$a \mid b$ if $\exists c$ s.t. $b = ac$
$(a \neq 0)$

Th-1 : $a, b, c \in \mathbb{Z}$

① If $a \mid b$ & $a \mid c \Rightarrow a \mid (b+c)$

② if $a \mid b \Rightarrow a \mid bc \ \forall c \in \mathbb{Z}$

③ If $a \mid b$ & $b \mid c \Rightarrow a \mid c$

Th-2 : $a, b, c \in \mathbb{Z}$ s.t. $a \mid b$ & $a \mid c \Rightarrow a \mid mb + nc$
$m, n \in \mathbb{Z}$.

Th-3 : (Division Algo.)

$a \in \mathbb{Z}$ & $d \in \mathbb{Z}^+$ then $\exists !$ q & $r \in \mathbb{Z}$

s.t. $a = dq + r$, $0 \leq r < d$

Def: $a \equiv b \bmod m \Leftrightarrow a - b = km$

Prime nos.

Th-4 There infinitely many primes.

$\boxed{\text{G.C.D.}}$ a & $b \in \mathbb{Z}$ not both zero the largest d s.t. $d \mid a$ & $d \mid b$
is called $\gcd(a, b)$.

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

Fundamental Thm. of Arith.

$(n > 1)$ $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ if $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$
$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$

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

— $\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$

Repr^n of integers $\quad b \in \mathbb{Z}^+$ $(b>1)$

If $n \in \mathbb{Z}^+$ $\quad n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$

$k (\geq 0) \in \mathbb{Z}$

$a_i \ (\geq 0) \in \mathbb{Z}$ $(0 \leq i \leq k)$ $\quad a_i < b$

& $a_k \neq 0$

- Binary
- Hexadecimal

Octal

Decimal

$(0 \leq i \leq 9, \underset{10}{A}, \underset{11}{B}, \underset{12}{C}, \underset{13}{D}, \underset{14}{E}, \underset{15}{F})$

Th. $\quad a, b \in \mathbb{Z}^+ \quad \exists\, s, t \in \mathbb{Z}$ s.t. $\gcd(a,b) = sa + tb$

Th. $\quad a, b$ & $c \in \mathbb{Z}^+$ s.t. $\gcd(a,b) = 1$ & $a \mid bc$ then $a \mid c$

Th. p prime & $p \mid a_1 a_2 \cdots a_n$ $\quad a_i \in \mathbb{Z}$ then $p \mid a_i$ for some i

Linear Congruences $\quad ax \equiv b \pmod{m}$

Ex. $\quad$ Solve $3x \equiv 4 \pmod 7$

$a = 1$

$a = \frac{3}{2}$

$\Rightarrow \bar{3}^{1} \cdot 3x \equiv \bar{3}^{1} \cdot 4 \pmod 7$

but $\bar{3}^{1} = 5$

$\Rightarrow x \equiv 5 \cdot 4 \pmod 7 = 6$

How to find other solns.?

Ex. $\quad x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Chinese Remainder Th.

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime
$\gcd(m_i, m_j) = 1 \quad i \neq j$

$a_1, a_2, \ldots, a_n \in \mathbb{Z}$ then the system

$x \equiv a_1 \pmod{m_1}$ $\ldots\ldots$ $x \equiv a_n \pmod{m_n}$
$x \equiv a_2 \pmod{m_2}$

has a $\overset{!}{\circ}$ soln. modulo $m = m_1 m_2 \ldots m_n$

i.e. $\exists$ a soln. x (with $0 \le x < m$)

$\square$ Put $M_k = \dfrac{m}{m_k}$ $(k = 1, 2, \ldots, n)$

$\Rightarrow \gcd(m_k, M_k) = 1 \Rightarrow \exists\, y_k \in \mathbb{Z}$ s.t.

$\boxed{y_k = \bar{M}_k^{1}}$ $M_k y_k \equiv 1 \pmod{m_k}$ $\boxed{\because \underset{k=0}{a m_k} + y_k M_k \equiv 1 \pmod{m_k}}$

Soln is $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$

F.L.T. $\quad p$ prime $\quad a \in \mathbb{Z}$ s.t. $p \nmid a$

$a^{p-1} \equiv 1 \pmod{p}$ or $a^p \equiv a \bmod p$.

$2^{340} \equiv 1 \pmod{341}$

~~RSA~~ $\quad \cancel{c} = \cancel{M^e} \bmod n$ $\quad$ ~~key~~, ~~(mod n)~~ ~~n = pq~~
~~(encrypted text)~~ $\quad \cancel{(e, (p-1)(q-1))} = 1$

Exponentiation in $\mathbb{Z}_n$

$a^j = a \cdot_n a \cdot_n a \cdot_n \cdots \cdot_n a = a^j \pmod{n}$

Rules (1) For any $a \in \mathbb{Z}_n$ & $i, j\ (\geq 0) \in \mathbb{Z}$

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

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

$\boxed{\text{Example}}$ ~~Let $a \in \{1, \dots, 6\}$~~

Bob's Algo.

$\boxed{\text{RSA}}$

1. Choose large prime #s p & q
2. $n = p \cdot q$
3. Choose $e \neq 1$ s.t. $\gcd(e, (p-1)(q-1)) = 1$
4. Compute $d = e^{-1} \bmod ((p-1)(q-1))$
5. Publish e & n → (public key)
6. Keep d secret (private key)

Alice - sending message to Bob (x)

1. Read the public directory for Bob's keys e & n
2. Compute $y = x^e \bmod n$
3. send y to Bob
4. Bob receive y from Alice & compute

$$z = y^d \bmod n \quad \text{(using secret key } d\text{)}$$

5. Read z

$\boxed{\text{This works if we show } z = x}$

~~This works~~ if $z = y^d \pmod n$ ~~—~~

Also it is secure i.e. knowing n, e & y one cannot find p, q or d & so cannot find x

$\boxed{\text{Proof}}$

$$y^d = x^{ed} \bmod n$$

$$= x^{1 + K(p-1)(q-1)} \bmod n$$

$\because \gcd(e, (p-1)(q-1)) = 1$

$\Rightarrow$ By line 4

$e \cdot d = 1 \pmod{(p-1)(q-1)}$

$\Rightarrow \exists$ integer K s.t.

$e \cdot d = 1 + K(p-1)(q-1)$

By. F.L.T. (assume that $\gcd(x, p) = 1$, $\gcd(x, q) = 1$)

$$\Rightarrow x^{p-1} \equiv 1 \pmod p$$

$$x^{q-1} \equiv 1 \pmod q$$

$$\Rightarrow y^d \equiv x \pmod p$$

$$\& \; y^d \equiv x \pmod q$$

$\Rightarrow$ By C.R.T. ($\because gcd(p,q)=1$) we have

Factoring an integer

$$y^d \equiv x \pmod{p \cdot q} \equiv x \pmod{n}$$