Basics of Number theory

Thm: Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < b.$$

Pf: Consider a set S of non-negative integers of the form $a - bt$, $t \in \mathbb{Z}$.

- S is non-empty and it contains positive integers.

Let r be the smallest element of S.

$r = a - bq$ for some $q \in \mathbb{Z}$.

We have to show that $r < b$.

If not $r - b \geq 0$

$\underbrace{r - b}_{\in S} = a - b(q+1)$.

If $r_1 = r_2$

$\Rightarrow b(q_1 - q_2) = 0$

$\Rightarrow q_1 = q_2$

Uniqueness of r : Let r_1 and r_2 be two positive integers $\in S$

$r_1 = a - bq_1$ and $r_2 = a - bq_2$

$\Rightarrow r_1 - r_2 = b(q_2 - q_1) \Rightarrow b \mid (r_1 - r_2) \Rightarrow r_1 = r_2$.

$I \subseteq \mathbb{Z}$ is called "ideal" if.

$a, b \in I \Rightarrow a+b \in I$.

$\forall z \in \mathbb{Z}, \; az \in I$.

- I also contains 0 element
- If $a \in I \Rightarrow -a \in I$
- $a, b \in I \Rightarrow a-b \in I$.
- if $1 \in I \Rightarrow I = \mathbb{Z}$.

Ideal generated by a.

For a given $a \in \mathbb{Z}$.

we consider a set

$$a\mathbb{Z} = \{az : z \in \mathbb{Z}\}.$$

Prove that $a\mathbb{Z}$ is an ideal.

Lemma: Let $a, b \in \mathbb{Z}$. Then $b \in a\mathbb{Z}$ if and only if $a \mid b$.

Lemma: For every ideal I, $b \in I$ if and only if $b\mathbb{Z} \subseteq I$

Combining these two lemmas, we have:

Lemma: Let $a, b \in \mathbb{Z}$. Then $b\mathbb{Z} \subseteq a\mathbb{Z}$ if and only if $a \mid b$.

Fact: I_1 and I_2 are ideals. Then the set

$$I_1 + I_2 = \{a+b : a \in I_1,\ b \in I_2\}$$

is also an ideal.

Thm: Let I be an ideal of $\mathbb{Z}$. Then $\exists$ a unique positive integer d such that $I = d\mathbb{Z}$.

Pf: Consider the set of non-zero positive integers. Let d be the smallest positive element in I.

we have to show

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

Case 1: $d\mathbb{Z} \subseteq I$

Case 2: $I \subseteq d\mathbb{Z}$.

Let $a \in I$.

$\Rightarrow a = dq + r$ for some $q, r \in \mathbb{Z}$.

$\Rightarrow r = a - dq$ where $0 \leq r < d$.

$\Rightarrow r \in I \Rightarrow r$ is the least element $\Rightarrow \Leftarrow$.

$\Rightarrow r = 0 \Rightarrow d \mid a \Rightarrow a \in d\mathbb{Z}$.

Greatest common Divisor:

Thm: For all $a, b \in \mathbb{Z}$, there exists a unique greatest common divisor of a and b!
Moreover $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Pf: Let $I = a\mathbb{Z} + b\mathbb{Z}$. By previous Thm, $\exists$ a unique d such that $I = d\mathbb{Z}$.
Now, we have to show that d is the gcd of a and b.
Observe that $a, b, d \in I$.

Since $a \in I = d\mathbb{Z}$

$\Rightarrow d \mid a$.

Similarly $b \in I = d\mathbb{Z}$

$\Rightarrow d \mid b$.

As a result d is a common divisor of a and b.

Since $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

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

Let us assume d' is a common divisor of a and b.

$a = a'd'$ and $b = b'd'$. By plugging-in we have.

$d = (a's + b't)\, d'$

$\Rightarrow d' \mid d$.

$\Rightarrow d$ is a greatest common divisor of a and b.

Uniqueness of gcd. (Trivial).

Thm: Let $a, b, r \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then there exists $s, t \in \mathbb{Z}$ such that $as + bt = r$ if and only $d \mid r$.

pf: $as+bt=r$ for some s,t

$\Leftrightarrow r \in a\mathbb{Z}+b\mathbb{Z}$

$\Leftrightarrow r \in d\mathbb{Z}$

$\Leftrightarrow d \mid r$

As a corollary of the above result.

If a and b are relatively prime to each other.
Then there exists s and t such that

$$as+bt=1.$$

Modular Arithmetic

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

Then $a \equiv b \bmod n$ and $a' \equiv b' \bmod n$

$\Rightarrow a + a' \equiv b + b' \bmod n$

$a \cdot a' \equiv b \cdot b' \bmod n$.

Pf: $n \mid (a-b)$. $n \mid (a'-b')$

$(a-b) = nk$ $\quad$ $(a'-b') = nk'$

$(a+a') - (b+b') = n(k+k')$

$n \mid (a-b)$

$n \mid (a'-b')$

$(aa' - bb') = nK$

$aa' - a'b + a'b - bb'$

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

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

(i) For every $b \in \mathbb{Z}$, the congruence $aZ \equiv b \bmod n$ has a solution $z \in \mathbb{Z}$ if and only if $d \mid b$.

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

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

Pf: (i) $az \equiv b \bmod n \iff az - b = ny$ for some $y \in \mathbb{Z}$.

$\iff b = az - ny$.

$\iff b = a\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$

$\iff d \mid b$.

(ii) $az \equiv 0 \bmod n$

$\Rightarrow n \mid az$

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

$\Rightarrow d \mid a, \; d \mid n$.

From $n \mid az \Rightarrow \frac{n}{d} \mid \frac{a}{d} z \Rightarrow \frac{n}{d} \mid z$

$d = \gcd(a, n)$

$\Rightarrow 1 = \gcd\left(\frac{a}{d}, \frac{n}{d}\right)$

$\Rightarrow z \equiv 0 \bmod \frac{n}{d}$.

(iii) $az \equiv az' \bmod n$

$\Rightarrow n \mid a(z - z')$.

$\Rightarrow \frac{n}{d} \mid \frac{a}{d}(z - z')$

$\Rightarrow z \equiv z' \bmod \frac{n}{d}$.

Modular Inverse: An integer $z \in \mathbb{Z}$ is called the multiplicative inverse of a modulo n if $az \equiv 1 \bmod n$, where $a, n \in \mathbb{Z}$, $n > 0$

Lemma: Let $a, n \in \mathbb{Z}$, $n > 0$. 'a has a multiplicative inverse iff $\gcd(a, n) = 1$

$$\gcd(a,n) = 1 \iff ax + ny = 1 \text{ for some } x, y \in \mathbb{Z}.$$
$$\iff ax \equiv 1 \bmod n.$$

Prop: If z and z' are two multiplicative inverse of modulo r, then $z \equiv z' \bmod n$.

⇓

Multiplicative inverse modulo n is "unique"

Corollary: Suppose $a, b, n \in \mathbb{Z}$, $n > 0$, $a \neq 0$. Such that a is co-prime to n. Then the Congruence

$$ax \equiv b \bmod n$$ has a unique soln

The soln is $x \equiv \bar{a}^{-1} b \bmod n$

Chinese Remainder Theorem (CRT)

Thm: Let $\{n_i\}_{i=1}^{k}$ be a family of pairwise relative prime numbers and let $a_1, a_2, \ldots, a_k$ be any arbitrary integers. Then there exists a unique soln a to the following system of modular eqn

$$\exists = \begin{cases} a \equiv a_1 \bmod n_1 \\ a \equiv a_2 \bmod n_2 \\ \vdots \\ a \equiv a_k \bmod n_k \end{cases}$$

Pf:

Let $e_1, e_2, \ldots e_k$ be k integers satisfying the following:

for each $i = 1 \ldots k$ $\quad e_i \equiv 1 \bmod n_i$

$\equiv 0 \bmod n_j \quad j \neq i$

Soln $\quad a = \sum_{i=1}^{k} a_i e_i$

Argue why this a satisfies $\mathbb{E}$.

$$a = a_1 e_1 + a_2 e_2 + \cdots + a_k e_k$$

$$a \bmod n_1 = a_1 e_1 \bmod n_1 + a_2 e_2 \bmod n_2 + \cdots + a_k e_k \bmod n_1$$

$$\| \qquad \| 0 \qquad\qquad \| 0 \qquad\qquad \| 0$$

How to construct e_i

$n_1, n_2, \ldots n_k$

$gcd(n_i, n_j) = 1 \quad i \neq j$

$N = \prod_{i=1}^{k} n_i$

for each $i = 1, \ldots k$ $N_i^* = \frac{N}{n_i}$

$gcd(N_i^*, n_i) = 1$

$N_i^* \textcircled{x} \equiv 1 \bmod n_i$

↓

Inverse of $N_i^* \bmod n_i$

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

$e_i = N_i^* x$

$e_i \bmod n_i$

$\Rightarrow N_i^* x \bmod n_i \equiv 1 \bmod n_i$

$e_i \bmod n_j$

$= N_i^* x \bmod n_j \equiv 0$

Uniqueness:

Let a' be another soln to $\mathbb{F}$.

which implies for every i

$$n_i \mid (a' - a_i)$$

$$n_i \mid (a - a_i)$$

$$\Rightarrow n_i \mid (a - a') \quad \text{for } i = 1, \ldots k$$

$$n \mid (a - a') \Rightarrow a \equiv a' \bmod n.$$

We can visualize CRT in terms of the following map.

$$\tau : \mathbb{Z}_N \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

τ is a bijection.

$$\tau(a) = (a \bmod n_1, \ldots, a \bmod n_k)$$

Chinese Remainder Map:

Let $\{n_i\}_{i=1}^{k}$ be a family of pairwise relatively prime numbers. and $n = \prod_{i=1}^{k} n_i$. We define the map

$$\Theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

Defined by

$$\theta(\alpha) = (\alpha_1, \alpha_2, \ldots \alpha_k) \text{ where } \alpha \in \mathbb{Z}_n \text{ and } \alpha_i \equiv \alpha \bmod n_i \in \mathbb{Z}_{n_i}$$

Show that:

(i) θ is unambiguous.

(ii) θ is bijective

(iii) for all $\alpha, \beta \in \mathbb{Z}_n$

(a) $\theta(\alpha+\beta) = (\alpha_1+\beta_1 \cdots, \alpha_k+\beta_k)$

(b) $\theta(\alpha\beta) = (\alpha_1\beta_1 \cdots \alpha_k\beta_k)$

(c) $\theta(-\alpha) = (-\alpha_1, \cdots -\alpha_k)$

(d) $\alpha \in \mathbb{Z}_n^*$ iff $\alpha_i \in \mathbb{Z}_{n_i}^*$ $\forall i = 1 \ldots k$. $\theta(\alpha^{-1}) = (\alpha_1^{-1}, \cdots \alpha_k^{-1})$

Thm: Let p be a prime and e be a positive integer

Then
$$\phi(p^e) = p^e - p^{e-1}$$
$$= p^e\left(1 - \frac{1}{p}\right).$$

Thm: If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then

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

Euler's totient fn

For every positive integer n

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

Thm: Let $\{n_i\}_{i=1}^{k}$ be a family of pairwise relative prime numbers and $n = \prod_{i=1}^{k} n_i$

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

(Multiplicative fn)

Thm: Let p be a prime and e be a positive integer

Then
$$\phi(p^e) = p^e - p^{e-1}$$
$$= p^e\left(1 - \frac{1}{p}\right).$$

Thm: If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then

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

Multiplicative order:

Thm: Let n be a positive integer and $\alpha \in \mathbb{Z}_n^*$ of multiplicative order k.

Then for every i, j $\alpha^i = \alpha^j \iff i \equiv j \bmod k$

Pf: $\alpha^i = \alpha^j$

$\Rightarrow \alpha^{(i-j)} = \alpha^0 = 1$

$\Rightarrow \alpha^{(i-j)} = 1$

k is multiplicative order of α

$k \mid (i-j)$

Euler's Theorem:

Thm: Let n be a positive integer and $\alpha \in \mathbb{Z}_n^*$
Then $\alpha^{\phi(n)} \equiv 1 \bmod n$.

Pf: $\tau_\alpha : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$

for all $\beta \in \mathbb{Z}_n^*$

$$\tau_\alpha(\beta) = \alpha\beta \bmod n.$$

τ_α is bijective

β_1, β_2

$\tau_\alpha(\beta_1) = \tau_\alpha(\beta_2)$

$\alpha(\beta_1 - \beta_2) \equiv 0 \bmod n$

$$\prod_{\beta \in \mathbb{Z}_n^*} \beta = \prod_{\beta \in \mathbb{Z}_n^*} \alpha\beta.$$

$$\Rightarrow \prod_{\beta \in \mathbb{Z}_n^*} \beta = \alpha^{\phi(n)} \cdot \prod_{\beta \in \mathbb{Z}_n^*} \beta.$$

$$\beta_1 \beta_2 \cdots \beta_k = \alpha^k \beta_1 \beta_2 \cdots \beta_k \bmod n.$$

Fermat's little theorem:

Thm: Let p be a prime number. Then for every $\alpha \in \mathbb{Z}_p$

$$\alpha^p \equiv \alpha \bmod p.$$