• Divisibility Thm:-

- $a, b \in \mathbb{Z}$, such that $b > 0$.

  unique $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that $0 \le r < b$.

  $a = bq + r$ holds. $a = bq' + r'$ holds

- $S = \{a - bs : s \in \mathbb{Z}\}$. $(r - r') = b(q - q')$

  $r \ge b$ $r = b + k$. $k \ge 0$

  $r = a - bq \Rightarrow b + k = a - bq \Rightarrow k = a - b(q+1)$ $k \in S$.

- Every ideal I of $\mathbb{Z}$ is a principal ideal, i.e; $I = d\mathbb{Z}$ (unique).
  - $a \in I$., d is the min element of I.

  By divisibility Thm

  $a = dq + r$. $\quad 0 \le r < d$

  $\Rightarrow a - dq = r$.

  $d\mathbb{Z} = e\mathbb{Z}$.

  $d = \pm e$.

- For $a, b \in \mathbb{Z}$, $\exists$ a unique greatest common divisor d of a and b. Moreover, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Let $I = a\mathbb{Z} + b\mathbb{Z}$.

and $I = d\mathbb{Z}$.

$a, b, d \in I$.

$\Rightarrow a \in d\mathbb{Z} \Rightarrow d \mid a$.

Similarly, $b \in d\mathbb{Z} \Rightarrow d \mid b$

$d \in a\mathbb{Z} + b\mathbb{Z}$.

$\Rightarrow d = as + bt, \quad s, t \in \mathbb{Z}$.

e be a common divisor of a and b.

$\rightarrow$ d is a common divisor of a and b.

$\rightarrow$ $a = a'e, \quad b = b'e$

$\Rightarrow d = e(a's + b't) \Rightarrow e \mid d$.

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

Then $\exists s, t \in \mathbb{Z}$ such that $as + bt = r$ holds iff $d \mid r$.

In particular, a, and b are relatively prime iff $\exists s, t$ such that $as + bt = 1$.

$r = as + bt$
$\in a\mathbb{Z} + b\mathbb{Z}$.
$\in d\mathbb{Z} \Rightarrow d \mid r$.

$a, b \in \mathbb{Z}$ and $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

$as + ct = 1$
$\Rightarrow abs + bct = b$.

If p is a prime, $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Thm: If $a_1 \dots a_k$ are integers and p is a prime such that $p \mid \prod_{i=1}^{k} a_i$, then $p \mid a_i$ for some $i \in \{1, \dots, k\}$

$p \mid \underbrace{a_1 \cdots a_m}_{a'} a_{m+1}$

- Fundamental Thm. of Arithmetic.
- # of primes is infinite.

$a(s_1 - s_2) + b(t_1 - t_2)$
$\equiv 0 \bmod a$

$a(s_1 - s_2) + b(t_1 - t_2)$
$\equiv -0 \bmod b$.

$a \mid b(t_1 - t_2)$

$t_1 \equiv t_2 \bmod a$

$I_m = \{0, \dots, m-1\}$.

$\tau : I_b \times I_a \to I_{ab}$.

$(s, t) \longmapsto (as + bt) \bmod ab$.

τ is a bijection. iff $\gcd(a, b) = 1$

$as_1 + bt_1 \equiv as_2 + bt_2 \bmod ab$.

$a(s_1 - s_2) + b(t_1 - t_2) \equiv 0 \bmod ab$.

If p is a prime, then for any integer $1 \leq k \leq p-1$

$\binom{p}{k}$ is divisible by p.

$$t = \frac{p!}{k!(p-k)!}$$

$$p! = t \times k! \times (p-k)!$$

$t \times k! \times (p-k)!$ is divisible by p.

Thm: Let $\sim$ be an equivalence relation over a set S.

For $a \in S$, $[a]$ denotes its equivalence class.

Then for all $a, b \in S$:

(i) $a \in [a] \implies$ Reflexive

(ii) $a \in [b] \Rightarrow [a] = [b]$.

$t \in [a]$, $t \sim a \sim b$

$t \sim b \Rightarrow t \in [b]$.

$t \in [b]$, $t \sim b$

$\longrightarrow$ partitions the set S.

mod operation with respect to 'n'.

is an equivalence rel^{n}

$a \equiv b \bmod n$

$\Rightarrow n \mid (a-b)$.

$ax - by = n$.

$a \bmod n = b \bmod n$.

Thm: Let $a, b, a', b', n \in \mathbb{Z}$ where $n > 0$.

If $a \equiv a' \bmod n$

$b \equiv b' \bmod n$.

Then $a+b \equiv (a'+b') \bmod n$.

$ab = (a' \cdot b') \bmod n$.

$n \mid (a-b)$

$d \mid (a \cdot b)$

- Suppose $a, b, n \in \mathbb{Z}$ such that $n > 0$ and $a \equiv b \bmod n$. Then $\gcd(a,n) = \gcd(b,n)$

- $d \mid a, d \mid n \leftarrow$ Let $d = \gcd(a,n)$ $\quad as + ny = d$ $\quad as - bs' + n(y-y') = d - d'$

$\parallel$ $d' = \gcd(b,n)$ $\quad bs' + ny' = d'$

$a \in \{0, \dots, 2^e - 1\}$.

$bin(a) = 1001$ $\quad a = 9$

$bin(\bar{a}) = 0110$ $\quad \bar{a} = 6$

$$\bar{a} + 1 = -a \bmod 2^e$$

↘ 2's complement!

2^4 $\quad \underline{0/1}\ \underline{0/1}\ \underline{0/1}\ \underline{0/1} = 0$ ✓

$a - b = a + (-b)$

$a + \bar{b} + 1$

$\underline{946}$ $\quad 6 \times 10^0 + 4 \times 10 + 9 \times 10^2$

$\underline{1}\ \underline{1}\ \underline{1}\ \underline{1} = 15$ ✓

Thm: Let $a, n \in \mathbb{Z}$ with $n > 0$, and let $d = \gcd(a, n)$.

(i) for every $b \in \mathbb{Z}$, $az \equiv b \bmod n$ has a soln $z \in \mathbb{Z}$ iff $d \mid b$.

(ii) for every $z \in \mathbb{Z}$, $az \equiv 0 \bmod n$ iff $z \equiv 0 \bmod n/d$.

(iii) for every $z, z' \in \mathbb{Z}$, $az \equiv az' \bmod n$ iff $z \equiv z' \bmod n/d$.

Pf.

(i) $az - b = ny$
$\Leftrightarrow az - ny = b.$
$\Leftrightarrow d(a'z - n'y) = b$

(ii) $n \mid az$
$n' = n/d \mid a' = (a/d) \cdot z$
$\Rightarrow n' \mid a' \cdot z$

$n' = n/d$ $\quad a' = a/d.$
$\gcd(a', n') = 1$

$n' \mid z$
$\Rightarrow z \equiv 0 \bmod n/d.$

Let $a \in \mathbb{Z}$ and $n > 0$ be an integer.

$d = \gcd(a, n)$.

$\tau_a : I_n \to I_n$, where $I_n = \{0, \ldots, n-1\}$.

defined as

$\tau_a(z) = az \bmod n$.

✓ τ_a is bijective iff $\gcd(a,n) = 1$.

$az \equiv az' \bmod n$.

$a(z - z') \equiv 0 \bmod n$.

$z \equiv z' \bmod n$.

– If $\gcd(a,n) = d > 1$, then $|\mathrm{Im}(\tau_a)| = n/d$.

Let $b \in I_n$.

and for every $b \in \mathrm{Im}(\tau_a)$, $\exists$ exactly d pre-images of b. $az \equiv b \bmod n$.

$z_0, z_0 + n/d, z_0 + 2(n/d)$.

Cancellation law.

Let $a, n \in \mathbb{Z}$ with $n > 0$.

if $\gcd(a, n) = 1$ and $az \equiv az' \bmod n$. then $z \equiv z' \bmod n$.

Modular Inverse:

Let $a, n \in \mathbb{Z}$ with $n > 0$. we say that z is a multiplicative inverse of a modulo n if $az \equiv 1 \bmod n$.

If $a \equiv a' \bmod n$, then z is a multiplicative inverse of a modulo n iff z is a multiplicative inverse of a' modulo n.

$az \equiv b \bmod n$.

$\gcd(a,n) = 1$. $\Rightarrow$ β such that $a\beta \equiv 1 \bmod n$.

$z = \beta b$.

$ax + ny = 1$.

$\Rightarrow a\textcircled{x} = 1 - ny$.

If $\gcd(a,n) = d > 1$.

$a = a'd$

$b = b'd$

$n = n'd$

$a'dz \equiv b'd \bmod n'd$

$\Rightarrow a'z \equiv b' \bmod n'$.

$= \gcd(a', n') = 1$

Chinese Remainder Theorem (CRT).

Let $\{n_i\}_{i=1}^{k}$ be a pairwise relatively prime family of integers.

Let $a_1, \ldots, a_k$ be arbitrary integers. Then $\exists$ a soln $a \in \mathbb{Z}$ to the following system of congruences.

$$a \equiv a_i \bmod n_i \quad \forall\, i = 1 (1) k.$$

Moreover, any $a' \in \mathbb{Z}$ is a soln to the above system of congruences.

iff $a' \equiv a \bmod n$, where $n = \prod_{i=1}^{k} n_i$

pf: Let us assume we can construct K many integers $e_1 \dots e_K$ such that the following holds:

$$e_j = \begin{cases} 1 \bmod n_i & \text{if } i = j \\ 0 \bmod n_i & \text{if } i \neq j \end{cases}$$

We consider $a = (a_1 e_1 + \dots + a_k e_k)$.

$a \equiv a_i \bmod n_i \quad \forall i = 1, 2, \dots, K.$

$n^* = \prod_{i=1}^{K} n_i$

$e_i \equiv 1 \bmod n_i$
$= 0 \bmod n_j$

$e_i \equiv 1 \bmod n_i$

$e_2 = (n_1 n_3 n_4) \bmod n_2$

$e_i = n^* / n_i$

$e_i = \prod_{\substack{j=1 \\ j \neq i}}^{K} n_j$

Let a' be an another soln

$$a' \equiv a_i \bmod n_i \quad \text{for every } i \in \{1, \ldots k\}$$

We also have:

$$a \equiv a_i \bmod n_i \quad \text{for every } i \in \{1, \ldots k\}.$$

For every i

$$(a - \acute{a}) \equiv 0 \bmod n_i$$

$$n_i \mid (a - \acute{a})$$

$$\prod_{i=1}^{k} n_i \mid (a - \acute{a}) \Rightarrow a \equiv \acute{a} \bmod n.$$

If $a' \equiv a \bmod n$, then $n \mid (a' - a)$

$n_i \mid (a' - a) \quad \forall\, i = 1(1)k$

$\Rightarrow a' \equiv a \bmod n_i$

$= a_i \bmod n_i$

$$\tau : I_n \to I_{n_1} \times I_{n_2} \times \cdots \times I_{n_k}.$$

$\tau(a) = (a \bmod n_1,\ a \bmod n_2, \ldots,\ a \bmod n_k)$. is a bijective mapping.

$a \in \{0, \ldots, n-1\}$.

$$\tau : I_n^* \to I_{n_1}^* \times I_{n_2}^* \times \cdots \times I_{n_k}^*.$$ is a bijective fn

$$I_n^* = \{a : \gcd(a, n) = 1\}.$$

$$\mathbb{Z}_n^* = \{[a] : \gcd(a, n) = 1\}.$$

Euler's phi fn. is defined for all positive integers n as.

$$\phi(n) = |\mathbb{Z}_n^*|.$$

Thm: Let $\{n_i\}_{i=1}^{k}$ be a pairwise relatively prime family of positive integers.

and $n = \prod_{i=1}^{k} n_i$

Then $\phi(n) = \prod_{i=1}^{k} \phi(n_i)$.

$\mathbb{Z}_{p^e} = p^e - p^{e-1}$

$|\mathbb{Z}_{p^e}^*|$

Thm: Let p be a prime, and e be a positive integer. Then $\phi(p^e) = p^{e-1}(p-1)$.

Thm: $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Then $\phi(n) = n \prod_{i=1}^{r} \left(1 - 1/p_i\right)$.