F}_q) &\iff (x, y) \in \mathcal{E}(\overline{\mathbb{F}}_q) \wedge x, y \in \mathbb{F}_q \\
 &\iff (x, y) \in \mathcal{E}(\overline{\mathbb{F}}_q) \wedge x^q = x, y^q = y \\
 &\iff \phi_q(x, y) \stackrel{\text{def}}{=} (x^q, y^q) = (x, y).
 \end{aligned}$$



## Frobenius Endomorphism

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ , and let  $n \geq 1$ .

The  $n$ th iterate of the Frobenius endomorphism

$$\phi_q^n : \mathcal{E}(\mathbb{F}_q) \rightarrow \mathcal{E}(\mathbb{F}_q) \quad (268)$$

is given by

$$\phi_q^n(a : b : c) = (a^{q^n} : b^{q^n} : c^{q^n}). \quad (269)$$

It is a nonseparable endomorphism of degree  $q^n$ .

## Proof.

- The Frobenius endomorphism  $\phi_q(X, Y) = (X^q, Y^q)$  is an endomorphism.
- The iterate  $\phi_{q^n}$  is also an endomorphism, by iteration of the proof of the Frobenius endomorphism.
- The iterate  $\phi_q^n(X, Y) = (X^{q^n}, Y^{q^n})$  has degree  $q^n$  and is nonseparable, since the derivative of  $r(X) = X^{q^n}$  is  $r'(X) = q^n X^{q^n-1} = 0$ .



## Frobenius Endomorphism

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ ,  $q = p^r$  with  $p$  prime and  $r \geq 1$ , and let  $n \geq 1$ . Then

$$\ker(\phi_q^n - [1]) = \mathcal{E}(\mathbb{F}_{q^n}) \quad (270)$$

and  $\phi_q^n - [1]$  is a separable endomorphism, so

$$\#\mathcal{E}(\mathbb{F}_{q^n}) = \deg(\phi_q^n - [1]). \quad (271)$$

Note that for each  $P \in \mathbb{P}^2(\bar{\mathbb{F}}_q)$ ,

$$(\phi_q^n - [1])(P) = \phi_q^n(P) - P, \quad (272)$$

where  $[1]$  is the identity mapping.

## Proof.

- Let  $(x, y) \in \mathcal{E}(\overline{\mathbb{F}}_{q^n})$ . Then by (267),

$$(x, y) \in \mathcal{E}(\mathbb{F}_{q^n}) \iff \phi_q^n(x, y) = (x, y)$$

and by (272),

$$\phi_q^n(x, y) = (x, y) \iff (x, y) \in \ker(\phi_q^n - [1]).$$

- By (210), the endomorphism  $\phi_q^n + [-1]$  is separable, since  $p \nmid -1$ . Thus by (270) and (190),

$$\#\mathcal{E}(\mathbb{F}_{q^n}) = \#\ker(\phi_q^n - [1]) = \deg(\phi_q^n - [1]).$$



## Bounds on Group Order



Helmut Hasse (1898-1979)

## Bound on Group Order

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . Then

$$\#\mathcal{E}(\mathbb{F}_q) \leq 2q + 1. \quad (273)$$

### Proof.

- The curve contains the base point  $O$  which is the only point on the curve not in affine space  $\mathbb{A}^2(\mathbb{F}_q)$ .
- For the remaining points it is sufficient to consider the affine Weierstrass equation  $f^a(X, Y) = 0$  over  $\mathbb{F}_q$ .
- Since the equation  $f^a(X, Y) = 0$  is quadratic in  $Y$ , for each  $X = x \in \mathbb{F}_q$  there are at most two solutions  $Y = \pm y \in \mathbb{F}_q$ . So there are at most  $2q$  affine points on the curve.



## The Famous Hasse Bound

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . Then

$$|q + 1 - \#\mathcal{E}(\mathbb{F}_q)| \leq 2\sqrt{q}. \quad (274)$$

### Proof.

By (271), we have

$$t \stackrel{\text{def}}{=} q + 1 - \#\mathcal{E}(\mathbb{F}_q) = q + 1 - \deg(\phi_q - [1]). \quad (275)$$

## Proof (cont'd).

- For integers  $r, s$  with  $(s, q) = 1$ , we have

$$\deg([r]\phi_q - [s]) = r^2q + s^2 - rst. \quad (276)$$

Indeed, by (253),

$$\begin{aligned} \deg(r\phi_q + s[-1]) &= r^2 \deg \phi_q + s^2 \deg[-1] + \\ &\quad rs\{\deg(\phi_q + [-1]) - \deg \phi_q - \deg[-1]\}. \end{aligned}$$

Since  $\deg \phi_q = q$  and  $\deg[-1] = 1$ , by (275),

$$\begin{aligned} &rs\{\deg(\phi_q + [-1]) - \deg \phi_q - \deg[-1]\} \\ &= rs(\deg(\phi_q + [-1]) - q - 1) = -rst. \end{aligned}$$

## Proof (cont'd).

- Since  $\deg([r]\phi_q - [s]) \geq 0$ , the multiplication of (276) with  $1/s^2$  gives

$$q \left(\frac{r}{s}\right)^2 - t \left(\frac{r}{s}\right) + 1 \geq 0 \quad (277)$$

for all  $r, s$  with  $(s, q) = 1$ .

- The set of rational numbers  $r/s$  with  $(s, q) = 1$  is dense in  $\mathbb{R}$ . Indeed, the rational numbers of the form  $r/2^m$  or  $r/3^m$  (choose according to  $q$ ) are dense in  $\mathbb{R}$ .
- By a limiting process in (277),

$$qx^2 - tx + 1 \geq 0$$

for all real numbers  $x$ . Thus the discriminant  $\Delta$  of the polynomial  $qX^2 - tX + 1$  is  $\leq 0$ , i.e.,  $\Delta = t^2 - 4q \leq 0$ . Hence,  $|t| \leq 2\sqrt{q}$ .



## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_4$  given by  $Y^2 = X^3 - Y$ .

Write  $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$  with  $\alpha^2 + \alpha + 1 = 0$ .

The  $\mathbb{F}_4$ -rational points are

$$\begin{array}{lll} (0 : 1 : 0), & (0 : 0 : 1), & (0 : 1 : 1), \\ (1 : \alpha : 1), & (1 : \alpha^2 : 1), & (\alpha : \alpha : 1), \\ (\alpha : \alpha^2 : 1), & (\alpha^2 : \alpha : 1), & (\alpha^2 : \alpha^2 : 1). \end{array}$$

Thus  $\#\mathcal{E}(\mathbb{F}_4) = 9$  and so

$$|4 + 1 - 9| = 4 = 2\sqrt{4}.$$

Hence, the Hasse bound (274) is attained with equality!

## Frobenius Trace

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$  and let

$$t = q + 1 - \#\mathcal{E}(\mathbb{F}_q). \quad (278)$$

Then

$$\phi_q^2 - [t]\phi_q + [q] = 0 \quad (279)$$

is an endomorphism of  $\mathcal{E}$  and  $t$  is the unique integer such that this equality holds.

By (279), for each  $(x : y : 1) \in \mathcal{E}(\bar{\mathbb{F}}_q)$ ,

$$\left(x^{q^2} : y^{q^2} : 1\right) - t(x^q : y^q : 1) + q(x : y : 1) = O. \quad (280)$$

## Proof.

If the endomorphism  $\psi = \phi_q^2 - [t]\phi_q + [q]$  is not 0, its kernel is finite as  $\deg \psi$  is finite and by (190,191)  $\deg \psi \geq \#\ker(\psi)$ . We show that the kernel is infinite and so  $\psi = 0$ .

- Let  $m \geq 1$  with  $(m, q) = 1$ . The endomorphism  $\phi_q$  induces a transformation matrix  $\phi_q^{(m)}$  describing the action of  $\phi_q$  on  $\mathcal{E}[m]$  as in (223). Write

$$\phi_q^{(m)} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

- Since  $\phi_q - [1]$  is separable by (210), we obtain

$$\begin{aligned} \#\ker(\phi_q - [1]) &= \deg(\phi_q - [1]) \text{ by (190),} \\ &\equiv \det\left(\phi_q^{(m)} - I\right) \text{ by (251),} \\ &= ad - bc - (a + d) + 1 \pmod{m}. \end{aligned}$$

## Proof (cont'd)

- By (251),  $ad - bc = \det(\phi_q^{(m)}) \equiv \deg(\phi_q) = q \pmod{m}$ .
- By (270, 271, 278),  $\#\ker(\phi_q - [1]) = \#\mathcal{E}(\mathbb{F}_q) = q + 1 - t$  and so by the last three identities,

$$\text{trace}(\phi_q^{(m)}) = a + d \equiv t \pmod{m}.$$

- By the Cayley-Hamilton theorem of linear algebra,

$$A^2 - \text{trace}(A)A + \det(A)I = 0$$

for any  $2 \times 2$  matrix  $A$  and so for  $A = \phi_q^{(m)}$ ,

$$\left(\phi_q^{(m)}\right)^2 - t\phi_q^{(m)} + qI \equiv 0 \pmod{m}.$$

Thus the endomorphism  $\psi = \phi_q^2 - [t]\phi_q + [q]$  is identically zero on  $\mathcal{E}[m]$ . Since there are infinitely many choices for  $m$ , the kernel of  $\psi$  is infinite as claimed.

## Proof (cont'd)

- Let  $t, t'$  be distinct integers with

$$\phi_q^2 - [t]\phi_q + [q] = 0 \quad \text{and} \quad \phi_q^2 - [t']\phi_q + [q] = 0.$$

Then

$$[t - t']\phi_q = (\phi_q^2 - [t']\phi_q + [q]) - (\phi_q^2 - [t]\phi_q + [q]) = 0.$$

Since  $\phi_q : \mathcal{E}(\bar{\mathbb{F}}_q) \rightarrow \mathcal{E}(\bar{\mathbb{F}}_q)$  is surjective, the endomorphism  $[t - t']$  annihilates  $\mathcal{E}(\bar{\mathbb{F}}_q)$  and thus also  $\mathcal{E}[m]$  for each  $m \geq 1$ .

If  $(m, q) = 1$ , then by (214),  $\mathcal{E}[m]$  has points  $P$  of order  $m$ . For such a point  $P$ ,  $[t - t'](P) = (t - t')P = O$  and so  $t - t'$  is multiple of  $m$ , i.e.,  $t - t' \equiv 0 \pmod{m}$ . Since there are infinitely many such  $m$ ,  $t - t' = 0$  and so  $t$  is unique (see (254)). □

## Frobenius Trace

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$  and let  $t = q + 1 - \#\mathcal{E}(\mathbb{F}_q)$ .

Let  $m \geq 1$  with  $(m, q) = 1$  and let  $\phi_q^{(m)}$  be the transformation matrix describing the action of  $\phi_q$  on  $\mathcal{E}[m]$ .

Then

$$\text{trace} \left( \phi_q^{(m)} \right) \equiv t \pmod{m} \quad (281)$$

and

$$\det \left( \phi_q^{(m)} \right) \equiv q \pmod{m}. \quad (282)$$

See former proof.

The number  $t$  is the *Frobenius trace* of  $\phi_q$  and  $X^2 - tX + q$  is the *characteristic polynomial of Frobenius*.

## Group Order



Carl Jacobi (1804-1851)

Contents

Group Structure

Frobenius  
Endomorphism

Bounds on Group  
Order

**Group Order**

Zeta Function

Supersingular  
Curves

\* Schoof's  
Algorithm

## Example (Maple)

Consider the algebraic curves  $\mathcal{E}$  over  $\mathbb{F}_{11}$  given by  $Y^2 = X^3 + AX + B$  with  $A, B \in \mathbb{F}_{11}^*$ .

The number of  $\mathbb{F}_{11}$ -rational points of  $\mathcal{E}$  depending on  $A, B$  were calculated by `countPoints`:

$A \setminus B$	1	2	3	4	5	6	7	8	9	10
1	14	16	7	9	11	13	15	17	8	10
2	16	9	13	6	10	14	18	11	15	8
3	7	13	8	14	9	15	10	16	11	17
4	9	17	14	11	8	16	13	10	7	15
5	11	10	9	8	7	17	16	15	14	13
6	13	14	15	16	6	18	8	9	10	11
7	15	18	10	13	16	8	11	14	6	9
8	6	11	16	10	15	9	14	8	13	18
9	8	15	11	7	14	10	17	13	9	16
10	10	8	6	15	13	11	9	18	16	14

The curves with the following parameters  $(A, B)$  are singular:  
 $(2, 3), (2, 8), (6, 1), (6, 10), (7, 4), (7, 7), (8, 2), (8, 9), (10, 5), (10, 6)$ .

## Group Order (Using Frobenius Trace)

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . Write

$$t = q + 1 - \#\mathcal{E}(\mathbb{F}_q) \quad (283)$$

and

$$X^2 - tX + q = (X - \alpha)(X - \beta) \quad (284)$$

over  $\mathbb{C}$ . Then for each  $n \geq 1$ ,

$$\#\mathcal{E}(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n). \quad (285)$$

Thus if  $\#\mathcal{E}(\mathbb{F}_q)$  is known, then  $\#\mathcal{E}(\mathbb{F}_{q^n})$  can be calculated.

## Group Order (Using Frobenius Trace)

For each  $n \geq 0$ , put

$$s_n = \alpha^n + \beta^n. \quad (286)$$

Then

$$s_0 = 2, \quad s_1 = t, \quad \text{and} \quad s_{n+1} = ts_n - qs_{n-1} \quad \text{for } n \geq 1. \quad (287)$$

**Proof.**

We have  $s_0 = \alpha^0 + \beta^0 = 2$  and  $s_1 = \alpha + \beta = t$  by comparing the coefficient of  $X$  in (284).

Let  $n \geq 2$ . Since  $\alpha$  is a zero of  $X^2 - tX + q$ , we have

$$\alpha^2 - t\alpha + q = 0.$$

Multiplying with  $\alpha^{n-1}$  gives

$$\alpha^{n+1} - t\alpha^n + q\alpha^{n-1} = 0.$$

## Proof (cont'd)

Similarly,

$$\beta^{n+1} - t\beta^n + q\beta^{n-1} = 0.$$

Adding both relations gives

$$(\alpha^{n+1} + \beta^{n+1}) - t(\alpha^n + \beta^n) + q(\alpha^{n-1} + \beta^{n-1}) = 0.$$

Thus by definition,

$$s_{n+1} - ts_n + qs_{n-1} = 0.$$



Since  $q, t$  are integers, the recurrence (287) shows that  $\alpha^n + \beta^n$  is an integer for all  $n \geq 0$ .

## Proof of Eq. (285).

Let

$$\begin{aligned} f(X) &= (X^n - \alpha^n)(X^n - \beta^n) \\ &= X^{2n} - (\alpha^n + \beta^n)X^n + q^n. \end{aligned}$$

The polynomial  $g(X) = X^2 - tX + q = (X - \alpha)(X - \beta)$  divides  $f(X)$ . This can be proved using Maple:

```
> f(X) := X^(2*n) - (a^n + b^n)*X + q^n;
> g(X) := X^2 - (a+b)*X + q;
> rem(f, g, X);
0
```

Since  $f(X), g(X)$  have integer coefficients and  $g(X)$  is monic, polynomial division yields a quotient polynomial  $h(X)$  with integer coefficients.

## Proof (cont'd).

- Substituting the Frobenius endomorphism  $X = \phi_q$  gives

$$\begin{aligned}
 (\phi_q^n)^2 - [\alpha^n + \beta^n]\phi_q^n + [q^n] &= f(\phi_q) & (288) \\
 &= h(\phi_q)(\phi_q^2 - [t]\phi_q + [q]) \\
 &= 0
 \end{aligned}$$

as endomorphisms, where  $\phi_q^n$  is the  $n$ th iterate of  $\phi_q$  and the last equation follows from (279).

- By (279), there is exactly one integer  $t$  with

$$(\phi_q^n)^2 - [t]\phi_{q^n} + [q^n] = 0,$$

which is determined by  $t = q^n + 1 - \#\mathcal{E}(\mathbb{F}_{q^n})$ . Thus by (288),

$$\alpha^n + \beta^n = q^n + 1 - \#\mathcal{E}(\mathbb{F}_{q^n}).$$

□

## Example

The elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_2$  given by  $Y^2 + XY = X^3 + 1$  has  $\#\mathcal{E}(\mathbb{F}_2) = 4$  points:

$$(0 : 1 : 0), (1 : 0 : 1), (0 : 1 : 1), (1 : 1 : 1).$$

Thus

$$t = q + 1 - \#\mathcal{E}(\mathbb{F}_2) = 2 + 1 - 4 = -1.$$

Consider the polynomial

$$X^2 - tX + q = X^2 + X + 2 = (X - \alpha)(X - \beta)$$

where

$$\alpha = \frac{-1 + \sqrt{-7}}{2} \quad \text{and} \quad \beta = \frac{-1 - \sqrt{-7}}{2}.$$

## Example (cont'd)

In view of the extension field  $\mathbb{F}_4$ , we obtain by (285)

$$\begin{aligned} \#\mathcal{E}(\mathbb{F}_4) &= q^2 + 1 - (\alpha^2 + \beta^2) \\ &= 4 + 1 - \left(\frac{-1 + \sqrt{-7}}{2}\right)^2 - \left(\frac{-1 - \sqrt{-7}}{2}\right)^2. \end{aligned}$$

Alternatively, use the recurrence

$$s_0 = q = 2, \quad s_1 = t = -1, \quad s_2 = ts_1 - qs_0 = -3$$

to obtain

$$\#\mathcal{E}(\mathbb{F}_4) = q^2 + 1 - s_2 = 4 + 1 - (-3) = 8.$$

## Example (cont'd)

Consider small extension fields of  $\mathbb{F}_2$ :

- Recurrence:  $s_0 = q = 2$ ,  $s_1 = t = -1$ , and for  $n \geq 2$ ,

$$s_n = ts_{n-1} - qs_{n-2} = -s_{n-1} - 2s_{n-2}.$$

- Define group order:  $N_n = \#\mathcal{E}(\mathbb{F}_{2^n}) = 2^n + 1 - s_n$ .

- Maple computation:

$n$	0	1	2	3	4	5	6	7	8	9	10
$s_n$	2	-1	-3	5	1	-11	9	13	-31	5	57

and

$n$	1	2	3	4	5	6	7	8	9	10
$N_n$	4	8	4	16	44	56	116	288	508	968

## Example (cont'd)

Let  $n = 101$ . Then by using Maple,

$$\begin{aligned} s_{101} &= \left( \frac{-1 + \sqrt{-7}}{2} \right)^{101} + \left( \frac{-1 - \sqrt{-7}}{2} \right)^{101} \\ &= 2.969292316 \cdot 10^{15} \end{aligned}$$

and so

$$\begin{aligned} \#\mathcal{E}(\mathbb{F}_{2^{101}}) &= 2^{101} + 1 - 2.969292316 \cdot 10^{15} \\ &= 2.535301200 \cdot 10^{30}. \end{aligned}$$

## Group Order (Using Hasse Bound)

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . By the Hasse bound (274),

$$q + 1 - 2\sqrt{q} \leq \#\mathcal{E}(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}. \quad (289)$$

The *order* of a point  $P \in \mathcal{E}(\mathbb{F}_q)$  is the smallest integer  $k \geq 1$  such that  $kP = O$ .

- By Lagrange, the point order divides the group order, since the point order of  $P$  is the order of the cyclic subgroup  $\langle P \rangle$  of  $\mathcal{E}(\mathbb{F}_q)$  generated by  $P$ .
- By (289), the group order  $\#\mathcal{E}(\mathbb{F}_q)$  lies within an interval of length  $4\sqrt{q}$ .
- *Group order criterion*: If there is a point  $P$  whose order  $M$  lies in the interval

$$q + 1 - 2\sqrt{q}, \dots, q + 1 + 2\sqrt{q} \quad (290)$$

and no other multiple of  $M$  lies in this interval, then  $\#\mathcal{E}(\mathbb{F}_q) = M$ .

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_{101}$  given by  $Y^2 = X^3 + 7X + 1$ .

- The point  $P = (0 : 1 : 1)$  has order 116, so  $\#\mathcal{E}(\mathbb{F}_{101})$  is a multiple of 116.
- By the Hasse bound (289),

$$101 + 1 - 2\sqrt{101} \leq \#\mathcal{E}(\mathbb{F}_{101}) \leq 101 + 1 + 2\sqrt{101},$$

i.e.,  $82 \leq \#\mathcal{E}(\mathbb{F}_{101}) \leq 122$ .

- The only multiple of 116 in this interval is 116 and so  $\#\mathcal{E}(\mathbb{F}_{101}) = 116$ .
- Since  $P$  has order 116, it follows that the group  $\mathcal{E}(\mathbb{F}_{101})$  is cyclic with generator  $P$ .

## Example

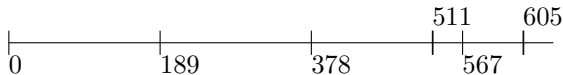
Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_{557}$  given by  $Y^2 = X^3 - 10X + 21$ .

- The point  $P = (2 : 3 : 1)$  has order 189, so  $\#\mathcal{E}(\mathbb{F}_{557})$  is a multiple of 189.
- By the Hasse bound (289),

$$557 + 1 - 2\sqrt{557} \leq \#\mathcal{E}(\mathbb{F}_{557}) \leq 557 + 1 + 2\sqrt{557},$$

i.e.,  $511 \leq \#\mathcal{E}(\mathbb{F}_{557}) \leq 605$ .

- The only multiple of 189 in this interval is  $3 \cdot 189 = 567$  and so  $\#\mathcal{E}(\mathbb{F}_{557}) = 567$ .



## Baby Step, Giant Step – Point Order

Consider elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  and let  $O \neq P \in \mathcal{E}(\mathbb{F}_q)$ .  
Find the order of  $P$ .

- Let  $\#\mathcal{E}(\mathbb{F}_q) = N$  (unknown). By Lagrange,  $[N]P = O$ .
- By the Hasse bound (274),

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

- Try all values of  $N$  in this interval to see if  $[N]P = O$ ; traversing the interval takes  $4\sqrt{q}$  steps. Speed up by BSGS.
- The *order* of  $P \neq O$  is the smallest integer  $k \geq 1$  such that  $[k]P = O$ . Then by Lagrange  $k \mid N$ .

## Baby Step, Giant Step – Algorithm

**1** Compute  $Q = [q + 1]P$ .

**2** *Baby steps*: Take  $m = \lceil \sqrt[q]{q} \rceil$ , compute and store

$$[0]P, [1]P, [2]P, \dots, [m]P.$$

**3** *Giant steps*: Compute

$$Q + [k(2m)]P \quad \text{for } k = -m, -(m-1), \dots, m-1, m$$

until there is a match  $Q + [i(2m)]P = [\pm j]P$  with a point (or its negative) on the stored list.

**4** Set  $M = q + 1 + 2mi \mp j$ . We have  $[M]P = O$ .

**5** Factorize  $M = p_1^{e_1} \cdots p_r^{e_r}$  into prime powers.

**6** Compute  $[M/p_i]P$  for  $1 \leq i \leq r$ . If  $[M/p_i]P = O$  for some  $i$ , resume with the factorization of  $M = M/p_i$ . Otherwise,  $M$  is the order of  $P$ .

## Baby Step, Giant Step – Correctness

There is a match in step 3.

### Proof.

- By the Frobenius trace formula (278),

$$[q + 1]P - [\#\mathcal{E}(\mathbb{F}_q)]P = [k]P$$

for some integer  $k(=t)$  with  $|k| \leq 2m^2$ . Since by Lagrange, element order divides group order,  $[\#\mathcal{E}(\mathbb{F}_q)]P = O$  and so

$$[q + 1]P = [k]P.$$

## Proof (cont'd)

- There are integers  $k_0, k_1$  with  $-m < k_0 \leq m$ ,  $-m \leq k_1 \leq m$  such that

$$k = k_0 + 2mk_1.$$

Indeed, let  $k_0 \equiv k \pmod{2m}$  with  $-m < k_0 \leq m$  and  $k_1 = (k - k_0)/(2m)$ . Then

$$|k_1| \leq (2m^2 + m)/(2m) < m + 1.$$

- Let  $k = k_0 + 2mk_1$  and  $i = -k_1$ . Then

$$\begin{aligned} Q + [i(2m)]P &= [q + 1 - 2mk_1]P = [q + 1 - k + k_0]P \\ &= [N]P + [k_0]P = [k_0]P = [\pm j]P, \end{aligned}$$

where  $j = |k_0| \geq 0$ . Thus there is a match. □

## Baby Step, Giant Step – Correctness

Step 6 yields the order of  $P$ .

Let  $G$  be an additive group and let  $g \in G$ . Suppose  $Mg = 0$  for some  $M \geq 1$  and let  $M = p_1^{e_1} \cdots p_r^{e_r}$  be the prime factorization. If  $(M/p_i)g \neq 0$  for all  $i$ , then  $M$  is the order of  $g$ .

### Proof.

Let  $Mg = 0$ . Suppose  $M$  is not the order of  $g$ . Then  $M$  is a multiple of the order of  $g$ . Thus there must be a prime divisor  $p_i$  of  $M$  such that  $(M/p_i)g = 0$ .  $\square$

## Baby Step, Giant Step – Point Order

- Running time has the order of  $m = \sqrt[4]{q}$  (giant steps).
- Store only the  $x$ -coordinate of  $[j]P$  (along with  $j$ ), since looking for a match with  $[\pm j]P$  requires only the  $x$ -coordinate. When a match is found, the two possible  $y$ -coordinates can be computed.
- *Giant steps*: Precompute  $Q$  and  $[2m]P$ . Then  $Q + [k + 1]([2m]P)$  can be computed from  $Q + [k]([2m]P)$  by adding  $[2m]P$ .
- The factorization of  $M$  may be difficult to achieve. If so, find all small prime factors  $p_i$  of  $M$  and check  $[M/p_i]P \neq O$ . If so,  $M$  will be a good candidate for the order of  $P$ .

## Example

Reconsider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_{557}$  given by  $Y^2 = X^3 - 10X + 21$  and let  $P = (2 : 3 : 1) \in \mathcal{E}(\mathbb{F}_{557})$ .

- $Q = [558]P = (418 : 33 : 1)$ .
- Take  $m = \lceil \sqrt[4]{557} \rceil = 5$  and store the points  $[j]P$ ,  $0 \leq j \leq 5$ :

$$O, \quad (2 : 3 : 1), \quad (58 : 164 : 1), \quad (44 : 294 : 1), \\ (56 : 339 : 1), \quad (132 : 364 : 1).$$

- Match  $Q + [i(2m)]P = [\pm j]P$  is given for  $i = 1 = j$ . So  $[q + 1 + 2mi - j]P = [567]P = O$ .
- Factorize  $567 = 3^4 \cdot 7$  and compute  $[567/3]P = [189]P = O$ .
- Factorize  $189 = 3^3 \cdot 7$  and compute  $[189/3]P = (38 : 535 : 1) \neq O$ ,  $[189/7]P = (136 : 360 : 1) \neq O$ . So  $P$  has order 189.

## Baby Step, Giant Step – Group Order

Determine the group order  $\#\mathcal{E}(\mathbb{F}_q)$ .

- Repeat the steps 1-6 with randomly chosen points  $P$  in  $\mathcal{E}(\mathbb{F}_q)$  until the least common multiple (lcm) of the orders of the points divides only one integer  $N$  with

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

Then  $N = \#\mathcal{E}(\mathbb{F}_q)$ .

- Note that if  $P_1$  has order  $M_1$  and  $P_2$  has order  $M_2$ , then  $P_1 + P_2$  has order  $\text{lcm}(M_1, M_2)$ .

## Quadratic Character

Define the mapping  $\chi : \mathbb{F}_q^* \rightarrow \{\pm 1\}$  by

$$\chi(x) = \begin{cases} 1 & \text{if } x \text{ is a square in } \mathbb{F}_q, \\ -1 & \text{otherwise.} \end{cases} \quad (291)$$

The multiplicative group  $\mathbb{F}_q^*$  is cyclic of order  $q - 1$ , i.e., for some generator  $\xi$  of  $\mathbb{F}_q^*$ ,

$$\mathbb{F}_q^* = \langle \xi \rangle = \{\xi, \xi^2, \dots, \xi^{q-1} = 1\}.$$

Thus for each integer  $m \geq 0$ ,

$$\chi(\xi^m) = \begin{cases} 1 & \text{if } m \text{ is even,} \\ -1 & \text{otherwise.} \end{cases} \quad (292)$$

## Quadratic Character

The mapping  $\chi$  is a group homomorphism, called *quadratic character* of  $\mathbb{F}_q^*$ , i.e., for all  $x, y \in \mathbb{F}_q^*$ ,

$$\chi(xy) = \chi(x)\chi(y). \quad (293)$$

The mapping  $\chi$  can be extended to  $\chi : \mathbb{F}_q \rightarrow \{\pm 1, 0\}$  by setting  $\chi(0) = 0$ .

## Quadratic Character – Example

Consider the Galois field  $\mathbb{F}_8 = \mathbb{F}_2[X]/\langle X^3 + X + 1 \rangle$ . The elements are

$$\begin{aligned} 0, & \quad \alpha^3 = \alpha + 1, \\ 1, & \quad \alpha^4 = \alpha^2 + \alpha, \\ \alpha, & \quad \alpha^5 = \alpha^2 + \alpha + 1, \\ \alpha^2, & \quad \alpha^6 = \alpha^2 + 1, \end{aligned}$$

where  $\alpha$  is a zero of  $X^3 + X + 1$ , i.e.,  $\alpha^3 + \alpha + 1 = 0$ .

The squares of  $\mathbb{F}_8^*$  are

$$1^2 = 1, (\alpha)^2 = \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^3)^2 = \alpha^6$$

and the non-squares are

$$\alpha, \alpha^3, \alpha^5.$$

## Group Order (Using Characters)

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$  with characteristic  $p \neq 2, 3$  given by  $Y^2 = X^3 + AX + B \in \mathbb{F}_q[X]$ . Put

$$h(X) = X^3 + AX + B. \quad (294)$$

Then

$$\#\mathcal{E}(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(h(x)). \quad (295)$$

## Proof.

Let  $x \in \mathbb{F}_q$ .

- If  $h(x) = 0$ , then  $y = 0$  is the only solution.
- If  $h(x) \neq 0$  is a square in  $\mathbb{F}_q$ , the equation  $Y^2 = h(X)$  has two solutions  $(x, y)$  and  $(x, -y)$ .
- If  $h(x) \neq 0$  is not a square in  $\mathbb{F}_q$ , the equation  $Y^2 = h(X)$  has no solution.

Thus for each  $x \in \mathbb{F}_q$ , the equation  $Y^2 = h(X)$  has  $\chi(h(x)) + 1$  solutions  $y$  in  $\mathbb{F}_q$ .

The number of such solutions is

$$\sum_{x \in \mathbb{F}_q} (\chi(h(x)) + 1) = q + \sum_{x \in \mathbb{F}_q} \chi(h(x)).$$

Adding the base point  $O$  yields the result. □

## Group Order – Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_5$  given by  $Y^2 = X^3 + X + 1$ .  
Then

$$\begin{aligned} \#\mathcal{E}(\mathbb{F}_5) &= 1 + 5 + \sum_{x=0}^4 \chi(x^3 + x + 1) \\ &= 6 + \chi(1) + \chi(3) + \chi(1) + \chi(1) + \chi(4) \\ &= 6 + 1 - 1 + 1 + 1 + 1 = 9, \end{aligned}$$

since the squares modulo 5 are 1 and 4; i.e.,  $1^2 = 1$ ,  $2^2 = 4$ ,  $3^2 = 4$ , and  $4^2 = 1$  in  $\mathbb{Z}_5$ , and the nonsquares modulo 5 are 2 and 3.

## Group Order – Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_{31}$  given by  $Y^2 = X^3 - X$ .

- $-1$  is not a square in  $\mathbb{F}_{31}$ , i.e.,  $\chi(-1) = -1$ , since  $31 \equiv 3 \pmod{4}$ .

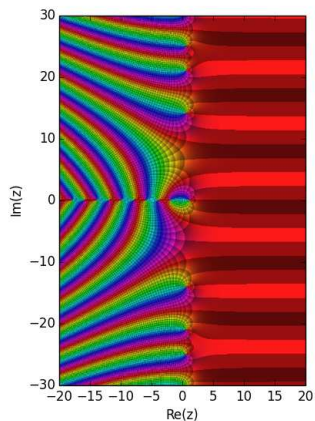
- For each  $x \in \mathbb{F}_{31}$  with  $x^3 - x \neq 0$ ,

$$\begin{aligned}\chi((-x)^3 - (-x)) &= \chi(-(x^3 - x)) = \chi(-1)\chi(x^3 - x) \\ &= -\chi(x^3 - x).\end{aligned}$$

- The equation  $X^3 - X = 0$  has three solutions  $x = 0, 1, -1$  in  $\mathbb{F}_{31}$  and in these cases we have  $\chi(x^3 - x) = 0$ .
- Otherwise, the above equation shows that either  $x^3 - x$  or  $(-x)^3 - (-x)$  is a square in  $\mathbb{F}_{31}$ . Thus  $\chi(x^3 - x) + \chi((-x)^3 - (-x)) = 0$ .
- It follows that

$$\#\mathcal{E}(\mathbb{F}_{31}) = 1 + 31 + \sum_{x \in \mathbb{F}_{31}} \chi(x^3 - x) = 32.$$

# Zeta-Function



Riemann zeta function  $\zeta(z)$  plotted with domain coloring.

## Zeta-Function

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . Write

$$N_n = \#\mathcal{E}(\mathbb{F}_{q^n}), \quad n \geq 1. \quad (296)$$

The *Z-function* of  $\mathcal{E}$  is the formal power series in  $\mathbb{Q}[[T]]$  defined by

$$Z(T; \mathcal{E}/\mathbb{F}_q) = \exp \left( \sum_{n=1}^{\infty} \frac{N_n}{n} T^n \right), \quad (297)$$

where  $\exp(t) = \sum_n t^n/n!$  is the exponential function.

## Zeta-Function

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$  with  $\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t$ . Then

$$Z(T; \mathcal{E}/\mathbb{F}_q) = \frac{qT^2 - tT + 1}{(1 - T)(1 - qT)}. \quad (298)$$

### Proof.

Factorize  $X^2 - tX + q = (X - \alpha)(X - \beta)$  over  $\mathbb{C}$ . Then by comparison of coefficients,

$$t = \alpha + \beta \quad \text{and} \quad q = \alpha\beta$$

and by (285),

$$N_n = q^n + 1 - \alpha^n - \beta^n, \quad n \geq 1.$$

## Proof (cont'd).

$$\begin{aligned}
Z(T; \mathcal{E}/\mathbb{F}_q) &= \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\right) \\
&= \exp\left(\sum_{n=1}^{\infty} (q^n + 1 - \alpha^n - \beta^n) \frac{T^n}{n}\right) \\
&= \exp(-\log(1 - qT) - \log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T)) \\
&= \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)} \\
&= \frac{qT^2 - tT + 1}{(1 - T)(1 - qT)},
\end{aligned}$$

where  $\log(x) = \sum_n (-1)^{n-1} (x-1)^n/n$  by Taylor series expansion and so  $-\log(1-x) = \sum_n x^n/n$ .  $\square$

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_2$  given by  $Y^2 + Y = X^3$ . The  $\mathbb{F}_2$ -rational points are  $O, (0 : 0 : 1), (0 : 1 : 1)$ , thus  $t = q + 1 - \#\mathcal{E}(\mathbb{F}_2) = 2 + 1 - 3 = 0$  and  $N_1 = 3$ . Therefore,

$$X^2 - tX + q = X^2 + 2 = (X + i\sqrt{2})(X - i\sqrt{2}).$$

> series( (2\*x^2+1)/((1-x)\*(1-2\*x)), x=0,8);

$$1 + 3x + 9x^2 + 21x^3 + 45x^4 + 93x^5 + 189x^6 + 381x^7 + O(x^8).$$

We have

$$N_n = 2^n + 1 - (i\sqrt{2})^n - (-i\sqrt{2})^n, \quad n \geq 1.$$

Explicitly,

$$N_n = \begin{cases} 2^n + 1 & \text{if } n \text{ is odd,} \\ 2^n + 1 - 2(-2)^{n/2} & \text{if } n \text{ is even.} \end{cases}$$

## Zeta-Function

The *zeta function* of  $\mathcal{E}$  over  $\mathbb{F}_q$  is

$$\zeta_{\mathcal{E}}(s) = Z(q^{-s}; \mathcal{E}/\mathbb{F}_q), \quad (299)$$

where  $s$  is a complex variable; i.e., for  $T = q^{-s}$ ,

$$\zeta_{\mathcal{E}}(s) = \frac{q^{1-2s} - tq^{-s} + 1}{(1 - q^{-s})(1 - q^{1-s})}. \quad (300)$$

\*The zeta function  $\zeta_{\mathcal{E}}(s)$  has properties similar to the classical Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \quad (301)$$

## Zeta-Function

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . Then

$$\zeta_{\mathcal{E}}(s) = \zeta_{\mathcal{E}}(1-s). \quad (302)$$

### Proof.

By (300) we have

$$\begin{aligned} \zeta_{\mathcal{E}}(s) &= \frac{q^{1-2s} - tq^{-s} + 1}{(1 - q^{-s})(1 - q^{1-s})}, && \text{expand by } q^{2s-1}, \\ &= \frac{1 - tq^{s-1} + q^{-1+2s}}{(q^s - 1)(q^{s-1} - 1)} \\ &= \zeta_{\mathcal{E}}(1-s). \end{aligned}$$



## Zeta-Function

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . If  $\zeta_{\mathcal{E}}(s) = 0$ , then  $\Re(s) = \frac{1}{2}$ .

### Proof.

We have  $X^2 - tX + q = (X - \alpha)(X - \beta)$ . By comparing coefficients,  $q = \alpha\beta$  and  $t = \alpha + \beta$ . So the numerator of  $Z(T; \mathcal{E}/\mathbb{F}_q)$  in (298) can be written as

$$qT^2 - tT + 1 = (1 - \alpha T)(1 - \beta T).$$

Thus by using  $T = q^{-s}$ ,

$$\zeta_{\mathcal{E}}(s) = 0 \iff \alpha = q^s \text{ or } \beta = q^s.$$

By the quadratic formula, the zeros of  $X^2 - tX + q$  are

$$\alpha, \beta = \frac{1}{2} \left( t \pm \sqrt{t^2 - 4q} \right).$$

## Proof (cont'd).

By the Hasse bound (274),

$$|t| \leq 2\sqrt{q}$$

and so  $t^2 - 4q \leq 0$ . Thus  $\alpha$  and  $\beta$  are complex conjugates.

Then

$$q = \alpha\beta = \alpha\bar{\alpha} = |\alpha|^2$$

and so

$$|\alpha| = |\beta| = \sqrt{q}.$$

If  $q^s = \alpha$  or  $\beta$ , then

$$q^{\Re(s)} \stackrel{!}{=} |q^s| = \sqrt{q}.$$

Hence,  $\Re(s) = \frac{1}{2}$ . □

## Zeta Function

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ .

- Define the *degree* of  $P \in \mathcal{E}(\bar{\mathbb{F}}_q)$ , written  $\deg(P)$ , as the smallest integer  $n \geq 1$  such that  $P \in \mathcal{E}(\mathbb{F}_{q^n})$ .
- The set

$$S_P = \{P, \phi_q(P), \phi_q^2(P), \dots, \phi_q^{n-1}(P)\} \quad (303)$$

has  $n = \deg(P)$  elements and  $\phi_q^n(P) = P$ . Each point in  $S_P$  has also degree  $n$ .

## Zeta Function

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ . Then

$$\zeta_{\mathcal{E}}(s) = \prod_{S_P} \left(1 - \frac{1}{q^{s \cdot \deg(P)}}\right)^{-1}, \quad (304)$$

where the product is over the points  $P \in \mathcal{E}(\bar{\mathbb{F}}_q)$  with exactly one point from each set  $S_P$ .

## Proof.

If  $\deg(P) = m$ , then  $P$  and all other points in  $S_P$  have coordinates in  $\mathbb{F}_{q^m}$ .

Since  $\mathbb{F}_{q^m}$  is a subfield of  $\mathbb{F}_{q^n}$  iff  $m \mid n$ , it follows that  $S_P$  contributes  $m$  points to  $N_n = \#\mathcal{E}(\mathbb{F}_{q^n})$  iff  $m \mid n$ ; otherwise, it contributes no points to  $N_n$ . Thus

$$N_n = \sum_{m \mid n} \sum_{\substack{S_P \\ \deg(P)=m}} m.$$

## Proof (cont'd)

We have

$$\begin{aligned}
 \log Z(T; \mathcal{E}/\mathbb{F}_q) &= \sum_{n=1}^{\infty} \frac{N_n}{n} T^n \\
 &= \sum_{n=1}^{\infty} \frac{1}{n} T^n \sum_{m|n} \sum_{\substack{S_P \\ \deg(P)=m}} m \\
 &= \sum_{j=1}^{\infty} \sum_{m=1}^{\infty} \frac{1}{mj} \sum_{\substack{S_P \\ \deg(P)=m}} m T^{mj}, \quad (mj = n), \\
 &= \sum_{j=1}^{\infty} \sum_{S_P} \frac{1}{j} T^{j \cdot \deg(P)} \\
 &= - \sum_{S_P} \log \left( 1 - T^{\deg(P)} \right).
 \end{aligned}$$

Substitute  $T = q^{-s}$  and exponentiate to obtain the result. □

## Supersingular Curves

Hasse (1936) discovered supersingular elliptic curves during his work on the Riemann hypothesis for elliptic curves by observing that in positive characteristic elliptic curves could have endomorphism rings of unusually large rank.

Wikipedia (2018)

## Supersingular Curves

An elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  with  $\text{char}(\mathbb{K}) = p > 0$  is *supersingular* if it has no points of order  $p$ ; i.e.,  $\mathcal{E}[p] = \{O\}$ .

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$  with  $q = p^r$ ,  $p$  prime. Let  $t = q + 1 - \#\mathcal{E}(\mathbb{F}_q)$  be the Frobenius trace. Then

$$\mathcal{E} \text{ is supersingular} \iff t \equiv 0 \pmod{p}, \quad (305)$$

i.e.,  $\#\mathcal{E}(\mathbb{F}_q) \equiv 1 \pmod{p}$ .

## Proof.

- Write  $X^2 - tX + q = (X - \alpha)(X - \beta)$ . Then by (285),

$$\#\mathcal{E}(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

- Consider the sequence  $(s_n)$  given by  $s_n = \alpha^n + \beta^n$ . Then by (287),  $s_0 = 2$ ,  $s_1 = t$ , and  $s_{n+1} = ts_n - qs_{n-1}$  for all  $n \geq 1$ .
- Suppose  $t \equiv 0 \pmod p$ . Then  $s_1 = t \equiv 0 \pmod p$  and so  $s_{n+1} \equiv 0 \pmod p$  for all  $n \geq 1$  by the recurrence. Thus

$$\#\mathcal{E}(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 \pmod p.$$

By Lagrange,  $\mathcal{E}(\mathbb{F}_{q^n})$  has no point of order  $p$ . Since  $\bar{\mathbb{F}}_q = \bigcup_{n \geq 1} \mathbb{F}_{q^n}$ ,  $\mathcal{E}(\bar{\mathbb{F}}_q)$  has no point of order  $p$ . Hence,  $\mathcal{E}$  is supersingular over  $\bar{\mathbb{F}}_q$ .

## Proof (cont'd).

- Suppose  $t \not\equiv 0 \pmod{p}$ . By the recurrence,  $s_{n+1} \equiv ts_n \pmod{p}$  for all  $n \geq 1$ . Since  $s_1 = t$ , we have  $s_n \equiv t^n \pmod{p}$  for all  $n \geq 1$ . Thus

$$\#\mathcal{E}(\mathbb{F}_{q^n}) = q^n + 1 - s_n \equiv 1 - t^n \pmod{p}.$$

By Fermat's little theorem,  $x^{p-1} \equiv 1 \pmod{p}$  for all nonzero points  $x \in \mathbb{F}_p$ . Thus

$$\#\mathcal{E}(\mathbb{F}_{q^{p-1}}) \equiv 1 - t^{p-1} \equiv 0 \pmod{p}.$$

So the order of  $\mathcal{E}(\mathbb{F}_{q^{p-1}})$  is divisible  $p$  and thus  $\mathcal{E}(\mathbb{F}_{q^{p-1}})$  has a point of order  $p$ . Hence,  $\mathcal{E}$  is not supersingular.



## Supersingular Curves

Let  $\mathcal{E}$  is an elliptic curve over  $\mathbb{F}_p$  with  $p \geq 5$  prime. Then

$$\mathcal{E} \text{ is supersingular} \iff t = 0, \quad (306)$$

i.e.,  $\#\mathcal{E}(\mathbb{F}_p) = p + 1$ .

### Proof.

- Let  $t = 0$ . Then by (305),  $\mathcal{E}(\mathbb{F}_p)$  is supersingular.
- Let  $\mathcal{E}$  be supersingular with  $t \neq 0$ . Then by (305),  $t \equiv 0 \pmod{p}$  and so  $|t| \geq p$ . By the Hasse bound (274),  $|t| \leq 2\sqrt{p}$  and so  $p \leq 2\sqrt{p}$ , which is only valid for  $p \leq 4$ .  $\square$

## Example

- The elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_2$  given by  $Y^2 + Y = X^3 + X$  has five  $\mathbb{F}_2$ -rational points,

$$O, (0 : 0 : 1), (0 : 1 : 1), (1 : 0 : 1), (1 : 1 : 1).$$

Here  $t = p + 1 - \#\mathcal{E}(\mathbb{F}_p) = 2 + 1 - 5 = -2$ .

- The elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_3$  given by  $Y^2 = X^3 - X + 2$  has only the base point  $O$  as  $\mathbb{F}_3$ -rational point.

Here  $t = p + 1 - \#\mathcal{E}(\mathbb{F}_p) = 3 + 1 - 1 = 3$ .

Both curves are supersingular, but  $t = p + 1 - \#\mathcal{E}(\mathbb{F}_p) \neq 0$ . So the above restriction  $p \geq 5$  is necessary.

## Supersingular Curves

Let  $q$  be an odd prime power with  $q \equiv 2 \pmod{3}$  and let  $b \in \mathbb{F}_q^*$ . Then the elliptic curve  $\mathcal{E}(\mathbb{F}_q)$  given by

$$Y^2 = X^3 + b \tag{307}$$

is supersingular.

### Proof.

- Consider the homomorphism  $\phi : \mathbb{F}_q^* \rightarrow \mathbb{F}_q^* : x \mapsto x^3$ . Since  $q - 1$  is not a multiple of 3,  $\mathbb{F}_q^*$  has no element of order 3 and so  $\ker \phi$  is trivial; i.e., there is no  $x \in \mathbb{F}_q^*$  with  $x^3 = 1$ . Thus  $\phi$  is one-to-one and so onto. Hence, each  $x \in \mathbb{F}_q^*$  has a *unique* cubic root (preimage).
- For each  $y \in \mathbb{F}_q$ , there is a *unique*  $x \in \mathbb{F}_q$  given by the cubic root of  $y^2 - b$  such that  $(x, y) \in \mathcal{E}(\mathbb{F}_q)$ . For each of the  $q$  values for  $Y$ , we obtain  $q$  values for  $X$ . Including the base point  $O$ , we have  $\#\mathcal{E}(\mathbb{F}_q) = q + 1$ . Therefore, by (305),  $\mathcal{E}(\mathbb{F}_q)$  is supersingular.  $\square$

## Fast Point Multiplication

Let  $\mathcal{E}$  be a supersingular elliptic curve over  $\mathbb{F}_q$  and let  $P = (x : y : 1) \in \mathcal{E}(\mathbb{F}_{q^n})$  for some (large)  $n \geq 1$ .

Given  $k \geq 1$ . Compute  $[k]P$ .

- Let  $t = 0$ . Then by (279),

$$\phi_q^2 + [q] = 0 \quad (308)$$

and so by plugging in  $P$ ,

$$[q](x, y) = -\phi_q^2(x, y) = (x^{q^2}, -y^{q^2}). \quad (309)$$

- Compute  $x^{q^2}$  and  $y^{q^2}$  by finite field arithmetic.
- Express  $x$  and  $y$  by a normal basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . Then  $x^{q^2}$  and  $y^{q^2}$  can be computed by shift operations.

## Fast Point Multiplication

- 1 Expand  $k$  in base  $q$ ,

$$k = k_0 + k_1q + \dots + k_rq^r, \quad 0 \leq k_i < q. \quad (310)$$

- 2 Compute

$$[k_i]P = (x_i, y_i), \quad 0 \leq i \leq r. \quad (311)$$

- 3 Compute

$$[q^i]([k_i]P) = -\phi_{q^i}^2(x_i, y_i) = \left(x_i^{q^{2i}}, (-1)^i y_i^{q^{2i}}\right), \quad 0 \leq i \leq r \quad (312)$$

- 4 Compute the sum of  $[q^i]([k_i]P)$  for  $0 \leq i \leq r$  to obtain  $[k]P$ .

The main saving is in step 3 in which finite field calculations can be used.

## Normal Bases

Let  $n \geq 1$ . The finite field  $\mathbb{F}_{q^n}$  is a vector space of dimension  $n$  over  $\mathbb{F}_q$ .

Let  $\{\beta_1, \dots, \beta_n\}$  be an  $\mathbb{F}_q$ -basis of  $\mathbb{F}_{q^n}$ . Each element  $\alpha \in \mathbb{F}_{q^n}$  has a unique representation of the form

$$\alpha = a_1\beta_1 + \dots + a_n\beta_n \quad (313)$$

with  $a_1, \dots, a_n \in \mathbb{F}_q$ .

There exists  $\beta \in \mathbb{F}_{q^n}$  such that

$$\{\beta, \beta^q, \dots, \beta^{q^{n-1}}\} \quad (314)$$

is an  $\mathbb{F}_q$ -basis of  $\mathbb{F}_{q^n}$ , called *normal basis*.

## Normal Bases

Let  $\{\beta, \beta^q, \dots, \beta^{q^{n-1}}\}$  be a normal basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . For  $\alpha \in \mathbb{F}_{q^n}$  write

$$\alpha = a_1\beta + a_2\beta^q + \dots + a_n\beta^{q^{n-1}} \quad (315)$$

with  $a_1, \dots, a_n \in \mathbb{F}_q$ . Then

$$\begin{aligned} \alpha^q &= a_1\beta^q + a_2\beta^{q^2} + \dots + a_n\beta^{q^n} \\ &= a_n\beta^{q^n} + a_1\beta^q + \dots + a_{n-1}\beta^{q^{n-1}} \\ &= a_n\beta + a_1\beta^q + \dots + a_{n-1}\beta^{q^{n-1}}, \end{aligned} \quad (316)$$

since  $a_i^q = a_i$  and  $\beta^{q^n} = \beta$ .

Thus if  $\alpha$  has coordinates  $(a_1, \dots, a_n)$ , then  $\alpha^q$  has (cyclically shifted) coordinates  $(a_n, a_1, \dots, a_{n-1})$ .

## Example

The field  $\mathbb{F}_8$  over  $\mathbb{F}_2$  generated by  $\alpha$  with  $\alpha^3 + \alpha + 1 = 0$  has the elements

$$\begin{aligned} 0, & & \alpha^4 &= \alpha^2 + \alpha, \\ \alpha, & & \alpha^5 &= \alpha^2 + \alpha + 1, \\ \alpha^2, & & \alpha^6 &= \alpha^2 + 1, \\ \alpha^3 &= \alpha + 1, & \alpha^7 &= 1. \end{aligned}$$

Then  $\{\alpha^3, \alpha^6, \alpha^5\}$  is a normal basis of  $\mathbb{F}_8$  over  $\mathbb{F}_2$ ,

$$\begin{aligned} 0 &= (0, 0, 0), & \alpha^3 &= (1, 0, 0), \\ 1 &= (1, 1, 1), & \alpha^4 &= (1, 1, 0), \\ \alpha &= (0, 1, 1), & \alpha^5 &= (0, 0, 1), \\ \alpha^2 &= (1, 0, 1), & \alpha^6 &= (0, 1, 0). \end{aligned}$$

We have

$$\begin{aligned} \alpha &= 0 \cdot \alpha^3 + 1 \cdot \alpha^6 + 1 \cdot \alpha^5, \\ \alpha^2 &= 1 \cdot \alpha^3 + 0 \cdot \alpha^6 + 1 \cdot \alpha^5, \\ \alpha^4 &= 1 \cdot \alpha^3 + 1 \cdot \alpha^6 + 0 \cdot \alpha^5. \end{aligned}$$

## \*Schoof's Algorithm

The algorithm was published by René Schoof in 1985 and it was a theoretical breakthrough, as it was the first deterministic polynomial time algorithm for counting points on elliptic curves. Before Schoof's algorithm, approaches to counting points on elliptic curves such as the naive and baby-step giant-step algorithms were, for the most part, tedious and had an exponential running time.

Wikipedia (2018)

## Schoof's Algorithm

Given elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  with  $\text{char}(\mathbb{F}_q) = p > 0$ ,  $p$  odd, given by  $Y^2 = X^3 + AX + B$ .

- By the Frobenius trace (278) and Hasse bound (274),

$$\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t \quad (317)$$

with  $|t| \leq 2\sqrt{q}$ .

- Let  $S = \{2, 3, \dots, L\}$  be a set of primes with  $p \notin S$  and

$$\prod_{\ell \in S} \ell > 4\sqrt{q}. \quad (318)$$

- If we have  $t \pmod{\ell}$  for all  $\ell \in S$ , then by the Chinese Remainder theorem we know  $t \pmod{\prod_{\ell \in S} \ell}$ ; i.e., we know  $t$ .

## Schoof's Algorithm

Case  $\ell = 2$ :  $t \equiv \#\mathcal{E}(\mathbb{F}_q) \pmod{2}$ , i.e.,  $\#\mathcal{E}(\mathbb{F}_q)$  even or odd.

- Suppose  $X^3 + AX + B$  has no root in  $\mathbb{F}_q$ . For each  $x \in \mathbb{F}_q$  with  $y_0 = x^3 + Ax + B \neq 0$ , there are either two points  $(x, \pm\sqrt{y_0})$  or no point on the curve. The number of such points is even.
- Suppose  $X^3 + AX + B$  has a root  $x_0$  in  $\mathbb{F}_q$ . Over  $\bar{\mathbb{F}}_q$ ,

$$X^3 + AX + B = (X - x_0)(X - x_1)(X - x_2) \quad (319)$$

with  $x_1, x_2 \in \bar{\mathbb{F}}_q$ . Since  $\mathcal{E}$  is nonsingular,  $x_0, x_1, x_2$  are pairwise distinct. By comparing the coefficients of  $X^2$ ,  $x_0 + x_1 + x_2 = 0$ . So  $x_1, x_2$  are either both in  $\mathbb{F}_q$  or none of them is in  $\mathbb{F}_q$ . Thus there are either three points  $(x_0, 0), (x_1, 0), (x_2, 0)$  or there is only one point  $(x_0, 0)$  on the curve. The number of such points is odd.

## Schoof's Algorithm

Case  $\ell = 2$  (cont'd):

- If the base point  $O$  is added,  $\#\mathcal{E}(\mathbb{F}_q) \equiv 1 \pmod{2}$  iff  $X^3 + AX + B$  has no root in  $\mathbb{F}_q$ .
- The roots of  $X^q - X$  are exactly the elements of  $\mathbb{F}_q$ ; i.e.,

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha). \quad (320)$$

- $X^3 + AX + B$  has a root in  $\mathbb{F}_q$  iff it has a root in common with  $X^q - X$ .
- $(X^q - X, X^3 + AX + B) = 1$  iff  $X^3 + AX + B$  has no root in  $\mathbb{F}_q$ .
- Use the Euclidean algorithm to compute this gcd.
- \*Case  $\ell > 2$  (see algorithm).

## Schoof's Symbolic Algorithm

Case  $\ell > 2$ :

- $\psi_\ell$  is a polynomial in  $X$  ( $\ell$  odd) and for  $(x, y) \in \mathcal{E}(\bar{\mathbb{F}}_q)$ ,

$$(x, y) \in \mathcal{E}[\ell] \iff \psi_\ell(x) = 0;$$

i.e., the roots of  $\psi_\ell$  are exactly the  $x$ -coordinates of the points in  $\mathcal{E}[\ell]$ .

- Since  $\phi_q^2 - t\phi_q + q = 0$ , for each point  $(x, y)$  of order  $\ell$ ,

$$(x^{q^2}, y^{q^2}) + q(x, y) = t(x^q, y^q).$$

- Let  $q_\ell \equiv q \pmod{\ell}$  with  $|q_\ell| < \ell/2$ . Then

$$(x^{q^2}, y^{q^2}) + q_\ell(x, y) = t(x^q, y^q).$$

Since  $(x^q, y^q)$  is also a point of order  $\ell$ , this relation determines  $t \pmod{\ell}$ .

## Schoof's Symbolic Algorithm

Case  $\ell > 2$  (cont'd):

- Suppose for some  $(x, y) \in \mathcal{E}[\ell]$ ,

$$(x^{q^2}, y^{q^2}) \neq \pm q_\ell(x, y).$$

- Then put

$$(x', y') = (x^{q^2}, y^{q^2}) + q_\ell(x, y) \neq O.$$

Thus  $t \not\equiv 0 \pmod{\ell}$ .

- The  $x$ -coordinates of the summands on the right-hand side are distinct and so  $x'$  is found by the formula using the line through the two points, rather than the tangent line.

## Schoof's Symbolic Algorithm

Case  $\ell > 2$  (cont'd):

- Write

$$j(x, y) = (x_j, y_j), \quad j \in \mathbb{Z},$$

where  $x_j = r_{1,j}(x)$  and  $y_j = r_{2,j}(x)y$ . Compute  $x_j, y_j$  using division polynomials.

- Then

$$x' = \left( \frac{y^{q^2} - y_{q\ell}}{x^{q^2} - x_{q\ell}} \right)^2 - x^{q^2} - x_{q\ell}$$

and by using  $y^2 = x^3 + Ax + B$ ,

$$\begin{aligned} & \left( y^{q^2} - y_{q\ell} \right)^2 \\ &= y^2 \left( y^{q^2-1} - r_{2,q\ell}(x) \right)^2 \\ &= (x^3 + Ax + B) \left( (x^3 + Ax + B)^{(q^2-1)/2} - r_{2,q\ell}(x) \right)^2. \end{aligned}$$

## Schoof's Symbolic Algorithm

Case  $\ell > 2$  (cont'd):

- Find  $j \in \mathbb{Z}$  such that

$$(x', y') = j(x^q, y^q) = (x_j^q, y_j^q).$$

- For  $(x, y) \in \mathcal{E}[\ell]$ ,

$$(x', y') = \pm(x_j^q, y_j^q) \iff x' = x_j^q.$$

- The roots of  $\psi_\ell$  are the  $x$ -coordinates of the points in  $\mathcal{E}[\ell]$  and so

$$(x', y') = \pm(x_j^q, y_j^q) \iff x' - x_j^q \equiv 0 \pmod{\psi_\ell}.$$

- The polynomial  $\psi_\ell$  has degree  $(\ell^2 - 1)/2$  and its roots are simple. Thus there are  $(\ell^2 - 1)/2$  distinct  $x$ -coordinates of the points in  $\mathcal{E}[\ell]$ .

## Schoof's Symbolic Algorithm

Case  $\ell > 2$  (cont'd):

- Suppose we have found  $j$  such that

$$(x', y') = \pm(x_j^q, y_j^q) = (x_j^q, \pm y_j^q).$$

- Determine the sign by looking at the  $y$ -coordinates.
- Both  $y'/y$  and  $y_j^q/y$  can be written as functions of  $x$ . If

$$(y' - y_j^q)/y \equiv 0 \pmod{\psi_\ell},$$

then  $t \equiv j \pmod{\ell}$ ; otherwise,  $t \equiv -j \pmod{\ell}$ .

- The remaining (rare) case is where

$$(x^{q^2}, y^{q^2}) = \pm q(x, y)$$

for all  $(x, y) \in \mathcal{E}[\ell]$ .

## Schoof's Symbolic Algorithm

Given elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  with  $q = p^r$ ,  $p$  odd prime, given by  $Y^2 = X^3 + AX + B$ . Find Frobenius trace  $t$ .

- 1 Choose a set of primes  $S = \{2, 3, \dots, L\}$  with  $p \notin S$  and  $\prod_{\ell \in L} \ell > 4\sqrt{q}$ .
- 2 If  $\ell = 2$ , then  $t \equiv 0 \pmod{2}$  iff  $(X^3 + AX + B, X^q - X) \neq 1$ .
- 3 For each odd prime  $\ell \in S$ :
  - a Let  $q_\ell \equiv q \pmod{\ell}$  with  $|q_\ell| < \ell/2$ .
  - b Compute the  $x$ -coordinate  $X'$  of

$$(X', Y') = (X^{q^2}, Y^{q^2}) + [q_\ell](X, Y) \pmod{\psi_\ell}.$$

## Schoof's Algorithm (cont'd)

- c For  $j = 1, 2, \dots, (\ell - 1)/2$ :
  - i Compute the  $x$ -coordinate of  $(X_j, Y_j) = [j](X, Y)$  using division polynomials.
  - ii If  $X' - X_j^q \equiv 0 \pmod{\psi_\ell}$ , goto step iii. Otherwise, try the next value of  $j$ . If all values of  $j$  have been tried, goto step d.
  - iii Compute  $Y'$  and  $Y_j$ . If  $(Y' - Y_j^q)/Y \equiv 0 \pmod{\psi_\ell}$ , then  $t \equiv j \pmod{\ell}$ ; otherwise,  $t \equiv -j \pmod{\ell}$ .

## Schoof's Algorithm (cont'd)

- d If all values of  $j$  have been tried without success, let  $w^2 \equiv q \pmod{\ell}$ . If  $w$  does not exist, then  $t \equiv 0 \pmod{\ell}$ .
- e If  $(\text{numerator}(X^q - X_w), \psi_\ell) = 1$ , then  $t \equiv 0 \pmod{\ell}$ .  
Otherwise, compute

$$(\text{numerator}((Y^q - Y_w)/Y), \psi_\ell).$$

If this gcd is not 1, then  $t \equiv 2w \pmod{\ell}$ ; otherwise,  $t \equiv -2w \pmod{\ell}$ .

## Schoof's Algorithm (cont'd)

- Use the values  $t \bmod \ell$  computed for each  $\ell \in S$  to calculate  $t \bmod \prod_{\ell \in S} \ell$  by the Chinese Remainder theorem. Choose the value of  $t$  that fulfills the congruence with  $|t| \leq 2\sqrt{q}$ . The number of points in  $\mathcal{E}(\mathbb{F}_q)$  is  $q + 1 - t$ . Done.

Schoof's algorithm has polynomial running time.

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_{19}$  given by  $Y^2 = X^3 + 2X + 1$ . Then  $\#\mathcal{E}(\mathbb{F}_{19}) = 19 + 1 - t$  with  $|t| \leq 2\sqrt{19}$ .

Let  $\ell = 2$ .

- Compute

$$X^{19} \equiv X^2 + 13X + 14 \pmod{X^3 + 2X + 1}.$$

Then

$$(X^{19} - X, X^3 + 2X + 1) = (X^2 + 12X + 14, X^3 + 2X + 1) = 1.$$

Thus  $X^3 + 2X + 1$  has no roots in  $\mathbb{F}_{19}$  and so (by adding the base point  $O$ )  $t \equiv 1 \pmod{2}$ .

## Example (cont'd)

Let  $\ell = 5$ .

- We have  $19 \equiv 4 \equiv -1 \pmod{5}$  and so  $q_\ell = -1$ .
- Thus  $[19](X, Y) = -(X, Y) = (X, -Y)$  for all points in  $\mathcal{E}[5]$ .
- Check for  $j = 2$ ,

$$\begin{aligned} (X', Y') &\stackrel{\text{def}}{=} (X^{361}, Y^{361}) + (X, -Y) \\ &\stackrel{?}{=} [\pm 2](X^{19}, Y^{19}) \stackrel{\text{def}}{=} (X'', Y''). \end{aligned}$$

- The fifth division polynomial is

$$\begin{aligned} \psi_5 = & 5X^{12} + 10X^{10} + 17X^8 + 5X^7 + X^6 + 9X^5 \\ & + 12X^4 + 2X^3 + 5X^2 + 8X + 8. \end{aligned}$$

## Example (cont'd)

- The  $x$ -coordinate of  $(X^{361}, Y^{361}) + (X, -Y)$  is

$$\begin{aligned} X' &= \left( \frac{Y^{361} - Y}{X^{361} - X} \right)^2 - X^{361} - X \\ &= (X^3 + 2X + 1) \left( \frac{(X^3 + 2X + 1)^{180} - 1}{X^{361} - X} \right)^2 - X^{361} - X. \end{aligned}$$

- The  $x$ -coordinate of  $[\pm 2](X^{19}, Y^{19})$  is

$$X'' = \left( \frac{3X^{38} + 2}{2Y^{19}} \right)^2 - 2X^{19}.$$

## Example (cont'd)

- Replacing  $Y^2$  by  $X^2 + 2X + 1$  gives a polynomial relation in  $X$ ,

$$\left(\frac{Y^{361} - Y}{X^{361} - X}\right)^2 - X^{361} - X \stackrel{?}{\equiv} \left(\frac{3X^{38} + 2}{2Y^{19}}\right)^2 - 2X^{19} \pmod{\psi_5},$$

which indeed holds.

- Thus  $t \equiv \pm 2 \pmod{5}$ .
- To determine the sign, look at the  $y$ -coordinates.

## Example (cont'd)

- The  $y$ -coordinate  $y'$  of  $(X^{361}, Y^{361}) + (X, -Y)$  is

$$Y (9X^{11} + 13X^{10} + 15X^9 + 15X^7 + 18X^6 + 17X^5 + 8X^4 + 12X^3 + 8X + 6) \pmod{\psi_5}.$$

- The  $y$ -coordinate  $Y''$  of  $[2](X^{19}, Y^{19})$  is

$$Y (13X^{10} + 15X^9 + 16X^8 + 13X^7 + 8X^6 + 6X^5 + 17X^4 + 18X^3 + 8X + 18) \pmod{\psi_5}.$$

- We have

$$(Y' + Y''^{19})/Y \equiv 0 \pmod{\psi_5}.$$

Thus  $t \equiv -2 \pmod{5}$ .

## Example (cont'd)

- We have

$$t \equiv \begin{cases} 1 & \text{mod } 2, \\ 2 & \text{mod } 3, \\ 3 & \text{mod } 5. \end{cases}$$

- We have  $2 \cdot 3 \cdot 5 = 30 > 4\sqrt{19} \approx 17.435$  and so by the Chinese Remainder theorem,

$$t \equiv 23 \pmod{30}.$$

Since  $|t| < 2\sqrt{19} < 9$ , we have  $t = -7$ . Thus

$$\#\mathcal{E}(\mathbb{F}_{19}) = 19 + 1 - (-7) = 27.$$

## Part VII

# Elliptic Curve Cryptography

# EC Cryptography

Curves,  
Cryptosystems,  
and Quantum  
Computing

K.-H.  
Zimmermann

## Contents

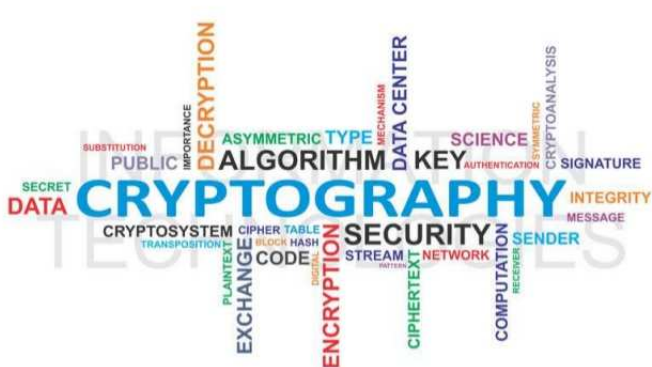
RSA Analog

Discrete Log

Attacking  
Discrete Log

\* Primality  
Testing

Factorization



## EC Cryptography

The U.S. National Institute of Standards and Technology (NIST) has endorsed elliptic curve cryptography in its Suite B set of recommended algorithms, specifically elliptic curve Diffie-Hellman (ECDH) for key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature. The U.S. National Security Agency (NSA) allows their use for protecting information classified up to top secret with 384-bit keys.

Wikipedia (2018).

## EC Cryptography

- Inventors Neal Koblitz and Victor Miller (1985)
- Elliptic curve algorithms enter 2004
- ECC requires smaller keys compared to non-ECC cryptography
- Usage in key agreement and digital signatures

## Contents

- RSA analog
- Discrete logarithm
- Attacking discrete logarithm
- \*Primality testing
- Factoring

## RSA Analog

COMPARABLE KEY SIZES FOR  
EQUIVALENT SECURITY

<b>Symmetric scheme (key size in bits)</b>	<b>ECC-based scheme (size of <math>n</math> in bits)</b>	<b>RSA/DSA (modulus size in bits)</b>
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

## RSA Analog

- Version of Menezes, Vanstone
- Version of Koyama, Maurer, Okamoto, Vanstone
- Imbedding plaintext
- Recommended elliptic curves

## Key Generation (Menezes, Vanstone, 1993)

Alice and Bob generate key:

- Choose (public) elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_p$  with  $p > 3$  prime.
- Choose (public) random point  $P \in \mathcal{E}(\mathbb{F}_p)$  such that  $P$  generates large subgroup  $H$  of  $\mathcal{E}(\mathbb{F}_p)$ .
- Take (secret) random values  $a, k \in \mathbb{Z}_{|H|}$ .

## Confidential Message Transmission

Alice has message  $m$  she wants to send to Bob. Suppose

$$m = (m_1, m_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*.$$

Alice encrypts the message  $m$ :

- $Q = [a]P$  with  $P$  and  $Q$  public.
- $Y = [k]Q$  with  $Y = (y_1, y_2)$ ,  $y_1 \neq 0 \neq y_2$ .
- $C = [k]P$ .
- $c_i \equiv y_i m_i \pmod{p}$  for  $i = 1, 2$ .
- Alice sends the encrypted message  $c = (C, c_1, c_2)$  to Bob.

## Confidential Message Transmission

Bob decrypts the cipher  $c$ :

- $[a]C = Y$ ,
- $m = (c_1 y_1^{-1} \bmod p, c_2 y_2^{-1} \bmod p)$ .

Correctness:

- $[a]C = [a][k]P = [k][a]P = [k]Q = Y$
- $y_i \neq 0$  is invertible in  $\mathbb{Z}_p$  and so  $m_i \equiv c_i y_i^{-1} \bmod p$  for  $i = 1, 2$ .

Security is based on the mathematical problem of computing discrete logarithms.

## Example

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_{557}$  given by  $Y^2 = X^3 - 10X + 21$ .

- Take the point  $P = (2, 3)$  of order 189.
- Choose the private keys  $k = 3$  and  $a = 2$ .
- Take plaintext  $m = (12, 7)$ .

## Example (cont'd)

### Encryption:

- $Q = [a]P = [2](2, 3) = (58, 164)$
- $Y = [k]Q = [3](58, 164) = (162, 24)$
- $C = [k]P = [3](2, 3) = (44, 294)$
- $c_1 \equiv y_1 m_1 = 12 \cdot 162 \equiv 273 \pmod{557}$
- $c_2 \equiv y_2 m_2 = 7 \cdot 24 \equiv 168 \pmod{557}$

Then Alice sends  $((44, 294), 273, 168)$  to Bob.

## Example (cont'd)

Singular computation:

```
> list P, Q, Y, C;  
> P[1] = 2;  
> P[2] = 3;  
> P[3] = 1;  
> Q = ellipticMult( 557, -10, 21, P, 2);  
    // Q = (58,164)  
> Y = ellipticMult( 557, -10, 21, Q, 3);  
    // Y = (162,24)  
> C = ellipticMult( 557, -10, 21, P, 3);  
    // C = (44,294)
```

## Key Generation (Koyama et al., 1992)

Public key generation:

- Each user chooses two distinct large primes  $p, q$  with  $p \equiv q \equiv 2 \pmod{3}$  and computes  $n = pq$ .
- Each user chooses integers  $e, d$  with

$$ed \equiv 1 \pmod{(p+1)(q+1)}$$

or  $\pmod{\text{lcm}(p+1, q+1)}$ .

- Each user makes  $n, e$  public and keeps  $d, p, q$  private.

## Confidential Message Transmission

Alice wants to send message  $m$  to Bob.

- Alice downloads Bob's public key  $n, e$ .
- Alice represents  $m$  as pair  $(m_1, m_2) \pmod n$  and regards it as point  $P$  on elliptic curve  $\mathcal{E}$  given by

$$Y^2 = X^3 + b \pmod n.$$

Note that  $b = m_2^2 - m_1^3 \pmod n$ .

- Alice sends  $C = [e]P$  to Bob.

Bob computes  $P = [d]C$ .

## Properties of Elliptic Curve

- The formula for point addition does not require  $b$ .  
Eavesdropper Eve can compute it as  $b = c_2^2 - c_1^3 \pmod n$ ,  
since  $C = (c_1, c_2) \in \mathcal{E}(\mathbb{Z}_n)$ .

- By the Chinese Remainder theorem,

$$\mathcal{E}(\mathbb{Z}_n) = \mathcal{E}(\mathbb{F}_p) \oplus \mathcal{E}(\mathbb{F}_q). \quad (321)$$

- Example: The point  $P = (11, 32)$  on the elliptic curve given by  $Y^2 = X^3 + 8$  modulo 35 can be viewed as the pair of points  $(1, 2)$  modulo 5 and  $(4, 4)$  modulo 7.
- By (321),  $\#\mathcal{E}(\mathbb{Z}_n) = \#\mathcal{E}(\mathbb{F}_p) \cdot \#\mathcal{E}(\mathbb{F}_q)$ .
- Both curves  $\mathcal{E}(\mathbb{F}_p)$  and  $\mathcal{E}(\mathbb{F}_q)$  are supersingular by (307) and so by (306),

$$\#\mathcal{E}(\mathbb{F}_p) = p + 1 \quad \text{and} \quad \#\mathcal{E}(\mathbb{F}_q) = q + 1. \quad (322)$$

- Thus  $[p + 1]P = O \pmod p$  and  $[q + 1]P = O \pmod q$ .

## Correctness

Write

$$de = 1 + k(p + 1)$$

for some integer  $k$ . Then

$$\begin{aligned} [d]C &= [de]P = [1 + k(p + 1)]P \\ &= P + [k(p + 1)]P = P + O = P \pmod{p}. \end{aligned}$$

Similarly,

$$[d]C = P \pmod{q}.$$

By (321) and the Chinese Remainder theorem, one obtains  $[d]C = P \pmod{n}$ . □

## Basic Attacks

- If Eve could factor  $n$  as  $pq$ , she would know  $(p+1)(q+1)$  and so could find  $d$  with  $ed \equiv 1 \pmod{(p+1)(q+1)}$ . Then she can decrypt  $m$  from  $C$  and  $d$  similarly to RSA.
- If Eve could find out  $d$ , she would be able to factor  $n$  with some probability similarly to RSA; see Washington (pages 183-184).

## Imbedding Plaintext

**Require:** Elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_p$  given by  $Y^2 = X^3 + AX + B$ ,  
prime  $p$ , message  $m$  expressed as number  $0 \leq m < p/100$

**Ensure:** Point  $P \in \mathcal{E}(\mathbb{F}_p)$  depending on  $m$

**for**  $j$  from 0 to 99 **do**

$x \leftarrow 100m + j$

$s \leftarrow x^3 + Ax + B.$

**if**  $s$  is a square mod  $p$  **then**

$P \leftarrow (x, \sqrt{s})$

**return**

**end if**

**end for**

- Decoding  $m$  from  $P = (x, y)$  by  $m = \lfloor x/100 \rfloor$ .
- The probability that  $s$  is a square is roughly  $1/2$ , since  $s \in \mathbb{F}_p^*$  is essentially random and  $\mathbb{F}_p^*$  is cyclic of even order.
- So the probability of not being able to find a point for  $m$  after trying 100 values is roughly  $2^{-100}$ .

## NIST Curves

NIST recommended 5 prime curves and 10 binary curves for optimal security and implementation efficiency:

- Five prime fields  $\mathbb{F}_p$  for primes  $p$  of size 192, 224, 256, 384, 521 bits. For each of these prime fields, one elliptic curve was recommended.
- Five binary fields  $\mathbb{F}_{2^n}$  for  $n$  equal to 163, 233, 283, 409, and 571. For each of these fields, one elliptic curve and one Koblitz curve were recommended.

## Discrete Logarithm

Elliptic curves over  $\mathbb{F}_{2^n}$  are particularly advantageous, since the arithmetic processors for the underlying field are easy to construct and relatively simple to implement for large  $n$ .

F.L. Bauer (2000).

## Discrete Log

- Analog of Diffie-Hellman
- Analog of Massey-Omura
- Analog of ElGamal
- Analog of Digital Signature Algorithm (DSA)
- EC integrated encryption scheme
- \*Trusted authority

## Discrete Log

Given an elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  and points  $P, Q$  of  $\mathcal{E}(\mathbb{F}_q)$ , where  $Q$  is a multiple of  $P$ .

The *discrete logarithm* of  $Q$  to base  $P$  is any integer  $x$  such that

$$Q = [x]P.$$

Write  $x = \log_P Q$  for the minimum  $x \geq 0$ .

## Analog of Diffie-Hellman – Protocol

- Alice and Bob agree on elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  and point  $P \in \mathcal{E}(\mathbb{F}_q)$  (public).
- Alice chooses secret integer  $a$ , computes  $P_A = [a]P$ , and sends  $P_A$  to Bob.
- Bob chooses secret integer  $b$ , computes  $P_B = [b]P$ , and sends  $P_B$  to Alice.
- Alice and Bob establish common key:
  - Alice computes  $Q_A = [a]P_B$ .
  - Bob computes  $Q_B = [b]P_A$ .
  - Then

$$\begin{aligned} Q_A &= [a]P_B = [a][b]P & (323) \\ &= [b][a]P = [b]P_A = Q_B \end{aligned}$$

is the common key,  $P_{A,B} = [ab]P$ .

## Diffie-Hellman Problem

Given  $P$ ,  $P_A$ , and  $P_B$  in  $\mathcal{E}(\mathbb{F}_q)$ , compute  $P_{A,B}$ .

- The eavesdropper Eve knows curve  $\mathcal{E}$ , field  $\mathbb{F}_q$ , point  $P$  (public), and points  $P_A, P_B$  (transmitted data).
- If Eve could solve discrete logs in  $\mathcal{E}(\mathbb{F}_q)$ , she would be able to use  $P$  and  $P_A$  to find  $a$ , or  $P$  and  $P_B$  to find  $b$ .
- Then by (323) Eve could compute

$$[a]P_B = P_{A,B} \quad \text{or} \quad [b]P_A = P_{A,B}. \quad (324)$$

## Decision Diffie-Hellman Problem

Given  $P$ ,  $P_A$ , and  $P_B$  in  $\mathcal{E}(\mathbb{F}_q)$ , and given  $Q \in \mathcal{E}(\mathbb{F}_q)$ , determine whether or not  $Q = P_{A,B}$ .

Suppose Eve receives an anonymous tip telling her  $P_{A,B}$ . Can Eve show that this information is sound?

For some curves, Eve eventually can ...

## Example

Consider the supersingular elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  with  $q \equiv 2 \pmod{3}$  given by  $Y^2 = X^3 + 1$  (see (307)).

- The field  $\mathbb{F}_{q^2}$  contains a primitive 3rd root of unity  $\xi$ , since the cyclic group  $\mathbb{F}_{q^2}^*$  has order  $q^2 - 1$  and  $q^2 \equiv 1 \pmod{3}$  implies  $3 \mid q^2 - 1$ .
- We have  $\xi \notin \mathbb{F}_q$ , since the cyclic group  $\mathbb{F}_q^*$  has order  $q - 1$  and  $q - 1 \not\equiv 0 \pmod{3}$  implies  $3 \nmid q - 1$ .
- Given a third root of unit  $\xi$ , the mapping

$$\phi : \mathcal{E}(\overline{\mathbb{F}}_q) \rightarrow \mathcal{E}(\overline{\mathbb{F}}_q) : (x, y) \mapsto (\xi x, y) \quad (325)$$

with  $\phi(O) = O$  is a group isomorphism; to prove this, use the addition law.

## Modified Weil Pairing

Define the *modified Weil pairing*

$$\tilde{e}_n(P_1, P_2) = e_n(P_1, \phi(P_2)), \quad (326)$$

where  $e_n$  is the usual Weil pairing (248) and  $P_1, P_2 \in \mathcal{E}[n]$ .

- $\tilde{e}_n$  is well-defined, since if  $P \in \mathcal{E}(\bar{\mathbb{F}}_q)$  has order  $n$ , then  $\phi(P)$  has also order  $n$ , since  $\phi$  is an isomorphism.
- Since the Weil pairing is bilinear and  $\phi$  is an isomorphism,

$$\begin{aligned} \tilde{e}_n([a]P_1, [b]P_2) &= e_n([a]P_1, \phi([b]P_2)) \\ &= e_n([a]P_1, [b]\phi(P_2)) \quad (327) \\ &= e_n(P_1, \phi(P_2))^{ab} \\ &= \tilde{e}_n(P_1, P_2)^{ab}. \end{aligned}$$

## Modified Weil Pairing

If  $P \in \mathcal{E}(\mathbb{F}_q)$  has order  $n$  and  $3 \nmid n$ , then  $\tilde{e}_n(P, P)$  is a primitive  $n$ -th root of unity.

### Proof (Sketch).

- The only relation of the form

$$[u]P = [v]\phi(P)$$

with integers  $u, v$  is the trivial relation:  $u, v \equiv 0 \pmod{n}$ .

- Thus  $\{P, \phi(P)\}$  is a basis of  $\mathcal{E}[n]$ .
- Hence,  $\tilde{e}_n(P, P) = e_n(P, \phi(P))$  is a primitive  $n$ -th root of unity as known from the Weil pairing.



## Example (cont'd)

- Assume  $3 \nmid n$ . Then as shown  $\tilde{e}_n(P, P) = \xi$  is a primitive  $n$ th root of unity.
- In view of the transmitted points  $P_A, P_B$ , we obtain by (327)

$$\tilde{e}_n(P_A, P_B) = \tilde{e}_n([a]P, [b]P) = \tilde{e}_n(P, P)^{ab} = \xi^{ab} \quad (328)$$

and in view of the common key  $P_{A,B}$ , we obtain by (327)

$$\tilde{e}_n(P, P_{A,B}) = \tilde{e}_n(P, [ab]P) = \tilde{e}_n(P, P)^{ab} = \xi^{ab}. \quad (329)$$

Thus

$$\tilde{e}_n(P_A, P_B) = \tilde{e}_n(P, P_{A,B}). \quad (330)$$

## Example (cont'd)

- In view of the anonymous tip  $Q = [k]P$  for some  $k$ , we obtain by (327)

$$\tilde{e}_n(P, Q) = \tilde{e}_n(P, [k]P) = \tilde{e}_n(P, P)^k = \xi^k. \quad (331)$$

- Eve computes both roots of unity,

$$\tilde{e}_n(P_A, P_B) = \xi^{ab} \quad \text{and} \quad \tilde{e}_n(P, Q) = \xi^k \quad (332)$$

If  $\xi^{ab} = \xi^k$ , i.e.,  $k \equiv ab \pmod{n}$ , then by (330) Eve may infer that  $Q = P_{A,B}$ .

## Tripartite Diffie-Hellman

- Alice, Bob, and Claire agree publically on a supersingular elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  given by  $Y^2 = X^3 + 1$  with  $q \equiv 2 \pmod{3}$ , and a point  $P \in \mathcal{E}(\mathbb{F}_q)$  of order  $n$  (large prime).
- Alice, Bob, and Claire choose secret integers  $a, b, c \pmod{n}$ , resp.
- Alice broadcasts  $[a]P$ , Bob broadcasts  $[b]P$ , and Claire broadcasts  $[c]P$ .
- Alice computes  $\tilde{e}_n([b]P, [c]P)^a$ , Bob computes  $\tilde{e}_n([a]P, [c]P)^b$ , and Claire computes  $\tilde{e}_n([a]P, [b]P)^c$ .
- Then by (327), all three users have computed the same root of unity,

$$\tilde{e}_n(P, P)^{abc}, \quad (333)$$

which can be used to produce a key.

## Massey-Omura Analog – Protocol

- Users agree on elliptic curve  $\mathcal{E}(\mathbb{F}_q)$ . Let  $N = \#\mathcal{E}(\mathbb{F}_q)$ .
- Each user takes secret random integer  $m_U$  with  $(m_U, N) = 1$ . Then by the extended Euclidean algorithm,

$$sm_U + rN = 1, \quad s, r \in \mathbb{Z}, \quad (334)$$

and so  $m_U^{-1} \equiv s \pmod{N}$ .

- Alice wants to send a message represented as a point  $P \in \mathcal{E}(\mathbb{F}_q)$  to Bob.
  - Alice computes  $P_A = [m_A]P$  and sends  $P_A$  to Bob.
  - Bob computes  $P_B = [m_B]P_A$  and sends  $P_B$  back.
  - Alice computes  $P'_A = [m_A^{-1}]P_B$  and sends  $P'_A$  back.
  - Bob computes  $P'_B = [m_B^{-1}]P'_A$ .

The Massey-Omura public key system is rarely used in practice.

## Massey-Omura Analog – Correctness

We have

$$P'_B = [m_B^{-1}m_A^{-1}m_Bm_A]P = P. \quad (335)$$

## Proof.

- We have  $m_A^{-1}m_A \equiv 1 \pmod{N}$  and so  $m_A^{-1}m_A = 1 + kN$  for some integer  $k$ .
- The group  $\mathcal{E}(\mathbb{F}_q)$  has order  $N$  and so  $[N]R = O$  for each point  $R \in \mathcal{E}(\mathbb{F}_q)$ .
- Thus  $[m_A^{-1}m_A]R = [1 + kN]R = [1]R + [k][N]R = R$  for each point  $R \in \mathcal{E}(\mathbb{F}_q)$ .
- Therefore,

$$\begin{aligned} P'_B &= [(m_B^{-1}m_B)(m_A^{-1}m_A)]P \\ &= [m_B^{-1}m_B][m_A^{-1}m_A]P \\ &= [m_B^{-1}m_B]P = P. \end{aligned}$$

## ElGamal Analog – Protocol

- Each user chooses an elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$ , point  $P \in \mathcal{E}(\mathbb{F}_q)$ , integer  $s$ , and computes  $B = [s]P$ . All data are public up to private key  $s$ .
- Alice wants to send a message  $m$  to Bob.
  - Alice downloads Bob's public key given by the pair  $(P, B)$ . Bob has private key  $s$ .
  - Alice expresses her message  $m$  by a point  $M \in \mathcal{E}(\mathbb{F}_q)$ .
  - Alice chooses a secret random integer  $k$ , computes  $R = [k]P$ ,  $S = M + [k]B$ , and sends  $(R, S)$  to Bob.
  - Bob decrypts by computing

$$M = S - [s]R. \quad (336)$$

Correctness:

$$\begin{aligned} S - [s]R &= (M + [k]B) - [s][k]P \\ &= M + [k][s]P - [s][k]P = M. \end{aligned}$$

## ElGamal Analog – Eavesdropper

- The eavesdropper Eve knows Bob's public key pair  $(P, B)$  and the points  $R, S$  (transmitted data).
- If Eve is able to calculate discrete logs, she can use  $P$  and  $B$  to find Bob's private key  $s$  and then decrypt  $S - [s]R = M$ .
- Suppose Alice uses the same key  $k = k'$  for two messages  $M$  and  $M'$ .

- Eve can recognize this because then

$$R = [k]P = [k']P = R'.$$

- Suppose  $M$  is a public announcement made public one day later, so Eve can find out  $M$ .
- Then Eve finds also the other message  $M'$ , since

$$M - S + S' = M - (M + [k]B) + (M' + [k']B) = M'.$$

The ElGamal public key system is rarely used in practice.

## Analog of Digital Signature Algorithm – Setup

Alice sets up her signature scheme:

- Alice chooses elliptic curve  $\mathcal{E}(\mathbb{F}_q)$ , where  $\#\mathcal{E}(\mathbb{F}_q) = fr$  with  $r$  large prime and  $f$  small integer.
- Alice choose point  $P \in \mathcal{E}(\mathbb{F}_q)$  of order  $r$ , secret integer  $a$ , and computes  $Q = [a]P$ .
- Alice makes public the quintuple

$$(\mathbb{F}_q, \mathcal{E}, r, P, Q). \quad (337)$$

No need to keep  $f$  secret as it can eventually be deduced from  $q$  and  $r$  using the Hasse bound (see section about group order).

The Digital Signature Algorithm (DSA) is the basis of the Digital Signature Standard (DSS).

## Analog of Digital Signature Algorithm – Signature

Alice signs the document  $m$ :

- Alice chooses random integer  $k$  with  $1 \leq k < r$  and computes

$$R = [k]P = (x, y). \quad (338)$$

- Alice computes

$$s = k^{-1}(h(m) + ax) \pmod{r}, \quad (339)$$

where  $h(m)$  is a hash value of  $m$ .

- The signed document is the triple

$$(m, R, s). \quad (340)$$

All users take the same cryptographic hash function  $h$ .

## Analog of Digital Signature Algorithm – Verification

Bob verifies the signature:

- Bob receives  $(m, R, s)$  and computes

$$u = s^{-1}h(m) \pmod r \quad \text{and} \quad v = s^{-1}x \pmod r.$$

- Bob computes  $V = [u]P + [v]Q$ .
- Bob declares the signature valid if  $V = R$ .

Correctness:

$$\begin{aligned} V &= [u]P + [v]Q = [s^{-1}h(m)]P + [s^{-1}x][a]P \\ &= [s^{-1}(h(m) + xa)]P \\ &= [k]P = R \text{ by (339).} \end{aligned}$$

The verification process requires two point multiplications, while the ElGamal Digital Signature system needs three point multiplications.

## EC Integrated Encryption Scheme (ECIES) – Setup

ECIES is a public key encryption system introduced by Bellare, Rogaway (2001).

- Each user chooses elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  and point  $A \in \mathcal{E}(\mathbb{F}_q)$  of large prime order  $N$ .
- Each user chooses secret integer  $s$  and computes  $B = [s]A$ .
- Each user has public key

$$(q, \mathcal{E}, N, A, B). \quad (341)$$

- Public data: cryptographic hash functions  $h_1, h_2$  and symmetric encryption function  $\gamma_k$  depending on a key  $k$ .

## EC Integrated Encryption Scheme (ECIES) – Encryption

Alice encrypts message  $m$  as follows:

- Alice downloads Bob's public key  $(q, \mathcal{E}, N, A, B)$ .
- Alice chooses random integer  $k$  with  $1 \leq k \leq N - 1$ .
- Alice computes points  $R = [k]A$  and  $Z = [k]B$ .
- Alice writes output of hash value  $h_1(R, Z)$  as pair  $(k_1, k_2)$ , where  $k_1$  and  $k_2$  have specific lengths.
- Alice computes ciphertext  $c = \gamma_{k_1}(m)$  and hash value  $t = h_2(c, k_2)$ .
- Alice sends  $(R, c, t)$  to Bob.

## EC Integrated Encryption Scheme (ECIES) – Decryption

Bob decrypts  $(R, c, t)$  as follows:

- Bob computes  $Z = [s]R$  using his secret key  $s$ .
- Bob computes  $h_1(R, Z)$  and writes the output as  $(k_1, k_2)$ .
- Bob computes  $t' = h_2(c, k_2)$ .
- If fingerprints  $t, t'$  are not equal, Bob rejects the ciphertext; otherwise, he continues.
- Bob computes  $m = \delta_{k_1}(c)$ , where  $\delta_k$  is the decryption function corresponding to  $\gamma_k$ ; i.e.,  $\delta_k \gamma_k$  is the identity mapping.

Correctness:

$$[s]R = [s][k]A = [k]B = Z.$$

## EC Integrated Encryption Scheme (ECIES) – Attacker

Attacker Adam can choose various ciphertexts and so force Bob to decrypt them:

- Adam can generate ciphertexts by choosing  $c$  and  $k'_2$  and then compute  $t' = h_2(c, k'_2)$ .
- But Adam does not know  $Z$  and so cannot use the same value  $k_2$  that Bob obtains from  $h_1(R, Z)$ .
- Therefore it is unlikely that  $t' = h_2(c, k'_2)$  and  $t = h_2(c, k_2)$  will be equal.
- So with high probability, Bob can reject the ciphertext using the fingerprint and hence does not make a decryption.

ECIES has the advantage over Massey-Omura, ElGamal and others that the message need not be represented as point on the curve.

## Trusted Authority

### Organization of trusted authority (TA):

- Each user has a public key based on its identity; e.g., email address.
- Authentication happens in the initial communication between user and TA.
- After this, the user is the only one who has the information to decrypt messages encrypted by its public key.

## Trusted Authority – Setup

Consider the elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_p$  with  $p \equiv 2 \pmod{3}$  given by  $Y^2 = X^3 + 1$  (see Diffie-Hellman).

- Let  $\xi \in \mathbb{F}_{p^2}$  be a primitive 3rd root of unity; we have  $\xi \notin \mathbb{F}_p$ , since  $\mathbb{F}_p^*$  has order  $p - 1$  and  $p - 1 \not\equiv 0 \pmod{3}$ .
- Reconsider the mapping

$$\phi : \mathcal{E}(\overline{\mathbb{F}}_{p^2}) \rightarrow \mathcal{E}(\overline{\mathbb{F}}_{p^2}) : (x, y) \mapsto (\xi x, y)$$

with  $\phi(O) = O$ , which is a group isomorphism.

- Reconsider the modified Weil pairing

$$\tilde{e}_n(P_1, P_2) = e_n(P_1, \phi(P_2)),$$

where  $e_n$  is the usual Weil pairing and  $P_1, P_2 \in \mathcal{E}[n]$ .  $\tilde{e}_n$  is well-defined, since if  $P \in \mathcal{E}(\overline{\mathbb{F}}_q)$  has order  $n$ , then  $\phi(P)$  has also order  $n$ .

## Trusted Authority – Setup

- If  $P \in \mathcal{E}(\mathbb{F}_p)$  has order  $n$  and  $3 \nmid n$ , then  $\tilde{e}_n(P, P)$  is a primitive  $n$ -th root of unity.
- The curve  $\mathcal{E}(\mathbb{F}_p)$  is supersingular by (307) and so by (306),  $\#\mathcal{E}(\mathbb{F}_p) = p + 1$ .
- Let  $p = 6\ell - 1$  for some prime  $\ell$ . Then for each  $P \in \mathcal{E}(\mathbb{F}_p)$ ,  $Q = [6]P$  has order  $\ell$  or 1. Indeed,

$$[\ell]Q = [6\ell]P = [p + 1]P = O.$$

- The following primes  $p$ ,  $3 \leq p \leq 1000$ , qualify:

11, 17, 29, 41, 101, 113, 137, 257, 281, 317, 353,  
401, 617, 641, 653, 677, 761, 821, 941, 977,

since  $11 = 6 \cdot 2 - 1$ ,  $17 = 6 \cdot 3 - 1$ ,  $29 = 6 \cdot 5 - 1$ , etc.

## Trusted Authority – Setup

TA sets up the system as follows:

- Chooses large prime  $p = 6\ell - 1$  for some prime  $\ell$ .
- Chooses point  $P \in \mathcal{E}(\mathbb{F}_p)$  of order  $\ell$ .
- Chooses hash functions  $h_1, h_2$ :
  - $h_1$  maps binary strings of arbitrary length to points of order  $\ell$  on  $\mathcal{E}(\mathbb{F}_p)$  (see Washington, Exercise 6.8).
  - $h_2$  maps  $\ell$ th roots of unity to binary strings of length  $n$ , where  $n$  is the message length.
- Chooses secret random value  $s \in \mathbb{F}_\ell^*$  and computes  $P_{\text{pub}} = [s]P$ .
- Makes  $p, h_1, h_2, n, P, P_{\text{pub}}$  public, keeps  $s$  secret.

## Trusted Authority – Private Key Setup

TA acts as follows when user with identity  $ID$  wants a private key:

- Computes  $Q_{ID} = h_1(ID)$ ; this is a point of order  $\ell$  on the curve.
- Computes  $D_{ID} = [s]Q_{ID}$ .
- After verifying that  $ID$  is the identification of the user with whom it is communicating, TA sends  $D_{ID}$  to the user.

$D_{ID}$  is the user's private key.

## Trusted Authority – Message Encryption

Alice wants to send message  $m$  to Bob.

- Looks up Bob's identity, such as  $ID = \text{bob(at)tuhh.de}$  as binary string, and computes  $Q_{ID} = h_1(ID)$ .
- Chooses random value  $r$  with  $1 \leq r \leq \ell - 1$ .
- Computes  $g_{ID} = \tilde{e}_\ell(Q_{ID}, P_{\text{pub}})$ .
- Computes the ciphertext pair

$$c = ([r]P, m \oplus h_2(g_{ID}^r)),$$

where  $\oplus$  denotes the Boolean XOR operation, and sends it to Bob.

## Trusted Authority – Message Decryption

Bob decrypts the ciphertext  $(u, v)$  as follows:

- Uses his private key  $D_{\text{ID}}$  to compute  $h_{\text{ID}} = \tilde{e}_{\ell}(D_{\text{ID}}, u)$ .
- Computes  $m' = v \oplus h_2(h_{\text{ID}})$ .

Correctness:

$$\begin{aligned} \tilde{e}_{\ell}(D_{\text{ID}}, u) &= \tilde{e}_{\ell}([s]Q_{\text{ID}}, [r]P) = \tilde{e}_{\ell}(Q_{\text{ID}}, P)^{sr} \\ &= \tilde{e}_{\ell}(Q_{\text{ID}}, P_{\text{pub}})^r = g_{\text{ID}}^r. \end{aligned}$$

Thus

$$\begin{aligned} m' &= v \oplus h_2(h_{\text{ID}}) = v \oplus h_2(\tilde{e}_{\ell}(D_{\text{ID}}, u)) \\ &= (m \oplus h_2(g_{\text{ID}}^r)) \oplus h_2(g_{\text{ID}}^r) = m. \end{aligned}$$

## Attacking Discrete Log

There is no provable lower bound for the amount of work of a cryptanalyst analyzing a public-key cryptosystem.

Arto Salomaa (1990)

## Attacking Discrete Log

- Complete enumeration
- Baby-step, giant-step
- Pollard's rho method
- Pohlig-Hellman method
- MOV attack
- Index calculus

## Complete Enumeration

The simplest attacking method is complete enumeration.

**Require:** Given elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$ , points  $P, Q$  on  $\mathcal{E}(\mathbb{F}_q)$ , where  $Q$  is a multiple of  $P$ , integer  $N$  is the order of  $G = \langle P \rangle$ .

**Ensure:** Integer  $k$  with  $Q = [k]P$ .

```

for  $k \leftarrow 1$  to  $N$  do
  if  $Q = [k]P$  then
    return  $k$ 
  end if
end for

```

This attack is extremely time-consuming. The other attacks here are much faster.

## Baby-Step Giant-Step Algorithm

Given elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  and points  $P, Q$  on  $\mathcal{E}(\mathbb{F}_q)$ , where  $Q = [k]P$  is a multiple of  $P$  for some integer  $k$ .

Let  $G = \langle P \rangle$  with order  $N$  (known).

### Procedure Outline (Shanks, 1971)

- Fix an integer  $m \geq \sqrt{N}$  and compute the point  $[m]P$ .
- Generate a list of points  $[i]P$ ,  $0 \leq i < m$ .
- Compute the points  $Q - [jm]P$ ,  $0 \leq j < m$ , until a match with an element of the stored list is found.
- If  $[i]P = Q - [jm]P$  is a match, then  $Q = [k]P$  with  $k \equiv i + jm \pmod{N}$ .

Time complexity  $O(\sqrt{N})$ .

## Baby-Step Giant-Step Algorithm

Correctness:

- Since  $m^2 > N$ , the answer  $k$  satisfies  $0 \leq k < m^2$ .
- Write

$$k = k_0 + mk_1 \quad (342)$$

with  $k \equiv k_0 \pmod{m}$ ,  $0 \leq k_0 < m$ , and  $k_1 = (k - k_0)/m$   
with  $0 \leq k_1 < m$ , since

$$k_1 \leq (k - k_0)/m < (m^2 - 0)/m = m.$$

- If  $i = k_0$  and  $j = k_1$ , there is a match:

$$\begin{aligned} Q - [k_1 m]P &= [k]P - [k_1 m]P & (343) \\ &= [k - k_1 m]P = [k_0]P. \end{aligned}$$

## Baby-Step Giant-Step Algorithm

**Require:** Elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$ , points  $P, Q \in \mathcal{E}(\mathbb{F}_q)$ , where  $Q$  is a multiple of  $P$ , integer  $N$  is the order of  $G = \langle P \rangle$ , list  $L = []$ .

**Ensure:** Integer  $k$  with  $Q = [k]P$ .

$m \leftarrow \lceil \sqrt{N} \rceil$

**for**  $i = 0$  to  $m - 1$  **do**

    Append  $(i, [i]P)$  to list  $L$

**end for**

**for**  $j = 0$  to  $m - 1$  **do**

**if**  $Q - [jm]P$  matches  $[i]P$  in list  $L$  **then**

$k \leftarrow i + jm \pmod{N}$

**return**  $k$

**end if**

**end for**

## Baby-Step Giant-Step Algorithm

- *Baby step*: point addition

$$P + [i - 1]P \mapsto [i]P. \quad (344)$$

- *Giant step*: point addition

$$-[mP] + (Q - [(j - 1)m]P) \mapsto Q - [jm]P. \quad (345)$$

- The group order  $N$  is not needed, only an upper bound as given by the Hasse bound (274),

$$m^2 \geq q + 1 + 2\sqrt{q}. \quad (346)$$

## Example

Consider the elliptic curve  $\mathcal{E}(\mathbb{F}_{41})$  given by  $Y^2 = X^3 + 2X + 1$  and let  $P = (0, 1)$ ,  $Q = (30, 40)$ .

- By the Hasse bound,  $\#\mathcal{E}(\mathbb{F}_{41}) \leq 41 + 1 + 2\sqrt{41} = 58.806$ .  
Take  $m = 8$ .

- Baby-step list  $[i]P$ ,  $1 \leq i \leq 7$ ,

$$(0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), \underline{(26, 9)}.$$

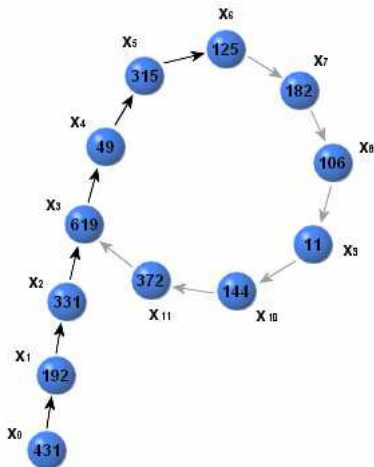
- Giant-step list  $Q - [8j]P$  for  $j = 0, 1, 2$  gives

$$(30, 40), (9, 25), \underline{(26, 9)}.$$

So there is a match for  $i = 7$  and  $j = 2$ .

- Thus  $Q = (30, 40) = [7 + 2 \cdot 8]P = [23]P$  and hence  $k = 23$ .

## Pollard's rho Method



## Pollard's rho Method

Given finite group  $G$  of order  $N$  and  $P, Q \in G$ , where  $Q$  is a multiple of  $P$ . Find an integer  $k$  with  $Q = [k]P$ .

### Procedure Outline (Pollard, 1978)

- Choose function  $f : G \rightarrow G$  that behaves randomly.
- Start with random  $P_0 \in G$  and iterate  $P_{i+1} = f(P_i)$ .
- Since  $G$  is finite, there are  $i_0 < j_0$  such that  $P_{i_0} = P_{j_0}$ . Then  $P_{i_0+1} = f(P_{i_0}) = f(P_{j_0}) = P_{j_0+1}$ . More generally,

$$P_{i_0+\ell} = P_{j_0+\ell}, \quad \ell \geq 0. \quad (347)$$

- The sequence  $(P_i)$  is periodic with period  $j_0 - i_0$  (or a divisor of  $j_0 - i_0$ ).
- The (smallest) equality  $P_{i_0} = P_{j_0}$  can be expected after  $O(\sqrt{N})$  steps.
- Use Floyd's algorithm for cycle detection.

## Pollard's rho Method

Choice of suitable function  $f$ :

- Divide  $G$  into  $r$  disjoint subsets  $S_1, \dots, S_r$  of approximately equal size, say  $r = 20$ .
- Choose  $2r$  random integers  $a_i, b_i \pmod N$  and put

$$M_i = [a_i]P + [b_i]Q. \quad (348)$$

- Define

$$f(g) = g + M_i, \quad \text{if } g \in S_i. \quad (349)$$

The iteration of  $f$  provides a random walk in  $G$  with steps given by the  $M_i$ 's.

## Pollard's rho Method

- Choose random integers  $a_0, b_0 \pmod N$  and put

$$P_0 = [a_0]P + [b_0]Q. \quad (350)$$

- Calculate the sequence  $(P_j)_{j \geq 0}$  and keep track of the expression of the points  $P_j$  in terms of  $P$  and  $Q$ .
- If  $P_j = [u_j]P + [v_j]Q$  and  $f(P_j) = P_{j+1} = P_j + M_i$ , then

$$P_{j+1} = [u_j + a_i]P + [v_j + b_i]Q \quad (351)$$

with  $(u_{j+1}, v_{j+1}) = (u_j, v_j) + (a_i, b_i)$ .

## Pollard's rho Method

- If there is a match  $P_{j_0} = P_{i_0}$ , then

$$[u_{j_0}]P + [v_{j_0}]Q = [u_{i_0}]P + [v_{i_0}]Q \quad (352)$$

and so

$$[u_{i_0} - u_{j_0}]P = [v_{j_0} - v_{i_0}]Q. \quad (353)$$

- If  $(v_{j_0} - v_{i_0}, N) = d$ , then  $(v_{j_0} - v_{i_0}, N/d) = 1$  and so

$$k \equiv (v_{j_0} - v_{i_0})^{-1}(u_{i_0} - u_{j_0}) \pmod{N/d}. \quad (354)$$

- Since  $1 \leq k \leq N$ , this gives  $d$  choices for  $k$ :  $k, 2k, \dots, dk$ . Often  $d$  is small and so all possibilities can be tried to get  $Q = [k]P$ .
- In cryptography,  $N$  is often prime and so  $d = 1$  or  $d = N$ . If  $d = N$ , we need to start over; otherwise,  $d = 1$  and we obtain directly  $k$ .

## Pollard's rho Method

**Require:** Elliptic curve  $\mathcal{E}(\mathbb{F}_q)$ , points  $P, Q \in \mathcal{E}(\mathbb{F}_q)$ , where  $Q$  is a multiple of  $P$ , integer  $N = \#\mathcal{E}(\mathbb{F}_q)$ , point  $P_0$ , partition  $S_1, \dots, S_r$  of  $G = \langle P \rangle$ , and function  $f : \mathcal{E}(\mathbb{F}_q) \rightarrow \mathcal{E}(\mathbb{F}_q)$ .

**Ensure:** Integer  $k$  with  $Q = [k]P$ .

noMatch  $\leftarrow$  TRUE

$i \leftarrow 0$

**while** noMatch **do**

$i \leftarrow i + 1$  {Use Floyd's algorithm}

$P_i \leftarrow f(P_{i-1})$

$P_{2i} \leftarrow f(f(P_{2(i-1)}))$

**if**  $P_i = P_{2i}$  **then**

        noMatch  $\leftarrow$  FALSE

**end if**

**end while**

Compute  $k$  from  $P_i$  and  $P_{2i}$ .

## Example

Consider the elliptic curve  $\mathcal{E}(\mathbb{F}_{1093})$  given by  $Y^2 = X^3 + X + 1$  and points  $P = (0, 1)$  with order 1067 and  $Q = (431, 959)$ . Find an integer  $k$  with  $Q = [k]P$ .

- Let  $r = 3$  and put

$$\begin{aligned} P_0 &= [3]P + [5]Q, & M_0 &= [4]P + [3]Q, \\ M_1 &= [9]P + [17]Q, & M_2 &= [19]P + [6]Q. \end{aligned}$$

- Define  $f : \mathcal{E}(\mathbb{F}_{1093}) \rightarrow \mathcal{E}(\mathbb{F}_{1093})$  by

$$f(x, y) = (x, y) + M_i, \quad \text{if } x \equiv i \pmod{3},$$

where  $x$  is an integer with  $0 \leq x < 1093$ . For instance,

$$f(P_0) = P_0 + M_2 = (727, 589)$$

since  $P_0 = (326, 69)$  and  $326 \equiv 2 \pmod{3}$ .

## Example (cont'd)

- Compute the sequence  $(P_j)$ ,

$$\begin{array}{lll}
 P_0 = (326, 69), & P_1 = (727, 589), & P_2 = (560, 365), \\
 P_3 = (1070, 260), & P_4 = (473, 903), & \underline{P_5 = (1006, 951)}, \\
 \dots & & \\
 P_{57} = (895, 337), & \underline{P_{58} = (1006, 951)}, & P_{59} = (523, 938), \\
 \dots & & 
 \end{array}$$

There is a match:  $P_5 = P_{58}$ .

- By keeping track of the coefficients of  $P$  and  $Q$ ,

$$P_5 = [88]P + [46]Q \quad \text{and} \quad P_{58} = [685]P + [620]Q.$$

- Thus

$$O = P_{58} - P_5 = [597]P + [574]Q.$$

Then  $O = [597]P + [574][k]P = [597 + k \cdot 574]P$ .

## Example (cont'd)

- Since  $P$  has order 1067,

$$597 + k \cdot 574 \equiv 0 \pmod{1067}$$

or  $597 \equiv k(-574) \pmod{1067}$ . We have

$$(-574)^{-1} \cdot 597 \equiv 499 \pmod{1067}$$

and so  $Q = [499]P$  with  $k = 499$ .

- The points  $P_0, P_1, \dots, P_{58}$  need to be stored until a match is found:  $P_5 = P_{58}$ . It can be done better ...
- By Floyd's cycle detection method, compute the pairs  $(P_i, P_{2i})$  and store only the current pair. Then for  $i = 53$  there is a match  $P_{53} = P_{106}$  with

$$[620]P + [557]Q = P_{53} = P_{106} = [1217]P + [1131]Q.$$

Thus  $[597]P + [574]Q = O$  and hence  $k = 499$ .

## Floyd's Cycle Detection Algorithm (1969)

Given finite set  $S$ , function  $f : S \rightarrow S$ , and  $x_0 \in S$ .

- Define the sequence  $(x_i)$  as follows,

$$x_{i+1} = f(x_i), \quad i \geq 0. \quad (355)$$

- Since  $S$  is finite, there are smallest non-negative integers  $\mu$  (initial segment) and  $\lambda$  (period) such that

$$x_\mu = x_{\lambda+\mu}. \quad (356)$$

Example:  $S = \mathbb{Z}_{11}$ ,  $f(x) = (x^2 + 1) \pmod{11}$ , and  $x_0 = 3$ . The sequence is

$$3, 10, 2, 5, 4, 6, 4, 6, 4, 6, \dots$$

and so  $\mu = 4$  and  $\lambda = 2$ , i.e.,  $x_4 = 4 = x_{4+2}$ .

## Floyd's Cycle Detection Algorithm

- By (356), for each  $i \geq \mu$  and  $k \geq 0$ ,

$$x_i = x_{i+k\lambda}, \quad (357)$$

since looping  $k$  times the cycle of length  $\lambda$  ends in the same element of the cycle.

- By (357), we have

$$i = k\lambda \geq \mu \text{ for some } k \iff x_i = x_{2i}. \quad (358)$$

- Existence of  $i$  in (358): Take the smallest  $i \geq \mu$  which has the form  $i = k\lambda$  inside the cycle. Then by (357),  $x_i = x_{2i}$ .

Example:  $\mu = 5$  and  $\lambda = 3$ . Then  $i = 2 \cdot 3 = 6 \geq 5$  and  $2i = 12 = 6 + 2 \cdot 3$ .

## Floyd's Cycle Detection Algorithm

Floyd's algorithm:

- 1 Compute simultaneously  $(x_i)$  and  $(x_{2i})$  to find the minimal  $i_0 > 0$  with  $x_{i_0} = x_{2i_0}$ ; it is only necessary to store the current elements  $x_i$  and  $x_{2i}$ .
- 2 Find in  $(x_i)$  the first repeated element  $x_\mu$ ,  $\mu \leq i_0$ .
- 3 Find in  $(x_i)$  the shortest repeated cycle  $x_{\mu+\lambda}$ ,  $\lambda \geq 1$ .

Example: Let  $S = \mathbb{Z}_{11}$ ,  $f(x) = (x^2 + 1) \bmod 11$ , and  $x_0 = 3$ .

$i$	0	1	2	3	<b>4</b>	5	6
$x_i$	3	10	2	5	4	6	4
$x_{2i}$	3	2	4	4	4	4	4

## Pohlig-Hellman Method (1978)

Given finite group  $G$  and  $P, Q \in G$ , where  $P$  has order  $N$  and  $Q$  is a multiple of  $P$ . Find an integer  $k$  with  $Q = [k]P$ .

- Suppose  $N$  has known prime factorization

$$N = \prod_i p_i^{e_i}. \quad (359)$$

- Idea: Find  $k \bmod p_i^{e_i}$  for each  $i$ , use the Chinese Remainder theorem to combine these and obtain  $k \bmod N$ .
- For prime  $p$  with  $p \mid N$ , write  $k$  in its base  $p$  expansion

$$k = k_0 + k_1p + k_2p^2 + \dots \quad (360)$$

with  $0 \leq k_i < p$ .

- Idea: Evaluate  $k \bmod p^e$  by successively determining  $k_0, \dots, k_{e-1}$ , where  $p^e$  is the exact power of  $p$  dividing  $N$ .

## Pohlig-Hellman Method

For each prime  $p$  with  $p^e$  being the exact power of  $p$  dividing  $N$ :

- 1 Compute list  $L = \{[jN/p]P \mid 0 \leq j \leq p - 1\}$ .
- 2 Determine  $k_0$  with  $[N/p]Q = [k_0N/p]P$  using  $L$ .
- 3 If  $e = 1$ , stop; otherwise continue.
- 4 Suppose  $k_0, \dots, k_{r-1}$  and  $Q_1, \dots, Q_{r-1}$  have already been computed.
- 5 Let  $Q_r = Q_{r-1} - [k_{r-1}p^{r-1}]P$ .
- 6 Determine  $k_r$  with  $[N/p^{r+1}]Q_r = [k_rN/p]P$  using  $L$ .
- 7 If  $r = e - 1$ , stop; otherwise, increment  $r$  and return to 4.

Then

$$k \equiv k_0 + k_1p + \dots + k_{e-1}p^{e-1} \pmod{p^e}.$$

## Pohlig-Hellman Method

Correctness:

- We have

$$\begin{aligned} [N/p]Q &= [(N/p)k]P = [(N/p)(k_0 + k_1p + \dots)]P \\ &= [k_0N/p]P + [(k_1 + k_2p + \dots)N]P \\ &= [k_0N/p]P, \end{aligned}$$

since  $[N]P = O$ . Thus step 2 finds  $k_0$ .

- Then

$$Q_1 = Q - [k_0]P = [k_1p + k_2p^2 + \dots]P$$

and so

$$\begin{aligned} [N/p^2]Q_1 &= [(k_1 + k_2p + \dots)N/p]P \\ &= [k_1N/p]P + [(k_2 + k_3p + \dots)N]P \\ &= [k_1N/p]P, \end{aligned}$$

since  $[N]P = O$ . Thus step 6 finds  $k_1$ , and so on.

## Pohlig-Hellman Method

**Require:** Elliptic curve  $\mathcal{E}(\mathbb{F}_q)$ , points  $P, Q \in \mathcal{E}(\mathbb{F}_q)$ , where  $P$  has order  $N$  and  $Q$  is a multiple of  $P$ , prime factorization

$$N = \prod_{i=1}^m p_i^{e_i}.$$

**Ensure:** Integer  $k$  with  $Q = [k]P$ .

$$Q_0 \leftarrow Q$$

**for**  $i = 1$  to  $m$  **do**

$$L \leftarrow \{[jN/p_i]P \mid 0 \leq j \leq p_i - 1\}.$$

Find  $k_0$  with  $[N/p_i]Q = [k_0N/p_i]P$  using  $L$ .

**for**  $r = 1$  to  $e_i - 1$  **do**

$$Q_r \leftarrow Q_{r-1} - [k_{r-1}p_i^{r-1}]P$$

Find  $k_r$  with  $[N/p_i^{r+1}]Q_r = [k_rN/p_i]P$  using  $L$ .

**end for**

$$k^{(i)} \leftarrow k_0 + k_1p_i + \dots + k_{e_i-1}p_i^{e_i-1}$$

**end for**

Use the Chinese Remainder theorem to obtain  $k \pmod N$  from  $k^{(i)} \pmod{p_i^{e_i}}$ ,  $1 \leq i \leq m$ .

## Example

Consider the elliptic curve  $\mathcal{E}(\mathbb{F}_{599})$  given by  $Y^2 = X^3 + 1$ .

$P = (60, 19)$  has order  $N = 600$  and  $Q = (277, 239)$ . Find integer  $k$  with  $Q = [k]P$ .

- Prime factorization  $600 = 2^3 \cdot 3 \cdot 5^2$ .
- Compute  $k \bmod 8$ ,  $\bmod 3$ , and  $\bmod 25$ , and combine the results by the Chinese Remainder theorem to obtain  $k \bmod 600$ .

## Example (cont'd)

Computation  $k \bmod 8$ :

- Compute list

$$L = \{[0 \cdot N/2]P = O, [1 \cdot N/2]P = (598, 0)\}.$$

- Since  $[N/2]Q = O = [0 \cdot N/2]P$ , we have  $k_0 = 0$ . Thus

$$Q_1 = Q - [0]P = Q.$$

- Since  $[N/4]Q_1 = [150]Q_1 = (598, 0) = [1 \cdot N/2]P$ , we have  $k_1 = 1$ . Thus

$$Q_2 = Q_1 - [1 \cdot 2]P = (35, 243).$$

- Since  $[N/8]Q_2 = [75]Q_2 = O = [0 \cdot N/2]P$ , we have  $k_2 = 0$ .
- Therefore,

$$k = 0 + 1 \cdot 2 + 0 \cdot 4 \equiv 2 \pmod{8}.$$

## Example (cont'd)

Computation  $k \bmod 3$ :

- Compute list  $L$ :

$$[0 \cdot N/3]P = O, [1 \cdot N/3]P = (0, 1), [2 \cdot N/3]P = (0, 598).$$

- Since  $[N/3]Q = (0, 598) = [2 \cdot N/3]P$ , we have  $k_0 = 2$ .
- Therefore,

$$k \equiv 2 \pmod{3}.$$

## Example (cont'd)

Computation  $k \bmod 25$ :

- Compute list  $L$ :

$$[0 \cdot N/5]P = O, [1 \cdot N/5]P = (84, 179),$$

$$[2 \cdot N/5]P = (491, 134), [3 \cdot N/5]P = (491, 465),$$

$$[4 \cdot N/5]P = (84, 420).$$

- Since  $[N/5]Q = (84, 179) = [1 \cdot N/5]P$ , we have  $k_0 = 1$ .

Thus

$$Q_1 = Q - [1]P = (130, 129).$$

- Since  $[N/25]Q_1 = (491, 465) = [3 \cdot N/5]P$ , we have  $k_1 = 3$ .

- Therefore,

$$k = 1 + 3 \cdot 5 \equiv 16 \pmod{25}.$$

## Example (cont'd)

### Simultaneous congruences

$$k \equiv 2 \pmod{8},$$

$$k \equiv 2 \pmod{3},$$

$$k \equiv 16 \pmod{25}.$$

By the Chinese Remainder theorem,  $k = 266$  is uniquely determined modulo 600.

## Pohlig-Hellman Method

- The method works well if all prime numbers dividing  $N$  are small.
- If  $p$  is a large prime factor, it will be hard to list all elements of  $L$ .
- For cryptographic reasons (discrete log), the group order should contain a large prime factor.

## The MOV Attack

- Introduced by Menezes, Okamoto, Vanstone (1990).
- Uses Weil pairing to reduce the discrete log problem in  $\mathcal{E}(\mathbb{F}_q)$  to one in  $\mathbb{F}_{q^m}^*$ .
- Discrete log problem in  $\mathbb{F}_{q^m}^*$  can be attacked more efficiently (index calculus).
- For supersingular curves, the discrete log problem reduces to one in smaller group ( $m = 2$ ).

## The MOV Attack

Given elliptic curve  $\mathcal{E}$  over  $\mathbb{F}_q$  and  $P, Q \in \mathcal{E}(\mathbb{F}_q)$ , where  $N$  is the order of  $P$  and  $(N, q) = 1$ . Find an integer  $k$  with  $Q = [k]P$ .

There exists an integer  $k$  such that

$$Q = [k]P \iff [N]Q = O \text{ and } e_N(P, Q) = 1. \quad (361)$$

## Proof.

- Let  $Q = [k]P$ . Then  $[N]Q = [N][k]P = [k][N]P = O$ .  
Moreover,

$$e_N(P, Q) = e_N(P, [k]P) = e_N(P, P)^k = 1^k = 1.$$

- Let  $[N]Q = O$  and  $e_N(P, Q) = 1$ . Then  $Q \in \mathcal{E}[N]$ . Since  $(N, q) = 1$ , by (214),  $E[N] \simeq \mathbb{Z}_N \oplus \mathbb{Z}_N$ . Choose  $R$  such that  $\{P, R\}$  is a basis of  $\mathcal{E}[N]$ . Then there are integers  $a, b$  with

$$Q = [a]P + [b]R.$$

Since  $\{P, R\}$  is a basis of  $\mathcal{E}[N]$ ,  $\xi = e_N(P, R)$  is a primitive  $N$ -th root of unity and so

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, R)^b = 1^a \xi^b = \xi^b.$$

Thus  $b \equiv 0 \pmod{N}$  and so  $[b]R = O$ . Hence,  $Q = [a]P$ .  $\square$

## The MOV Attack

- All points of  $\mathcal{E}[N]$  have coordinates in

$$\bar{\mathbb{F}}_q = \bigcup_{k \geq 1} \mathbb{F}_{q^k}.$$

Since the set  $\mathcal{E}[N]$  is finite, there exists  $m \geq 1$  such that

$$E[N] \subset \mathcal{E}(\mathbb{F}_{q^m}).$$

- It follows that for the set of  $N$ -th roots of unity  $U_N$ ,

$$U_N \subset \mathbb{F}_{q^m}^*.$$

- All calculations will be made in  $\mathbb{F}_{q^m}$ .

## Procedure Outline

- Choose random point  $T \in \mathcal{E}(\mathbb{F}_{q^m})$ .
- Compute the order  $M$  of  $T$ .
- Let  $d = (M, N)$  and  $T_1 = [M/d]T$ . Then  $T_1$  has order  $d$  which divides  $N$ , so  $T_1 \in \mathcal{E}[N]$ .
- Compute  $\xi_1 = e_N(P, T_1)$  and  $\xi_2 = e_N(Q, T_1)$ . Then  $\xi_1, \xi_2$  are in  $U_d \subset \mathbb{F}_{q^m}^*$ , since  $\xi_1^d = e_N(P, [d]T_1) = e_N(P, O) = 1$  and  $\xi_2^d = e_N(Q, [d]T_1) = e_N(Q, O) = 1$ .

- We have

$$\xi_2 = e_N(Q, T_1) = e_N([k]P, T_1) = e_N(P, T_1)^k = \xi_1^k$$

- Solve the discrete log problem  $\xi_2 = \xi_1^k$  in  $\mathbb{F}_{q^m}^*$ . This gives  $k \pmod d$ .
- Repeat with random points  $T$  until the lcm of the various  $d$ 's obtained is  $N$ . This gives  $k \pmod N$ .

## The MOV Attack

Let  $\mathcal{E}$  be an elliptic curve over  $\mathbb{F}_q$ , let  $t = q + 1 - \#\mathcal{E}(\mathbb{F}_q) = 0$ , and let  $N \geq 1$ . If there exists a point  $P \in \mathcal{E}(\mathbb{F}_q)$  of order  $N$ , then  $\mathcal{E}[N] \subset \mathcal{E}(\mathbb{F}_{q^2})$ .

Note: An elliptic curve over  $\mathbb{F}_q$  with  $q = p^r$  is supersingular if  $t \equiv 0 \pmod p$ . This is equivalent to  $t = 0$  when  $q = p \geq 5$ .

## Proof.

- The Frobenius endomorphism  $\phi_q$  fulfills  $\phi_q^2 - [t]\phi_q + [q] = 0$ . Since  $t = 0$ , we obtain

$$\phi_q^2 + [q] = 0.$$

- Let  $P \in \mathcal{E}[N]$  have order  $N$  and let  $\#\mathcal{E}[N] = q + 1$ . Then  $N \mid q + 1$  or  $-q \equiv 1 \pmod{N}$ . Thus

$$\phi_q^2(P) = -[q]P = [1]P = P.$$

But by (267),  $\phi_q^2(P) = P$  is equivalent to  $P \in \mathcal{E}(\mathbb{F}_{q^2})$ .



## Index Calculus

Given prime  $p$  and generator  $g$  of cyclic group  $\mathbb{F}_p^*$ .

- Each  $h \in \mathbb{F}_p^*$  can be written as  $h = g^k$  for some integer  $k$  which is uniquely determined mod  $p - 1$ .
- Let  $k = \log_g(h)$  denote the *discrete logarithm* of  $h$  w.r.t.  $g$  and  $p$ ; i.e.,

$$g^{\log_g(h)} \equiv h \pmod{p}. \quad (362)$$

- For nonzero group elements  $h_1, h_2$ ,

$$g^{\log_g(h_1 h_2)} \equiv h_1 h_2 \equiv g^{\log_g(h_1) + \log_g(h_2)} \pmod{p} \quad (363)$$

and so

$$\log_g(h_1 h_2) \equiv \log_g(h_1) + \log_g(h_2) \pmod{p - 1}. \quad (364)$$

## Example

Let  $p = 1217$ . The cyclic group  $\mathbb{F}_{1217}^*$  has generator  $g = 3$ . Solve

$$3^k \equiv 37 \pmod{1217}.$$

Outline:

- Choose factor basis  $B = \{2, 3, 5, 7, 11, 13\}$ .
- Find relations of the form

$$3^x = \pm \text{product of some primes in } B \pmod{1217}.$$

- Compute  $3^j \cdot 37 \pmod{1217}$  for several random values  $j$  until an integer is obtained that factors into a product of primes in  $B$ .

## Example (cont'd)

Find relations of the form  $3^x \equiv \pm \text{product of primes in } B \pmod{p}$ :

$$3^1 \equiv 3 \pmod{1217},$$

$$3^{24} \equiv -2^2 \cdot 7 \cdot 13 \pmod{1217},$$

$$3^{25} \equiv 5^3 \pmod{1217},$$

$$3^{30} \equiv -2 \cdot 5^2 \pmod{1217},$$

$$3^{54} \equiv -5 \cdot 11 \pmod{1217},$$

$$3^{87} \equiv 13 \pmod{1217},$$

and  $3^{(p-1)/2} \equiv -1 \pmod{1217}$  with  $(p-1)/2 = 608$ .

## Example (cont'd)

Convert congruences into discrete logs writing  $L(h) = \log_g(h)$ :

$$1 \equiv L(3) \pmod{1216},$$

$$24 \equiv 608 + 2L(2) + L(7) + L(13) \pmod{1216},$$

$$25 \equiv 3L(5) \pmod{1216},$$

$$30 \equiv 608 + L(2) + 2L(5) \pmod{1216},$$

$$54 \equiv 608 + L(5) + L(11) \pmod{1216},$$

$$87 \equiv L(13) \pmod{1216},$$

and  $L(-1) = (p-1)/2 = 608$ .

## Example (cont'd)

These congruences yield the discrete logs of the elements of the factor basis:

$$L(3) \equiv 1 \pmod{1216},$$

$$L(5) \equiv 819 \pmod{1216},$$

$$L(13) \equiv 87 \pmod{1216},$$

$$L(2) \equiv 216 \pmod{1216},$$

$$L(11) \equiv 1059 \pmod{1216},$$

$$L(7) \equiv 113 \pmod{1216}.$$

For instance,  $25 \equiv 3L(5) \pmod{1216}$  and so

$$L(5) \equiv 3^{-1} \cdot 25 \equiv 811 \cdot 25 \equiv 819 \pmod{1216}.$$

Moreover,  $30 \equiv 608 + L(2) + 2L(5) \pmod{1216}$  and so

$$L(2) \equiv 30 - 608 - 2 \cdot 819 \equiv 216 \pmod{1216}.$$

## Example (cont'd)

Compute  $3^j \cdot 37 \pmod{1217}$  for several random values  $j$  until an integer is obtained that factors into a product of primes in  $B$ .

Here we find for  $j = 16$ ,

$$3^{16} \cdot 37 \equiv 616 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}.$$

Thus

$$L(37) \equiv 3L(2) + L(7) + L(11) - 16L(3) \equiv 588 \pmod{1216}.$$

Hence,

$$3^{588} \equiv 37 \pmod{1217}.$$

## Index Calculus

- The choice of the factor basis  $B$  is important.
- Good method for producing relations of the form

$$g^x \equiv \text{product of primes in } B \pmod{p}$$

is the quadratic sieve with subexponential running time  $O(\exp(\sqrt{2 \ln p \ln \ln p}))$ .

- The presented methods for attacking discrete logs for elliptic curves over  $\mathbb{F}_p$  have exponential running time  $O(\sqrt{p})$  with  $\sqrt{p} = \exp(\frac{1}{2} \ln p)$ .
- The index calculus can be generalized to the algebraic number field sieve using algebraic number theory.
- There is an analog of the index calculus for groups given by hyperelliptic curves.

## \* Primality Testing

The problems of factorization and primality testing are related, but very different in nature. The largest announced factorization up to the year 2007 was of an integer with 200 digits. However, it was at that time possible to prove primality of primes of several thousand digits.

Lawrence C. Washington (2008).

## Primality Testing

Prove that a number  $n$  is composite without presenting a factor:

- Fermat's Little theorem says that if  $n$  is prime and  $a$  is any integer with  $(a, n) = 1$ , then  $a^{n-1} \equiv 1 \pmod{n}$ .
- Thus if  $a^{n-1} \not\equiv 1 \pmod{n}$  for some integer  $a$  with  $(a, n) = 1$ , then  $n$  is composite.

## Primality Testing

- When an integer  $n$  is composite, it can be proved by knowing a nontrivial factor or failing a pseudoprimerality test.
- When  $n$  is prime, passing several pseudoprimerality tests is an indication that  $n$  is probably prime.
- The Goldwasser-Kilian (GK) primality test is based on elliptic curves and was used to prove primality of numbers with more than 1000 decimal digits.
- A classical version of this test is the Pocklington primality test.

## Pocklington Primality Test

Given integer  $n > 1$ . Suppose there exists a prime  $q$  with  $q \mid n - 1$  and  $q > \sqrt{n} - 1$ . If there exists an integer  $a$  with

$$\mathbf{1} \quad a^{n-1} \equiv 1 \pmod{n} \text{ and}$$

$$\mathbf{2} \quad (a^{(n-1)/q} - 1, n) = 1,$$

then  $n$  is prime.

## Proof.

If  $n$  is composite, there exists a prime  $p$  with  $p \mid n$  and  $p \leq \sqrt{n}$ . Since  $q > p - 1$ ,  $(q, p - 1) = 1$  and so there exists an integer  $v$  with  $vq \equiv 1 \pmod{p - 1}$ . Then by condition 1,

$$a^{(n-1)/q} \equiv a^{vq(n-1)/q} = a^{v(n-1)} \equiv 1 \pmod{p}.$$

Thus  $p$  divides  $a^{(n-1)/q} - 1$  and  $n$  contradicting condition 2.  $\square$

## Pocklington Primality Test

- The test is probabilistic in the sense that a randomly chosen  $a$  may or may not fulfill condition 2. If it fails to satisfy condition 1, then  $n$  is not prime.
- Once an  $a$  is found ( $a = 2$  will usually work), the test exhibits that  $n$  is prime.
- Unlike the primality test of Miller-Rabin, Pocklington's test yields " $n$  is prime" with certainty.
- There is a more general version which is based on the prime factorization of  $n - 1$ .

## Pocklington Primality Test

Given integer  $n > 1$  with  $n - 1 = rs$  and  $r \geq \sqrt{n}$ . Suppose for each prime  $\ell$  with  $\ell \mid r$ , there exists an integer  $a_\ell$  with

$$\mathbf{1} \quad a_\ell^{n-1} \equiv 1 \pmod{n} \text{ and}$$

$$\mathbf{2} \quad \left( a_\ell^{(n-1)/\ell} - 1, n \right) = 1.$$

Then  $n$  is prime.

## Proof.

Let  $p$  be prime with  $p \mid n$  and  $r = r' \ell^e$  with  $\ell \nmid r'$ .

- Let  $b \equiv a_\ell^{(n-1)/\ell^e} \pmod{p}$ . Then

$$b^{\ell^e} \equiv a_\ell^{n-1} \equiv 1 \pmod{p}$$

and

$$b^{\ell^{e-1}} \equiv a_\ell^{(n-1)/\ell} \not\equiv 1 \pmod{p},$$

since  $(a_\ell^{(n-1)/\ell} - 1, n) = 1$ . So the order of  $b \pmod{p}$  is  $\ell^e$ .

Hence,  $\ell^e \mid p - 1$ .

- For each prime power factor  $\ell^e$  of  $r$ ,  $\ell^e \mid p - 1$  and so  $r \mid p - 1$ . Thus

$$p > r \geq \sqrt{n}.$$

If  $n$  is composite, it has a prime factor of at most  $\sqrt{n}$ . But this is not the case and so  $n$  is prime.  $\square$

## Example

Let  $n = 153533$ . Then  $n - 1 = 4 \cdot 131 \cdot 293$ . Let  $r = 4 \cdot 131$ . The primes dividing  $r$  are  $\ell = 2$  and  $\ell = 131$ .

- We have

$$2^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad \left(2^{(n-1)/2} - 1, n\right) = 1$$

and so  $a_2 = 2$ .

- We have

$$2^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad \left(2^{(n-1)/131} - 1, n\right) = 1$$

and so  $a_{131} = 2$ .

By the Pocklington test, 153533 is prime.

## Goldwasser-Kilian Primality Test

Given integer  $n > 1$  and elliptic curve  $\mathcal{E} \bmod n$ . Suppose there exist distinct primes  $\ell_1, \dots, \ell_k$  and finite points  $P_1, \dots, P_k \in \mathcal{E}(\mathbb{Z}_n)$  such that

$$\mathbf{1} \quad [\ell_i]P_i = O \text{ for } 1 \leq i \leq k,$$

$$\mathbf{2} \quad \prod_{i=1}^k \ell_i > (n^{1/4} + 1)^2.$$

Then  $n$  is prime.

## Proof.

Let  $p$  be prime with  $n = n'p^e$  with  $p \nmid n'$ . Then by the Chinese Remainder theorem,

$$\mathcal{E}(\mathbb{Z}_n) = \mathcal{E}(\mathbb{Z}_{p^e}) \oplus \mathcal{E}(\mathbb{Z}_{n'}).$$

- The point  $P_i$  has finite order and so  $P_i \bmod p^e$  has finite order. By further reduction,  $P_{i,p} = P_i \bmod p$  has finite order. Since  $[\ell_i]P_i = O$ ,  $[\ell_i]P_{i,p} = O$  in  $\mathcal{E}(\mathbb{F}_p)$ . i.e.,  $P_{i,p}$  has order  $\ell_i$ . Thus  $\ell_i \mid \#\mathcal{E}(\mathbb{F}_p)$  for all  $i$  and hence  $\prod_i \ell_i \mid \#\mathcal{E}(\mathbb{F}_p)$ .
- By the Hasse bound (274),

$$\left(n^{1/4} + 1\right)^2 < \prod_i \ell_i \leq \#\mathcal{E}(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p} = \left(p^{1/2} + 1\right)^2.$$

Thus  $p > \sqrt{n}$  and so all prime factors of  $n$  are  $> \sqrt{n}$ . Hence,  $n$  is prime.  $\square$

## Example

Let  $n = 907$  and  $\mathcal{E}$  be the elliptic curve given by  $Y^2 = X^3 + 10X - 2 \pmod n$ .

- Let  $\ell = 71$ . Then

$$\ell > \left(907^{1/4} + 1\right)^2 \approx 42.1.$$

Let  $P = (819, 784)$ . Then  $[71]P = O$  and so 907 is prime.

- How to find  $\mathcal{E}$  and  $P$ ?
  - First look at elliptic curves  $\mathcal{E} \pmod{907}$  until one is found whose order is divisible by a prime  $\ell$  with  $\ell$  slightly larger than 42.1.
  - Take a known point  $Q$  on  $\mathcal{E} \pmod{907}$ . Here, say  $Q = (1, 3)$ . Using BSGS,  $Q$  has order  $923 = 13 \cdot 71$ . Then  $P = [13]Q$  has order 71.

## Factorization

A key reason for the increasing interest in elliptic curves on the part of cryptographers is the recent ingenious use of elliptic curves by H.W. Lenstra to obtain a new factorization method that in many respects is better than the earlier known ones. The discovery of an improvement using an unexpected new device serves as a warning that one should never be too complacent about the supposed imperviousness of the factoring problem to dramatic breakthroughs.

Neal Koblitz (1994).

## Pollard's $p - 1$ Method

**Require:** Composite odd integer  $n > 1$

**Ensure:** Factorization of  $n$

Choose integer bound  $B$  {Factor basis}

$k \leftarrow \text{lcm}(1, 2, \dots, B)$

Choose random integer  $a$  with  $2 \leq a \leq n - 1$

Compute  $a^k \pmod n$  by repeated squaring

Compute  $d \leftarrow (a^k - 1, n)$  by Euclidean algorithm

**if**  $d > 1$  **then**

Restart with  $n$  replaced by  $n/d$  {Factor of  $n$  is  $d$ }

**else**

Restart with new choice of  $B$  and  $a$

**end if**

## Correctness

Let  $k$  be divisible by all positive integers  $\leq B$ .

Suppose  $p$  is prime with  $p \mid n$  and  $p - 1$  is a product of small primes  $\leq B$ .

Then  $k$  is multiple of  $p - 1$ . Thus by Fermat's Little theorem,

$$a^k \equiv 1 \pmod{p}.$$

Hence,  $p \mid (a^k - 1, n)$  provides a nontrivial factor of  $n$ . □

The Pollard  $p - 1$  method does not work if all prime divisors  $p$  of  $n$  have  $p - 1$  divisible by a large prime.

## Example

Let  $n = 540143$ . Choose  $B = 8$ . Then

$$k = \text{lcm}(1, 2, \dots, 8) = 840.$$

Pick  $a = 2$ . Then

$$2^{840} \equiv 53047 \pmod{n}$$

and

$$(53046, n) = 421.$$

Thus

$$540143 = 421 \cdot 1283$$

with 421 being prime.

## Lenstra's Method (Hendrik Lenstra, 1987)

**Require:** Composite odd integer  $n > 1$

**Ensure:** Factorization of  $n$

Choose several random elliptic curves  $\mathcal{E}_i \bmod n$  given by  
 $Y^2 = X^3 + a_i X + b_i$  (say, 10 to 20)

Choose points  $P_i \in \mathcal{E}_i \bmod n$  {See the GK primality test.}

Choose large integer  $B$  (say,  $10^8$ )

Compute  $[B!]P_i$  on  $\mathcal{E}_i \bmod n$  for each  $i$

**if** Computation of slope of  $[B!]P_i$  for some  $i$  fails **then**

Factor of  $n$  found

**else**

Restart with increased  $B$  or newly chosen curves and points

**end if**

Quadratic sieve and number field sieve outperform Lenstra's method, but Lenstra's method is good for searching medium sized prime factors  $\leq 10^{40}$ .

## Example

Factorize  $n = 4453$ . Take the elliptic curve  $\mathcal{E} \bmod 4453$  given by  $Y^2 = X^3 + 10X - 2 \bmod 4453$  and  $P = (1, 3)$ .

- Compute  $[2]P$ : The slope of the tangent line at  $P$  is

$$\frac{3X^2 + 10}{2Y}(P) = \frac{13}{6} \equiv 3713 \pmod{4453},$$

since  $(6, 4453) = 1$  and so 6 is invertible mod 4453 with  $6^{-1} \equiv 3711 \pmod{4453}$ . Thus  $[2]P = (x, y)$  with

$$\begin{aligned} x &\equiv 3713^2 - 2 \equiv 4332 \pmod{4453}, \\ y &\equiv -3713(x - 1) \equiv 3230 \pmod{4453}. \end{aligned}$$

## Example (cont'd)

- Compute  $[3]P$  by adding  $[2]P$  and  $P$ . The slope is

$$\frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

But  $(4331, 4453) = 61 \neq 1$  and so 4331 is not invertible mod 4453. However, 61 is a factor of 4453 with  $4453 = 61 \cdot 73$ .

## Example (cont'd)

- By the Chinese Remainder theorem,

$$\mathcal{E}(\mathbb{Z}_{4453}) = \mathcal{E}(\mathbb{Z}_{61}) \oplus \mathcal{E}(\mathbb{Z}_{73}).$$

- Multiples of  $P$  mod 61:

$$P \equiv (1, 3), [2]P \equiv (1, 58), [3]P \equiv O, [4]P \equiv (1, 3), \dots$$

Multiples of  $P$  mod 73:

$$P \equiv (1, 3), [2]P \equiv (25, 18), [3]P \equiv (28, 44), \dots, [64]P = O.$$

- The slope of  $[3]P$  mod 4453 has 61 in the denominator and is thus infinite mod 61.
- Note that if  $[3]P = O$  mod 73, the slope will be 0 mod 4453 in the denominator and the factorization will not be possible. But this case is unlikely.

## EC Cryptography

However, in August 2015, the U.S. National Security Agency (NSA) announced that it plans to replace Suite B with a new cipher suite due to concerns about quantum computing attacks on ECC.

Wikipedia (2018).

# Part VIII

# Quantum Computing

## Quantum Computing

- Quantum computing is computing using quantum-mechanical phenomena.
- Large-scale quantum computers may be able to efficiently solve problems which are not practically feasible on classical computers.
- Post-quantum cryptography: cryptographic algorithms secure against QC attacks.
- Announcements (2017/2018): 50-qubit QC (IBM), 49-qubit QC (Intel), 72-qubit QC (Google).

## Quantum Hype and Quantum Skepticism (2019)

- Quantum computing is one of the U.S. National Science Foundation's "Ten Big Ideas".
- Quantum computation offers an exponential advantage of classical computation in theory.
- Quantum computers that compromise PK cryptography are unlikely to be built within the next decade including infrastructure (protocols).
- Qubits kept in highly sensitive superpositions will inevitably be corrupted by interaction with outside world.
- Error-correcting methods are needed as near term quantum computers are likely to be error-prone.
- Thriving marketplace is needed to sustain a virtuous cycle of developing increasingly useful quantum computers.

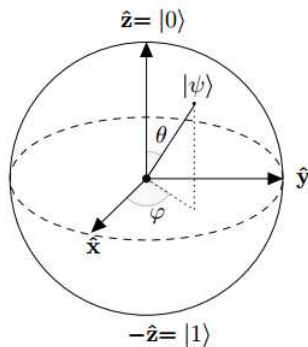
## Quantum Computing

- Quantum bits
- Multi-quantum bits
- Operations on multi-quantum bits
- Measurement

## Literature

- J.B. Conway: *A Course in Functional Analysis*, Springer, New York, 1990.
- J. Gruska: *Quantum Computing*, Techn. Report, Brno, 2018.
- P. Kaye, R. Laflamme, M. Mosca, *An Introduction to Quantum Computing*, Oxford Univ. Press, Oxford, 2007.
- E. Rieffel, W. Polak: *Quantum Computing – A Gentle Introduction*, The MIT Press, Cambridge, MA, 2011.
- T.F. Sturm, J. Schulze: *Quantum Computing aus algorithmischer Sicht*, Oldenbourg, Munich, 2009.
- R. de Wolf: *Quantum Computing – Lecture Notes*, Techn. Report, Amsterdam, 2018.

## Quantum Bits



Block sphere, Felix Bloch (1905-1983)

## Quantum Bits

- Qubits
- Hilbert space
- Representation of qubits
- Bloch sphere

## Quantum Bits

- A *qubit* is a two-state quantum mechanical system.
- A qubit can be in superposition of both states at the same time.
- In the classical system, a bit is in one state or the other (0 or 1).

## Quantum Bits

- A qubit can be measured in one of two *basis states* given by (ket notation),

$$|0\rangle \text{ and } |1\rangle.$$

- A *qubit* is a linear superposition of the basis states,

$$v = \lambda_0 |0\rangle + \lambda_1 |1\rangle \quad (365)$$

where  $\lambda_0, \lambda_1 \in \mathbb{C}$  are the *probability amplitudes* with absolute magnitude

$$\|\lambda\| = \|(\lambda_0, \lambda_1)\| = \sqrt{|\lambda_0|^2 + |\lambda_1|^2} = 1, \quad (366)$$

where the *absolute value* of complex number  $z = x + iy$  is

$$|z| = |x + iy| = \sqrt{x^2 + y^2}, \quad x, y \in \mathbb{R}. \quad (367)$$

- The *probability* of the state  $|i\rangle$  in qubit  $v$  is  $|\lambda_i|^2$  for  $i = 0, 1$ .

## Quantum Bits – Examples

## ■ Qubits

$$v = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle,$$

$$v = \frac{1}{\sqrt{3}} |0\rangle + \sqrt{\frac{2}{3}} |1\rangle.$$

- A *pure qubit* is a qubit  $v$  which is the multiple of a basis state; i.e.,  $v = \lambda_0 |0\rangle$  or  $v = \lambda_1 |1\rangle$  and  $\lambda_i \in \mathbb{C}$  with  $|\lambda_i|^2 = 1$ ,  $i = 0, 1$ .

Examples:

$$v = i |0\rangle,$$

$$v = -i |1\rangle.$$

## Quantum Bits

Let  $\mathcal{H}$  denote a 2-dimensional  $\mathbb{C}$ -Hilbert space with Hilbert basis  $\{|0\rangle, |1\rangle\}$ .

- A *qubit* of  $\mathcal{H}$  is an element  $v \in \mathcal{H}$  with  $\|v\| = 1$ . The set of all qubits forms the unit sphere

$$\mathcal{S}_{\mathcal{H}} = \{v \in \mathcal{H} \mid \|v\| = 1\}. \quad (368)$$

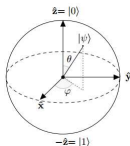
- The mapping  $\mathcal{H} \rightarrow \mathbb{C}^2$  given by

$$|0\rangle \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad (369)$$

is a  $\mathbb{C}$ -vector space isomorphism; i.e.,

$$\lambda_0 |0\rangle + \lambda_1 |1\rangle \mapsto \lambda_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (370)$$

## Bloch Sphere



Geometrical representation of qubit:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle \quad (371)$$

where  $0 \leq \theta \leq \pi$  and  $0 \leq \varphi < 2\pi$ .

Note that in the general representation,

$$|\psi\rangle = e^{i\alpha} a |0\rangle + e^{i\beta} b |1\rangle = e^{i\alpha} \left( a |0\rangle + e^{i(\beta-\alpha)} b |1\rangle \right) \quad (372)$$

the overall phase is neglected.

## Bloch Sphere

K.-H.  
Zimmermann

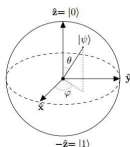
Contents

Quantum Bits

Multi-Qubits

Operations on  
Multi-Qubits

Measurement



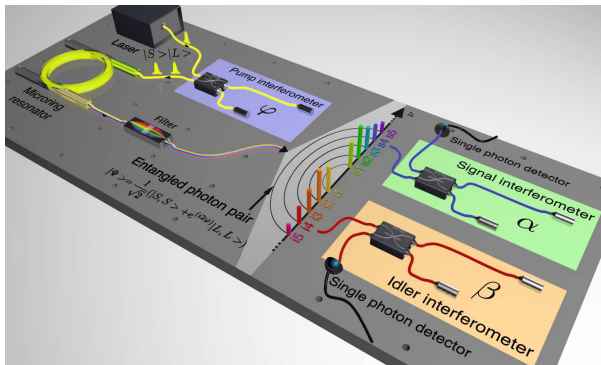
$\theta$	$\varphi$	$ \psi\rangle$	$\theta$	$\varphi$	$ \psi\rangle$
0	0	$ 0\rangle$	0	$\pi$	$ 0\rangle$
$\pi/2$	0	$a 0\rangle + a 1\rangle$	$\pi/2$	$\pi$	$a 0\rangle - a 1\rangle$
$\pi$	0	$ 1\rangle$	$\pi$	$\pi$	$- 1\rangle$
0	$\pi/2$	$ 0\rangle$	0	$3\pi/2$	$ 0\rangle$
$\pi/2$	$\pi/2$	$a 0\rangle + ai 1\rangle$	$\pi/2$	$3\pi/2$	$a 0\rangle - ai 1\rangle$
$\pi$	$\pi/2$	$i 1\rangle$	$\pi$	$3\pi/2$	$-i 1\rangle$

where  $a = \sin(\pi/4) = \cos(\pi/4) = 1/\sqrt{2}$ .

## Physical Realization of Qubit

Physical support	Name	$ 0\rangle$	$ 1\rangle$
Photon	polarization encoding	horizontal	vertical
Electrons	electronic spin	up	down
Nucleus	nuclear spin (NMR)	up	down
Optical lattice	atomic spin	up	down
Quantum dot	dot spin	down	up

## Multi-Quantum Bits



## Multi-Quantum Bits

- Tensor product Hilbert space
- Representation of multi-qubits
- Pure, separable, and entangled multi-qubits

## Multi-Quantum Bits

- A quantum computer performs calculations by manipulating qubits within a quantum register.
- A quantum register is a collection of qubits taken together.
- A quantum register is mathematically given by a tensor of a tensor product Hilbert space.
- In a classical system, a binary register is defined by the cartesian product of binary states.

## Tensor Product Space

Let  $\mathcal{H}$  be a 2-dimensional  $\mathbb{C}$ -Hilbert space with Hilbert basis  $\{|0\rangle, |1\rangle\}$ .

- Each element  $v \in \mathcal{H}^{\otimes n}$  with  $\|v\| = 1$  is an  $n$ -qubit and the set of all  $n$ -qubits is

$$S_{\mathcal{H}^{\otimes n}} = \{v \in \mathcal{H}^{\otimes n} \mid \|v\| = 1\}. \quad (373)$$

- For each integer  $x$ ,  $0 \leq x < 2^n$ , with binary representation

$$x = x_{n-1} \dots x_1 x_0 = \sum_{j=0}^{n-1} 2^j x_j, \quad x_j \in \{0, 1\}, \quad (374)$$

define the  $n$ -qubit  $|x\rangle_n \in \mathcal{H}^{\otimes n}$  as

$$\begin{aligned} |x\rangle_n &= |x_{n-1} \dots x_1 x_0\rangle \\ &= |x_{n-1}\rangle \dots |x_1\rangle |x_0\rangle \\ &= |x_{n-1}\rangle \otimes \dots \otimes |x_1\rangle \otimes |x_0\rangle. \end{aligned} \quad (375)$$

## Tensor Product Space – Notation

The tensor products

$$|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle$$

can be written as

$$|0\rangle |0\rangle, \quad |0\rangle |1\rangle, \quad |1\rangle |0\rangle, \quad |1\rangle |1\rangle$$

or shorter as

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle$$

or using decimals as

$$|0\rangle_2, \quad |1\rangle_2, \quad |2\rangle_2, \quad |3\rangle_2.$$

Note that  $|3\rangle_2 = |11\rangle$  and  $|3\rangle_3 = |011\rangle$ .

## Tensor Product Space

Let  $\mathcal{H}$  be a 2-dimensional  $\mathbb{C}$ -Hilbert space with Hilbert basis  $\{|0\rangle, |1\rangle\}$ .

- The vector space  $\mathcal{H}^{\otimes n}$  is a  $2^n$ -dimensional Hilbert space over  $\mathbb{C}$  with Hilbert basis

$$\{|x\rangle_n \mid 0 \leq x \leq 2^n - 1\}. \quad (376)$$

- Each  $n$ -qubit  $v \in \mathcal{S}_{\mathcal{H}^{\otimes n}}$  can be uniquely written as

$$v = \sum_{j=0}^{2^n-1} \lambda_j |j\rangle_n \quad (377)$$

with  $\lambda = (\lambda_j) \in \mathbb{C}^{2^n}$  and  $\|\lambda\| = 1$ .

## Bi-Qubits – Examples

$$v = \frac{1}{2} |00\rangle + \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |11\rangle,$$

$$v = \frac{1}{3} |00\rangle + \frac{1}{3} |01\rangle + \frac{\sqrt{5}}{3} |10\rangle + \frac{\sqrt{2}}{3} |11\rangle,$$

$$v = \frac{1}{4} |00\rangle + \frac{\sqrt{5}}{4} |01\rangle + \frac{\sqrt{5}}{4} |10\rangle + \frac{\sqrt{5}}{4} |11\rangle.$$

## Tensor Product Space

The mapping  $\mathcal{H}^{\otimes n} \rightarrow \mathbb{C}^{2^n}$  given by

$$|x\rangle_n \mapsto e_{x+1} \quad (378)$$

is a  $\mathbb{C}$ -vector space isomorphism, where  $e_1, \dots, e_{2^n}$  is the standard basis of  $\mathbb{C}^{2^n}$ .

$$|6\rangle_3 = |110\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle \mapsto \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

## Multi-Quantum Bits

- A *pure  $n$ -qubit* is an  $n$ -qubit  $v \in \mathcal{S}_{\mathcal{H}^{\otimes n}}$  which is the multiple of a basis state; i.e.,

$$v = \lambda |x\rangle_n \quad (379)$$

for some  $x \in \{0, \dots, 2^n - 1\}$  and  $\lambda \in \mathbb{C}$  with  $|\lambda|^2 = 1$ .

- The assignment of an  $n$ -qubit to a pure  $n$ -qubit will be effected by measurement!

## Tensor Permutation

Let  $\sigma, \tau$  be bijections (permutations) of the set  $\{0, \dots, n-1\}$ .

- The linear mapping  $Q_\sigma : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$  given by

$$\begin{aligned} x_{n-1} \otimes \dots \otimes x_1 \otimes x_0 & \quad (380) \\ \mapsto x_{\sigma^{-1}(n-1)} \otimes \dots \otimes x_{\sigma^{-1}(1)} \otimes x_{\sigma^{-1}(0)} \end{aligned}$$

is called *tensor permutation* of  $\mathcal{H}^{\otimes n}$ .

- We have

$$Q_\sigma Q_\tau = Q_{\sigma\tau}. \quad (381)$$

## Multi-Quantum Bits

Proof:

$$\begin{aligned}
 & Q_{\sigma}Q_{\tau}(x_{n-1} \otimes \dots \otimes x_0) \\
 &= Q_{\sigma}(x_{\tau^{-1}(n-1)} \otimes \dots \otimes x_{\tau^{-1}(0)}) \\
 &= Q_{\sigma}(d_{n-1} \otimes \dots \otimes d_0), \quad d_i = x_{\tau^{-1}(i)}, \\
 &= (d_{\sigma^{-1}(n-1)} \otimes \dots \otimes d_{\sigma^{-1}(0)}) \\
 &= (x_{\tau^{-1}(\sigma^{-1}(n-1))} \otimes \dots \otimes x_{\tau^{-1}(\sigma^{-1}(0))}) \\
 &= (x_{(\sigma\tau)^{-1}(n-1)} \otimes \dots \otimes x_{(\sigma\tau)^{-1}(0)}) \\
 &= Q_{\sigma\tau}(x_{n-1} \otimes \dots \otimes x_0).
 \end{aligned}$$

□

## Multi-Quantum Bits

- An  $n$ -qubit  $v$  is *separable* if there exists  $1 \leq p < n$  such that

$$v = x \otimes y, \quad (382)$$

where  $x \in \mathcal{S}_{\mathcal{H}^{\otimes p}}$  and  $y \in \mathcal{S}_{\mathcal{H}^{\otimes q}}$  with  $q = n - p$ .

- An  $n$ -qubit  $v$  is *indirectly separable* if there exists tensor permutation  $Q$  of  $\mathcal{H}^{\otimes n}$  such that  $Qv$  is separable.
- An  $n$ -qubit  $v$  is *inseparable* or *entangled* if  $v$  is neither separable nor indirectly separable.

## Multi-Quantum Bits – Examples

### ■ The bi-qubit

$$v = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

is separable, since

$$v = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle).$$

### ■ The 3-qubit

$$v = \frac{1}{\sqrt{2}}|010\rangle + \frac{1}{\sqrt{2}}|111\rangle$$

is indirectly separable, since if  $Q_\sigma$  is the tensor permutation given by  $\sigma = (01)(2)$  (fix position 2, transpose positions 0,1), then

$$Q_\sigma v = \frac{1}{\sqrt{2}}|001\rangle + \frac{1}{\sqrt{2}}|111\rangle = \left( \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \right) \otimes |1\rangle.$$

## Multi-Quantum Bits – Example

The following bi-qubits known as *Bell qubits* are inseparable:

$$\beta_{00} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle),$$

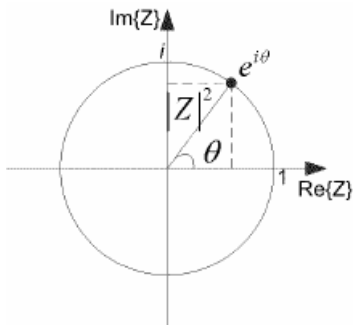
$$\beta_{01} = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle),$$

$$\beta_{10} = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle),$$

$$\beta_{11} = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle).$$

The vectors  $\beta_{00}, \beta_{01}, \beta_{10}, \beta_{11}$  form a Hilbert basis of  $\mathcal{H}^{\otimes 2}$ .

## Operations on Multi-Qubits



## Operations on Multi-Qubits

- Gates for qubits, bi-qubits, and multi-qubits
- Gates for Boolean functions
- Quantum Fourier transform

## Gates for Qubits

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$ .

The **I**-gate is the unitary operator  $\mathbf{I} : \mathcal{H} \rightarrow \mathcal{H}$  defined by

$$\mathbf{I}|0\rangle = |0\rangle \quad \text{and} \quad \mathbf{I}|1\rangle = |1\rangle. \quad (383)$$

Matrix representation of  $\mathbf{I}$  w.r.t. the standard basis:

$$M_{\mathbf{I}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (384)$$

We have

$$M_{\mathbf{I}}^* = M_{\mathbf{I}}. \quad (385)$$

The gate realizes the identity operator.

## Gates for Qubits

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$ .

The **X**-gate or *not*-gate is the unitary operator  $\mathbf{X} : \mathcal{H} \rightarrow \mathcal{H}$  defined by

$$\mathbf{X} |0\rangle = |1\rangle \quad \text{and} \quad \mathbf{X} |1\rangle = |0\rangle. \quad (386)$$

Matrix representation of  $\mathbf{X}$  w.r.t. the standard basis:

$$M_{\mathbf{X}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (387)$$

We have

$$M_{\mathbf{X}}^* = M_{\mathbf{X}}. \quad (388)$$

The gate changes the pure states, measurement changes the bit value.

## Gates for Qubits

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$ .

The **Y**-gate is the unitary operator  $\mathbf{Y} : \mathcal{H} \rightarrow \mathcal{H}$  defined by

$$\mathbf{Y}|0\rangle = i|1\rangle \quad \text{and} \quad \mathbf{Y}|1\rangle = -i|0\rangle. \quad (389)$$

Matrix representation of  $\mathbf{Y}$  w.r.t. the standard basis:

$$M_{\mathbf{Y}} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (390)$$

We have

$$M_{\mathbf{Y}}^* = M_{\mathbf{Y}}. \quad (391)$$

The gate exchanges the pure states, but with different values.

## Gates for Qubits

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$ .

The  $\mathbf{Z}$ -gate is the unitary operator  $\mathbf{Z} : \mathcal{H} \rightarrow \mathcal{H}$  defined by

$$\mathbf{Z}|0\rangle = |0\rangle \quad \text{and} \quad \mathbf{Z}|1\rangle = -|1\rangle. \quad (392)$$

Matrix representation of  $\mathbf{Z}$  w.r.t. the standard basis:

$$M_{\mathbf{Z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (393)$$

We have

$$M_{\mathbf{Z}}^* = M_{\mathbf{Z}}. \quad (394)$$

This matrix is called *Pauli matrix*.

## Gates for Qubits

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$ .

The  $\mathbf{P}$ -gate or *phase gate* is the unitary operator  $\mathbf{P} : \mathcal{H} \rightarrow \mathcal{H}$  defined by

$$\mathbf{P} |0\rangle = |0\rangle \quad \text{and} \quad \mathbf{P} |1\rangle = i |1\rangle. \quad (395)$$

Matrix representation of  $\mathbf{P}$  w.r.t. the standard basis:

$$M_{\mathbf{P}} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \quad (396)$$

We have

$$M_{\mathbf{P}}^* = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}. \quad (397)$$

The gate does not change the pure states.

## Gates for Qubits

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$ .

The  $\mathbf{H}$ -gate or *Hadamard gate* is the unitary operator  $\mathbf{H} : \mathcal{H} \rightarrow \mathcal{H}$  defined by

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (398)$$

Matrix representation of  $\mathbf{H}$  w.r.t. the standard basis:

$$M_{\mathbf{H}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (399)$$

We have

$$M_{\mathbf{H}}^* = M_{\mathbf{H}}. \quad (400)$$

The gate changes the pure states into states with equal probability.

## Implementation of Hadamard Gate

A beamsplitter is an optical device that splits a beam of light into two separate beams:

$$\mathbf{B} |0\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |1\rangle, \quad (401)$$

$$\mathbf{B} |1\rangle = \frac{i}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle. \quad (402)$$

Matrix representation of  $\mathbf{B}$  w.r.t. the standard basis:

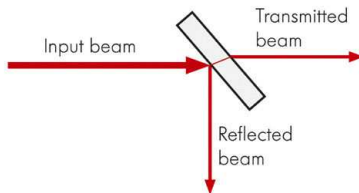
$$M_{\mathbf{B}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \quad (403)$$

We have

$$M_{\mathbf{B}}^* = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}. \quad (404)$$

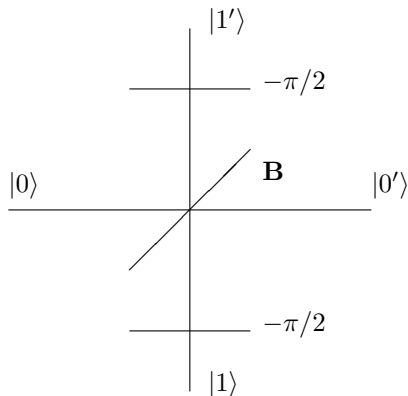
## Implementation of Hadamard Gate

A beamsplitter splits a beam of light into two separate beams:



## Implementation of Hadamard Gate

A Hadamard gate can be realized optically by a beamsplitter and two  $-\pi/2$  phase shifters:



## Implementation of Hadamard Gate

- A  $-\pi/2$  phase shifter provides a multiplication with

$$e^{-i\pi/2} = -i. \quad (405)$$

- A Hadamard gate can be realized optically by a beamsplitter and two  $-\pi/2$  phase shifters:

$$\begin{aligned} \mathbf{H} |0\rangle &= \frac{1}{\sqrt{2}} |0\rangle + e^{-i\pi/2} \frac{i}{\sqrt{2}} |1\rangle \\ &= \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle, \end{aligned} \quad (406)$$

$$\begin{aligned} \mathbf{H} |1\rangle &= \frac{i}{\sqrt{2}} e^{-i\pi/2} |0\rangle + e^{-i\pi/2} \frac{1}{\sqrt{2}} e^{-i\pi/2} |1\rangle \\ &= \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle. \end{aligned} \quad (407)$$

## Multi-Qubit Extension

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$  and  $A, B : \mathcal{H} \rightarrow \mathcal{H}$  be linear operators given by

$$A|0\rangle = a_{11}|0\rangle + a_{21}|1\rangle, \quad (408)$$

$$A|1\rangle = a_{12}|0\rangle + a_{22}|1\rangle, \quad (409)$$

$$B|0\rangle = b_{11}|0\rangle + b_{21}|1\rangle, \quad (410)$$

$$B|1\rangle = b_{12}|0\rangle + b_{22}|1\rangle. \quad (411)$$

Matrix representations of  $A$  and  $B$ :

$$M_A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad (412)$$

$$M_B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}. \quad (413)$$

## Multi-Qubit Extension (cont'd)

Matrix representation of *Kronecker product*  $A \otimes B$ :

$$\begin{aligned}
 M_{A \otimes B} &= \begin{pmatrix} a_{11}M_B & a_{12}M_B \\ a_{21}M_B & a_{22}M_B \end{pmatrix} \\
 &= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.
 \end{aligned} \tag{414}$$

## Tensor Permutations

Each tensor permutation is a unitary operation given by a permutation matrix.

### Example

Let  $\mathcal{H}$  be the  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$  and  $P: \mathcal{H}^{\otimes 2} \rightarrow \mathcal{H}^{\otimes 2}$  be the tensor permutation which permutes the tensor components; i.e.,

$$P|00\rangle = |00\rangle, P|01\rangle = |10\rangle, P|10\rangle = |01\rangle, P|11\rangle = |11\rangle.$$

Matrix representation of  $P$  w.r.t. the standard basis:

$$M_P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

## Multi-Qubit Extension

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$  and let  $n, k$  be integers with  $0 \leq k < n$ .

The operator

$$\mathbf{H}_k^{(n)} = \underbrace{\mathbf{I} \otimes \dots \otimes \mathbf{I}}_{n-k-1} \otimes \mathbf{H} \otimes \underbrace{\mathbf{I} \otimes \dots \otimes \mathbf{I}}_k \quad (415)$$

is unitary on  $\mathcal{H}^{\otimes n}$ , where  $\mathbf{H}$  is the Hadamard gate.

## Gates for Bi-Qubits

The unitary operators

$$\mathbf{H}_0^{(2)} = \mathbf{I} \otimes \mathbf{H} \quad \text{and} \quad \mathbf{H}_1^{(2)} = \mathbf{H} \otimes \mathbf{I} \quad (416)$$

have the matrix representations w.r.t. the standard bases

$$M_{\mathbf{H}_0^{(2)}} = \begin{pmatrix} M_{\mathbf{H}} & 0 \\ 0 & M_{\mathbf{H}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad (417)$$

$$M_{\mathbf{H}_1^{(2)}} = \begin{pmatrix} M_{\mathbf{I}} & M_{\mathbf{I}} \\ M_{\mathbf{I}} & -M_{\mathbf{I}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \quad (418)$$

## Tri-Qubit Extension

We have

$$\begin{aligned} \mathbf{H}_1^{(3)}(|x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle) &= (\mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I})(|x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle) \\ &= |x_2\rangle \otimes (\mathbf{H} |x_1\rangle) \otimes |x_0\rangle. \end{aligned} \quad (419)$$

## Example

$$\begin{aligned} \mathbf{H}_1^{(3)} \left( \sqrt{\frac{1}{2}} |001\rangle + \sqrt{\frac{1}{2}} |111\rangle \right) &= \sqrt{\frac{1}{2}} (|0\rangle \otimes (\mathbf{H} |0\rangle) \otimes |1\rangle) + \sqrt{\frac{1}{2}} (|1\rangle \otimes (\mathbf{H} |1\rangle) \otimes |1\rangle) \\ &= \sqrt{\frac{1}{2}} \left( |0\rangle \otimes \left( \sqrt{\frac{1}{2}} (|0\rangle + |1\rangle) \right) \otimes |1\rangle \right) + \sqrt{\frac{1}{2}} \left( |1\rangle \otimes \left( \sqrt{\frac{1}{2}} (|0\rangle - |1\rangle) \right) \otimes |1\rangle \right) \\ &= \frac{1}{2} (|001\rangle + |011\rangle + |101\rangle - |111\rangle). \end{aligned}$$

## Gates for Multi-Qubits

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$  and let  $n \geq 1$  be an integer.

The linear operator  $\mathbf{H}^{\otimes n} : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$  given by

$$\begin{aligned} \mathbf{H}^{\otimes n}(x_1 \otimes \dots \otimes x_n) &= \mathbf{H}^{\otimes n} |x_1 \dots x_n\rangle_n & (420) \\ &= \mathbf{H} |x_1\rangle \otimes \dots \otimes \mathbf{H} |x_n\rangle \end{aligned}$$

is unitary.

### Proof.

Since the linear operator  $\mathbf{H}$  is unitary and the tensor product of unitary operators is unitary, the linear operator  $\mathbf{H}^{\otimes n}$  is unitary.  $\square$

## Gates for Bi-Qubits

The unitary operator

$$\mathbf{H}^{\otimes 2} = \mathbf{H} \otimes \mathbf{H} \quad (421)$$

has the matrix representation w.r.t. the standard basis

$$\begin{aligned} M_{\mathbf{H}^{\otimes 2}} &= \frac{1}{\sqrt{2}} \begin{pmatrix} M_{\mathbf{H}} & M_{\mathbf{H}} \\ M_{\mathbf{H}} & -M_{\mathbf{H}} \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \end{aligned} \quad (422)$$

## Gates for Multi-Qubits

If  $n$  Hadamard gates are prepared in parallel to  $n$  qubits each prepared in state  $|0\rangle$ , a superposition of all  $2^n$  binary registers is obtained:

$$\begin{aligned}
 \mathbf{H}^{\otimes n} |0\rangle_n &= \mathbf{H} |0\rangle \otimes \dots \otimes \mathbf{H} |0\rangle & (423) \\
 &= \bigotimes_{i=1}^n \left( \sqrt{\frac{1}{2}} (|0\rangle + |1\rangle) \right) \\
 &= \frac{1}{\sqrt{2^n}} \bigotimes_{i=1}^n (|0\rangle + |1\rangle) \\
 &= 2^{-n/2} \sum_{j=0}^{2^n-1} |j\rangle_n.
 \end{aligned}$$

The Hadamard gate is responsible for the high degree of parallelism in quantum computing.

## Gates for Multi-Qubits – Example

Case  $n = 2$ :

$$\begin{aligned}
 \mathbf{H}^{\otimes 2} |00\rangle_2 &= \mathbf{H} |0\rangle \otimes \mathbf{H} |0\rangle && (424) \\
 &= \left( \sqrt{\frac{1}{2}}(|0\rangle + |1\rangle) \right) \otimes \left( \sqrt{\frac{1}{2}}(|0\rangle + |1\rangle) \right) \\
 &= \frac{1}{2} ((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)) \\
 &= \frac{1}{2} (|00\rangle_2 + |01\rangle_2 + |10\rangle_2 + |11\rangle_2).
 \end{aligned}$$

## Gates for Multi-Qubits

Let  $\mathbb{B} = \{0, 1\}$ .

The *Hadamard function*  $h : \mathbb{N}_0^2 \rightarrow \mathbb{B}$  is defined as

$$h(x, y) = \bigoplus_{j=0}^m x_j \odot y_j \quad (425)$$

where  $x = \sum_{j=0}^m x_j 2^j$ ,  $y = \sum_{j=0}^m y_j 2^j$ , and  $x_j, y_j \in \mathbb{B}$ .

$\oplus$  and  $\odot$  denote the addition and multiplication mod 2, resp.

We have

$$h(x, y) = 1 \quad (426)$$

iff in the binary representations of  $x$  and  $y$  the number of 1's at equal positions is odd.

### Example

$$h(0000, 0111) = 0, h(000\underline{1}, 011\underline{1}) = 1, h(00\underline{11}, 01\underline{11}) = 0, h(0\underline{111}, 0\underline{111}) = 1.$$

## Gates for Multi-Qubits

The unitary operator  $\mathbf{H}^{\otimes n}$  satisfies

$$\mathbf{H}^{\otimes n} |x\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} (-1)^{h(x,y)} |y\rangle_n \quad (427)$$

for all  $0 \leq x < 2^n$ .

Matrix representation w.r.t. the standard basis:

$$M_{\mathbf{H}^{\otimes n}} = 2^{-n/2} \left( (-1)^{h(i,j)} \right)_{i,j=0,\dots,2^n-1}. \quad (428)$$

## Proof.

Let  $x = \sum_{j=0}^{n-1} x_j 2^j$ ,  $x_j \in \mathbb{B}$ . Then

$$\begin{aligned}
 \mathbf{H}^{\otimes n} |x\rangle_n &= \bigotimes_{j=0}^{n-1} \mathbf{H} |x_{n-1-j}\rangle \\
 &= 2^{-n/2} \bigotimes_{j=0}^{n-1} (|0\rangle + (-1)^{x_{n-1-j}} |1\rangle) \\
 &\stackrel{!}{=} 2^{-n/2} \sum_{y=0}^{2^n-1} (-1)^{x_{n-1} \odot y_{n-1} \oplus \dots \oplus x_0 \odot y_0} |y\rangle_n \\
 &= 2^{-n/2} \sum_{y=0}^{2^n-1} (-1)^{h(x,y)} |y\rangle_n,
 \end{aligned}$$

where  $y = \sum_{j=0}^{n-1} y_j 2^j$ ,  $y_j \in \mathbb{B}$ . ( $\stackrel{!}{=}$  by induction step.) □

## Gates for Multi-Qubits – Example

Case  $n = 3$ :

$$\begin{aligned}
 \mathbf{H}^{\otimes 3} |011\rangle_3 &= \mathbf{H} |0\rangle \otimes \mathbf{H} |1\rangle \otimes \mathbf{H} |1\rangle \\
 &= \left( \sqrt{\frac{1}{2}}(|0\rangle + |1\rangle) \right) \otimes \left( \sqrt{\frac{1}{2}}(|0\rangle - |1\rangle) \right) \otimes \left( \sqrt{\frac{1}{2}}(|0\rangle - |1\rangle) \right) \\
 &= \frac{1}{2\sqrt{2}} ((|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)) \\
 &= \frac{1}{2\sqrt{2}} (|000\rangle_3 - |001\rangle_3 - |010\rangle_3 + |011\rangle_3 \\
 &\quad + |100\rangle_3 - |101\rangle_3 - |110\rangle_3 + |111\rangle_3),
 \end{aligned}$$

where

$$\begin{aligned}
 h(000, 011) &= 0, & h(001, 011) &= 1, & h(010, 011) &= 1, & h(011, 011) &= 0, \\
 h(100, 011) &= 0, & h(101, 011) &= 1, & h(110, 011) &= 1, & h(111, 011) &= 0.
 \end{aligned}$$

## Gates for Boolean Functions

Let  $\mathbb{B} = \{0, 1\}$  and  $n \geq 0$  integer.

- An  $n$ -ary *Boolean function* is a mapping  $f : \mathbb{B}^n \rightarrow \mathbb{B}$ .
- Identify the domain  $\mathbb{B}^n$  with the standard basis of the Hilbert space  $\mathcal{H}^{\otimes n}$ ; i.e.,

$$(x_{n-1}, \dots, x_1, x_0) \mapsto |x_{n-1} \dots x_1 x_0\rangle_n, \quad (429)$$

where

$$|x_{n-1} \dots x_1 x_0\rangle_n = |x_{n-1}\rangle \otimes \dots \otimes |x_1\rangle \otimes |x_0\rangle. \quad (430)$$

## Gates for Boolean Functions

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$  and  $f : \mathbb{B}^n \rightarrow \mathbb{B}$  be a Boolean function.

The  $U_f$  gate is the unitary operator

$$U_f : \mathcal{H}^{\otimes(n+1)} \rightarrow \mathcal{H}^{\otimes(n+1)} \quad (431)$$

defined by

$$U_f |x\rangle_n |y\rangle_1 = |x\rangle_n |y \oplus f(x)\rangle_1 \quad (432)$$

for all  $x \in \mathbb{B}^n$  and  $y \in \mathbb{B}$ , where  $\oplus$  denotes the binary addition.

## Gates for Boolean Functions

The gate  $U_f$  has the property

$$U_f^{-1} = U_f. \quad (433)$$

## Proof.

We have

$$\begin{aligned} U_f U_f (|x\rangle_n |y\rangle_1) &= U_f (|x\rangle_n |y \oplus f(x)\rangle_1) \\ &= |x\rangle_n |y \oplus f(x) \oplus f(x)\rangle_1 \\ &= |x\rangle_n |y \oplus 0\rangle_1 \\ &= |x\rangle_n |y\rangle_1, \end{aligned}$$

since  $z \oplus z = 0$  and  $z \oplus 0 = z$  for all  $z \in \mathbb{B}$ . □

## Gates for Boolean Functions – Example

Consider the unary NOT function

$$f : \mathbb{B} \rightarrow \mathbb{B} : x \mapsto \neg x. \quad (434)$$

The gate

$$\mathbf{U}_f : \mathcal{H}^{\otimes 2} \rightarrow \mathcal{H}^{\otimes 2} \quad (435)$$

is given by

$$\mathbf{U}_f |x\rangle_1 |y\rangle_1 = |x\rangle_1 |y \oplus \neg x\rangle_1. \quad (436)$$

Value table:

$ x\rangle  y\rangle$	$\mathbf{U}_f  x\rangle  y\rangle$
$ 0\rangle  0\rangle$	$ 0\rangle  0 \oplus \neg 0\rangle =  0\rangle  1\rangle$
$ 1\rangle  0\rangle$	$ 1\rangle  0 \oplus \neg 1\rangle =  1\rangle  0\rangle$
$ 0\rangle  1\rangle$	$ 0\rangle  1 \oplus \neg 0\rangle =  0\rangle  0\rangle$
$ 1\rangle  1\rangle$	$ 1\rangle  1 \oplus \neg 1\rangle =  1\rangle  1\rangle$

## Gates for Boolean Functions – Example

Consider the binary AND function

$$f : \mathbb{B}^2 \rightarrow \mathbb{B} : (x_1, x_0) \mapsto x_1 \wedge x_0. \quad (437)$$

The gate

$$U_f : \mathcal{H}^{\otimes 3} \rightarrow \mathcal{H}^{\otimes 3} \quad (438)$$

is given by

$$U_f |x_1 x_0\rangle_2 |y\rangle_1 = |x_1 x_0\rangle_2 |y \oplus (x_1 \wedge x_0)\rangle_1. \quad (439)$$

Value table:

$ x_1 x_0\rangle  y\rangle$	$U_f  x_1 x_0\rangle  y\rangle$
$ 00\rangle  0\rangle$	$ 00\rangle  0 \oplus (0 \wedge 0)\rangle =  00\rangle  0\rangle$
$ 00\rangle  1\rangle$	$ 00\rangle  1 \oplus (0 \wedge 0)\rangle =  00\rangle  1\rangle$
$ 01\rangle  0\rangle$	$ 01\rangle  0 \oplus (0 \wedge 1)\rangle =  01\rangle  0\rangle$
$ 01\rangle  1\rangle$	$ 01\rangle  1 \oplus (0 \wedge 1)\rangle =  01\rangle  1\rangle$
$ 10\rangle  0\rangle$	$ 10\rangle  0 \oplus (1 \wedge 0)\rangle =  10\rangle  0\rangle$
$ 10\rangle  1\rangle$	$ 10\rangle  1 \oplus (1 \wedge 0)\rangle =  10\rangle  1\rangle$
$ 11\rangle  0\rangle$	$ 11\rangle  0 \oplus (1 \wedge 1)\rangle =  11\rangle  1\rangle$
$ 11\rangle  1\rangle$	$ 11\rangle  1 \oplus (1 \wedge 1)\rangle =  11\rangle  0\rangle$

## Gates for Boolean Functions

Application of gate  $\mathbf{U}_f$  to  $\mathbf{H}_0^{(n+1)} |x\rangle_n |1\rangle$ ,

$$\begin{aligned}
 \mathbf{U}_f \mathbf{H}_0^{(n+1)} |x\rangle_n |1\rangle &= \mathbf{U}_f \left( |x\rangle_n \otimes \left( \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right) \right) \quad (440) \\
 &= |x\rangle_n \otimes \frac{1}{\sqrt{2}} (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) \\
 &= |x\rangle_n \otimes \frac{1}{\sqrt{2}} (|f(x)\rangle - |1 \oplus f(x)\rangle) \\
 &= |x\rangle_n \otimes \frac{1}{\sqrt{2}} (-1)^{f(x)} (|0\rangle - |1\rangle) \\
 &= (-1)^{f(x)} \cdot |x\rangle_n \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).
 \end{aligned}$$

## Quantum Fourier Transform

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space with basis  $\{|0\rangle, |1\rangle\}$  and let  $n \geq 1$  be an integer.

The  $\mathbf{F}^{\otimes n}$  gate or *Fourier transform* is the unitary operator

$$\mathbf{F}^{\otimes n} : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n} \quad (441)$$

defined by

$$\mathbf{F}^{\otimes n} |x\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{xy}{2^n}\right) |y\rangle_n \quad (442)$$

for all  $0 \leq x < 2^n$ .

## Quantum Fourier Transform – Example

Case  $n = 2$ :

$$\mathbf{F}^{\otimes 2} |0\rangle_2 = \frac{1}{4} (|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2),$$

$$\mathbf{F}^{\otimes 2} |1\rangle_2 = \frac{1}{4} (|0\rangle_2 + i|1\rangle_2 - |2\rangle_2 - i|3\rangle_2),$$

$$\mathbf{F}^{\otimes 2} |2\rangle_2 = \frac{1}{4} (|0\rangle_2 - |1\rangle_2 + |2\rangle_2 - |3\rangle_2),$$

$$\mathbf{F}^{\otimes 2} |3\rangle_2 = \frac{1}{4} (|0\rangle_2 - i|1\rangle_2 - |2\rangle_2 + i|3\rangle_2).$$

Matrix representation w.r.t. standard basis:

$$M_{\mathbf{F}^{\otimes 2}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

## Quantum Fourier Transform

The inverse Fourier transform of  $\mathbf{F}^{\otimes n}$  is the adjoint operator  $(\mathbf{F}^{\otimes n})^*$  given by

$$(\mathbf{F}^{\otimes n})^* |x\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(-2\pi i \frac{xy}{2^n}\right) |y\rangle_n \quad (443)$$

for all  $0 \leq x < 2^n$ .

## Quantum Fourier Transform – Example

Case  $n = 2$ :

$$(\mathbf{F}^{\otimes 2})^* |0\rangle_2 = \frac{1}{4} (|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2),$$

$$(\mathbf{F}^{\otimes 2})^* |1\rangle_2 = \frac{1}{4} (|0\rangle_2 - i|1\rangle_2 - |2\rangle_2 + i|3\rangle_2),$$

$$(\mathbf{F}^{\otimes 2})^* |2\rangle_2 = \frac{1}{4} (|0\rangle_2 - |1\rangle_2 + |2\rangle_2 - |3\rangle_2),$$

$$(\mathbf{F}^{\otimes 2})^* |3\rangle_2 = \frac{1}{4} (|0\rangle_2 + i|1\rangle_2 - |2\rangle_2 - i|3\rangle_2).$$

Matrix representation w.r.t. standard basis:

$$M_{(\mathbf{F}^{\otimes 2})^*} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

## Proof.

Consider the linear operator  $\mathbf{U} : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$  defined by

$$\mathbf{U} |z\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(-2\pi i \frac{zy}{2^n}\right) |y\rangle_n \quad (444)$$

for all  $0 \leq z < 2^n$ .

Claim that  $\mathbf{U} = (\mathbf{F}^{\otimes n})^*$ .

## Proof (cont'd).

Indeed,

$$\begin{aligned}
\langle \mathbf{U} |z\rangle_n, |x\rangle_n \rangle &= \left\langle 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(-2\pi i \frac{zy}{2^n}\right) |y\rangle_n, |x\rangle_n \right\rangle \\
&= 2^{-n/2} \sum_{y=0}^{2^n-1} \overline{\exp\left(-2\pi i \frac{zy}{2^n}\right)} \langle |y\rangle_n, |x\rangle_n \rangle \\
&= 2^{-n/2} \exp\left(2\pi i \frac{zx}{2^n}\right) \\
&= 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{yx}{2^n}\right) \langle |z\rangle_n, |y\rangle_n \rangle \\
&= \left\langle |z\rangle_n, 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{yx}{2^n}\right) |y\rangle_n \right\rangle \\
&= \langle |z\rangle_n, \mathbf{F}^{\otimes n} |x\rangle_n \rangle.
\end{aligned}$$

## Proof (cont'd).

Moreover,

$$\begin{aligned}
& \mathbf{UF}^{\otimes n} |x\rangle_n \\
&= \mathbf{U} \left( 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{xy}{2^n}\right) |y\rangle_n \right) \\
&= 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{xy}{2^n}\right) \mathbf{U} |y\rangle_n \\
&= 2^{-n/2} \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{xy}{2^n}\right) 2^{-n/2} \sum_{z=0}^{2^n-1} \exp\left(-2\pi i \frac{yz}{2^n}\right) |z\rangle_n \\
&= 2^{-n} \sum_{y=0}^{2^n-1} \sum_{z=0}^{2^n-1} \exp\left(2\pi i \frac{y(x-z)}{2^n}\right) |z\rangle_n \\
&= 2^{-n} \sum_{z=0}^{2^n-1} \left( \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{x-z}{2^n} y\right) \right) |z\rangle_n \stackrel{!}{=} |x\rangle_n.
\end{aligned}$$

## Proof (cont'd).

For each number  $r \neq 1$ , the sum of the first  $n$  terms of a geometric series is

$$a + ar + ar^2 + \dots + ar^{n-1} = a \left( \frac{1 - r^n}{1 - r} \right). \quad (445)$$

Thus for  $x \neq z$ ,

$$\begin{aligned} \sum_{y=0}^{2^n-1} \exp \left( 2\pi i \frac{x-z}{2^n} \right)^y &= \frac{1 - \exp \left( 2\pi i \frac{x-z}{2^n} \right)^{2^n}}{1 - \exp \left( 2\pi i \frac{x-z}{2^n} \right)} \\ &= \frac{1 - \exp (2\pi i (x-z))}{1 - \exp \left( 2\pi i \frac{x-z}{2^n} \right)} \\ &= \frac{1 - 1}{1 - \exp \left( 2\pi i \frac{x-z}{2^n} \right)} \\ &= 0. \end{aligned}$$

So for  $x \neq z$ , the inner sum is 0, and for  $x = z$ , the inner sum is  $2^n$ . □

## Quantum Fourier Transform

The **F**-gate has the representations

$$\begin{aligned} \mathbf{F}^{\otimes n} |x\rangle_n & \quad (446) \\ &= 2^{-n/2} \bigotimes_{m=1}^n \left( |0\rangle + \exp\left(2\pi i \frac{x}{2^m}\right) |1\rangle \right) \end{aligned}$$

for all  $0 \leq x < 2^n$ , or

$$\begin{aligned} \mathbf{F}^{\otimes n} |x_{n-1} \dots x_1 x_0\rangle & \quad (447) \\ &= 2^{-n/2} \bigotimes_{m=1}^n \left( |0\rangle + \exp\left(2\pi i \sum_{j=0}^{m-1} \frac{x_j}{2^{m-j}}\right) |1\rangle \right) \end{aligned}$$

for all  $(x_{n-1}, \dots, x_1, x_0) \in \mathbb{B}^n$ .

## Proof.

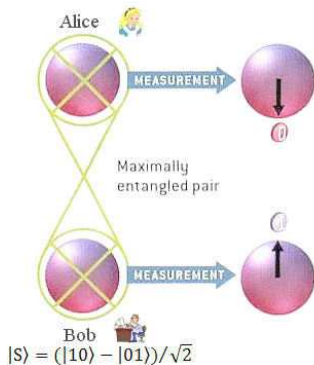
The first equality follows by induction on  $n$ .

In the second equality, the exponential term of the first equation is transformed as follows,

$$\begin{aligned}
 \exp\left(2\pi i \frac{x}{2^m}\right) &= \exp\left(2\pi i \sum_{j=0}^{n-1} \frac{x_j 2^j}{2^m}\right) \\
 &= \exp\left(2\pi i \sum_{j=0}^{m-1} \frac{x_j}{2^{m-j}} + 2\pi i \sum_{j=m}^{n-1} x_j 2^{j-m}\right) \\
 &= \exp\left(2\pi i \sum_{j=0}^{m-1} \frac{x_j}{2^{m-j}}\right) \prod_{j=m}^{n-1} \exp\left(2\pi i x_j 2^{j-m}\right) \\
 &= \exp\left(2\pi i \sum_{j=0}^{m-1} \frac{x_j}{2^{m-j}}\right).
 \end{aligned}$$



## Measurement



## Measurement

- Qubit measurement
- Measurement operators
- Multi-qubit measurement
- Partial measurement

## Qubit Measurement

- Measurement is an operation to gain information about the state of a qubit

$$v = \lambda_0 |0\rangle + \lambda_1 |1\rangle, \quad (448)$$

where

$$|\lambda_0|^2 + |\lambda_1|^2 = 1. \quad (449)$$

- The result of measurement is either  $|0\rangle$  with probability  $p_0 = |\lambda_0|^2$  or  $|1\rangle$  with probability  $p_1 = |\lambda_1|^2$ .
- After measurement, the qubit is in the pure state  $\frac{\lambda_0}{|\lambda_0|} |0\rangle$  or  $\frac{\lambda_1}{|\lambda_1|} |1\rangle$  (classical bit).
- The measurement of the original qubit  $v$  cannot be repeated.

## Qubit Measurement

The measurement of a qubit  $v = \lambda_0 |0\rangle + \lambda_1 |1\rangle$  is the realization of a random variable  $X^v$  with

$$\mathbb{P}(X^v = 0) = p_0 = |\lambda_0|^2 \quad (450)$$

and

$$\mathbb{P}(X^v = 1) = p_1 = |\lambda_1|^2. \quad (451)$$

## Measurement Operators

Let  $n \geq 1$ . A collection of measurement operators  $\{M_0, \dots, M_{m-1}\}$  on  $\mathcal{H}^{\otimes n}$  consists of linear operators

$$M_j : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}, \quad 0 \leq j \leq m-1, \quad (452)$$

such that

$$\sum_{j=0}^{m-1} M_j^* M_j = I, \quad (453)$$

where  $M_j^*$  denotes the *adjoint operator* of  $M_j$ .

## Measurement Operators

For each collection of measurement operators  $\{M_0, \dots, M_{m-1}\}$  on  $\mathcal{H}^{\otimes n}$  and each  $n$ -qubit  $v \in \mathcal{S}_{\mathcal{H}^{\otimes n}}$ ,

$$\begin{aligned}
 \sum_{j=0}^{m-1} \|M_j v\|^2 &= \sum_{j=0}^{m-1} \langle M_j v, M_j v \rangle & (454) \\
 &= \sum_{j=0}^{m-1} \langle v, M_j^* M_j v \rangle \\
 &= \left\langle v, \sum_{j=0}^{m-1} M_j^* M_j v \right\rangle \\
 &= \langle v, v \rangle = \|v\|^2 \\
 &= 1.
 \end{aligned}$$

## Multi-Qubit Measurement

The *measurement* of an  $n$ -qubit  $v \in \mathcal{S}_{\mathcal{H}^{\otimes n}}$  by the collection of measurement operators  $\{M_0, \dots, M_{m-1}\}$  on  $\mathcal{H}^{\otimes n}$  is the realization of a random variable  $X_{M_0, \dots, M_{m-1}}^v$  with

$$\mathbb{P}(X_{M_0, \dots, M_{m-1}}^v = j) = p_j = \|M_j v\|^2. \quad (455)$$

Well-definedness follows from

$$\sum_{j=0}^{m-1} \|M_j v\|^2 = 1. \quad (456)$$

After measurement, the  $n$ -qubit  $v$  becomes the  $n$ -qubit

$$\frac{M_j v}{\|M_j v\|} = \frac{1}{\sqrt{p_j}} M_j v. \quad (457)$$

## Dual Space

Consider the Hilbert space  $\mathcal{H}^{\otimes n}$  with standard basis

$$\{|0\rangle_n, |1\rangle_n, \dots, |2^n - 1\rangle_n\}. \quad (458)$$

- For each basis element  $|j\rangle_n \in \mathcal{H}^{\otimes n}$ ,  $0 \leq j \leq 2^n - 1$ , define the linear functional  $\langle j|_n : \mathcal{H}^{\otimes n} \rightarrow \mathbb{C}$  given by (bra notation)

$$\langle j|_n (|k\rangle_n) = \langle j|_n, |k\rangle_n = \delta_{j,k}, \quad (459)$$

where  $\delta_{j,k} = 1$  if  $j = k$  and 0 if  $j \neq k$  (Kronecker delta).

- The set

$$\{\langle 0|_n, \langle 1|_n, \dots, \langle 2^n - 1|_n\} \quad (460)$$

forms a basis of the dual space of  $\mathcal{H}^{\otimes n}$ .

## Dual Space

The linear operator  $M_j = |j\rangle_n \langle j|_n$  given by

$$M_j |k\rangle_n = |j\rangle_n \langle j|_n |k\rangle_n \quad (461)$$

is a projection of  $\mathcal{H}^{\otimes n}$  onto the one-dimensional subspace spanned by  $|j\rangle_n$ , since

$$M_j \sum_{k=0}^{2^n-1} \lambda_k |k\rangle_n = \sum_{k=0}^{2^n-1} \lambda_k |j\rangle_n \langle j|_n |k\rangle_n = \lambda_j |j\rangle_n. \quad (462)$$

## Multi-Qubit Measurement

The measurement of an  $n$ -qubit  $v = \sum_{k=0}^{2^n-1} \lambda_k |k\rangle_n \in \mathcal{S}_{\mathcal{H}^{\otimes n}}$  by the collection of measurement operators  $\{M_0, \dots, M_{2^n-1}\}$  on  $\mathcal{H}^{\otimes n}$  with

$$M_j = |j\rangle_n \langle j|_n, \quad 0 \leq j \leq 2^n - 1, \quad (463)$$

is the realization of a random variable  $X_n^v$  with

$$\mathbb{P}(X_n^v = j) = p_j = |\lambda_j|^2. \quad (464)$$

After measurement, the  $n$ -qubit  $v$  becomes the pure  $n$ -qubit

$$\frac{\lambda_j}{|\lambda_j|} |j\rangle_n. \quad (465)$$

## Proof.

The operator  $M_j$  is self-adjoint. Indeed, let  $v, w \in \mathbf{H}^{\otimes n}$ . Then

$$\begin{aligned} \langle M_j v, w \rangle &= \langle M_j \sum_{k=0}^{2^n-1} \lambda_k |k\rangle, w \rangle \\ &= \langle \lambda_j |j\rangle, w \rangle = \bar{\lambda}_j \langle |j\rangle, \sum_{k=0}^{2^n-1} \mu_k |k\rangle \rangle \\ &= \bar{\lambda}_j \mu_j. \end{aligned}$$

Similarly,

$$\begin{aligned} \langle v, M_j w \rangle &= \langle v, M_j \sum_{k=0}^{2^n-1} \mu_k |k\rangle \rangle \\ &= \langle v, \mu_j |j\rangle \rangle = \mu_j \langle \sum_{k=0}^{2^n-1} \lambda_k |k\rangle, |j\rangle \rangle \\ &= \bar{\lambda}_j \mu_j. \end{aligned}$$

## Proof (cont'd)

Moreover, we have

$$\begin{aligned}
 M_j^* M_j &= (|j\rangle_n \langle j|_n)^* |j\rangle_n \langle j|_n = |j\rangle_n \langle j|_n |j\rangle_n \langle j|_n \\
 &= |j\rangle_n (\langle j|_n |j\rangle_n) \langle j|_n = |j\rangle_n \delta_{j,j} \langle j|_n \\
 &= |j\rangle_n \langle j|_n = M_j.
 \end{aligned}$$

Thus for each  $n$ -qubit  $v = \sum_{k=0}^{2^n-1} \lambda_k |k\rangle_n$ ,

$$\sum_{j=0}^{2^n-1} M_j^* M_j v = \sum_{j=0}^{2^n-1} M_j v = \sum_{j=0}^{2^n-1} \lambda_j |j\rangle_n = v$$

and so

$$\sum_{j=0}^{2^n-1} M_j^* M_j = I.$$

Hence,  $\{M_0, \dots, M_{2^n-1}\}$  is a set of measurement operators.

## Proof (cont'd)

Therefore,  $\mathbb{P}(X_n = j) = p_j$  becomes

$$\begin{aligned}\|M_j v\|^2 &= \langle M_j v, M_j v \rangle = \langle v, M_j^* M_j v \rangle \\ &= \langle v, M_j v \rangle = \langle v, \lambda_j |j\rangle_n \rangle \\ &= \langle \lambda_j |j\rangle_n, \lambda_j |j\rangle_n \rangle \\ &= \overline{\lambda_j} \lambda_j = |\lambda_j|^2.\end{aligned}$$

The state after measurement is

$$\frac{1}{\sqrt{p_j}} M_j v = \frac{1}{\sqrt{|\lambda_j|^2}} \lambda_j |j\rangle_n = \frac{\lambda_j}{|\lambda_j|} |j\rangle_n.$$



## Multi-Qubit Measurement – Example

Consider the bi-qubit

$$v = \frac{1}{\sqrt{2}} |00\rangle_2 - \frac{1}{2} |01\rangle_2 + \frac{1}{2} |10\rangle_2.$$

Measurement:

Resulting State	Probability
$ 00\rangle$	$\frac{1}{2}$
$- 01\rangle$	$\frac{1}{4}$
$ 10\rangle$	$\frac{1}{4}$
$ 11\rangle$	0

## Partial Multi-Qubit Measurement

Let  $n \geq 1$ . Let  $p$  be an integer with  $1 \leq p < n$  and  $q = n - p$ .

Take the collection of measurement operators  $\{M_0, \dots, M_{2^p-1}\}$  on  $\mathcal{H}^{\otimes n}$  with

$$M_j = \sum_{r=0}^{2^q-1} \left( |j\rangle_p \otimes |r\rangle_q \right) \left( |j\rangle_p \otimes |r\rangle_q \right)^*, \quad 0 \leq j \leq 2^p - 1. \quad (466)$$

The *partial measurement* of the first  $p$  qubits of an  $n$ -qubit

$$v = \sum_{k=0}^{2^n-1} \lambda_k |k\rangle_n \quad (467)$$

by  $\{M_0, \dots, M_{2^p-1}\}$  is the realization of a random variable  $X_p^v$  with

$$\mathbb{P}(X_p^v = j) = p_j = \sum_{r=0}^{2^q-1} |\lambda_{j \cdot 2^q + r}|^2 \quad (468)$$

where  $0 \leq j \leq 2^p - 1$

## Partial Multi-Qubit Measurement

After measurement, the  $n$ -qubit  $v$  becomes the  $n$ -qubit

$$|j\rangle_p \otimes \sum_{r=0}^{2^q-1} \frac{\lambda_j \cdot 2^{q+r}}{\sqrt{p_j}} |r\rangle_q. \quad (469)$$

## Proof.

Above we have seen that

$$M_j^* M_j = M_j, \quad 0 \leq j \leq 2^p - 1.$$

For each  $n$ -qubit  $v = \sum_{k=0}^{2^n-1} \lambda_k |k\rangle_n$ , write

$$v = \sum_{j=0}^{2^p-1} \sum_{r=0}^{2^q-1} \lambda_{j,r} |j\rangle_p \otimes |r\rangle_q$$

where  $\lambda_{j,r} = \lambda_{j \cdot 2^q + r}$  and  $|j\rangle_p \otimes |r\rangle_q = |j \cdot 2^q + r\rangle_n$ .

## Proof (cont'd)

Therefore,

$$\begin{aligned}
 M_j v &= \sum_{r=0}^{2^q-1} \sum_{k=0}^{2^n-1} \lambda_k \left( |j\rangle_p \otimes |r\rangle_q \right) \left( |j\rangle_p \otimes |r\rangle_q \right)^* |k\rangle_n \\
 &= \sum_{r=0}^{2^q-1} \lambda_{j \cdot 2^q + r} \left( |j\rangle_p \otimes |r\rangle_q \right) \\
 &= |j\rangle_p \otimes \sum_{r=0}^{2^q-1} \lambda_{j \cdot 2^q + r} |r\rangle_q.
 \end{aligned}$$

## Proof (cont'd)

It follows that

$$\begin{aligned}
 \sum_{j=0}^{2^p-1} M_j^* M_j v &= \sum_{j=0}^{2^p-1} M_j v \\
 &= \sum_{j=0}^{2^p-1} |j\rangle_p \otimes \sum_{r=0}^{2^q-1} \lambda_{j \cdot 2^q + r} |r\rangle_q \\
 &= v.
 \end{aligned}$$

Thus

$$\sum_{j=0}^{2^p-1} M_j^* M_j = I$$

and hence  $\{M_0, \dots, M_{2^p-1}\}$  is a set of measurement operators.

## Proof (cont'd)

Therefore,  $\mathbb{P}(X_p^v = j) = p_j$  becomes

$$\begin{aligned}
 \|M_j v\|^2 &= \langle M_j v, M_j v \rangle = \langle v, M_j^* M_j v \rangle \\
 &= \langle v, M_j v \rangle \\
 &= \sum_{r=0}^{2^q-1} \overline{\lambda_{j \cdot 2^q+r}} \lambda_{j \cdot 2^q+r} \\
 &= \sum_{r=0}^{2^q-1} |\lambda_{j \cdot 2^q+r}|^2.
 \end{aligned}$$

The state after the measurement is

$$\frac{1}{\sqrt{p_j}} M_j v = |j\rangle_p \otimes \sum_{r=0}^{2^q-1} \frac{\lambda_{j \cdot 2^q+r}}{\sqrt{p_j}} |r\rangle_q.$$



## Partial Multi-Qubit Measurement – Example

Let  $n = 3$ ,  $p = 1$ , and  $q = n - p = 2$ . Then

$$|000\rangle_3 = |0\rangle_1 \otimes |00\rangle_2,$$

$$|001\rangle_3 = |0\rangle_1 \otimes |01\rangle_2,$$

$$|010\rangle_3 = |0\rangle_1 \otimes |10\rangle_2,$$

$$|011\rangle_3 = |0\rangle_1 \otimes |11\rangle_2,$$

$$|100\rangle_3 = |1\rangle_1 \otimes |00\rangle_2,$$

$$|101\rangle_3 = |1\rangle_1 \otimes |01\rangle_2,$$

$$|110\rangle_3 = |1\rangle_1 \otimes |10\rangle_2,$$

$$|111\rangle_3 = |1\rangle_1 \otimes |11\rangle_2.$$

## Partial Multi-Qubit Measurement – Example (cont'd)

Take the 3-qubit

$$\begin{aligned} v &= \frac{1}{\sqrt{3}} (|011\rangle_3 + |100\rangle_3 + |101\rangle_3) \\ &= \frac{1}{\sqrt{3}} |0\rangle_1 \otimes |11\rangle_2 + \frac{1}{\sqrt{3}} (|1\rangle_1 \otimes (|00\rangle_2 + |01\rangle_2)). \end{aligned}$$

Measurement of first qubit gives state

$$|0\rangle_1 \otimes |11\rangle_2$$

with probability  $p_0 = \frac{1}{3}$  and state

$$|1\rangle_1 \otimes \frac{1}{\sqrt{2}} (|00\rangle_2 + |01\rangle_2)$$

with probability  $p_1 = \frac{2}{3}$ .

## Partial Multi-Qubit Measurement – Separability

Let  $n \geq 1$ . Let  $p$  be an integer with  $1 \leq p < n$  and  $q = n - p$ .

Take the collection of measurement operators  $\{M_0, \dots, M_{2^p-1}\}$  on  $\mathcal{H}^{\otimes n}$  with

$$M_j = \sum_{r=0}^{2^q-1} \left( |j\rangle_p \otimes |r\rangle_q \right) \left( |j\rangle_p \otimes |r\rangle_q \right)^*, \quad 0 \leq j \leq 2^p - 1. \quad (470)$$

The partial measurement of the first  $p$  qubits of a separable  $n$ -qubit

$$v = x \otimes y = \sum_{k=0}^{2^p-1} \lambda_k |k\rangle_p \otimes \sum_{r=0}^{2^q-1} \mu_r |r\rangle_q \quad (471)$$

by  $\{M_0, \dots, M_{2^p-1}\}$  is the realization of a random variable  $X_p^v$  with

$$\mathbb{P}(X_p^v = j) = p_j = |\lambda_j|^2 \quad (472)$$

where  $0 \leq j \leq 2^p - 1$ .

## Partial Multi-Qubit Measurement – Separability

After measurement, the  $n$ -qubit  $v$  becomes the  $n$ -qubit

$$\left( \frac{\lambda_j}{|\lambda_j|} |j\rangle_p \right) \otimes y. \quad (473)$$

## Proof.

Above we have seen that

$$M_j^* M_j = M_j, \quad 0 \leq j \leq 2^p - 1.$$

We have

$$\begin{aligned} v &= x \otimes y = \sum_{k=0}^{2^p-1} \lambda_k |k\rangle_p \otimes \sum_{r=0}^{2^q-1} \mu_r |r\rangle_q \\ &= \sum_{k=0}^{2^p-1} \sum_{r=0}^{2^q-1} \lambda_k \mu_r (|k\rangle_p \otimes |r\rangle_q) \\ &= \sum_{i=0}^{2^p-1} \sum_{r=0}^{2^q-1} \lambda_k \mu_r |k \cdot 2^q + r\rangle_n \\ &= \sum_{j=0}^{2^n-1} \nu_j |j\rangle_n, \end{aligned}$$

where  $\nu_{k \cdot 2^q + r} = \lambda_k \mu_r$  and  $|k \cdot 2^q + r\rangle_n = |k\rangle_p \otimes |r\rangle_q$ .

## Proof (cont'd)

Therefore,

$$\begin{aligned}
 & M_j v \\
 &= \sum_{r=0}^{2^q-1} \sum_{k=0}^{2^p-1} \sum_{s=0}^{2^q-1} \lambda_k \mu_r \left( |j\rangle_p \otimes |r\rangle_q \right) \left( |j\rangle_p \otimes |r\rangle_q \right)^* \left( |k\rangle_p \otimes |s\rangle_q \right) \\
 &= \sum_{r=0}^{2^q-1} \lambda_j \mu_r \left( |j\rangle_p \otimes |r\rangle_q \right) \\
 &= \lambda_j |j\rangle_p \otimes \sum_{r=0}^{2^q-1} \mu_r |r\rangle_q.
 \end{aligned}$$

It follows that

$$\sum_{j=0}^{2^p-1} M_j^* M_j = I.$$

Hence,  $\{M_0, \dots, M_{2^p-1}\}$  is a set of measurement operators.

## Proof (cont'd)

Therefore,  $\mathbb{P}(X_p^v = j) = p_j$  becomes

$$\begin{aligned}
 \|M_j v\|^2 &= \langle M_j v, M_j v \rangle = \langle v, M_j^* M_j v \rangle \\
 &= \langle v, M_j v \rangle \\
 &= \bar{\lambda}_j \lambda_j + \sum_{r=0}^{2^q-1} \bar{\mu}_r \mu_r \\
 &= |\lambda_j|^2 + \sum_{r=0}^{2^q-1} |\mu_r|^2 \\
 &= |\lambda_j|^2.
 \end{aligned}$$

## Proof (cont'd)

The state after the measurement is

$$\begin{aligned} \frac{1}{\sqrt{p_j}} M_j v &= \frac{\lambda_j}{|\lambda_j|} |j\rangle_n \otimes \sum_{r=0}^{2^q-1} \mu_r |r\rangle_q \\ &= \frac{\lambda_j}{|\lambda_j|} |j\rangle_n \otimes y. \end{aligned}$$



## Multi-Qubit Measurement – Example

Consider the separable bi-qubit

$$\begin{aligned} v &= \frac{1}{\sqrt{6}} |00\rangle - \frac{1}{\sqrt{6}} |01\rangle + \frac{1}{\sqrt{3}} |10\rangle - \frac{1}{\sqrt{3}} |11\rangle \\ &= \left( \frac{1}{\sqrt{3}} |0\rangle + \sqrt{\frac{2}{3}} |1\rangle \right) \otimes \left( \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right). \end{aligned}$$

The measurement of the first qubit shows the following:

Result	Resulting State	Probability
0	$ 0\rangle \otimes \left( \frac{1}{\sqrt{2}}  0\rangle - \frac{1}{\sqrt{2}}  1\rangle \right)$	$\frac{1}{3}$
1	$ 1\rangle \otimes \left( \frac{1}{\sqrt{2}}  0\rangle - \frac{1}{\sqrt{2}}  1\rangle \right)$	$\frac{2}{3}$

# Part IX

## Quantum Algorithms

## Quantum Algorithms

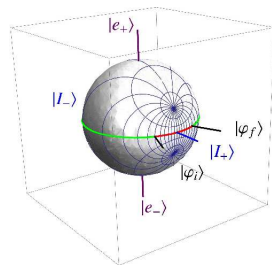
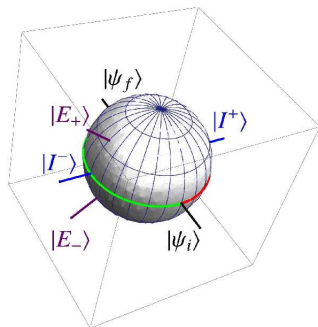
- Quantum computing is computing using quantum-mechanical phenomena.
- List of available QC algorithms:

[www.quantumalgorithmzoo.org](http://www.quantumalgorithmzoo.org)

maintained by St. Jordan (Microsoft Quantum).

- Large-scale quantum computers may be able to efficiently solve problems which are not practically feasible on classical computers.
- Post-quantum cryptography aims at cryptographic algorithms secure against QC attacks. Theory is in its infancy.
- Announcements (2017/2018): 50-qubit QC (IBM), 49-qubit QC (Intel), 72-qubit QC (Google).

## Quantum Algorithms



## Contents

- Generalities
- Deutsch
- Deutsch-Jozsa
- \* Grover
- \* Shor

## Contents

Generalities  
Deutsch  
Deutsch-Jozsa  
\* Grover  
\* Shor

## Quantum Algorithms

- General quantum algorithms
- Deutsch algorithm
- Deutsch-Jozsa algorithm
- \*Grover algorithm
- \*Shor algorithm

## Quantum Algorithms

A quantum algorithm consists of three parts:

- 1 Input: classical  $n$ -bit tuple, conversion into  $n$ -qubit.
- 2 Processing: application of a finite sequence of unitary operators on the given  $n$ -qubit.
  - Processing is deterministic and reversible (by using the inverse unitary operators).
- 3 Output: measurement gives classical  $n$ -bit tuple.
  - Measurement is probabilistic and irreversible.

## Quantum Algorithms – Formulation

- Initial state:  $n$ -qubit  $v \in \mathcal{S}_{\mathcal{H}^{\otimes n}}$ .
- Computation: unitary operator  $U : \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n}$  or associated representation matrix  $M_U \in \mathbb{C}^{2^n \times 2^n}$ .

- Final state:

$$w = U(v) = \sum_{j=0}^{2^n-1} w_j |j\rangle_n \in \mathcal{S}_{\mathcal{H}^{\otimes n}}. \quad (474)$$

- Measurement: random variable  $Y = X_n^w$ , where

$$\mathbb{P}(Y = j) = |w_j|^2, \quad 0 \leq j \leq 2^n - 1. \quad (475)$$

- Complexity of classical computation:
  - runtime  $O(2^{2n})$ , size of unitary matrix  $M_U$ ,
  - storage  $O(2^n)$ , size of Hilbert space  $\mathcal{H}^{\otimes n}$ .

## Quantum Algorithms – Full Separability

- A fully separable  $n$ -qubit  $v \in \mathcal{H}^{\otimes n}$  has the form

$$v = \bigotimes_{m=1}^n (\alpha_m |0\rangle + \beta_m |1\rangle), \quad (476)$$

where  $\alpha_m, \beta_m \in \mathbb{C}$ ,  $1 \leq m \leq n$ .

- The  $n$ -qubit  $v$  has storage complexity  $O(n)$ .
- Each  $n$ -qubit  $|x\rangle_n$ ,  $0 \leq x \leq 2^n - 1$ , has a fully separated representation

$$|x\rangle_n = \bigotimes_{m=1}^n ((1 - x_{n-m}) |0\rangle + x_{n-m} |1\rangle), \quad (477)$$

where  $x = \sum_{j=0}^{n-1} x_j 2^j$ ,  $x_j \in \mathbb{B}$ ,  $0 \leq j \leq n - 1$ .

## Quantum Algorithms – Hadamard Gate

$$\mathbf{H}^{\otimes n} \left( \bigotimes_{m=1}^n (\alpha_m |0\rangle + \beta_m |1\rangle) \right) = \bigotimes_{m=1}^n (\hat{\alpha}_m |0\rangle + \hat{\beta}_m |1\rangle), \quad (478)$$

where

$$\hat{\alpha}_m = \frac{\alpha_m + \beta_m}{\sqrt{2}}, \quad \hat{\beta}_m = \frac{\alpha_m - \beta_m}{\sqrt{2}}, \quad 1 \leq m \leq n. \quad (479)$$

Runtime complexity  $O(n)$ .

## Proof.

$$\begin{aligned}
& \mathbf{H}^{\otimes n} \left( \bigotimes_{m=1}^n (\alpha_m |0\rangle + \beta_m |1\rangle) \right) \\
&= \bigotimes_{m=1}^n (\mathbf{H}(\alpha_m |0\rangle + \beta_m |1\rangle)) \\
&= \bigotimes_{m=1}^n (\alpha_m \mathbf{H} |0\rangle + \beta_m \mathbf{H} |1\rangle) \\
&= \bigotimes_{m=1}^n \left( \alpha_m \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta_m \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \\
&= \bigotimes_{m=1}^n \left( \frac{\alpha_m + \beta_m}{\sqrt{2}} |0\rangle + \frac{\alpha_m - \beta_m}{\sqrt{2}} |1\rangle \right).
\end{aligned}$$



## Quantum Algorithms – Hadamard Gate

By (478),

$$\mathbf{H}^{\otimes n} |0\rangle_n = \bigotimes_{m=1}^n \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \quad (480)$$

and

$$\mathbf{H}^{\otimes n} |1\rangle_n = \bigotimes_{m=1}^n \left( \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right). \quad (481)$$

## Quantum Algorithms – Fourier Transform

$$\begin{aligned}
 \mathbf{F}^{\otimes n} & \left( \bigotimes_{m=1}^n (\alpha_m |0\rangle + \beta_m |1\rangle) \right) & (482) \\
 & = \sum_{x=0}^{2^n-1} \bigotimes_{m=1}^n \left( \frac{\alpha_m(1-x_{n-m}) + \beta_m x_{n-m}}{\sqrt{2}} |0\rangle \right. \\
 & \quad \left. + \frac{\alpha_m(1-x_{n-m}) + \beta_m x_{n-m}}{\sqrt{2}} \exp \left( 2\pi i \sum_{j=0}^{m-1} \frac{x_j}{2^{m-j}} \right) |1\rangle \right).
 \end{aligned}$$

Runtime complexity  $O(2^n)$ .

## Proof.

$$\begin{aligned}
& \mathbf{F}^{\otimes n} \left( \bigotimes_{m=1}^n (\alpha_m |0\rangle + \beta_m |1\rangle) \right) \\
&= \mathbf{F}^{\otimes n} \sum_{x=0}^{2^n-1} \left( \prod_{m=1}^n (\alpha_m (1-x_{n-m}) + \beta_m x_{n-m}) \right) |x\rangle_n \\
&= \sum_{x=0}^{2^n-1} \left( \prod_{m=1}^n (\alpha_m (1-x_{n-m}) + \beta_m x_{n-m}) \right) \mathbf{F}^{\otimes n} |x\rangle_n \\
&= \sum_{x=0}^{2^n-1} \left( \prod_{m=1}^n (\alpha_m (1-x_{n-m}) + \beta_m x_{n-m}) \right) \\
&\quad \bigotimes_{m=1}^n \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} \exp \left( 2\pi i \sum_{j=0}^{m-1} \frac{x_j}{2^{m-j}} \right) |1\rangle \right), \text{ by (447),} \\
&= \sum_{x=0}^{2^n-1} \bigotimes_{m=1}^n \left( \frac{\alpha_m (1-x_{n-m}) + \beta_m x_{n-m}}{\sqrt{2}} |0\rangle \right. \\
&\quad \left. + \frac{\alpha_m (1-x_{n-m}) + \beta_m x_{n-m}}{\sqrt{2}} \exp \left( 2\pi i \sum_{j=0}^{m-1} \frac{x_j}{2^{m-j}} \right) |1\rangle \right).
\end{aligned}$$

□

## Measurement – Classical Computation

Measurement of  $n$ -qubit  $w = \sum_{j=0}^{2^n-1} w_j |j\rangle_n \in \mathcal{S}_{\mathcal{H}^{\otimes n}}$  by classical computation:

$$\alpha_0 = 0, \quad \alpha_k = \sum_{j=0}^k |w_j|^2, \quad 1 \leq k \leq 2^n. \quad (483)$$

Choose value  $r \in [0, 1]$  uniformly at random such that if  $r \in [\alpha_k, \alpha_{k+1})$ , the result is  $Y = k$ .

### Example

Let

$$(p_0, p_1, p_2, p_3) = (0.1, 0.2, 0.4, 0.3).$$

Then

$$(\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4) = (0.0, 0.1, 0.3, 0.7, 1.0)$$

Choose  $r \in [0, 1]$  uniformly at random.

- If  $r \in [0.0, 0.1)$ , then  $Y = 0$ .
- If  $r \in [0.1, 0.3)$ , then  $Y = 1$ .
- If  $r \in [0.3, 0.7)$ , then  $Y = 2$ .
- If  $r \in [0.7, 1.0]$ , then  $Y = 3$ .

## Deutsch Algorithm (1985)

**Require:** Boolean function  $f : \mathbb{B} \rightarrow \mathbb{B}$ , Hilbert space  $\mathcal{H}^{\otimes 2}$  with basis  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

**Ensure:**  $Y = 1$  if  $f$  is balanced, i.e.,  $f(0) \neq f(1)$ , and  $Y = 0$  if  $f$  is constant, i.e.,  $f(0) = f(1)$ .

$$\psi_0 \leftarrow |01\rangle_2$$

$$\psi_1 \leftarrow \mathbf{H}^{\otimes 2} \psi_0$$

$$\psi_2 \leftarrow \mathbf{U}_f \psi_1$$

$$\psi_3 \leftarrow \mathbf{H}_1^{(2)} \psi_2$$

$$Y \leftarrow X_1^{\psi_3} \{\text{Partial measurement of first qubit}\}$$

## Unary Boolean Functions

- The number of  $n$ -ary Boolean functions is  $2^{2^n}$ ,  $n \geq 0$ .
- The unary Boolean functions are

$x$	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
0	0	0	1	1
1	0	1	0	1

The functions  $f_0, f_3$  are constant, and the functions  $f_1 = \text{id}, f_2 = \text{not}$  are balanced.

## Proof.

First statement:

$$\begin{aligned}\psi_1 &= \mathbf{H}^{\otimes 2} |01\rangle_2 = (\mathbf{H} |0\rangle) \otimes (\mathbf{H} |1\rangle) & (484) \\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= \frac{1}{\sqrt{2}} \sum_{x=0}^1 |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.\end{aligned}$$

## Proof (cont'd).

Second statement:

$$\begin{aligned}
 \psi_2 &= \mathbf{U}_f \psi_1 = \mathbf{U}_f \left( \frac{1}{\sqrt{2}} \sum_{x=0}^1 |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & (485) \\
 &= \frac{1}{\sqrt{2}} \sum_{x=0}^1 \mathbf{U}_f \left( |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
 &= \frac{1}{\sqrt{2}} \sum_{x=0}^1 \left( |x\rangle \otimes \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right) \\
 &= \frac{1}{\sqrt{2}} \sum_{x=0}^1 \left( |x\rangle \otimes \frac{(-1)^{f(x)} (|0\rangle - |1\rangle)}{\sqrt{2}} \right) \\
 &= \frac{1}{\sqrt{2}} \sum_{x=0}^1 \left( (-1)^{f(x)} \cdot |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
 &= \frac{1}{\sqrt{2}} \left( (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.
 \end{aligned}$$

## Proof (cont'd).

Third and fourth statements:

$$\begin{aligned}
 \psi_3 &= \mathbf{H}_1^{(2)} \psi_2 = (\mathbf{H} \otimes \mathbf{I}) \psi_2 & (486) \\
 &= \frac{1}{\sqrt{2}} \left( (-1)^{f(0)} \mathbf{H}(|0\rangle) + (-1)^{f(1)} \mathbf{H}(|1\rangle) \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \frac{1}{2} \left( (-1)^{f(0)} (|0\rangle + |1\rangle) + (-1)^{f(1)} (|0\rangle - |1\rangle) \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \left( \frac{(-1)^{f(0)} + (-1)^{f(1)}}{2} |0\rangle + \frac{(-1)^{f(0)} - (-1)^{f(1)}}{2} |1\rangle \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \pm |f(0) \oplus f(1)\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \begin{cases} \pm |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) = f(1), \\ \pm |1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(0) \neq f(1). \end{cases}
 \end{aligned}$$

Thus the partial measurement of the first qubit results in  $|0\rangle$  with probability 1 if  $f$  is constant, and otherwise in  $|1\rangle$  with probability 1. □

## Deutsch-Jozsa Algorithm (1992)

**Require:** Boolean function  $f : \mathbb{B}^n \rightarrow \mathbb{B}$  constant or balanced,  
Hilbert space  $\mathcal{H}^{\otimes(n+1)}$

**Ensure:**  $Y = 0$  if  $f$  is constant with probability 1; otherwise,  $f$  is balanced.

$$\psi_0 \leftarrow |0\rangle_n |1\rangle_1$$

$$\psi_1 \leftarrow \mathbf{H}^{\otimes(n+1)} \psi_0$$

$$\psi_2 \leftarrow \mathbf{U}_f \psi_1$$

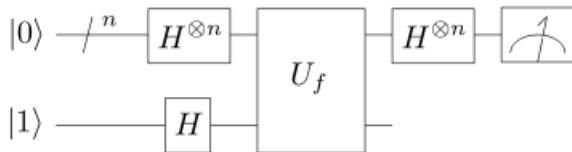
$$\psi_3 \leftarrow (\mathbf{H}^{\otimes n} \otimes \mathbf{I}) \psi_2$$

$$Y \leftarrow X_n^{\psi_3} \{\text{Partial measurement of first } n \text{ qubits}\}$$

## Deutsch-Jozsa Algorithm

- If an  $n$ -ary Boolean function  $f$  is assumed to be either constant or balanced, a conventional deterministic algorithm requires  $2^{n-1} + 1$  evaluations for the decision.
- The DJ algorithm produces an answer that is always correct with a single evaluation of  $f$ .
- Inspiration for two of the most revolutionary quantum algorithms of Grover and Shor.

## Deutsch-Jozsa Quantum Circuit



## Proof.

First statement:

$$\begin{aligned}
 \psi_1 &= \mathbf{H}^{\otimes(n+1)}(|0\rangle_n |1\rangle) && (487) \\
 &= \mathbf{H}^{\otimes n} |0\rangle_n \otimes \mathbf{H} |1\rangle \\
 &= (\mathbf{H} |0\rangle \otimes \dots \otimes \mathbf{H} |0\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &= \left( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &= 2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle_n \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ by (423)}.
 \end{aligned}$$

## Proof (cont'd).

Second statement:

$$\begin{aligned}
 \psi_2 &= \mathbf{U}_f \psi_1 & (488) \\
 &= 2^{-n/2} \sum_{x=0}^{2^n-1} \mathbf{U}_f \left( |x\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
 &= 2^{-n/2} \sum_{x=0}^{2^n-1} \left( |x\rangle_n \otimes \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right) \\
 &= 2^{-n/2} \sum_{x=0}^{2^n-1} \left( |x\rangle_n \otimes \frac{(-1)^{f(x)} (|0\rangle - |1\rangle)}{\sqrt{2}} \right) \\
 &= 2^{-n/2} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot |x\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.
 \end{aligned}$$

## Proof (cont'd).

Third statement:

$$\begin{aligned}
 \psi_3 &= (\mathbf{H}^{\otimes n} \otimes \mathbf{I})\psi_2 && (489) \\
 &= 2^{-n/2} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot \mathbf{H}^{\otimes n} |x\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot \sum_{y=0}^{2^n-1} (-1)^{h(x,y)} |y\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \text{ by (427)} \\
 &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left( \sum_{x=0}^{2^n-1} (-1)^{f(x)+h(x,y)} \right) |y\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
 &= \left[ \frac{1}{2^n} \left( \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right) |0\rangle_n + \frac{1}{2^n} \sum_{y=1}^{2^n-1} \left( \sum_{x=0}^{2^n-1} (-1)^{f(x)+h(x,y)} \right) |y\rangle_n \right] \\
 &\quad \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.
 \end{aligned}$$

## Proof (cont'd).

If  $f$  is constant, then

$$a_0 = \frac{1}{2^n} \left( \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right) \quad (490)$$

has the value  $a_0 = \pm 1$ . But  $\psi_3$  has norm 1 and so

$$\psi_3 = \pm |0\rangle_n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (491)$$

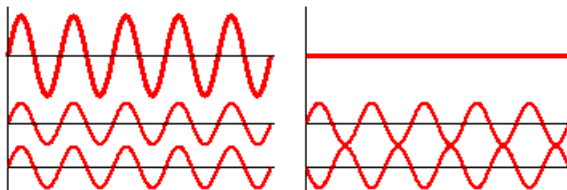
Partial measurement of the first  $n$  qubits gives  $|0\rangle_n$  with probability 1 (constructive interference).

If  $f$  is balanced, then  $a_0 = 0$ . Partial measurement of the first  $n$  qubits does not result in  $|0\rangle_n$  with probability 1 (destructive interference). □

## Wave Inference

Inference means superposition of two waves to generate a wave of greater, lower, or the same amplitude.

- When in phase, constructive inference results in a wave of greater amplitude.
- When  $180^\circ$  out of phase, destructive inference results.



## Grover Algorithm (1996)

**Require:** Boolean function  $f : \mathbb{B}^n \rightarrow \mathbb{B}$ ,  $M = |f^{-1}(1)|$ , Hilbert space  $\mathcal{H}^{\otimes(n+1)}$ ,  $R = \left\lceil \frac{\pi}{4} \sqrt{2^n/M} \right\rceil$ .

**Ensure:** Measurement yields value  $x$  with  $f(x) = 1$  with high probability.

$$\psi_0 \leftarrow |0\rangle_n |1\rangle_1$$

$$\psi_1 \leftarrow \mathbf{H}^{\otimes(n+1)} \psi_0$$

**for**  $r$  from 1 to  $R$  **do**

$$\hat{\psi}_{r+1} \leftarrow \mathbf{U}_f \psi_r$$

$$\psi_{r+1} \leftarrow ((\mathbf{H}^{\otimes n} (2|0\rangle_n \langle 0|_n - \mathbf{I}^{\otimes n}) \mathbf{H}^{\otimes n}) \otimes \mathbf{I}) \hat{\psi}_{r+1}$$

**end for**

$Y \leftarrow X_n^{\psi_{R+1}}$  {Partial measurement of first  $n$  qubits; correct with high probability.}

## Grover Algorithm

- *Satisfiability problem:* Given Boolean function  $f : \mathbb{B}^n \rightarrow \mathbb{B}$ . Find an argument  $y \in \mathbb{B}^n$  with  $f(y) = 1$ .
- The satisfiability problem is NP-hard; i.e., a conventional deterministic algorithm for finding  $y \in \mathbb{B}^n$  with  $f(y) = 1$  requires  $O(2^n)$  steps.
- The Grover algorithm produces an answer in  $O(\sqrt{2^n})$  steps and so has quadratic speedup.
- Thus Grover's method could brute-force a 128-bit symmetric cryptographic key in about  $2^{64}$  iterations.
- Hence, symmetric key lengths need to be doubled for protection against the Grover quantum attack.

## Proof.

First statement:

$$\begin{aligned}
 \psi_1 &= \mathbf{H}^{\otimes(n+1)}(|0\rangle_n |1\rangle) = \mathbf{H}^{\otimes n} |0\rangle_n \otimes \mathbf{H} |1\rangle & (492) \\
 &= (\mathbf{H} |0\rangle \otimes \dots \otimes \mathbf{H} |0\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &= \left( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
 &= 2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle_n \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ by (423)}.
 \end{aligned}$$

## Proof (cont'd).

Loop statement: Define the sequences  $(\alpha_{r,0})_{r \in \mathbb{N}}$  and  $(\alpha_{r,1})_{r \in \mathbb{N}}$ .

- Initialize

$$\alpha_{1,0} = 2^{-n/2} \quad \text{and} \quad \alpha_{1,1} = 2^{-n/2}. \quad (493)$$

- By induction,

$$\psi_r = \sum_{x=0}^{2^n-1} \alpha_{r,f(x)} |x\rangle_n \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad r \geq 1. \quad (494)$$

## Proof (cont'd).

Loop statement:

$$\begin{aligned}
 \hat{\psi}_{r+1} &= \mathbf{U}_f \psi_r && (495) \\
 &= \sum_{x=0}^{2^n-1} \alpha_{r,f(x)} \mathbf{U}_f \left( |x\rangle_n \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right) \\
 &= \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot \alpha_{r,f(x)} \cdot |x\rangle_n \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \text{ by (440)}.
 \end{aligned}$$

## Proof (cont'd).

The operator  $2|0\rangle_n \langle 0|_n - \mathbf{I}^{\otimes n}$  is a *Householder reflection*,

$$(2|0\rangle_n \langle 0|_n - \mathbf{I}^{\otimes n}) |x\rangle_n = \begin{cases} |0\rangle_n & \text{if } x = 0, \\ -|x\rangle_n & \text{if } x \neq 0. \end{cases} \quad (496)$$

It fixes  $|0\rangle_n$  and reflects all other base vectors.

Indeed,

$$2|0\rangle_n \langle 0|_n (|x\rangle_n) = \begin{cases} 2|0\rangle_n & \text{if } x = 0, \\ 0 & \text{if } x \neq 0, \end{cases}$$

and so

$$(2|0\rangle_n \langle 0|_n - \mathbf{I}^{\otimes n}) |x\rangle_n = 2|0\rangle_n \langle 0|_n |x\rangle_n - \mathbf{I}^{\otimes n} |x\rangle_n$$

has the required form.

## Proof (cont'd).

Grover's diffusion operator:

$$\begin{aligned}
 \hat{G} &= \mathbf{H}^{\otimes n} (2|0\rangle_n \langle 0|_n - \mathbf{I}^{\otimes n}) \mathbf{H}^{\otimes n} & (497) \\
 &= 2 (\mathbf{H}^{\otimes n} |0\rangle_n) (\langle 0|_n \mathbf{H}^{\otimes n}) - \mathbf{H}^{\otimes n} \mathbf{I}^{\otimes n} \mathbf{H}^{\otimes n} \\
 &= 2 \left( 2^{-n/2} \sum_{z=0}^{2^n-1} |z\rangle_n \right) \left( 2^{-n/2} \sum_{y=0}^{2^n-1} \langle y|_n \right) - \mathbf{I}^{\otimes n} \text{ by (423)} \\
 &= 2^{1-n} \sum_{z=0}^{2^n-1} \sum_{y=0}^{2^n-1} |z\rangle_n \langle y|_n - \mathbf{I}^{\otimes n}.
 \end{aligned}$$

Note that by function composition and (399),

$$\mathbf{H}^{\otimes n} \mathbf{I}^{\otimes n} \mathbf{H}^{\otimes n} = (\mathbf{H}\mathbf{I}\mathbf{H})^{\otimes n} = \mathbf{I}^{\otimes n}.$$

## Proof (cont'd).

Grover's diffusion operator:

$$\begin{aligned}
 \hat{G} \sum_{x=0}^{2^n-1} a_x |x\rangle_n &= \sum_{x=0}^{2^n-1} a_x \hat{G} |x\rangle_n, \quad a_x \in \mathbb{C}, & (498) \\
 &= \sum_{x=0}^{2^n-1} a_x \left( 2^{1-n} \sum_{z=0}^{2^n-1} \sum_{y=0}^{2^n-1} |z\rangle_n \langle y|_n |x\rangle_n - \mathbf{I}^{\otimes n} |x\rangle_n \right) \\
 &= \sum_{x=0}^{2^n-1} a_x \left( 2^{1-n} \sum_{z=0}^{2^n-1} |z\rangle_n - |x\rangle_n \right) \\
 &= \sum_{x=0}^{2^n-1} \left( 2^{1-n} \sum_{z=0}^{2^n-1} a_z - a_x \right) |x\rangle_n \\
 &= \sum_{x=0}^{2^n-1} \left( 2 \left( \frac{1}{2^n} \sum_{z=0}^{2^n-1} a_z \right) - a_x \right) |x\rangle_n.
 \end{aligned}$$

## Proof (cont'd).

Setting  $a_x = (-1)^{f(x)} \cdot \alpha_{r,f(x)}$  in (498) gives

$$\begin{aligned} \frac{1}{2^n} \sum_{z=0}^{2^n-1} a_z &= \frac{1}{2^n} \sum_{z=0}^{2^n-1} (-1)^{f(z)} \cdot \alpha_{r,f(z)} && (499) \\ &= \frac{1}{2^n} \cdot M \cdot (-1)^1 \cdot \alpha_{r,1} + \frac{1}{2^n} \cdot (2^n - M) \cdot (-1)^0 \cdot \alpha_{r,0} \\ &= -\frac{M}{2^n} \cdot \alpha_{r,1} + \left(1 - \frac{M}{2^n}\right) \cdot \alpha_{r,0}. \end{aligned}$$

## Proof (cont'd).

Using (495) and (498),

$$\begin{aligned}\psi_{r+1} &= (\hat{G} \otimes \mathbf{I}) \hat{\psi}_{r+1} & (500) \\ &= \sum_{x=0}^{2^n-1} \alpha_{r+1,f(x)} |x\rangle_n \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\end{aligned}$$

when the coefficients  $\alpha_{r+1,0}$  and  $\alpha_{r+1,1}$  are defined accordingly.

## Proof (cont'd).

Using the setting  $a_x = (-1)^{f(x)} \cdot \alpha_{r,f(x)}$ , a comparison of coefficients in (498) and (500) gives

$$\begin{aligned}
 \alpha_{r+1,0} &= 2 \left( \frac{1}{2^n} \sum_{z=0}^{2^n-1} a_z \right) - (-1)^0 \cdot \alpha_{r,0} & (501) \\
 &= 2 \left( -\frac{M}{2^n} \cdot \alpha_{r,1} + \left( 1 - \frac{M}{2^n} \right) \cdot \alpha_{r,0} \right) - \alpha_{r,0} \\
 &= \left( 1 - \frac{M}{2^{n-1}} \right) \cdot \alpha_{r,0} - \frac{M}{2^{n-1}} \cdot \alpha_{r,1} \\
 &= \alpha_{r,0} - \frac{M}{2^{n-1}} (\alpha_{r,0} + \alpha_{r,1}).
 \end{aligned}$$

## Proof (cont'd).

Similarly,

$$\begin{aligned}\alpha_{r+1,1} &= 2 \left( \frac{1}{2^n} \sum_{z=0}^{2^n-1} a_z \right) - (-1)^1 \cdot \alpha_{r,1} & (502) \\ &= 2 \left( -\frac{M}{2^n} \cdot \alpha_{r,1} + \left( 1 - \frac{M}{2^n} \right) \cdot \alpha_{r,0} \right) + \alpha_{r,1} \\ &= \left( 2 - \frac{M}{2^{n-1}} \right) \cdot \alpha_{r,0} + \left( 1 - \frac{M}{2^{n-1}} \right) \cdot \alpha_{r,1} \\ &= 2\alpha_{r,0} + \alpha_{r,1} - \frac{M}{2^{n-1}} (\alpha_{r,0} + \alpha_{r,1}).\end{aligned}$$

## Proof (cont'd).

The sequences  $(\alpha_{r,0})_r$  and  $(\alpha_{r,1})_r$  are real-valued.  
By the normalization of  $\psi_r$  in (494),

$$(2^n - M)\alpha_{r,0}^2 + M\alpha_{r,1}^2 = 1, \quad r \in \mathbb{N}_0. \quad (503)$$

Explicit representations of  $(\alpha_{r,0})_r$  and  $(\alpha_{r,1})_r$  are derived next.

## Proof (cont'd).

Use the Ansatz

$$\alpha_{1,0} = \frac{1}{\sqrt{2^n - M}} \cos \frac{\beta}{2} \quad \text{and} \quad \alpha_{1,1} = \frac{1}{\sqrt{M}} \sin \frac{\beta}{2}. \quad (504)$$

Then by (493),

$$\frac{1}{\sqrt{2^n - M}} \cos \frac{\beta}{2} = \frac{1}{\sqrt{2^n}} \quad (505)$$

and so

$$\cos \frac{\beta}{2} = \sqrt{\frac{2^n - M}{2^n}} \quad \text{and} \quad \sin \frac{\beta}{2} = \sqrt{\frac{M}{2^n}}. \quad (506)$$

Thus

$$\beta = 2 \arcsin \sqrt{\frac{M}{2^n}}. \quad (507)$$

## Proof (cont'd).

For each  $r \geq 1$ , put

$$\alpha_{r,0} = \frac{1}{\sqrt{2^n - M}} \cos \varphi_r \quad \text{and} \quad \alpha_{r,1} = \frac{1}{\sqrt{M}} \sin \varphi_r. \quad (508)$$

Then

$$\begin{aligned} \cos \varphi_{r+1} &= \sqrt{2^n - M} \cdot \alpha_{r+1,0} & (509) \\ &= \sqrt{2^n - M} \cdot \left( \left( 1 - \frac{M}{2^{n-1}} \right) \cdot \alpha_{r,0} - \frac{M}{2^{n-1}} \cdot \alpha_{r,1} \right) \\ &= \left( 1 - \frac{M}{2^{n-1}} \right) \cos \varphi_r - \sqrt{2^n - M} \cdot \frac{\sqrt{M}}{2^{n-1}} \sin \varphi_r \\ &= \left( 1 - 2 \frac{M}{2^n} \right) \cos \varphi_r - 2 \sqrt{\frac{2^n - M}{2^n}} \cdot \sqrt{\frac{M}{2^n}} \sin \varphi_r \\ &= \left( 1 - 2 \sin^2 \frac{\beta}{2} \right) \cos \varphi_r - 2 \cos \frac{\beta}{2} \cdot \sin \frac{\beta}{2} \cdot \sin \varphi_r \\ &= \cos \beta \cdot \cos \varphi_r - \sin \beta \cdot \sin \varphi_r = \cos(\varphi_r + \beta). \end{aligned}$$

## Proof (cont'd).

Put

$$\varphi_r = \frac{2r-1}{2}\beta, \quad r \geq 1. \quad (510)$$

Then

$$\varphi_1 = \frac{\beta}{2} \quad (511)$$

and

$$\varphi_{r+1} = \frac{2(r+1)-1}{2}\beta = \frac{2r-1}{2}\beta + \beta = \varphi_r + \beta. \quad (512)$$

This yields the explicit representation of the sequences of coefficients  $(\alpha_{r,0})_r$  and  $(\alpha_{r,1})_r$  in (508), where

$$\beta = 2 \arcsin \sqrt{\frac{M}{2^n}}. \quad (513)$$

## Proof (cont'd).

The probability that the measurement yields an argument  $y$  with  $f(y) = 1$  is given by

$$\begin{aligned}\mathbb{P}(f(Y) = 1) &= M\alpha_{R+1,1}^2 \text{ by (494),} & (514) \\ &= \sin^2 \varphi_{R+1} \text{ by (508),} \\ &= \left( \sin \left( \frac{2R+1}{2} \beta \right) \right)^2 \text{ by (510), .}\end{aligned}$$

The optimal number of iterations  $R$  is given by

$$\frac{2R+1}{2} \beta \approx \frac{\pi}{2}. \quad (515)$$

## Proof (cont'd).

Thus

$$\frac{2R+1}{2} \approx \frac{\pi}{2} \cdot \frac{1}{\frac{\beta}{2}} \quad (516)$$

and so

$$R \approx \frac{\pi}{4} \cdot \frac{1}{\frac{\beta}{2}} - \frac{1}{2} \quad (517)$$

Hence,

$$R \approx \frac{\pi}{4} \cdot \frac{1}{\arcsin \sqrt{\frac{M}{2^n}}} - \frac{1}{2}. \quad (518)$$

## Proof (cont'd).

Using the power series expansion

$$\arcsin(z) = z + \left(\frac{1}{2}\right) \frac{z^3}{3} + \left(\frac{1 \cdot 3}{2 \cdot 4}\right) \frac{z^5}{5} + \dots, \quad (519)$$

we obtain

$$R \approx \frac{\pi}{4} \cdot \frac{1}{\arcsin \sqrt{\frac{M}{2^n}}} - \frac{1}{2} \leq \frac{\pi}{4} \sqrt{\frac{2^n}{M}}. \quad (520)$$



## Example – Maple

For  $n = 30$  the input size is

$$2^{30} = 1,073,741,824.$$

If there is only one solution, i.e.,  $M = 1$ , the number of iterations is

$$R \approx 25736.$$

The measurement yields an argument  $y$  with  $f(y) = 1$  which has probability (514),

$$0.9999999990.$$

## Shor Algorithm

- Quantum algorithm for integer factorization (Peter Shor, 1994).
- Factoring of integer  $n$  in polynomial time depending on input size  $\log_2 n$ .
- Could break public-key cryptographic schemes like RSA (factoring large integers is intractable on classical computers).
- Research on new cryptosystems secure from quantum computers (post-quantum cryptography).

## Shor Algorithm (1994)

**Require:** Integer  $n = p \cdot q$ , distinct odd primes  $p$  and  $q$ , small number  $0 < \epsilon < 1$ .

**Ensure:** Factorization of  $n$  with success probability  $\geq 1 - \frac{1}{2^K}$  if the loop is repeated  $K$  times.

$L \leftarrow \lceil \log_2(n+1) \rceil$

**while** (true) **do**

    Choose  $a \in \{2, \dots, n-1\}$  uniformly at random

**if**  $(a, n) > 1$  **then**

**return**  $d \leftarrow (a, n)$  {Factor found}

**end if**

$r \leftarrow$  order of  $a \pmod n$  {Quantum part}

**if**  $r$  is even and  $a^{r/2} + 1 \not\equiv 0 \pmod n$  **then**

$p \leftarrow (a^{r/2} - 1, n)$

$q \leftarrow (a^{r/2} + 1, n)$

**return**  $p, q$  {Factors of  $n$ }

**end if**

**end while**

## Shor Algorithm

- The binary representation of  $n \in \mathbb{N}$  has

$$L = \lceil \log_2(n + 1) \rceil = \lfloor \log_2 n \rfloor + 1 \quad (521)$$

binary digits.

- Shor's algorithm has complexity  $O(KL^3)$  without the quantum part:
  - Euclidean algorithm has complexity  $O(L^3)$ .
  - Modular exponentiation has complexity  $O(M(L) \cdot L)$ , where  $M(L)$  is the complexity of multiplication of two numbers with  $L$  bits each, say schoolbook  $M(L) = O(L^2)$ , and  $L$  is the bitlength of the exponent.
  - Repetition  $K$  times.
- Quantum part has  $O(L^3)$  elementary quantum gates; counted as operations on a classical computer, the algorithm has polynomial runtime.

## Shor Algorithm

Given integers  $a, n$  with  $1 \leq a < n$  and  $(a, n) = 1$ . Let  $r$  be the order of  $a \bmod n$ .

If  $r$  is even and  $a^{r/2} + 1 \not\equiv 0 \pmod n$ , then

$$(a^{r/2} - 1, n) \quad \text{and} \quad (a^{r/2} + 1, n) \quad (522)$$

are two nontrivial factors of  $n$ .

## Proof.

Since  $r$  is the order of  $a \pmod n$ ,

$$(a^{r/2} - 1)(a^{r/2} + 1) = a^r - 1 \equiv 0 \pmod n.$$

Thus  $n$  divides  $a^r - 1$  and so  $n$  has a common factor with  $a^{r/2} - 1$  or  $a^{r/2} + 1$ .

Since  $a$  has order  $r$  modulo  $n$ ,  $a^{r/2} - 1 \not\equiv 0 \pmod n$ . Moreover, by hypothesis,  $a^{r/2} + 1 \not\equiv 0 \pmod n$ . Thus  $n$  has a common factor with both,  $a^{r/2} + 1$  and  $a^{r/2} - 1$ . These factors are given by the gcd's. □

## Example

Let  $n = 15$ .

- $a = 2$  has order  $r = 4 \pmod{15}$ , since  $2^4 \equiv 1 \pmod{15}$ .  
Moreover,  $2^2 + 1 = 5 \not\equiv 0 \pmod{15}$ . Thus two factors of 15 are
$$(2^2 + 1, 15) = 5 \quad \text{and} \quad (2^2 - 1, 15) = 3.$$
- $a = 11$  has order  $r = 2 \pmod{15}$ , since  $11^2 \equiv 1 \pmod{15}$ .  
Moreover,  $11^1 + 1 = 12 \not\equiv 0 \pmod{15}$ . Thus two factors of 15 are
$$(11 + 1, 15) = 3 \quad \text{and} \quad (11 - 1, 15) = 5.$$

## Shor Algorithm

Let  $n = p \cdot q$  with distinct odd primes  $p$  and  $q$ .

Choose integer  $a$  with  $1 \leq a \leq n - 1$  and  $(a, n) = 1$  uniformly at random. Let  $r$  be the order of  $a \bmod n$ . Then

$$\mathbb{P}(\{r \text{ even with } a^{r/2} + 1 \not\equiv 0 \pmod{n}\}) \geq \frac{1}{2}. \quad (523)$$

Repeating this experiment  $K$  times (while-loop) gives success probability

$$\geq 1 - \frac{1}{2^K}. \quad (524)$$

(M.A. Nielsen, I.L. Chuang: *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge, 2000.)

## Shor Algorithm – Quantum Part

**Require:** Integer  $1 \leq a \leq n - 1$ , small  $\epsilon > 0$ ,  $L = \lceil \log_2 n \rceil + 1$ , Hilbert space  $\mathcal{H}^{\otimes(m+L)}$ .

**Ensure:** Measurement  $0 \leq y \leq 2^m - 1$  yields order  $r$  of  $a \pmod n$  if possible.

$$m \leftarrow 2L + 1 + \lceil \log_2(1 + 1/(2\epsilon)) \rceil$$

$$\psi_0 \leftarrow |0\rangle_m |1\rangle_L$$

$$\psi_1 \leftarrow (\mathbf{H}^{\otimes m} \otimes \mathbf{I}^{\otimes L}) \psi_0$$

$$\psi_2 \leftarrow \mathbf{E}_a \psi_1$$

$$\psi_3 \leftarrow (\mathbf{F}^{\otimes m} \otimes \mathbf{I}^{\otimes L}) \psi_2$$

$$Y \leftarrow X_m^{\psi_3} \text{ \{Partial measurement of first } m \text{ qubits: } Y = y\}$$

$$\text{Write } \frac{y}{2^m} = [a_0, \dots, a_K] \text{ \{Continued fraction\}}$$

**for**  $k$  from 0 to  $K$  **do**

$$\text{Write } \frac{s}{r} = [a_0, \dots, a_k] \text{ \{Convergent of } \frac{y}{2^m} \}}$$

**if**  $r$  is the order of  $a$  **then**

**return**  $r$

**end if**

**end for**

Loop with next value of  $a$  \{Non-quantum part\}

## Exponential Gate

Let  $m, n, a, L$  be positive integers,  $1 < n < 2^L$  and  $1 \leq a < n$ .

The  $\mathbf{E}_a$ -gate or *exponential gate* is the linear operator  $\mathbf{E}_a : \mathcal{H}^{\otimes(m+L)} \rightarrow \mathcal{H}^{\otimes(m+L)}$  defined by

$$\mathbf{E}_a |x\rangle_m |y\rangle_L = \begin{cases} |x\rangle_m |a^x y \bmod n\rangle_L & \text{if } 0 \leq y \leq n-1, \\ |x\rangle_m |y\rangle_L & \text{if } n \leq y \leq 2^L-1. \end{cases} \quad (525)$$

## Exponential Gate

The  $\mathbf{E}_a$ -gate is a unitary operator.

### Proof.

If  $y < n$  and  $a \bmod n$  has order  $r$ , then

$$\begin{aligned} \mathbf{E}_a^r |x\rangle_m |y\rangle_L &= |x\rangle_m |a^{rx} y \bmod n\rangle_L \\ &= |x\rangle_m |y \bmod n\rangle_L \\ &= |x\rangle_m |y\rangle_L. \end{aligned}$$

If  $y \geq n$ ,

$$\mathbf{E}_a |x\rangle_m |y\rangle_L = |x\rangle_m |y\rangle_L.$$

Hence,

$$\mathbf{E}_a^{-1} = \mathbf{E}_a^{r-1}. \quad (526)$$



## Shor Algorithm – Quantum Part

First statement:

$$\begin{aligned}
 \psi_1 &= (\mathbf{H}^{\otimes m} \otimes \mathbf{I}^{\otimes L}) (|0\rangle_m |1\rangle_L) & (527) \\
 &= \mathbf{H}^{\otimes m} |0\rangle_m \otimes \mathbf{I}^{\otimes L} |1\rangle_L \\
 &= (\mathbf{H} |0\rangle \otimes \dots \otimes \mathbf{H} |0\rangle) \otimes |1\rangle_L \\
 &= \left( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) \otimes |1\rangle_L \\
 &= 2^{-m/2} \sum_{x=0}^{2^m-1} |x\rangle_m |1\rangle_L .
 \end{aligned}$$

## Shor Algorithm – Quantum Part

Second statement:

$$\begin{aligned}
 \psi_2 &= \mathbf{E}_a \psi_1 && (528) \\
 &= 2^{-m/2} \sum_{x=0}^{2^m-1} \mathbf{E}_a (|x\rangle_m |1\rangle_L) \\
 &= 2^{-m/2} \sum_{x=0}^{2^m-1} |x\rangle_m |a^x \bmod n\rangle_L.
 \end{aligned}$$

## Shor Algorithm – Quantum Part

Third statement:

$$\begin{aligned}
 \psi_3 &= (\mathbf{F}^{\otimes m} \otimes \mathbf{I}^{\otimes L}) \psi_2 & (529) \\
 &= 2^{-m/2} \sum_{x=0}^{2^m-1} (\mathbf{F}^{\otimes m} |x\rangle_m) \otimes (\mathbf{I}^{\otimes L} |a^x \bmod n\rangle_L) \\
 &= 2^{-m/2} \sum_{x=0}^{2^m-1} \left( 2^{-m/2} \sum_{y=0}^{2^m-1} \exp\left(2\pi i \frac{xy}{2^m}\right) |y\rangle_m \right) |a^x \bmod n\rangle_L \\
 &= \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} \exp\left(2\pi i \frac{xy}{2^m}\right) |y\rangle_m |a^x \bmod n\rangle_L.
 \end{aligned}$$

## Shor Algorithm – Quantum Part

Since  $r$  is the order of  $a \pmod n$ , we have

$$|a^r \pmod n\rangle_L = |1\rangle_L. \quad (530)$$

For each  $x$  with  $0 \leq x < 2^m$  write

$$x = j \cdot r + k, \quad (531)$$

where  $0 \leq k \leq r - 1$  (residue) and  $0 \leq j \leq \lfloor \frac{2^m - 1 - k}{r} \rfloor$  (quotient).

Then

$$|a^x \pmod n\rangle_L = |a^k\rangle_L. \quad (532)$$

Put

$$b_k = \left\lfloor \frac{2^m - 1 - k}{r} \right\rfloor + 1. \quad (533)$$

## Shor Algorithm – Quantum Part

Then

$$\begin{aligned}
 \psi_3 & & (534) \\
 &= \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} \exp\left(2\pi i \frac{xy}{2^m}\right) |y\rangle_m |a^x \bmod n\rangle_L \\
 &= \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{k=0}^{r-1} \sum_{j=0}^{b_k-1} \exp\left(2\pi i \frac{(j \cdot r + k)y}{2^m}\right) |y\rangle_m |a^k \bmod n\rangle_L \\
 &= \sum_{y=0}^{2^m-1} |y\rangle_m \\
 &\quad \otimes \left( \sum_{k=0}^{r-1} \frac{\exp\left(2\pi i \frac{ky}{2^m}\right)}{2^m} \left( \sum_{j=0}^{b_k-1} \exp\left(2\pi i \frac{jry}{2^m}\right) \right) |a^k \bmod n\rangle_L \right).
 \end{aligned}$$

## Shor Algorithm – Quantum Part

Partial measurement of the first  $m$  qubits (468):

$$\begin{aligned}
 \mathbb{P}(Y = y) &= p_y && (535) \\
 &= \sum_{k=0}^{r-1} \left| \frac{\exp\left(2\pi i \frac{ky}{2^m}\right)}{2^m} \left( \sum_{j=0}^{b_k-1} \exp\left(2\pi i \frac{jry}{2^m}\right) \right) \right|^2 \\
 &= \frac{1}{2^{2m}} \sum_{k=0}^{r-1} \left| \sum_{j=0}^{b_k-1} \left( \exp\left(2\pi i \frac{ry}{2^m}\right) \right)^j \right|^2,
 \end{aligned}$$

since each root of unity has norm 1.

## Measurement Approximation

- Given  $Y = y$ . Find good approximation of  $\frac{y}{2^m}$  via fraction  $\frac{s}{r}$  with  $0 \leq s \leq r$ .

- Good measurement set

$$E = \tag{536}$$

$$\left\{ y \mid 0 \leq y < 2^m, \left| \frac{y}{2^m} - \frac{s}{r} \right| \leq \frac{1}{2r^2} \text{ for some } 0 \leq s \leq r \right\}.$$

- If  $y \notin E$ , then

$$\left| \frac{y}{2^m} - \frac{s}{r} \right| > \frac{1}{2r^2} \text{ for all } 0 \leq s \leq r \tag{537}$$

$$\iff \left| \frac{ry}{2^m} - s \right| > \frac{1}{2r} \text{ for all } 0 \leq s \leq r$$

$$\iff \frac{ry}{2^m} = s + \Delta y \text{ for some } 0 \leq s \leq r \text{ and } \frac{1}{2r} < |\Delta y| \leq \frac{1}{2}.$$

## Measurement Approximation

Probability of  $y \notin E$ :

$$\begin{aligned}
 p_y &= \frac{1}{2^{2m}} \sum_{k=0}^{r-1} \left| \left( \sum_{j=0}^{b_k-1} \exp\left(2\pi i \frac{ry}{2^m}\right) \right)^j \right|^2 & (538) \\
 &= \frac{1}{2^{2m}} \sum_{k=0}^{r-1} \left| \sum_{j=0}^{b_k-1} (\exp(2\pi i(s + \Delta y)))^j \right|^2 \\
 &= \frac{1}{2^{2m}} \sum_{k=0}^{r-1} \left| \sum_{j=0}^{b_k-1} (\exp(2\pi i\Delta y))^j \right|^2 \\
 &= \frac{1}{2^{2m}} \sum_{k=0}^{r-1} \left| \frac{1 - \exp(2\pi i b_k \Delta y)}{1 - \exp(2\pi i \Delta y)} \right|^2
 \end{aligned}$$

by using the geometric series (445).

## Measurement Approximation

- We have

$$\begin{aligned}
 |1 - \exp(i\varphi)|^2 &= |1 - \cos(\varphi) - i \sin(\varphi)|^2 & (539) \\
 &= (1 - \cos(\varphi))^2 + \sin^2(\varphi) \\
 &= 2 - 2 \cos(\varphi) = 4 \sin^2 \frac{\varphi}{2}.
 \end{aligned}$$

- For  $-\pi \leq \varphi \leq \pi$ ,

$$|1 - \exp(i\varphi)|^2 = 4 \sin^2 \frac{\varphi}{2} \geq 4 \left(\frac{\varphi}{\pi}\right)^2 = \frac{4}{\pi^2} \varphi^2. \quad (540)$$

- Since  $|2\pi\Delta y| \leq \pi$ ,

$$p_y \leq \frac{1}{2^{2m}} \sum_{k=0}^{r-1} \frac{4}{\frac{4}{\pi^2} (2\pi\Delta y)^2} = \frac{1}{2^{2m}} \frac{r}{4(\Delta y)^2}. \quad (541)$$

## Measurement Approximation

Put

$$A = \frac{2^m}{2r^2}. \quad (542)$$

Then for some  $0 \leq s \leq r$ ,

$$\begin{aligned} p_y &\leq \frac{1}{2^{2m}} \frac{r}{4(\Delta y)^2} & (543) \\ &= \frac{1}{2^{2m}} \frac{r}{4\left(\frac{ry}{2^m} - s\right)^2} \\ &= \frac{1}{4r^4 A^2} \cdot \frac{r}{4\left(\frac{y}{2rA} - s\right)^2} \\ &= \frac{1}{4r(y - 2srA)^2}. \end{aligned}$$

## Measurement Approximation

If  $y \notin E$ , there exists  $0 \leq s \leq r$  such that

$$\begin{aligned} \frac{1}{2r} < |\Delta y| \leq \frac{1}{2} &\iff \frac{1}{2r} < \left| \frac{ry}{2^m} - s \right| \leq \frac{1}{2} & (544) \\ &\iff \frac{2^m}{2r^2} < \left| y - s \frac{2^m}{r} \right| \leq \frac{2^m}{2r} \\ &\iff A < |y - 2rsA| \leq rA. \end{aligned}$$

Thus

$$2srA + A < y \leq 2srA + rA \quad (545)$$

or

$$2srA - rA \leq y < 2srA - A. \quad (546)$$

## Measurement Approximation

$$\mathbb{P}(Y \notin E) \leq \frac{1}{2(A-1)}. \quad (547)$$

Proof.

$$\begin{aligned} \mathbb{P}(Y \notin E) &\leq \frac{1}{4r} \left[ \sum_{A < y \leq rA} \frac{1}{y^2} \quad (s=0) \right. \\ &\quad + \sum_{s=1}^{r-1} \sum_{A < |y - 2srA| \leq rA} \frac{1}{(y - 2srA)^2} \\ &\quad \left. + \sum_{2^{m-r}A \leq y < 2^m - A} \frac{1}{(y - 2^m)^2} \right] \quad (s=r, 2^m = 2r^2A) \\ &\leq \frac{1}{4r} \left[ \int_{A-1}^{rA} \frac{1}{y^2} dy + \sum_{s=1}^{r-1} 2 \int_{A-1}^{rA} \frac{1}{y^2} dy + \int_{A-1}^{rA} \frac{1}{y^2} dy \right] \\ &\leq \frac{1}{4r} 2r \int_{A-1}^{rA} \frac{1}{y^2} dy = \frac{1}{2} \left[ -\frac{1}{y} \right]_{A-1}^{rA} \\ &= \frac{1}{2} \left( \frac{1}{A-1} - \frac{1}{rA} \right) \leq \frac{1}{2(A-1)}. \end{aligned}$$

## Measurement Approximation

Given small, ugly number  $\epsilon$  with  $0 < \epsilon < 1$  and

$$\mathbb{P}(Y \notin E) \leq \frac{1}{2(A-1)} \stackrel{!}{\leq} \epsilon. \quad (548)$$

Then

$$\frac{1}{2(A-1)} \leq \epsilon \iff A \geq 1 + \frac{1}{2\epsilon} \quad (549)$$

$$\iff \frac{2^m}{2r^2} \geq 1 + \frac{1}{2\epsilon}$$

$$\iff m - 1 - 2 \log_2 r \geq \log_2 \left( 1 + \frac{1}{2\epsilon} \right)$$

$$\iff m \geq 2 \log_2 r + 1 + \log_2 \left( 1 + \frac{1}{2\epsilon} \right).$$

## Measurement Approximation

Choose the integer  $m$  such that

$$m \geq 2L + 1 + \left\lceil \log_2 \left( 1 + \frac{1}{2\epsilon} \right) \right\rceil, \quad (550)$$

where  $L = \lceil \log_2(n+1) \rceil = \lceil \log_2 n \rceil + 1$  and  $1 \leq r \leq n$ .

Then there is a good measurement result  $y \in E$  with probability  $\geq 1 - \epsilon$  such that for some  $0 \leq s \leq r$ ,

$$\left| \frac{y}{2^m} - \frac{s}{r} \right| \leq \frac{1}{2r^2}. \quad (551)$$

For instance, if  $\epsilon = 10^{-7}$ , then

$$m \geq 2L + 1 + \left\lceil \log_2 \left( 1 + \frac{1}{2 \cdot 10^{-7}} \right) \right\rceil = 2L + 24.$$

## Measurement Approximation

Take

$$m \geq 2L + 1 + \left\lceil \log_2 \left( 1 + \frac{1}{2 \cdot \epsilon} \right) \right\rceil,$$

where

$\epsilon$	$\left\lceil \log_2 \left( 1 + \frac{1}{2 \cdot \epsilon} \right) \right\rceil$
$10^{-1}$	3
$10^{-2}$	6
$10^{-3}$	9
$10^{-4}$	13
$10^{-5}$	16
$10^{-6}$	19
$10^{-7}$	23
$10^{-8}$	26
$10^{-9}$	29
$10^{-10}$	33

## Measurement Approximation

Let  $m, r \geq 1$  be integers with  $r^2 \leq 2^m$ , and let  $0 \leq y < 2^m$  and  $0 \leq s \leq r$ . If

$$\left| \frac{y}{2^m} - \frac{s}{r} \right| \leq \frac{1}{2r^2}, \quad (552)$$

then  $\frac{s}{r}$  is a convergent of the continuous fraction  $\frac{y}{2^m}$ .

(M.A. Nielsen, I.L. Chuang: *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge, 2000.)

## Measurement Approximation

Find the order  $r$  of  $a$  mod  $n$ .

- Compute the (finite) continued fraction

$$\frac{y}{2^m} = [a_0, \dots, a_K]. \quad (553)$$

- For each  $k$ ,  $0 \leq k \leq K$ , take the convergent

$$\frac{s_k}{r_k} = [a_0, \dots, a_k]. \quad (554)$$

and check if  $r_k$  is the order of  $a$  mod  $n$ .

- If this algorithm fails for the measured  $y$ , choose another integer  $a$ .

## Example

Let  $n = 33$ .

- We have

$$L = \lceil \log_2(n + 1) \rceil = 6.$$

- Let  $\epsilon = 10^{-1}$ . Then

$$m = 2L + 1 + \left\lceil \log_2\left(1 + \frac{1}{2\epsilon}\right) \right\rceil = 16.$$

- With probability  $\geq 1 - \epsilon = 90\%$  we obtain  $Y = y$  with

$$\left| \frac{y}{2^m} - \frac{s}{r} \right| \leq \frac{1}{2r^2}.$$

- Here  $r = 10$  (yet unknown),  $2^m = 2^{16} = 65536$  and

$$\left| \frac{y}{65536} - \frac{s}{10} \right| \leq \frac{1}{200} = 0.005.$$

## Example (cont'd)

Suppose  $y = 19412$ .

- The Euclidean algorithm yields

$$19412 = 0 \cdot 65536 + 19412,$$

$$65536 = 3 \cdot 19412 + 7300,$$

$$19412 = 2 \cdot 7300 + 4812,$$

$$7300 = 1 \cdot 4812 + 2488,$$

$$4812 = 1 \cdot 2488 + 2324,$$

$$2488 = 1 \cdot 2324 + 164,$$

$$2324 = 14 \cdot 164 + 28,$$

$$164 = 5 \cdot 28 + 24,$$

$$28 = 1 \cdot 24 + 4,$$

$$24 = 6 \cdot 4 + 0.$$

- This gives the continuous fraction

$$\frac{19412}{65536} = [0, 3, 2, 1, 1, 1, 14, 5, 1, 6].$$

## Example (cont'd)

- Consider successively the convergents:

$$[0, 3] = \frac{1}{3},$$

$$[0, 3, 2] = \frac{1}{3 + \frac{1}{2}} = \frac{2}{7},$$

$$[0, 3, 2, 1] = \frac{1}{3 + \frac{1}{2 + \frac{1}{1}}} = \frac{3}{10} \left( = \frac{s}{r} \right).$$

The last fraction provides the order  $r = 10$  of  $a = 5 \bmod 33$ ; i.e.,

$$5^{10} \equiv 1 \pmod{33}.$$

- Since the order  $r = 10$  is even and  $5^5 + 1 = 3126 = 24 \not\equiv 0 \pmod{33}$ , nontrivial factors of 33 are

$$(5^5 + 1, 33) = 3 \quad \text{and} \quad (5^5 - 1, 33) = 11.$$

# Part X

## Basic Number Theory (Appendix)

## Contents

Unique  
FactorizationEuclidean  
AlgorithmContinued  
FractionsLagrange's  
TheoremChinese  
Remainder

Totient Function

Fast  
Exponentiation

Prime Numbers

Quadratic  
ReciprocityComplex  
Numbers

## Basic Number Theory

It would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics.

A. Adrian Albert, 1941

## Basic Number Theory

- Unique factorization
- Euclidean algorithm
- Continued fractions
- Lagrange's theorem
- Chinese remainder theorem
- Euler's totient function
- Fast modular exponentiation
- Prime numbers
- Quadratic reciprocity
- Complex numbers

## Unique Factorization Theorem

Any non-zero integer can be factored into a product of primes in a unique way, up to the order of the primes.

### Example

```
> ifactor(123456789000);
```

$$2^2 \cdot 3^2 \cdot 5^3 \cdot 3803 \cdot 3607$$

## Euclidean Algorithm

Let  $a$  and  $b$  be integers with  $a > b > 0$ . Successive division with remainder,

$$\begin{aligned} a &= q_1 b + r_1, & 0 < r_1 < b, \\ b &= q_2 r_1 + r_2, & 0 < r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= q_{n+1} r_n + r_{n+1}, & r_{n+1} = 0, \end{aligned}$$

computes the gcd  $(a, b) = r_n$ .

## Euclidean Algorithm – Complexity

Let  $(F_n)$  denote the sequence of Fibonacci numbers with  $F_0 = 0$ ,  $F_1 = 1$  and  $F_n = F_{n-1} + F_{n-2}$  for  $n \geq 2$ . The Euclidean algorithm takes  $n$  divisions for consecutive Fibonacci numbers  $F_{n+2}$  and  $F_{n+1}$ :

$$\begin{aligned} F_{n+2} &= 1 \cdot F_{n+1} + F_n, \\ F_{n+1} &= 1 \cdot F_n + F_{n-1}, \\ &\vdots \\ F_4 &= 1 \cdot F_3 + F_2, \\ F_3 &= 1 \cdot F_2 + 0. \end{aligned}$$

## Euclidean Algorithm – Complexity

- Suppose  $F_{n+2} > b \geq F_{n+1}$  for some  $n \geq 0$ .
- We have  $F_{n+1} > \varphi^{n-1}$ , where  $\varphi = \frac{1+\sqrt{5}}{2}$  is the golden ratio. Thus  $\log_{10} b > (n-1) \log_{10} \varphi$ .
- Since  $\log_{10} \varphi = 0.48121 > 2/5$ ,  $(n-1) < 5/2 \log_{10} b$ .
- Thus  $n \leq 5/2 \log_{10} b + 1$  and hence the number of divisions is  $O(h)$ , where  $h$  is the number of decimal digits in  $b$ .

## Extended Euclidean Algorithm

Let  $a$  and  $b$  be integers with  $a > b > 0$ . There are integers  $s$  and  $t$  such that

$$(a, b) = s \cdot a + t \cdot b.$$

### Example

```
> igcdex(25, 32, 's', 't');  
1  
> s, t;  
9, -7
```

## Extended Euclidean Algorithm

$$\begin{aligned}
 r_1 &= a - bq_0 &= as_1 + bt_1, \\
 r_2 &= b - r_1q_1 &= as_2 + bt_2, \\
 r_3 &= r_1 - r_2q_2 &= as_3 + bt_3, \\
 &\vdots \\
 r_n &= r_{n-2} - r_{n-1}q_{n-1} &= as_n + bt_n.
 \end{aligned}$$

The number of steps is  $O(h)$ , where  $h$  is the number of digits in  $b$ .

## Continued Fractions

## The Euclidean algorithm

$$67 = 2 \cdot 24 + 19,$$

$$24 = 1 \cdot 19 + 5,$$

$$19 = 3 \cdot 5 + 4,$$

$$5 = 1 \cdot 4 + 1,$$

leads to a system of fractional equations

$$\frac{67}{24} = 2 + \frac{19}{24},$$

$$\frac{24}{19} = 1 + \frac{5}{19},$$

$$\frac{19}{5} = 3 + \frac{4}{5},$$

$$\frac{5}{4} = 1 + \frac{1}{4}.$$

## Continued Fractions

This gives the *continued fraction*

$$\begin{aligned}
 \frac{67}{24} &= 2 + \frac{19}{24} = 2 + \frac{1}{\frac{24}{19}} \\
 &= 2 + \frac{1}{1 + \frac{5}{19}} = 2 + \frac{1}{1 + \frac{1}{\frac{19}{5}}} \\
 &= 2 + \frac{1}{1 + \frac{1}{3 + \frac{4}{5}}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{\frac{5}{4}}}} \\
 &= 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}} \\
 &= 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}}.
 \end{aligned}$$

*Partial quotients:* 2, 1, 3, 1, 4, *complete quotients:*  $\frac{67}{24}, \frac{24}{19}, \frac{19}{5}, \frac{5}{4}$ .

## Continued Fractions

- Each rational number  $\frac{b}{c} > 1$  can be represented as continued fraction

$$\frac{b}{c} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots \frac{1}{a_n}}},$$

where  $a_0, \dots, a_n \geq 1$  are integers and  $a_n > 1$ .

- Each rational number has exactly one representation as continued fraction. Indeed, write

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}} = a'_0 + \frac{1}{a'_1 + \frac{1}{a'_2 + \dots}}$$

Since  $a_0, a'_0$  are the integral parts,  $a_0 = a'_0$ . Cancelling  $a_0$  and inverting gives

$$a_1 + \frac{1}{a_2 + \dots} = a'_1 + \frac{1}{a'_2 + \dots}$$

Continuing this way implies uniqueness.

## Continued Fractions

*Euler's rule:*

*Consider the sequence  $(a_0, a_1, \dots, a_n)$ : First take the product of all the terms. Then take every product that can be obtained by omitting any pair of consecutive terms. Then take every product that can be obtained by omitting any two separate pairs of consecutive terms, and so on. The sum of all such products gives the value of  $[a_0, a_1, \dots, a_n]$ .*

Example:

- $[a_0] = a_0,$
- $[a_0, a_1] = a_0 a_1 + 1,$
- $[a_0, a_1, a_2] = a_0 a_1 a_2 + a_0 + a_2,$
- $[a_0, a_1, a_2, a_3] = a_0 a_1 a_2 a_3 + a_2 a_3 + a_0 a_3 + a_0 a_1 + 1..$

## Continued Fractions – Example

Case  $n = 1$ :

$$a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{[a_0, a_1]}{[a_1]}.$$

Case  $n = 2$ :

$$\begin{aligned} a_0 + \frac{1}{a_1 + \frac{1}{a_2}} &= a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} \\ &= \frac{[a_0, a_1, a_2]}{[a_1, a_2]}. \end{aligned}$$

Case  $n = 3$ :

$$\begin{aligned} a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} &= a_0 + \frac{a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3} \\ &= \frac{a_0 a_1 a_2 a_3 + a_0 a_1 + a_0 a_3 + a_2 a_3 + 1}{a_1 a_2 a_3 + a_1 + a_3} \\ &= \frac{[a_0, a_1, a_2, a_3]}{[a_1, a_2, a_3]}. \end{aligned}$$

## Continued Fractions

The general continued fraction has the value

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_n}}}} = \frac{[a_0, a_1, \dots, a_n]}{[a_1, a_2, \dots, a_n]}.$$

## Continued Fractions

Recurrence relation:

$$[a_0, a_1, \dots, a_n] = a_0[a_1, a_2, \dots, a_n] + [a_2, a_3, \dots, a_n].$$

Case  $n = 2$ :

$$\begin{aligned} [a_0, a_1, a_2] &= a_0[a_1, a_2] + [a_2] = a_0(a_1a_2 + 1) + a_2 \\ &= a_0a_1a_2 + a_0 + a_2. \end{aligned}$$

Case  $n = 3$ :

$$\begin{aligned} [a_0, a_1, a_2, a_3] &= a_0[a_1, a_2, a_3] + [a_2, a_3] \\ &= a_0(a_1a_2a_3 + a_1 + a_3) + (a_2a_3 + 1) \\ &= a_0a_1a_2a_3 + a_0a_1 + a_0a_3 + a_2a_3 + 1. \end{aligned}$$

## Continued Fractions – Example

Example:

$$\begin{aligned} [4, 2] &= 4 \cdot 2 + 1 = 9, \\ [1, 4, 2] &= 1 \cdot [4, 2] + [2] = 9 + 2 = 11, \\ [2, 1, 4, 2] &= 2 \cdot [1, 4, 2] + [4, 2] = 2 \cdot 11 + 9 = 31. \end{aligned}$$

Thus

$$2 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}} = \frac{[2, 1, 4, 2]}{[1, 4, 2]} = \frac{31}{11}.$$

## Continued Fractions

By Euler's rule, the value  $[a_0, a_1, \dots, a_n]$  is unchanged if the terms are written in reverse order,

$$[a_0, a_1, \dots, a_n] = [a_n, a_{n-1}, \dots, a_0].$$

Equivalent recurrence relation:

$$[a_n, a_{n-1}, \dots, a_0] = a_n [a_{n-1}, \dots, a_0] + [a_{n-2}, \dots, a_0]$$

or

$$[a_0, a_1, \dots, a_n] = a_n [a_0, a_1, \dots, a_{n-1}] + [a_0, a_1, \dots, a_{n-2}]$$

Example:  $[2, 4, 1, 2] = [2, 1, 4, 2] = 31$ .

## Continued Fractions

Given a continued fraction

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}$$

Stopping at an earlier term than  $a_n$  gives the *convergents* of the continued fraction,

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_m}}}} = \frac{[a_0, a_1, \dots, a_m]}{[a_1, a_2, \dots, a_m]}, \quad 0 \leq m \leq n.$$

That is,

$$a_0, a_0 + \frac{1}{a_1}, a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, \dots$$

## Continued Fractions – Example

The successive convergents of  $\frac{67}{24}$  are

2,

$$2 + \frac{1}{1} = \frac{[2,1]}{[1]} = 3,$$

$$2 + \frac{1}{1 + \frac{1}{3}} = \frac{[2,1,3]}{[1,3]} = \frac{11}{4} = 2.75,$$

$$2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1}}} = \frac{[2,1,3,1]}{[1,3,1]} = \frac{14}{5} = 2.80,$$

$$2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}} = \frac{[2,1,3,1,4]}{[1,3,1,4]} = \frac{67}{24} = 2.79.$$

These numbers are alternately less than and greater than  $\frac{67}{24}$ .

## Continued Fractions

- Recurrence relation:

$$[a_0, a_1, \dots, a_n] = a_n [a_0, a_1, \dots, a_{n-1}] + [a_0, a_1, \dots, a_{n-2}].$$

- Setting  $b_0 = a_0$ ,  $b_1 = a_0 a_1 + 1$ ,  $c_0 = 1$ ,  $c_1 = a_1$ , and

$$b_n = [a_0, a_1, \dots, a_n],$$

$$c_n = [a_1, a_2, \dots, a_n], \quad n \geq 2,$$

we obtain

$$b_n = a_n b_{n-1} + b_{n-2}$$

$$c_n = a_n c_{n-1} + c_{n-2}, \quad n \geq 2.$$

- Both sequences  $(b_n)$  and  $(c_n)$  are strictly increasing.

## Continued Fractions

For  $n \geq 1$ ,

$$b_n c_{n-1} - c_n b_{n-1} = (-1)^{n-1}.$$

Thus  $b_n$  and  $c_n$  are relatively prime.

**Proof.**

For  $n = 1$ ,

$$b_1 c_0 - c_1 b_0 = (a_0 a_1 + 1) - a_1 a_0 = 1.$$

For  $n \geq 2$ ,

$$\begin{aligned} & b_n c_{n-1} - c_n b_{n-1} \\ &= (a_n b_{n-1} + b_{n-2}) c_{n-1} - (a_n c_{n-1} + c_{n-2}) b_{n-1} \\ &= -(b_{n-1} c_{n-2} - c_{n-1} b_{n-2}). \end{aligned}$$

Thus consecutive expressions alternate, as required.  $\square$

## Continued Fractions

For  $n \geq 1$ , write

$$\frac{b_n}{c_n} - \frac{b_{n-1}}{c_{n-1}} = \frac{(-1)^{n-1}}{c_{n-1}c_n}.$$

- The difference on the left is positive if  $n$  is odd, and negative if  $n$  is even.
- Since  $(c_n)$  is strictly increasing, the difference decreases as  $n$  increases (by the right-hand side).
- Thus  $b_1/c_1 > b_0/c_0$ , and  $b_2/c_2 < b_1/c_1$  but  $a_2/b_2 > b_0/c_0$  and so on.
- Since  $b/c = b_n/c_n$  for some  $n$ , all even convergents are less than  $b/c$  and all odd convergents are greater than  $b/c$ .

## Lagrange's Theorem

For each finite group  $G$ , the order (number of elements) of each subgroup  $U$  of  $G$  divides the order of  $G$ ; i.e.,

$$|G| = [G : U] \cdot |U|,$$

where  $[G : U]$  is the index of  $U$  in  $G$ .

### Proof.

The left cosets  $gU = \{gu \mid u \in U\}$ ,  $g \in G$ , of  $U$  in  $G$  form a partition of  $G$  by using the equivalence relation

$$g \simeq h \quad :\iff \quad gh^{-1} \in U, \quad g, h \in G.$$

Moreover, for each  $g \in G$ , the mapping  $\phi : U \rightarrow gU : u \mapsto gu$  is a bijection between  $U$  and the left coset  $gU$ . Thus the left cosets of  $U$  in  $G$  have the same size as  $U$ .  $\square$

## Lagrange's Theorem

The *order* of an element  $g$  of a finite group  $G$  is the smallest integer  $n \geq 1$  for which  $g^n$  is the identity element.

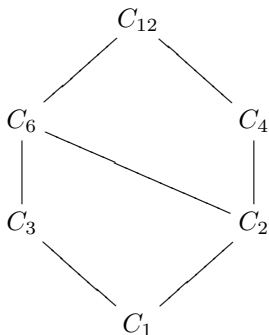
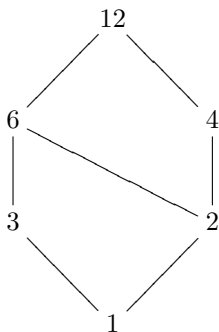
By Lagrange's theorem, the order of an element  $g$  in a finite group  $G$  divides the order of  $G$ .

## Cyclic Groups

A *cyclic group* is a group which is generated by a single element.

- Each finite cyclic group of order  $n$  is isomorphic to the additive group of  $\mathbb{Z}_n$ .
- Each infinite cyclic group is isomorphic to the additive group of  $\mathbb{Z}$ .
- Each subgroup and quotient group of a cyclic group is cyclic.
- The lattice of subgroups of  $\mathbb{Z}$  is isomorphic to the lattice of natural numbers ordered by divisibility.
- The lattice of subgroups of  $\mathbb{Z}_n$  is isomorphic to the lattice of natural numbers dividing  $n$  ordered by divisibility.

## Cyclic Groups

Lattice of subgroups of  $C_{12}$ :

## Chinese Remainder Theorem

Let  $n_1, \dots, n_k$  be pairwise relatively prime numbers  $\geq 2$  and let  $a_1, \dots, a_k$  be integers. There is a solution  $x$  of the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

If  $x$  and  $x'$  are two solutions, then  $x \equiv x' \pmod{N}$ , where  $N = n_1 \cdots n_k$ .

### Example

```
> chrem([1,2,1], [3,5,7]);
22
```

## Euler's Totient Function

For each integer  $n \geq 2$ , the set of units (or invertible elements) modulo  $n$  is given by

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}.$$

Define

$$\phi(n) = |\mathbb{Z}_n^*|.$$

### Example

We have  $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$  and so  $\phi(15) = 8$ .

## Euler's Totient Function

For primes  $p$  and  $q$ , and numbers  $n \geq 2$  and  $r$ ,

$$\phi(p) = p - 1,$$

$$\phi(p^r) = p^r - p^{r-1},$$

$$\phi(pq) = (p - 1)(q - 1),$$

$$\phi(n) = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

### Example

```
> with(numtheory):
> phi(123456789);
82260072
```

## Euler's Totient Function

Curves,  
Cryptosystems,  
and Quantum  
Computing

K.-H.  
Zimmermann

Contents

Unique  
Factorization

Euclidean  
Algorithm

Continued  
Fractions

Lagrange's  
Theorem

Chinese  
Remainder

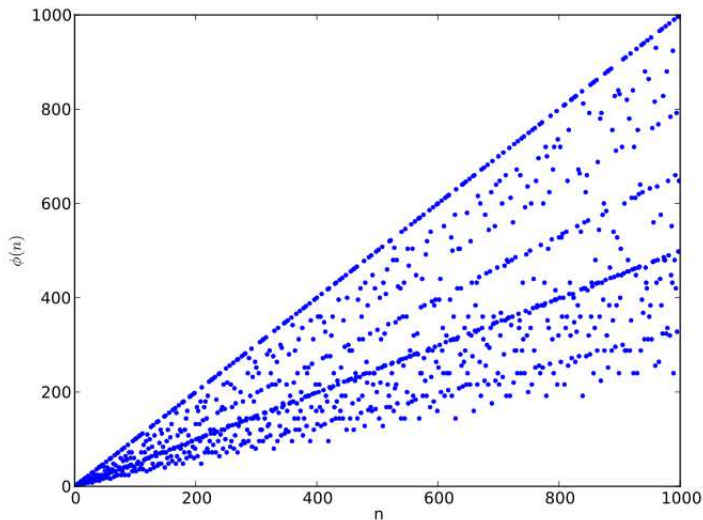
**Totient Function**

Fast  
Exponentiation

Prime Numbers

Quadratic  
Reciprocity

Complex  
Numbers



## Euler's Theorem

Let  $n \geq 2$  and  $a$  be integers. If  $(a, n) = 1$ , then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

This is a special case of Lagrange's theorem.

### Example

- We have  $\phi(15) = 8$ .
- Thus for each integer  $a$  with  $(a, n) = 1$ , we have  $a^{\phi(15)} = a^8 \equiv 1 \pmod{15}$ .
- The remaining non-zero elements are zero divisors.

## Fermat's Little Theorem

Let  $p$  be a prime and  $a$  be an integer. Then

$$a^p \equiv a \pmod{p}.$$

### Proof.

We have  $\phi(p) = p - 1$ . Since  $p$  is a prime, for each integer  $a$  with  $1 \leq a \leq p - 1$ , we have  $(a, p) = 1$ . Thus by Euler's theorem,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Hence,  $a^p \equiv a \pmod{p}$ . This congruence also holds for  $a = 0$ .  $\square$

## Fast Modular Exponentiation

**Require:** Modulus  $n \geq 2$  and positive integers  $x$  and  $e$

**Ensure:** Exponentiation  $x^e \bmod n$

$a \leftarrow e, b \leftarrow 1, c \leftarrow x$

**while**  $a > 0$  **do**

**if**  $a$  is even **then**

$a \leftarrow a/2, b \leftarrow b, c \leftarrow c^2 \bmod n$

**else**

$a \leftarrow a - 1, b \leftarrow bc \bmod n, c \leftarrow c$

**end if**

**end while**

**return**  $b$

Time complexity  $O(\log_2 e)$ .

## Fast Modular Exponentiation

Trace for the computation of  $x^{19} \bmod n$ :

$a$	$b$	$c$
19	1	$x$
18	$x$	$x$
9	$x$	$x^2$
8	$x \cdot x^2$	$x^2$
4	$x \cdot x^2$	$x^4$
2	$x \cdot x^2$	$x^8$
1	$x \cdot x^2$	$x^{16}$
0	$x \cdot x^2 \cdot x^{16}$	$x^{19}$

All operations are conducted modulo  $n$ . The computation makes use of the Horner scheme.

## Prime Number Theorem

Let  $\pi(x)$  be the number of primes in the range of 2 to  $x$ . Then  $\pi(x)$  is approximately  $x/\ln x$ , i.e.,

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

### Example

The number of 100-digit primes is about

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 9 \cdot 10^{97}.$$

The density of the 100-digit primes among the odd 100-digit numbers is about

$$\frac{9 \cdot 10^{97}}{\frac{1}{2}(10^{100} - 10^{99})} = 0.02.$$

## Sieve of Eratosthenes

Generate a list of all primes  $\leq 100$ :

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

## Quadratic Reciprocity

Let  $p > 2$  be a prime.

- A nonzero element  $x \in \mathbb{F}_p$  is a *square* or *quadratic residue* modulo  $p$  if  $x = y^2$  for some  $y \in \mathbb{F}_p$ . The remaining nonzero elements are the *nonsquares* or *nonresidues* modulo  $p$ .
- For  $p = 11$ , the squares modulo 11 are  $1^2 = 1$ ,  $2^2 = 4$ ,  $3^2 = 9$ ,  $4^2 = 5$ , and  $5^2 = 3$ . The nonsquares are 2, 6, 7, 8, and 10.
- If  $g$  is a generator of  $\mathbb{F}_p^*$ , the squares of  $g$  are exactly of the form  $g^j$  with  $j$  even. Thus  $\mathbb{F}_p^*$  has  $(p-1)/2$  squares  $g^{2j}$ ,  $1 \leq j \leq (p-1)/2$ , and  $(p-1)/2$  nonsquares  $g^{2j+1}$ ,  $1 \leq j \leq (p-1)/2$ .

## Legendre Symbol

Let  $p > 2$  be a prime and  $a$  be an integer.

The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

In Maple:

```
> with(numtheory):
> legendre(4, 11);
1
> legendre(6, 11);
-1
```

## Property of Legendre Symbol

Let  $p > 2$  be a prime and  $a$  be an integer.

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

### Proof.

- If  $p \mid a$ , both sides are 0 modulo  $p$ .
- Let  $p \nmid a$ .

By Little Fermat in  $\mathbb{F}_p$ , the square of  $a^{(p-1)/2}$  is 1. So  $a^{(p-1)/2} = \pm 1$ .

Let  $g$  be a generator of  $\mathbb{F}_p$  with  $a = g^j$ . Then  $a$  is a square iff  $j$  is even.

And  $a^{(p-1)/2} = g^{j(p-1)/2}$  is 1 iff  $j(p-1)/2$  is a multiple of  $p-1$  (since  $g$  generates  $\mathbb{F}_p^*$ ), i.e.,  $j$  is even.  $\square$

## Properties of Legendre Symbol

- $\left(\frac{a}{p}\right)$  depends only on the residue of  $a$  modulo  $p$ .
- $\left(\frac{1}{p}\right) = 1$  and  $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ .
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .
- If  $b$  is prime to  $p$ , then  $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ .

### Proof.

Part 1 is obvious.

Part 2 follows from the above property.

Part 3 follows from the above property and  
 $(ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2}$ .

Part 4 holds since  $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)$ . □

## Properties of Legendre Symbol

For each odd prime  $p$ ,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

### Proof (Sketch).

Let  $f(n) = (-1)^{(n^2-1)/8}$  for  $n$  odd, and  $f(n) = 0$  for  $n$  even.

- $p^2 \equiv 1 \pmod{8}$  for any odd prime  $p$ . So  $\mathbb{F}_{p^2}$  has a primitive 8-th root of unity  $\xi$ .
- Define the Gauss sum  $G = \sum_{j=0}^7 f(j)\xi^j$  in  $\mathbb{F}_{p^2}$ .
- We have  $G^p = \left(\frac{2}{p}\right)G$  and  $G^p = f(p)G$ .
- Division by  $G \neq 0$  gives the result. □

## Law of Quadratic Reciprocity

Let  $p$  and  $q$  be odd primes.

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod{4}, \\ \left(\frac{p}{q}\right) & \text{otherwise.} \end{cases}$$

## Proof (Sketch).

- Take a power  $t$  of  $p$  with  $p^t \equiv 1 \pmod{q}$  (such as  $t = q - 1$ ).
- Then the field  $\mathbb{F}_{p^t}$  has a primitive  $q$ -th root of unity  $\xi$ .
- Define the Gauss sum  $G = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^j$  in  $\mathbb{F}_{q^t}$ .
- Basic fact:  $G^2 = (-1)^{(q-1)/2} q$ .
- We have  $G^p = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right) G$  and  $G^p = \left(\frac{p}{q}\right) G$ .
- Division by  $G \neq 0$  gives the result. □

## Example

Determine whether 7411 is a square modulo 9283.

- 7411 and 9283 are both primes.
- Both numbers are  $\equiv 3 \pmod{4}$ .
- By quadratic reciprocity,

$$\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right).$$

- Taking the residue modulo 7411,

$$-\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right).$$

- Since  $1872 = 2^4 \cdot 3^2 \cdot 13$ ,

$$-\left(\frac{1872}{7411}\right) = -\left(\frac{2^4}{7411}\right) \left(\frac{3^2}{7411}\right) \left(\frac{13}{7411}\right) = -\left(\frac{13}{7411}\right).$$

## Example (cont'd)

- Since  $13 \equiv 1 \pmod{4}$ , by quadratic reciprocity

$$-\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right).$$

- Since  $7411 \equiv 1 \pmod{13}$ ,

$$-\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1.$$

Thus 7411 is a quadratic nonresidue modulo 9283.

## Jacobi Symbol

Let  $a$  be an integer and  $n > 0$  be an odd number with prime factorization  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ .

The *Jacobi symbol* is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

### Warning

If  $\left(\frac{a}{n}\right) = 1$  for  $n$  composite, it is not necessarily true that  $a$  is a square modulo  $n$ .

For instance,  $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = (-1)(-1) = 1$ , but there is no integer  $y$  with  $y^2 \equiv 2 \pmod{15}$ .

## Jacobi Symbol

Straightforward generalization of previous results to Jacobi symbol.

- For any positive odd number  $n$ ,

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

- For any two positive odd integers  $m$  and  $n$ ,

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right).$$

## Example

Determine whether 7411 is a square modulo 9283.

- Using the Jacobi symbol, factoring is not necessary (except pulling out powers of 2)!
- Since  $1872 = 16 \cdot 117$ ,

$$-\left(\frac{1872}{7411}\right) = -\left(\frac{2^4}{7411}\right) \left(\frac{117}{7411}\right) = -\left(\frac{117}{7411}\right).$$

- Since  $117 \equiv 1 \pmod{4}$ , by quadratic reciprocity

$$-\left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right).$$

- Since  $7411 \equiv 40 \pmod{117}$ ,

$$-\left(\frac{7411}{117}\right) = -\left(\frac{40}{117}\right).$$

## Example (cont'd)

- Since  $40 = 2^3 \cdot 5$ ,

$$-\left(\frac{40}{117}\right) = -\left(\frac{2^3}{117}\right) \left(\frac{5}{117}\right) = -\left(\frac{2}{117}\right) \left(\frac{5}{117}\right).$$

- Since  $117 \equiv -3 \pmod{8}$ ,

$$-\left(\frac{2}{117}\right) \left(\frac{5}{117}\right) = \left(\frac{5}{117}\right).$$

- Since  $5 \equiv 1 \pmod{4}$ ,

$$\left(\frac{5}{117}\right) = \left(\frac{117}{5}\right).$$

## Example (cont'd)

- Since  $117 \equiv 2 \pmod{5}$ ,

$$\left(\frac{117}{5}\right) = \left(\frac{2}{5}\right).$$

- But 2 is not a square in  $\mathbb{F}_5$  and so

$$\left(\frac{2}{5}\right) = -1.$$

## Complex Numbers

The *field of complex numbers* is given by the set

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

The terms  $a + bi$  are considered as formal sums, where  $i$  with  $i^2 = -1$  is the *imaginary unit*.

### ■ Addition

$$(a + bi) + (a' + b'i) = (a + a') + (b + b')i$$

### ■ Multiplikation

$$\begin{aligned} (a + bi) \cdot (a' + b'i) &= aa' + (ab' + a'b)i + bb'i^2 \\ &= (aa' - bb') + (ab' + a'b)i. \end{aligned}$$

## Complex Numbers

- Zero element  $0 = 0 + 0i$ , unit element  $1 = 1 + 0i$ .
- Additive inverse

$$-(a + bi) = (-a) + (-b)i.$$

- Multiplikative inverse

$$\begin{aligned} 1 &= (a + bi) \cdot (a' + b'i) = aa' + (ab' + a'b)i + bb'i^2 \\ &= (aa' - bb') + (ab' + a'b)i. \end{aligned}$$

Comparing coefficients

$$aa' - bb' = 1 \quad \text{and} \quad ab' + a'b = 0.$$

gives

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

## Complex Numbers

The field  $\mathbb{C}$  can also be defined as set of pairs

$$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\}$$

with addition

$$(a, b) + (a', b') = (a + a', b + b')$$

and multiplication

$$(a, b) \cdot (a', b') = (aa' - bb', ab' + a'b).$$

The zero element is  $0 = (0, 0)$ , the unit element is  $1 = (1, 0)$ , and the imaginary unit  $i$  is  $(0, 1)$ .

## Complex Numbers

$M = \{(a, 0) \mid a \in \mathbb{R}\}$  is a subfield of  $\mathbb{C}$  isomorphic to  $\mathbb{R}$ .

### Proof.

The mapping  $\phi : \mathbb{R} \rightarrow M : a \mapsto (a, 0)$  is bijective with

$$\phi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \phi(a) + \phi(b)$$

and

$$\phi(a \cdot b) = (a \cdot b, 0) = (a, 0) \cdot (b, 0) = \phi(a) \cdot \phi(b).$$



## Complex Numbers

> `Complex(2,3);`

$$2 + 3i$$

> `Complex(2,3) + Complex(-3,5);`

$$-1 + 8i$$

> `Complex(2,3) * Complex(-4,5);`

$$-23 - 2i$$

> `solve( z^2+z+1=0, z );`

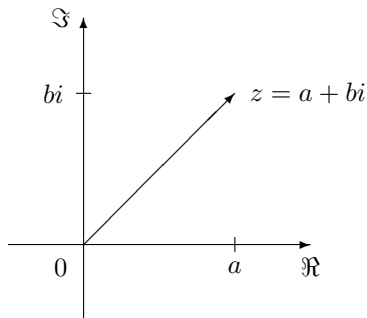
$$-\frac{1}{2} + \frac{1}{2}\sqrt{-3}, \quad -\frac{1}{2} - \frac{1}{2}\sqrt{-3}.$$

## Complex Numbers

The representation of  $z \in \mathbb{C}$  with  $z = a + bi$ ,  $a, b \in \mathbb{R}$ , is called *normal form* with

$$a = \Re z \quad \text{and} \quad b = \Im z,$$

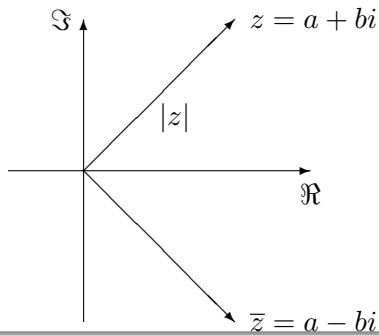
$\Re z$  *real part* and  $\Im z$  *imaginary part* of  $z$ .



## Complex Numbers

Let  $z = a + bi \in \mathbb{C}$ .

- $\bar{z} = a - bi$  is the *conjugate complex* of  $z$ .
- $|z| = \sqrt{a^2 + b^2}$  is the *absolute value* of  $z$ .



## Complex Numbers

### *Complex conjugation*

$$\mathbb{C} \rightarrow \mathbb{C} : z = a + bi \mapsto \bar{z} = a - bi$$

is an involutory automorphism

$$\overline{\bar{z}} = z, \quad \overline{\bar{y} + \bar{z}} = \overline{y + z} \quad \text{and} \quad \overline{y \cdot \bar{z}} = \overline{y \cdot z}, \quad y, z \in \mathbb{C}.$$

For all  $y, z \in \mathbb{C}$ :

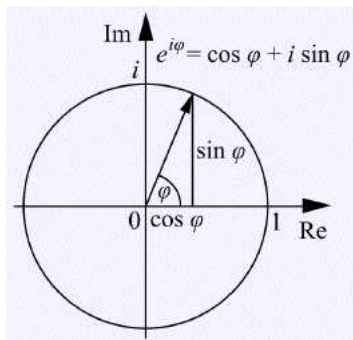
- $z = \bar{z} \iff z \in \mathbb{R},$
- $|z| = |\bar{z}|,$
- $z \cdot \bar{z} = |z|^2,$
- $|y \cdot z| = |y| \cdot |z|,$
- $|y + z| \leq |y| + |z|$  (triangular inequality).

## Complex Numbers

Each complex number  $z$  has the unique representation

$$z = r(\cos \phi + i \sin \phi)$$

with  $r = |z|$  and  $-\pi < \phi \leq \pi$ .



## Complex Numbers

The *polar representation* of  $z = a + ib$ ,  $a, b \in \mathbb{R}$ , is

$$z = r(\cos \phi + i \sin \phi)$$

with  $r = \sqrt{a^2 + b^2}$  and

- $a > 0, b > 0$ :  $\phi > 0$  and  $\tan \phi = \frac{b}{a}$ .
- $a < 0, b > 0$ :  $\phi > 0$  and  $\tan(180^\circ - \phi) = \frac{b}{|a|}$ .
- $a < 0, b < 0$ :  $\phi < 0$  and  $\tan(180^\circ + \phi) = \frac{b}{a}$ .
- $a < 0, b < 0$ :  $\phi < 0$  and  $\tan(-\phi) = \frac{|b|}{a}$ .

## Complex Numbers

```
> polar(4+2*I);
```

$$\text{polar}(2\sqrt{5}, \arctan(\frac{1}{2}))$$

```
> r := |4+2*I|;
```

```
> a := argument(4+2*I);
```

$$r := 2\sqrt{5}, \quad a := \arctan(\frac{1}{2})$$

```
> evalf(convert(arctan(1/2), degrees));
```

26.56505117 degrees

The polar form of  $4 + 2i$  is

$$4.47(\cos 26.56^\circ + i \sin 26.56^\circ).$$

## Complex Numbers

The *exponential function*  $\exp : \mathbb{C} \rightarrow \mathbb{C}$  is the power series

$$e^z := \exp(z) = \sum_{i=0}^{\infty} \frac{z^i}{i!} = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \dots$$

This sum converges for all  $z \in \mathbb{C}$  (radius  $\infty$ ).

- The *power function*  $\mathbb{C} \rightarrow \mathbb{C} : z \mapsto a^z$  to base  $a \in \mathbb{R}_{>0}$  is

$$a^z := \exp(z \cdot \log a).$$

- The *sine and cosine functions* are

$$\cos \phi := \Re e^{i\phi} \quad \text{and} \quad \sin \phi := \Im e^{i\phi}, \quad \phi \in \mathbb{R}.$$

## Complex Numbers

The sine and cosine functions fulfill

$$\sin \phi = \phi - \frac{\phi^3}{3!} + \frac{\phi^5}{5!} - \frac{\phi^7}{7!} \pm \dots$$

$$\cos \phi = 1 - \frac{\phi^2}{2!} + \frac{\phi^4}{4!} - \frac{\phi^6}{6!} \pm \dots$$

## Eulerian Formula

For each  $\phi \in \mathbb{R}$ ,

$$e^{i\phi} = \cos \phi + i \sin \phi.$$

## Complex Numbers

Each complex number  $z \in \mathbb{C}$  has the unique representation

$$z = r e^{i\phi}$$

with  $r = |z|$  and  $-\pi < \phi \leq \pi$ .

### Example

The complex number  $z = 4 + 2i$  has the polar form  $z = r(\cos \phi + i \sin \phi)$  with  $r = 2\sqrt{5}$  and  $\phi = \arctan(\frac{1}{2})$ , and thus the representation  $z = r e^{i\phi}$ .

## Complex Numbers

For each  $n \in \mathbb{Q}$  and  $\phi \in \mathbb{R}$ ,

$$(\cos \phi + i \sin \phi)^n = \cos n\phi + i \sin n\phi$$

### Proof.

By Euler's formula,

$$(e^{i\phi})^n = (\cos \phi + i \sin \phi)^n$$

and

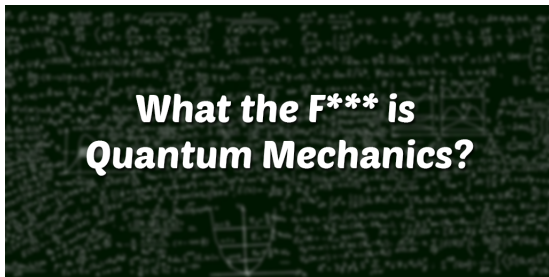
$$(e^{i\phi})^n = e^{i(n\phi)} = \cos n\phi + i \sin n\phi.$$



# Part XI

## Quantum Mechanics (Appendix)

## Quantum Mechanics



Contents

Wave Functions

Harmonic  
Oscillator

Hydrogen Atom

Heisenberg  
Uncertainty

Hydrogen Ion

Schrödinger  
Equation

## Quantum Mechanics – Contents

- Wave functions
- Harmonic oscillator
- Hydrogen atom
- Hydrogen ion
- Schrödinger equation

## Quantum Mechanics – Reading

- Leon van Dommelen: *Quantum Mechanics for Engineers*, Techn. Report, Tallahassee, FL, 2012.
- David J. Griffiths: *Introduction to Quantum Mechanics*, Prentice Hall, Upper Saddle River, NJ, 1995.
- C. Jansson: *Quantum Information Theory for Engineers*, Techn. Report, TUHH, 2017.

## Quantum Mechanics

- Fundamental theory describing nature at smallest scale (atoms and subatomic particles).
- Energy, momentum and other quantities of a system are restricted to discrete values (quantization), objects have dual characteristics (wave-particle duality), and there are limits to precision (uncertainty principle).
- In the modern theory, a mathematical function (wave function) provides information about the probability amplitude of position, momentum, and other physical properties of a particle.
- Classical physics describes nature at macroscopic scale and can be seen as an approximation valid at large scale.

## Newtonian Physics

Newton picture for a particle with mass  $m$ :

- velocity  $v_x = \frac{dx}{dt}$ ,
- linear momentum  $p_x = mv_x$ ,
- force (Newton's second law)  $F_x = m \frac{dv_x}{dt}$ .

Numerical position, numerical velocity or linear momentum for the particle do not exist!

## Quantum Physics

- What does exist is the so-called wave function  $\psi(x, y, z; t)$  depending on location  $r = (x, y, z)$  and time  $t$ .
- The wave function  $\psi(x, y, z; t)$  gives the quantum amplitude that the particle can be found at position  $r = (x, y, z)$ .
- Born's statistical interpretation:

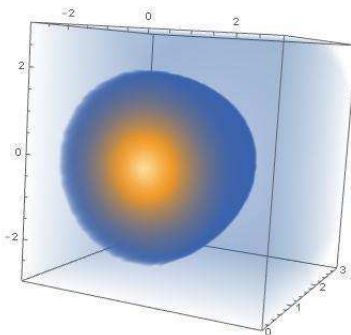
$$|\psi(r; t)|^2 d^3r \quad (555)$$

is the probability of finding the particle within a small volume of size  $d^3r = dx dy dz$  around the given location  $r = (x, y, z)$ ; the particle can be found in a so-called blob.

- Normalization: The total probability of finding the particle somewhere is

$$\int_r |\psi(r; t)|^2 d^3r = 1. \quad (556)$$

## Visualization of Wave Function



Lighter regions are regions where the particle is more likely to be found if the location is narrowed down.

## Heisenberg Uncertainty Principle

There is always a minimum combined uncertainty in position and linear momentum.

- A particle cannot have a mathematically precise position  $x$ , as this would require an infinite uncertainty in linear momentum  $p_x$ .
- A particle cannot have a mathematically precise linear momentum  $p_x$ , as this would imply an infinite uncertainty in position  $x$ .
- The area of the blob of a particle cannot be contracted to a point. The minimum area is comparable in size to the reduced Planck constant (Dirac constant),

$$\hbar = \frac{h}{2\pi} \approx 1.054 \cdot 10^{-34} \text{ J s.} \quad (557)$$

## Operators of Quantum Mechanics

The following operators are the key to quantum mechanics.

- The  $x$ -position operator  $\hat{x}$  maps wave function  $\psi$  to  $x\psi$ ,

$$\psi(x, y, z; t) \mapsto x\psi(x, y, z; t). \quad (558)$$

The operators  $\hat{y}$  and  $\hat{z}$  are similarly defined.

- The  $x$ -momentum operator  $\hat{p}_x$  maps wave function  $\psi$  to its  $x$ -derivative

$$\psi \mapsto \hat{p}_x \psi = \frac{\hbar}{i} \frac{\partial}{\partial x} \psi = \frac{\hbar}{i} \psi_x(x, y, z; t). \quad (559)$$

The operators  $\hat{p}_y$  and  $\hat{p}_z$  are similarly defined,

$$\hat{p}_y = \frac{\hbar}{i} \frac{\partial}{\partial y} \quad \text{and} \quad \hat{p}_z = \frac{\hbar}{i} \frac{\partial}{\partial z}. \quad (560)$$

The factor  $i$  makes them Hermitian operators.

## Operators of Quantum Mechanics

- The kinetic energy operator is

$$\hat{T} = -\frac{\hbar^2}{2m}\nabla^2 \quad (561)$$

with Laplacian operator

$$\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}. \quad (562)$$

- The total energy operator or Hamiltonian is the sum of the kinetic energy operator and the potential energy operator  $V = V(x, y, z; t)$ ,

$$H = -\frac{\hbar^2}{2m}\nabla^2 + V. \quad (563)$$

## Eigenfunctions and Eigenstates

Total energy or Hamiltonian of the system:

$$H = -\frac{\hbar^2}{2m}\nabla^2 + V. \quad (564)$$

The solutions of the time-independent Schrödinger equation

$$H\psi = E\psi \quad (565)$$

are the eigenfunctions  $\psi$  with associated eigenvalues  $E$  (for energy).

## Orthodox Statistical Interpretation

- The only measurable values (position, momentum, energy, ...) are the eigenvalues of the corresponding operator (position, momentum, total energy, ...).
- E.g., if the total energy of a particle is measured, the only numbers that can come out are the eigenvalues of the total energy Hamiltonian.
- Niels Bohr (1885-1962): According to the orthodox interpretation, measurement causes the wave function  $\psi$  to collapse into one of the eigenfunctions of the quantity being measured.

## Orthodox Statistical Interpretation

- The wave function of a system is a linear combination of eigenfunctions,

$$\psi = c_1\psi_1 + c_2\psi_2 + \dots \quad (566)$$

- Measurement causes the wave function to collapse into one of the eigenfunctions of the quantity being measured with the measured value being the corresponding eigenvalue; e.g., energy measurement:

$$\left. \begin{array}{l} \psi = c_1\psi_1 + c_2\psi_2 + \dots \\ \text{energy is uncertain} \end{array} \right\} \xrightarrow{\text{measurement}} \left\{ \begin{array}{l} \psi = c_n\psi_n \\ \text{energy certain } c_n. \end{array} \right. \quad (567)$$

- By measurement, the wave function  $\psi$  will collapse to eigenfunction  $\psi_n$  with probability  $|c_n|^2$ ; i.e., the square magnitudes of the coefficients of the eigenfunctions give the probabilities of the corresponding eigenvalues.

## Orthodox Interpretation

- If the wave function before the measurement is (in terms of eigenfunctions)

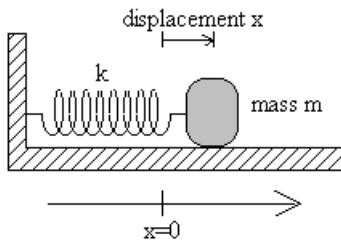
$$\psi = c_1\psi_1 + c_2\psi_2 + \dots, \quad (568)$$

it will collapse after measurement to eigenfunction  $\psi_n$  with probability  $|c_n|^2$ ; this requires the condition

$$\sum_n |c_n|^2 = 1. \quad (569)$$

- After real-life measurement follow-up measurements have statistics that are consistent with a collapsed wave function  $\psi = c_n\psi_n$  (with certainty).

## Harmonic Oscillator



## Harmonic Oscillator

- Application: particle constrained to remain at approximately the same position; e.g., atom in a solid or molecule.
- Harmonic oscillator: forces that push back the particle to its nominal position are proportional to the distance the particle is away from it; particle's displacement is given by  $(x, y, z)$ .
- The particle vibrates back and forth around its nominal position with frequency (adopted from classical physics)

$$\omega = \sqrt{\frac{c}{m}} \quad (570)$$

in radians per second, where  $c$  is the spring constant (measure of strength of the force).

## Harmonic Oscillator

- Total energy Hamiltonian of the system:

$$H = -\frac{\hbar}{2m} \left( \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} \right) + \frac{1}{2}c(x^2 + y^2 + z^2), \quad (571)$$

where  $r = \sqrt{x^2 + y^2 + z^2}$  is the particle distance from the nominal position.

- Each eigenfunction  $\psi$  and its eigenvalue  $E$  must satisfy the time-independent Schrödinger equation

$$H\psi = E\psi. \quad (572)$$

The boundary condition is that  $\psi$  becomes 0 at large distance from the nominal position.

## Harmonic Oscillator

By separation of variables, each eigenfunction is a product of 1D eigenfunctions,

$$\psi(x, y, z) = \psi_x(x)\psi_y(y)\psi_z(z). \quad (573)$$

This gives the 1D eigenvalue problems

$$\left( -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + \frac{1}{2}cx^2 \right) \psi_x = E_x \psi_x \quad (574)$$

$$\left( -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial y^2} + \frac{1}{2}cy^2 \right) \psi_y = E_y \psi_y \quad (575)$$

$$\left( -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial z^2} + \frac{1}{2}cz^2 \right) \psi_z = E_z \psi_z. \quad (576)$$

## Harmonic Oscillator

The 1D eigenvalue problem

$$\left( -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + \frac{1}{2} c x^2 \right) \psi_x = E_x \psi_x \quad (577)$$

has the solutions

$$\psi_{x,n_x}(x) = h_{n_x}(x), \quad (578)$$

$$E_{x,n_x} = \frac{2n_x + 1}{2} \hbar\omega, \quad n_x \in \mathbb{N}_0, \quad (579)$$

where the  $h_{n_x}(x)$  come from Hermite polynomials. Similarly,

$$E_{y,n_y} = \frac{2n_y + 1}{2} \hbar\omega, \quad n_y \in \mathbb{N}_0, \quad (580)$$

$$E_{z,n_z} = \frac{2n_z + 1}{2} \hbar\omega, \quad n_z \in \mathbb{N}_0. \quad (581)$$

## Harmonic Oscillator

### Eigenfunctions

$$h_n(\xi) = \frac{1}{(\pi\ell^2)^{1/4}} \frac{H_n(\xi)}{\sqrt{2^n n!}} e^{-\xi^2/2}, \quad (582)$$

where  $\omega = \sqrt{c/m}$ ,  $\ell = \sqrt{\hbar/(m\omega)}$ ,  $\xi = x/\ell$ , and  $H_n$  is the  $n$ th Hermite polynomial,

$$H_n(x) = (-1)^n \sum_{k_1+2k_2=n} \frac{n!}{k_1!k_2!} (-1)^{k_1+k_2} (2x)^{k_1}, \quad n \geq 0, \quad (583)$$

or given by the recurrence relation

$$H_{-1}(x) = 0, \quad (584)$$

$$H_0(x) = 1, \quad (585)$$

$$H_n(x) = 2xH_{n-1}(x) - 2(n-1)H_{n-2}(x). \quad (586)$$

## Harmonic Oscillator

- Total energy eigenvalues

$$E_{n_x n_y n_z} = \frac{2n_x + 2n_y + 2n_z + 3}{2} \hbar\omega, \quad n_x, n_y, n_z \in \mathbb{N}_0, \quad (587)$$

with quantum numbers  $n_x, n_y, n_z \geq 0$ .

- Corresponding eigenfunctions of the complete system

$$\psi_{n_x n_y n_z}(x, y, z) = h_{n_x}(x) h_{n_y}(y) h_{n_z}(z). \quad (588)$$

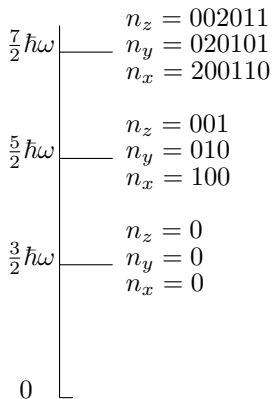
- Ground state energy

$$E_{000} = \frac{3}{2} \hbar\omega. \quad (589)$$

So even at absolute zero temperature, the particle is not completely at rest in its nominal position (by the Heisenberg uncertainty principle).

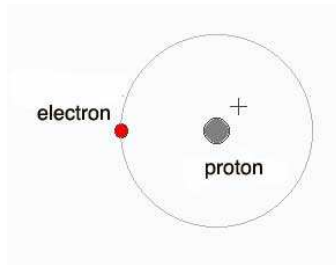
## Harmonic Oscillator

Lower part of energy spectrum:



The energy values are discrete and evenly spaced with constant energy difference of  $\hbar\omega$  between successive levels.

## Hydrogen Atom



## Hydrogen Atom

- A hydrogen atom consists of a nucleus with a single proton and an electron encircling the nucleus.
- The nucleus is much heavier than the electron; it is assumed to be stationary and only the motion of the electron is considered.
- The energy levels of the electron determine the photons that the atom will absorb or emit.

## Hydrogen Atom

Potential energy of the system:

$$V = -\frac{e^2}{4\pi\epsilon_0 r}, \quad (590)$$

where  $r$  is the distance between proton and electron,

$$e = 1.6 \cdot 10^{-19} \text{ C} \quad (591)$$

is the magnitude of electric charges of electron and proton, and

$$\epsilon_0 = 8.85 \cdot 10^{-12} \text{ C}^2/\text{Jm} \quad (592)$$

is the permittivity of space.

## Hydrogen Atom

Total energy Hamiltonian of the system:

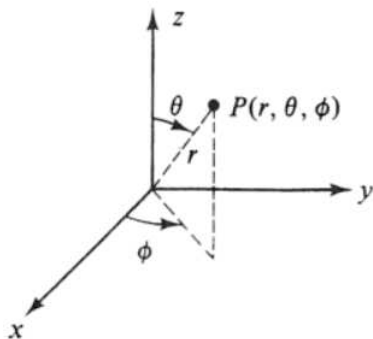
$$H = -\frac{\hbar^2}{2m_e} \nabla^2 + V, \quad (593)$$

where

$$m_e = 9.109 \cdot 10^{-31} \text{ kg} \quad (594)$$

is the mass of the electron.

## Spherical Coordinates



$$r = \sqrt{x^2 + y^2 + z^2}, \quad (595)$$

$$\theta = \arccos \frac{z}{r}, \quad (596)$$

$$\phi = \arctan \frac{y}{x}. \quad (597)$$

## Hydrogen Atom

Total energy Hamiltonian in spherical coordinates:

$$H = -\frac{\hbar^2}{2m_e r^2} \left[ \frac{\partial}{\partial r} \left( r^2 \frac{\partial}{\partial r} \right) + \frac{1}{\sin \theta} \frac{\partial}{\partial \theta} \left( \sin \theta \frac{\partial}{\partial \theta} \right) + \frac{1}{\sin^2 \theta} \frac{\partial^2}{\partial \phi^2} \right] - \frac{e^2}{4\pi\epsilon_0} \frac{1}{r}. \quad (598)$$

By separation of variables, the wave function has the form

$$\psi(r, \theta, \phi) = R(r)\Theta(\theta)\Phi(\phi) \quad (599)$$

and so the eigenvalue problem is

$$H(R\Theta\Phi) = E(R\Theta\Phi). \quad (600)$$

## Hydrogen Atom

- The eigenfunctions  $\psi_{nlm}$  are numbered as

$$n > l \geq |m| \geq 0 \quad (601)$$

with principal quantum number  $n \geq 1$ , azimuthal quantum number  $l$ , and magnetic quantum number  $m$ .

- Eigenfunctions

$$\psi_{nlm}(r, \theta, \phi) = R_{nl}(r)Y_l^m(\theta, \phi), \quad (602)$$

where the  $R_{nl}$  are radial wave functions and the  $Y_m^l$  are the spherical harmonics,

$$Y_l^m(\theta, \phi) = (-1)^m \sqrt{\frac{2l+1}{4\pi} \frac{(l-|m|)!}{(l+|m|)!}} P_l^m(\cos \theta) e^{im\phi}, \quad (603)$$

where  $P_l^m$  is the associated Legendre function of the first kind.

## Hydrogen Atom

### ■ Eigenfunctions

$$\begin{aligned} \psi_{nlm}(r, \theta, \phi) & \qquad \qquad \qquad (604) \\ &= -\frac{2}{n^2} \sqrt{\frac{(n-l-1)!}{[(n+l)!a_0]^3}} \left(\frac{2\rho}{n}\right)^l L_{n+l}^{(2l+1)} e^{-\rho/n} Y_l^m(\theta, \phi), \end{aligned}$$

where  $L_{n+l}^{(2l+1)}$  is the  $2l + 1$ -th derivative of the associated Laguerre polynomial  $L_{n+l}$ ,  $\rho = r/a_0$  is the scaled radial distance from the nucleus, and  $a_0$  is the Bohr radius

$$a_0 = \frac{4\pi\epsilon_0\hbar^2}{m_e e^2} \approx 0.53 \cdot 10^{-10} \text{ m} \approx 0.5 \text{ \AA}. \qquad (605)$$

## Hydrogen Atom

- Energy eigenvalues

$$E_n = -\frac{\hbar^2}{2m_e a_0^2} \frac{1}{n^2} = \frac{E_1}{n^2}, \quad n \geq 1, \quad (606)$$

with

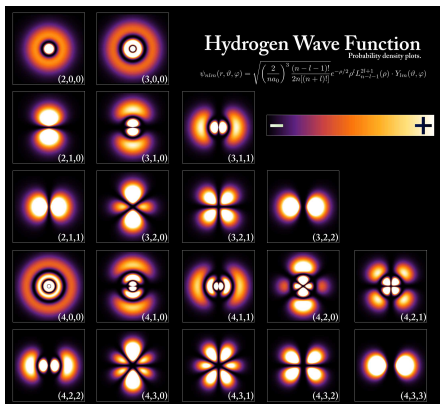
$$E_1 = -\frac{\hbar^2}{2m_e a_0^2} = -13.6 \text{ eV}, \quad (607)$$

where eV stands for electron volt ( $1 \text{ eV} = 1.6 \cdot 10^{-19} \text{ J}$ ).

- The ground state of lowest energy  $E_1$  is given by eigenfunction

$$\psi_{100}(r) = \frac{1}{\sqrt{\pi a_0^3}} e^{-r/a_0}. \quad (608)$$

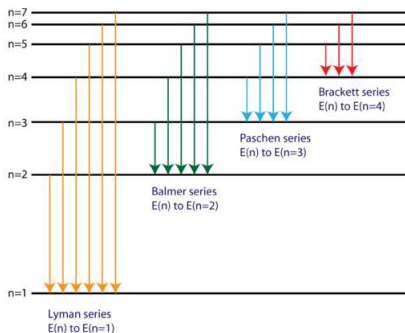
## Hydrogen Atom



Wave functions of the electron in a hydrogen atom at different energy levels. The brighter areas represent a higher probability of finding the electron.

## Hydrogen Atom

Electron transitions for the Hydrogen atom



The energy lost by the electron during transition is emitted as a photon: UV light (Lyman), visible light (Balmer), infrared light (Paschen); the ionization energy is 13.6 eV.

## Heisenberg Uncertainty

The position operator  $\hat{x}$  and the linear momentum operator  $\hat{p}_x$  do not commute, since

$$\begin{aligned}\hat{p}_x \hat{x} \psi &= \frac{\hbar}{i} \frac{\partial}{\partial x} (x\psi) = \frac{\hbar}{i} \psi + \frac{\hbar}{i} x \frac{\partial \psi}{\partial x} \\ &= -i\hbar \psi + \hat{x} \hat{p}_x \psi.\end{aligned}\quad (609)$$

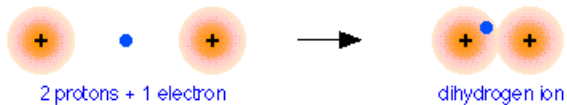
Thus their commutator is

$$[\hat{x}, \hat{p}_x] = \hat{x} \hat{p}_x - \hat{p}_x \hat{x} = i\hbar. \quad (610)$$

A nonzero commutator demands a minimum amount of uncertainty in the quantities  $x$  and  $p_x$  given by their standard deviations  $\sigma_x$  and  $\sigma_{p_x}$ ,

$$\sigma_x \sigma_{p_x} \geq \frac{1}{2} \hbar. \quad (611)$$

This is the precise uncertainty relationship first formulated by Werner Heisenberg (1901-1976).

Hydrogen Molecular Ion  $H_2^+$ 

## Hydrogen Molecular Ion

- Total energy Hamiltonian of the  $\text{H}_2^+$ -ion:

$$H = -\frac{\hbar^2}{2m_e} \nabla^2 - \frac{e^2}{r\pi\epsilon_0} \left[ \frac{1}{r_L} + \frac{1}{r_R} \right], \quad (612)$$

where  $r_L$  and  $r_R$  are the distances between the electron and the left and right protons, resp., i.e.,

$$r_L = |r - r_{Lp}| \quad \text{and} \quad r_R = |r - r_{Rp}|, \quad (613)$$

where  $r_{Lp}$  and  $r_{Rp}$  are the positions of the left and right protons, resp.

- Born-Oppenheimer approximation: the nuclei of the protons are at fixed positions.
- Model of 2-qubit system.

## Hydrogen Molecular Ion – Energy when fully dissociated

When the protons are far apart, there are two lowest energy states  $\psi_L$  and  $\psi_R$ , in which the electron is in the ground state around the left and right proton, resp. In either case, there is an hydrogen atom and a free proton.

The wave functions are

$$\psi_L(r) = \psi_{100}(|r - r_{Lp}|) \quad \text{and} \quad \psi_R(r) = \psi_{100}(|r - r_{Rp}|), \quad (614)$$

where  $r$ ,  $r_{Lp}$ , and  $r_{Rp}$  are the positions of electron, left proton, and right proton, resp.

The wave function of the hydrogen atom in the ground state is given by (608),

$$\psi_{100}(r) = \frac{1}{\sqrt{\pi a_0^3}} e^{-r/a_0}. \quad (615)$$

## Hydrogen Molecular Ion – Energy when sharing the electron

The protons share the electron such that there is a probability of finding the electron around either proton.

- The wave function is the linear combination

$$\psi = a\psi_L + b\psi_R, \quad (616)$$

where the electron is shared by the protons in ways that depend on the chosen values of  $a$  and  $b$ .

- The functions  $\psi_L$  and  $\psi_R$  are not eigenfunctions of the system (see (628)).

# Schrödinger Equation

## The Schrödinger equation

$$\left[ -\frac{\hbar^2}{2m} \nabla^2 + V \right] \Psi = i\hbar \frac{\partial \Psi}{\partial t}$$

The operator  $\nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$  is the Laplacian in Cartesian coordinates.

$\Psi$  is the wavefunction.

$V$  is the potential.

$\hbar$  is the Planck constant divided by  $2\pi$ .

The particle mass is represented by  $m$ .

## Schrödinger Equation

- *Newton's 2nd law of motion* states that the linear momentum changes in time proportional to the applied force,

$$F = \frac{dp}{dt} = m \frac{dv}{dt} = ma. \quad (617)$$

- Schrödinger's equation is the equivalent in quantum mechanics and states that the time derivative of the wave function is obtained by applying the Hamiltonian on it,

$$i\hbar \frac{\partial \psi}{\partial t} = H\psi. \quad (618)$$

## Schrödinger Equation

Write the wave function  $\psi$  in terms of the energy eigenfunctions  $\psi_n$  of the Hamiltonian,

$$\psi = \sum_n c_n(t) \psi_n. \quad (619)$$

Then the coefficients  $c_n$  must evolve in time as complex exponentials,

$$c_n(t) = c_n(0) e^{-iE_n t / \hbar}, \quad n \geq 0, \quad (620)$$

with initial values  $c_n(0)$  given by the wave function.

Solution is not valid if the Hamiltonian depends explicitly on time, say by external influences on the system.

## Schrödinger Equation

The coefficients vary with time but their square magnitudes do not:

$$\begin{aligned} |c_n(t)|^2 &= \overline{c_n(t)}c_n(t) = \overline{c(0)}e^{iE_n t/\hbar}c_n(0)e^{-iE_n t/\hbar} \\ &= |c_n(0)|^2. \end{aligned} \quad (621)$$

So the probability of measuring a given energy level does not vary with time.

## Schrödinger Equation

Solution for harmonic oscillator:

$$\psi(x, y, z; t) = \sum_{n_x=0}^{\infty} \sum_{n_y=0}^{\infty} \sum_{n_z=0}^{\infty} c_n(0) e^{-iE_{n_x, n_y, n_z} t / \hbar} \psi_{n_x, n_y, n_z}(x, y, z), \quad (622)$$

where

$$E_{n_x, n_y, n_z} = \frac{2n_x + 2n_y + 2n_z}{2} \hbar \omega \quad (623)$$

and

$$\psi_{mln}(x, y, z) = h_{n_x}(x) h_{n_y}(y) h_{n_z}(z). \quad (624)$$

## Schrödinger Equation

Solution for hydrogen atom:

$$\psi(r, \theta, \phi; t) = \sum_{n=1}^{\infty} \sum_{l=0}^{n-1} \sum_{m=-l}^l c_{nlm}(0) e^{-iE_n t/\hbar} \psi_{nlm}(r, \theta, \phi), \quad (625)$$

where

$$E_n = -\frac{\hbar^2}{2m_e a_0^2 n^2} \quad (626)$$

and

$$\psi_{mln}(r, \theta, \phi) = R_{nl}(r) Y_l^m(\theta, \phi). \quad (627)$$

## Schrödinger Equation

Solution for hydrogen ion:

$$\psi = c_L e^{-iE_L t/\hbar} \frac{\psi_L + \psi_R}{\sqrt{2}} + c_H e^{-iE_H t/\hbar} \frac{\psi_L - \psi_R}{\sqrt{2}}, \quad (628)$$

where  $E_L$  is the ground state of lowest energy and  $E_H$  is the state of highest energy.

## Part XII

# Abstract Hilbert Spaces (Appendix)

## Contents

Inner Product  
Spaces

Normed Spaces

Convergence and  
Completeness

Hilbert Spaces

Tensor Spaces

Unitary Operators

## Hilbert Spaces

- Inner product spaces
- Normed spaces
- Convergence and completeness
- Hilbert spaces
- Tensor spaces
- Unitary operators

## Vector Spaces

A  $\mathbb{K}$ -vector space is a set  $V$  with vector addition

$$+ : V \times V \rightarrow V : (v, w) \mapsto v + w \quad (629)$$

and scalar multiplication

$$\cdot : \mathbb{K} \times V \rightarrow V : (\alpha, v) \mapsto \alpha \cdot v \quad (630)$$

such that  $(V, +)$  is an abelian group and for all  $\alpha, \beta \in \mathbb{K}$  and  $v, w \in V$ ,

$$(\alpha + \beta)v = \alpha v + \beta v, \quad (631)$$

$$\alpha(v + w) = \alpha v + \alpha w, \quad (632)$$

$$(\alpha\beta)v = \alpha(\beta v), \quad (633)$$

$$1 \cdot v = v. \quad (634)$$

## Inner Product Spaces

A  $\mathbb{K}$ -vector space  $V$  is an *inner product space* if it supports an *inner product*; i.e., a mapping

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{K}$$

such that for all  $u, v, w \in V$  and  $\alpha, \beta \in \mathbb{K}$ ,

$$\langle v, v \rangle \neq 0 \iff v \neq 0, \quad (635)$$

$$\langle v, w \rangle = \overline{\langle w, v \rangle}, \quad (636)$$

$$\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle, \quad (637)$$

where  $\mathbb{K} \rightarrow \mathbb{K} : z \mapsto \bar{z}$  is an involutory field automorphism.

## Inner Product Spaces – Example

If  $\mathbb{K} = \mathbb{R}$ , (636) becomes *symmetry*

$$\langle v, w \rangle = \langle w, v \rangle$$

and (636), (637) show that both mappings

$$v \mapsto \langle v, w \rangle \text{ and } w \mapsto \langle v, w \rangle$$

are  $\mathbb{R}$ -linear. Therefore, the mapping

$$(v, w) \mapsto \langle v, w \rangle$$

is  $\mathbb{R}$ -bilinear.

## Field of Complex Numbers

- The *complex conjugate* of a complex number  $z = x + iy$  is

$$\bar{z} = x - iy.$$

- The *length* of a complex number  $z = x + iy$  is

$$|z| = \sqrt{x^2 + y^2}$$

with  $|z|^2 = z\bar{z}$ .

- *Complex conjugation*

$$\mathbb{C} \rightarrow \mathbb{C} : z \mapsto \bar{z}$$

is an involutory field automorphism,

$$\overline{z + w} = \bar{z} + \bar{w}, \quad \overline{z \cdot w} = \bar{z} \cdot \bar{w}, \quad \bar{\bar{z}} = z, \quad |\bar{z}| = |z|,$$

and  $\bar{z} = z$  iff  $z \in \mathbb{R}$ .

## Inner Product Spaces – Example

If  $\mathbb{K} = \mathbb{C}$ , (636), (637) give

$$\begin{aligned}
 \langle \alpha u + \beta v, w \rangle &= \overline{\langle w, \alpha u + \beta v \rangle} & (638) \\
 &= \overline{\alpha \langle w, u \rangle + \beta \langle w, v \rangle} \\
 &= \overline{\alpha} \overline{\langle w, u \rangle} + \overline{\beta} \overline{\langle w, v \rangle} \\
 &= \overline{\alpha} \langle u, w \rangle + \overline{\beta} \langle v, w \rangle,
 \end{aligned}$$

i.e.,  $v \mapsto \langle v, w \rangle$  is *skew-linear*.

The inner product  $\langle \cdot, \cdot \rangle$  is a *sesquilinear form*.

We will restrict ourselves to  $\mathbb{K} = \mathbb{C}$ .

## Cauchy-Schwarz Inequality

Let  $V$  be an inner product space. Then for all  $u, v \in V$ ,

$$|\langle u, v \rangle|^2 \leq \langle u, u \rangle \langle v, v \rangle. \quad (639)$$

Equality holds iff  $v = \alpha u$  for some  $\alpha \in \mathbb{C}$ .

## Proof.

For  $\lambda \in \mathbb{C}$  and  $u, v \in V$ ,

$$0 \leq \langle u - \lambda v, u - \lambda v \rangle = \langle u, u \rangle - \lambda \langle u, v \rangle - \bar{\lambda} \langle v, u \rangle + |\lambda|^2 \langle v, v \rangle.$$

Let  $\langle v, u \rangle = \beta e^{i\theta}$ ,  $\beta \in \mathbb{R}$ , and  $\lambda = e^{-i\theta} t$ ,  $t \in \mathbb{R}$ . Then

$$\begin{aligned} 0 &\leq \langle u, u \rangle - e^{-i\theta} t \beta e^{i\theta} - e^{i\theta} t \beta e^{-i\theta} + t^2 \langle v, v \rangle \\ &= \langle u, u \rangle - 2\beta t + t^2 \langle v, v \rangle = \alpha - 2\beta t + \gamma t^2 = q(t), \end{aligned}$$

where  $\alpha = \langle u, u \rangle$  and  $\gamma = \langle v, v \rangle$  are real numbers. So  $q(t)$  is a real-valued quadratic polynomial with  $q(t) \geq 0$  for all  $t$ . Thus  $q(t) = 0$  has at most one real solution  $t$ ; i.e., the discriminant is non-positive:

$$D = 4\beta^2 - 4\alpha\gamma \leq 0.$$

Hence,  $0 \geq 4\beta^2 - 4\alpha\gamma = |\langle u, v \rangle|^2 - \langle u, u \rangle \langle v, v \rangle$  as claimed.  $\square$

## Normed Spaces

A  $\mathbb{K}$ -vector space  $V$  is a *normed space* if it supports a *norm*; i.e., a mapping

$$\|\cdot\| : V \rightarrow \mathbb{R}_{\geq 0},$$

such that for all  $v, w \in V$  and  $\alpha \in \mathbb{C}$ ,

$$\|v\| \neq 0 \iff v \neq 0, \quad (640)$$

$$\|\alpha v\| = |\alpha| \cdot \|v\|, \quad (641)$$

$$\|v + w\| \leq \|v\| + \|w\|. \quad (642)$$

## Normed Spaces

Each inner product space  $V$  is also a normed space with norm

$$\|v\| = \sqrt{\langle v, v \rangle}, \quad v \in V. \quad (643)$$

The Cauchy-Schwarz inequality (639) becomes

$$|\langle u, v \rangle| \leq \|u\| \|v\|, \quad u, v \in V. \quad (644)$$

## Normed Spaces – Proof

- The mapping  $\| \cdot \| : V \rightarrow \mathbb{R}_{\geq 0} : v \mapsto \|v\|$  is well-defined.
- (635) and (640) are equivalent.
- (641) follows from (636), (637):

$$\|\alpha v\|^2 = \langle \alpha v, \alpha v \rangle = \alpha \bar{\alpha} \langle v, v \rangle = |\alpha|^2 \cdot \|v\|^2.$$

- (642) follows from Cauchy-Schwarz (644),

$$\begin{aligned} \|v + w\|^2 &= \langle v + w, v + w \rangle \\ &= \langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle + \langle w, w \rangle \\ &= \|v\|^2 + 2\Re\langle v, w \rangle + \|w\|^2 \\ &\leq \|v\|^2 + 2|\langle v, w \rangle| + \|w\|^2 \\ &\leq \|v\|^2 + 2\|v\| \cdot \|w\| + \|w\|^2 \\ &= (\|v\| + \|w\|)^2. \end{aligned}$$



## Inner Product Spaces – Examples

- $\mathbb{R}^n$  ( $\mathbb{R}$ -vector space):

$$\langle u, v \rangle = \sum_{i=1}^n u_i v_i, \quad (645)$$

$$\|v\| = \left( \sum_{i=1}^n v_i^2 \right)^{1/2}. \quad (646)$$

- $\mathbb{C}^n$  ( $\mathbb{C}$ -vector space):

$$\langle u, v \rangle = \sum_{i=1}^n \bar{u}_i v_i, \quad (647)$$

$$\|v\| = \left( \sum_{i=1}^n |v_i|^2 \right)^{1/2}. \quad (648)$$

## Normed Spaces – Parallelogram Law

Let  $V$  be an inner product space. Then for all  $u, v \in V$ ,

$$\|u + v\|^2 + \|u - v\|^2 = 2\|u\|^2 + 2\|v\|^2. \quad (649)$$

**Proof.**

We have

$$\begin{aligned} \|u + v\|^2 &= \langle u + v, u + v \rangle \\ &= \langle u, u \rangle + \langle u, v \rangle + \langle v, u \rangle + \langle v, v \rangle \\ \|u - v\|^2 &= \langle u - v, u - v \rangle, \\ &= \langle u, u \rangle - \langle u, v \rangle - \langle v, u \rangle + \langle v, v \rangle. \end{aligned}$$

Adding these equations gives

$$\|u + v\|^2 + \|u - v\|^2 = 2\langle u, u \rangle + 2\langle v, v \rangle = 2\|u\|^2 + 2\|v\|^2.$$



## Normed Spaces

Most real and complex normed spaces do not have inner products.

- Consider the  $p$ -norm

$$\|v\|_p = \left( \sum_{i=1}^n |v_i|^p \right)^{\frac{1}{p}}.$$

- If a normed linear space  $V$  satisfies the parallelogram law, the norm arises from an inner product.
- This particularly holds for the  $p$ -norm iff  $p = 2$ , the so-called *Euclidean norm*.

## Convergence

Given a normed space  $(V, \|\cdot\|)$ .

- A sequence  $(v_n)_{n \in \mathbb{N}_0} \subseteq V$  *converges* to an element  $v \in V$  if  $(\|v - v_n\|)_{n \in \mathbb{N}_0}$  converges to 0 in  $\mathbb{R}$ ,

$$\lim_{n \rightarrow \infty} v_n = v \iff \lim_{n \rightarrow \infty} \|v - v_n\| = 0. \quad (650)$$

- A sequence  $(v_n)_{n \in \mathbb{N}_0} \subseteq V$  is *Cauchy* if

$$\lim_{k, n \rightarrow \infty} \|v_k - v_n\| = 0. \quad (651)$$

## Hilbert Space

A *Hilbert space* is a complete inner product space; i.e., an inner product space in which every Cauchy sequence converges.

## Examples

The spaces  $\mathbb{R}^n$  and  $\mathbb{C}^n$  are "typical" Hilbert spaces.

## Hilbert Space

Given a Hilbert space  $\mathcal{H}$ .

- Two vectors  $u, v \in \mathcal{H}$  are *orthogonal*, written  $u \perp v$ , if

$$\langle u, v \rangle = 0. \quad (652)$$

- The *orthogonal complement*  $U^\perp$  of a subset  $U \subseteq \mathcal{H}$  is

$$U^\perp = \{v \in \mathcal{H} \mid \langle u, v \rangle = 0 \forall u \in U\}. \quad (653)$$

## Hilbert Space

Let  $\mathcal{H}$  be a Hilbert space. The orthogonal complement  $U^\perp$  of  $U \subseteq \mathcal{H}$  is a closed linear subspace of  $\mathcal{H}$  and  $U \subseteq (U^\perp)^\perp$ .

### Proof.

- Let  $v, w \in U^\perp$ ,  $u \in U$ , and  $\alpha, \beta \in \mathbb{C}$ . Then

$$\langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle = 0$$

and so  $\alpha v + \beta w \in U^\perp$ ; i.e.,  $U^\perp$  is a subspace of  $\mathcal{H}$ .

- Let  $(v_n) \subseteq U^\perp$  with  $\lim_{n \rightarrow \infty} v_n = v$  and  $u \in U$ . Then

$$\begin{aligned} |\langle u, v \rangle| &= |\langle u, v \rangle - \langle u, v_n \rangle| = |\langle u, v - v_n \rangle| \\ &\leq \|u\| \cdot \|v - v_n\| \xrightarrow{n \rightarrow \infty} 0 \quad \text{by (644)} \end{aligned}$$

and so  $v \in U^\perp$ ; i.e.,  $U^\perp$  is closed. □

## Linear Functionals

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space. A *continuous linear functional* on  $\mathcal{H}$  is a mapping

$$\Lambda : \mathcal{H} \rightarrow \mathbb{C} : v \mapsto \Lambda(v), \quad (654)$$

which is  $\mathbb{C}$ -linear,

$$\Lambda(\alpha u + \beta v) = \alpha \Lambda(u) + \beta \Lambda(v), \quad u, v \in \mathcal{H}, \alpha, \beta \in \mathbb{C}, \quad (655)$$

and satisfies for some constant  $c = c(\Lambda) \in \mathbb{R}_{>0}$ ,

$$|\Lambda(u - v)| \leq c \cdot \|u - v\|, \quad u, v \in \mathcal{H}. \quad (656)$$

## Linear Functionals – Example

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space and  $u \in \mathcal{H}$ . The mapping

$$\Lambda_u : \mathcal{H} \rightarrow \mathbb{C} : v \mapsto \langle u, v \rangle \quad (657)$$

is  $\mathbb{C}$ -linear, since for all  $v, w \in \mathcal{H}$  and  $\alpha, \beta \in \mathbb{C}$ ,

$$\begin{aligned} \Lambda_u(\alpha v + \beta w) &= \langle u, \alpha v + \beta w \rangle = \alpha \langle u, v \rangle + \beta \langle u, w \rangle \\ &= \alpha \Lambda_u(v) + \beta \Lambda_u(w), \end{aligned}$$

and is continuous by Cauchy-Schwarz (644),

$$|\Lambda_u(v - w)| = \langle u, v - w \rangle \leq \|u\| \cdot \|v - w\|, \quad v, w \in \mathcal{H},$$

with  $c(\Lambda_u) = \|u\|$ .

## Riesz Representation

Each continuous linear functional  $\Lambda$  on a  $\mathbb{C}$ -Hilbert space has the form (657); i.e., there is a unique  $u \in \mathcal{H}$  such that  $\Lambda = \Lambda_u$  with

$$\Lambda_u : \mathcal{H} \rightarrow \mathbb{C} : v \mapsto \langle u, v \rangle. \quad (658)$$

### Proof.

- *Uniqueness:* Let  $u, u' \in \mathcal{H}$  with  $\langle u, v \rangle = \langle u', v \rangle$  for all  $v \in \mathcal{H}$ . Then  $\langle u - u', v \rangle = 0$ . In particular, taking  $v = u - u'$  gives

$$\|u - u'\|^2 = \langle u - u', u - u' \rangle = 0$$

and so  $u = u'$ .

## Proof (cont'd).

- *Existence:* Let  $K = \ker \Lambda$ . Since  $\Lambda$  is linear and continuous,  $K$  is a closed linear subspace of  $\mathcal{H}$ . If  $K = \mathcal{H}$ , take  $u = 0 \in \mathcal{H}$  and so  $\Lambda = 0$ .

Otherwise, take  $u \in K^\perp$  with  $\Lambda(u) = 1$ , and let  $v \in \mathcal{H}$  with  $\alpha = \Lambda(v)$ . Then  $\Lambda(v - \alpha u) = \Lambda(v) - \alpha\Lambda(u) = 0$  and so  $v - \Lambda(v)u \in K$ . Therefore,

$$0 \stackrel{\perp}{=} \langle u, v - \Lambda(v)u \rangle = \langle u, v \rangle - \Lambda(v)\|u\|^2.$$

So if  $u_0 = u/\|u\|^2$ , then

$$\Lambda(v) = \langle u, v \rangle / \|u\|^2 = \langle u_0, v \rangle.$$



## Bounded Linear Operators

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space.

- A linear functional  $\Lambda : \mathcal{H} \rightarrow \mathbb{C}$  is *bounded* if there is a constant  $c > 0$  such that

$$|\Lambda(v)| \leq c \cdot \|v\|, \quad v \in \mathcal{H}. \quad (659)$$

- For a bounded linear functional  $\Lambda$ , define the *norm* of  $\Lambda$  as

$$\|\Lambda\| = \sup\{|\Lambda(v)| \mid \|v\| \leq 1, v \in \mathcal{H}\} < \infty. \quad (660)$$

We have

$$\begin{aligned} \|\Lambda\| &= \sup\{|\Lambda(v)| \mid \|v\| \leq 1, v \in \mathcal{H}\} \\ &= \sup\{|\Lambda(v)|/\|v\| \mid 0 \neq v \in \mathcal{H}\} \\ &= \inf\{c > 0 \mid |\Lambda(v)| \leq c\|v\|, v \in \mathcal{H}\}. \end{aligned} \quad (661)$$

- A linear functional is bounded iff it is continuous.

## Bounded Linear Operators

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space and  $u \in \mathcal{H}$ . The mapping

$$\Lambda_u : \mathcal{H} \rightarrow \mathbb{C} : v \mapsto \langle u, v \rangle \quad (662)$$

is a linear functional. By Cauchy-Schwarz (644),

$$|\Lambda_u(v)| = |\langle u, v \rangle| \leq \|u\| \|v\|. \quad (663)$$

So  $\Lambda_u$  is bounded and

$$\Lambda_u \left( \frac{u}{\|u\|} \right) = \left\langle u, \frac{u}{\|u\|} \right\rangle = \frac{1}{\|u\|} \langle u, u \rangle = \|u\|. \quad (664)$$

Hence,  $\|\Lambda_u\| = \|u\|$ .

## Orthonormal Bases

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space.

- The *linear span* of a family  $\{e_n \mid n = 1, \dots, N\} \subseteq \mathcal{H}$ ,  $N \in \mathbb{N} \cup \{\infty\}$ , is the set of all *finite*  $\mathbb{C}$ -linear combinations of the  $e_n$ ; i.e.,

$$\text{span}\{e_1, \dots, e_N\} = \left\{ \sum_{\substack{i \\ \text{finite}}} \alpha_i e_i \mid \alpha_i \in \mathbb{C} \right\}. \quad (665)$$

- The sequence  $(e_n)$  is a (*countable*) *orthonormal system* (ONS) if

$$\langle e_i, e_j \rangle = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j, \end{cases} \quad (666)$$

i.e.,  $\|e_i\| = 1$  and  $e_i \perp e_j$  if  $i \neq j$ .

- An orthonormal basis of  $\mathcal{H}$  is a *Hilbert basis* of  $\mathcal{H}$ .

## Hilbert Space

Each finite-dimensional  $\mathbb{C}$ -inner product space  $V$  is complete.

### Proof.

Let  $\{e_1, \dots, e_N\}$  be a Hilbert basis of  $V$ .

Suppose the sequence of vectors  $u_n = \sum_{i=1}^N a_i^{(n)} e_i$  is Cauchy; i.e.,

$$\|u_k - u_n\|^2 = \sum_i |a_i^{(k)} - a_i^{(n)}|^2 \xrightarrow{k, n \rightarrow \infty} 0.$$

Then for each  $1 \leq i \leq N$ ,  $(a_i^{(n)})$  is Cauchy, since  $|a_i^{(k)} - a_i^{(n)}| \rightarrow 0$  as  $k, n \rightarrow \infty$ . But  $\mathbb{C}$  is complete and so  $(a_i^{(n)})$  has a limit  $a_i$ . Then  $(u_n)$  converges to  $u = \sum_{i=1}^N a_i e_i$ , since

$$\|u - u_n\|^2 = \sum_i |a_i - a_i^{(n)}|^2 \xrightarrow{n \rightarrow \infty} 0.$$



## Gram-Schmidt Orthonormalization Procedure

**Require:** Given  $\mathbb{C}$ -Hilbert space  $\mathcal{H}$  with basis  $\{v_1, \dots, v_n\}$ .

**Ensure:** ONS  $\{e_1, \dots, e_n\}$ .

$$e_1 \leftarrow v_1 / \|v_1\|.$$

**for**  $k \leftarrow 1$  to  $n - 1$  **do**

$$\hat{e}_{k+1} \leftarrow v_{k+1} - \sum_{i=1}^k \langle v_{k+1}, e_i \rangle e_i$$

$$e_{k+1} \leftarrow \hat{e}_{k+1} / \|\hat{e}_{k+1}\|$$

**end for**

## Tensor Spaces

The *tensor product* of two  $\mathbb{K}$ -vector spaces  $V, W$  is a  $\mathbb{K}$ -vector space  $V \otimes_{\mathbb{K}} W$  with a  $\mathbb{K}$ -bilinear mapping

$$\phi : V \times W \rightarrow V \otimes_{\mathbb{K}} W : (v, w) \rightarrow v \otimes w,$$

bilinearity means that for all  $v, v' \in V$ ,  $w, w' \in W$ , and  $\lambda \in \mathbb{K}$ ,

$$(v + v') \otimes w = v \otimes w + v' \otimes w, \quad (667)$$

$$v \otimes (w + w') = v \otimes w' + v \otimes w', \quad (668)$$

$$\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w). \quad (669)$$

## \*Tensor Spaces

Let  $V, W$  be  $\mathbb{K}$ -vector spaces.

- Let  $F$  be the  $\mathbb{K}$ -vector space  $F$  with basis elements  $v \otimes w$ , where  $v \in V$  and  $w \in W$ . The elements of  $F$  are  $\mathbb{K}$ -linear combinations of the form

$$\sum_{\text{finite}} \lambda_{v \otimes w} v \otimes w. \quad (670)$$

- Consider the  $\mathbb{K}$ -subspace  $R$  of  $F$  generated by

$$(v_1 + v_2) \otimes w - v_1 \otimes w - v_2 \otimes w, \quad (671)$$

$$v \otimes (w_1 + w_2) - v \otimes w_1 - v \otimes w_2, \quad (672)$$

$$(\lambda v) \otimes w - v \otimes (\lambda w) \quad (673)$$

for all  $v, v_1, v_2 \in V$ ,  $w, w_1, w_2 \in W$  and  $\lambda \in \mathbb{K}$ .

## \*Tensor Spaces

- Define the quotient  $\mathbb{K}$ -vector space

$$V \otimes_{\mathbb{K}} W = F/R = \{v + R \mid v \in F\}. \quad (674)$$

- The relations in  $V \otimes_{\mathbb{K}} W$  are

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w, \quad (675)$$

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2, \quad (676)$$

$$(\lambda v) \otimes w = v \otimes (\lambda w) \quad (677)$$

for all  $v, v_1, v_2 \in V$ ,  $w, w_1, w_2 \in W$  and  $\lambda \in \mathbb{K}$ .

- Scalar multiplication in  $V \otimes_{\mathbb{K}} W$  is given by

$$\lambda(v \otimes w) = (\lambda v) \otimes w \quad (678)$$

for all  $v \in V$ ,  $w \in W$  and  $\lambda \in \mathbb{K}$ .

## Tensor Spaces

Let  $V$  and  $W$  be  $\mathbb{K}$ -vector spaces with  $\mathbb{K}$ -bases  $v_1, \dots, v_m$  and  $w_1, \dots, w_n$ , resp.

- The tensor product  $V \otimes_{\mathbb{K}} W$  has basis

$$\{v_i \otimes w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}. \quad (679)$$

- Let the vector space  $U$  have  $\mathbb{K}$ -basis  $u_1, \dots, u_{mn}$ .  
Then the mapping  $V \otimes_{\mathbb{K}} W \rightarrow U$  given by

$$v_i \otimes w_j \mapsto u_{(i-1)n+j} \quad (680)$$

is a  $\mathbb{K}$ -vector space isomorphism.

- The tensor product  $V \otimes_{\mathbb{K}} W$  has dimension

$$\dim_{\mathbb{K}} V \otimes_{\mathbb{K}} W = \dim_{\mathbb{K}} V \cdot \dim_{\mathbb{K}} W. \quad (681)$$

## Tensor Spaces – Universal Property

Let  $U$ ,  $V$ , and  $W$  be finite-dimensional  $\mathbb{K}$ -vector spaces and

$$\phi : V \times W \rightarrow V \otimes_{\mathbb{K}} W : (v, w) \mapsto v \otimes w.$$

For each  $\mathbb{K}$ -bilinear mapping

$$\psi : V \times W \rightarrow U$$

there is a unique  $\mathbb{K}$ -linear mapping

$$\rho : V \otimes_{\mathbb{K}} W \rightarrow U$$

such that

$$\psi = \rho \circ \phi. \tag{682}$$

## Tensor Spaces – Universal Property

For finite-dimensional  $\mathbb{K}$ -vector spaces  $V$  and  $W$ , the tensor spaces  $V \otimes_{\mathbb{K}} W$  and  $W \otimes_{\mathbb{K}} V$  are isomorphic.

### Proof.

Let

$$\phi : V \times W \rightarrow V \otimes_{\mathbb{K}} W : (v, w) \mapsto v \otimes w.$$

For the  $\mathbb{K}$ -bilinear mapping

$$\psi : V \times W \rightarrow W \otimes_{\mathbb{K}} V : (v, w) \mapsto w \otimes v$$

by (682) there is a unique  $\mathbb{K}$ -linear mapping

$$\rho : V \otimes_{\mathbb{K}} W \rightarrow W \otimes_{\mathbb{K}} V : v \otimes w \mapsto w \otimes v.$$

Similarly, there is a unique  $\mathbb{K}$ -linear mapping

$$\rho' : W \otimes_{\mathbb{K}} V \rightarrow V \otimes_{\mathbb{K}} W : w \otimes v \mapsto v \otimes w.$$

The maps  $\rho, \rho'$  are inverse to each other and so isomorphisms.  $\square$

## Tensor Product Space

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space.

The Hilbert space

$$\mathcal{H}^{\otimes n} = \mathcal{H} \otimes_{\mathbb{C}} \mathcal{H} \otimes_{\mathbb{C}} \dots \otimes_{\mathbb{C}} \mathcal{H}, \quad n \text{ times,}$$

is the  $n$ -fold tensor product of  $\mathcal{H}$  over  $\mathbb{C}$  equipped with the  $\mathcal{H}$ -induced scalar product

$$\langle v_1 \otimes \dots \otimes v_n, w_1 \otimes \dots \otimes w_n \rangle = \prod_{i=1}^n \langle v_i, w_i \rangle_{\mathcal{H}},$$

where  $\langle \cdot, \cdot \rangle_{\mathcal{H}}$  denotes the scalar product on  $\mathcal{H}$ .

## Unitary Operators

Let  $\mathcal{H}$  be  $\mathbb{C}$ -Hilbert space. For each bounded linear operator  $A : \mathcal{H} \rightarrow \mathcal{H}$  there is a uniquely determined bounded linear operator  $A^* : \mathcal{H} \rightarrow \mathcal{H}$  such that

$$\langle Au, v \rangle = \langle u, A^*v \rangle, \quad u, v \in \mathcal{H}. \quad (683)$$

$A^*$  is the *adjoint operator* of  $A$ .

### Proof.

For each  $v \in \mathcal{H}$  define the linear functional

$$u \mapsto \langle Au, v \rangle.$$

By the Riesz representation theorem, there is a unique  $w \in \mathcal{H}$  such that

$$\langle Au, v \rangle = \langle u, w \rangle.$$

Putting  $A^*v = w$  gives  $\langle Au, v \rangle = \langle u, A^*v \rangle$ . □

## Unitary Operators

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space. Let  $A, B : \mathcal{H} \rightarrow \mathcal{H}$  be bounded linear operators and  $\lambda \in \mathbb{C}$ . Then

$$(A + B)^* = A^* + B^*, \quad (AB)^* = B^*A^*, \quad (684)$$

and

$$(\lambda A)^* = \bar{\lambda}A^*, \quad (A^*)^* = A. \quad (685)$$

### Proof.

Let  $u, v \in \mathcal{H}$ .

$$\begin{aligned} \langle (A + B)u, v \rangle &= \langle Au, v \rangle + \langle Bu, v \rangle = \langle u, A^*v \rangle + \langle u, B^*v \rangle \\ &= \langle u, (A^* + B^*)v \rangle. \end{aligned}$$

By the uniqueness of the adjoint operator,  $(A + B)^* = A^* + B^*$ .

## Proof (cont'd)

Let  $u, v \in \mathcal{H}$ .

$$\langle (AB)u, v \rangle = \langle A(Bu), v \rangle = \langle Bu, A^*v \rangle = \langle u, B^*(A^*v) \rangle.$$

By the uniqueness of the adjoint operator,  $(AB)^* = B^*A^*$ .

Let  $\lambda \in \mathbb{C}$ .

$$\begin{aligned} \langle (\lambda A)u, v \rangle &= \langle A(\lambda u), v \rangle = \langle \lambda u, A^*v \rangle = \bar{\lambda} \langle u, A^*v \rangle \\ &= \langle u, \bar{\lambda} A^*v \rangle. \end{aligned}$$

By the uniqueness of the adjoint operator,  $(\lambda A)^* = \bar{\lambda} A^*$ .

Finally,

$$\langle A^*u, v \rangle = \overline{\langle v, A^*u \rangle} = \overline{\langle Av, u \rangle} = \langle u, Av \rangle.$$

But  $\langle A^*u, v \rangle = \langle u, (A^*)^*v \rangle$  and so by the uniqueness of the adjoint operator,  $(A^*)^* = A$ .  $\square$

## Unitary Operators

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space and  $A : \mathcal{H} \rightarrow \mathcal{H}$  be a linear operator. If  $A$  is presented by a matrix  $M_A$ , the adjoint operator  $A^*$  is represented by the conjugate transpose of  $M_A$ .

### Proof.

Let  $\{e_1, \dots, e_n\}$  be a Hilbert basis of  $\mathcal{H}$ . Let  $M_A = (l_{ij})$  and  $M_{A^*} = (m_{ij})$  be representation matrices of  $A$  and  $A^*$ , resp. Then

$$Ae_i = \sum_{k=1}^n l_{ki} e_k \quad \text{and} \quad A^*e_i = \sum_{k=1}^n m_{ki} e_k.$$

Thus

$$\langle Ae_i, e_j \rangle = \sum_{k=1}^n \bar{l}_{ki} \langle e_k, e_j \rangle = \bar{l}_{ji}$$

and

$$\langle e_i, A^*e_j \rangle = \sum_{k=1}^n m_{kj} \langle e_i, e_k \rangle = m_{ij}.$$

But  $\langle Ae_i, e_j \rangle = \langle e_i, A^*e_j \rangle$  and so  $m_{ij} = \bar{l}_{ji}$ . □

## Unitary Operators

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space.

- A linear operator  $A : \mathcal{H} \rightarrow \mathcal{H}$  is *unitary* if

$$A^* A = \text{id}_{\mathcal{H}} = A A^*, \quad (686)$$

where  $A^*$  is the adjoint operator of  $A$  and  $\text{id}_{\mathcal{H}}$  is the identity operator.

- For each unitary operator  $A : \mathcal{H} \rightarrow \mathcal{H}$  and each  $v \in \mathcal{H}$  with  $\|v\|^2 = 1$ ,

$$\|Av\|^2 = \langle Av, Av \rangle = \langle v, A^* Av \rangle = \langle v, v \rangle = \|v\|^2 = 1. \quad (687)$$

- In quantum computing, unitary operators on Hilbert spaces are called *quantum gates*.

## Unitary Operators

Let  $\mathcal{H}$  be a  $\mathbb{C}$ -Hilbert space.

Let

$$A_k : \mathcal{H}^{\otimes n_k} \rightarrow \mathcal{H}^{\otimes n_k}, \quad n_k \geq 1, \quad (688)$$

be a collection of linear operators,  $1 \leq k \leq m$ .

The *tensor product* of these operators is the linear operator

$$A_1 \otimes \dots \otimes A_m : \mathcal{H}^{\otimes (n_1 + \dots + n_m)} \rightarrow \mathcal{H}^{\otimes (n_1 + \dots + n_m)} \quad (689)$$

given by

$$(A_1 \otimes \dots \otimes A_m)(u_1 \otimes \dots \otimes u_m) = (A_1 u_1) \otimes \dots \otimes (A_m u_m), \quad (690)$$

where  $u_k \in \mathcal{H}^{\otimes n_k}$ ,  $1 \leq k \leq m$ .

## Unitary Operators

The adjoint operator of  $A_1 \otimes \dots \otimes A_m$  is

$$(A_1 \otimes \dots \otimes A_m)^* = A_1^* \otimes \dots \otimes A_m^*. \quad (691)$$

### Proof.

Case  $m = 2$ :

$$\begin{aligned} & \langle (A_1 \otimes A_2)(u_1 \otimes u_2), v_1 \otimes v_2 \rangle \\ &= \langle A_1 u_1 \otimes A_2 u_2, v_1 \otimes v_2 \rangle = \langle A_1 u_1, v_1 \rangle \cdot \langle A_2 u_2, v_2 \rangle \\ &= \langle u_1, A_1^* v_1 \rangle \cdot \langle u_2, A_2^* v_2 \rangle = \langle u_1 \otimes u_2, A_1^* v_1 \otimes A_2^* v_2 \rangle \\ &= \langle u_1 \otimes u_2, (A_1^* \otimes A_2^*)(v_1 \otimes v_2) \rangle. \end{aligned}$$

By the uniqueness of the adjoint operator,

$$(A_1 \otimes A_2)^* = A_1^* \otimes A_2^*. \quad \square$$

## Unitary Operators

If  $A_1, \dots, A_m$  are unitary operators, then  $A_1 \otimes \dots \otimes A_m$  is also unitary.

### Proof.

Case  $m = 2$ :

$$\begin{aligned} & (A_1 \otimes A_2)^*(A_1 \otimes A_2)(u_1 \otimes u_2) \\ &= (A_1^* \otimes A_2^*)(A_1 u_1 \otimes A_2 u_2) \\ &= A_1^* A_1 u_1 \otimes A_2^* A_2 u_2 \\ &= u_1 \otimes u_2. \end{aligned}$$

Thus  $(A_1 \otimes A_2)^*(A_1 \otimes A_2)$  is the identity operator. □