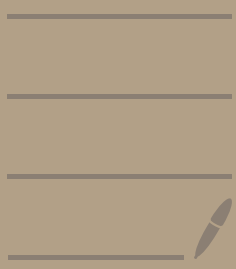
# Number Theory



Def.

$n \in \mathbb{Z} \setminus \{0\}$ $\quad m \in \mathbb{Z}$ , $n \mid m \iff$

$m \in n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$

Def.

$n \in \mathbb{N}_1$ , $\mathbb{Z}_n = \mathbb{Z} / n\mathbb{Z}$

element in $\mathbb{Z}_n$ is called a residue class module n.

Def.

$n \in \mathbb{N}_2$ $\quad \mathbb{Z}_n^\times$ is the group construct by all inversible element

$$\mathbb{Z}_n^\times = \{k + n\mathbb{Z} : 0 \le k \le n-1, \exists l \in \mathbb{Z}, kl \equiv 1 \bmod n\}$$

Lemma I.

$$\gcd(a,b) = \gcd(a \bmod b, b)$$

Proof.

denote c as a common divisiter of a, b

$c \mid a$, $c \mid b$

suppose $r = a - kb$

thus $r/d = a/d - kb/d \in \mathbb{Z}$

thus $d \mid r$

therefore $(a,b)$ and $(b, a \bmod b)$ have same divisiter

Lemma II.

$a, b, c \in \mathbb{N}$, $ax+by=c$ has interger solution $\Leftrightarrow \gcd(a,b) \mid c$

Proof.

if $ax+by=c$ has interger solution.

$$\frac{c}{\gcd(a,b)} = \frac{a}{\gcd(a,b)}x + \frac{b}{\gcd(a,b)}y \in \mathbb{Z}$$

$$\gcd(a,b) \mid c$$

if $\gcd(a,b) \mid c$

suppose $a = m \cdot \gcd(a,b)$

$b = n \cdot \gcd(a,b)$

$c = k \cdot \gcd(a,b)$

function equivalent to $mx+ny=k$ $\gcd(m,n)=1$ ①

if $mx+ny=1$ has interger solution, so do equation ①

$m = q_1 n + r_1 \quad 0 < r_1 < n$

$n = q_2 r_1 + r_2 \quad 0 < r_2 \leq r_1$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$

$r_{n-1} = q_{n+1} r_n + 1$

thus $\exists\ A_{n-2}, B_{n-1}$ that $r_{n-2} A_{n-2} + r_{n-1} B_{n-1} = 1$

by induction

$r_1 A_1 + r_2 B_2 = 1$

$b_1 A_0 + r_1 B_0 = 1$

there exist integer solution for equation ①

**Prop.** $n \in \mathbb{Z}_n^\times = \{ k + n\mathbb{Z} : 1 \le k \le n-1, \gcd(k,n) = 1 \}$

thus $|\mathbb{Z}_n^\times| = \phi(n)$

especially, if $p$ is a prime.

$\mathbb{Z}_p^\times = \{ 1+p\mathbb{Z}, 2+p\mathbb{Z}, \cdots\cdots, (p-1)+p\mathbb{Z} \}$

thus $|\mathbb{Z}_p^\times| = p-1$

**Proof.** $\exists\ l \in \mathbb{Z}, kl \equiv 1 \mod n \iff kl = 1 + tn$

$\iff l \cdot k + (-t)n = 1$

$\iff \gcd(k,n) = 1$

**Prop.** $(\mathbb{Z}_n, +)$ is a cyclic group

$(\mathbb{Z}_n, \cdot)$ is a monoid

where $(\cdot)$ is well-defined that $(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = ab+n\mathbb{Z}$

thus $\mathbb{Z}_n^\times$ is a group

**Prop.** $(G, \cdot)$ a finite group, for $\forall a \in G$, $a^{|G|} = e$

**Proof.** $|\langle a \rangle| \mid |G|$ & $|a| = |\langle a \rangle|$

$$a^{|G|} = (a^{|a|})^{|G|/|a|} = e^{|G|/|a|} = e$$

**Prop.** $n \in \mathbb{N}_+$ $\gcd(a,n) = 1$, $a^{\phi(n)} \equiv 1 \mod n$

especially $n$ is a prime $a^{n-1} \equiv 1 \mod n$

**Proof.** $a^{|\mathbb{Z}_n^\times|} = a^{\phi(n)} = 1$

thus $a^{\phi(n)} \equiv 1 \mod n$

Theorem. (Willson theorem)

$$(p-1)! \equiv -1 \mod p \iff p \text{ is a prime } (p \neq 2)$$

Proof.

$|\mathbb{Z}_p^\times| = p-1$

if $a \in \mathbb{Z}_p^\times$ and its inverse is itself

thus $a = a^{-1} \iff a^2 \equiv 1 \mod p \iff p \mid (a^2-1) = (a+1)(a-1)$

either $p \mid (a+1)$ or $p \mid (a-1)$

thus $a = 1$ or $p-1$

$(p-1)! \equiv 1 \cdot (2 \cdot p-2) \cdot (3 \cdot p-3) \cdots (p-1) \equiv 1 \cdot 1 \cdot 1 \cdots (p-1) \equiv p-1 \equiv -1 \mod p$