

EE4.07 Coding Theory

W. Dai

Imperial College London (IC)

2015

Syllabus

Instructor: Dr. Wei Dai

Lectures: 2 hours per week \times 10 weeks = 20 hours

Office hours: Tuesday and Friday 10:00-10:55 (Room 811, EEE Building)

Assessment: One exam in the next summer.

Textbook: No textbook is required. You can rely on lecture notes.

References:

- ▶ “Introduction to coding theory” Ron M. Roth
- ▶ “Coding Theory: a First Course,” S. Lin and C. Xing
- ▶ “Codes: An Introduction to Information Communication and Cryptography,” N. L. Biggs

Contents

1. Mathematical foundations: finite fields

2. Cryptography

- ▶ Password management: store, exchange, and secret share
- ▶ Public key cryptography
- ▶ Digital signature

3. Error correcting codes

- ▶ Linear block codes
- ▶ Hamming codes
- ▶ Reed-Solomon codes and decoding

4. Modern codes

- ▶ Brief introduction to information theory
- ▶ Low-density parity check (LDPC) codes
- ▶ Polar codes

Section 1

Finite Fields

- ▶ Basic facts
 - ▶ Euclidean algorithm
 - ▶ Unique factorisation theorem
- ▶ Finite fields: definition and construction
- ▶ Finite fields: general properties
- ▶ Primitive elements
- ▶ Polynomial factorisation and minimal polynomials

For basic number theory, the best reference is Wikipedia.

For contents relevant to finite fields, refer to Lin&Xing's book, Chapter 3.

Three Facts for Coding Theory

Euclidean geometry: all theorems are derived from a small number of axioms.

This course: mostly relies on three facts.

- ▶ A polynomial of degree n has at most n roots.
- ▶ Every positive integer $n > 1$ can be uniquely represented as a product of prime numbers. (will be proved.)
- ▶ Euclidean algorithm to compute the greatest common divisor. (Details will be given.)

Greatest Common Divisor (GCD)

How to find the gcd for $0 < b < a$?

$$\gcd(5, 13) = 1. \text{ (Easy!)}$$

$$\gcd(20, 36) = 4. \text{ (OK)}$$

$$\text{But } \gcd(654, 2406) = ?$$

The Euclidean Algorithm

Lemma 1.1 (Euclidean Algorithm)

Let $a, b \in \mathbb{Z}^+$. Without loss of generality (WLOG), assume $a < b$. To find the greatest common divisor of a and b ,

$$\begin{array}{rcl} a & = q_1 b & + r_1 \\ b & = q_2 r_1 & + r_2 \\ r_1 & = q_3 r_2 & + r_3 \\ & \vdots & \vdots \\ r_{n-2} & = q_n r_{n-1} & + r_n \\ r_{n-1} & = q_{n+1} r_n & \end{array}$$

(last non-zero remainder.)

Then $d := \gcd(a, b) = r_n$.

The Euclidean Algorithm: An Example

$$\text{gcd}(654, 2406)$$

$$2406 = 3 \times 654 + 444$$

$$654 = 1 \times 444 + 210$$

$$444 = 2 \times 210 + 24$$

$$210 = 8 \times 24 + 18$$

$$24 = 1 \times 18 + 6 \leftarrow$$

$$2406 = 3 \times 654 + 444$$

$$654 = 1 \times 444 + 210$$

$$444 = 2 \times 210 + 24$$

$$210 = 8 \times 24 + 18$$

$$24 = 1 \times 18 + 6$$

$$18 = 3 \times 6$$

Example 1.2

$$\text{gcd}(654, 2406) = ?:$$

$$\text{gcd}(654, 2406) = 6.$$

The Euclidean Algorithm: Theory

$$r = a \bmod b$$

Let $a = qb + r$, $1 \leq r < b$.
Theorem 1.3 Let $d_1 = \gcd(a, b)$. $d_2 = \gcd(b, r)$. $\therefore d_2 = \gcd(b, r) \geq \gcd(b, r) = d_1$.

For $0 < r < b < a$, define $r = a \bmod b \neq 0$. Then $\gcd(a, b) = \gcd(b, r)$.

Proof: Let $a = bq + r$ where $1 \leq r < b$.

Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(b, r)$. Want to show $d_1 = d_2$.

$$\left. \begin{array}{l} d_1 | a \text{ and } d_1 | b \Rightarrow d_1 | (a - bq) \Rightarrow d_1 | r \\ d_2 = \gcd(b, r) \end{array} \right\} \Rightarrow d_1 \leq d_2.$$

$$\left. \begin{array}{l} d_2 | b \text{ and } d_2 | r \Rightarrow d_2 | (bq + r) \Rightarrow d_2 | a \\ d_1 = \gcd(a, b) \end{array} \right\} \Rightarrow d_2 \leq d_1.$$

Therefore, $d_1 = d_2$. \diamond

Corollary 1.4 (Validation of Euclidean Alg.)

In the Euclidean algorithm,

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n.$$

Bézout's Identity

$$\boxed{a, n \text{ coprime} \Leftrightarrow \gcd(a, n) = 1 \Leftrightarrow ab + xn = 1 \Leftrightarrow ab \equiv 1 \pmod{n}}$$

Lemma 1.5 (Bézout's Identity or Bézout's Lemma)

Given positive integers a and b , let $d = \gcd(a, b)$. Then d can be written as an integer linear combination of a and b , i.e., $\exists x, y \in \mathbb{Z}$ s.t.

$$d = \gcd(a, b) = \boxed{xa + yb}, \quad r_{n-2} = q_n r_{n-1} + r_n \Rightarrow r_n = r_{n-2} - q_n r_{n-1}$$

$$\begin{aligned} r_n &= -q_n r_{n-1} + r_{n-2} \\ &= -q_n (-q_{n-1} r_{n-2} + r_{n-3}) + r_{n-2} \quad \text{for all } i, r_i \text{ can be expressed} \\ &= (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3} \quad \text{by the linear combination of} \\ &= \dots = xa + yb. \quad r_{i-1} \& r_{i-2}. \end{aligned}$$

$$\text{Example 1.6 } (\gcd(13, 5) = 1)$$

Euclidean Alg.

$$\begin{aligned} 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Bézout's Identity

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (13 - 2 \cdot 5) - 5 = \textcolor{blue}{2} \cdot 13 - \textcolor{blue}{5} \cdot 5 \end{aligned}$$

Euclidean Algorithm for Polynomials

$$x^4 + x^3 + x^2 + x + 1 \quad x^4 + x^3 + x^2 + x + 1 = (x^2 - x + 2)(x^2 + x) + (-x + 1)$$

Extend the Euclidean algorithm to polynomials. $\gcd(a(x), b(x)) = 2$.

Example 1.7

$$-x + 1 = \left(-\frac{x}{2} + \frac{1}{2}\right) \cdot 2$$

Let $a(x) = \underline{\underline{x^4 + x^3 + x^2}} + x^2 + x + 1$ and $b(x) = x^2 + x$. Find $\gcd(a(x), b(x))$.

$$\begin{aligned} \text{Note that } & x^4 + x^3 + x^2 + x + 1 = (x^2 - x + 2)(x^2 + x) + a(x) \\ & x^2 + x = (-x + 2)(-x + 1) + 2b(x) \\ & -x + 1 = \left(-\frac{1}{2}x + \frac{1}{2}\right) \cdot 2. \\ & = (x + 2)a(x) - (x^3 + x^2 + 3)b(x) \end{aligned}$$

One has

$$\begin{aligned} 2 &= \frac{2x+2}{x^2+x} + (x+2)(-x+1) \\ &= b(x) + (x+2)(a(x) - (x^2 - x + 2)b(x)) \\ &= (x+2)a(x) + (-x^3 - x^2 - 3)b(x). \end{aligned}$$

As a result,

$$\begin{aligned} 1 &= \gcd(a(x), b(x)) \\ &= \frac{1}{2}(x+2)a(x) - \frac{1}{2}(x^3 + x^2 + 3)b(x). \end{aligned}$$

Fundamental Theorem of Arithmetic

Theorem 1.8 (Unique Factorisation Theorem)

Any $n \in \mathbb{Z}^+$, $n > 1$, can be uniquely represented as a product of prime powers:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i}$$

Example 1.9 (Applications)

If we know the factorisation of a and b ,

- Greatest common divisor:

$$\begin{aligned}\underline{\gcd(a, b)} &= 2^{\min(a_2, b_2)} 3^{\min(a_3, b_3)} 5^{\min(a_5, b_5)} 7^{\min(a_7, b_7)} \dots \\ &= \prod p_i^{\min(a_{p_i}, b_{p_i})},\end{aligned}$$

- Least common multiple:

$$\begin{aligned}\underline{\lcm(a, b)} &= 2^{\max(a_2, b_2)} 3^{\max(a_3, b_3)} 5^{\max(a_5, b_5)} 7^{\max(a_7, b_7)} \dots \\ &= \prod p_i^{\max(a_{p_i}, b_{p_i})}.\end{aligned}$$

Some Examples

Example 1.10

$$\begin{aligned} 4 &= 2^2. \\ 6 &= 2 \cdot 3. \end{aligned} \Rightarrow \begin{aligned} \gcd(4, 6) &= 2^1 \cdot 3^0 = 2. \\ \text{lcm}(4, 6) &= 2^2 \cdot 3^1 = 12. \end{aligned}$$

$$\begin{aligned} 4 &= 2^2. \\ 9 &= 3^2. \end{aligned} \Rightarrow \begin{aligned} \gcd(4, 9) &= 2^0 \cdot 3^0 = 1. \\ \text{lcm}(4, 9) &= 2^2 \cdot 3^2 = 36. \end{aligned}$$

$$\begin{aligned} 654 &= 2 \cdot 3 \cdot 109. \\ 2406 &= 2 \cdot 3 \cdot 401. \end{aligned} \Rightarrow \begin{aligned} \gcd(654, 2406) &= 6. \\ \text{lcm}(654, 2406) &= 262254. \end{aligned}$$

Proof of Unique Factorisation Theorem

Unique factorisation, prime $\vee = 1 \times n$

..... n

'true' ? 'composite' $n = a \cdot b$, $1 < a \leq b < n$

$a \cdot b$ are product of primes
 \Downarrow

$p_1 \cdots p_n$

$q_1 \cdots q_m$

$n = ab$ is product of primes.

Existence: By induction.

Assume it is true for all numbers less than n . (*existence*)

If n is prime, n is the product of one prime n .

Otherwise, $\exists a, b$ where $n = a \cdot b$ and $1 < a \leq b < n$. By the induction hypothesis, $a = p_1 p_2 \cdots p_n$ and $b = q_1 q_2 \cdots q_m$ are products of primes.

Then $n = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m$ is the product of primes. \diamond

Uniqueness: will need the Euclid's lemma.

Euclid's Lemma

$$\begin{aligned} & \because p \nmid a \therefore \gcd(p, a) = 1 \therefore xp + ya = 1 \\ & \therefore xp \mid b \quad ya \mid b \\ & \therefore p \mid xp \quad p \mid ya \Rightarrow p \mid yab \\ & \therefore p \mid (xp + ya) \Rightarrow p \mid b. \end{aligned}$$

Lemma 1.11 (Euclid's Lemma)

Let p be a prime number. If $p \mid ab$, then $p \mid a$ or $p \mid b$ (or both). Or equivalently,

$$n = \prod_{i=1}^k p_i^{a_i}$$

$$\text{eg. } a = 2^3 \cdot 5 \Rightarrow ab = 2^5 \cdot 5^2$$

- If $p \nmid a$ and $p \nmid b$, then $p \nmid ab$.
- If $p \nmid a$ and $p \mid ab$, then $p \mid b$.

$$\begin{aligned} p &\nmid 2 \mid a \Rightarrow p \nmid ab \\ p &\nmid 2 \mid ab \Rightarrow p \mid a \\ &\quad \text{or } p \mid b \end{aligned}$$

Proof of the last statement: Since $p \nmid a$, $\gcd(p, a) = 1$.

By Bézout's Identity, $\exists x, y \in \mathbb{Z}$ s.t.

$$xp + ya = 1.$$

Multiply both sides by b ,

$$xp \cdot b + ya \cdot b = b.$$

Since $p \mid xp \cdot b$ and $p \mid ya \cdot b$ (by assumption), it holds that $p \mid xp \cdot b + ya \cdot b$.

Hence $p \mid b$.



Proof of Unique Factorisation Theorem (Uniqueness)

$$\because p_1 | p_1 p_2 \cdots p_m \Rightarrow p_1 | n \Rightarrow p_1 | q_1 q_2 \cdots q_n \quad \therefore \text{say } p_1 | q_j \text{ in the end.}$$
$$\therefore p_1 q_1 \text{ or } p_1 q_2 \cdots q_n \quad \because p_i, q_j \text{ are primes}$$

Assume that $n > 1$ is the product of primes in two different ways:

$$n = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

We shall show $m = n$ and that the q_i are a rearrangement of the p_i .
similarly every p corresponds a same q , and eventually $m=n$.

WLOG, assume $m \leq n$. By Euclid's lemma, p_1 must divide one of the q_j . Relabel the q_j if necessary, say that $p_1 | q_1$. But q_1 is prime. Hence $p_1 = q_1$ so that

$$\frac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_n.$$

Repeat the process, we eventually arrive at

$$\frac{n}{p_1 \cdots p_m} = 1 = q_{m+1} \cdots q_n.$$

From this, it is clear that $m = n$ and every q_j is a p_i . \diamond

Fields: Definition

Definition 1.12 (Field)

A field \mathbb{F} is a nonempty set of elements with two operations, called addition (+) and multiplication (\cdot).

- ▶ \mathbb{F} is closed under + and \cdot , i.e., $a + b$ and $a \cdot b$ are in \mathbb{F} .
 - ▶ Commutative: $a + b = b + a$
 - ▶ Associative: $a + (b + c) = (a + b) + c$
 - ▶ Distributive $a(b + c) = ab + ac$
- ▶ Exists two distinct identity 0 and 1 (additive and multiplicative identities, respectively)
 - ▶ $a + 0 = a, \forall a \in \mathbb{F}$
 - ▶ $a \cdot 1 = a$ and $a \cdot 0 = 0, \forall a \in \mathbb{F}$
 - ▶ Additive inverse: $\forall a \in \mathbb{F}, \exists (-a) \in \mathbb{F}$, s.t. $a + (-a) = 0$.
 - ▶ Multiplicative inverse: $\forall a \in \mathbb{F} \setminus \{0\}, \exists a^{-1} \in \mathbb{F}$, s.t. $a \cdot a^{-1} = 1$.

C	✓
R	✓
Q	✓
Z	✗
N	✗

Example: $\mathbb{R}, \mathbb{Q}, \mathbb{Z}_7$ are fields, \mathbb{Z} is not. (no multiplicative inverse!)

Integer Ring

$\text{Modulo } (\bmod)$	$a = qn + r$
$\Rightarrow r = a \bmod n$	

Congruent Modulo (\equiv)

$$(a \bmod n) \equiv (b \bmod n) \quad a \equiv b \pmod{n}$$

if a, n coprime
we can find b s.t.
 $ab \equiv 1 \pmod{n}$.

Definition 1.13 (Modulo)

The **modulo** operator finds the remainder of one number divided by another.

$$(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$$

$$(a \times b) \bmod n = (a \bmod n \times b \bmod n) \bmod n$$

Proof: $\gcd(a, n) = 1$
 $\Rightarrow ab + kn = 1$
 $\Rightarrow ab \equiv 1 \pmod{n}$

Examples: $5 \bmod 4 = 1$, $14 \bmod 4 = 2$.

$$\text{eg. } 11 \equiv 4 \pmod{7} \quad -11 \equiv 3 \pmod{7}$$

$$[11 + (-11)] \bmod 7 = (11 \bmod 7 + (-11) \bmod 7) \bmod 7 \\ = (4 + 3) \bmod 7 = 0$$

Definition 1.14 (Integer Ring)

$$\text{eg. } 5 \times 5 \equiv 1 \pmod{12}, \quad 11 \times 5 \equiv 7 \pmod{12}$$

► $\mathbb{Z}_m = \{0, \dots, m-1\}$: a nonempty set of $\boxed{1}$ elements.

$$5 \equiv \frac{1}{5} \pmod{12} \quad 11 \equiv \frac{7}{5} \pmod{12}$$

$$\text{eg. } \frac{5}{6} \bmod{12} = x \quad (?)$$

$$6x \equiv 5 \pmod{12}$$

Can't find x ?
not defined.
within
bound

Example of $m = 4$:

$$\mathbb{Z}_m = \{0, 1, 2, 3\}.$$

$$1 + 1 = 2 \pmod{4}; \quad 2 + 3 = 1 \pmod{4}.$$

$$3 \cdot 3 = 1 \pmod{4}; \quad 2 \cdot 2 = 4 = 0 \pmod{4}.$$

Examples: Integer Rings Versus Fields

field: $\begin{cases} \text{addition} \rightarrow \text{addition inverse } a + (-a) = 0 \\ \text{multiplication} \rightarrow \text{multiplication inverse } a(a^{-1}) = 1 \end{cases}$ exist!

$$-0 \equiv 0 \pmod{3}$$

$$-1 \equiv 2 \pmod{3}$$

$$1^{-1} = \frac{1}{1} \pmod{3} : x \Rightarrow 1 \cdot x \equiv 1 \pmod{3}$$

$$\Rightarrow x=1 \text{ within field}$$

► \mathbb{Z}_3 is a field. $-2 \equiv 1 \pmod{3}$

$$\triangleright -0 = 0, -1 = 2, -2 = 1.$$

$$\triangleright 1^{-1} = 1, 2^{-1} = 2.$$

$$\therefore 1^{-1} \equiv 1 \pmod{3}$$

$$2^{-1} = \frac{1}{2} \pmod{3} : x \Rightarrow 2x \equiv 1 \pmod{3}$$

$$\Rightarrow x=2 \text{ within bound}$$

► \mathbb{Z}_4 is not a field.

mod number (to be decided)

$$\triangleright -0 = 0, -1 = 3, -2 = 2, -3 = 1.$$

$$\triangleright 1^{-1} = 1, \nexists 2^{-1}, 3^{-1} = 3.$$

$$\therefore 2^{-1} \equiv 2 \pmod{3}$$

{For fields, mod number must be prime.}

$$-0 \equiv 0 \pmod{4}$$

$$1^{-1} = \frac{1}{1} \pmod{4} : x \Rightarrow 1 \cdot x \equiv 1 \pmod{4} \Rightarrow x=1 \quad \checkmark$$

$$-1 \equiv 3 \pmod{4}$$

$$2^{-1} = \frac{1}{2} \pmod{4} : x \Rightarrow 2x \equiv 1 \pmod{4} \Rightarrow x=0.5 \quad x \text{ not}$$

$$-2 \equiv 2 \pmod{4}$$

$$3^{-1} = \frac{1}{3} \pmod{4} : x \Rightarrow 3x \equiv 1 \pmod{4} \Rightarrow x=3 \quad \checkmark. \quad \therefore \mathbb{Z}_4 \text{ is not field.}$$

$$-3 \equiv 1 \pmod{4}$$

When a Multiplicative Inverse Exists

Lemma 1.15 (Existence of the multiplicative inverse)

Let $a, n \in \mathbb{Z}^+$ with $a < n$. The multiplicative inverse $a^{-1} \pmod{n}$ exists iff $\gcd(a, n) = 1$. (a, n coprime)

$$a^{-1} \text{ exists} \iff a \cdot n \text{ coprime}$$

assume $d = \gcd(a, n) > 1$

$\therefore x = a^{-1}$ exists

$$\therefore xa \equiv 1 \pmod{n}$$

$$\therefore xa - yn \equiv 1 \pmod{n}$$

$$\therefore d | xa - yn$$

$\therefore d | 1$ (linear combination of a, n)

1. If $\gcd(a, n) = 1$, by Bézout's identity, $\exists x, y \in \mathbb{Z}$ s.t. $xa - yn = 1$.

$$1 = xn + ya \equiv ya \pmod{n}. \text{ Hence } y \text{ is a } a^{-1}$$

2. If $a^{-1} \pmod{n}$ exists, want to show that $\gcd(a, n) = 1$.

Suppose not, i.e., $d = \gcd(a, n) > 1$.

By assumption that a^{-1} exists, $\exists x = a^{-1}$ and y s.t.

$$1 = xa \pmod{n} = xa - yn.$$

$$\therefore xn + ya = 1$$

As $d | a$ and $d | n$, it follows $d | (xa - yn)$, i.e. $d | 1$.

$$\therefore xn + ya \equiv 1 \pmod{n}$$

This contradicts with $d > 1$.

$$\therefore ya \equiv 1 \pmod{n}$$

$\therefore y = a^{-1}$ exists.



Finite Fields of Integers

Theorem 1.16

\mathbb{Z}_m is a field if and only if m is a prime. (Hence notation \mathbb{F}_p .)

Proof of the "if" part: m be a prime $\Rightarrow \mathbb{Z}_m$ is a field.

$\forall a \in \mathbb{Z}_m \setminus \{0\}$, since m is a prime, one has $\gcd(a, m) = 1$.

By Lemma 1.15, a^{-1} exists. *every element in the field*: $\frac{\text{have } a^{-1}}{\gcd(a, n) = 1}$ ◇

Proof of the "only if" part: \mathbb{Z}_m is a field $\Rightarrow m$ is a prime.

Suppose m is not a prime. $\exists 1 < a, b < m$ s.t. $a \cdot b = m$. \downarrow *a, b coprime for all a prime*

Since $a = \gcd(a, m) \neq 1$, by Lemma 1.15, a^{-1} does not exist. ◇

if m not prime $\Rightarrow m = ab$

$\therefore \gcd(a, m) \neq 1$ for $1 < a < m$

$\therefore a^{-1}$ doesn't exist

$\therefore \mathbb{Z}_m$ is not field.

An Alternative Proof

Recall: \mathbb{Z}_m is a field if and only if m is a prime. (Hence notation \mathbb{F}_p .)

Lemma 1.17

Let $a, b \in \mathbb{F}_p$. Then $ab = 0$ implies $a = 0$ or $b = 0$.

Proof: Suppose that $a \neq 0$. Then $0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = b$. \diamond

Alternative proof of the “only if” part:

$ab=m \Rightarrow ab \equiv m \pmod{m}$

Suppose m is not a prime. $\exists 1 < a, b < m$ s.t. $a \cdot b = m \equiv 0 \pmod{m}$.

Either a or b is zero mod m . Contradict with $1 < a, b < m$. \diamond

$a \pmod{m} = 0$
or
 $b \pmod{m} = 0$ contradict.

Set of Polynomials

Polynomials over a field \mathbb{F}_p : $f(x) = \sum_{i=0}^d a_i x^i$, $a_i \in \mathbb{F}_p$.

Degree: highest degree of its terms: $\deg(f) = d$ if $a_d \neq 0$.

Monic polynomials: $a_d = 1$.

$$\begin{array}{r} x^3 + x \\ \overline{x^3 + 0x^2 + x + 1} \\ \hline x^3 + x^2 \\ \hline x^2 + x \\ \hline x^2 + x \\ \hline 0 \end{array}$$

$$a(x) = (x+1)b(x) + 1$$

Polynomial division:

$$a(x) = q(x)b(x) + r(x) \text{ where } 0 \leq \deg(r(x)) < \deg(b(x)).$$

Example: Let $a(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ and $b(x) = x^2 + x \in \mathbb{F}_2[x]$.

Then $a(x) = (x+1)b(x) + 1$.

$f(x) \in \mathbb{F}[x]$ is **irreducible** if $f(x) = g(x)h(x)$, $g, h \in \mathbb{F}[x]$, implies either g or h is a constant (similar to **prime numbers**).

$x^2 + 1 \in \mathbb{R}[x]$: irreducible

$x^2 + 1 \in \mathbb{F}_2[x]$: reducible $\rightarrow x^2 + 1 = x^2 + 2x + 1 = (x+1)(x+1)$

$x^2 + 1 \in \mathbb{F}_3[x]$: irreducible

$x^2 + 1 \in \mathbb{F}_5[x]$: reducible $\rightarrow x^2 + 1 = x^2 - 4 = (x-2)(x+2) = (x+3)(x+2)$

Finite Fields: Polynomials

$$\mathbb{F}_p[x] = \left\{ g(x) = \sum_{i=0}^d a_i x^i : a_i \in \mathbb{F}_p \right\}. \quad A \text{ mod } n$$

$\mathbb{F}_p[x]/f(x)$: $\mathbb{F}_p[x]$ with "mod $f(x)$ " algebra. $\mathbb{F}_p[x] / \text{mod } f(x) \Rightarrow \mathbb{F}_p[x]/f(x)$

It contains all the polynomials with degree less than $\deg(f)$.

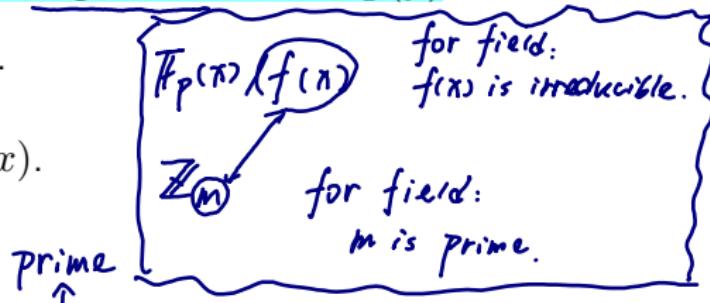
Example: $f(x) = x^2 + x \in \mathbb{F}_2[x]$.

$$\mathbb{F}_2[x]/f(x) = \{0, 1, x, x+1\}.$$

$$x \cdot (x+1) = x^2 + x \equiv 0 \pmod{f(x)}.$$

Theorem 1.18

$\mathbb{F}_p[x]/f(x)$ is a field iff $f(x)$ is irreducible over \mathbb{F}_p .



Proof: Same idea as before.

- \mathbb{F}_q contains numbers: $q = p$.
- \mathbb{F}_q contains polynomials: $q = p^d$ where $d = \deg(f)$.

Example Fields Containing Polynomials

Some irreducible polynomials over \mathbb{F}_2

$x, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1, x^4 + x + 1, \dots$

Each of these polynomial generates a finite field.

Example 1.19

$\# \text{ terms}$ $\leq P^d$	$\mathbb{F}_2[x] / x^3 + x + 1$	$\mathbb{F}_2[x] / x^3 + x^2 + 1$
0	0	x^0
1	1	x^0
x	x	x^1
x^2	x^2	x^2
x^3	$x + 1$	$x^2 + 1$
x^4	$x^2 + x$	$x^2 + x + 1$
x^5	$x^2 + x + 1$	$x + 1$
x^6	$x^2 + 1$	$x^2 + x$

$$x^3 + x^2 + 1 \quad | \quad \overline{x^3 + 0x^2 + 0x + 0}$$

$$x^3 + x^2 + 0x + 1$$

$$x^3 + x^2 + 1 \quad | \quad \overline{x^3 + 0x^2 + 0x + 0}$$

$$x^3 + x^2 + 0x + 1$$

$$x^3 + x^2 + 1 \quad | \quad \overline{x^4 + 0x^3 + 0x^2 + 0x + 1}$$

$$x^4 + x^3 + 0x^2 + x$$

$$\overline{+ x^3 + 0x^2 + x}$$

$$x^3 + x^2 + 0x + 1$$

$$\overline{+ x^2 + x + 1}$$

Another Example

Example 1.20 (An Example of \mathbb{F}_{16})

$\mathbb{F}_2[x]/x^4 + x + 1$	$\mathbb{F}_2[x]/x^4 + x + 1$
0	0
1	$x^3 + x + 1$
x	$x^2 + 1$
x^2	$x^3 + x$
x^3	$x^2 + x + 1$
x^4	$x^3 + x^2 + x$
x^5	$x^3 + x^2 + x + 1$
x^6	$x^3 + 1$

$$x^5 = x \cdot x^4 \equiv x \cdot (x^3 + 1) = x^4 + x \equiv 1$$

$$\begin{aligned}x^{16} &= x \cdot x^5 \equiv x \\&\vdots\end{aligned}$$

$$\text{Useful Exercise } x^3+x^2 \quad x^3+x^2+1$$

i) $(axb) \bmod n = (a \bmod n \cdot b \bmod n) \bmod n$

$$\therefore (x^3+x^2)(x^3+x^2+1)/x^4+x+1 = x^6 \cdot x^{13}/x^4+x+1 = x^{19-15} / (x^4+x+1 = x+1)$$

ii) $f = x^4+x+1, g = x^3+x^2$

Example 1.21 (An Exercise)

$$h = g^{-1} \Rightarrow hg \equiv 1 \pmod{f}$$

1. Understand Examples 1.19 and 1.20.

$\Rightarrow hg + kf = 1$ $\therefore 1 = (x^2+x+1) - (x+1)x$

2. For the field $\mathbb{F}_2[x]/x^4+x+1$ in Example 1.20, compute:

$$\begin{aligned} & \left(\begin{array}{l} x^4+x \\ x^3+x^2 \end{array} \right) \left(\begin{array}{l} x^4+x^2 \\ x^3+x^2+1 \end{array} \right)^{-1} = ? \quad \text{iii) } f = x^4+x+1, g = x^3+x^2 \\ & \quad \begin{array}{l} x^4+x^2 = (x+1)(x^3+x^2+1) + x^2 \\ x^3+x^2+1 = (x+1)(x^3+x^2+1) + x^2 \end{array} \\ & \quad \begin{array}{l} x^3+x^2+1 = (x+1)x^2 \\ x^3+x^2 = (x+1)x^2 + 1 \end{array} \\ & \quad \begin{array}{l} x^3+x^2+1 = (x+1)x^2 + 1 \\ x^3+x^2 = (x+1)x^2 + 1 \end{array} \\ & \quad \begin{array}{l} x^3+x^2+1 = (x+1)x^2 + 1 \\ x^3+x^2+1 = (x+1)x^2 + 1 \end{array} \end{aligned}$$

Answer: x^3+x^2+1

► $\left(\begin{array}{l} x^3+x^2 \\ x^2+x+1 \end{array} \right)^{-1} = ?$ (Use Euclidean algorithm)

► Answer: x^3+x^2

$$\begin{aligned} & \left(\begin{array}{l} x^3+x^2 \\ x^3+x^2+0x+0 \end{array} \right) \left(\begin{array}{l} x^3+x^2+0x+0+1 \\ x^2+x+1 \end{array} \right)^{-1} = ? \quad \text{(Use Euclidean algorithm)} \\ & \quad \begin{array}{l} x^3+x^2+0x+0 = (x+1)f + x^2g \\ x^2+x+1 = (x+1)f + x^2g \end{array} \\ & \quad \begin{array}{l} x^2+x+1 = (x+1)f + x^2g \\ x^2+x+1 = (x+1)f + x^2g \end{array} \\ & \quad \begin{array}{l} x^2+x+1 = (x+1)f + x^2g \\ x^2+x+1 = (x+1)f + x^2g \end{array} \end{aligned}$$

Answer: x^2 .

\downarrow

$\rightarrow h$

Finite Fields: General Properties?

Previously, we saw two ways to construct finite fields.

- ▶ \mathbb{F}_p : p many integers.
- ▶ $\mathbb{F}_p[x]/f(x)$: $p^{\deg(f)}$ many polynomials.

What can we say about the size of a finite field \mathbb{F} in general?

Characteristic: Definition

Let \mathbb{F} be an arbitrary field. *(unit element)*

By definition, \exists a multiplicative identity, denoted by '1'.

Consider a sequence in \mathbb{F}_q : $1, 1+1, \dots$

Since $|\mathbb{F}_q| = q < \infty$, we will see repetitions.

That is, $\exists t \in \mathbb{Z}^+$ s.t. $\underbrace{1 + \dots + 1}_{t \text{ times}} = t \cdot 1 = 0$.

Remark: To compute $1 + \dots + 1 = t \cdot 1$, we have used the algebra defined for this field \mathbb{F} .

$$\text{e.g. } \mathbb{F}_3 : 3 \times 1 = 0$$

Definition 1.22 Δ $\mathbb{F}_{2^4} : 2 \times 1 = 0$

The smallest t s.t. $t \cdot 1 = 0$ is called **characteristic** of \mathbb{F} .

For \mathbb{F}_{p^m} , $t = p$.

Characteristic: Property

Lemma 1.23

The characteristic t is always a prime.

Proof: Otherwise, $t \cdot 1 = ab \cdot 1 = 0$.

1st equation uses normal algebra for integers. 2nd equation uses the algebra for the finite field.

This implies $a = 0$ or $b = 0$ (by Lemma 1.17).

Contradict with that t is the smallest.

Finite Fields: Size

Theorem 1.24

All finite fields are of the size p^m .

Proof: For any given finite field \mathbb{F}_q , let p be its characteristic.

Choose a nonzero element from \mathbb{F}_q , say b_1 .

Choose another nonzero element from \mathbb{F}_q , say b_2 , such that b_2 and b_1 are linearly independent, i.e.,

$$\lambda_1 b_1 + \lambda_2 b_2 = 0, \quad \lambda_1, \lambda_2 \in \underline{\mathbb{F}_p} \Leftrightarrow \lambda_1 = \lambda_2 = 0.$$

Consider a maximal set

$$\mathcal{B} = \{b_1, \dots, b_m\} \subset \underline{\mathbb{F}}$$

*b_1, \dots, b_m : basic element
(with different dims)*

which are linearly independent over $\underline{\mathbb{F}_p}$.

*$\lambda_1, \dots, \lambda_m$: basic number
(within certain P)*

Define the linear span of \mathcal{B}

$$\text{span}(\mathcal{B}) = \{\lambda_1 b_1 + \dots + \lambda_m b_m : \lambda_i \in \mathbb{F}_p\}.$$

$$= P^m$$

Finite Fields: Size and Dimension

Proof continued:

1. Then $|\text{span}(\mathcal{B})| = p^m \leq |\mathbb{F}_q|$.

If $(\lambda_1^{(1)}, \dots, \lambda_m^{(1)}) \neq (\lambda_1^{(2)}, \dots, \lambda_m^{(2)})$, then $\sum \lambda_i^{(1)} b_i \neq \sum \lambda_i^{(2)} b_i$.

Suppose not, i.e., $\sum \lambda_i^{(1)} b_i = \sum \lambda_i^{(2)} b_i$. Then $\sum (\lambda_i^{(1)} - \lambda_i^{(2)}) b_i = 0$ which, by linear independence of b_i 's, implies that $\lambda_i^{(1)} = \lambda_i^{(2)}$.

This contradicts the assumption that $(\lambda_1^{(1)}, \dots, \lambda_m^{(1)}) \neq (\lambda_1^{(2)}, \dots, \lambda_m^{(2)})$.

2. It also holds that $|\text{span}(\mathcal{B})| = |\mathbb{F}_q|$:

Otherwise $\exists b_{m+1}$ linearly independent of \mathcal{B} .

This contradicts with the definition of the maximal independent set \mathcal{B} .

Hence, for any finite field \mathbb{F}_q , $q = p^m$.



\mathcal{B} is a basis of \mathbb{F}_q .

m is the dimension of \mathbb{F}_q .

Primitive Elements

$\forall a \in \mathbb{F}$, consider the sequence a, a^2, a^3, \dots . Since $|\mathbb{F}_q| = q$ is finite, we will see repetitions. That is, $\exists t$ s.t. $a^t = 1$.

order of a : smallest number that $a^{\text{ord}(a)} = 1$.

Definition 1.25 e.g. \mathbb{F}_5 . $a = 2$. $\begin{array}{l} a^1 = 2 \\ a^2 = 4 \\ a^3 = 3 \\ a^4 = 1 \end{array} \Rightarrow \text{ord}(a) = 4.$

The **order** of $a \in \mathbb{F}$ ($\text{ord}(a)$) is the smallest t s.t. $a^t = 1$.

An element of order $q - 1$ is called a **primitive element** of \mathbb{F}_q .
 $\begin{array}{l} a^1 = 1 \\ a^2 = 4 \\ a^3 = 3 \\ a^4 = 1 \end{array} \Rightarrow \text{ord}(a) = 4.$

primitive element: order = $(q-1)$ (not unique)

Example 1.26

$$\boxed{\alpha^{q-1} = 1}$$

Consider the field $\mathbb{F}_2[x]/x^4 + x + 1$ in Example 1.20.

It can be verified that

$$\text{ord}(x) = \text{ord}(x^2) = \text{ord}(x^4) = 15.$$

Hence x , x^2 , and x^4 are primitive elements (Primitive element is **not unique**).

It can also be verified that $\text{ord}(x^3) = 5$. Hence x^3 is not a primitive element.

Represent a Field by a Primitive Element

Let α be a primitive element. Since $\alpha^0 = 1, \alpha, \dots, \alpha^{q-2}$ are distinct,
 $\mathbb{F} = \{0, 1, \alpha, \dots, \alpha^{q-2}\}$. *: remove $\{\alpha\}$

- Standard notation: $\mathbb{F}^* = \mathbb{F} \setminus \{0\} = \{\alpha^0, \dots, \alpha^{q-2}\}$. $(q-1)$ elements
 $\alpha^{q-1} = \alpha^0 = 1$

Why primitive elements? Recall Example 1.21

- Calculate multiplication:
 - $(x^3 + x^2)(x^3 + x^2 + 1) = ?$
 - $\alpha^6 \cdot \alpha^{13} = \alpha^{19} = \alpha^{15+4} = \alpha^4 = x + 1.$
- Find inverse:
 - $(x^3 + x^2)^{-1} = ?; (x^3 + x^2 + 1)^{-1} = ?$
 - Note that $\alpha^{q-1} = 1 = \alpha^0$. The multiplicative inverse of $\alpha^a = \alpha^{q-1-a}$.
 $\alpha^{-6} = \alpha^{15-6} = \alpha^9 = x^3 + x; \alpha^{-13} = x^2.$

Existence of Primitive Elements

Theorem 1.27

Every finite field \mathbb{F}_q contains a primitive element.

To prove this theorem, we need several lemmas. After presenting and proving these lemmas, we shall prove the theorem.

Lemma 1: Fermat's Little Theorem



Theorem 1.28 (Fermat's Little Theorem)

For every $\beta \in \mathbb{F}_q^*$, we have $\beta^{q-1} = 1$.

Or equivalently, $\forall \beta \in \mathbb{F}_q$, it holds that $\beta^q = \beta$.

e.g.: \mathbb{F}_3^*

$$1^2 = 1$$

$$2^2 = (4) \equiv 1$$

$$1^4 = 1$$

$$2^4 = (16) \equiv 1$$

$$3^4 = (81) \equiv 1$$

$$4^4 = (256) \equiv 1$$

History (from Wikipedia):

Pierre de Fermat first stated the theorem in a letter dated October 18, 1640, to his friend and confidant Frénicle de Bessy.

Fermat did not prove his assertion, only stating: "... , the proof of which I would send to you, if I were not afraid to be too long."

Euler provided the first published proof in 1736, but Leibniz had given virtually the same proof in an unpublished manuscript from sometime before 1683.

(The same proof technique will be used to prove Euler's Theorem.)

Proof of Fermat's Little Theorem

$$\begin{cases} \beta \neq 0 \\ \beta \neq 0 \end{cases} \Rightarrow \beta \cdot \beta \neq 0$$

Proof: For any $\beta \in \mathbb{F}_q^*$, define $\beta\mathbb{F}_q^* = \{\beta\beta_1, \dots, \beta\beta_{q-1}\}$. *new set by $\beta \cdot \beta_i$ is a subset, since \mathbb{F}_q^* is closed on multiplication.*

► $\beta\beta_i \neq 0 \Rightarrow \beta\mathbb{F}_q^* \subseteq \mathbb{F}_q^*$. *exist*

Otherwise $\beta_i = \beta^{-1}\beta\beta_i = \beta^{q-1} \cdot 0 = 0$. A contradiction.

► $\beta\beta_i \neq \beta\beta_j$ for $i \neq j$. $\beta_i = \beta^{-1}(\beta\beta_i) \neq 0 \Rightarrow \beta\beta_i \neq 0$. *(subset. # same)*

Otherwise $\beta_i = \beta^{-1}(\beta\beta_i) = \beta^{-1}(\beta\beta_j) \neq \beta^{-1}(\beta\beta_j) = \beta_j \Rightarrow \beta\beta_i + \beta\beta_j$. *(unique)*

Hence, $\mathbb{F}_q^* = \beta\mathbb{F}_q^*$.

Therefore, $\prod_{\gamma \in \mathbb{F}_q^*} \gamma = \prod_{\gamma \in \beta\mathbb{F}_q^*} \gamma$. $\therefore \beta_1 \beta_2 \cdots \beta_{q-1} = (\beta\beta_1)(\beta\beta_2) \cdots (\beta\beta_{q-1})$

That is,

$$\begin{aligned} & \beta_1 \cdot \beta_2 \cdots \beta_{q-1} \quad \therefore \boxed{\underbrace{\beta^{q-1}}_{=1}} \\ & = (\beta\beta_1) \cdot (\beta\beta_2) \cdots (\beta\beta_{q-1}) \\ & = \beta^{q-1} \cdot (\beta_1 \cdot \beta_2 \cdots \beta_{q-1}). \end{aligned}$$

We conclude $\beta^{q-1} = 1$.



Examples Related to Fermat's Little Theorem

$$\mathbb{F} = \mathbb{F}_5 : \quad 1 \cdot \mathbb{F}^* = \{1, 2, 3, 4\} \quad 2 \cdot \mathbb{F}^* = \{2, 4, 1, 3\}$$
$$3 \cdot \mathbb{F}^* = \{3, 1, 4, 2\} \quad 4 \cdot \mathbb{F}^* = \{4, 3, 2, 1\}$$

Example 1.29

Let $\mathbb{F} = \mathbb{F}_5$. Find \mathbb{F}^* and $\beta \cdot \mathbb{F}^*$ for all $\beta \in \mathbb{F}^*$.

$$\begin{array}{ll} \mathbb{F}^* = 1 \cdot \mathbb{F}^* = \{1, 2, 3, 4\} & 2 \cdot \mathbb{F}^* = \{2, 4, 1, 3\} \\ 3 \cdot \mathbb{F}^* = \{3, 1, 4, 2\} & 4 \cdot \mathbb{F}^* = \{4, 3, 2, 1\} \end{array}$$

$$\mathbb{F} = \mathbb{F}_5[x]/(x^2 + x + 1)$$

x^0	x^1
x^2	x^3
x^4	x^5

$$\mathbb{F} = \mathbb{F}_5[x]/(x^2 + x + 1) \quad 1 \cdot \mathbb{F} = \{1, x, x+1\}$$

$$\mathbb{F} = \mathbb{F}_5[x]/(x^2 + x + 1) \quad x \cdot \mathbb{F} = \{x, (x^2) \rightarrow x+1, (x^2+x) \rightarrow 1\}$$

$$(x+1) \cdot \mathbb{F} = \{x+1, (x^2+x) \rightarrow 1, (x^2+2x+1) \rightarrow x\}$$

Let $\mathbb{F} = \mathbb{F}_2[x] / (x^2 + x + 1)$. Find \mathbb{F}^* and $\beta \cdot \mathbb{F}^*$ for all $\beta \in \mathbb{F}^*$.

$$\mathbb{F}^* = 1 \cdot \mathbb{F}^* = \{1, x, x+1\}$$

$$x \cdot \mathbb{F}^* = \{x, x+1, 1\}$$

$$(x+1) \cdot \mathbb{F}^* = \{x+1, 1, x\}$$

Existence of Primitive Elements: Lemma 2

Suppose $t = ka + b$, $a = \text{ord}(\beta)$.

$$\beta^t = \beta^{ka+b} = \beta^b = 1 \text{ holds for } 0 < b < a.$$

Contradict with a is the smallest $\beta^a = 1$.

$$\therefore t = ka \Rightarrow \text{ord}(\beta) | t.$$

Lemma 1.31

For any $\beta \in \mathbb{F}^*$, if $\underbrace{\beta^t = 1}$ for some $t \in \mathbb{Z}^+$, then $\underbrace{\text{ord}(\beta)} | t$.

Proof: Let $a = \text{ord}(\beta)$ & $t = ka + b$ where $0 < b < a$.

Then $\beta^t = \beta^b = 1$.

Contradict with that a is the smallest number that $\beta^a = 1$. \diamond

$$\therefore \beta^{q-1} = 1 \quad \therefore \text{ord}(\beta) | q-1$$

Corollary 1.32

$\forall \beta \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, it holds that $\text{ord}(\beta) | q - 1$.

Proof: This is proved by Fermat's little theorem (Theorem 1.28) and Lemma 1.31.

Existence of Primitive Elements: Lemma 3

Lemma 1.33

$$\beta_1^{r_1} \equiv 1 \quad \beta_2^{r_2} \equiv 1$$

Suppose that $\text{ord}(\beta_1) = r_1$, $\text{ord}(\beta_2) = r_2$, and $\gcd(r_1, r_2) = 1$. Let $r = \text{ord}(\beta_1\beta_2)$. Then $r = r_1r_2$.

Proof: $\beta_1^{r_1} \equiv 1 \Rightarrow \beta_1^{rr_2} \equiv 1, \beta_2^{r_2} \equiv 1 \Rightarrow \beta_2^{rr_1} \equiv 1 \Rightarrow \beta_1^{rr_2}\beta_2^{rr_1} = \beta_1^{rr_1} \equiv 1$

1. Since $(\beta_1\beta_2)^{r_1r_2} = 1$, it holds $r|r_1r_2$ by Lemma 1.31. $\Rightarrow r|r, r_2$.
2. $r_1r_2|r: \beta^{rr_2} \equiv 1 \Rightarrow \beta^{rrr_1} = (\beta_1\beta_2)^{rr_1} = (\beta_1^{r_1})^r \beta_2^{rr_1} = \beta_2^{rr_1} \Rightarrow r_2|rr_1$
 $1 = (\beta_1\beta_2)^{rr_1} = (\beta_1^{r_1})^r \beta_2^{rr_1} = \beta_2^{rr_1}$. Then $r_2|rr_1$. Then $r_2|r$.
Similarly, $r_1|r$.

Hence $\text{lcm}(r_1, r_2)|r$ or equivalently $r_1r_2|r$.

3. That $r|r_1r_2$ and $r_1r_2|r$ implies $r = r_1r_2$.

$$\because \gcd(r_1, r_2) = 1$$

$$\therefore r_1|r$$

$$\text{Similarly } r_2|r$$

$$\therefore r|r_1r_2$$

$$\therefore r = r_1r_2$$

◇

An Example Related to Lemmas 2 & 3

Consider $\mathbb{F} = \mathbb{F}_7$.

$$\mathbb{F}^* = \{1, 2, 3, 4, 5, 6\}^{q-1}$$

$$\text{ord}(\beta) | q-1$$

$$\text{ord}(1) = 1 \quad \text{always hold}$$

$$\text{ord}(3) = 6$$

$$\text{ord}(5) = 6$$

$$\text{ord}(2) = 3$$

$$\text{ord}(4) = 3$$

$$\text{ord}(6) = 2$$

You may check the above results with Corollary 1.32.

Note that $\text{ord}(2) = 3$ and $\text{ord}(6) = 2$.

Fact 1.33 implies that $\text{ord}(2 \cdot 6) = 3 \times 2 = 6 = \text{ord}(5)$.

Existence of Primitive Elements: the Proof

Proof of Theorem 1.27 (the existence):

Let $\mathbb{F}_q^* = \{\alpha_1, \dots, \alpha_{q-1}\}$ and $r_i = \text{ord}(\alpha_i)$.

Define $m := \text{lcm}(r_1, \dots, r_{q-1})$. Based on the unique factorisation theorem (Theorem 1.8), m can be written as $m = p_1^{k_1} \cdots p_\ell^{k_\ell}$.

$\exists \alpha_i \in \mathbb{F}_q^*$ s.t. $p_1^{k_1} \mid \text{ord}(\alpha_i)$:

$$k_1 = \max \left(k_1^{(1)}, \dots, k_1^{(i)}, \dots, k_1^{(q-1)} \right) \text{ from Example 1.9.}$$

Let $\beta_1 = \alpha_i^{\text{ord}(\alpha_i)/p_1^{k_1}}$, then $\text{ord}(\beta_1) = p_1^{k_1}$.

Similarly, find $\beta_2, \dots, \beta_\ell$.

(since β_i 's are coprime)

Let $\beta = \beta_1 \cdots \beta_\ell$. Clearly, $\text{ord}(\beta) = m$ (Lemma 1.33).

Hence, $m \mid (q-1)$ (Corollary 1.32) or $m \leq q-1$.

On the other hand, all $q-1$ elements in \mathbb{F}_q^* are roots of $x^m - 1$. Therefore $m \geq q-1$.

It then can be concluded that $m = q-1$ and β is a primitive element. ◇

Uniqueness of Finite Fields

Definition 1.34

Two fields \mathbb{F} and \mathbb{G} are **isomorphic** if there exists a **one-to-one mapping** $\varphi : \mathbb{F} \rightarrow \mathbb{G}$ that satisfies

$$\varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(a+b) = \varphi(a) + \varphi(b).$$

Theorem 1.35

The finite field \mathbb{F}_q is unique up to isomorphism.

Proof is not required. *actual polynomial to create \mathbb{F}_q is not important as long as dimension is fixed.*

Example: $\mathbb{F}_2[x] / (x^3 + x + 1)$ and $\mathbb{F}_2[x] / (x^3 + x^2 + 1)$ are isomorphic.

Example

$$\varphi(x^4 + 1) \cdot x^5 = \varphi(x^4 + x^5) = \varphi(x^4 + x + 1 + x^5) = \varphi(x + 1) = x + 1$$

$$\varphi : \mathbb{F}_2[x] / (x^3 + x^2 + 1) \rightarrow \mathbb{F}_2[y] / (y^3 + y + 1)$$

$$x \mapsto \varphi(x) = y + 1$$

$\varphi :$	$\mathbb{F}_2[x] / (x^3 + x^2 + 1)$	$\mathbb{F}_2[y] = y^3 + y + 1$
0	0	0
1	1	1
x	x	$y + 1$
x^2	x^2	$y^2 + 1$
x^3	$x^2 + 1$	y^2
x^4	$x^2 + x + 1$	$y^2 + y + 1$
x^5	$x + 1$	y
x^6	$x^2 + x$	$y^2 + y$

Verify $\varphi(ab) = \varphi(a)\varphi(b)$:

$$\varphi(x^2 \cdot (x + 1)) = \varphi(x^3 + x^2) = \varphi(x^2 + 1 + x^2) = \varphi(1) = 1.$$

$$\varphi(x^2)\varphi(x + 1) = (y^2 + 1) \cdot y = y^3 + y = y + 1 + y = 1.$$

Polynomial Factorisation

Problem: factorise the polynomial $x^{q^m-1} - 1$.

Be **careful** about the concept of "irreducible polynomial":

Have to **specify the field** we are considering.

Example 1.36

Consider a polynomial $M(x) = x^2 + 1$.

1. $M(x)$ is irreducible w.r.t. \mathbb{R} .
2. $M(x)$ is reducible w.r.t. \mathbb{C} : $M(x) = (x + j)(x - j)$.

Consider a polynomial $M(x) = x^2 + x + 1$.

1. $M(x)$ is irreducible w.r.t. \mathbb{F}_2 .
2. $M(x)$ is reducible w.r.t. $\mathbb{F}_4 = \mathbb{F}_2[y]/y^2 + y + 1$
 - ▶ $\mathbb{F}_4 = \{0, 1, y, y + 1\}$.
 - ▶ $M(x) = (x - y)(x - (y + 1)) = x^2 - (y + y + 1)x + y(y + 1)$.

A Preview of the Final Result

- ▶ Let α be a primitive element of \mathbb{F}_{q^m} . (\mathbb{F}_{q^m} is well defined?)
 $x^{q^m-1} - 1 = \prod_{i=0}^{q^m-2} (x - \alpha^i)$. (Irreducible polynomials in $\mathbb{F}_{q^m}[x]$)
- ▶ $x^{q^m-1} - 1 = \prod_{k=1}^s M^{(k)}(x)$. (Irreducible polynomials in $\mathbb{F}_q[x]$)

Example 1.37

Want to factorise $x^3 - 1 \in \mathbb{F}_2[x]$.

Let α be a primitive element of $\mathbb{F}_4 = \mathbb{F}_2[y]/y^2 + y + 1$.

That is, $\mathbb{F}_4^* = \{1, \alpha, \alpha^2\} = \{1, y, y+1\}$.

$$\begin{aligned}x^3 - 1 &= (x - 1)(x - \alpha)(x - \alpha^2) \\&= (x - 1)(x - y)(x - (y + 1)) \\&= (x - 1)(x^2 + x + 1).\end{aligned}$$

Both $x - 1$ and $x^2 + x + 1$ are irreducible polynomial in $\mathbb{F}_2[x]$.

A factorisation of $x^3 - 1$ in terms of irreducible polynomials in $\mathbb{F}_2[x]$.

Next introduce **minimal polynomials** $M^{(k)}(x)$ for factorisation.

Minimal Polynomials

Definition 1.38

A **minimal polynomial** of $\beta \in \mathbb{F}_{q^m}$ w.r.t. \mathbb{F}_q is a nonzero monic polynomial $M(x) \in \mathbb{F}_q[x]$ of **the least degree** s.t. $M(\beta) = 0$.

Minimal Polynomials: Examples

Example 1.39

The minimal polynomial of $i := \sqrt{-1} \in \mathbb{C}$ in $\mathbb{R}[x]$ is $x^2 + 1$.

Example 1.40

Consider $\mathbb{F}_4 = \mathbb{F}_2[y]/y^2 + y + 1 = \{0, 1, y, y + 1\}$.

Find minimal polynomials of $\beta \in \mathbb{F}_4$ in $\mathbb{F}_2[x]$.

- ▶ $\beta = 0$: the constant poly. $M(x) = 0$.
- ▶ $\beta = 1$: $M(x) = x + 1$.
- ▶ $\beta = y$: $M(x) = x^2 + x + 1$.

There are two possible polynomials of degree one in $\mathbb{F}_2[x]$: $f_1(x) = x$ and $f_2(x) = x + 1$. It is easy to verify that $f_1(y) \neq 0$ and $f_2(y) \neq 0$.

Try polynomials of degree two in $\mathbb{F}_2[x]$. As $M(y) = 0$, $M(x)$ is the minimal polynomial.

- ▶ $\beta = y + 1$: $M(x) = x^2 + x + 1$.

Minimal Polynomials: Properties

Theorem 1.41

1. *The minimal polynomial of $\beta \in \mathbb{F}_{q^m}$ in $\mathbb{F}_q[x]$ is unique.*
2. *A polynomial $M(x) \in \mathbb{F}_q[x]$ is the minimal polynomial of $\beta \in \mathbb{F}_{q^m}$ iff $M(x)$ is irreducible and $M(\beta) = 0$.*

Proof of Part I:

Suppose that both $M_1(x) \neq M_2(x)$ are minimal polynomials.

Then $M_1(x) = q(x)M_2(x) + r(x)$ for some r s.t. $\deg(r) < \deg(M_2)$.

Since $r(\beta) = M_1(\beta) - q(\beta)M_2(\beta) = 0$ and $\deg(r) < \deg(M_2)$,

by the definition of minimal polynomial $r(x) = 0$.

Hence, $q(x) = c$ and $M_1(x) = M_2(x)$.

Proof (Continued)

Part II “only if” part:

Let $M(x)$ be the minimal polynomial of β . Then $M(\beta) = 0$ obviously.

Suppose that $M(x)$ is not irreducible.

Then $M(x) = h(x)f(x)$ with $\deg(h), \deg(f) < \deg(M)$.

$M(\beta) = 0$ implies either $h(\beta) = 0$ or $f(\beta) = 0$.

Contradicts that $M(x)$ is the minimal polynomial.

Part II “if” part:

Let $M(\beta) = 0$ and $M(x)$ is irreducible.

Suppose that $M(x)$ is not the minimal polynomial of β .

Let $f(x)$ be the minimal polynomial.

Write $M(x) = q(x)f(x) + r(x)$ where $\deg(r) < \deg(f)$.

Since $r(\beta) = 0$ and $f(x)$ is minimal, one has $r(x) = 0$.

Contradicts with that $M(x)$ is irreducible.



Construction of Minimal Polynomials

Theorem 1.42

Let α be a primitive element of \mathbb{F}_{q^m} . The minimal polynomial of α^i in $\mathbb{F}_q[x]$ is

$$M^{(i)}(x) = \prod_{j \in \mathcal{C}_i} (x - \alpha^j),$$

where \mathcal{C}_i is the **cyclotomic coset** of q modulo $q^m - 1$ containing i .

Definition 1.43 (Cyclotomic Coset)

The cyclotomic coset of q modulo $n = q^m - 1$ containing i is

$$\mathcal{C}_i = \{i \cdot q^j \bmod n : j = 0, 1, 2, \dots\} \subset \mathbb{Z}_n$$

Example 1.44

Cyclotomic cosets of $2 \bmod 15 (= 2^4 - 1)$ are

$$\mathcal{C}_0 = \{0\}, \mathcal{C}_1 = \{1, 2, 4, 8\}, \mathcal{C}_3 = \{3, 6, 12, 9\}, \mathcal{C}_5 = \{5, 10\}, \mathcal{C}_7 = \{7, 14, 13, 11\}.$$

An Example of Minimal Polynomials

Consider the field $\mathbb{F}_4 = \mathbb{F}_2[y]/y^2 + y + 1 = \{0, 1, y, y + 1\}$.
Find the minimal poly. of $y + 1 \in \mathbb{F}_4$ in $\mathbb{F}_2[x]$.

- ▶ Cyclotomic cosets of 2 modulo $(2^2 - 1 = 3)$:
 - ▶ $\mathcal{C}_0 = \{0\}$, $\mathcal{C}_1 = \{1, 2\}$.
- ▶ y is primitive: $y \neq 1$, $y^2 = y + 1 \neq 1$, $y^3 = y^2 + y = 1$.
- ▶ Theorem 1.42 claims
$$M^{(1)}(x) = (x - y)(x - y^2) = x^2 + x + 1$$
is the minimal poly. of $y + 1$ in $\mathbb{F}_2[x]$.

Cyclotomic Coset: Properties (1)

Lemma 1.45

Let \mathcal{C}_i be the cyclotomic coset of q modulo $q^m - 1$ containing i . Define $q\mathcal{C}_i := \{qj \bmod q^m - 1 : j \in \mathcal{C}_i\}$. Then $q\mathcal{C}_i = \mathcal{C}_i$.

Proof: Define $r := |\mathcal{C}_i|$. Write $\mathcal{C}_i = \{i, iq, \dots, iq^{r-1} \pmod{q^m - 1}\}$. To show $q\mathcal{C}_i = \mathcal{C}_i$, it suffices to show $iq^r \equiv i \pmod{q^m - 1}$.

By definition of cyclotomic coset, $iq^r \pmod{q^m - 1} \in \mathcal{C}_i$. Suppose $iq^r = iq^\ell \pmod{q^m - 1}$ with $1 \leq \ell \leq r - 1$. Then

$iq^{r-\ell} = i \pmod{q^m - 1}$ and $|\mathcal{C}_i| \leq r - \ell < r$. This contradicts with $|\mathcal{C}_i| = r$. \diamond

$$i \cdot q^m \equiv i \pmod{q^m - 1}$$

Cyclotomic Coset: Properties (2)

Corollary 1.46

Let α be a primitive element of \mathbb{F}_{q^m} . Then

$$M^{(i)}(x) = \prod_{j \in \mathcal{C}_i} (x - \alpha^j) = \prod_{j \in \mathcal{C}_i} (x - \alpha^{jq}).$$

Proof: By Fermat's little theorem (Theorem 1.28) $\alpha^{q^m-1} = 1$.
$$\prod_{j \in \mathcal{C}_i} (x - \alpha^{jq}) = \prod_{\ell \in q\mathcal{C}_i} (x - \alpha^\ell) = \prod_{j \in \mathcal{C}_i} (x - \alpha^j).$$



Proof Sketch of Theorem 1.42

Proof Sketch:

- ▶ $M^{(i)}(x) \in \mathbb{F}_q[x]$
 - ▶ $M^{(i)}(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0$ where $a_i \in \mathbb{F}_q$.
- ▶ $M^{(i)}(x)$ is “minimal”.

Lemma 1.47

Every \mathbb{F}_{q^m} contains a sub-field \mathbb{F}_q . For any $\beta \in \mathbb{F}_{q^m}$, $\beta \in \mathbb{F}_q$ iff $\beta^q = \beta$.

Proof: \Rightarrow : If $\beta \in \mathbb{F}_q$, by Fermat's little theorem (Theorem 1.28) $\beta^q = \beta$.

\Leftarrow : The polynomial $x^q - x$ has at most q distinct roots in \mathbb{F}_{q^m} . As all elements in \mathbb{F}_q are roots of $x^q - x$ and $|\mathbb{F}_q| = q$, it holds

$$\mathbb{F}_q = \{\text{all roots of } x^q - x \text{ in } \mathbb{F}_{q^m}\}.$$



A Useful Lemma

Lemma 1.48

Let p be the characteristic of \mathbb{F}_q . It holds that $(x + y)^p = x^p + y^p$.

Proof: $(x + y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i}$.

Clearly $\binom{p}{0} = \binom{p}{p} = 1$.

For any $1 \leq i \leq p - 1$, $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{i!} \in \mathbb{Z}^+$.

Note that $\gcd(i!, p) = 1$ but $\binom{p}{i} \in \mathbb{Z}^+$. By Euclid's Lemma (Theorem 1.11), $i! \mid (p-1)\cdots(p-i+1)$ and $\binom{p}{i} = p \cdot s$ for some $s \in \mathbb{Z}^+$.

By the definition of the characteristic, $\binom{p}{i} = 0$, $\forall 1 \leq i \leq p - 1$. \diamond

Corollary 1.49

On the field \mathbb{F}_{q^m} , $(x + y)^q = x^q + y^q$.

$$M^{(i)}(x) \in \mathbb{F}_q[x]$$

Let $r = |\mathcal{C}_i|$. Write

$$\begin{aligned} M^{(i)}(x) &= \sum_{\ell} a_{\ell} x^{\ell} = \prod_{j \in \mathcal{C}_i} (x - \alpha^j) \\ &\stackrel{(a)}{=} \sum_{\ell} \left(\sum_{j_1, \dots, j_{r-\ell}} \alpha^{j_1} \cdots \alpha^{j_{r-\ell}} \right) x^{\ell}, \end{aligned}$$

where (a) comes from the expansion of $\prod_{j \in \mathcal{C}_i} (x - \alpha^j)$. At the same time,

$$\begin{aligned} M^{(i)}(x) &= \prod_{j \in \mathcal{C}_i} (x - \alpha^j) \stackrel{(a)}{=} \prod_{j \in \mathcal{C}_i} (x - \alpha^{jq}) \\ &= \sum_{\ell} \left(\sum_{j_1, \dots, j_{r-\ell}} \alpha^{j_1 q} \cdots \alpha^{j_{r-\ell} q} \right) x^{\ell} \\ &\stackrel{(b)}{=} \sum_{\ell} \left(\sum_{j_1, \dots, j_{r-\ell}} \alpha^{j_1} \cdots \alpha^{j_{r-\ell}} \right)^q x^{\ell} \\ &= \sum_{\ell} a_{\ell}^q x^{\ell}, \end{aligned}$$

where (a) comes from Corollary 1.46, (b) comes from Corollary 1.49.
Hence, $a_{\ell} = a_{\ell}^q$, which implies $a_{\ell} \in \mathbb{F}_q$ and $M^{(i)}(x) \in \mathbb{F}_q[x]$. \diamond

$M^{(i)}(x)$ is “minimal”

Step 1: The roots of $M^{(i)}(x)$ in \mathbb{F}_{q^m} are α^j , $j \in C_i$. As α is primitive, $\alpha^j \neq \alpha^k$ for $j \neq k$. The roots are distinctive.

Step 2: Let $f(x) \in \mathbb{F}_q[x]$ and $f(\alpha^i) = 0$. We shall show $M^{(i)}(x) | f(x)$. Write $f(x) = f_0 + f_1x + \dots + f_nx^n$. For any $j \in C_i$, $\exists \ell$ s.t. $j = iq^\ell \pmod{q^m - 1}$.

$$\begin{aligned}f(\alpha^j) &= f(\alpha^{iq^\ell}) = f_0 + f_1\alpha^{iq^\ell} + \dots + f_n\alpha^{iq^\ell \cdot n} \\&= f_0^{q^\ell} + f_1^{q^\ell}\alpha^{iq^\ell} + \dots + f_n^{q^\ell}\alpha^{iq^\ell \cdot n} \\&= (f_0 + f_1\alpha^i + \dots + f_n\alpha^{in})^{q^\ell} = f(\alpha^i)^{q^\ell} = 0,\end{aligned}$$

i.e., α^j is also a root of f . Hence, $M^{(i)}(x) | f(x)$.

As this holds for all $f(x)$ s.t. $f(\alpha^i) = 0$, $M^{(i)}(x)$ is the minimal polynomial. ◇

Representatives of Cyclotomic Cosets

Definition 1.50

Consider the cyclotomic cosets of $q \bmod n$.

A subset $\{i_1, \dots, i_j\} \subset \mathbb{Z}_n$ is a **complete set of representatives** of cyclotomic cosets if

$$C_{i_1} \cup \dots \cup C_{i_j} = \mathbb{Z}_n.$$

Example 1.51

Cyclotomic cosets of $2 \bmod 15$ are

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}, C_3 = \{3, 6, 12, 9\}, C_5 = \{5, 10\}, C_7 = \{7, 14, 13, 11\}.$$

The complete set of representatives is $\{0, 1, 3, 5, 7\}$.

Factorisation

Theorem 1.52

Let α be a primitive element of \mathbb{F}_{q^m} . Let $\{i_1, \dots, i_s\}$ be a complete set of representatives of cyclotomic cosets of q modulo $q^m - 1$. Then

$$x^{q^m-1} - 1 = \prod_{i=0}^{q^m-2} (x - \alpha^i) = \prod_{k=1}^s M^{(i_k)}(x).$$

Proof:

The first equality: The degrees are the same. The coefficients before x^{q^m-1} are the same. The roots are also the same.

The second equality: holds from the definitions of $M^{(i_k)}(x)$ and the complete set of representatives. ◇

Section 2

Cryptography

- ▶ Introduction
- ▶ Password management: store, exchange, and secret share
- ▶ The public key cryptography
 - ▶ The RSA cryptosystem
 - ▶ The ElGamal cryptosystem
- ▶ Digital signature

The contents are heavily based on Biggs' book, Chapters 13 & 14.

Cryptography

Definition 2.1 (Cryptography)

A framework of cryptography includes a set of plaintext messages \mathcal{M} , a set of ciphertext messages \mathcal{C} , and a set of keys \mathcal{K} . For each $k \in \mathcal{K}$, there is an encryption function $E_k : \mathcal{M} \rightarrow \mathcal{C}$ and the corresponding decryption function $D_\ell : \mathcal{C} \rightarrow \mathcal{M}$ such that

$$D_\ell(E_k(m)) = m, \text{ for all } m \in \mathcal{M}.$$

Cryptography: An Example

One of the oldest cryptographic systems is said to have been used by Julius Caesar over two thousand years ago.

Let \mathcal{A} be the English alphabet set. Let $\mathcal{K} = \{1, 2, \dots, 25\}$. For a given key $k \in \mathcal{K}$, replace each letter by the one that is k places later.

For example, if $k = 5$, then the message

SEE \sqcup YOU \sqcup TOMORROW becomes XJJ \sqcup DTZ \sqcup YTRTWWTB

For the Caesar system, a simple attack is exhaustive search as there are only 25 keys.
shift 1 ~ shift 25.

A natural extension is to use any permutation of 26 letters, yielding $26! \approx 10^{27}$ keys. Exhaustive search is impossible.

$\begin{matrix} A & \xrightarrow{\hspace{1cm}} & B \\ \downarrow & & \downarrow \\ A-2 & & A-1 \\ 26 & & 25 \end{matrix}$

However, in this case another method, called *frequency analysis*, is a much more effective attack.

It uses the observation that the frequencies of the English letters are fairly constant over a wide range of texts.

Another Example: Hill's Cryptography System

Consider a 29-symbol alphabet including 26 English letters, the space \sqcup , comma, and full stop. It is mapped to \mathbb{F}_{29} .

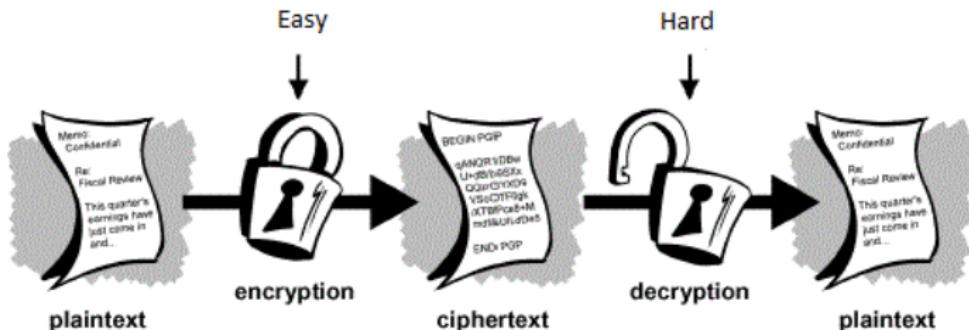
Given a stream of symbols, split it into blocks of size n so that each block can be written as $\mathbf{m} \in \mathbb{F}_{29}^n$. A key $\mathbf{K} \in \mathbb{F}_{29}^{n \times n}$ is an invertible matrix. The encryption function is given by

$$\mathbf{c} = \mathbf{K}\mathbf{m},$$

and the decryption function is

$$\mathbf{m} = \mathbf{K}^{-1}\mathbf{c}.$$

Diagram of Cryptography Systems



Adapted from http://www.akadia.com/services/email_security.html

- ▶ Popular cryptography systems are built on large prime numbers.
- ▶ Symmetric cryptography: encryption key $k =$ decryption key ℓ .
- ▶ Asymmetric cryptography: $k \neq \ell$.

Existence of Large Prime Numbers

Theorem: There exist infinitely many prime numbers.

Proof:

1. Suppose that there exist only finitely many prime numbers.
2. List all these prime numbers, p_1, p_2, \dots, p_N . \triangle any smaller prime cannot divide x :
 $(p_i \nmid x)$
3. Let $x = p_1 \cdot p_2 \cdots p_N + 1$. $\text{gcd}(p_i, x) = 1$
4. Claim: x is a prime number. $\Rightarrow x \equiv 1 \pmod{p_i} \therefore x$ can be expressed by Π prime Proved by the Unique Factorisation Theorem 1.8 as $\text{gcd}(p_i, x) = 1$.
5. This contradicts the assumption that the list of p_1, p_2, \dots, p_N contains all the prime numbers. $\therefore x$ is prime. ◇

$$30 = \overbrace{2 \times 3 \times 5}^{\text{smaller}}$$

Large Prime Numbers

A list of large prime numbers (<http://primes.utm.edu>)

Prime	When	Prime	When	Prime	When
$2^{57885161} - 1$	2013	$2^{43112609} - 1$	2008	$2^{42643801} - 1$	2009
$2^{37156667} - 1$	2008	$2^{32582657} - 1$	2006	$2^{30402457} - 1$	2005

Large prime numbers matter:

To check whether a 64bit number is a prime or not by brute force,
how long will it take?

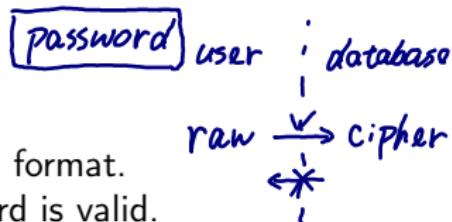
Assume a computer can evaluate 1G (10^9) "basic operations" per second.

$$2^{64}/(10^9 \cdot 3600 \cdot 24 \cdot 365) \approx 585 \text{ years!}$$

Nowadays, a prime number between 512b and 1024b is often used.
Any brute force method is impractical!

How to Store Passwords on a Server?

- ▶ A set of users wish to log in securely to a server.
- ▶ Each user choose a password.
- ▶ The passwords are stored in a file
 - ▶ Should not be saved in the 'raw' format.
 - ▶ Easy to check whether a password is valid.
 - ▶ Very difficult to extract the passwords from the file.



Solution: use the discrete logarithmic function.

The Discrete Logarithm

Normal exponential function:

$$x \mapsto y = b^x,$$

Normal logarithmic function:

$$y \mapsto x = \log_b y.$$

It can be solved by Taylor expansion **efficiently**.

e.g. $3^{29} \pmod{17}$ easy $\rightarrow [12]$
 $3^{(7)} \pmod{17}$ hard $\leftarrow [12]$
by trials and errors.

Definition 2.2 (Discrete logarithm problem (DLP))

Let p be a prime number and $b \in \mathbb{F}_p^*$ be a primitive element.

For any given $y \in \mathbb{F}_p^*$, find the $x \in \mathbb{F}_p^*$ such that

$$y = b^x \pmod{p}.$$

- generator so that y can go through all possible values in \mathbb{F}_p^* .
► It is well-defined if and only if b is primitive. (y distributes uniformly!)

Computation Complexity

1) write in 2) extremely large

'binary' form

$$3^{211} = 3^{128} \cdot 3^{64} \cdot 3^{16} \cdot 3^2 \cdot 3^1 = 3^{2k} \cdot 3^{2^{k-1}} = 3^{2k+1} \pmod{p}$$

Discrete exponential function: computational complexity $O(\log(p))$

Example: $3^{211} = ? \pmod{811}$ (computable!)

Note that $211 = 128 + 64 + 16 + 2 + 1$.

One has $3^{211} = 3^{128} \cdot 3^{64} \cdot 3^{16} \cdot 3^2 \cdot 3^1 \pmod{811}$.

It can be achieved by computing

$$\begin{aligned}3^2 &= 3 \cdot 3 \pmod{811}, \quad 3^4 = 3^2 \cdot 3^2 \pmod{811}, \\ \dots, \quad 3^{2^k} &= 3^{2^{k-1}} \cdot 3^{2^{k-1}} \pmod{811}.\end{aligned}$$

Discrete logarithmic function: computational complexity $O(p)$.

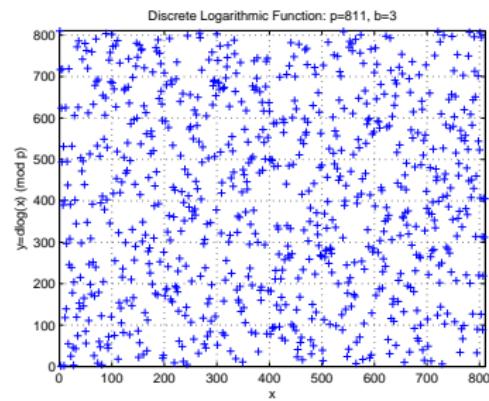
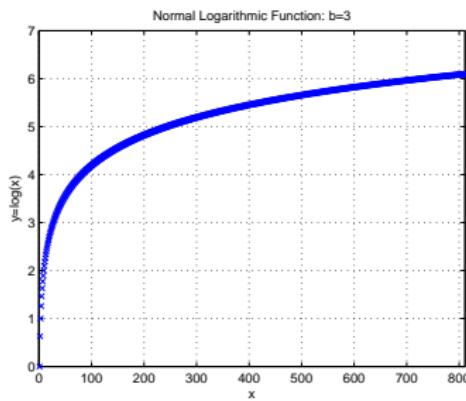
- ▶ It is usually solved by brute force search.
 - ▶ No sufficiently efficient algorithm in general.

Examples

Let $p = 811$ and $b = 3$.

The output of discrete logarithmic function looks random:

$$\log_3 2 = 717; \log_3 3 = 1; \log_3 4 = 624; \log_3 5 = 494; \dots$$



Store Passwords on a Server: A Solution

admin: choose
 a large prime P (open to public)
 a primitive element b

user i :
 1) convert password to number x_i
 2) use discrete exponential algorithm to encrypt:
 $y_i = b^{x_i} \pmod{P}$

- ▶ The administrator chooses a prime p and a primitive element b .
Server: Store (i, y_i) .
 - ▶ The values of p and b are also kept on the server.
- ▶ The user i chooses a password. This is converted into a number $x_i \in \mathbb{F}_p^*$.
- ▶ Let $y_i = b^{x_i} \pmod{p}$ and the pair (i, y_i) is stored.

Cryptography for Information Exchange

In the previous scheme:

Decoding is difficult for everyone.

In the information exchange scenario, for example, Alice sends some message to Bob.

Alice's information to Bob should be encrypted.

Bob would like to be able to decrypt the message **easily**.

The traditional choice: **Symmetric cryptography**

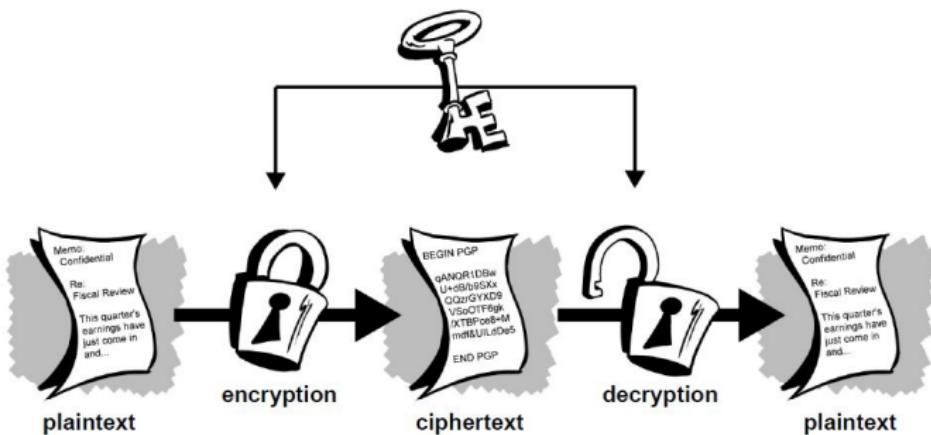
The encryption and decryption keys are the same, i.e., $k = \ell$.

The keys are known to both Alice and Bob for encryption and decryption respectively.

Disadvantages: A secure channel is needed for key exchange.

Disasters may happen if the key is leaked.

Symmetric Key Cryptography



From <http://chriscacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/>

The key is to keep the key safe.

Key Exchange

Problem: Alice and Bob want to share a secret key but their information exchange could be observed by their adversary Eve. How is it possible for Alice and Bob to share a key without making it known to Eve?

Solution: Diffie-Hellman key exchange.

Wikipedia: The scheme was first published by Whitfield Diffie and Martin Hellman in 1976, although it had been separately invented a few years earlier within GCHQ, the British signals intelligence agency, by James H. Ellis, Clifford Cocks and Malcolm J. Williamson but was kept classified.

Diffie-Hellman Key Exchange

1. Alice and Bob agree on a large prime p and an integer $g \bmod p$. The values of p and g are publicly known.
2. Alice picks a secret integer a that she does not reveal to anyone, and Bob picks an integer b that he keeps secret. They compute

$$A = g^a \bmod p, \quad \text{and} \quad B = g^b \bmod p,$$

respectively. They next exchange these computed values.
Note that Eve sees the values of A and B .

3. Alice and Bob uses their secret integers to compute

$$A' = B^a \bmod p, \quad \text{and} \quad B' = A^b \bmod p,$$

$(g^b)^a \bmod p$ $(g^a)^b \bmod p$

respectively. Note that $A' = B' = g^{ab}$ is the shared secret key for information exchange.

Secret Share: Motivation

Secrecy-reliability tradeoff in storing an encryption key

- ▶ Maximum secrecy: keep a single copy of the key in one location
 - ▶ What if it gets lost.
- ▶ Reliability: store multiple copies at different locations
 - ▶ What if a copy falls into the wrong hand.

Secret Sharing: (k, n) threshold scheme.

Store the secret S into n pieces of encrypted words S_1, \dots, S_n such that

- ▶ Knowledge of any K or more S_i pieces makes S easily computable.
- ▶ Knowledge of any $k - 1$ or fewer S_i pieces leaves S undetermined.

Shamir's Secret Sharing

Idea of Adi Shamir's threshold scheme: k points to define a polynomial of degree $k - 1$. 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth.

A (k, n) threshold scheme to share our secret S :

1. Let p be a prime number. Let $n < p$ and $S < p$.
2. Randomly choose $k - 1$ positive integers a_1, \dots, a_{k-1} . Set $\underline{a_0 = S}$.
3. Set $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}$.
4. Evaluate $f(x)$ at n points to obtain $(t_i, f(t_i))$, $t_i \in \mathbb{F}_p^*$ and $i = 1, \dots, n$.

Claim: given any k such pairs $(t_i, f(t_i))$, we can find the coefficients of the polynomial and therefore a_0 .

Finding the Polynomial Coefficients

Polynomial coefficients can be found via

- ▶ Solving the linear system:

$$\begin{bmatrix} f(t_{i_1}) \\ f(t_{i_2}) \\ \vdots \\ f(t_{i_k}) \end{bmatrix} = \begin{bmatrix} 1 & t_{i_1} & \cdots & t_{i_1}^{k-1} \\ 1 & t_{i_2} & \cdots & t_{i_2}^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_{i_k} & \cdots & t_{i_k}^{k-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{bmatrix}.$$

- ▶ Or polynomial interpolation:

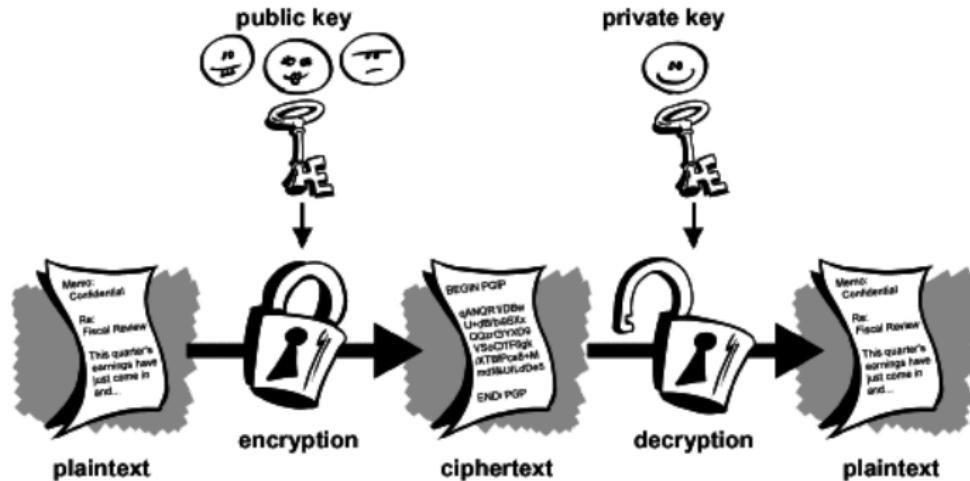
$$f(x) = \sum_{j=1}^k f(t_{i_j}) \prod_{\ell \neq j} \frac{x - t_{i_\ell}}{x_{i_j} - x_{i_\ell}}.$$

Cryptography for Information Exchange (2)

A modern solution: Public key algorithms (Asymmetric Cryptography)

Encryption key $k \neq \ell$ decryption key.

The encryption key is public while the decryption key is kept secret.



From http://www.akadia.com/services/email_security.html

Comparison

Comparisons of asymmetric cryptography over the symmetric one.

Advantages:

- ▶ No secret channel is necessary for the key exchange.
- ▶ Less key-management problems. Only $2n$ keys are needed for n entities to communicate securely with one another (each entity maintains a private key and a public key). In a system based on symmetric ciphers, you would need $\binom{n}{2} = n(n - 1)/2$ secret keys (each pair of entities agrees on a key). *Conversely:*
- ▶ More robust to “brute-force” attack in which all possible keys are attempted.
- ▶ Can provide digital signatures.

Disadvantages:

- ▶ Much slower. The computational complexity of asymmetric cryptography is much larger.

In practice, these two schemes are rarely used exclusively. For example, your browser encrypts a symmetric key using the server's public key.

The ElGamal Cryptography

Key generation:

- ▶ Choose a prime p and a primitive element $b \in \mathbb{F}_p^*$. init: p & b are stored on the server.
- ▶ Private key: choose an integer $a' \in \mathbb{N}$.
- ▶ Public key: $\boxed{a = b^{a'}} \in \mathbb{F}_p^*$. ① public = primitive^{private}

Encryption: Alice transmits her public key a to Bob and keeps the private key a' secret. Bob randomly choose $t \in \mathbb{N}$ and encrypt the message m to

$$\textcircled{2} \text{ msg pair } (\underbrace{\text{primitive}^{\text{random}}}_{1}, \underbrace{\text{msg} \cdot \text{public}^{\text{random}}}_{2})$$

Decryption: Alice can recover m via

$$m = ma^t (b^t)^{-a'} = ma^t a^{-t} \bmod p.$$

$$\textcircled{3} \text{ msg} = \text{msg} \cdot \text{public}^{\text{random}} \cdot [\text{primitive}^{\text{random}}]^{\text{-private}}$$

Advantage: $= \text{msg} \cdot \text{public}^{\text{random}} \cdot [\text{primitive}^{\text{private}}]^{\text{-random}} = \text{msg}$.

The random number t generates a random encryption function.
~~public~~

RSA Cryptography

Euler's func $\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$

$a^{\phi(n)} \equiv 1 \pmod{n}$

$\phi(n) = (p_1-1)(p_2-1)$

① primes p_1, p_2, P_1, P_2 are primes

RSA public key cryptography:

Published in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT

Key generation:

► Choose primes $p_1 \neq p_2$. Let $n = p_1 p_2$ and $t = (p_1 - 1)(p_2 - 1)$.

► Public key: (n, e) where $1 < e < t$ and $\gcd(e, t) = 1$.

$C \equiv m^e \pmod{n}$

$\Rightarrow C \equiv m^{kp_1 p_2} \pmod{n}$

$C^d \equiv (m^e)^{kp_1 p_2 d} \equiv m^{ed} \pmod{n}$

$C^d \equiv m^{ed} \pmod{n}$

Private key: d where $1 < d < t$ and $d \cdot e \pmod{t} = 1$.

Find d by the Euclidean algorithm.

- ② $n = p_1 p_2, \phi(n) = (p_1-1)(p_2-1)$
- ③ $e : e & \phi(n)$ coprime (public)
- ④ $d : d \cdot e \pmod{\phi(n)} = 1$ (private)
- $d \equiv e^{-1} \pmod{\phi(n)}$

Encryption: Bob sends his public key (n, e) to Alice and keeps the private key d secret. Alice encrypts the message m to c via

$$\because de \pmod{\phi(n)} = 1$$

$$\therefore de = h\phi(n) + 1$$

Decryption: Bob can recover m from c via

$$\therefore c \equiv m^{h\phi(n)+1} \pmod{n}$$

$$\therefore c \equiv m^{h\phi(n)} \cdot m \pmod{n}$$

$$\therefore m \equiv m \pmod{n}$$

$$\therefore m^{h\phi(n)+1} = m^{de} = c^d \equiv m \pmod{n}$$

$\therefore K^{ed} - KP_1 - KP_2 = tP_2$

$P_1(K^{ed} - KP_1 - h) = tP_2$

$P_1 t P_2 = P_1 t \frac{t}{P_1} \cdot t = t^2 P_1$

② n, n not coprime: $(KP_1) = KP_1 + tP_1 P_2$

$\therefore n$ is uniquely rep. by $P_1 P_2$

$\therefore m \equiv KP_1 \text{ or } m \equiv KP_2$

$\therefore m^{ed} = m + t^2 n$

Suppose $m = KP_1$, wlog. $\therefore m^{ed} = m \pmod{n}$

$\therefore m \cdot P_2 \text{ coprime.}$

$$\therefore (KP_1)^{\phi(n)} \equiv 1 \pmod{P_2}$$

$$(KP_1)^{P_2-1} \equiv 1 \pmod{P_2}$$

$$[(KP_1)^{P_2-1}]^{h(P_2-1)} \equiv 1 \pmod{P_2}$$

$$(KP_1)^{h\phi(n)} \cdot KP_1 \equiv KP_1 \pmod{P_2}$$

$$\therefore (KP_1)^{ed} \equiv KP_1 \pmod{P_2}$$

$$\therefore (KP_1)^{ed} \equiv KP_1 + tP_2 \pmod{n}$$

An Example

- ▶ Bob chooses $p_1 = 47$ and $p_2 = 59$. *2 primes*
- ▶ $n = 47 \times 59 = 2773$. $t = 46 \times 58 = 2668$. *$n=p_1p_2$ $\phi(n) = (p_1-1)(p_2-1)$*
- ▶ $e = 157$ is a valid public key as $\gcd(e, 2668) = 1$. *$e, \phi(n)$ coprime*
- ▶ Use Euclidean algorithm, $d = 17$. *$ed \equiv 1 \pmod{\phi(n)}$*
- ▶ To send a message $m = 5$, Alice computes the ciphertext
 $c = m^e = 5^{157} = 1044 \pmod{2773}$.
- ▶ Bob deciphers the ciphertext via
$$\hat{m} = c^d = 1044^{17} = 5 \pmod{2773},$$
which is the correct message.

Theory Behind RSA

Recall Fermat's Little Theorem (Thm 1.28): $\forall a \in \mathbb{F}_p^*, a^{p-1} = 1 \pmod{p}$

Theorem 2.3 (Euler's Theorem)

Let $p_1 \neq p_2$ be two prime numbers. Define $n := p_1 p_2$ and

$t := (p_1 - 1)(p_2 - 1)$. Then $\forall a \in \mathbb{Z}^+$,

$$\phi(n) = (p_1 - 1)(p_2 - 1)$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$$a^{kt+1} = a \pmod{n}, \forall k \geq 0$$

The correctness of RSA:

$$(m^e)^d = m^{ed} = m^{qt+1} = m^{qt} \cdot m = m \pmod{n}$$

Proof of Euler's Theorem: A Lemma

With a slight abuse of notation, define $x = y \bmod p$ if $|x - y| = 0 \bmod p$.

Lemma 2.4 $\begin{cases} x \equiv y \pmod{p_1} \\ x \equiv y \pmod{p_2} \end{cases} \quad \begin{aligned} &\because \begin{cases} p_1 \mid p_1 k_1 \\ \gcd(p_1, p_2) = 1 \end{cases} \quad \therefore x - y \equiv p_1 k_1 p_2 \\ &\therefore p_2 \mid k_1 \Rightarrow k_1 = k_3 p_2 \quad \therefore x \equiv y \pmod{p_1 p_2} \\ &\therefore x - y \equiv p_1 k_1 = p_2 k_2 \end{aligned}$

For any two positive integers x and y , if $x = y \bmod p_1$ and $x = y \bmod p_2$, then $x = y \bmod p_1 p_2$.

Proof: Since $x = y \bmod p_1$ and $x = y \bmod p_2$, it is clear that

$x - y = k_1 p_1 = k_2 p_2$ for some integers k_1 and k_2 .

By Euclid's Lemma (Lemma 1.11), $p_2 \mid (p_1 k_1)$ and $\gcd(p_2, p_1) = 1$ imply that $p_2 \mid k_1$, or equivalently $k_1 = k_3 p_2$ for some integer k_3 .

Hence, $x - y = (k_3 p_2) p_1$ and $x \equiv y \bmod p_1 p_2$. \diamond

Proof of Euler's Theorem

Fix an $a \in \{1, 2, \dots, p_1 p_2 - 1\}$.

- ▶ We first show that $a^{de} = a \pmod{p_1}$.

If $p_1 | m$, then it is clear that $a^{de} = a + (a^{de} - 1) a = a \pmod{p_1}$.

If $p_1 \nmid m$, then by Fermat's Little Theorem (Thm 1.28)

$a^{p_1-1} \equiv 1 \pmod{p_1}$ and therefore $a^{de} \equiv a^{k(p_1-1)(p_2-1)+1} \equiv a \pmod{p_1}$.

- ▶ Similarly $a^{de} = a \pmod{p_2}$.
- ▶ Hence $a^{de} = a \pmod{p_1 p_2}$.

Euler's Theorem is therefore proved. ◇

Attack

Decryption is **hard** without the private key.

- ▶ Decryption is the inverse function of encryption.
 - ▶ Uniquely defined as $m = c^d$.
- ▶ Find d from public available information?
$$d = e^{-1} \bmod t \quad (t = (p_1 - 1)(p_2 - 1))$$

$\phi[n] = (p_1 - 1)(p_2 - 1) \quad p_1, p_2 ?$

$\phi[n] \equiv 1 \pmod{\phi[n]} \quad \phi[n] ?$

$m = c^d \quad d ?$

$Without \ knowing \ the \ factorization \ n = p_1 p_2,$
it is difficult to find t and hence d .

Digital Signature: The General Principle

Problem:

- ▶ Alice wishes to send a message m to Bob.
- ▶ Bob would like to verify that the message comes from Alice.

In physical world, Alice signs the letter.

In digital world, any fixed signature can be easily copied.

General principle:

private key enc.

- ▶ Alice sends $(m, y = s(m))$,
 - ▶ $y = s(m)$ is the message dependent signature.
 - ▶ The signature function s should be kept secret.
- ▶ Bob checks whether $m = s^{-1}(y)$.
 - ▶ He doesn't know the signature function s .

RSA Signature Scheme

- ▶ Let $p_1 \neq p_2$, $n = p_1 p_2$, and $t = (p_1 - 1)(p_2 - 1)$.
- ▶ Public key: (n, e) where $1 < e < t$ & $\gcd(e, t) = 1$.
- ▶ Private key: $1 < d < t$ s.t. $d \cdot e \equiv 1 \pmod{t}$.

“Sign” the message:

Alice computes $y = s(m) = m^d \pmod{n}$ and sends (m, y) .

Read the signature: If the message comes from Alice, then
$$y^e = (m^d)^e = m^{kt+1} = m \pmod{n}$$

Extend ElGamal Cryptography to ElGamal Signature?

RSA based schemes:

- ▶ In cryptography, we have $D_\ell(E_k(m))$.
- ▶ In digital signature, we have $E_k(D_\ell(m))$.
- ▶ This works as $(m^e)^d = (m^d)^e$.

This principle cannot be directly applied to ElGamal scheme.

ElGamal Signature Scheme

Notation:

$\forall x \in \mathbb{F}_p^*$, let $|x| \in \{1, \dots, p-1\}$ be the integer to represent $x \in \mathbb{F}_p^*$.

- ▶ Choose a prime p and a primitive element $b \in \mathbb{F}_p^*$.
- ▶ Choose a private key $a' \in \mathbb{N}$. Set the public key $a = b^{a'} \in \mathbb{F}_p^*$.
- ▶ Random choose $1 \leq t \leq p-1$ such that $\gcd(t, p-1) = 1$.
 - ▶ Set u s.t. $t \cdot u \equiv 1 \pmod{p-1}$.
- ▶ The signature function $s_t : \mathcal{M} \rightarrow (\mathbb{F}_p^*, \mathbb{N})$ is defined by
$$s_t(m) = (i, j), \text{ where } i = b^t, j = u(|m| - a'|i|).$$

The algebra in computing j is w.r.t. normal integers.

That is, the multiplication and subtraction are not w.r.t. \mathbb{F}_p .

- ▶ (i, j) is a valid signature for the message m if

$$\begin{aligned} a^{|i|} i^j &= b^{a'|i|} b^{tu(|m|-a'|i|)} \\ &= b^{|m|} \text{ in } \mathbb{F}_p^*. \end{aligned}$$

Summary

- ▶ Factorize a product of two large prime numbers
 - ▶ RSA public key cryptography
 - ▶ RSA signature scheme
- ▶ Discrete logarithm problem
 - ▶ Store passwords
 - ▶ Diffie-Hellman key exchange
 - ▶ ElGamal public key cryptography
 - ▶ ElGamal signature scheme
- ▶ Polynomial
 - ▶ Secret share