CONGRUENCES AND MODULAR ARITHMETIC

(Defn) Let $m \in \mathbb{N}$ (modulus). $a, b \in \mathbb{Z}$ are congruent modulo m if $m \mid (a-b)$ or equivalently $a \text{ rem } m = b \text{ rem } m$

$a \equiv b \pmod{m}$

$a \in \mathbb{Z}$

Integers congruent to a modulo m: $a + km$, $k \in \mathbb{Z}$

Properties

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m}$ & $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

4. $a \equiv c \pmod m$ & $b \equiv d \pmod m$

$$\Rightarrow \begin{cases} a+b \equiv c+d \pmod m \\ a-b \equiv c-d \pmod m \\ ab \equiv cd \pmod m \end{cases} \longrightarrow \begin{aligned} a &= c+km \\ b &= d+\ell m \end{aligned}$$

$$ab = cd + (kd+\ell c)m + k\ell m^2$$

$$ab - cd = m(\cdot)$$

$$m \mid ab-cd \Rightarrow ab \equiv cd \pmod m$$

5. f: polynomial with integer coefficients

$a \equiv b \pmod m \Rightarrow f(a) \equiv f(b) \pmod m$

6. $a \equiv b \pmod m$, $d \mid m$ for $d \in \mathbb{N}$

then $a \equiv b \pmod d$

7. $ab \equiv ac \pmod m$ iff $b \equiv c \pmod{\frac{m}{\gcd(a,m)}}$

$a = kd \quad m = \ell d \quad d = \gcd(a,m)$

$\gcd(k,\ell) = 1$

$m \mid a(b-c)$

$\ell d \mid kd(b-c)$

$\Rightarrow \ell \mid k(b-c)$

$\ell \mid b-c$

$\Rightarrow b \equiv c \pmod \ell$

(Defn) Let $m \in \mathbb{N}$. $\{a_0, a_1, \ldots, a_{m-1}\} \subseteq \mathbb{Z}$ is a complete residue system modulo m if every $a \in \mathbb{Z}$ is congruent to exactly one integer a_i $(0 \le i \le m-1)$ modulo m

denoted $\mathbb{Z}_m$

$m = 5$

$\mathbb{Z}_5 = \{10, -9, 22, 3, -16\}$: complete residue system modulo 5

$10 \to 0$, $-9 \to 1$, $22 \to 2$, $3 \to 3$, $-16 \to 4$

$11 + 7 = 18 \equiv 3 \bmod 5$

$11 +_m 7 := 3$

Arithmetic in $\mathbb{Z}_m$

$a, b \in \mathbb{Z}_m$: $\exists$ a unique $c \in \mathbb{Z}_m$ s.t

$a \,(+/-/\cdot)\, b \equiv c \pmod m$

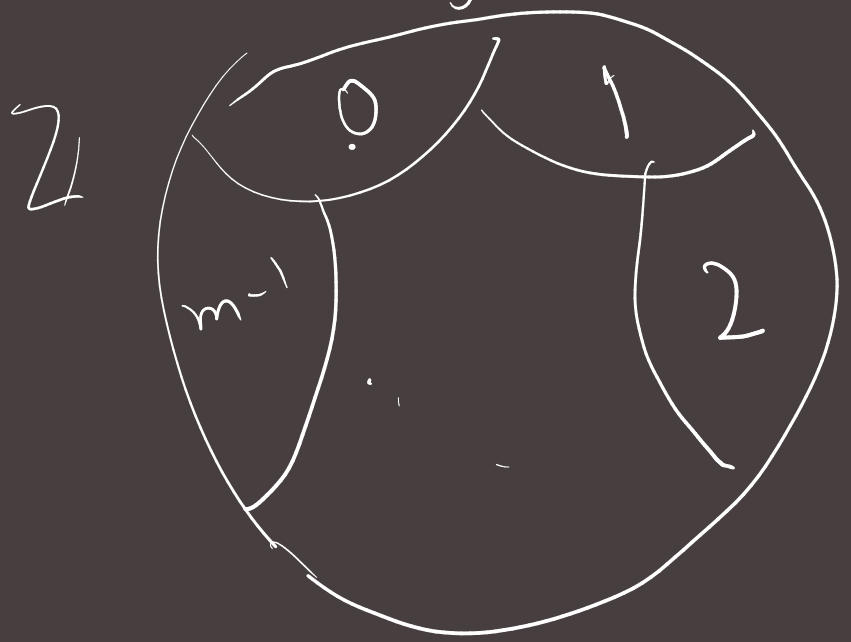
Sum/Difference/Product of a & b : c

$\mathbb{Z}$: integral domain (under $+, \times$ of integers)

$m\mathbb{Z}$: ideal of $\mathbb{Z}$

Algebraic description of $\mathbb{Z}_m$: $\mathbb{Z}/m\mathbb{Z}$

$\mathbb{Z}_m$: set of equivalence classes corresponding to relation 'congruence modulo m'



Most common representation of $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$

$$a+b \pmod m = \begin{cases} a+b & \text{if } a+b<m \\ a+b-m & \text{o.w.} \end{cases}$$

$$a-b \pmod m = \begin{cases} a-b & \text{if } a-b \geq 0 \\ a-b+m & \text{o.w} \end{cases}$$

$$ab \pmod m = ab \text{ rem } m$$

Arithmetic in $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

what about division?

$$a/b \bmod m : \quad a\boxed{b^{-1}} \pmod m$$

↓ multiplicative inverse of b modulo m.

(Dfn) An element $a \in \mathbb{Z}_m$ is said to be invertible modulo m if $\exists\ u \in \mathbb{Z}_m$ s.t. $ua \equiv 1 \pmod m$

↳ inverse of a mod m

(Thm) An element $a \in \mathbb{Z}_m$ is invertible iff $\gcd(a,m) = 1$

Proof

($\Rightarrow$) $a \in \mathbb{Z}_m$ is invertible

$\exists\, u \in \mathbb{Z}_m$ s.t. $au \equiv 1 \pmod m$

$au = km + 1$ for some $k \in \mathbb{Z}$

$1 = au - km$ (integer linear combination of a & m)

1 is the smallest +ve integer

$1 = \gcd(a, m)$

($\Leftarrow$) Suppose that $\gcd(a,m) = 1$

Bézout's relation $\Rightarrow \exists\, u, v \in \mathbb{Z}$ s.t. $au + mv = 1$

$\Rightarrow m \mid au - 1$ i.e., $au \equiv 1 \pmod m$

extended gcd algorithm can find u.

(Defn) $m \in \mathbb{N}$. $\{a_1, a_2, \cdots, a_\ell\} \subseteq \mathbb{Z}$ is called a reduced residue system modulo m if every integer a coprime to m is congruent to exactly one a_i $(1 \le i \le \ell)$

denoted $\mathbb{Z}_m^*$

$m = 9$ $\{1, 2, 4, 5, 7, 8\} = \mathbb{Z}_9^*$

$2^{-1} = 5$

$4^{-1} = 7$

$8^{-1} = 8$

Standard rep. of $\mathbb{Z}_m^*$

$\{a \mid 0 \le a \le m-1 \text{ and } \gcd(a, m) = 1\}$

(Algebraically) $\mathbb{Z}_m^*$ is the set of all units in $\mathbb{Z}_m$ & is a commutative group under multiplication modulo m.

(Defn) $\phi(m)$: size of reduced residue system modulo m

↓

Euler's phi/totient function.

(Thm) Let $m \in \mathbb{N}$ & $a \in \mathbb{Z}$ s.t. $\gcd(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Proof: $\{a_1, a_2, \ldots, a_{\phi(m)}\}$: reduced residue system modulo m.

$$\left.\begin{aligned} a a_1 &\equiv a_1' \pmod{m} \\ a a_2 &\equiv a_2' \pmod{m} \\ &\vdots \\ a a_{\phi(m)} &\equiv a_{\phi(m)}' \pmod{m} \end{aligned}\right\} \quad (a a_1)(a a_2) \cdots (a a_{\phi(m)}) \equiv \underbrace{a_1' a_2' \cdots a_{\phi(m)}'}_{\cdots (1)} \pmod{m}$$

a'_i is coprime to m (for all $i \in [1, \phi(m)]$)
(∵ a, a_i are both coprime to m).

$a'_i \not\equiv a'_j \pmod m$ for $i \neq j$

Suppose $a'_i \equiv a'_j \pmod m$

$$aa_i \equiv aa_j \pmod m$$
$$(a^{-1})aa_i \equiv (a^{-1})aa_j \pmod m$$
$$a_i \equiv a_j \pmod m$$

Contradiction!

$$\{a'_1, a'_2, \cdots, a'_{\phi(m)}\} = \mathbb{Z}_m^* \quad \text{i.e.,} \quad \underbrace{a_1 a_2 \cdots a_{\phi(m)}}_{b} \equiv a'_1 a'_2 \cdots a'_{\phi(m)} \pmod m$$

From (1) $a^{\phi(m)} b \equiv b \pmod m$ (multiply both sides with b^{-1})

$$a^{\phi(m)} \equiv 1 \pmod m$$

Fermat's little theorem

$p \in \mathbb{P}$. Let a be an integer not divisible by p.
Then $a^{p-1} \equiv 1 \pmod{p}$. Let $b \in \mathbb{Z}$. Then

$$b^p \equiv b \pmod{p}.$$

Proof: $\varphi(p) = p-1$ (all non-zero integers in $\mathbb{Z}_p$ are invertible)

Euler's thm $\Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$b \in \mathbb{Z}$ $\rightarrow p \mid b$ $\quad b^p \equiv b \equiv 0 \pmod{p}$

$\searrow p \nmid b$ $\quad b^{p-1} \equiv 1 \mod p$

$b^{p-1} b \equiv b \pmod{p}$

(Thm) : $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $\quad e_i > 0$ $\quad p_i$: distinct

$$\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

$$= \left(p_1^{e_1} - p_1^{e_1 - 1}\right)\left(p_2^{e_2} - p_2^{e_2 - 1}\right) \cdots \left(p_r^{e_r} - p_r^{e_r - 1}\right)$$

Proof : $\mathbb{Z}_{p_i^{e_i}} = \left\{ p_i^{e_i}, 1, 2, \ldots, p_i^{e_i} - 1 \right\}$

elements in $\mathbb{Z}_{p_i^{e_i}}$ divisible by p_i : $p_i, 2p_i, 3p_i, \ldots, (p_i^{e_i - 1})p_i$

$$\mathbb{Z}^*_{p_i^{e_i}} = \mathbb{Z}_{p_i^{e_i}} \setminus \{ \overbrace{p_i, 2p_i, \cdots (p_i^{e_i - 1})p_i}^{S} \}$$

$$\phi(p_i^{e_i}) = |\mathbb{Z}^*_{p_i^{e_i}}| = |\mathbb{Z}_{p_i^{e_i}}| - |S| = p_i^{e_i} - p_i^{e_i - 1}$$

Lemma: $m, n \in \mathbb{Z}^+$ $\gcd(m,n) = 1$

Then $\phi(mn) = \phi(m)\,\phi(n)$

$p_1^{e_1}, p_2^{e_2}, \ldots, p_r^{e_r}$ are pairwise co-prime

$$\phi(m) = \phi\left(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}\right) = \prod_{i=1}^{r} \phi\left(p_i^{e_i}\right) \quad \text{[from lemma]}$$

$$= \prod_{i=1}^{r} \left(p_i^{e_i} - p_i^{e_{i-1}}\right)$$

Proof of Lemma

$\mathbb{Z}_{mn}$	1	2	3	$\cdots$	m
	$m+1$	$m+2$	$m+3$		$2m$
	$\vdots$				
	$(n-1)m+1$	$(n-1)m+2$	$\cdots$		nm

In every row, $\exists$ exactly $\phi(m)$ integers coprime to m.

In column k, $\exists$ exactly $\phi(n)$ integers coprime to n.

Column $k \sim \mathbb{Z}_n$.

Column k: $0 \cdot m + k$

$1 \cdot m + k$

$\vdots$

$(n-1)\, m + k$

$0 \le i, j \le n-1, \quad i \neq j$

$im + k \not\equiv jm + k \pmod{n}$

Suppose not. $im + k \equiv jm + k \pmod{n}$

$n \mid (i-j)\, m$

But $\gcd(m, n) = 1$

$\therefore n \mid (i-j)$ i.e., $i \equiv j \pmod{n}$

contradicts choice of i, j

Column $k \sim \mathbb{Z}_n$.

$\phi(m)$ rows co-prime to m

In each such row, exactly $\phi(n)$ integers are coprime to n.

#elements co prime mn $=$ #elements co-prime to both m & n

$= \phi(m)\phi(n)$.