

RECAP

Division theorem: $\forall a \in \mathbb{Z}, n \in \mathbb{N}^+ \exists! q, r: a = qn + r, 0 \leq r < n$

$$q = \lfloor a/n \rfloor, r = a \bmod n$$

GCD: $\gcd(a, b) = \min \{d > 0 \mid \exists x, y \in \mathbb{Z}: d = ax + by\}$
 $(|a| + |b| > 0)$

Bézout's identity:

$$\gcd(a, b) = \min \{d > 0 \mid \exists x, y \in \mathbb{Z}: d = ax + by\}$$

Euclid's algorithm: $\gcd(a, b) \rightsquigarrow \gcd(b, a \bmod b)$

Extended Euclid: $\rightsquigarrow (\gcd(a, b), (x, y))$

$\xrightarrow{\text{Bézout's coefficients}}$

MODULAR ARITHMETIC

Operator $r = a \bmod n$ is defined by the division theorem:

$\forall a \in \mathbb{Z}, n > 0: \exists! q, r: a = q \cdot n + r$
 $q = \lfloor a/n \rfloor \in \mathbb{Z}, 0 \leq r < n, r = a \bmod n$

operator mod: $\mathbb{Z} \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \cup \{0\}$

BASIC PROPERTIES

$\forall a, b \in \mathbb{Z}, m > 0:$

$$m_1 (a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$$

$$m_2 (ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

(distributivity of mod w.r.t. + and ·)

$$m_3 (a \bmod m) = (b \bmod m) \Leftrightarrow \exists k \in \mathbb{Z}: a - b = km$$

m₄ For $m, n > 0:$

$$m \mid n \Rightarrow (x \bmod n) \bmod m = x \bmod m$$

m₁–m₄ have simple PROOFS based on the division theorem. Here we prove m₄ (the rest as EXERCISE):

Let $x = qm + r, 0 \leq r < m$ ($r = x \bmod m$)

$\hookrightarrow r = q'm + r', 0 \leq r' < m$ ($r' = (x \bmod m) \bmod m$)

$\hookrightarrow x = q''m + r'', 0 \leq r'' < m$ ($r'' = x \bmod m$)

M₄: need to show that $r' = r''$ if $m \mid n$!

Since $m \mid n$: $\exists k \in \mathbb{Z}^+: n = km$. Thus

a) $x = qm + r = q \cdot k \cdot m + q'm + r' = (qk + q')m + r'$

b) $x = q''m + r''$

By uniqueness: $(qk + q') = q''$, and $r' = r''$

We can define the congruence relation!

$$\forall a, b \in \mathbb{Z}: a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$$

Congruence modulo n is an equivalence relation over $\mathbb{Z} \times \mathbb{Z}$, since:

- $a \equiv a \pmod{n}$ (reflexive)
- $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$ (symmetric)
- $(a \equiv b \pmod{n}) \wedge (b \equiv c \pmod{n}) \Rightarrow (a \equiv c \pmod{n})$ (transitive)

QUOTIENT STRUCTURES

Any equivalence relation over $\mathbb{Z} \times \mathbb{Z}$ partitions \mathbb{Z} into equivalence classes. Under congruence mod n, each equivalence class is made of all integers x with the same value of $x \pmod{n}$.

There are n classes (corresponding to reminders $r=0, 1, \dots, n-1$)

DEF $\forall a \in \mathbb{Z}$, let $[a]_n$ be its equivalence class : $[a]_n = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$

Since $0, 1, \dots, n-1$ belong to distinct classes, we can use these numbers as principal representatives of the classes

DEF The congruent structure \mathbb{Z}_n is
 $\mathbb{Z}_n = \{[a]_n : 0 \leq a \leq n-1\}$

Elements of $[\bar{a}]_n$: every integer $x \in [\bar{a}]_n$ is s.t. $x \bmod n = \bar{a} \bmod n$

$$\xrightarrow{\text{M3}} \exists k \in \mathbb{Z} : x - \bar{a} = kn \Rightarrow x = \bar{a} + kn$$

thus: $[\bar{a}]_n = \{\bar{a} + kn : k \in \mathbb{Z}\}$

Each equality class is an arithmetic progression

OPERATIONS OVER \mathbb{Z}_n : \oplus, \odot

We define:

$$[\bar{a}]_n \oplus [\bar{b}]_n = [\bar{a} + \bar{b}]_n$$

$$[\bar{a}]_n \odot [\bar{b}]_n = [\bar{a}\bar{b}]_n$$

These operations are well defined because they do not depend on the class' representatives:

In fact $(\bar{a} + k_1 n + \bar{b} + k_2 n) \bmod n = (\bar{a} + \bar{b}) \bmod n$
 $(\bar{a}k_1 n)(\bar{b}k_2 n) \bmod n = (\bar{a}\bar{b}) \bmod n$ PROVE IT

CONVENTION: When working in \mathbb{Z}_n we will drop the $[\cdot]_n$ notation, but simply use \bar{a} . We will mostly use principal representatives $0, 1, \dots, n-1$ for each equality class. Also, we will use $+$ and \cdot rather than \oplus and \odot , using the principal representative of the result's class: e.g., $[\bar{a}]_n \oplus [\bar{b}]_n \rightsquigarrow (\bar{a} + \bar{b}) \bmod n$

IMPORTANT: This is just NOTATIONAL CONVENIENCE. When working in \mathbb{Z}_n it must be clear that each x represents the (infinite) class $[x]_n$

GROUP PROPERTIES OF QUOTIENT STRUCTURES

$(\mathbb{Z}_n, +)$ is an additive group

- closure of $+$: $a+b \equiv (a+b) \text{ mod } n \in \mathbb{Z}_n$
- associativity (commutativity: ABELIAN group)
- neutral element: $0 (\equiv [0]_n)$ $a+0=0+a=a$
- inverse (opposite): $[a]_n^{-1} = -a \text{ mod } n$
 $a+(-a) \equiv (a-a) \text{ mod } n = 0 \text{ mod } n = 0$

Is (\mathbb{Z}_n, \circ) a multiplicative group?

- closure and associativity: OK
- neutral element: $1 (a \cdot 1 = a)$

But 0 cannot have an inverse!

$$\nexists a \in \mathbb{Z}_n : a \cdot 0 = 1$$

$$\text{Since } [a]_n \circ [0]_n = [a \cdot 0]_n = [0]_n \quad \forall a \in \mathbb{Z}$$

Is $(\mathbb{Z}_n^+ = \mathbb{Z}_n - [0]_n, \circ)$ a group? **NOT NECESSARILY!** It depends on n !

For some values of n , $\exists a \in \mathbb{Z}_n^+$:

$$\nexists a^{-1} \in \mathbb{Z}_n^+ : a \cdot a^{-1} = 1 !$$

EXAMPLE In $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, 2 has no inverse:

$$2 \cdot 0 = 0, 2 \cdot 1 = 2, 2 \cdot 2 = 0, 2 \cdot 3 = 2$$
$$[0]_4 \quad [2]_4 \quad [0]_4 \quad [2]_4$$

However, if we can define an important subset of \mathbb{Z}_n^+ which is a multiplicative group:

DEF $\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n : \gcd(a, n) = 1 \}$

In order to be sound, the definition must be independent of the representative.

In other words:

if $a \in \mathbb{Z}_n^* : \forall b = a + kn \in [a]_n : \gcd(b, n) = 1$

This can be easily proved by Bezout's id.:

$$\begin{aligned} a \in \mathbb{Z}_n^* \Rightarrow \gcd(a, n) = 1 \Rightarrow \\ \exists x, y : 1 = ax + ny \\ = ax + knx - knx + ny = \\ = (a + kn)x + (y - kx)n \end{aligned}$$

Since 1 is the least positive integer linear combination of $a + kn$ and n , we have:

$$\gcd(a + kn, n) = 1$$

The definition is independent of the representative

PROPERTY (\mathbb{Z}_n^*, \cdot) is a multiplicative group

- Closure: $a, b \in \mathbb{Z}_n^* \Rightarrow a \cdot b \in \mathbb{Z}_n^*$

By Bezout: $1 = ax_1 + ny_1 = bx_2 + ny_2$

$$\Rightarrow 1 = (ax_1 + ny_1)(bx_2 + ny_2)$$

$$\Rightarrow 1 = ab(\underbrace{x_1 x_2}_{\bar{x}}) + n(\underbrace{ax_1 y_2 + bx_2 y_1 + ny_1 y_2}_{\bar{y}})$$

$$\Rightarrow 1 = ab\bar{x} + n\bar{y}$$

Since 1 is the least positive integer linear combination of ab and n , we have:

$$\gcd(ab, n) = 1 \Rightarrow ab \in \mathbb{Z}_n^*$$

- Inverse. Let $a \in \mathbb{Z}_n^*$, I have to determine $b \in \mathbb{Z}_n^*$ such that $(a \cdot b) \bmod n = 1$
(conventionally, $b \stackrel{\text{def}}{=} a^{-1}$) $\Leftrightarrow [b]_n = [a]_n^{-1}$

Since $a \in \mathbb{Z}_n^*$: $\gcd(a, n) = 1 \Rightarrow$

$$\exists x, y \in \mathbb{Z} : 1 = ax + ny \quad (\Rightarrow \text{also } \gcd(x, n) = 1)$$

Let us take the mod of both sides:

$$\begin{aligned} 1 \bmod n &= (ax + ny) \bmod n \\ &\stackrel{\text{mod}}{=} ((ax) \bmod n + (ny) \bmod n) \bmod n \\ &= ax \bmod n \end{aligned}$$

Thus $ax \bmod n = 1 \Rightarrow [x]_n = [a]_n^{-1}$

Therefore $a^{-1} \equiv x \pmod{n}$ (to use the principal representative of $[x]_n$)

IMPORTANT e^{-1} can be computed through
 $\text{EE}(e, n) \rightarrow \{1, (x, y)\} : 1 = ex + ny$

INVERSE(e, n) $\{e \in \mathbb{Z}_n^*\}$

$\{1, (x, y)\} \in \text{EE}(e, n)$
 return $x \bmod n$

EXERCISE Show uniqueness of e^{-1} in \mathbb{Z}_n^*
 (needed in the proof:

$(eb \mid n) \wedge (\gcd(e, n) = 1) \Rightarrow b \mid n$) PROVE IT

EXAMPLE $[4]_15^{-1} \quad 4 \in \mathbb{Z}_{15}^*$

Since $\gcd(4, 15) = 1 : 4 \in \mathbb{Z}_{15}^*$

$\text{EE}(15, 4) \rightarrow \{1, (-1, 1 - 15/4)(-1) = (-1, 4)\}$

$\text{EE}(4, 3) \rightarrow \{1, (1, -14/3 \cdot 1) = (1, -1)\}$

$\text{EE}(3, 1) \rightarrow \{1, (0, 1)\}$

$\text{EE}(1, 0) \rightarrow \{1, (1, 0)\}$

Thus $1 = 15(-1) + 4 \cdot (4)$

Therefore in \mathbb{Z}_{15}^* : $4^{-1} = 4$

Indeed: $4 \cdot 4 = 16 \equiv 1 \pmod{15}$

IMPORTANT CASE If p is prime:

$\forall e \in \{1, 2, \dots, p-1\} : \gcd(e, p) = 1$

$\Rightarrow \mathbb{Z}_p^* = \{1, 2, \dots, p-1\}, |\mathbb{Z}_p^*| = p-1$

EULER'S FUNCTION $\varphi(n)$:

$$\forall n \in \mathbb{Z}^+ : \varphi(n) = |\mathbb{Z}_n^*| = |\{k \in \mathbb{Z}^* : (1 \leq k \leq n-1) \wedge \gcd(k, n) = 1\}|$$

NOTE: $\varphi(n) = n-1$ for n prime

PROPERTIES (no proof)

- $\varphi(p^k) = (p-1)p^{k-1}$, p prime
- $\gcd(p, q) = 1 \Rightarrow \varphi(pq) = \varphi(p)\varphi(q)$
- $\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$

NOTE! In order to be able to compute $\varphi(n)$ efficiently, we must know the prime factors of n : COMPUTATIONALLY DIFFICULT!

EULER'S THEOREM (crucial for RSA)

$$\forall n > 1, \forall a \in \mathbb{Z}_n^* : a^{\varphi(n)} = \underbrace{a \cdot a \cdot \dots \cdot a}_{\varphi(n) \text{ times}} = 1$$

(no proof). In other words:

$$\gcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \pmod{n} = 1$$

Important corollary of Euler's theorem :

FERMAT'S LITTLE THEOREM

If P is prime : \mathbb{Z}_P^+

$$\forall a \in \mathbb{Z}_P - \{0\} = \{1, 2, \dots, P-1\}$$

$$a^{P-1} \equiv 1 \pmod{P} \quad (a^{P-1} \equiv 1 \pmod{P})$$

PROOF

For prime P , $\phi(P) = P-1$ and

$\mathbb{Z}_P^* = \mathbb{Z}_P - \{0\}$. Apply Euler's theorem.

