Elementary Number Theory

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$

Facts

- $a, b \in \mathbb{Z}$, $a \mid b$ if $\exists\, k \in \mathbb{Z}$ s.t. $b = ak$
- $a, b \in \mathbb{Z}$, d – common divisor $d \mid a$ & $d \mid b$
- $\gcd(a, b)$ = largest of the common divisor
- $\gcd(a, b) = 1$ (a & b are relatively prime)
- $a, b \in \mathbb{Z}$ $(\neq 0)$, $\exists\, s, t$ (integers) s.t. $\gcd(a, b) = sa + tb$
- (Euclid) If $a \mid (bc)$ & $\gcd(a, b) = 1$ then $a \mid c$
- $a, b \in \mathbb{Z}$ A common multiple of a, b is any integer m s.t. $a \mid m$ & $b \mid m$
- $\operatorname{lcm}(a, b)$ = smallest +ve common multiple
- Let $a, b \in \mathbb{Z}$ then $\operatorname{lcm}(a, b) = ab / \gcd(a, b)$

Facts n (fixed) +ve integer For $a, b \in \mathbb{Z}$

- a is congruent b modulo n if $n \mid a - b$

  $a \equiv b \pmod{n}$
- $\equiv \bmod n$ is an equivalence relation
- If $a \equiv b \pmod{n}$ & $c \equiv d \pmod{n}$

  then (i) $a + c \equiv b + d \pmod{n}$

  (ii) $ac \equiv bd \pmod{n}$

✲ If $\gcd(a, n) = 1$ then the eqn $ax \equiv b \pmod{n}$ is solvable & its soln. is uniquely determined modulo n

$\square$ $\because$ $\gcd(a,n)=1 \Rightarrow \exists\ s\ \&\ t$ s.t. $1 = as + nt$

$\Rightarrow b = bas + bnt \Rightarrow b \equiv abs \pmod{n}$

$\Rightarrow x = bs$ is a soln.

Suppose x & x' are two solns. $\Rightarrow ax \equiv b$ & $ax' \equiv b \pmod{n}$

$\Rightarrow ax \equiv ax' \Rightarrow n \mid (ax - ax')$

$\Rightarrow n \mid a(x-x') \Rightarrow n \mid (x-x') \Rightarrow x \equiv x' \pmod{n}$ $\blacksquare$

$\bar{a} = \{ b \in \mathbb{Z} \mid a \equiv b \pmod{n} \} = \{ a + nk \mid k \in \mathbb{Z} \}$

<u>Th.</u> $\mathbb{Z}_n$ is a field $\Leftrightarrow$ n is a prime no.

$\square$ Suppose n is prime, $a (\neq 0) \in \mathbb{Z}_n$

Then $\gcd(a,n) = 1$ $\because$ $a \in \{1, 2, \ldots, n-1\}$
$\Rightarrow$ n can not devide a

$\Rightarrow \exists\ x \in \mathbb{Z}$ s.t. $ax \equiv 1 \pmod{n}$

$\Rightarrow x$ is the inverse of $a \Rightarrow \mathbb{Z}_n$ is a field if n is prime.

On the other hand if $n = ab$ (composite no.) $a, b < n$

$\Rightarrow ab = 0$ in $\mathbb{Z}_n$ a is a zero div.
& a is not invertible $\blacksquare$
$\mathbb{Z}_n$ is not a field

$\boxed{\text{Lemma}}$ If j, k, q & r are +ve integers s.t. $k = jq + r$ then $\gcd(j,k) = \gcd(r,j)$

$\square$ suppose d is a factor of j & k $\Rightarrow k = i_1 d$ & $j = i_2 d$

$\Rightarrow r = k - jq = (i_1 - i_2 q)\, d \Rightarrow d$ is factor of r (also a factor of j) it is a common factor of r & j

Converse can be done $\because$

$j = i_3 d$ & $r = i_4 d \Rightarrow k = (i_3 q + i_4)\, d$ $\blacksquare$

Euclid's div. algo $n (> 0) \in \mathbb{Z}$ Then for every non-neg. integer m, $\exists$ unique integers q & r s.t.

$$m = nq + r, \quad 0 \le r < n$$

Lemma For any $a \in \mathbb{Z}_n$ & ≥ 0 integers i & j

$$(a^i \bmod n) \cdot_n (a^j \bmod n) = a^{i+j} \pmod n$$

and $(a^i \bmod n)^j \bmod n = a^{ij} \pmod n$

Lemma: Let p be a prime no. For a fixed (non zero) $a \in \mathbb{Z}_p$

$\{ i \cdot a \pmod p \}_{i=1}^{p-1}$ are a permutation of the set $\{1, 2, \dots, p-1\}$

□ If $i \cdot a = j \cdot a \bmod p \Rightarrow i = j \bmod p$

Example: $p = 5$ $\{1, 2, 3, 4\}$ let $a = 2$

$$\{ i \cdot 2 \pmod 5 \}_{i=1}^{4} = \{2, 4, 1, 3\}$$

Fermat's Little Th. Let p be a prime no. then

$a^{p-1} \pmod p = 1$ in $\mathbb{Z}_p$ for each nonzero $a \in \mathbb{Z}_p$

□ Since ~~$\{ i \cdot a \pmod p \}_{i=1}^{p-1} = \{ i \}_{i=1}^{p-1}$~~

$$\{ (1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \dots ((p-1) \cdot a) \} \bmod p = \{ 1 \cdot 2 \cdot 3 \dots (p-1) \} \bmod p$$

$\Rightarrow$ $(p-1)! \, a^{p-1} \equiv (p-1)! \pmod p$ Since each element $1, 2, \dots, p-1$ has inverse

we get $a^{p-1} \equiv 1 \pmod p$

$\boxed{\text{F. L. T. v2}}$ $\forall$ +ve a & prime p if $a \neq \lambda p$ then $a^{p-1} \bmod p = 1$

$\boxed{\text{Cipher}}$ $\{A, B, C, \ldots, Z\} \to \{0, 1, 2, \ldots, 25\}$

$$f(p) = (p+3) \bmod 26$$

$\boxed{\text{Example}}$ "MEET YOU IN THE PARK"

$p \to$ 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

$f(p) \Rightarrow (p+3) \bmod 26$

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13

"PHHW BRX LQ WKH SDUN"

$f^{-1}(p) = (p-3) \bmod 26$

– In general $f(p) = p + k \pmod{26}$ Shift Cipher

$f^{-1}(p) = p - k \pmod{26}$

– $f(p) = (ap + b) \bmod 26$ such that f is a bijection

$K = ?$ if $f(p) = 7p + 3$

$\square$ $K = 10 \Rightarrow f(10) = 7 \cdot 10 + 3 = 21 \bmod 26$

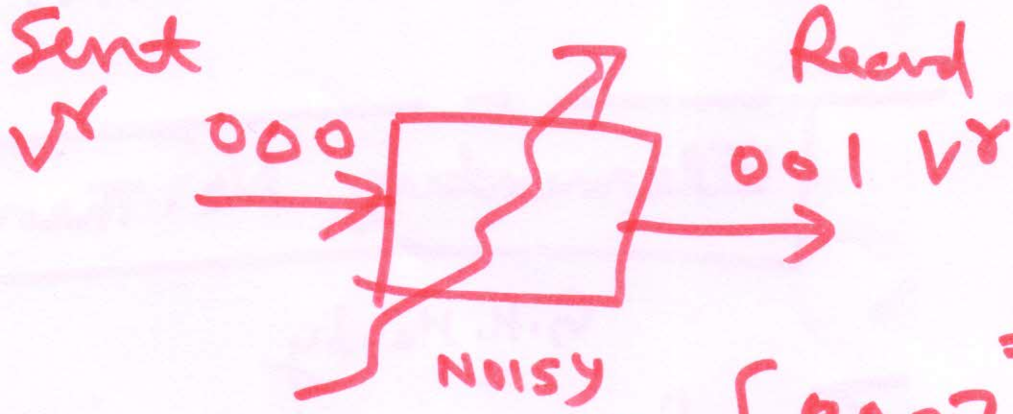
$\therefore K \to V$ " V

$\boxed{\text{Carmichael \#}}$ A composite integer n that satisfies $b^{n-1} \equiv 1 \pmod{n}$ $\forall$ ~~+ve~~ integers b with $\gcd(b, n) = 1$ is called Carmichael #.

$$561 = 3 \cdot 11 \cdot 17$$

YES → 1 → 111

NO → 0 → 000



$y = 001$

$\mathcal{C} = \left\{ \begin{matrix} 000 \\ 111 \end{matrix} \right\}$

$d(000, 001) = 1$

$d(111, 001) = 2$

$x = 111 \longrightarrow y = 101$

$d(101, 000) = 2$

$d(101, 111) = 1$

$x = 111 \longrightarrow y = 100$

$\mathcal{C} = \left\{ \begin{matrix} 00000 \\ 11111 \end{matrix} \right\}$ can correct 2 errors

$\mathcal{C} = \left\{ \begin{matrix} 000 \\ 111 \end{matrix} \right\}$ can correct 1-error

---

Elementary No. Theory

G.H. Hardy

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$

Fundamental Th. of Airthmetic

$n > 1$ $\quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

- $a, b \in \mathbb{Z}$ $\quad a | b$ if $\exists\, K \in \mathbb{Z}$ s.t. $b = aK$
- d - common divisor $\quad d | a$ & $d | b$.
- $\gcd(a, b)$ = largest of the common divisor

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

$$\gcd(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$$

$$\operatorname{lcm}(a,b) = \prod_i p_i^{\max\{\alpha_i,\beta_i\}}$$

$\gcd(a,b) = 1$ relatively prime

- $a, b \in \mathbb{Z}$ $(\neq 0)$ $\exists$ s, t integers s.t.

$$\gcd(a,b) = sa + tb$$

- If $a \mid (bc)$ & $\gcd(a,b) = 1$ then $a \mid c$

n (+ve) integer

$a, b \in \mathbb{Z}$

$a \equiv b \pmod{n}$

if $n \mid a-b$

If $\gcd(a,n)=1$ the eqn

$ax \equiv b \pmod{n}$ is

solvable & its soln. is ! (unique)

$\square$ If $\gcd(a,n)=1$

$\Rightarrow \exists\ s\ \&\ t$ s.t.

$1 = as + nt$

$\Rightarrow b = bas + bnt$

$\Rightarrow b \equiv abs \pmod{n}$

$\Rightarrow x = bs$ is a soln.

Suppose x & x' are two solns

$\Rightarrow ax \equiv b$ & $ax' \equiv b \pmod{n}$

$\Rightarrow ax \equiv ax' \pmod{n} \Rightarrow n \mid ax - ax'$

$\Rightarrow n \mid (x-x') \Rightarrow x \equiv x' \pmod{n}$

$\mathbb{Z}_n$ is a field $\Leftrightarrow$ n is a prime no.

suppose n is prime $a (\neq 0) \in \mathbb{Z}_n$

then $\because a \in \{1, 2, 3, \ldots, n-1\}$

$\gcd(a, n) = 1$

$\Rightarrow \exists\, x \in \mathbb{Z}$ s.t.

$ax \equiv 1 \pmod{n}$

$\Rightarrow$ Every non zero element has a inverse $\Rightarrow \mathbb{Z}_n$ is a field.

Suppose n is not a prime

$n = ab$ (composite)

$\Rightarrow_{n=} ab = 0$ in $\mathbb{Z}_n$

$\Rightarrow \mathbb{Z}_n$ is not a field.

$\boxed{\text{lemma}}$ If j, k, q & r are +ve integers s.t. $k = jq + r$ then

$\gcd(j, k) = \gcd(r, j)$

$\square$ Suppose d is a factor of j & k

$\Rightarrow k = i_1 d$ & $j = i_2 d$

$r = k - jq = (i_1 - i_2 q)\, d$

$\therefore d$ is a factor r

$j = i_3 d$ & $r = i_4 d$ $\quad k = (i_3 q + i_4) d$

$\boxed{\text{Divi} \cdot \text{Algo.}}$ $n\,(>0) \in \mathbb{Z}$ then $\forall \geq 0$ m $\exists\,!$ integers q & r s.t.

$m = nq + r$, $0 \leq r < n$

For any $a \in \mathbb{Z}_n$ & ≥ 0 integers i & j

① $(a^i \bmod n) \cdot_n (a^j \bmod n) = a^{i+j} \pmod n$

② $(a^i \bmod n)^j \bmod n = a^{ij} \pmod n$

$p = 5$ $\{1, 2, 3, 4\}$ $a = 2$

$\{ i \cdot 2 \pmod 5 \}_{i=1}^{4} = \{2, 4, 1, 3\}$

$p = 7$ $\{1, 2, 3, 4, 5, 6\}$

$\{ i \cdot 2 \pmod 7 \}_{i=1}^{6} =$

$\{2, 4, 6, 1, 3, 5\}$

$\boxed{\text{Lemma}}$ Let p be a prime no.

For a fixed non zero $a \in \mathbb{Z}_p$

$\{ i \cdot a \pmod{p} \}_{i=1}^{p-1}$ are a permutation of the set $\{1, 2, \dots, p-1\}$

$\boxed{\text{Fermat's Little Th.}}$ p prime no.

$$a^{p-1} \pmod{p} = 1 \text{ in } \mathbb{Z}_p$$

for each non zero $a \in \mathbb{Z}_p$

$\square$ $\{ (1 \cdot a) \cdot (2 \cdot a) (3 \cdot a) \cdots ((p-1) \cdot a) \} \bmod p$

$$= \{ 1 \cdot 2 \cdot 3 \cdots (p-1) \} \bmod p$$

$$(p-1)! \, a^{p-1} \equiv (p-1)! \bmod p$$

$\because$ each $1, 2, 3, \dots, p-1$ has inverses

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

$\boxed{\text{V.2 F.L.T.}}$ $\forall$ +ve a & prime p

$$a^{p-1} \equiv 1 \pmod{p} \text{ if } a \neq \lambda p$$