Unit 6

OMR Sheet No.________ Registration No. ①

Note: i) This sheet must be submitted to the invigilator along with the question paper on completion of examinatio
ii) Exchange of sheet will be considered as UMC.

Divisibility and Modular Arithmetic

Division: If a and b are integers with a we say that a divides b if there is an integ c such that b = ac or if $\frac{b}{a}$ is an integer. When a divides b, a is a factor or divisor of b and that b is a multiple of a. a|b is notation that a divides b. and $a \nmid b$ when a doesnot divide b.

Eg Determine whether 3|7 and whether 3|12

$3 \nmid 7$ since $\frac{7}{3}$ is not an integer and

3|12 since $\frac{12}{3} = 4$ is an integer.

Eg Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Sol Positive integers divisible by d are of the type dk, k is positive integer.

Also $0 \le dk \le n$

$\Rightarrow 0 \le k \le \frac{n}{d}$

∴ there are $\left\lfloor \frac{n}{d} \right\rfloor$ positive integers not exceeding n that are divisible by d.

Theorem: Let a, b, c be integers, a ≠ 0. Then

i) if a|b and a|c then a|(b+c).

ii) if a|b, then a|bc for all integers c;

iii) if a|b, b|c then a|c

Corollary: If a, b and c are integers where a ≠ 0 such that a|b and a|c then a|mb+nc whenever m and n are integers

LOVELY PROFESSIONAL UNIVERSITY PUNJAB (INDIA)
Secrecy Cell
Examination Division

Division Algorithm

Let a be an integer and d a positive int
Then there are unique integers q and r
with $0 \leq r < d$ such that $a = dq + r$.

Def: Here a = dividend, d = divisor, q = quotient
r = remainder.

Notation: $q = a \text{ div } d \left[= \left\lfloor \frac{a}{d} \right\rfloor\right]$
$r = a \bmod d \; [= a - d]$

Eg What are the quotient and remainder when 101 is divided by 11?

Sol We have $101 = 11 \times 9 + 2$
$\therefore q = 9 = 101 \text{ div } 11$
$r = 2 = 101 \bmod 11$

Eg What are the quotient and remainder when -11 is divided by 3?

Sol We have
$-11 = 3(-4) + 1$
$q = -4 = -11 \text{ div } 3$.
$r = 1 = -11 \bmod 3$

Modular Arithmetic

Def: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a-b$.
$a \equiv b \pmod{m}$

Theorem: Let a and b be integers, let m be a positive integers. Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.

Eg Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Sol If $17 \equiv 5 \pmod{6}$
then 6 divides $17 - 5 = 12$ which is true
$\therefore$ 17 is congruent to 5 modulo 6.

If $24 \equiv 14 \bmod 6$
$\Rightarrow$ 6 divides $24 - 14 = 10$ which is not true
$\therefore 24 \not\equiv 14 \pmod{6}$

Sheet No.________ Registration No. 3

e: i) This sheet must be submitted to the invigilator along with the question paper on completion of examination.
ii) Exchange of sheet will be considered as UMC.

Theorem: Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer k s.t

$a = b + km$

$a \equiv b \mod m$

$\Leftrightarrow m$ divides $a - b$

$\Leftrightarrow a - b = mk$, integer k

$\Leftrightarrow a = b + mk$

* The set of all integers congruent to an integer a modulo m is called congruence class of a modulo m.

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Eg we know $7 \equiv 2 \pmod{5}$

$11 \equiv 1 \pmod{5}$

$\therefore 18 \equiv 3 \pmod{5}$ & $77 \equiv 2 \pmod{5}$

* If $ac \equiv bc \pmod{m}$ then $a \equiv b \pmod{m}$ maybe false.

For eg $7 \cdot 5 \equiv 8 \cdot 5 \mod 5$

$\because$ 5 divides $7 \cdot 5 = 35 - 8 \cdot 5 = 40$

$35 - 40 = -5$

but $7 \not\equiv 8 \mod 5$

If $a \equiv b \mod m$ and $c \equiv d \pmod{m}$ then $a^c \equiv b^d \pmod{m}$ maybe false

Corollary: Let m be a positive integer and let a and b be integers. Then $(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$

and $ab \mod m = ((a \mod m)(b \mod m)) \mod m$

Lovely Professional University Punjab (India)
Secrecy Cell
Examination Division

Arithmetic modulo m

We can define arithmetic operations on the set of non negative integers less than m i.e $\{0, 1, 2, \dots m-1\}$

Now $a +_m b = (a+b) \bmod m$

$\cdot$ $a \cdot_m b = (a \cdot b) \bmod m$.

Eg Find $7 +_{11} 9$ and $7 \cdot_{11} 9$

$7 +_{11} 9 = (7+9) \bmod 11$

$= 16 \bmod 11 = 5$

$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11$

$= 8$

Note: The operation $+_m$ & $\cdot_m$ satisfy the following properties:

Closure: If $a, b \in \mathbb{Z}_m$ then $a +_m b$, $a \cdot_m b \in \mathbb{Z}_m$

Associativity: If $a, b, c \in \mathbb{Z}_m$ then

$(a +_m b) +_m c = a +_m (b +_m c)$ and

$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

Commutativity: If $a, b \in \mathbb{Z}_m$ then

$a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$

Identity elements: 0 and 1 are identity elts for addition & multiplication modulo m.

$a +_m 0 = a = 0 +_m a$

$a \cdot_m 1 = a = 1 \cdot_m a$

Additive inverse: If $a \neq 0$ belongs to $\mathbb{Z}_m$, then $m-a$ is an additive inverse of a modulo m and 0 is its own additive inverse $a +_m (m-a) = 0$ and $0 +_m 0 = 0$

Distributivity: If $a, b, c \in \mathbb{Z}_m$ then

$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and

$(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Sheet No.__________ Registration No. 5

e: i) This sheet must be submitted to the invigilator along with the question paper on completion of examination.
ii) Exchange of sheet will be considered as UMC.

Primes and Greatest Common Divisors

A prime is an integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Def: An integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

* The integer n is composite iff ∃ an integer a such that $a | n$ and $1 < a < n$

Eg: 7 is prime because its only factors are 1 and 7.
9 is not prime because it has factors 1, 3 and 9

Theorem: The fundamental theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Eg Prime factorisation of

a) $100 = 2.2.5.5 = 2^2.5^2$

b) $641 = 641$

c) $999 = 3.3.3.37 = 3^3.37$

d) $1024 = 2.2.2.2.2.2.2.2.2.2 = 2^{10}$

Theorem: If n is a composite integer then n has a prime divisor less than or equal to $\sqrt{n}$

Eg Show that 101 is prime

We know $10 < \sqrt{101} < 11$

Prime no. less than 11 are 2, 3, 5, 7

Now $2 \nmid 101$

$3 \nmid 101$

$5 \nmid 101$

$7 \nmid 101$

∴ 101 has no prime divisor. ∴ 101 is itself prime.

Eg Find prime factorization of 7007

$7007 = 7 \cdot 1001$

Now prime factors of 1001

$31 < \sqrt{1001} < 32$

Prime no.s less than 32 are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31

$2 \nmid 1001$, $3 \nmid 1001$, $5 \nmid 1001$,

$7 \mid 1001$

$1001 = 7 \cdot 143$

$\therefore 7007 = 7 \cdot 7 \cdot 143$

Now $11 < \sqrt{143} < 12$

Prime no.s less than 12 are 2, 3, 5, 7, 11

$2, 3, 5, 7 \nmid 143$ and $143 = 11 \cdot 13$.

$\therefore 7007 = 7^2 \cdot 11 \cdot 13$.

$$\begin{array}{r} 27 \\ \times 27 \\ \hline 189 \\ 54 \\ \hline 729 \end{array} \quad 4$$

$$\begin{array}{r} 31 \\ 31 \\ \hline 31 \\ 93 \\ \hline 961 \end{array}$$

Theorem: There are infinitely many primes.

* Primes of the form $2^p - 1$ are called Mersenne primes.

eg: $2^2 - 1 = 3$ $\quad 2^5 - 1 = 31$ $\quad$ are Mersenne primes

$2^3 - 1 = 7$ $\quad 2^7 - 1 = 127$

But $2^{11} - 1 = 2048 - 1 = 2047$ is not Mersenne prime since $2047 = 23 \cdot 89$

⑥

5.
*

Sheet No.__________ Registration No. ⑦

e: i) This sheet must be submitted to the invigilator along with the question paper on completion of examination.
ii) Exchange of sheet will be considered as UMC.

Greatest Common Divisors and Least common Multiples

Def: Let a and b be integers; not both zero. The largest integer d such that $d | a$ and $d | b$ is called the greatest common divisor of a and b ($gcd(a, b)$).

Eg What is $gcd(24, 36)$?
Divisors of 24 = 1, 2, 3, 4, 6, 8, 12, 24
Divisors of 36 = 1, 2, 3, 4, 6, 9, 12, 18, 36.
$\therefore gcd(24, 36) = 12$.

Eg What is $gcd(17, 22)$?
Divisors of 17 are 1, 17
Divisors of 22 are 1, 2, 11, 22.
$gcd(17, 22) = 1$

Def: The integers a and b are relatively prime if their gcd is 1.
$\therefore$ 17 and 22 are relatively prime.

Def: The integers $a_1, a_2, \dots, a_n$ are pairwise relatively prime if $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Eg Determine whether 10, 17 and 21 are pairwise relatively prime and whether the integers 10, 19 and 24 are pairwise relatively prime.
$gcd(10, 17) = 1$, $gcd(10, 21) = 1$, $gcd(17, 21) = 1$
$\therefore$ 10, 17 and 21 are pairwise relatively prime.
$gcd(10, 19) = 1$, $gcd(19, 24) = 1$
but $gcd(10, 24) = 2$
$\therefore$ 10, 19 & 24 are not pairwise relatively prime.

To find gcd(a, b)

If $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$

$b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$

then $gcd(a, b) = p_1^{min(a_1, b_1)} p_2^{min(a_2, b_2)}, \dots p_n^{min(}$

Eg Find gcd (120, 500)

$120 = 2.2.2.3.5 = 2^3 3 5$

$500 = 2.2.5.5.5 = 2^2.5^3$.

$gcd(120, 500) = 2^2.3^0.5 = 20$

Def: The least common multiple of the positive integers a and b is the smallest positive integers that is divisible by both a and b (lcm (a, b))

$lcm(a, b) = p_1^{max(a_1, b_1)} p_2^{max(a_2, b_2)} \dots p_n^{max(a_n, b_n)}$

Eg $lcm(2^3 3^5 7^2, 2^4 3^3) = 2^4.3^5.7^2$

Theorem: Let a and b be positive integers. Then $ab = gcd(a, b)\, lcm(a, b)$

Euclidean Algorithm

lemma: Let $a = bq + r$ where a, b, q and r are integers. Then g.c.d (a, b) = gc~~d(b,~~ r)

Ques Find the gcd(414, 662) by Euclidean algorithm

$662 = 414.1 + 248$

$414 = 248.1 + 166$

$248 = 166.1 + 82$

$166 = 82.2 + 2$

$82 = 2.41$ ~~2~~

414) 662 (1
414
248) 414 (1
248
166) 248 (1
166
82) 166 (2
164
gcd ← ②) 82 (41
82
0

Hence gcd (414, 662) = 2, because 2 is the last nonzero remainder.

GCD's as linear combination

gcd(a, b) can be expressed as a linear combination with integer coefficients of a and b. For eg gcd (6, 14) = 2

$2 = 6\underline{(-2)} + 14.\underline{1}$

⑧

Sheet No.______ Registration No. ⑨

e: i) This sheet must be submitted to the invigilator along with the question paper on completion of examination.
ii) Exchange of sheet will be considered as UMC.

Theorem : Bézout's theorem

If a and b are positive integers, then there exist integers s and t such that $gcd(a,b) = sa + tb$

Def : If a and b are positive integers, then integers s and t such that $gcd(a,b) = sa + tb$ are called Bézout coefficients of a and b

Also the eq $gcd(a,b) = sa + tb$ is called Bézout identity.

Q Express $gcd(252,198) = 18$ as a linear combination of 252 and 198

Firstly, show $gcd(252,198) = 18$

$252 = 198 \cdot 1 + 54$

$198 = 54 \cdot 3 + 36$

$54 = 36 \cdot 1 + 18$

$36 = 18 \cdot 2$

$\therefore gcd(252,198) = 18$

54
198 3
162
36

Now moving backwards,

$18 = 54 - 36 \cdot 1$

$= 54 - (198 - 54 \cdot 3) \cdot 1$

$= 54 \cdot 1 - 198 \cdot 1 + 54 \cdot 3$

$= 54 \cdot 4 - 198 \cdot 1$

$= (252 - 198 \cdot 1) \cdot 4 - 198 \cdot 1$

$= 252 \cdot 4 - 198 \cdot 4 - 198 \cdot 1$

$= 252 \cdot 4 - 198 \cdot 5$

$\therefore 18 = 4 \cdot 252 - 5 \cdot 198$

Bezout coefficients of 252 and 198 are 4 and -5

Lemma: If a, b and c are positive integers such that $\gcd(a, b) = 1$ and $a | bc$ then $a | c$.

Lemma: If p is a prime and $p | a_1 a_2 \cdots a_n$ where a_i is an integer, then $p | a_i$ for some i.

Eg $14 \equiv 8 \pmod 6$

but dividing ~~throughout~~ both sides of congruence by 2

$7 \not\equiv 4 \pmod 6$.

Theorem: Let m be a positive integer and let a, b and c be integers. If $ac = bc \pmod m$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod m$

$ac \equiv bc \pmod m$

$\Rightarrow$ m divides $ac - bc$

$\Rightarrow m \mid (a-b)c$.

$\Rightarrow m \mid a-b \quad \because \gcd(c, m) = 1$

$\Rightarrow a \equiv b \pmod m$.

Twin primes: Two prime no.s with a difference of 2. Eg → 3 and 5, 5 and 7

⑩

Sheet No.__________ Registration No. ⑪

e: i) This sheet must be submitted to the invigilator along with the question paper on completion of examination.
ii) Exchange of sheet will be considered as UMC.

Exercise

14) Which positive integers less than 12 are relatively prime to 12?
1, 5, 7, 11

15) Which positive integers less than 30 are relatively prime to 30?
1, 7, 11, 13, 17, 19, 23, 29

16) Determine whether the integers in each of these sets are pairwise relatively prime.

a) 21, 34, 55
gcd(21, 34) = 1
gcd(34, 55) = 1
gcd(21, 55) = 1
∴ pairwise relatively prime

b) 14, 17, 85
gcd(17, 85) = 17 ≠ 1
∴ Not pairwise relatively prime.

c) 25, 41, 49, 64
5^2 7^2 8 2^6
pairwise relatively prime

d) 17, 18, 19, 23
gcd(a_i, a_j) = 1
∴ pairwise relatively prime

24) & 26) Find gcd (lcm)
a) $2^2.3^3.5^5$, $2^5.3^3.5^2$ — $2^2.3^3.5^2$ $(2^5.3^3.5^5)$
b) $2.3.5.7.11.13$, $2^{11}.3^9.11.17^{14}$ — $2.3.11$ $(2^{11}.3^9.5.7.11.13.17^{14})$
c) $17, 17^{17}$ — 17 (17^{17})
d) $2^2.7$, $5^3.13$ — 1 $(2^2.5^3.7.13)$
e) $0, 5$ — 5.
f) $2.3.5.7$, $2.3.5.7$ — $2.3.5.7$ $(2.3.5.7)$

25) & 27) Find gcd (lcm)
a) $3^7.5^3.7^3$, $2^{11}.3^5.5^9$ — $3^5.5^3$ $(2^{11}.3^7.5^9.7^3)$
b) $11.13.17$, $2^9.3^7.5^5.7^3$ — 1 $(2^9.3^7.5^5.7^3.11.$ $17)$
c) 23^{31}, 23^{17} — 23^{17} (23^{31})
d) $41.43.53$, $41.43.53$ — $41.43.53$ $(41.43.53)$

e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$ - 1 $(2^{12} 3^{13} 5^{17} 7^{21})$ ⑫

f) 1111, 0 - 1111 (0)

39) Express gcd as a linear combination of these integers

a) 10, 11

$11 = 10 \cdot 1 + 1$

$10 = 1 \cdot 10$

$\gcd(10, 11) = 1$

$1 = 11 - 10 \cdot 1$

b) 21, 44

$44 = 21 \cdot 2 + 2$

$21 = 2 \cdot 10 + 1$

$2 = 1 \cdot 2$

$\gcd(21, 44) = 1$

$1 = 21 - 2 \cdot 10$

$= 21 - (44 - 21 \cdot 2) \cdot 10$

$= 21 - 44 \cdot 10 + 21 \cdot 20$

$= 21 \cdot 21 - 44 \cdot 10$

c) 36, 48

$48 = 36 \cdot 1 + 12$

$36 = 12 \cdot 3$

$\gcd(36, 48) = 12$

$12 = 48 - 36 \cdot 1$

d) 34, 55

$55 = 34 \cdot 1 + 21$

$34 = 21 \cdot 1 + 13$

$21 = 13 \cdot 1 + 8$

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2$

$\gcd(34, 55) = 1$

$1 = 3 - 2 \cdot 1$

$= 3 - (5 - 3 \cdot 1) \cdot 1$

$= 3 - 5 \cdot 1 + 3 \cdot 1$

$= 3 \cdot 2 - 5 \cdot 1$

$= (8 - 5 \cdot 1) \cdot 2 - 5 \cdot 1$

$= 8 \cdot 2 - 3 \cdot 5$

$= 8 \cdot 2 - 3 \cdot (13 - 8 \cdot 1)$

$= 8 \cdot 5 - 3 \cdot 13$

$= (21 - 13 \cdot 1) \cdot 5 - 3 \cdot 13$

$= 21 \cdot 5 - 13 \cdot 8 = 21 \cdot 5 - (34 - 21) \cdot 8$

$= 21 \cdot 13 - 34 \cdot 8 = (55 - 34 \cdot 1) \cdot 13 - 34 \cdot 8$

$= 55 \cdot 13 - 21 \cdot 34$

Linear Congruences

⑬

A congruence of the form $ax \equiv b \pmod{m}$ where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

If $a\bar{a} = 1 \pmod{m}$, if such integer $\bar{a}$ exists then it is called inverse of a modulo m.

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

* Inverse of 3 modulo 7.

$3a \equiv 1 \pmod{7}$

$\Rightarrow 7$ divides $3a - 1$

If $a = 1$ ×

$a = 2$ ×

$a = 3$ ×

$a = 4$ ×

$a = 5$ ✓ $7 \mid 14$.

$\therefore a = 5$

Hence 5 is an inverse of 3 modulo 7.

In fact $[5] = \{-9, -2, 5, 12, 19, \ldots\}$.

So, all these are inverse.

Eg Find an inverse of 3 modulo 7 by first finding Bézout coefficients of 3 and 7.

$\gcd(3, 7) = 1$

$$3\overline{)7}\,\llcorner 2 \qquad \begin{array}{r}6\\\hline 1\end{array}\overline{)2}\,\llcorner 2 \qquad \begin{array}{r}2\\\hline \times\end{array}$$

$7 = 3.2 + 1$

$2 = 1.2 + 0$.

So $1 = 1.7 - 2.3$.

$\therefore$ 1 and -2 are Bezout coefficients of 7 and 3. So we have -2 is an inverse of 3 modulo 7.

~~Eg Find an inverse of 101 modulo 4620~~

~~$4620 = 45.101 + 75$~~

~~$75 = 1.45 + 30$~~

~~$30 = 30.1$~~

~~$101\overline{)4620}\,\llcorner 45$~~

~~404~~

~~580~~

~~505~~

~~$45\overline{)75}\,\llcorner 1$~~

~~45~~

~~$1\overline{)30}\,\llcorner 30$~~

~~30~~

~~0~~

21
34
84
13
55
65
65
71

$2^3.5.7$

$8 \times 25 \times 7$

200×7

1400

Eg 7 : Find an inverse of 101 modulo 46
Using Euclidean algorithm

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

Now gcd(4620, 101) = 1
since the last non remainder is 1.

Now to find Bezout coefficients.

$1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (23 - 7 \cdot 3)$

$= 8 \cdot 3 - 1 \cdot 23$

$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23)$

$= 8 \cdot 26 - 9 \cdot 23$

$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26)$

$= -9 \cdot 75 + 26 \cdot 26$

$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75)$

$= 26 \cdot 101 - 35 \cdot 75$

$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$

$= -35 \cdot 4620 + 1601 \cdot 101$

-35 and 1601 are Bezout coefficients for 4620 and 101

∴ 1601 is an inverse of 101 modulo 4620

101) 4620 (45
404
580
505
75) 101 (1
75
26) 75 (2
52
23) 26 (1
23
3) 23 (7
21
2) 3 (1
2
1) 2 (2
2
x

22
35
45
175
140
1575
26
1601

Eg What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$

$ax \equiv$

$\gcd(3, 7) = 1$

$7 = 3 \cdot 2 + 1$

$1 = 7 - 2 \cdot 3$

inverse of 3 mod 7 is -2.

Now, multiplying both sides of the congruence by -2 .

$7 \mid 3x-4$

$7 \mid (3x-4)\cdot -2$.

$3x \equiv 4 \pmod{7}$

$\Rightarrow -2\cdot 3x \equiv -2\cdot 4 \pmod{7}$

$\Rightarrow -6x \equiv -8 \pmod{7}$

Now $-6 \equiv 1 \bmod 7$

Also $-8 \equiv -1 \bmod 7$

$-8 \equiv 6 \bmod 7$.

$\frac{-8}{7}$

-1

$\Rightarrow x \equiv -8 \equiv 6 \bmod 7$

Now we need to determine whether every x with $x \equiv 6 \bmod 7$, .

Assume $x \equiv 6 \bmod 7$.

Then $3 \equiv 3 \bmod 7$

$\Rightarrow 3x \equiv 18 \bmod 7$

$\equiv 4 \bmod 7$.

which ~~follows~~ shows that all such x satisfy the congruence.

$\therefore$ Solutions are $x \equiv 6 \bmod 7$

namely, ..., $-15, -8, -1, 6, 13, 20, 27, \ldots$

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively p
positive integers greater than one and a_1,
an arbitrary integers Then the system

$x \equiv a_1 (\text{mod } m_1)$

$x \equiv a_2 (\text{mod } m_2)$

$x \equiv a_3 (\text{mod } m_3)$

$\vdots$

$x = a_n (\text{mod } m_n)$

has a unique solution modulo $m = m_1 m_2 - m$
(i.e there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution)

Eg solve $x \equiv 2 (\text{mod } 3)$
$x \equiv 3 (\text{mod } 5)$
$x \equiv 2 (\text{mod } 7)$

we have 3, 5 and 7 pairwise relatively prime positive integers > 1

$\because$ $\gcd(3,5) = \gcd(5,7) = \gcd(3,7) = 1$

Now $m = 3.5.7 = 105$ $m_1 = 3,\ m_2 = 5,\ m_3 = 7$

$M_1 = \frac{m}{3} = 35$

$M_2 = \frac{m}{5} = 21$

$M_3 = \frac{m}{7} = 15$

Find inverse y_k of M_k modulo m_k

Inverse of 35 modulo 3.

$\gcd(35, 3) = 1$.

$35 = 11 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$$\begin{aligned} 1 &= 1 \cdot 3 - 1 \cdot 2 \\ &= 1 \cdot 3 - 1 \cdot (35 - 11 \cdot 3) \\ &= -1 \cdot 35 + 12 \cdot 3 \end{aligned}$$

Inverse is -1

$\therefore$ inverse is $-1 + 3 = 2$ $y_1 = 2$

```
3)35(11
  33
  --
   2)3(1
     2
     -
     1)2(2
       2
       -
       0
```

rse of 21 modulo 5

$\gcd(5,21) = 1$

$21 = 4 \cdot 5 +$ [illegible]

$5 = 5 \cdot 1$

$1 = 21 - 4 \cdot 5$

Inverse is 1

$y_2 = 1$

Inverse of 15 modulo 7

$\gcd(15,7) = 1$

$15 = 2 \cdot 7 + 1$

$7 = 7 \cdot 1$

$1 = 15 - 2 \cdot 7$

$y_3 = 1$

The solution of the system are those x s.t

$x \equiv (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \bmod m$

$= (2 . 35 . 2 + 3 . 21 . 1 + 2 . 15 . 1) \bmod m$

$= (140 + 63 + 30) \bmod 105$

$= 233 \bmod 105$

$= 23 \pmod{105}$

∴ 23 is the smallest positive integer that satisfies the system.

Exercise

1) show that 15 is an inverse of 7 mod

gcd (7, 26) = 1

$26 = 3 \cdot 7 + 5$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1$

Now $1 = 5 - 2 \cdot 2$

$= 5 - 2 \cdot (7 - 1 \cdot 5)$

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

$= -2 \cdot 7 + 3 \cdot (26 - 3 \cdot 7)$

$= 3 \cdot 26 - 11 \cdot 7$

Inverse is −11 which is same as

$-11 + 26 = 15 \mod 26$.

2) show that 937 is an inverse of 13 modulo 2436.

13) 2436 (187
13
113
104
96
91
5) 13 (2
10
3) 5 (1
3
2) 3 (1
2
1) 2 (2
2
x

$2436 = 187 \cdot 13 + 5$

$13 = 2 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

130
26
104
13
91

$1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (5 - 1 \cdot 3)$

$= -1 \cdot 5 + 2 \cdot 3$.

$= -1 \cdot 5 + 2 \cdot (13 - 2 \cdot 5)$

$= \cancel{-1 \cdot 5}\ 2 \cdot 13 - 5 \cdot 5$

$= 2 \cdot 13 - 5 \cdot (2436 - 187 \cdot 13)$

$= -5 \cdot 2436 + 937 \cdot 13$.

Inverse is 937.

$^{4}\ ^{3}$
187
5
935

7 mo

d an inverse of a modulo m for each (1
the pairs

a) $a = 4,\ m = 9$

$9 = 2 \cdot 4 + 1$

$4 = 4 \cdot 1$

$1 = 9 - 2 \cdot 4$

Inverse is -2 or $-2 + 9 = 7$ or 16

b) $a = 19,\ m = 141$

$141 = 7 \cdot 19 + 8$

$19 = 2 \cdot 8 + 3$

$8 = 2 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

$1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (8 - 2 \cdot 3)$

$= -1 \cdot 8 + 3 \cdot 3$

$= -1 \cdot 8 + 3 \cdot (19 - 2 \cdot 8)$

$= 3 \cdot 19 - 7 \cdot 8$

$= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19)$

$= -7 \cdot 141 + 52 \cdot 19$

Inverse is 52

$$\begin{array}{r} 19 \\ 7 \\ \hline 133 \end{array}$$

c) $a = 55,\ m = 89$

$89 = 1 \cdot 55 + 34$

$55 = 1 \cdot 34 + 21$

$34 = 1 \cdot 21 + 13$

$21 = 1 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

$1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (5 - 1 \cdot 3)$

$= -1 \cdot 5 + 2 \cdot 3$

~~to $1 = 7 - 1 \cdot 6$~~

$= -1 \cdot 5 + 2 \cdot (8 - 1 \cdot 5)$

~~$= 7 - 1 \cdot (13 - 1 \cdot 7)$~~

$= 2 \cdot 8 - 3 \cdot 5$

= ~~$-1 \cdot 13 + 2 \cdot 7$~~

$= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8)$

= ~~$-1 \cdot 13 + 2 \cdot (21 - 1 \cdot 13)$~~

$= -3 \cdot 13 + 5 \cdot 8$

= ~~$2 \cdot 21$~~ $- 3 \cdot 13 + 5 \cdot (21 - 1 \cdot 13)$

$= 5 \cdot 21 - 8 \cdot 13$ ~~$+ 1 \cdot 21$~~)

$= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21)$

$= -8 \cdot 34 + 13 \cdot 21$

$= -8 \cdot 34 + 13 \cdot (55 - 1 \cdot 34)$

$= 13 \cdot 55 - 21 \cdot 34$

$= 13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55)$

= ~~$-8 \cdot 89 + 13 \cdot 55$~~

$= -21 \cdot 89 + 34 \cdot 55$

Inverse is ~~13~~ 34.

$$\begin{array}{r} 21 \\ 13 \\ \hline 34 \end{array}$$

d) $a = 89,\ m = 232$

$232 = 2 \cdot 89 + 54$
$89 = 1 \cdot 54 + 35$
$54 = 1 \cdot 35 + 19$
$35 = 1 \cdot 19 + 16$
$19 = 1 \cdot 16 + 3$
$16 = 5 \cdot 3 + 1$
$3 = 3 \cdot 1$

$1 = 16 - 5 \cdot 3$
$= 16 - 5 \cdot (19 - 1 \cdot 16)$
$= -5 \cdot 19 + 6 \cdot 16$
$= -5 \cdot 19 + 6 \cdot (35 - 1 \cdot 19)$
$= 6 \cdot 35 - 11 \cdot 19$
$= 6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35)$
$= -11 \cdot 54 + 17 \cdot 35$
$= -11 \cdot 54 + 17 \cdot (89 - 1 \cdot 54)$
$= 17 \cdot 89 - 28 \cdot 54$
$= 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89)$
$= -28 \cdot 232 + 73 \cdot 89$

Inverse is 73.

9. Solve the congruence $4x \equiv 5 \pmod 9$

$$\begin{array}{r} 56 \\ 17 \\ \hline 73 \end{array}$$

$\gcd(4, 9) = 1$
$9 = 4 \cdot 2 + 1$
$2 = 2 \cdot 2$.
$1 = 9 - 4 \cdot 2$.

inverse of 4 mod 9 is -2.

Now $4x \equiv 5 \pmod 9$
$-2 \cdot 4x \equiv -2 \cdot 5 \pmod 9$
$-8x \equiv -10 \pmod 9$

$-8 \equiv 1 \bmod 9$.
$-10 \equiv -1 \bmod 9$
$\equiv 8 \bmod 9$

$\therefore x \equiv 8 \pmod 9$

To verify, assume $x \equiv 8 \pmod 9$
$4x \equiv 32 \pmod 9$
$= 5 \pmod 9$

which is true for all $x \equiv 8 \bmod 9$.
Solutions $\ldots, -10, -1, 8, 17, 26, 35, \ldots$

the congruence $2x \equiv 7 \bmod 17$

$\gcd(2,17) = 1$

$17 = \cancel{16}\ 2 \cdot 8 + 1$

$2 = 1 \cdot 2$

$1 = 17 - 2 \cdot 8$

So inverse of 2 mod 17 is -8

multiply both sides of congruence by -8

$2x \equiv 7 \bmod 17$

$-8 \cdot 2x = -8 \cdot 7 \bmod 17$

$-16x = -8 \cdot 7 \bmod 17$

$(-8) \cdot 2 \equiv 1 \bmod 17$

$-56 \equiv 12 \bmod 17$

$\therefore x \equiv 12 \bmod 17$.

$\left\lfloor \frac{-56}{17} \right\rfloor$

$\lfloor -3. \rfloor$

$= -4$

$17 \times 3 = 51$

$-56 = -4 \times 17 + 12$

$68 - 56 = 12$

Now to check

$x \equiv 12 \bmod 17$

$2x \equiv 24 \bmod 17$

$\equiv 7 \bmod 17$

which is true.

31. which integers leave a remainder of 1 when divided by 2 and also leave a remainder of 1 when divided by 3?

Let the integer be x

$x \equiv 1 \bmod 2$

$x \equiv 1 \bmod 3$.

$\gcd(2,3) = 1$.

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2$

$1 = 3 - 2 \cdot 1$

$a_1 = a_2 = 1$

$m_1 = 2,\ m_2 = 3$

$m = m_1 m_2$

$= 2 \cdot 3 = 6$.

$M_1 = \frac{m}{m_1} = 3$

$M_2 = \frac{m}{m_2} = 2$.

y_1 is inverse of 3 mod 2 .

$y_1 = 1$

y_2 is inverse of 2 mod 3

$y_2 = -1 = 2 . \bmod 3$.

$y_2 = 2$

$x = (a_1 y_1 M_1 + a_2 y_2 M_2) \bmod m$

$= (3 + 4) \bmod 6$

$= 7 \bmod 6$

$= 1 \bmod 6$.

Solutions : $1 + 6k , k \in \mathbb{Z}$

32) Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?

$x \equiv 0 \bmod 5$

$x \equiv 1 \bmod 3$

$\gcd(3,5) = 1$

$a_1 = 0$ $\quad m_1 = 5$ $\quad m = 15$ $\quad M_1 = 3$

$a_2 = 1$ $\quad m_2 = 3$ $\quad M_2 = 5$

y_1 = inverse of 3 mod 5

$y_1 = 2$.

$5 = 3.1 + 2$

$3 = 2.1 + 1$

$2 = 1.2$

$1 = 3 - 2.1$

$= 3 - (5 - 3.1).1$

$= 3 - 5.1 + 3.1$

$= 3.2 - 5.1$

y_2 = inverse of 5 mod 3 $= 2 \bmod 3$

$y_2 = -1 = 2 (\bmod 3)$

$y_2 = 2$.

$x = (a_1 M_1 y_1 + a_2 M_2 y_2') \bmod m$

$= (0 + 1 . 5 . 2) \bmod 15$

$= 10 \bmod 15$

Solutions : $10 + 15k , k \in \mathbb{Z}$

e Chinese Remainder theorem to find l solutions to the system of congruences

$x \equiv 2 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 5$

Here 3, 4, 5 are pairwise relatively prime.

Now $m_1 = 3,\ m_2 = 4,\ m_3 = 5$

$m = m_1 m_2 m_3 = 3 \cdot 4 \cdot 5 = 60.$

$M_1 = \frac{m}{m_1} = 20$

$M_2 = \frac{m}{M_2} = 15$

$M_3 = \frac{m}{m_3} = 12$

Find inverse of $M_1 \bmod m_1$

20 mod 3.

$\gcd(20,3) = 1$

$20 = 6 \cdot 3 + 2$	$1 = 3 - 1 \cdot 2$
$3 = 1 \cdot 2 + 1$	$= 3 - 1 \cdot (20 - 6 \cdot 3)$
$2 = 2 \cdot 1$	$= -1 \cdot 20 + 7 \cdot 3$

Inverse is $-1 \equiv 2 \bmod 3$.

$y_1 = 2$.

Inverse of 15 mod 4.

$15 = 3 \cdot 4 + 3$	$1 = 4 - 1 \cdot 3$
$4 = 1 \cdot 3 + 1$	$= 4 - 1 \cdot (15 - 3 \cdot 4)$
$3 = 3 \cdot 1$	$= -1 \cdot 15 + 4 \cdot 4$

Inverse is $-1 \equiv 3 \bmod 4$.

$y_2 = 3$.

Inverse of 12 mod 5

$12 = 2 \cdot 5 + 2$	$1 = 5 - 2 \cdot 2$
$5 = 2 \cdot 2 + 1$	$= 5 - 2 \cdot (12 - 2 \cdot 5)$
$2 = 2 \cdot 1$	$= -2 \cdot 12 + 5 \cdot 5$

Inverse is $-2 \equiv 3 \bmod 5$

$y_3 = 3$.

$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3)$ mod

$= (2 \times 20 \times 2 + 1 \times 15 \times 3 + 3 \times 12 \times 3)$ mod

$= (80 + 45 + 108)$ mod 60

$= 233$ mod 60

$= 53$ mod 60

All solutions are $60k + 53$, $k \in \mathbb{Z}$

21) Find all solutions to the system of congruences

$x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$
$x \equiv 4 \pmod{11}$

$m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 11$ are pairwise relatively prime.

$m = 2 \cdot 3 \cdot 5 \cdot 11 = 330$

$M_1 = 165$ $\quad M_3 = 66$
$M_2 = 110$ $\quad M_4 = 30$

$\underline{y_1}$ $\quad$ 165 mod 2.

$165 = 82 \cdot 2 + 1$ $\qquad 1 = 165 - 82 \cdot 2$
$2 = 2 \cdot 1$

$y_1 = 1$

$\underline{y_2}$ $\quad$ 110 mod 3.

$110 = 36 \cdot 3 + 2$ $\qquad 1 = 3 - 1 \cdot 2$
$3 = 1 \cdot 2 + 1$ $\qquad = 3 - 1 \cdot (110 - 36 \cdot 3)$
$2 = 2 \cdot 1$ $\qquad = -1 \cdot 110 + 37 \cdot 3$

Inverse is $-1 \equiv 2$ mod 3

$y_2 = 2$

$\underline{y_3}$ $\quad$ 66 mod 5

$66 = 13 \cdot 5 + 1$ $\qquad 1 = 66 - 13 \cdot 5$
$5 = 5 \cdot 1$

$y_3 = 1$

$\underline{y_4}$ $\quad$ 30 mod ~~4~~ 11

$30 = 2 \cdot 11 + 8$ $\qquad 3 = 1 \cdot 2 + 1$
$11 = 1 \cdot 8 + 3$ $\qquad 2 = 2 \cdot 1$
$8 = 2 \cdot 3 + 2$

$1 = 3 - 1\cdot 2$

$= 3 - 1\cdot(8 - 2\cdot 3)$

$= -1\cdot 8 + 3\cdot 3$

$= -1\cdot 8 + 3\cdot(11 - 1\cdot 8)$

$= 3\cdot 11 - 4\cdot 8$

$= 3\cdot 11 - 4\cdot(30 - 2\cdot 11)$

$= -4\cdot 30 + 11\cdot 11$

Inverse is $-4 \equiv 7 \mod 11$

$y_4 = 7$

$x \equiv (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4) \mod m$

$= (1\cdot 165\cdot 1 + 2\cdot 110\cdot 2 + 3\cdot 66\cdot 1 + 4\cdot 30\cdot 7) \mod 330$

$= (165 + 440 + 198 + 840) \mod 330$

$= (33 + 110 + 180) \mod 330$

$= 323 \mod 330$

All solutions $330k + 323,\ k \in \mathbb{Z}$.

$$\begin{array}{r} 2 \\ 28 \\ 3 \\ \hline 84 \end{array} \quad \begin{array}{r} 165 \\ 198 \\ \hline 363 \end{array} \quad \begin{array}{r} 840 \\ 660 \\ \hline 180 \\ 110 \\ 33 \\ \hline 323 \end{array}$$

26) Find all solutions, if any, to the system of congruences

$x \equiv 5 \pmod 6$

$x \equiv 3 \pmod{10}$

$x \equiv 8 \pmod{15}$

Here 6, 10 and 15 are not relatively prime.

So we write them as

$x \equiv 5 \mod 6 \Rightarrow x \equiv 5 \mod 2$ & $x \equiv 5 \mod 3$

$x \equiv 1 \mod 2 \qquad x \equiv 2 \mod 3$

$x \equiv 3 \mod 10 \Rightarrow x \equiv 3 \mod 2$ & $x \equiv 3 \mod 5$

$x \equiv 1 \mod 2$

$x \equiv 8 \mod 15 \Rightarrow x \equiv 8 \mod 3$ & $x \equiv 8 \mod 5$

$x \equiv 2 \mod 3 \qquad x \equiv 3 \mod 5$

i.e. the above system of congruences is reduced to

$x \equiv 1 \bmod 2$

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

$a_1 = 1 \qquad m_1 = 2$

$a_2 = 2 \qquad m_2 = 3$

$a_3 = 3 \qquad m_3 = 5$

$m = m_1 m_2 m_3 = 2 \cdot 3 \cdot 5 = 30$

$M_1 = \frac{m}{m_1} = 15$

$M_2 = \frac{m}{m_2} = 10$

$M_3 = \frac{m}{m_3} = 6$

Now inverse y_1 of $M_1 \bmod m_1$

y_1 of $15 \bmod 2$

$\gcd(15, 2) = 1$

$15 = 2 \cdot 7 + 1$

$2 = 1 \cdot 2$

$\Rightarrow 1 = 15 - 2 \cdot 7$

$\therefore y_1 = 1$

Now inverse y_2 of $M_2 \bmod m_2$.

y_2 of $10 \bmod 3$.

$\gcd(10, 3) = 1$.

$10 = 3 \cdot 3 + 1$

$3 = 1 \cdot 3$

$1 = 10 - 3 \cdot 3$.

$\therefore y_2 = 1$

Inverse y_3 of $M_3 = 6 \bmod m_3 = 5$

$\gcd(5, 6) = 1$

$6 = 5 \cdot 1 + 1$

$5 = 1 \cdot 5$

$1 = 6 - 5 \cdot 1$

$y_3 = 1$.

$= (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \bmod m$

$= (1.15.1 + 2.10.1 + 3.6.1) \bmod 30$

$-(15+20+18) \bmod 30$.

$= 53 \bmod 30$

$= 23 \bmod 30$.

∴ solutions are $23 + 30k$, $k \in \mathbb{Z}$

27) Find all solutions, if any, to the system of congruences

$x \equiv 7 \pmod{9}$

$x \equiv 4 \pmod{12}$

$x \equiv 16 \pmod{21}$

Here 9, 12, 21 are not relatively prime.

$x \equiv 7 \bmod 9 \Rightarrow x \equiv 7 \bmod 3 \Rightarrow x \equiv 1 \bmod 3$.

$x \equiv 4 \bmod 12 \Rightarrow x \equiv 4 \bmod 4$ & $x \equiv 4 \bmod 3$

$\equiv 0 \bmod 4$ $\qquad \equiv 1 \bmod 3$.

$x \equiv 16 \bmod 21 \Rightarrow x \equiv 16 \bmod 3$ & $x \equiv 16 \bmod 7$

$\equiv 1 \bmod 3$ $\qquad \equiv 2 \bmod 7$

∴ $x \equiv 1 \pmod{3}$

$x \equiv 0 \pmod{4}$

$x \equiv 2 \pmod{7}$

$a_1 = 1$, $a_2 = 0$, $a_3 = 2$

$m_1 = 3$, $m_2 = 4$, $m_3 = 7$

$m = 3.4.7 = 84$.

$M_1 = 28$ $\quad M_2 = 21$ $\quad M_3 = 12$.

$y_1 =$ inv of 28 mod 3 .

$=$ ~~inv of 1 mod 3~~ .

~~3 = 1 3~~

$28 = 3.9 + 1$

$3 = 3.1$

$1 = 28 - 3.9$, coef of 28 is 1

$y_1 = 1$.

$y_2 =$ inv of 21 mod 4

$21 = 4.5 + 1$ $\qquad 1 = 21 - 4.5$

$4 = 1.4$ $\qquad$ coef of 21 is 1

∴ $y_2 = 1$

y_3 = inv of 12 mod 7

$12 = 1\cdot 7 + 5$

$7 = 5\cdot 1 + 2$

$5 = 2\cdot 2 + 1$

$2 = 1\cdot 2$

$1 = 5 - (2\cdot 2)$

$= 5 - 2\cdot(7 - 5\cdot 1)$

$= 5 - 2\cdot 7 + 2\cdot 5$

$= 3\cdot 5 - 2\cdot 7$

$= 3\cdot(12 - 1\cdot 7) - 2\cdot 7$

$= 3\cdot 12 \overset{-}{\cancel{+}} 3\cdot 7 - 2\cdot 7$

$= 3\cdot 12 - 5\cdot 7$

coef. of 12 is 3

$\therefore y_3 = 3$.

$x = (a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3) \bmod m$

$= (1.1\cdot 28 + 0.1.21 + 2\cdot 3.12) \bmod 84$

$= (28 + 72) \bmod 84$

$= 100 \bmod 84$

$= 16$.

12 6

All solutions: $16 + \overset{84}{\cancel{mo}} k$, $k \in \mathbb{Z}$.

ptography

ere we replace each letter by an elt of $\mathbb{Z}_{26}$ ㉙

i.e an integer from 0 to 25 equal to one less than its position in the alphabet.
For eg → replace A by 0, B by 1, C by 2, K by 10, and Z by 25.

Caesar cipher

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

In the encrypted message, the letter represented by p is replaced with the letter represented by $(p+3) \bmod 26$

* AT will be encrypted as DW

0 19

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

$f(0) = 3 \bmod 26$ → D

$f(19) = 22 \bmod 26$ → W

Eg what is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

First replace the letters in the message with numbers. This produces

12 4 4 19   24 14 20

8 13   19 7 4   15 0 17 10

Now replace each of the numbers p by $f(p) = (p+3) \bmod 26$ which gives

15 7 7 22   1 17 23

11 16   22 10 7   18 3 20 13

Translating back to letters

PHHW BRX LQ WKH SDUN

A – 0
B – 1
C – 2
D – 3
E – 4
F – 5
G – 6
H – 7
I – 8
J – 9
K – 10
L – 11
M – 12
N – 13

O – 14
P – 15
Q – 16
R – 17
S – 18
T – 19
U – 20
V – 21
W – 22
X – 23
Y – 24
Z – 25

* To recover the original message of secret message encrypted by Caesar cipher, the function f^{-1}, the inverse of f is used

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

This process of determining the original message from the encrypted message is called decryption.

* Decrypt DQG using Caesar cipher.

D Q G − 3 16 6.

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

$f^{-1}(3) = 0 \bmod 26$ — A

$f^{-1}(16) = 13 \bmod 26$ — N

$f^{-1}(6) = 3 \bmod 26$ — D

So original message was AND.

* $f(p) = (p+k) \bmod 26$. Such a cipher is called shift cipher.

For decryption, $f^{-1}(p) = (p-k) \bmod 26$.

Integer 'k' is called key.

Eg Encrypt "STOP GLOBAL WARMING" using shift cipher with shift $k = 11$

STOP GLOBAL WARMING

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6

$f(p) = (p+11) \bmod 26$

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17

DEZA RWZMLW HLCXTYR

* Decrypt the ciphertext message

LEWLYPLUJL PZ H NYLHA ALHJOLY

that was encrypted with shift cipher with shift $k = 7$

$f^{-1}(p) = (p-7) \bmod 26$

	4-E
	23-X
22	15-P
-11	4-E
Y-24	17-R
P-15	8-I
L-11	4-E
U-20	13-N
J-9	2-C
L-11	4-E

P-15	8-I
Z-25	18-S

H-7	0-A

(31)

N-13	6-G
Y-24	17-R
L-11	4-E
H-7	0-A
A-0	19-T

A-0	19-T
L-11	4-E
H-7	0-A
J-9	2-C
O-14	7-H
L-11	4-E
Y-24	17-R

EXPERIENCE IS A GREAT TEACHER.

Affine cipher

$f(p) = (ap+b) \bmod 26$
where a, b are integers so that f is a bijection

This f^n is bijection iff $\gcd(a, 26) = 1$
Such a mapping is affine transformation and resulting cipher is called ~~affine~~ affine cipher.

Eg What letter replaces the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption?

K - 10

$$f(10) = (70+3) \bmod 26$$
$$= 73 \bmod 26$$
$$= 21 \bmod 26.$$

$$26\overline{)73}(2$$
$$\underline{52}$$
$$\underline{21}$$

where 21 represents V.
so K is replaced by V in encrypted message.

Suppose $c = (ap + b) \bmod 26$
with $\gcd(a, 26) = 1$

$c \equiv (ap + b) \bmod 26$

$c - b \equiv ap \bmod 26$

Now find inverse $\bar{a}$ of $a \bmod 26$

$\bar{a}(c - b) = \bar{a}ap \bmod 26$

$= p \bmod 26$

$\Rightarrow p = \bar{a}(c - b) \bmod 26$

Q Decrypt $V = 21$
using $f(p) = (7p + 3) \bmod 26$
$\gcd(7, 26) = 1$

Find inverse of 7

$$26 = 7 \cdot 3 + 5$$
$$7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 5 \cdot 1) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (26 - 7 \cdot 3) - 2 \cdot 7 \\ &= 3 \cdot 26 - 11 \cdot 7 \end{aligned}$$

inverse $= -11$
$= \overset{+26}{15}$

$\therefore p = 15(21 - 3)$
$= 15(18)$
$= 270 \bmod 26$
$= 10$
$= K$.

$$\begin{array}{r} 180 \\ 90 \\ \hline 270 \end{array}$$

so ans K.