# Division Algorithm.

$a \in \mathbb{Z}$ & $b > 0$ a +ve integer

Then $\exists$ $q$ (quotient) & $r$ (remainder)

s.t. $\boxed{a = bq + r, \quad r < b.}$

Pf Exercise.

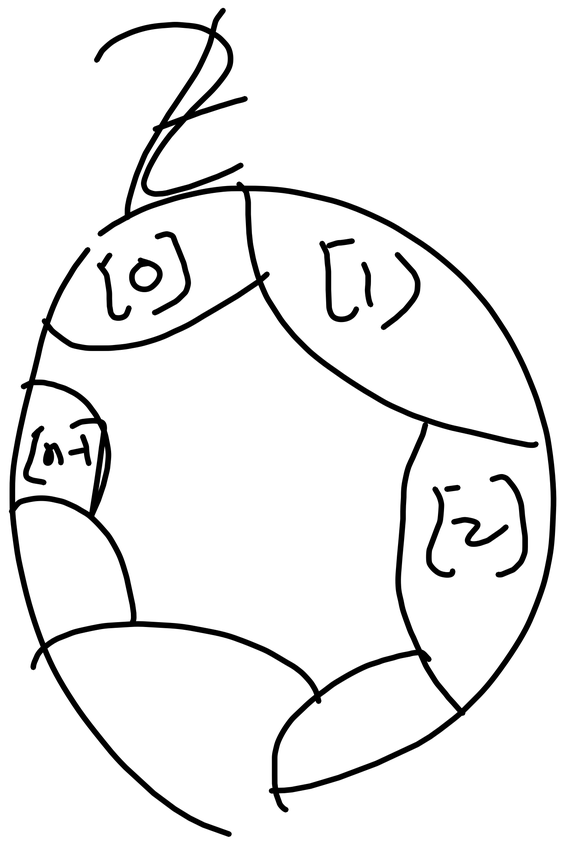
# Modular Arithmetic

Fix a +ve integer $n$.

Let $a, b \in \mathbb{Z}$. We write

$a \equiv b \bmod n$.

if $n \mid a-b$.



**Prop** If $a \equiv b \bmod n$
and $c \equiv d \bmod n$.
then $a+c \equiv b+d \bmod n$
$a \cdot c \equiv b \cdot d \bmod n$.

**Ex** If $p(x) \in \mathbb{Z}[x]$ and if $a \equiv b \bmod n$
then $p(a) \equiv p(b) \bmod n$.

**Ex** Let $x = a_{n-1} a_{n-2} \cdots a_0$ be an $n$-digit integer. Then $3 \mid x$ iff $3 \mid a_0 + \cdots + a_{n-1}$

$Z_n = \{0, 1, 2, \ldots, n-1\}$.

On $Z_n$ define $+_n$ as follows.

$a, b \in Z_n$.

$a +_n b$ is the unique integer $c \in Z_n$ s.t

$a + b \equiv c \mod n$.

$Z_7 = \{0, 1, 2, \ldots, 6\}$ $\quad 3 +_5 = 1$ in $Z_7$

## Multiplication.

Let $a, b \in \mathbb{Z}_n$. Then

$a \cdot b = c$ if

$c$ is the unique integer in $\mathbb{Z}_n$ s.t.

$ab \equiv c \pmod{n}$.

**Prop** $(\mathbb{Z}_n, +, \times)$ form a commutative ring.

# GCD Algorithm

**Defn.** Let $a, b \in \mathbb{Z}$. Then $d$ is the greatest common divisor (GCD) if:

(i) $d \mid a$ & $d \mid b$.

(ii) If $d'$ is a common divisor of $a+b$ then $d' \mid d$.

# Euclidean Algorithm.

Since $GCD(a,b) = GCD(|a|,|b|)$, assume $a,b$ non-negative. If $b=0$, then $GCD(a,b)=a$.

Assume $a,b>0$. w.l.s. assume $a \geq b$

Set $r_0 = a$, $r_1 = b$.

By div. algo. $\exists q_1 \geq r_2$ s.t.

$$\boxed{r_0 = r_1 q_1 + r_2}, \quad \boxed{r_2 < r_1}$$

$$r_1 = r_2 q_2 + r_3, \quad r_3 < r_2$$

$$r_{n-1} = q_n r_n + 0.$$

Claim $\gcd(a, b) = r_n$.

Prove by induction that

$$d = GCD(a,b) = GCD(r_i, r_{i+1})$$

$$r_0 = r_1 q_1 + r_2$$
$$r_1 = r_2 q_2 + r_3$$
$$\vdots$$
$$r_{n-1} = r_n q_n.$$

Trivially true for $i=0$.

Let $GCD(r_1, r_2) = d'$

Clearly, $d' \mid r_0$.

$\Rightarrow d' \mid d$.

$d \mid r_2$ Also $d \mid r_1$

$d \mid d$

EUCLID(a, b)

Input : non-negative integers a, b.

Output : GCD(a, b).

1. If $b = 0$ return $a$.

2. else return $(b, a \bmod b)$.

$a \bmod b$ = remainder obtained when $a$ is divided by $b$.

Ex Let $a, b \geq 0$.

If Euclid$(a,b)$ makes $k$ recursive

then $a \geq F_{k+2}$, $b \geq F_{k+1}$, where

$\{F_k\}$ is the Fibonacci sequence.

$0, 1, 1, 2, 3, 5, 8, 13 - - - -$

# Extended Euclid (a, b)

Let, $a, b \in \mathbb{Z}$ & $d = \gcd(a, b)$

Then $\exists\ \lambda, \mu \in \mathbb{Z}$ s.t.

$$\boxed{a\lambda + b\mu = d}$$

Pf Set $r_0 = a$, $r_1 = b$.

If $b = 0$, then $d = a$ & $\lambda = 1$, $\mu = 0$.

Otherwise by Euclid we have

$$r_0 = r_1 q_1 + r_2, \quad r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3, \quad r_3 < r_2$$

$$\vdots$$

$$r_{n-1} = r_n q_n.$$

Claim For each $i$, $\exists \lambda_i, \mu_i$ s.t.

$$r_i = \lambda_i a + \mu_i b.$$

Trivially true for $i = 0, 1$.

Assume true for integers $\leq i$.

$$r_{i-1} = r_i q_i + r_{i+1}$$

$$\therefore r_{i+1} = r_{i-1} - r_i q_i = (\lambda_{i-1} a + \mu_{i-1} b) - q_i (\lambda_i a + \mu_i b)$$

$$= a(\underbrace{\lambda_{i-1} - q_i \lambda_i}_{\lambda_{i+1}}) + b(\underbrace{\mu_{i-1} + q_i \mu_i}_{\mu_{i+1}})$$

# Extended-Euclid $(a,b)$

Input: non-negative integers $a, b$.

Output: a triplet $(d, \lambda, \mu)$ s.t.

$$d = GCD(a,b) = \lambda a + \mu b.$$

1. If $b = 0$ then return $(a, 1, 0)$.
2. Else $(d', \lambda', \mu') := \text{Extended-Euclid}(b, a \bmod b)$
3. $(d, \lambda, \mu) := (d', \lambda' - \lfloor a/b \rfloor \mu')$
4. return $(d, \lambda, \mu)$

## Correctness.

If $b = 0$ then obvious.

By induction hypothesis
A B

$d = GCD(b, a \bmod b) = d' = \lambda' b + \mu' \, a \bmod b.$

Note $a \bmod b = a - \lfloor a/b \rfloor b.$

$$d = \lambda' b + \mu' \{ a - \lfloor a/b \rfloor b \}$$

$$= \underbrace{\mu' a}_{\lambda} + \underbrace{(\lambda' - \mu' \lfloor a/b \rfloor) b}_{\mu}.$$

**Cor** If $GCD(a, n) = 1$, then $\exists b$ s.t

$$\boxed{ab \equiv 1 \bmod n.}$$

If $\exists \lambda, \mu$ s.t.

$$\lambda a + \mu n = 1.$$

$$\boxed{\lambda} a \equiv 1 \bmod n$$

**Cor.** If $p$ is prime, then $(\mathbb{Z}_p, +, \times)$ is a field.

$a^{-1}$ $a$ $1.2.3.4\ldots p-2 \equiv 1 \bmod p$

$1.2.3.\ p-1. \equiv -1 \bmod p$

$\mathbb{Z}_p^* = \{1, 2, 3, 4, \ldots, p-1\}$ $(p-1)! + 1 \mid p$.

Each $a \in \mathbb{Z}_p^*$, $a \neq \pm 1$ has an inverse in $\mathbb{Z}_p^*$ $\neq a$.

## Wilson's Thm

Let $n$ be a +ve integer.

Then $n$ is prime iff $n \mid (n-1)! + 1$

# Chinese Remainder Thm.

Let $n_1, n_2, \ldots, n_k$ be pair-wise co-prime +ve integers. Then the following system has a unique soln modulo $N$ where $N = n_1 n_2 \cdots n_k$.

$$X \equiv a_1 \bmod n_1$$
$$X \equiv a_2 \bmod n_2$$
$$\vdots$$
$$X \equiv a_k \bmod n_k.$$

Pf Uniqueness. Suppose $X$ & $Y$ are two soln.

$$X \equiv a_1 \bmod n_1$$
$$X \equiv a_2 \bmod n_2$$

Hence $\left.\begin{aligned} X &\equiv Y \bmod n_1 \\ X &\equiv Y \bmod n_2 \\ &\vdots \\ X &\equiv Y \bmod n_k \end{aligned}\right\} \Rightarrow N \mid (X-Y)$

Existence. for $k=2$.

Since $GCD(n_1, n_2) = 1$, $\exists \tilde{n}_1, \tilde{n}_2$ s.t.

$$n_1 \tilde{n}_1 \equiv 1 \bmod n_2$$

$$n_2 \tilde{n}_2 \equiv 1 \bmod n_1$$

Set $X = a_1 n_2 \tilde{n}_2 + a_2 n_1 \tilde{n}_1$

clearly $X \equiv a_1 n_2 \tilde{n}_2 \bmod n_1 \equiv a_1 \bmod n_1$

$X \equiv a_2 n_1 \tilde{n}_1 \bmod n_2 \equiv a_2 \bmod n_2$

Eulers $\varphi$-fn.

Defn $n > 1$ Define.

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1 \\ |\{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}| \end{cases}$$

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

Prop $\mathbb{Z}_n^*$ is a group wrt $\times$. of order $\varphi(n)$

**Thm** (a) Let $p$ be a prime & $\alpha > 0$.

$$\varphi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right).$$

(b) If $\gcd(m,n) = 1$, then

$$\varphi(mn) = \varphi(m)\varphi(n).$$

(c) Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Then $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

(a)


Hence $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

$= p^\alpha\left(1 - \frac{1}{p}\right)$

(b) Consider $\mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*$

Define $F : \mathbb{Z}_{nm}^{\times} \longrightarrow \mathbb{Z}_n^{\times} \times \mathbb{Z}_m^{\times}$ as follows

$a \in \mathbb{Z}_{nm}^{\times}$

$$F(a) = (\underbrace{a \bmod n}_{a_1}, \underbrace{a \bmod m}_{a_2})$$

By CRT, $F$ is 1-1 & onto.

$$|\mathbb{Z}_{nm}^{\times}| = |\mathbb{Z}_n^{\times}| \cdot |\mathbb{Z}_m^{\times}|$$

## Euler's Thm.

Let $a$ be co-prime to $n$. Then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

If $\mathbb{Z}_n^*$ is a multiplicative group of order $\varphi(n)$

$a \equiv a' \mod n \quad a' \in \mathbb{Z}_n^*$

$\therefore a^{\varphi(n)} \equiv (a')^{\varphi(n)} \equiv 1 \mod n.$

**Defn** $p$: an odd prime.

An integer $a \not\equiv 0 \bmod p$ is said to be a quadratic residue modulo $p$ if $\exists\ x \in \mathbb{Z}_p$ s.t.

$$x^2 \equiv a \bmod p.$$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

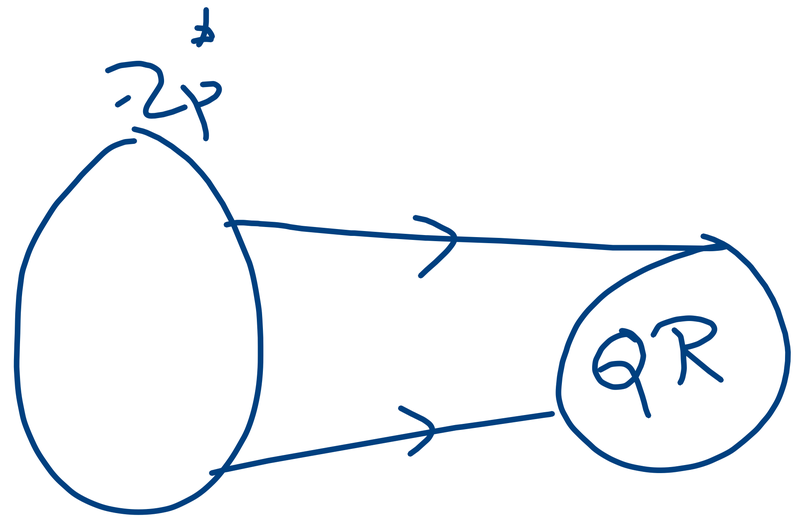
**Prop.** $p$: odd prime.

The # of QR in $\mathbb{Z}_p$ is $\frac{p-1}{2}$.

**Pf** Consider the following fn $f$ from $\mathbb{Z}_p \to \mathbb{Z}_p$

$$x \longrightarrow x^2 \bmod p.$$

Clearly the range is $QR_p$. $x^2 \equiv a \bmod p$




$$|QR| = \frac{1}{2}(p-1)$$

## Euler's Criterion.

An integer $a$ is a quadratic residue mod $p$ iff

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

→ Suppose $a$ is a quad. residue.

Then $\exists x$ s.t. $x^2 \equiv a \bmod p$.

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p. \text{ (by Fermat)}$$

← Suppose $a^{\frac{p-1}{2}} \equiv 1 \mod p$. Assume $a \in \mathbb{Z}_p^*$

We know that $\mathbb{Z}_p^*$ is a cyclic group

$$\mathbb{Z}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}.$$

Hence $\exists\, i$ s.t. $a \equiv g^i \mod p$.

$$1 \equiv a^{\frac{p-1}{2}} \equiv g^{\frac{i}{2}(p-1)} \mod p.$$

$$\Rightarrow p-1 \mid \frac{i}{2}(p-1) \Rightarrow \frac{i}{2} \text{ is an integer}$$

$$\therefore \boxed{i = 2k}$$

$$\boxed{a \equiv (g^k)^2 \mod p}$$

## Legendre Symbol

Let $p$ be an odd prime. Define Legendre's symbol of an integer $a$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p \\ +1 & \text{if } a \in QR_p \\ -1 & \text{if } a \in QNR_p. \end{cases}$$

---

**Cor** An integer $a$ is a quad non-residue iff $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

## Euler's Criterion

$c \not\equiv 0 \bmod p$

$$a \equiv \left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \bmod p.$$

## Properties of Legendre's symbol.

① $\left(\frac{2}{p}\right) = \begin{cases} (-1)^{\frac{p-1}{4}} & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\frac{p+1}{4}} & \text{if } p \equiv 3 \bmod 4 \end{cases}$

② $\left(\frac{2}{p}\right) = (-1)^{p^2-1/8}$

# Gauss' Reciprocity Thm

$p, q$ distinct odd primes

Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$