EE4.07 Coding Theory

W. Dai

Imperial College London (IC)

2018

Syllabus

Instructor: Dr. Wei Dai

GTA: Jingyuan Xia and Hengyan Liu

Lectures: 14:00-16:00 Fridays
Room 508 (12/10/2018-30/11/2018) Room 408 (7/12/2018-14/12/2018)

Assessment: Exam (75%) and coursework (25%)

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 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.

Two Facts for Coding Theory

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

This course: mostly relies on two 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.)

Greatest Common Divisor (GCD)

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

$\gcd(5, 13) = 1$. (Easy!)
$\gcd(20, 36) = 4$. (OK)
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,

$$\begin{array}{rlll}
a & = q_1 b & + r_1 & a.b \to r_1 \\
b & = q_2 r_1 & + r_2 & b.r_1 \to r_2 \\
r_1 & = q_3 r_2 & + r_3 & \vdots \\
\vdots & \vdots & \vdots & \\
r_{n-2} & = q_n r_{n-1} & + r_n & r_{n-2}.r_{n-1} \to r_n \\
r_{n-1} & = q_{n+1} r_n & & r_{n-1}.\boxed{r_n} \to 0
\end{array}$$

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

$r_n = \text{gcd}(a.b)$

The Euclidean Algorithm: An Example

$$\begin{aligned}
2406 &= 3 \times 654 + 444\\
654 &= 1 \times 444 + 210\\
444 &= 2 \times 210 + 24\\
210 &= 8 \times 24 + 18\\
24 &= 1 \times 18 + 6\\
18 &= 3 \times \boxed{6}
\end{aligned}$$

Example 1.2

$\gcd(654, 2406) = ?$:

$$\begin{aligned}
2406 &= 3 \times 654 && +444\\
654 &= 1 \times 444 && +210\\
444 &= 2 \times 210 && +24\\
210 &= 8 \times 24 && +18\\
24 &= 1 \times 18 && +6\\
18 &= 3 \times 6 &&
\end{aligned}$$

$\gcd(654, 2406) = 6$.

The Euclidean Algorithm: Theory

Theorem 1.3

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

Proof: Let $a = bq + r$ where $1 \leq r < b$.
Let $d_1 = \text{gcd}\,(a, b)$ and $d_2 = \text{gcd}\,(b, r)$. Want to show $d_1 = d_2$.

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

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

Therefore, $d_1 = d_2$. ◊

Corollary 1.4 (Validation of Euclidean Alg.)

In the Euclidean algorithm,

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

Bézout's Identity $(a,b) \rightleftarrows d$

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. $d = \mathrm{gcd}(a,b) = xa + yb$.

Proof:

$$\begin{aligned} r_n &= -q_n r_{n-1} + r_{n-2} \\ &= -q_n\left(-q_{n-1} r_{n-2} + r_{n-3}\right) + r_{n-2} \\ &= \left(1 + q_n q_{n-1}\right) r_{n-2} - q_n r_{n-3} \\ &= \cdots = xa + yb. \end{aligned}$$

◊

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

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

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

GCD of Polynomials

The GCD of two polynomials is a polynomial, of the highest degree, that divides both original polynomials.

In this course, the convention is that the leading coefficient is 1.

Example 1.7

$\gcd\left(x^2-1,\ 2x-2\right)=\left\{x-1,\ 2x-2,\ \frac{1}{2}x-\frac{1}{2},\ 10^6x-10^6\right\}$.
By convention, $\gcd\left(x^2-1,\ 2x-2\right)=x-1$.

Euclidean Algorithm for Polynomials

$$x^4+x^2+x+1 = (x^2-x+2)(x^2+x)+(-x+1)$$

Extend the Euclidean algorithm to polynomials.

$$x^2+x = (-x-2)(-x+1)+2$$

Example 1.8

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

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

$$2 = x^2+x-(-x-2)(-x+1)$$

Note that

$$\begin{aligned} x^4+x^2+x+1 &= \left(x^2-x+2\right)\left(x^2+x\right)+(-x+1) \\ x^2+x &= (-x-2)(-x+1)+2 \\ -x+1 &= \left(-\tfrac{1}{2}x+\tfrac{1}{2}\right)\cdot 2. \end{aligned}$$

$$= x^2+x-(-x-2)\left[x^4+x^2+x+1-(x^2-x+2)(x^2+x)\right]$$

One has

$$= b(x)-(-x-2)\left[a(x)-(x^2-x+2)b(x)\right]$$

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

$$= (x+2)a(x)+(-x^3-x^2-3)b(x)$$

$$\Rightarrow 1 = \tfrac{1}{2}(x+2)a(x)+\tfrac{1}{2}(-x^3-x^2-3)b(x)$$

As a result,

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

All Start from About 330 B.C.

In Book VII of *Elements*,
Euclid proved the following three results:

- *Euclid's lemma*: If a prime number p divides a product ab, then p divides at least one of the two numbers a and b.
- *Fundamental theorem of arithmetic*: Every natural number is either prime or else can be expressed as a product of primes in a way that is unique apart from the order in which they are written.
- There are infinitely many primes.

Fundamental Theorem of Arithmetic

Theorem 1.9 (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 1.10 (Applications)

If we know the factorisation of a and b,

- Greatest common divisor:

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

- Least common multiple:

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

Some Examples

Example 1.11

$$4 = 2^2. \quad 6 = 2 \cdot 3. \quad \Rightarrow \quad \gcd(4,6) = 2^1 \cdot 3^0 = 2. \quad \operatorname{lcm}(4,6) = 2^2 \cdot 3^1 = 12.$$

$$4 = 2^2. \quad 9 = 3^2. \quad \Rightarrow \quad \gcd(4,9) = 2^0 \cdot 3^0 = 1. \quad \operatorname{lcm}(4,9) = 2^2 \cdot 3^2 = 36.$$

$$654 = 2 \cdot 3 \cdot 109. \quad 2406 = 2 \cdot 3 \cdot 401. \quad \Rightarrow \quad \gcd(654,2406) = 6. \quad \operatorname{lcm}(654,2406) = 262254.$$

Proof of Unique Factorisation Theorem

Existence: By induction.
Assume it is true for all numbers less than n.
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

Lemma 1.12 (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,

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

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,

$$xpb + yab = b.$$

Since $p \mid xpb$ and $p \mid ab$ (by assumption), it holds that $p \mid xpb + yab$.
Hence $p \mid b$. ◊

Proof of Unique Factorisation Theorem (Uniqueness)

$$\begin{tikzcd}
 & P_1 \mid q_1 q_2 \cdots q_n \arrow[dl] \arrow[dr] & & \\
P_1 \mid q_1 \text{ or} & & P_1 \mid q_2 q_3 \cdots q_n \arrow[dl] \arrow[dr] & \\
 & P_1 \mid q_2 \text{ or} & & P_1 \mid q_3 q_4 \cdots q_n
\end{tikzcd}$$

$\Rightarrow P_i \mid q_j$ in the end

$\because P_i, q_j$ are primes

$\therefore P_i = q_j$.

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

$$n = p_1 p_2 \cdots p_m, \text{ and } n = q_1 q_2 \cdots q_n.$$

We shall show $m = n$ and that the q_j are a rearrangement of the p_i.

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. ◊

Gauss's Finite Arithmetic

In 1801

when Gauss was 24, he wrote a book *Disquisitiones Arithmeticae*, one of the most influential mathematics books ever. One of the topics is finite arithmetic.

Modular Arithmetic

Definition 1.13

Let a and $n > 0$ be integers. We define $a \bmod n$ to be the remainder when a is divided by n.

Write $a = qn + r$. Then $q = \lfloor a/n \rfloor$ and $r = a \bmod n$.

Example 1.14

$11 \bmod 7 = 4$ and $-11 \bmod 7 = 3$.

Definition 1.15

Two integers a and b are said to be *congruent modulo n* if $(a \bmod n) = (b \bmod n)$. This is written as $a \equiv b \pmod{n}$.

Example 1.16

$-10 \equiv 6 \pmod{8}$ and $1024 \equiv 0 \pmod{2}$.

Properties of Modular Arithmetic

1. $a + b \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n.$
2. $a - b \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n.$
3. $a \times b \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n.$

Proof for the addition:
$a + b \bmod n = r_a + r_b \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n.$

Ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

Examples

$k = \frac{a}{b} \pmod n$ ⟺ $bk \equiv a \pmod n$

$\underbrace{[\gcd(b, n) = 1]}$

· What value k, when × b, is a mod n ?

- $11 = 4 \bmod 7$ and $-11 = 3 \bmod 7$.
  - $11 + (-11) = 0 \bmod 7$; $4 + 3 = 0 \bmod 7$.
  - $11 - (-11) = 1 \bmod 7$; $4 - 3 = 1 \bmod 7$.
- $5 \times 5 = 1 \bmod 12$; $11 \times 5 = 7 \bmod 12$.
  $1/5 = 5 \bmod 12$; $7/5 = 11 \bmod 12$.
  But $5/6 \bmod 12$ is not defined.

$k = \frac{1}{5} \bmod 12$

$5k \equiv 1 \bmod 12$

$\Rightarrow k = 5$

$k = \frac{7}{5} \bmod 12$

$5k \equiv 7 \bmod 12$

$\Rightarrow k = 11$

$k = \frac{5}{6} \bmod 12$

$6k \equiv 5 \bmod 12$

not defined.

Fields: Definition

Definition 1.17 (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. $a \cdot a^{-1} = 1$.

Example: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_7$ are fields, $\mathbb{Z}$ is not.

C ✓ R ✓ Q ✓ Z ✗ N ✗ (a^{-1})

Integer Ring

Definition 1.18 (Modulo)

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

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

Definition 1.19 (Integer Ring)

- $\mathbb{Z}_m = \{0, \cdots, m-1\}$: a nonempty set of elements.
- "$+$" operator: $\boxed{+ \text{ mod } m}$
- "$\cdot$" operator: $\boxed{\cdot \text{ mod } m.}$

Example of $m = 4$:
$\mathbb{Z}_m = \{0, 1, 2, 3\}$.
$1 + 1 = 2 \pmod 4$; $2 + 3 = 1 \pmod 4$.
$3 \cdot 3 = 1 \pmod 4$; $2 \cdot 2 = 4 = 0 \pmod 4$.

Examples: Integer Rings Versus Fields

- $\mathbb{Z}_3$ is a field.
  - $-0 = 0$, $-1 = 2$, $-2 = 1$.
  - $1^{-1} = 1$, $2^{-1} = 2$.

$1 \cdot 1 \bmod 3 = 1$

$2 \cdot 2 \bmod 3 = 1$

- $\mathbb{Z}_4$ is not a field.
  - $-0 = 0$, $-1 = 3$, $-2 = 2$, $-3 = 1$.
  - $1^{-1} = 1$, $\nexists\, 2^{-1}$, $3^{-1} = 3$.

$1 \cdot 1 \bmod 4 = 1$

$2 \cdot ? \bmod 4 = 1$

$3 \cdot 3 \bmod 4 = 1$

When a Multiplicative Inverse Exists

Lemma 1.20 (Existence of the multiplicative inverse)

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

$\gcd(a.n) = 1 \Rightarrow ax + bn = 1$

$\Rightarrow a\underset{a^{-1}}{\boxed{x}} \equiv 1 \pmod{n}$

Proof:

1. If $\gcd(a, n) = 1$, by Bézout's identity $\exists x, y$ s.t. $1 = xn + ya \equiv ya \pmod{n}$. Hence y is a^{-1}.
2. If a^{-1} (mod 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.
   $1 = xa \bmod n = xa - yn$.
   As $d \mid a$ and $d \mid n$, it follows $d \mid (xa - yn)$, i.e. $d \mid 1$.
   This contradicts with $d > 1$. ◊

$\Rightarrow d = \gcd(a.n)$

$\Rightarrow d \mid a.\ d \mid n$

$\Rightarrow d \mid ax + bn = 1$

$a\overset{a^{-1}}{\boxed{x}} \equiv 1 \pmod{n} \Rightarrow ax + bn = 1 \quad \Rightarrow \gcd(a.n) = 1$

Finite Fields of Integers

Theorem 1.21

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

if not, there exists coprimes. and no m.i.

Proof of the "if" part: m be a prime$\Rightarrow\mathbb{Z}_m$ is a field.
$\forall a \in \mathbb{Z}_m \backslash \{0\}$, since m is a prime, one has gcd $(a, m) = 1$.
By Lemma 1.20, a^{-1} exists. $\Diamond$

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. $a \cdot b = m$.
Since $a = \gcd(a, m) \neq 1$, by Lemma 1.20, a^{-1} does not exist. $\Diamond$

An Alternative Proof

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

Lemma 1.22

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:
Suppose m is not a prime.$\exists 1 < a, b < m$ s.t. $a \cdot b = m = 0 \pmod m$. But from Lemma 1.22, either a or b is zero mod m. Contradict with $1 < a, b < m$. $ab \bmod m = ab = 0$ $\Diamond$

$\Rightarrow a = 0$ or $b = 0$

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: $a_d = 1$.

Polynomial division:

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

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).

Finite Fields: Polynomials

$\mathbb{F}_p[x]/f(x)$: an entity

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

($\mathbb{F}_p[x]/f(x)$): $\mathbb{F}_p[x]$ with "mod $f(x)$" algebra.
It contains all the polynomials with degree less than $\deg(f)$.

Example: $f(x) = x^2 + x \in \mathbb{F}_2[x]$.
$\mathbb{F}_2[x]/f(x) = \{0, 1, x, x+1\}$.
$x \cdot (x+1) = x^2 + x \equiv 0 \bmod f(x)$.

Theorem 1.23

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

Proof: Same idea as before.

polynomial: irreducible
number: prime

Some Comments

Examples of Irreducible polynomials and those that are not

- $x^2 + 1 \in \mathbb{R}[x]$ is irreducible.
- $x^2 + 1 \in \mathbb{F}_2[x]$ is not irreducible (reducible).
- $x^2 + 1 \in \mathbb{F}_3[x]$ is irreducible.
- $x^2 + 1 \in \mathbb{F}_5[x]$ is not irreducible.

A systematic way to write the elements in a polynomial ring $\mathbb{F}_p[x]/f(x)$ where $d = \deg(f(x))$.
$\cancel{\alpha_d x^d +} \alpha_{d-1}x^{d-1} + \cdots + \alpha_1 x + \enclose{circle}{\alpha_0}$, P choises where $\alpha_i \in \mathbb{F}_p$.
It contains p^d many distinct polynomials.

Size of the finite field $\mathbb{F}_q$

- $\mathbb{F}_q$ 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, $\cdots$

Each of these polynomial generates a finite field.

Example 1.24

instances of $\mathbb{F}_2[x]$	$\mathbb{F}_2[x]/x^3+x+1$	$\mathbb{F}_2[x]/x^3+x^2+1$
0	0	0
1	1	1
x	x	x
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

$\# = p^\alpha$

Another Example

Example 1.25 (An Example of $\mathbb{F}_{16}$)

	$\mathbb{F}_2[x]/x^4+x+1$		$\mathbb{F}_2[x]/x^4+x+1$
0	0	x^7	x^3+x+1
1	1	x^8	x^2+1
x	x	x^9	x^3+x
x^2	x^2	x^{10}	x^2+x+1
x^3	x^3	x^{11}	x^3+x^2+x
x^4	$x+1$	x^{12}	x^3+x^2+x+1
x^5	x^2+x	x^{13}	x^3+x^2+1
x^6	x^3+x^2	x^{14}	x^3+1

$x^{15} = x \cdot x^{14} \equiv x \cdot (x^3+1) \equiv x^4 + x \equiv 1$

$x^{16} = x \cdot x^{15} \equiv x$ $\{\text{period} = p^d \boxed{-1}\}$

Useful Exercise

a) $(x^3+x^2)(x^3+x^2+1) \equiv x^6 \cdot x^{13} \equiv x^{19-15} \equiv x^4 \equiv x+1$

b) $f = x^4+x+1$. $g = x^3+x^2$ gcd $= 1 \Rightarrow g^{-1}$ by Euc. alg.

$f = (x-1)g + x^2+x+1$

$g = x(x^2+x+1) - x \Rightarrow$

$x^2+x+1 = (-x-1)(-x)+1$

$$\begin{aligned} 1 &= x^2+x+1 + (x+1)(-x) \\ &= x^2+x+1 + (x+1)[g - x(x^2+x+1)] \\ &= (x+1)g + (-x^2-x+1)(x^2+x+1) \\ &= (x+1)g + (-x^2-x+1)[f-(x-1)g] \\ &= (-x^2-x+1)f + (x^3-x+2)g \\ &= (x^2+x+1)f + \underbrace{(x^3+x)}_{g^{-1}}g \end{aligned}$$

Example 1.26 (An Exercise)

1. Understand Examples 1.24 and 1.25.
2. For the field $\mathbb{F}_2[x]/x^4+x+1$ in Example 1.25, compute:
   - $(x^3+x^2)(x^3+x^2+1) = ?$
     - Answer: $x+1$
   - $(x^3+x^2)^{-1} = ?$ (Use Euclidean algorithm)
     - Answer: x^3+x.
   - $(x^3+x^2+1)^{-1} = ?$ (Use Euclidean algorithm)
     - Answer: x^2.

b') $x^3+x^2 \equiv x^6$

$(x^3+x^2)^{-1} \equiv x^{15-6} = x^9 \equiv x^3+x$

c') $x^3+x^2+1 \equiv x^{13}$

$(x^3+x^2+1)^{-1} = x^{15-13} = x^2$

Finite Fields: General Properties?

Previously, we saw two ways to construct finite fields.

- $\mathbb{F}_p$: p many integers.
- $\mathbb{F}_p\left[x\right]/f\left(x\right)$: $p^{\deg(f)}$ 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.
By definition, $\exists$ a multiplicative identity, denoted by '1'.
Consider a sequence in $\mathbb{F}_q$: 1, $1+1$, $\cdots$

Since $|\mathbb{F}_q| = q < \infty$, we will see repetitions.
That is, $\exists t \in \mathbb{Z}^+$ s.t. $\underbrace{1 + \cdots + 1}_{t \text{ times}} = t \cdot 1 = 0$.

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

Definition 1.27

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

Characteristic: Property

$$(\underbrace{1+\cdots+1}_{a})(\underbrace{1+\cdots+1}_{b}) = (\underbrace{1+\cdots+1}_{t}) = 0$$

Lemma 1.28

The characteristic t is always a prime.

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

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 1.22).

Contradict with that t is the smallest.

(contradict with the assumption)

Finite Fields: Size

Theorem 1.29

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.,

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

Consider a maximal set

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

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

Define the linear span of $\mathcal{B}$

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

$= p^m$

Finite Fields: Size and Dimension

Proof continued:

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

   If $\left(\lambda_1^{(1)}, \cdots, \lambda_m^{(1)}\right) \neq \left(\lambda_1^{(2)}, \cdots, \lambda_m^{(2)}\right)$, 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 $\sum \left(\lambda_i^{(1)} - \lambda_i^{(2)}\right) b_i = 0$ which, by linear independence of b_i's, implies that $\lambda_i^{(1)} = \lambda_i^{(2)}$.

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

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

   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 $\mathbb{F}_q$, $q = p^m$. $\Diamond$

$\mathcal{B}$ 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 $a, a^2, a^3, \cdots$. Since $|\mathbb{F}_q| = q$ is finite, we will see repetitions. That is, $\exists t$ s.t. $a^t = 1$.

order → element

characteric → field

Definition 1.30

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 $\mathbb{F}_q$.

Example 1.31

Consider the field $\mathbb{F}_2\,[x]\,/x^4 + x + 1$ in Example 1.25.
It can be verified that

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

Hence x, x^2, and x^4 are primitive elements (Primitive element is not unique).
It can also be verified that $\text{ord}\,\left(x^3\right) = 5$. Hence x^3 is not a primitive element.

Represent a Field by a Primitive Element

Let α be a primitive element. Since $\alpha^0 = 1, \alpha, \cdots, \alpha^{q-2}$ are distinct, $\mathbb{F} = \left\{0, 1, \alpha, \cdots, \alpha^{q-2}\right\}$.

- Standard notation: $\mathbb{F}^* = \mathbb{F} \backslash \{0\} = \left\{\alpha^0, \cdots, \alpha^{q-2}\right\}$.

Why primitive elements? Recall Example 1.26

- Calculate multiplication:
  - $\left(x^3 + x^2\right)\left(x^3 + x^2 + 1\right) =?$
  - $\alpha^6 \cdot \alpha^{13} = \alpha^{19} = \alpha^{15+4} = \alpha^4 = x + 1.$
- Find inverse:
  - $\left(x^3 + x^2\right)^{-1} =?$; $\left(x^3 + x^2 + 1\right)^{-1} =?$
  - 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 1.32

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

$\mathbb{F}_5^*$

$1^4 = 1$

$2^4 = 16 \equiv 1$

$3^4 = 81 \equiv 1$

$4^4 = 256 \equiv 1$

Theorem 1.33 (Fermat's Little Theorem)

For every $\beta \in \mathbb{F}_q^*$, we have $\underline{\beta^{q-1} = 1}$.
Or equivalently, $\forall \beta \in \mathbb{F}_q$, it holds that $\underline{\beta^q = \beta}$.

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: "$\cdots$, 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

Proof: For any $\beta \in \mathbb{F}_q^*$, define $\beta\mathbb{F}_q^* = \{\beta\beta_1, \cdots, \beta\beta_{q-1}\}$.

- $\beta\beta_i \neq 0 \Rightarrow \beta\mathbb{F}_q^* \subseteq \mathbb{F}_q^*$. (definition of field)
  Otherwise $\beta_i = \beta^{-1}\beta\beta_i = \beta^{-1} \cdot 0 = 0$. A contradiction.
- $\beta\beta_i \neq \beta\beta_j$ for $i \neq j$. $\Rightarrow \left|\beta\mathbb{F}_q^*\right| = q-1$.
  Otherwise $\beta_i = \beta^{-1}(\beta\beta_i) = \beta^{-1}(\beta\beta_j) = \beta_j$. A contradiction.

Hence, $\mathbb{F}_q^* = \beta\mathbb{F}_q^*$.
Therefore, $\prod_{\gamma\in\mathbb{F}_q^*} \gamma = \prod_{\gamma\in\beta\mathbb{F}_q^*} \gamma$.
That is,

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

We conclude $\beta^{q-1} = 1$. ◊

Examples Related to Fermat's Little Theorem

Example 1.34

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

$\mathbb{F}^* = 1 \cdot \mathbb{F}^* = \{1, 2, 3, 4\}$ $\qquad$ $2 \cdot \mathbb{F}^* = \{2, 4, 1, 3\}$

$3 \cdot \mathbb{F}^* = \{3, 1, 4, 2\}$ $\qquad$ $4 \cdot \mathbb{F}^* = \{4, 3, 2, 1\}$

Example 1.35

Let $\mathbb{F} = \mathbb{F}_2 [x] / \left(x^2 + x + 1\right)$. 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

Lemma 1.36

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

Proof: Let $a = \text{ord}(\beta)$ & $t = ka + b$ where $0 < b < a$.
Then $\beta^t = \beta^b = 1$. if ord$(\beta) \nmid t$, there exists $0<b<a$.
Contradict with that a is the smallest number that $\beta^a = 1$. ◊

Corollary 1.37

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

Proof: This is proved by Fermat's little theorem (Theorem 1.33) and Lemma 1.36.

Existence of Primitive Elements: Lemma 3

Lemma 1.38

Suppose that ord$(\beta_1) = r_1$, ord$(\beta_2) = r_2$, and gcd$(r_1, r_2) = 1$. Let $\beta = \beta_1\beta_2$ and $r =$ ord(β). Then $r = r_1 r_2$.

Proof:

1. Since $1 = (\beta_1\beta_2)^{r_1 r_2} = \beta^{r_1 r_2}$, it holds $r | r_1 r_2$ by Lemma 1.36.
2. $r_1 r_2 | r$:
   $1 = \beta^{r r_1} = (\beta_1\beta_2)^{r r_1} = \left(\beta_1^{r_1}\right)^r \beta_2^{r r_1} = \beta_2^{r r_1}$. Then $r_2 | r r_1$. Then $r_2 | r$.
   Similarly, $r_1 | r$.
   Hence $\mathrm{lcm}\,(r_1, r_2)\,| r$ or equivalently $r_1 r_2 | r$.
3. That $r | r_1 r_2$ and $r_1 r_2 | r$ implies $r = r_1 r_2$. $\Diamond$

An Example Related to Lemmas 2 & 3

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

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

$$\begin{array}{ll} \mathrm{ord}\,(1) = 1 & \mathrm{ord}\,(2) = 3 \\ \mathrm{ord}\,(3) = 6 & \mathrm{ord}\,(4) = 3 \\ \mathrm{ord}\,(5) = 6 & \mathrm{ord}\,(6) = 2 \end{array}$$

You may check the above results with Corollary 1.37.

Note that $\mathrm{ord}\,(2) = 3$ and $\mathrm{ord}\,(6) = 2$.
Fact 1.38 implies that $\mathrm{ord}\,(2 \cdot 6) = 3 \times 2 = 6 = \mathrm{ord}\,(5)$.

Existence of Primitive Elements: the Proof (1) !

Proof of Theorem 1.32 (the existence):

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

Define $m := \text{lcm}(r_1, \cdots, r_{q-1})$.

Based on the unique factorisation theorem (Theorem 1.9), m can be written as $m = p_1^{k_1} \cdots p_\ell^{k_\ell}$. Product of orders

$$\begin{aligned} \text{Let} \qquad r_1 &= p_1^{k_1^{(1)}} \cdots p_\ell^{k_\ell^{(1)}}, \\ &\vdots \\ r_{q-1} &= p_1^{k_1^{(q-1)}} \cdots p_\ell^{k_\ell^{(q-1)}}. \\ \text{Then} \qquad k_i &= \max\left(k_i^{(1)}, \cdots, k_i^{(q-1)}\right). \end{aligned}$$

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

element to produce the greatest prime factor.

Existence of Primitive Elements: the Proof (2)

recombine $\qquad\qquad$ by def.

Let $\beta_1 = \alpha_i^{\mathrm{ord}(\alpha_i)/p_1^{k_1}}$, then $\mathrm{ord}\,(\beta_1) = p_1^{k_1}$.
Similarly, find $\beta_2, \cdots, \beta_\ell$.
Clearly $\mathrm{ord}\,(\beta_i) = p_i^{k_i}$, $i = 1, \cdots, \ell$ by our construction.

Let $\beta = \beta_1 \cdot \cdots \cdot \beta_\ell$. Then $\mathrm{ord}\,(\beta) = m$ (Lemma 1.38).

Because $\mathrm{ord}\,(\beta_i)$'s are co-prime.

Hence, $m | (q-1)$ (Corollary 1.37) or $m \leq q-1$.

$\beta \in \mathbb{F}_q$ $\qquad\qquad$ $\alpha_i^m = 1$

On the other hand, by the definition of m, 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. $\quad\Diamond$

Uniqueness of Finite Fields

Definition 1.39

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

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

Theorem 1.40

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

Proof is not required.

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

Example

$$\begin{aligned} \varphi:\ \mathbb{F}_2[x]/\left(x^3+x^2+1\right) &\to \mathbb{F}_2[y]/\left(y^3+y+1\right) \\ x &\mapsto \varphi(x) = y+1 \end{aligned}$$

$\varphi:$	$\mathbb{F}_2[x]/\left(x^3+x^2+1\right)$	$\mathbb{F}_2[y] = y^3+y+1$
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 $\varphi(ab) = \varphi(a)\varphi(b)$:

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

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

$y^3 = -y-1 = y+1$

Polynomial Factorisation

Problem: factorise the polynomial $x^{q^m-1}-1$ in $\mathbb{F}_q\left[x\right]$.
Be careful about the concept of "irreducible polynomial":

Have to specify the field we are considering.

Example 1.41

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

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

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

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

An Example of Factorisation

Factorise $x^3 - 1 \in \mathbb{R}[x]$:

- Consider the easier problem: factorise $x^3 - 1$ in $\mathbb{C}[x]$.
- Group terms of conjugate roots
  - $$\begin{aligned} x^3 - 1 &= (x-1)\left(x - e^{j2\pi/3}\right)\left(x - e^{j4\pi/3}\right) \\ &= (x-1)\left(x^2 + x + 1\right). \end{aligned}$$

$$x^{q^m-1} - 1 = (x-\alpha^0)(x-\alpha^1)(x-\alpha^2)\cdots(x-\alpha^{q^m-2})$$

To factorise the polynomial $x^{q^m-1} - 1$ in $\mathbb{F}_q[x]$, we use the same strategy:

- Factorise $x^{q^m-1} - 1$ in $\mathbb{F}_{q^m}[x]$.
  - Let α be a primitive element of $\mathbb{F}_{q^m}$:
    $x^{q^m-1} - 1 = \prod_{i=0}^{q^m-2}\left(x - \alpha^i\right)$ (Irreducible polynomials in $\mathbb{F}_{q^m}[x]$).
  - Group appropriate terms together:
    $x^{q^m-1} - 1 = \prod_{k=1}^{s} M^{(k)}(x)$ (Irreducible polynomials in $\mathbb{F}_q[x]$).

A Preview of the Final Result

Example 1.42

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

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

Both $x - 1$ and $x^2 + x + 1$ are irreducible polynomial in $\mathbb{F}_2[x]$.
We have obtained the factorisation of $x^3 - 1$ in $\mathbb{F}_2[x]$.

Construction of Minimal Polynomials

Definition 1.43 (Cyclotomic Coset)

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

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

$C_0 = \{0 \cdot [2^0 . 2^1 . 2^2 . 2^3]\} \bmod 15 = \{0\}$

Example 1.44

$C_1 = \{1 \cdot [2^0 . 2^1 . 2^2 . 2^3]\} \bmod 15 = \{1.2.4.8\} = C_1 \cdot C_2 \cdot C_4 . C_8$

$C_2 = \{2 \cdot [2^0 . 2^1 . 2^2 . 2^3]\} \bmod 15 = \{2.4.8.1\}$

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

$C_3 = \{3 \cdot [2^0 . 2^1 . 2^2 . 2^3]\} \bmod 15 = \{3.6.12.9\}$

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

$C_5 = \{5 \cdot [2^0 . 2^1 . 2^2 . 2^3]\} \bmod 15 = \{5.10\}$

Definition 1.45 (Minimal Polynomial)

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

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

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

Towards Factorisation

$$x^{q^m-1} - 1 = \prod_{k=1}^{s} M^{(k)}(x)$$

Want to show:

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

Lemma 1.46

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 1.33) $\beta^q = \beta$.
$\Leftarrow$: 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 1.47

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

$i! \mid p(p-1)\cdots(p-i+1)$

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

p is prime

Note that $\gcd(i!, p) = 1$ but $\binom{p}{i} \in \mathbb{Z}^+$. By Euclid's Lemma (Theorem 1.12), $i! \mid \underbrace{(p-1)\cdots(p-i+1)}_{s}$ and $\binom{p}{i} = p \cdot s$ for some $s \in \mathbb{Z}^+$.
By the definition of the characteristic, $\binom{p}{i} = 0$, $\forall 1 \le i \le p-1$. ◊

Corollary 1.48

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

Properties of Cyclotomic Cosets

Lemma 1.49

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 $q\mathcal{C}_i = \mathcal{C}_i$.

$= \{ i \bmod q^m - 1 : \text{irre. of } j \} = \mathcal{C}_i$

Proof: Note that $i \cdot q^m = i \bmod q^m - 1$. It is clear that $\mathcal{C}_i = \{i \cdot q^j \bmod q^m - 1 :\ j = 0, 1, \cdots, m-1\} = \{i \cdot q^j \bmod q^m - 1 :\ j = 1, 2, \cdots, m\} = q\mathcal{C}_i$. $\Diamond$

$q\mathcal{C}_i = \{ i \cdot q^{j+1} \bmod q^m - 1 : j = 0, 1 \cdots m-1 \}$

$= \{ i \cdot q^j \bmod q^m - 1 : j = 1, 2 \cdots m \}$

Corollary 1.50

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

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

Proof: $\prod_{j \in \mathcal{C}_i} \left(x - \alpha^{jq}\right) = \prod_{\ell \in q\mathcal{C}_i} \left(x - \alpha^{\ell}\right) = \prod_{j \in \mathcal{C}_i} \left(x - \alpha^{j}\right)$. $\Diamond$

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

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

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

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

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

where (a) comes from Corollary 1.50, (b) comes from Corollary 1.48. Hence, $a_\ell = a_\ell^q$, which implies $a_\ell \in \mathbb{F}_q$ and $M^{(i)}(x) \in \mathbb{F}_q[x]$. ◊

Fermat's little

$M^{(i)}(x)$ is Irreducible

Step 1: For all $f(x) \in \mathbb{F}_q[x]$ s.t. $f\left(\alpha^i\right) = 0$, it holds that $M^{(i)}(x) \,|\, f(x)$.
Write $f(x) = f_0 + f_1 x + \cdots + f_n x^n$.
For any $j \in \mathcal{C}_i$, $\exists \ell$ s.t. $j = iq^\ell \bmod q^m - 1$.

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

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

Step 2: $M^{(i)}(x)$ is irreducible in $\mathbb{F}_q[x]$.
Suppose not. Then $M^{(i)}(x) = g(x)\, h(x)$ for nontrivial $g(x)$ and $h(x)$.
α^i is a root of $M^{(i)}(x) \Rightarrow \alpha^i$ is a root of one of $g(x)$ and $h(x)$.
W.l.o.g., α^i is a root of $g(x)$. Then $M^{(i)}(x) \,|\, g(x)$ which is impossible.
Hence $M^{(i)}(x)$ is irreducible. $\Diamond$

Representatives of Cyclotomic Cosets

Definition 1.51

Consider the cyclotomic cosets of q mod n.
A subset $\{i_1, \cdots, i_j\} \subset \mathbb{Z}_n$ is a complete set of representatives of cyclotomic cosets if

$$C_{i_1} \bigcup \cdots \bigcup C_{i_j} = \mathbb{Z}_n.$$

Example 1.52

Cyclotomic cosets of 2 mod 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 1.53

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

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

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. $\Diamond$

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 $E_k : \mathcal{M} \to \mathcal{C}$ and the corresponding decryption function $D_\ell : \mathcal{C} \to \mathcal{M}$ such that

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

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 $\mathcal{K} = \{1, 2, \cdots, 25\}$. 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␣YOU␣TOMORROW becomes XJJ␣DTZ␣YTRTWWTB

For the Caesar system, a simple attack is exhaustive search as there are only 25 keys.
A natural extension is to use any permutation of 26 letters, yielding $26! \approx 4 \times 10^{27}$ keys. Exhaustive search is impossible.

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

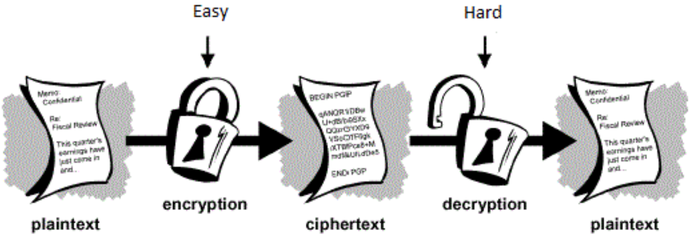
Consider a 29-symbol alphabet including 26 English letters, the space ␣, comma, and full stop. It is mapped to $\mathbb{F}_{29}$.
Given a stream of symbols, split it into blocks of size n so that each block can be written as $\boldsymbol{m} \in \mathbb{F}_{29}^{n}$. A key $\boldsymbol{K} \in \mathbb{F}_{29}^{n \times n}$ is an invertible matrix. The encryption function is given by

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

and the decryption function is

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

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:

$x = p_1 \cdots p_N + 1$

1. Suppose that there exist only finitely many prime numbers.

$x \equiv 1 \pmod{p_i}$

2. List all these prime numbers, $p_1,\ p_2,\ \cdots,\ p_N$.

$\gcd(x. p_i) = 1$

3. Let $x = p_1 \cdot p_2 \cdots p_N + 1$.

x cannot be expressed by p_i

4. Claim: x is a prime number.
   Proved by the Unique Factorisation Theorem 1.9 as $gcd\,(p_i, x) = 1$.

x is a prime

5. This contradicts the assumption that the list of $p_1,\ p_2,\ \cdots,\ p_N$ contains all the prime numbers. ◊

Large Prime Numbers

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

Prime	When	Prime	When	Prime	When
$2^{74207281}-1$	2016	$2^{57885161}-1$	2013	$2^{43112609}-1$	2008
$2^{42643801}-1$	2009	$2^{37156667}-1$	2008	$2^{32582657}-1$	2006

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

eg. $3^{29} \bmod 17 \xrightarrow{✓} 12$

$3^{(x)} \bmod 17 \xleftarrow{?} 12$

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 pri. key

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

P: prime

b: primitive

- It is well-defined if and only if b is primitive.

s.t. y can take any value in $\mathbb{F}_p^*$ and distributed uniformly.

$3^{16} \bmod 811 = 463$

Computation Complexity

$3^{211} \bmod 811 = 3^{128} \cdot 3^{64} \cdot 3^{16} \cdot 3^{2} \cdot 3^{1} \bmod 811 = (3^{16})^{4} \cdot (3^{16})^{4} \cdot (3^{16})^{4} \cdot 3^{16} \cdot 3^{2} \cdot 3^{1} \bmod 811$

$= [(479)^{3} \bmod 811 \cdot 463 \cdot 9 \cdot 3] \bmod 811$

$= 385 \times 462 \times 9 \times 3 \bmod 811 = 411$

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

Example: $3^{211} = ? \pmod{811}$

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

$3^2 = 3 \cdot 3 \pmod{811}$, $3^4 = 3^2 \cdot 3^2 \pmod{811}$,

$\cdots$, $3^{2^k} = 3^{2^{k-1}} \cdot 3^{2^{k-1}} \pmod{811}$.

Discrete logarithmic function: computational complexity $\underline{O(p)}$.

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

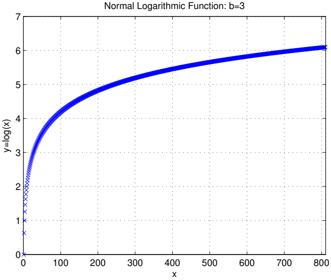
Examples

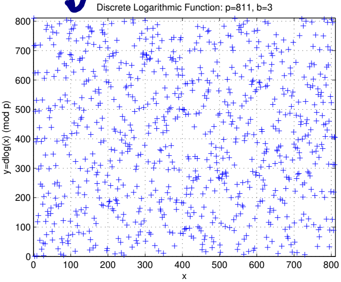
$y = b^x \bmod p$

primitive — prime

$x = \log_b y \bmod p$

Let $p = 811$ and $b = 3$.
The output of discrete logarithmic function looks random:
$\log_3 2 = 717$; $\log_3 3 = 1$; $\log_3 4 = 624$; $\log_3 5 = 494$; $\cdots$.





Store Passwords on a Server: A Solution

- The administrator chooses a prime p and a primitive element b.
  - 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.

$$x_i \xrightarrow{\checkmark} y_i$$

$$x_i \xleftarrow{?} y_i$$

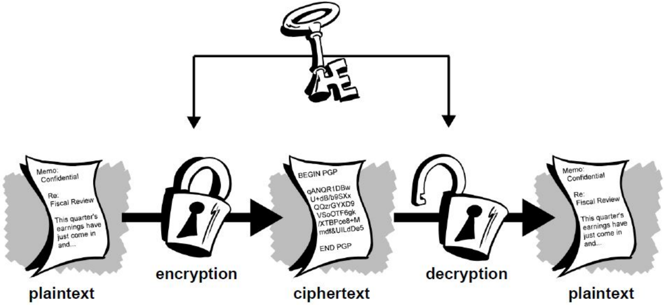
Cryptography for Information Exchange

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://chrispacia.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

$A' = B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$

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

$B' = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$

respectively. Note that $A' = B' = g^{ab}$ $(\bmod p)$ 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: $(\overset{\text{required}}{k}, \overset{\text{total}}{n})$ threshold scheme.

Store the secret S into n pieces of encrypted words $S_1, \cdots, S_n$ 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 $S < p$.
   (to construct field)
2. Randomly choose $k-1$ positive integers $a_1, \cdots, a_{k-1}$. Set $\underline{a_0 = S}$.
3. Set $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$.
4. Evaluate $f(x)$ at n points to obtain $(t_i, f(t_i))$, $t_i \in \mathbb{F}_p^*$ and $i = 1, \cdots, n$.

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:

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

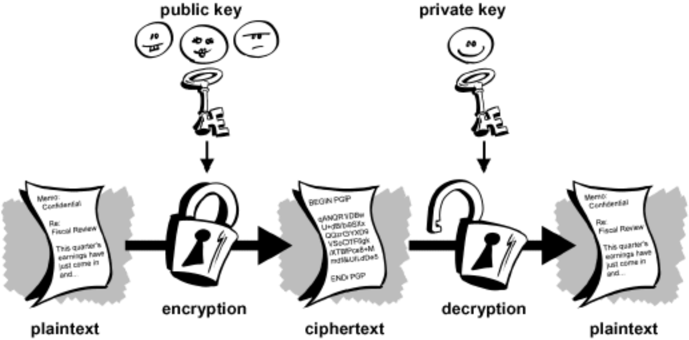
- Or polynomial interpolation:

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

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).
- 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 $b \in \mathbb{F}_p^*$.
- Private key: choose an integer $a' \in \mathbb{N}$.
- Public key: $\underline{a = b^{a'}} \in \mathbb{F}_p^*$. pri. always on the exp.

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

$$\underline{\left(b^t,\ ma^t\right)}$$

Decryption: Alice can recover m via

exchange exp. order

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

$$(b^t)^{-a'} = (b^{a'})^{-t} = a^{-t}$$

Advantage:

The random number t generates a random encryption function.

(pri. key to encrypt)

RSA Cryptography

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 $\underline{\gcd(e,t) = 1}$. ensure e^{-1} exists.
- Private key: d where $1 < d < t$ and $\underbrace{d \cdot e}$ mod $t = 1$.
  - Find d by the Euclidean algorithm.

$ed \equiv 1 \mod t$

$\Rightarrow \boxed{ed = kt+1}$

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

$$c = m^e \bmod n.$$

$m = c^d \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m^{kt+1} \bmod n$

$= m \bmod n$

Decryption: Bob can recover m from c via

$$m = c^d \bmod n.$$

An Example

- Bob chooses $p_1 = 47$ and $p_2 = 59$.
- $n = 47 \times 59 = 2773$. $t = 46 \times 58 = 2668$.
- $e = 157$ is a valid public key as $\gcd(e, 2668) = 1$.
- Use Euclidean algorithm, $d = 17$.
- 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 1.33): $\forall a \in \mathbb{F}_p^*,\ a^{p-1} = 1 \bmod p$

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 $\forall a \in \mathbb{Z}^+$,

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

The correctness of RSA: $ed \equiv 1 \bmod t$

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

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

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:

- $x = y \bmod p_1 \Rightarrow p_1 | (x - y)$.
  Hence $x - y = ap_1$ for some integer a. $a = \frac{x-y}{p_1}$
- $x = y \bmod p_2 \Rightarrow p_2 | (x - y) \Rightarrow p_2 | (ap_1) \Rightarrow p_2 | a$
  $\Rightarrow p_1 p_2 | (x - y)$

Hence $x = y \bmod p_1 p_2$. $\Diamond$

Proof of Euler's Theorem

Fix an $m \in \{1,\ 2,\ \cdots,\ p_1p_2 - 1\}$.

- We first show that $m^{de} = m \bmod p_1$.
  - If $p_1|m$, then $m = 0 \bmod p_1$ and $m^{de} = 0 \bmod p_1$. Hence $m^{de} = m \bmod p_1$.

    $de \equiv 1 \bmod t \Rightarrow de = kt+1$
  - If $p_1 \nmid m$ then by Fermat's Little Theorem (Thm 1.33) $m^{p_1-1} \equiv 1 \bmod p_1$. Hence $m^{de} \equiv m^{k(p_1-1)(p_2-1)+1} \equiv m \bmod p_1$.

    $m^{p_1-1} \equiv 1 \bmod p_1 \Rightarrow m^{k(p_1-1)(p_2-1)} \equiv 1 \bmod p_1$
- Similarly $m^{de} = m \bmod p_2$.
- Hence $m^{de} = m \bmod p_1p_2$.

Euler's Theorem is therefore proved. $\Diamond$

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?

  $d = e^{-1} \bmod t \quad (t = (p_1 - 1)(p_2 - 1))$.

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

General principle:

- Alice sends $(m, y = s(m))$,
  - $y = s(m)$ is the message dependent signature.
  - The signature function s should 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. $d \cdot e \ = 1 \bmod t$.

"Sign" the message:

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

Read the signature: If the message comes from Alice, then

$$\underline{y^e = \left(m^d\right)^e = m^{kt+1} = m \bmod n}.$$

encryption: $m = (m^e)^d$

signature: $m = (m^d)^e$

Extend ElGamal Cryptography to ElGamal Signature?

RSA based schemes:

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

This principle cannot be directly applied to ElGamal scheme.

ElGamal Signature Scheme

Notation:

$\forall x \in \mathbb{F}_p^*$, let $|x| \in \{1, \cdots p-1\}$ 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. $t \cdot u = 1 \bmod p-1$.
- The signature function $s_t : \mathcal{M} \to \left(\mathbb{F}_p^*, \mathbb{N}\right)$ is defined by
  $$s_t(m) = (i, j), \text{ where } i = b^t,\ j = u\left(|m| - a'|i|\right).$$
  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