1) Number Theory Part 3 → hon PB3 due next week

- hon PB3 very easy vs hPB 1,2
- hon PB3 require math rigor solution (and writing)

- Number Theory Part 4 (optional) Lecture around Crypto, Encryption (RSA). THXGV

Modulo multiplicative inverse

(a, n) coprimes $\iff \gcd(a, n) = 1$ no primes in common

$\iff$ a has inverse mod n

inverse = "a^{-1}"

$a \cdot a^{-1} = 1 \mod n \iff a \cdot a^{-1} = n \cdot k + 1$

k: generic integer

example

4 mod 15 has inverse $\gcd(4, 15) = 1$

$4^{-1} = 4 \qquad 4 \cdot 4 = 16 = 1 \mod 15$

6 mod 26 has no inverse $\gcd(6, 26) \neq 1$

There is <u>no</u> 6^{-1} $6^{-1} \cdot 6 = 1 \mod 26$

How to find inverse when exists?

1) multiply with itself until get 1

$a^v \equiv 1 \mod n$ $a^{-1} = a^{v-1}$ inverse

$v =$ multiplicative order ($a \bmod n$)

2) Extended Euclid Algorithm (a, b)

- Finds $d = GCD(a, b)$ just like simple-Euclid

- Finds $x, y \in \mathbb{Z}$

coef

$$\boxed{x \cdot a + y \cdot b = d = GCD}$$

(no modulo)

1) th a, n integers

$\exists v$ = order $a^v \equiv 1 \mod n \iff \gcd(a,n) = 1$ coprimes.

proof: $\Rightarrow$ easy

$a^v = 1 \mod n \Rightarrow \gcd(a,n) = 1$

assume (hypoth) $\boxed{d = \gcd(a,n) \neq 1} \Rightarrow d \mid a,\ d \mid n$

$a^v = 1 \mod n \Rightarrow a^v = nk + 1 \Rightarrow a^v - nk = 1$

$$\left.\begin{array}{l} d \mid a \Rightarrow d \mid a^v \\ d \mid n \Rightarrow d \mid n \cdot k \end{array}\right\} \Rightarrow d \mid \underline{a^v} - \underline{nk} \Rightarrow d \mid 1$$

contradict

proof: $d = \gcd(a,n) = 1 \Rightarrow \exists v \quad a^v \equiv 1 \mod n$.

$P(a) = \{a, a^2, a^3, a^4, \ldots\} \mod n$ set of a powers

- group

$P(a)$ cannot be infinite (mod n are only n values)

$\Rightarrow$ some powers same remainder mod n

$$a^t \equiv a^u \mod n \qquad t > u$$

$$a^t - a^u \equiv 0 \mod n \Rightarrow n \mid (a^t - a^u)$$

no factors in common

$$\Rightarrow n \mid a^u \cdot (a^{t-u} - 1)$$

$\gcd(n, a^u) = 1 \Rightarrow n, a^u$ no common factors

$$\Rightarrow n \mid (a^{t-u} - 1) \Rightarrow a^{t-u} \equiv 1 \mod n$$

$$v = t - u$$

② Find a^{-1} with extended Euclid procedure

Simple Euclid

1 $a, b \rightarrow q_1, r_1$ $(a = bq + r)$ $r \in \{0, 1, \dots, b-1\}$

2 $b\ r_1 \rightarrow q_2, r_2$ $b = r_1 \cdot q_2 + r_2$ $r_2 \in \{0, 1, \dots, r_1 - 1\}$

3 $r_1\ r_2 \rightarrow q_3\ r_3$ $r_1 = r_2 \cdot q_3 + r_3$ $r_3 \in \{0, 1, \dots, r_2 - 1\}$

$- - - -$

last "b"

t $r_{n-1}\ \boxed{r_n} \rightarrow q_{n+1}\ \boxed{r_{n+1} = 0}$

process

last remainder $\neq 0$

GCD

$x_k = y_{k+1}$

$y_k = x_{k+1} - q\, y_{k+1}$

$x = y_{prev}$

$y = x_{prev} - q \cdot y_{prev}$

last row $b = GCD$

$x = 0 \quad y = 1$

$a \cdot x + b \cdot y = gcd$

x_1

coef

a	b	q	r	$x = y_{prev}$	$y = x_{prev} - q \cdot y_{prev}$	verify
22	6	3	4	-1	$1 - 3\cdot(-1) = 4$	$22(-1) + 6\cdot 4 = 2$ ✓
6	4	1	2	1	$0 - 1\cdot 1 = -1$	$6\cdot 1 + 4(-1) = 2$ ✓
4	$\boxed{2}$	2	0	0	1	$4\cdot 0 + 2\cdot 1 = 2$ ✓

GCD

$ax + by = \gcd$

a	b	q	r	x	y	verify
51	9	5	6	-1	$1-5(-1)=6$	$51(-1)+9\cdot 6=3$ ✓
9	6	1	3	1	$0-1\cdot 1=-1$	$9\cdot 1+6(-1)=3$ ✓
6	$\boxed{3}$	2	0	0	1	$0\cdot 6+1\cdot 3=3$ ✓

GCD

Why x, y update works?

x, y not unique

$a = b\cdot q + r$

want $ax + by = \gcd$

know (prev line) b, r

$b\cdot x_{prev} + r\cdot y_{prev} = \gcd$

$x = ?$

$y = ?$

exercise

$x = y_{prev}$

$y = x_{prev} - q\cdot y_{prev}$