Number Theory

Integers
division, division Algorithm
Modular Arithmatic
Primes
G.C.D / L.C.M.
Euclidean algorithm (Imp.)
Cryptography

G.C.D as linear Combination
Bezout coefficient
Linear congruence
Inverse
Chinese Remainder Theorem

Integers : $\{-\infty \cdots -3, -2, -1, 0, 1, 2, 3, \cdots \infty\} = \mathbb{Z}$

Negative and positive number without floating points
numbers without fractions

Division If a and b are integers with $a \neq 0$ then a divides b if there exists an integer c s.t. $b = a \cdot c$

$\frac{b}{a} = a|b = c$

$2|10$ $\quad 10 = 2 \cdot 5$ ✓

$\frac{10}{2} = 5$

$3|7$ $\quad 3|12$ $\quad 7 = 3 \square$

$3 \nmid 7$ because $\nexists c$ s.t. $7 = 3 \cdot c$

$3|12$ because $\exists c$ s.t. $12 = 3 \cdot c \Rightarrow c = 4$

$12 = 3 \cdot 4$

How many Positive integers not more than 10 are divisible by 2

2, 4, 6, 8, 10

$\lfloor \quad \rfloor$ $\quad \lfloor n/d \rfloor = \lfloor \frac{10}{2} \rfloor = 5$

$n = 9$ $\quad 2, 4, 6, 8$ $\quad \lfloor 9/2 \rfloor = \lfloor 4.5 \rfloor = 4$ $\quad 4.5 \to 4$

How many $x \leq 100$ are divisible by 3 $\quad \lfloor \frac{100}{3} \rfloor = 33.33 \to 33$

Theorem

Let a, b, and c are integers then

<I> If $a|b$ & $a|c$ then $a|(b+c)$ $\quad a = 2$

<I>	If $a\|b$ & $a\|c$ then $a\|(b+c)$
<II>	If $a\|b$ then $a\|b\cdot c$ $\forall c \in \mathbb{Z}$
<III>	If $a\|b$ & $b\|c \Rightarrow a\|c$

$a=2$
$b=4$
$c=8$

Proof : If $a|b \Rightarrow \exists K_1$ s.t. $K_1 = \frac{b}{a}$ ⊕ $\Rightarrow K_1+K_2 = \frac{b+c}{a}$

(I) if $a|c \Rightarrow \exists K_2$ s.t. $K_2 = \frac{c}{a}$ ⊕ $\Rightarrow K = \frac{b+c}{a}$

It means $\exists K = K_1+K_2$ s.t. $K\cdot a = b+c$

$\Rightarrow \frac{b+c}{a} \Rightarrow a|(b+c)$

(II), (III) do by your own

The Division algorithm

Let a be an integer and d is the positive integer. then there are unique integers q and r, with $0 \le r < d$ s.t. $a = dq + r$

$a = 100$
$d = 10$

$100 = 10 \times 10 + 0$
$a = d \times q + r$

$r = a \pmod d$
$0 = 100 \pmod{10}$

$a = 100$ ✓
$d = 9$ ✓

$100 = 9 \times 11 + 1$
$a = d \times q + r$

9 | 100 (11)
99
+ 01

what is the quotient & remainder when 101 is divisible by 11.

$101 = 11 \times 9 + 2$

$2 = 101 \pmod{11}$

11 | 101 (9)
99 ✓
+ 2

what is quotient and remainder when -11 is divisible by 3

$-11 = 3(-4)+1 \Rightarrow 1 = -11 \bmod 3$

$3 \mid -11$ (quotient -4, remainder 1)

Modular arithmetic

If a and b are integers and m is Positive integer then a is Congruent to b modulo m if m divides $a-b$.

$$a \equiv b \pmod m$$

$\exists\ k \in \mathbb{Z}$ s.t. $\frac{a-b}{m} = k \Rightarrow m \mid (a-b)$

A → $20 \equiv 5 \pmod 3 \Rightarrow \frac{20-5}{3} \Rightarrow 3 \mid 15$ ✓

B → $20 \not\equiv 3 \pmod 5 \Rightarrow \frac{20-3}{5} \Rightarrow 5 \nmid 17$ ×

C → $20 \equiv 4 \pmod 2 \Rightarrow \frac{20-4}{2} \Rightarrow 2 \mid 16$ ✓

Let m be a positive integer. The integer a, b are Congruent to modulo m if $\exists$ a integer k such that $a = b + km \Rightarrow \frac{a-b}{m} = k$

Imp.

Let m be a Positive integer if $a \equiv b \pmod m$ & $c \equiv d \pmod m$

then $a+c \equiv b+d \pmod m$

$a \cdot c \equiv b \cdot d \pmod m$

if $10 \equiv 2 \pmod 4$ & $15 \equiv 3 \pmod 4$

$4 \mid 8$ ✓ $\quad 4 \mid 12$ ✓

$25 \equiv 5 \pmod 4$ $\quad 150 \equiv 6 \pmod 4$

$4 \mid 20$ ✓ $\quad 4 \mid 144$

$4 \mid 20$ (quotient 5, remainder 0)

$4 \mid 144$ (quotient 36, remainder 0)

$77 \equiv 2 \pmod 5$ then

$5 \mid (77-2)$ ✓

$7 \equiv 2 \pmod 5$
$11 \equiv 1 \pmod 5$

$18 \equiv 3 \pmod 5$

$10 \equiv 5 \pmod 5$ – ✓

$8 \equiv 3 \pmod 5$ – ✓

$18 \equiv 8 \pmod 5$ –

$80 \equiv 15 \pmod 5$

Primes

Every Positive integer "P" greater than 1 is called the Prime iff Positive factors of P are 1 & P

Smallest Prime → 1, ②, 3

Greatest Prime: Exist but Can't expressed

Ex: 2, 3, 5, 7, 11, 13, 17, ...,

Fundamental Th. of arithmetic

Every Positive integer > 1 Can be uniquely expressed as product of two or more Primes or as a Prime [where the Prime factors are written in order of non-decreasing size]

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$641 = 641$

$999 = 3 \cdot 333 = 3 \times 3 \times 111 = 3 \times 3 \times 3 \times 37 = 3^3 \cdot 37$

$1024 = 2 \cdot 512 = 2 \cdot 2 \times 256 = 2 \times 2 \times 2 \times 128 = 2^{10}$

(#) If n is a Composite integer then n has a Prime divisor less than or equal to $\sqrt{n}$

If n is composite $\boxed{n = a \cdot b}$ & has a factor a $1 < a < n$ where b is a positive integer $1 < b < n$

$a \le \sqrt{n}$ or $b \le \sqrt{n}$

Contradict $a > \sqrt{n}$ & $b > \sqrt{n}$

$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n \Rightarrow \boxed{a \cdot b > n}$ contradicting

A) $50 = \boxed{2 \cdot 5 \cdot 5}$ Comp

B) $17 = \boxed{17}$ prime

$10 = 2 \cdot 5$, 2 ✓ , 5 ✓

10 has a prime divisor less or equal to $\sqrt{10}$

$\sqrt{10} = 3.16$

$\underline{100} = 2 \cdot 2 \cdot 5 \cdot 5$ 2 ✓ , 5 ✓

100 has a prime divisor less or equal to $\sqrt{100}$

$\sqrt{100} = \underline{10}$ ✓

$25 = 5 \cdot 5$

25 has a prime divisor less or equal to $\sqrt{25} = \underline{5}$

Q: Which one following is true

A) n is Positive integer & it has a Prime factor less or equal to $\sqrt{n}$

B) n is a Positive integer > 1 can be expressed as Prime or Product of Prime

1) only A 2) only B 3) Both 4) Neither

Q: 150 has a Prime divisor less or equal to $\boxed{\sqrt{150}}$

G.C.d. L.C.M

Let a, b be are Positive integers

$a = p_1^{m_1} \cdot p_2^{m_2} \cdots p_n^{m_n}$

$b = p_1^{n_1} \cdot p_2^{n_2} \cdots p_n^{m_n}$

25, 15 $15 = 3 \cdot 5 = 3^1 \cdot 5^1$

$25 = 5 \times 5 = 3^0 \cdot 5^2$

$a = p_1^{m_1} \cdot p_2^{m_2} \cdots p_n^{m_n}$

$b = p_1^{n_1} \cdot p_2^{n_2} \cdots p_n^{m_n}$

25, 15 $\quad 15 = 3 \cdot 5 = 3^1 \cdot 5^1$, $25 = 5 \times 5 = 3^0 \cdot 5^2$

$$G.C.d.(a,b) = p_1^{\min(m_1,n_1)} \cdot p_2^{\min(m_2,n_2)} \cdots,$$

$$L.C.m.(a,b) = p_1^{\max(m_1,n_1)} \cdot p_2^{\max(m_2,n_2)} \cdots,$$

100, 350

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2 = 2^2 \cdot 5^2 \cdot 7^0$

$350 = 2 \cdot 175 = 2 \cdot 5 \cdot 5 \cdot 7 = 2^1 \cdot 5^2 \cdot 7^1$

$G.C.d(100, 350) = 2^{\min(2,1)} \cdot 5^{\min(2,2)} \cdot 7^{\min(0,1)}$

$= 2^1 \cdot 5^2 \cdot 7^0 = 2 \cdot 25$

$G.C.d(100, 350) = 50$

$L.C.m(100, 350) = 2^2 \cdot 5^2 \cdot 7^1 = 4 \times 25 \times 7 = 700$

Let a, b are Positive integer

$$a \cdot b = G.C.d(a,b) \times L.C.m.(a,b)$$

Verification $a = 100$, $b = 350$

$a \cdot b = 35000$

$gcd(a,b) = 50$

$l.c.m(a,b) = ?$

$35000 = 50 \times 700$

Euclidean Algorithm a, b. $b < a$

Let $a = b \cdot q + r$, a, b, q, r are integer

then $G.C.d(a,b) = G.C.d.(b,r)$

100, 350 $\quad G.C.d(100, 350)$

100, 350

$a = 350$

$b = 100$

G.C.d. (100, 350)

$100 < 350$ → divisor, dividend

$350 = 100 \times 3 + 50$

$100 = 50 \times 2 + 0$

$\gcd(100, 350) = 50$ = last divisor = Second last remainder

$\gcd(350, 100) = \gcd(100, 50)$

$\gcd(100, 50) = 50$

$\boxed{\gcd(350, 100) = 50}$

G.C.d (414, 662)

$414 < 662$

$662 = 414 \times 1 + 248$

$414 = 248 \times 1 + 166$

$248 = 166 \times 1 + 82$

$166 = 82 \times 2 + 2$

$82 = 2 \times 41 + 0$

$\gcd(414, 662) = ?$

$662 = 414 \times 1 + 248$

$\gcd(414, 662) = \gcd(414, 248)$

$414 = 248 \times 1 + 166 \Rightarrow \gcd(414, 248) = \gcd(248, 166)$

$248 = 166 \times 1 + 82 \Rightarrow \gcd(248, 166) = \gcd(166, 82)$

$166 = 82 \times 2 + 2 \Rightarrow \gcd(166, 82) = \gcd(82, 2)$

$82 = 2 \times 41 + 0 \Rightarrow \gcd(82, 2) = 2$

Bezout Co-efficients / G.C.D. as a linear Combination

If a and b are positive integers then ∃ integers s and t such that

$$G.C.D(a,b) = s\cdot a + t\cdot b$$

Bezout Coeff.

G.C.D (25, 20) = ?.

Bezout coeff. = ?

Linear combination

gcd(25, 20) = 5

B.C. $5 = \square \times 25 + \underset{-1}{\square} \times 20$

Hit & trial

$s = 1$, $t = -1$ Euclidean

20 < 25 yes

$25 = 20\times 1 + \boxed{05}$

$20 = 5\times 4 + 0$

$05 = 25 + (-1)\times 20$

gcd (100, 90)

$100 = 90\times 1 + \boxed{10}$

$90 = 10\times 9 + 0$

$100 = 90\times 1 + \boxed{10}$

$90 = 10\times 9 + 0$

$10 = gcd(100, 90) = 100 + (-1)\times 90$

$s = 1$, $t = -1$

(20, 18)

G.C.D (20, 16) = ?

Bezout coeff. = ?

$20 = 18\times 1 + \boxed{2}$

$18 = 2\times 9 + 0$

$gcd(20, 18) = 2 = 1\cdot 20 + (-1)\times 18$

$S = 1, \quad t = -1$

1 mark question

gcd(20,17) = 9. , 13, C for 20,17

(17,20)

$17 < 20$

$17 \overline{)20}^{1}$ → $20 = 17\times1 + \boxed{03}$ ⇒ $3 = 20 + (-1)\times17$

$03 \overline{)17}^{5}$ → $17 = 3\times5 + \boxed{2}$ ⇒ $2 = 17 + (-5)\times3$

$2 \overline{)3}^{1}$ → $3 = 2\times1 + \boxed{1}$ ⇒ $1 = 3 + (-1)\times2$

$\boxed{1} \overline{)2}^{2}$ → $2 = 1\times2 + 0$

$1 = 3 + (-1)\times[17 + (-5)\times3]$

$1 = (-1)\times17 + 6\times3$

$1 = (-1)\times17 + 6[20 + (-1)\times17]$

$\boxed{1 = 6\times20 + (-7)\times17}$

$\boxed{gcd(17,20) = 1}$

$\boxed{1 = gcd(1,2) = gcd(3,2) = gcd(3,17) = gcd(17,20)}$

$gcd(a,b) = S\times a + t\cdot b$

$\boxed{1 = 1\times3 + (-1)\times2}$

$= 1\times3 + (-1)\times[17 + (-5)\times3]$

$= 1\times3 + (-1)\times17 + 5\times3$

$\boxed{1 = (-1)\times17 + 6\times3}$

$= (-1)\times17 + 6\times[20 + (-1)\times17]$

$= (-1)\times17 + 6\times20 + (-6)\times17$

$\boxed{1 = 6\times20 + (-7)\times17}$

$1 = S\cdot20 + t\cdot17$

$S = 6$

$t = -7$

$1 = \square\times20 + \square\times17$

A> $S = 6, \ t = -7$

Hit & trial

Find the BEzout coeff. for 20, 13

$gcd(20,13) = 1 = \square\times20 + \square\times13$ Hit & trial

Using Euclidean Algo.

$13 \overline{)20}^{1}$ → $20 = 13\times1 + \boxed{07}$

$7 \overline{)13}^{1}$ → $13 = 7\times1 + \boxed{6}$

$6 \overline{)7}^{1}$ → $7 = 6\times1 + \boxed{1}$ ⇒ $1 = 7 + (-1)\times6$

$\boxed{1} \overline{)6}^{6}$ → $6 = 1\times6 + 0$

$= 7 + (-1)[13 + (-1)\times7]$

$= (-1)\times13 + 2\times7$

$S=2$
$t=-3$

$= (-1)\times 13 + 2[20 + (-1)\times 13]$
$= 2\times 20 + (-3)\times 13$
$= S\cdot a + t\cdot b$

G.C.d ✓	G.C.d as Linear Combination
Bezout coeffients ✓	inverse of a modm
Sol. of Linear Congruence	

gcd(252, 198)

$198 \overline{)252}$ 1
198
$54 \overline{)198}$ 3
162
$36 \overline{)54}$ 1
36
$18 \overline{)36}$ 2
36
00

$252 = 198\times 1 + 54$
$198 = 54\times 3 + 36$
$54 = 36\times 1 + \boxed{18}$
$36 = 18\times 2 + 0$

$18 = 1\times 54 + (-1)\times 36$
$18 = 1\times 54 + (-1)\times[198 + (-3)\times 54]$
$18 = (-1)\times 198 + 4\times 54$
$18 = (-1)\times 198 + 4[252 + (-1)\times 198]$
$18 = 4\times 252 + (-5)\times 198$

B.C. are 4, -5

If 18 is the gcd of (252, 198) & one of B.C. is 4 other one is

$18 = \underset{4}{\square}\times 252 + \square \times 198$

A –
B –
C –
D –

Inverse of a modulo m → $a\square \equiv 1 \bmod m$ → $a\square - 1/m$

inverse of a modm exists if $\gcd(a,m) = 1$

if a & m are relatively prime & $m > 1$ then an inverse of a modulo m exist

less than m there exist a unique $\bar{a}'$ s.t. $0 \le \bar{a}' < m$

Inverse of a mod m $\Rightarrow$ $a\square \equiv 1 \pmod m$

$\bar{a}^{-1}$

$0 \le \bar{a}^{-1} < m$ s.t. $a \cdot \bar{a}^{-1} \equiv 1 \pmod m$ (Hit & trial)

Ex:
- inverse of 3 mod 7 exists ✓ yes
- inverse of 5 mod 10 exist ✗ No

$3\overline{)7}\ 2,\ 6,\ 1,\ 3,\ 3,\ 0$ ↪ $1 = \gcd(3,7)$

$5\overline{)10}\ 2,\ 10,\ 00$ ⇝ $\gcd(5,10) = 5$

Inverse of 10 mod 18 does not exist

$\gcd(10,18) = 2$

$10\overline{)18}\ 1,\ 10,\ 8$

$8\overline{)10}\ 1,\ 08,\ 2$

$2\overline{)8}\ 4,\ 8,\ 0$

inverse of $3 \bmod 7 \Rightarrow 3\square \equiv 1 \bmod 7$

$\exists$ one integer $\bar{a}^{-1}$, $0 \le \bar{a}^{-1} < 7$ s.t. $3\cdot\bar{a}^{-1} \equiv 1 \pmod 7$

$\frac{3\square - 1}{7}$

$0\times\ \frac{3\boxed{0}-1}{7} = -\frac{1}{7}\times$ ← Hit & trial

$1\times\ \frac{3-1}{7}\times$

$2\times\ \frac{6-1}{7}\times$

$3\times\ \frac{8}{7}\times$

$4\times\ 11/7\times$

Inverse of 3 mod 7 is 5

5 ✓, $\frac{3\times5-1}{7}$, $\frac{14}{7}$ ✓

Using B.C.

$7 = 3\times2 + \boxed{1}$

$\boxed{1 = 1\cdot7 + (-2)\times3}$

$3\overline{)7}\ 2,\ 6,\ 1$

$1\overline{)3}\ 3,\ 3,\ 0$

1, −2 are B.C.

$1\times$

-2 ✓ is one of inverse

(-2), $-2+7 = (5)$, $5+7$

Q: Find the inverse of 7 mod 10

Hit & trial $[0 \le \bar{a}^{-1} < 10]$ unique

$7\square \equiv 1 \bmod 10$

$\frac{7\square - 1}{10}$

$0\times$
$1\times$
$2\times$
$\boxed{3}$ ✓

$\frac{7\times3-1}{10}$ ✓ $\frac{20}{10}$ ✓

13 ✓
$10\times$
$5\times$
$6\times$

inverse of 7 mod 10 is 3

$-37, -27, -17, -7, 3, 13, 23, 33, 43$

$7\overline{)10}$ → $10 = 7\times1 + \boxed{3}$

$3\overline{)7}\ 2,\ 6,\ 1$ → $7 = 3\times2 + \boxed{1}$

$3\overline{)3}\ 3,\ 3,\ 0$ → $3 = 1\times3 + 0$

Using Bezout coeff.

$1 = 7 + (-2)\times3$

$= 7 + (-2)\times[10 + (-1)\times7]$

$= -2\times10 + 3\times7$

$s = -2$, $t = 3$

$\frac{7\square - 1}{10}$ ⇝ $= -\frac{15}{10}\times$, $\frac{21-1}{10}$ ✓

Solution of linear Congruence

A Congruence in the Form $ax \equiv b \pmod m$ is called a linear Congruence where a, b are integers, m is positive integer

Solution ⟶ we will find all possible value of integer x that satisfy the above Congruence. $\frac{ax-b}{m}$

Solution exists if $\gcd(a,m) \mid b$ & infinite Sol. are there

$\gcd(a,m) = k$ then there are k (Number) of solutions of $ax \equiv b \pmod m$; $0 \le k < m$ ↓ integers

$4x \equiv 12 \pmod 8$ $\quad \gcd(4,8) = 4$, $4 \overline{)8}^{2}$ 8, 0

$\gcd(4,8) \mid 12$ yes then there are 4 values of x ↓ integers ; $0 \le x < 8$

$\frac{4x-12}{8}$

$0x \rightarrow \frac{4\times0-12}{8}$ ×

$1\checkmark \rightarrow \frac{4\times1-12}{8} = \frac{-8}{8}\checkmark$ $\quad x=1$

$2x \rightarrow \frac{4\times2-12}{8}$ ×

$3\checkmark \rightarrow \frac{4\times3-12}{8} = \frac{0}{8}\checkmark$ $\quad x=3$

$4x \rightarrow \frac{4\times4-12}{8}$ ×

$5\checkmark \rightarrow \frac{20-12}{8}\checkmark$ $\quad \frac{8}{8}$ $\quad x=5$

$6x \rightarrow \frac{24-12}{8}$ ×

$7\checkmark \rightarrow \frac{28-12}{8} = \frac{16}{8}\checkmark$ $\quad x=7$

There are infinite Solution of $4x \equiv 12 \pmod 8$

, $\cdots -7-8=-15$, $1-8=-7$, $x=1$, $1+8=9$, $9+8=17$, $17+8=25 \cdots$,

$-5-8=-13$, $3-8=-5$, $x=3$, $3+8=11$, $11+8=19$, $\cdots$,

$-3-8=-11$, $5-8=-3$, $x=5$, $5+8=13$, $13+8 \ldots$

$-1-8=-9$, $7-8=-1$, $x=7$, $7+8=15$, $15+8=23 \ldots$

If $x=k$ is Solution of $ax \equiv b \pmod m$

If $x = k$ is solution of $ax \equiv b \pmod m$
then $k \pm m$ is also the sol. of $ax \equiv b \pmod m$

Sol. of $3x \equiv 4 \pmod 7$

using the hit & trial

$\frac{3x \square - 4}{7}$

A = 5 ✗
B = 6 ✓
C = 4 ✗
D = 3 ✗

OR $\frac{3x-4}{7}$ $\gcd(3,7) = 1$ & $1 | 4$

∃ a value < 7 which is satisfy

$3x \equiv 4 \pmod 7$

$0 \le \text{Sol} < 7$

0	1	2	3	4	5, 6
$\frac{-4}{7}$ ✗	$\frac{-1}{7}$	$\frac{2}{7}$ ✗	$\frac{5}{7}$	$\frac{8}{7}$ ✗	$\frac{11}{7}$ ✗ $\frac{14}{7}$ ✓

OR using inverse

If $\gcd(a, m) = 1$ then $ax \equiv b \pmod m$ has a unique Sol. $< m$. s.t. $0 \le \text{sol} < m$

- Find the $\bar{a}^1$ of $a \bmod m$
- multiply the $\bar{a}^1$ to both side of $ax \equiv b \pmod m$
- $\bar{a}^1 \cdot b$ is the Sol.

$3x \equiv 4 \pmod 7$

This Linear Congruence can be Solved using inverse $\gcd(3,7) = 1$

Inverse of $3 \pmod 7$

$\gcd(3, 7)$ $3 < 7$

$3 \overline{)7}$ (2, 6) $\longrightarrow$ $7 = 3 \times 2 + 1 \Rightarrow 1 = 1 \times 7 + (-2) \times 3$

$1 \overline{)3}$ (3, 3, 0) $\longrightarrow$ $3 = 1 \times 3 + 0$

Bezout Coefficients of $3, 7$ are $1, -2$

Bezout coefficients of $3, 7$ are $1, -2$

then inverse of $3 \bmod 7 \Rightarrow 3\square \equiv 1 \bmod 7$

$\frac{3\square - 1}{7}$ $\quad 1\times$ $\quad -2 \checkmark$ $\quad \frac{3\times(-2)-1}{7} = -\frac{7}{7} \checkmark$

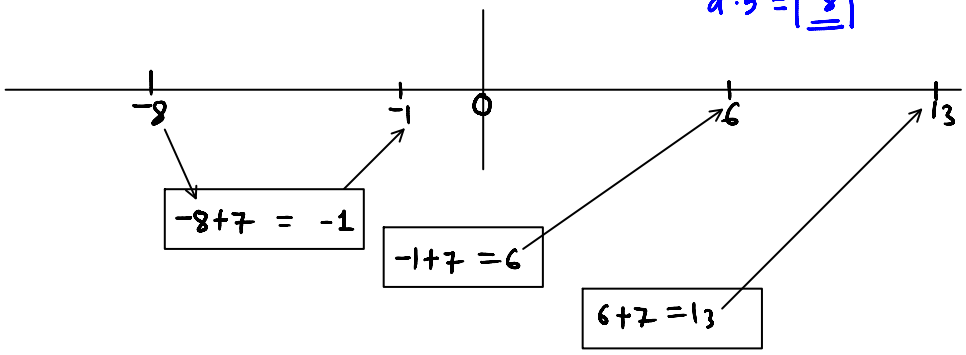
Hence $\boxed{-2 \text{ is an inverse of } 3 \bmod 7}$

Multiply $\bar{a}^1 = -2$ to both side of $\boxed{3x \equiv 4 \bmod 7}$

$-6x \equiv -8 \pmod 7$

$b = 4$

$\bar{a}^1 \cdot b = \boxed{-8}$



Q: 1) $4x \equiv 7 \pmod 8$

2) $4x \equiv 12 \pmod 8$

which one of the linear Congruence has the Sol.

$4x \not\equiv 7 \pmod 8$ $\quad \gcd(4,8) = 2 \nmid 7 \Rightarrow$ No Sol.

$\frac{4x-7}{8}$

$0x$ $\quad 5x$
$1x$ $\quad 6x$
$2x$ $\quad 7x$
$3x$
$4x$

$4x \equiv 12 \pmod 8$ has a Sol. because

$\gcd(4,8) = 4 \leftarrow 4 \mid 12$

using the hit & trial

$\frac{4x-12}{8}$

$0x$
$1\checkmark$
$2x$
$3\checkmark$
$4x$
$5\checkmark$
$6x$
$7\checkmark$

via, inverse $\quad \gcd(a,m) = 1$

$\frac{4x}{\gcd(4,8)} \equiv \frac{12}{\gcd(4,8)} \pmod 8$

$\frac{4x}{4} \equiv \frac{12}{4} \pmod 8$

$\boxed{x \equiv 3 \pmod 8}$ $\quad \gcd(1,8)$

inverse of $1 \bmod 8 = ?$

$\gcd(1,8) = 1$ ✓ $\quad 1 \mid \frac{8}{8}\ \frac{8}{0}$ ⇝ $8 = 1\times 8 + 0$

$1 = \square \times 1 + \square \times 8$

$1 = 9 \times 1 + (-1) \times 8$

$1\square \equiv 1 \bmod 8 \Rightarrow \frac{1\square - 1}{9}$

Q: B.C. are 9, −1 so 9 is an inverse of $1 \bmod 8$

Sol. $= \vec{a}^{-1} \cdot b$
$= 9 \times 3$
$= 27$ ✓
$27 - 3/8$ ✓

$5x \equiv 3 \pmod{10}$

Exam point of view

$\frac{5x-3}{10}$

A = 2 ⇝ $\frac{5\times 2 - 3}{10} = \frac{7}{10}$ ✗

B = 3 ⇝ $\frac{5\times 3 - 3}{10} = \frac{12}{10}$ ✗

C = 4 ⇝ $17/10$ ✗

D. No Sol. ✓

Proper sol. via hit & trial <m time

$\gcd(5,10) = 5$

$5 \nmid 3$ So No Sol.

Inverse method

$\gcd(5,10) \nmid 3$

No. Sol.

$5x \equiv 8 \pmod{6}$

Exam point of view hit & trial by options

$\frac{5x-8}{6}$

A → 1
B → 2
C → 3
D → 4

$x=1,\ \frac{5\times 1 - 8}{6} = \frac{-3}{6}$ ✗

$x=2,\ \frac{5\times 2 - 8}{6} = \frac{2}{6}$ ✗

$x=3,\ \frac{15-8}{6} = \frac{7}{6}$ ✗

$x=4,\ \frac{20-8}{6} = \frac{12}{6}$ ✓

Hit & trial <m

$\gcd(5,6) = 1$

$5 \mid \frac{1}{6}\ \frac{5}{1}\ \frac{5}{5}\ \frac{5}{0}$

$\gcd(5,6) = 1$ & $1 \mid 8$ Hence there exist 1 integer $0 \le K < 6$

0 → −8/6 ✗
1 → −3/6 ✗
2 → −2/6 ✗
3 → 2/6 ✗
4 → 12/6 ✓
5

via. inverse

if $\gcd(5,6) = 1$

$5x \equiv 8 \pmod 6$

inverse of 5 mod 6

$5\vec{a} \equiv 1 \bmod 6$

$\frac{5\square - 1}{6}$

$5 \mid \frac{1}{6}\ \frac{5}{1}$ ⟶ $6 = 5\times 1 + 1$

$1 \mid \frac{5}{5}\ \frac{5}{0}$ ⟶ $5 = 1\times 5 + 0$

$1 = 1\times 6 + (-1)\times 5$

B.C. are $1, -1$

$\frac{5\square - 1}{6}$ $\quad 1\times$ $\quad -1$ ✓

-1 is the inverse of 5 mod 6

$\vec{a}^{-1} = -1$

…, $-2-6=-8$, $4-6=-2$, $x=4$, $4+6=10$, $10+6=16$ …

OR

Via inverse

- Convert $ax = b \bmod m$

into the inverse Prob.

- find the inverse of $a' \equiv b' \pmod m$
- $\bar{a}' \times b$ is the Sol.

$ax \equiv b \bmod m$

$5x \equiv 8 \bmod 6$

$-5x \equiv -8 \bmod 6$

$\equiv$

$\ldots -8, -2, 4, \ldots$

Chinese Remainder Theorem Let $m_1, m_2 \cdots, m_n$ be relatively prime positive integers and $a_1, a_2 \cdots, a_n$ are arbitrary integers Then the system

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

has a unique solution modulo $m = m_1 \cdot m_2 \cdots, m_n$

$m = m_1 \cdot M_1$

$0 \le x < m$

- To construct a simultaneous sol. let $m = m_1 \cdot m_2 \cdot m_3 \cdots, m_n$
- $M_K = \frac{m}{m_K}$
- We know that $\exists\, y_K$ is an inverse of $M_K \pmod{m_K}$

$\gcd(M_K, m_K) = 1$

$$M_K \boxed{y_K} \equiv 1 \pmod{m_K}$$

$M_K \boxed{y_K} - 1$

m_K

- $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots, a_n M_n y_n$ $\quad x \equiv a_K M_K y_K \equiv a_K \bmod m_K$

Q: $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

has a unique Sol. to modulo $m = m_1 \cdot m_2 \cdot m_3 = 3 \times 5 \times 7 = 105$

There exist a unique value of x s.t. $0 \le x < 105$

$a_1 = 2, \; a_2 = 3, \; a_3 = 2$

$m_1 = 3, \; m_2 = 5, \; m_3 = 7$

- $m = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$
- $M_1 = \frac{m_1 \cdot m_2 \cdot m_3}{m_1} = \frac{m}{m_1} = \frac{3 \times 5 \times 7}{3} = 35$

$M_2 = \frac{m}{m_2} = \frac{3\times5\times7}{5} = 21$

$M_3 = \frac{m}{m_3} = \frac{3\times5\times7}{7} = 15$

y_1 is an inverse of $M_1 \pmod{m_1} \Rightarrow M_1 y_1 \equiv 1 \pmod{m_1}$

$\frac{M_1 \boxed{y_1} - 1}{m_1}$, y_1 is an inverse of $35 \bmod 3$

$35 y_1 \equiv 1 \bmod 3$

$\frac{35\boxed{y_1}-1}{3} \Rightarrow 0 \le y_1 < 3 \Rightarrow$ 0 ×, 1 ×, 2 ✓ $\quad \boxed{y_1 = 2}$

y_2 is an inverse of $M_2 \bmod m_2 \Rightarrow M_2 y_2 \equiv 1 \bmod m_2$

$0 \le y_2 < 5$ 0 ×, 1 ✓ $\Rightarrow \frac{M_2 y_2 - 1}{m_2} \Rightarrow \frac{21 \cdot y_2 - 1}{5}$

$\Rightarrow \boxed{y_2 = 1}$

y_3 is an inverse of $M_3 \bmod m_3 \Rightarrow M_3 y_3 \equiv 1 \bmod m_3$

$0 \le y_3 < 7$ 0 ×, 1 ✓ $\quad 15 y_3 \equiv 1 \bmod 7$

$M_3 = 15$, $m_3 = 7$ $\quad \frac{15\square - 1}{7}$ $\quad \frac{15 y_3 - 1}{7}$ $\quad \boxed{y_3 = 1}$

•••• $x = a_1 \cdot y_1 M_1 + a_2 \cdot y_2 \cdot M_2 + a_3 \cdot y_3 \cdot M_3$

$= 2 \cdot y_1 \cdot 35 + 3 \cdot y_2 \cdot 21 + 2 \cdot y_3 \cdot 15$

$= 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15$

$= 140 + 63 + 30$

$x = 233$

as $233 > 105$ (m)

$105 \overline{)\,233}$ (2), 210, 23

$\boxed{x = 23 \bmod (105)}$

Q: $x \equiv 2 \pmod 5$ $\quad a_1 = 2$, $m_1 = 5$ $\quad m = 5\times7 = 35$

$x \equiv 3 \pmod 7$ $\quad a_2 = 3$, $m_2 = 7$ $\quad M_1 = 7$, $M_2 = 5$

MCQ 1> This system has the unique Sol. to

modulo $m = ?$. $\boxed{m = 5 \times 7 = 35}$

MCQ 27 If the above system has the sol. to modulo $m = 35$ & y_i is the inverse of $M_i \bmod m_i$ $i = 1, 2$ then

$M_1, M_2, y_1, y_2 = ?$.

$M_1 = 7$
$m_1 = 5$

$\frac{7y_1 - 1}{5} \Rightarrow 0\times \quad 1\times \quad 2\times \quad 3\checkmark$ $\boxed{y_1 = 3}$

$M_2 = 5$
$m_2 = 7$

$\frac{5y_2 - 1}{7} \Rightarrow 0\times \quad 1\times \quad 2\times \quad 3\checkmark$ $\boxed{y_2 = 3}$

$m = ?$. y_1
$M_1 = ?$ y_2
$M_2 = ?$ x

MCQ 3: $\boxed{x = a_1 y_1 M_1 + a_2 y_2 M_2}$

↳ if y_1 is an inverse of $7 \bmod 5 = 3\checkmark$
y_2 is an inverse of $5 \bmod 7 = 3\checkmark$ then $x = ?$.

$x = ?\cdot 3 \cdot 7 + 3 \cdot 3 \cdot 5 = 42 + 45 = 87$

$87 > 35$

$35 \overline{)87}\ 2$
70
17

$\boxed{x = 17}$

Consider the following System

$m = 3 \times 2 = 6$

$x \equiv 2 \pmod 3$ $\quad a_1 = 2$, $m_1 = 3$ $\quad M_1 = \frac{3\times 2}{3} = 2$

$x \equiv 1 \pmod 2$ $\quad a_2 = 1$ $\quad m_2 = 2$ $\quad M_2 = \frac{3\times 2}{2} = 3$

MCQ: 1 If the system has a unique sol. to modulo m then $m = ?$.

$m = 6$

MCQ: 2 M_i $i = 1, 2$ $\quad M_1 = \frac{6}{3} = 2$, $M_2 = \frac{6}{2} = 3$

MCQ 3 If the system has unique sol. to mod 6 & y_1 is an inverse of $M_1 \pmod{m_1}$ then

$y_1 = ?$. $\quad m_1 = 3$

$M_1 = 2$

$\frac{My_1 - 1}{m_1} \Rightarrow \frac{2y_1 - 1}{3}$ $\quad 0\times \quad 1\times \quad 2\checkmark$ $\quad \boxed{y_1 = 2}$

Similarly $y_2 = ?$

$\frac{M_2 y_2 - 1}{m_2} = \frac{3y_2 - 1}{2}$ $\quad 0\times \quad 1\checkmark$ $\quad \boxed{y_2 = 1}$

MCQ 3

If the above system has the unique sol. to mod 6 & y_i is the inverse of $M_i \pmod{m_i}$ $i = 1, 2$ & their values are

$y_1 = 2$

$y_2 = 1$

then the sol x is $= ?$

$x = a_1 \cdot y_1 M_1 + a_2 \cdot y_2 \cdot M_2$

$= 2 \cdot 2 \cdot 2 + 1 \cdot 1 \cdot 3$

$= 8 + 3 = 11$

Now $11 > 6$ $\quad \boxed{m = 6}$

$6 \overline{)11}\ 1$

$\underline{6}$

5 $\quad \boxed{x = 5}$

- C.R.T. Revision
- F.L.T.
- Cryptography
- Revision unit 1-06 [MCQ]

Fermat's Little Theorem

If P is prime and a is an integer not divisible by P then $a^{P-1} \equiv 1 \pmod{P}$

$\frac{a^{P-1} - 1}{P}$ $\quad \Rightarrow a^P \equiv a \pmod{P}$

Ex: 341 is a Prime $a = 2$

$341 = 11 \times 31$

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

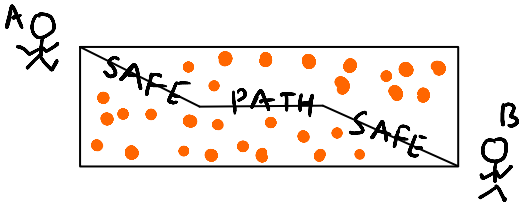
CRYPTOGRAPHY

Caesar Cipher — Encryption & Decryption

Encryption ⟶ $P + K \pmod{26}$

Decryption ⟶ $P - K \pmod{26}$

A 0	F 5	K 10	P 15	U 20	Z-25
B 1	G 6	L 11	Q 16	V -21	
C 2	H 7	M 12	R 17	W 22	
D 3	I 8	N 13	S 18	X 23	
E 4	J 9	O 14	T 19	Y 24	



B: "MEET ME IN THE PARK"

12 4 4 19 12 4 8 13 19 7 4 15 0 17 10

Code: $(P+3) \bmod 26$

15, 7, 7, 22 15, 7, 11, 16, 22, 10, 7 18, 3, 20, 13

B: PHHW PH LQ WKH SDUN

A PHHW PH LQ WKH SDUN

15, 7, 7, 22 15, 7 11, 16, 22, 10, 7, 18, 3, 20, 13

Decode $(P-3) \pmod{26}$

12, 4, 4, 19 12, 4, 8, 13, 19, 7, 4, 15, 0, 17, 10

M E E T ME IN THE P A R K

MCQ

Msg. of → "CLEAR" "Q" by (P+10) mod 26

2, 11, 4, 0 17, 16

(P+10) mod 26

12, 21, 14, 10, 27, 26

12, 21, 14, 10, 01, 0

M, V, O K, B A

27 mod 26

26 | 27 (1), 26, 01

26 mod 26

26 | 26 (1), 26, 00

MCQ If M V O K B is the Encrypted msg by the Code (P+10) mod 26 then the original msg is

M	V	O	K	B
12	21	14	10	01
-10	-10	-10	-10	-10
2	11	4	0	17
C	L	E	A	R

26 | 27 (1), 26, 01 → 27

Msg : "K"

Code: (7P+3) mod 26

K = 10

code: (7×10+3) mod 26

: 73 mod 26

26 | 73 (02), 52, 21

21 : V

K → 10 → 21 → V

ap+b (mod 26)

Affine code

↓

Encryptim is possible

↓

Decryptim is possible if inverse of a mod 26 exist

[a should be odd]

Decode $7p+3 \mod 26$ 7 is odd then yes it could be decrypted.

Find the inverse of $7 \mod 26$

$$26 = 7 \times 3 + \boxed{5}$$

$$7 = 5 \times 1 + \boxed{2}$$

$$5 = 2 \times 2 + \boxed{1}$$

$$1 = 5 + (-2) \times 2$$

$$1 = 5 + (-2) \times [7 + (-1) \times 5]$$

$$= -2 \times 7 + 3 \times 5$$

$$= -2 \times 7 + 3 \times [26 + (-3) \times 7]$$

$$= 3 \times 26 + (-11) \times 7$$

$\frac{7\square - 1}{26}$ $\quad 3x$ $\quad -11$

Resultant coefficients are 3, -11,

Hence -11 is the inverse of $7 \mod 26$

V: 21

21 - 11 = 10 : K is the original Msg