RECAP

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

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

GCD: $\gcd(a,b) = \max\{d > 0 : (d \mid a) \wedge (d \mid b)\}$

$(|a| + |b| > 0)$

Bezout'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: $\rightsquigarrow (\gcd(a,b), (x,y))$

Bezout's coefficients

MODULAR ARITHMETIC

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

$\forall a \in \mathbb{Z}, \; n > 0 : \exists! \; q, r : a = q \cdot n + r$

$q = \lfloor a/n \rfloor \in \mathbb{Z}, \; 0 \le r < n, \; r = a \bmod n$

operator $\bmod : \mathbb{Z} \times \mathbb{Z}^+ \to \mathbb{Z}^+ \cup \{0\}$

BASIC PROPERTIES

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

M1 $(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$

M2 $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

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

M3 $(a \bmod m) = (b \bmod m) \Leftrightarrow \exists k \in \mathbb{Z} : a - b = km$

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 $a = qm + r$, $0 \le r < m$ ($r = x \bmod n$)

$r = q'm + r'$, $0 \le r' < m$ ($r' = (x \bmod n) \bmod m$)

$a = q''m + r''$, $0 \le r'' < m$ ($r'' = x \bmod m$)

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

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

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

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

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

We can define the congruence relation:

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

a congruent to b modulo n

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

- $a \equiv a \bmod n$ (reflexive)
- $a \equiv b \bmod n \Leftrightarrow b \equiv a \bmod n$ (symmetric)
- $(a \equiv b \bmod n) \wedge (b \equiv c \bmod n) \Rightarrow (a \equiv c \bmod n)$ (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 $x \bmod n$.

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

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

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

$$\mathbb{Z}_n = \{[a]_n : 0 \le a \le n-1\}$$

Elements of $[a]_m$: any integer $x \in [a]_m$ is s.t. $x \bmod m = a \bmod m$

$\overset{m3}{\Rightarrow}$ $\exists k \in \mathbb{Z} : x - a = km \Rightarrow x = a + km$

Thus: $[a]_m = \{a + km : k \in \mathbb{Z}\}$

Each equivalence class is an arithmetic progression

OPERATIONS OVER $\mathbb{Z}_m$: $\oplus$, $\odot$

We define:

$$[a]_m \oplus [b]_m = [a+b]_m$$
$$[a]_m \odot [b]_m = [ab]_m$$

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

In fact $(a + k_1 m + b + k_2 m) \bmod m = (a+b) \bmod m$

$((a + k_1 m)(b + k_2 m)) \bmod m = (ab) \bmod m$

PROVE IT

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

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

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

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

  $a + (-a) = (a-a) \bmod n = 0 \bmod n = 0$

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

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

But 0 cannot have an inverse!

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

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

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

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

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

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

$2 \cdot 0 = 0$, $2 \cdot 1 = 2$, $2 \cdot 2 = 0$, $2 \cdot 3 = 2$

$[0]_4$ $[2]_4$ $[0]_4$ $[2]_4$

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

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

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.:

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

$\exists x, y : 1 = ax + ny$

$= ax + knx - knx + ny =$

$= (a + kn)x + (y - kx)n$

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: $1 = ax_1 + ny_2 = bx_2 + ny_2$

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

$\Rightarrow 1 = ab\underbrace{(x_1x_2)}_{\bar{x}} + n\underbrace{(ax_1y_2 + bx_2y_2 + ny_1y_2)}_{\bar{y}}$

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

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, $b \stackrel{def}{=} a^{-1}$) $\leftarrow [b]_n = [a]_n^{-1}$

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

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

Let us take the mod of both side:

$$1 \bmod n = (ax + ny) \bmod n$$
$$\stackrel{m1}{=} \left((ax) \bmod n + \underbrace{(ny) \bmod n}_{0}\right) \bmod n$$
$$= ax \bmod n$$

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

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

IMPORTANT a^{-1} can be computed through

$EE(a,m) \to \{1, (x,y)\} : 1 = ax + my$

INVERSE(a,m) $\{a \in \mathbb{Z}_m^*\}$

$\{d, (x,y)\} \leftarrow EE(a,m)$

if $d = 1$ return $x \bmod m$

EXERCISE Show uniqueness of a^{-1} in $\mathbb{Z}_m^*$

(needed in the proof:

$(ab \mid m) \wedge (\gcd(a,m) = 1) \Rightarrow b \mid m$) PROVE IT

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

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

$EE(15,4) \to \{1, (-1, 1 - \lfloor 15/4 \rfloor (-1) = (-1,4)\}$

$EE(4,3) \to \{1, (1, -\lfloor 4/3 \rfloor \cdot 1) = (1,-1)\}$

$EE(3,1) \to \{1, (0,1)\}$

$EE(1,0) \to \{1, (1,0)\}$

$(\bar{x}, \bar{y}) \to (\bar{y}, x - \lfloor a/b \rfloor y)$

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

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

Indeed : $4 \cdot 4 = 16 \equiv 1 \bmod 15$

IMPORTANT CASE If p is a prime :

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

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

$\mathbb{Z}_p^* = \mathbb{Z}_p^+$

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

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

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)

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

(no proof) In other words:

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

Important corollary of Euler's theorem:

FERMAT'S LITTLE THEOREM

If p is prime: $\mathbb{Z}_p^+$

$$\forall a \in \mathbb{Z}_p - \{0\} = \{1, 2, \ldots, p-1\}$$

$$a^{p-1} = 1 \quad (a^{p-1} \bmod n = 1)$$

$$a^{p-1} \equiv 1 \bmod n$$

PROOF

For prime p, $\varphi(p) = p-1$ and $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$. Apply Euler's theorem.