Mo Tu We Th Fr Sa Su

Date / /

LEC 5 Number Theory II 3.1

Encryption

beforehand: "keys" are exchanged

encryption: $m' = E_{(keys)}(m)$

decryption: $m = D_{("keys")}(m')$

ex1:

Turing' code V1.

victory

↓

m=22 09 03 20 15 18 25 (13) ← added

↑ prime

Beforehand: exchange secret prime k

Enc: $m' = mk$

Dec: $m = m'/k$ ↑

Hard to factor a product of 2 large primes

but:

$m_1' = m_1 k$ ⇒ $\gcd(m_1', m_2') = k$!

$m_2' = m_2 k$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

(45)

Turing 'code V2:

Beforehand: exchange: a public prime p, a secret prime e k $k \in \{0, 1, \cdots, p-1\}$

Encryption: message as a number $m \in \{0, 1, \cdots p-1\}$

compute $m' = rem(mk, p)$

m not need to be prime

Decryption: ? ⇒

from LEC4: a, b relatively prime iff $gcd(a,b)=1$ iff $\exists s,t$, $sa+tb=1$

congruent

Def x is congruent to y modulo n: $x \equiv y \pmod n$ iff $n \mid (x-y)$

Ex: $31 \equiv 16 \pmod 5$ ← ($31-16=5$, $5 \mid 5$ ✓)

Def The multiplicative inverse of x mod n is a number x^{-1}, in $\{0, 1, \cdots, n-1\}$ s.t. $x \cdot x^{-1} \equiv 1 \pmod n$

Ex: $2 \cdot 3 \equiv 1 \pmod 5$

$2 \equiv 3^{-1} \pmod 5$, $3 \equiv 2^{-1} \pmod 5$

$5 \cdot 5 \equiv 1 \pmod 6$ $(4 \cdot 6 + 1 = 25)$, $5 \equiv 5^{-1} \pmod 6$

Ex: 3 is a multiplicative inverse of 7, since $7 \cdot 3 \equiv 1 \pmod 5$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

Congruent

$\Rightarrow$ $rem(mk, p) \equiv mk \pmod p$

$p \mid rem(mk, p) - mk$

$\downarrow$

$q \cdot mk - p \Rightarrow p \mid (q-1)mk - p$

encryption

V2: $m' = rem(mk, p) \equiv mk \pmod p$

If $k \cdot k^{-1} \equiv 1 \pmod p$, then $m'k^{-1} \equiv mk \cdot k^{-1} \pmod p$

$mk^{-1} \equiv m \pmod p$ ($k \cdot k^{-1} = 1$)

$\rightarrow \equiv m \pmod p \Rightarrow m = rem(m'k^{-1}, p)$

$\downarrow$ $(q \cdot m'k^{-1} - p)$

$\in \{0, 1, \cdots, p-1\}$ $(p \mid m - m'k^{-1})$

the note in LEC5

textbook read note (2025.3.2)

Lemma: Congruences and Remainders

$a \equiv b \pmod n$ iff $rem(a, n) = rem(b, n)$

ex: $29 \equiv 15 \pmod 7$ $rem(29, 7) = 1 = rem(15, 7)$

proof: $a - b = (q_1 - q_2)n + (r_1 - r_2)$; $-n < r_1 - r_2 < n$

iff $a \equiv b \pmod n \Rightarrow$ left side divides n

$\Rightarrow r_1 - r_2$ is multiply by $n \Rightarrow r_1 - r_2 = 0$, $r_1 = r_2$

it means $rem(a, n) = rem(b, n)$

Mo Tu We Th Fr Sa Su

Memo No.

Date 03/02/2025

text book read in 3.2

Corollary 4.5.2 $a \equiv rem(a,n) \pmod n$

$n \mid a - qn - a = -q$ ✓

Lemma 4.6.2 *if p is prime and k is not a multiple of p, then k has a multiplicative inverse modulo p*

$\Rightarrow tk \equiv 1 \pmod p$ $(k^{-1}=t)$

Turing's Code V2

$m' = rem(mk, p) = mk - qp$

$m = rem(m'k^{-1}, p) = m'k^{-1} - qp$

$m' = rem(mk, p) \equiv mk \pmod p$ ↑ C 4.5.2

$m'k^{-1} \equiv m \pmod p$

it shows $m'k^{-1}$ is congruent to the orignal message m, $(p \mid -m + m'k^{-1})$, because m was in the set $\{0, \dots p-1\}$, $m<p$, so $m = rem(m'k^{-1}, p)$

$m'k^{-1} \equiv m \pmod p$ means p divide $m'k^{-1} - m$

$rem(m'k^{-1}, p) = m'k^{-1} - p$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

$$\frac{m'k^{-1}-m}{q\cdot p}=q \Rightarrow m'k^{-1}-pq=m$$

(2) so $m=rem(m'k^{-1},p)=m'k^{-1}-qp$ ✓

self-step: the decrypt of Turing's V2

$m^*=rem(mk,p)=mk-q\cdot p$ Encrypt

$rem(mk,p)\equiv mk \pmod p \Rightarrow m^*\equiv mk \pmod p$

↑ (from Corollary 4.5.2) ↖ (why) ↗

$\Rightarrow [\, mk-qp\equiv mk \pmod p,\ (p \mid mk-qp-mk)=q \,]$

$m^*k^{-1}\equiv m \pmod p$, $m^*k^{-1}-m=q\cdot p$

$\Rightarrow m=m^*k^{-1}-qp=rem(m^*k^{-1},p)$ ✓ Decrypt

THE PROSS OF TURING'S CODE V2

then from Lemma 4.6.1, t is the value of k^{-1}, and it's must exist when k is not a multiply of p when p is prime, $k^{-1}=t$, $tk\equiv 1 \pmod p$

(1) p is the public key, which is a large prime

k is a secrect key $\in\{1,2,\cdots p-1\}$

message m can be any interger in the set $\{0,1,2,\cdots p-1\}$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

$$\frac{m'k^{-1}-m}{q\cdot p}=q \Rightarrow m'k^{-1}-pq=m$$

② so $m=rem(m'k^{-1},p)=m'k^{-1}-qp$ ✓

self-step: the decrypt of Turing's V2

$m^*=rem(mk,p)=mk-q\cdot p$ Encrypt

$rem(mk,p)\equiv mk \pmod p \Rightarrow m^*\equiv mk \pmod p$

(from Corollary 4.5.2) (why) ↴

$\Leftarrow [\, mk-qp \equiv mk \pmod p,\ (p \mid mk-qp-mk)=q \,]$

$m^*k^{-1}\equiv m \pmod p$, $m^*k^{-1}-m=q\cdot p$

$\Rightarrow m=m^*k^{-1}-qp=rem(m^*k^{-1},p)$ ✓ Decrypt

THE PROSS OF TURING'S CODE V2

then from Lemma 4.6.1, t is the value of k^{-1}, and it's must exist when k is not a multiply of p when p is prime, $k^{-1}=t$, $tk\equiv 1 \pmod p$

① p is the public key, which is a large prime

k is a secrect key $\in \{1,2,\cdots p-1\}$

message m can be any interger in the set $\{0,1,2,\cdots p-1\}$

Mo Tu We Th Fr Sa Su Date / /

Cancellation

Lemma 4.6.2 Suppose p is a prime and k is not a multiple of p, then

$$ak \equiv bk \pmod{p} \Rightarrow a \equiv b \pmod{p}$$

$$\Rightarrow ak \cdot k^{-1} \equiv bk \cdot k^{-1} \pmod{p}$$

iff p is a prime and k is not a multiple of p has k^{-1} (lemma 4.6.1)

Corollary 4.6.3, $\uparrow$ p and k

$$\text{rem}(1 \cdot k, p), \text{rem}(2 \cdot k, p), \cdots, \text{rem}((p-1) \cdot k, p)$$

is a permutation (重組) of the sequence

$$1, 2, \cdots, (p-1)$$

because all $c \cdot k$ is not divides p, so the reminders are the range 1 to $p-1$

ex: $p=5$, $k=3$

$\text{rem}(3,5)$ $\text{rem}(2 \cdot 3, 5)$ $\text{rem}(3 \cdot 3, 5)$ $\text{rem}(4 \cdot 3, 5)$

$=3$ (3-0.5) $=1$ $=4$ $=2$

permutation of $1, 2, 3, 4$ $\{1, \cdots 5-1\}$ $p-1$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

Theorem 4.6.4 (Fermat's Little Theorem)

← p, k, $k^{p-1} \equiv 1 \pmod{p}$

proof (how to find k^{-1})

$(p-1)! = 1 \cdot 2 \cdots (p-1)$

$= rem(k, p) \cdot rem(k \cdot 2, p) \cdots rem((p-1)k, p)$

$\equiv k^{p-1} \cdot (p-1)! \pmod{p}$

from lemma 4.6.2 ⇒ $1 \equiv k^{p-1} \pmod{p}$

[$(p-1)!$ is not a mutiple of p]

⇒ $k^{p-1} \equiv 1 \pmod{p}$

$k^{p-2} \cdot k \equiv 1 \pmod{p}$, ~~$k^{p-2} = k^{-1}$~~

So k^{p-2} is a multiplicative inverse of k

so $k^{-1} = k^{p-2}$

Ex:

↳ find 6 (mod 17)'s multiplicative inverse

find $rem(6^{17-2}, 17) \Rightarrow rem(6^{15}, 17)$

$p = 17, \quad k = 6$ ~~$6^2 \equiv 36 \pmod{}$~~

$6^2 = 36 \equiv 2 \pmod{17}$ ⇒ $6^{15} \equiv 3 \pmod{17}$

$6^4 = 36^2 \equiv 4 \pmod{17}$ ⇒ $3 \cdot 6 \equiv 1 \pmod{17}$

$6^8 \equiv 16 \pmod{17}$

$6^{15} \equiv 16 \cdot 4 \cdot 2 \cdot 6 \pmod{17}$

↳ $64 \equiv 13 \cdot 2 \cdot 6 \equiv 9 \cdot 6 \equiv 3 \pmod{17}$

Mo Tu We Th Fr Sa Su

Memo No.

Date / /

$m^{\frac{p}{2}} \equiv mk \pmod p$

$m^{p-2} \cdot m^{\frac{p}{2}} = m^{p-2} \cdot rem(mk, p)$

$\equiv m^{p-2} \cdot mk \pmod p$

$\equiv m^{p-1} k \pmod p$

$\equiv k \pmod p$

RSA

Lemma 4.7.1 Let n be a positive integer. If k is relatively prime to n, then there exist an integer k^{-1} such that $k \cdot k^{-1} = 1 \pmod n$

⇒ Corollary 4.7.2 if $ak \equiv bk \pmod n$ then $a \equiv b \pmod n$

Lemma 4.7.3. $n \uparrow$ k is relatively prime to n, let $k_1, \cdots, k_r$ denote all the integers relatively prime to n in the range 1 to $n-1$. Then the sequence: $rem(k_1 \cdot k, n)$, $rem(k_2 \cdot k, n)$, $rem(k_3 \cdot k, n) \cdots$ $\cdots$, $rem(k_r \cdot k, n)$ is a permutation of the sequence: $k_1, k_2, \cdots, k_r$.

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

Euler's Theorem

Euler's ϕ function: $\phi(n)$

ex: $\phi(7)=6$, (1, 2, 3, 4, 5, 6 are relatively prime to 7)

$\phi(12)=4$, (1, 5, 7, 11)

$\gcd(a,b)=1 \Rightarrow$ relatively prime

If n is prime, then $\phi(n)=n-1$

Theorem 4.7.4. For any number n, if $p_1, p_2, \cdots p_i$ are the (distance) prime factors of n, then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_i}\right)$$

ex: $\phi(300) = \phi(2^2 \cdot 3 \cdot 5^2)$

$= 300 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= 80$

Corollary 4.7.5. Let $n=pq$ where p and q are different primes. Then $\phi(n)=(p-1)(q-1)$

Theorem 4.7.6. Suppose n is possitive integer and k is relatively prime to n. Then $k^{\phi(n)} \equiv 1 \pmod{n}$ ↑ textbook of NT II

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

Continue of LES note ↓ 2025.3.3

Known-plaintext attack:

known message m and encryption $m' = rem(mk, p)$

$\Leftarrow m' \equiv mk \pmod p$, p: public prime

gcd(m, p) = 1 ⇒ m, p are relative prime

compute $m \cdot m^{-1} = 1 \pmod p$

→ $m' m^{-1} \equiv k \cdot m \cdot m^{-1} \equiv k \pmod p$

$\pmod p \equiv 1 \pmod p$

so compute: $k^{-1} \pmod p$

Explain RSA With The fundemental number theory

Define (Euler's Toteent Function) $\phi(n)$ denotes the number of integers in $\{1, 2, 3, \cdots n-1\}$ that are relatively prime to n.

gcd(12, x) = 1

Example: n=12; ①, 2, 3, 4, ⑤, 6, ⑦, 8, 9, 10, ⑪, 12

so $\phi(12) = 4$

n=15: ① ② 3 ④ 5 6 ⑦ ⑧ 9 10 ⑪ 12 ⑬ ⑭ 15

$\phi(15) = 8$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

Euler's Theorem: if $\gcd(n,k)=1 \Rightarrow k^{\phi(n)} \equiv 1 \pmod n$

Pf **Lemma**: if $\gcd(n,k)=1$, then $ak \equiv bk \pmod n$

$\Downarrow$

$a \equiv b \pmod n$

$\Rightarrow$ k^{-1} multiply both sides

($\gcd(n,k)=1$, iff k has a multiplicative inverse)

Pf $\gcd(n,k)=1 \Leftrightarrow \exists s,t \ \ n\cdot s + k\cdot t = 1 \Leftrightarrow \exists t \ \ n \mid (kt-1)$

$\Leftrightarrow kt \equiv 1 \pmod n$

so t is the multiplicative inverse of k

Lemma: Suppose $\gcd(n,k)=1$

Let $k_1 \cdots k_r$ in $\{1, 2, 3, \cdots, n-1\}$ denote the integers relatively prime to n ($r=\phi(n)$)

Then $\{\text{rem}(k_1\cdot k, n), \cdots, \text{rem}(k_r\cdot k, n)\} = \{k_1, \cdots k_r\}$

① $\#=r$ ② $\#=r$

Pf ①: $\text{rem}(k_i\cdot k, n) = \text{rem}(k_j\cdot k, n)$ iff $i=j$

$\Rightarrow k_i k \equiv k_j \cdot k \pmod n$

$\Rightarrow k_i \equiv k_j \pmod n$ $\quad n \mid k_i - k_j$ iff $k_i - k_j = 0$

$\Rightarrow k_i = k_j$ because k_i & $k_j \in [1, n-1]$

Mo Tu We Th Fr Sa Su

Memo No.

Date / /

② : ~~gcd(n, rem(k_i, k·n)) = gcd(n, k_i k)~~

gcd(n, rem(k_i·k, n)) = gcd(n, k_i k) = 1

this means k_0 is relatively prime to n

↳ $\equiv k_i k \pmod n$ (同余)

(~~Euler's~~ Euclidean Alg)

⇒ rem(k_i k, n) is r. relatively primes to n

so showed ✓

Pf of (Euler's Theory)

from Lemma

$1 \cdot k_1 \cdot k_2 \cdots k_r \equiv rem(k_1 k, n) \cdots rem(k_r k, n)$

$\equiv k_1 k \; k_2 \cdot k \cdots k_r \cdot k \pmod n$

$\equiv k_1 \cdots k_r \cdot k^r \pmod n$

a = a, b = b

so $1 \equiv k^r \pmod n$ and $r = \phi(n)$ (From lemma)

then proved! if gcd(n, k) = 1, $k^{\phi(n)} \equiv 1 \pmod n$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

The RSA Algorithm

Fermat (Little Theorem): Suppose p is prime and $k \in \{1, 2 \cdots, p-1\}$, Then $k^{p-1} \equiv 1 \pmod p$

Pf $1, 2 \cdots, p-1$ are relatively prime to p

$k^{\phi(p)} \equiv 1 \pmod p$ ↑ $\phi(p) = p-1$

so $k^{p-1} \equiv 1 \pmod p$

$\Rightarrow k \cdot k^{p-2} \equiv 1 \pmod p$. so k^{p-2} is actually $k^{-1} \pmod p$

RSA

beforehand: receiver create public key and secrect key

1. Generate two distinct p and q (prime)
2. let $n = p \cdot q$
3. Select e, $\gcd(e, (p-1)(q-1)) = 1 \Rightarrow$ publickey is the pair (e, n)
4. Compute d st. $d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$

The seerect key is the pair (d, n)

Encryption: $m' = \text{rem}(m^e, n)$

Decryption: $m = \text{rem}((m')^d, n)$

why this work? $n \mid m^e - qn - m^e$

$m' = \text{rem}(m^e, n) \equiv m^e \pmod n \Rightarrow (m')^d \equiv m^{ed} \pmod n$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

$\exists r$ $ed = 1 + r\cdot(p-1)(q-1)$ $(p-1)(q-1) \mid de-1 = r$

$\uparrow$ $de \equiv 1 \pmod{(p-1)(q-1)}$ $de = r\cdot(p-1)(q-1)+1$

So $(m')^d \equiv m^{ed} \pmod n \equiv m\cdot m^{r(p-1)(q-1)} \pmod n$

$1+r(p-1)(q-1)$

$n = p\cdot q$

if $m \not\equiv 0 \pmod p$ then $m^{p-1} \equiv 1 \pmod p$ ✓

$m^{\phi(p)} \equiv 1 \pmod p$ ↑ (emma

if $m \not\equiv 0 \pmod q$ ... $m^{q-1} \equiv 1 \pmod q$ ✓

So. $(m')^d \equiv m\cdot m^{r(p-1)(q-1)} \pmod p$ $n = pq \Rightarrow p \mid pq$ ✓

and $(m')^d \equiv m\cdot m^{r(p-1)(q-1)} \pmod q$ $q \mid pq$

$m^{(p-1)}\cdot m^{r(q-1)} \equiv 1 \pmod p$

$(m')^d \equiv m \pmod p$ $\}$ $p \mid (m')^d - m$

$(m')^d \equiv m \pmod q$ $\}$ $q \mid (m')^d - m$

so $q\cdot p \mid (m')^d - m$ ←

$\Rightarrow (m')^d \equiv m \pmod n$ $n = p\cdot q$

$(m \in \{0, \dots n-1\})$

So $m = \text{rem}((m')^d, n)$ ←

$\frac{(m')^d - m}{n} = q$

$m = (m')^d - n\cdot q$

$= \text{rem}((m')^d, n)$

✓

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

$q \mid m^{q-1}-1$, $p \mid m^{p-1}-1$

$(m^{p-1})^{r(q-1)} \equiv (1)^{r\cdot q-1} \pmod{p}$

$\Rightarrow m^{r(p-1)(q-1)} \equiv 1 \pmod{p} \Rightarrow (m')^d \equiv m \pmod{p}$

same reason: $(m')^d \equiv m \pmod{q}$

$\begin{cases} p \mid (m')^d - m \\ q \mid (m')^d - m \end{cases}$ so $q \cdot p \mid (m')^d - m$

$\Rightarrow (m')^d \equiv m \pmod{q \cdot p}$ $\quad m = q \cdot n (m')^d - q \cdot n$

$\Rightarrow m = rem((m')^d, n)$ ✓