NUMBER THEORY

The study of the set of integers and their properties is known as number theory.

Definition: If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that

$$b = ac,$$

equivalently, if $\frac{b}{a}$ is an integer.

- The notation $a|b$ denotes that a divides b
- $a \nmid b$ denotes that a does not divide b.

Example:- Determine whether $3|7$ and whether $3|12$

Solution: We see that $3 \nmid 7$, because $\frac{7}{3}$ is not an integer. On the other hand, $3|12$ because

$$\frac{12}{3} = 4.$$

Note:-

1) $a|b \Leftrightarrow b$ is multiple of a and $0 \leq a \leq b$

2) $a^k \| b \Rightarrow a^{k+1} \nmid b$ but $a^k | b$

Theorem:- Let a, b, c be integers, where $a \neq 0$. Then

(i) if $a|b$ implies $a|bc$ for any integer c

By definition, $a|b \Rightarrow b = ax \quad \exists\, x \in \mathbb{Z}$

Multiply both sides by $c \quad x \in \mathbb{Z}$

$bc = axc \quad c \in \mathbb{Z}$

$bc = ax' \quad \therefore cx \in \mathbb{Z} \Rightarrow x' \in \mathbb{Z}$

$\Rightarrow a|bc$

(ii) if $a|b$ and $b|c$ imply $a|c$;

By definition $a|b \Rightarrow b = ax \quad x \in \mathbb{Z}$

$b|c \Rightarrow c = by \quad y \in \mathbb{Z}$

$\Rightarrow c = a(xy) \quad k = xy \in \mathbb{Z}$

$\Rightarrow c = ak$

$\Rightarrow a|c$

(3) $a|b$ and $a|c$ imply $a|(bx+cy)$ for any integers 'x' and 'y'.

By definition of $a|b \Rightarrow b = ax'$

$a|c \Rightarrow c = ay'$

To prove, $bx+cy = a$ (constant)

$\Rightarrow a|(bx+cy)$

L.H.S. $bx+cy = ax'.x + ay'.y = ax_1 + ay_1$

$= a(x_1+y_1) = az'$ $\quad z' \in \mathbb{Z}$

$\Rightarrow bx+cy = az'$

$\Rightarrow a|(bx+cy)$

(4) $a|b$ and $b|a$ imply $a = \pm b$

By definition $a|b \Rightarrow b = ax$

$b|a \Rightarrow a = bx$

$\Rightarrow a = ax.ax$

$\Rightarrow a = ax^2$

$\Rightarrow 1 = x^2$

$\Rightarrow x = \pm 1$ $\Rightarrow$ $\boxed{a = \pm b}$

5) $a|b$, $a>0$, $b>0$ implies $a \leq b$

Division Algorithm:- Let 'a' and d are integers with $d>0$. Then there exists unique integers q and r, with $0 \leq r < d$, such that $\boxed{a = dq + r}$ $\rightarrow$ (1)

- In equality (1), d is called the divisor
  a is called the dividend
  q is called the quotient
  r is called the remainder

Application of Division Algorithm

1) Every integer leaves remainder 0 and 1 when divided by 2.
2) Square of every integers leaves remainder 0 and 1 when divided by 2.

Proof: $2|a \Rightarrow a = 2k$ or $a = 2k+1$

$\Rightarrow a^2 = (2k)^2$

$= 4k^2$

$a^2 = 2(2k^2)$

$a^2 = 2k_1 + 0$

$a^2 = (2k+1)^2$

$= 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$

$a^2 = 2k_1 + 1$

3. Any integer a is either $4k$, $4k+1$, $4k+2$, $4k+3$, then a^2 is one of the form

$16k^2$, $16k^2 + 8k + 1$, $16k^2 + 16k + 4$, $16k^2 + 24k + 9$

Proof:-

$a = 4k$ | $a = 4k+1$ | $a = 4k+2$ | $a = 4k+3$

$a^2 = 16k^2$ | $a^2 = (4k+1)^2$ | $a^2 = (4k+2)^2$ | $a^2 = (4k+3)^2$

$= 16k^2 + 8k + 1$ | $= 16k^2 + 16k + 4$ | $= 16k^2 + 24k + 9$

4. (i) Square of any integer a, when a is even and is divided by 8, then it has remainder 0 or 4.

(ii) Square of any integer a, (a is odd) and is divided by 8 has remainder 1.

Greatest Common Divisor (GCD)

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. The greatest common divisor of a and b is denoted by gcd(a,b).

Example: What is the greatest common divisor of 24 and 36?

Solution Using fundamental theorem of arithemetic

2	24
2	12
2	6
3	3
	1

2	36
2	18
3	9
3	3
	1

Prime factorization

$24 = 2 \times 2 \times 2 \times 3$

$36 = 2 \times 2 \times 3 \times 3$

$\gcd(24, 36) = 2 \times 2 \times 3 = 12$

Example: What is the greatest common divisor of 17 and 22?

$17 = 1 \times 17$

$22 = 2 \times 11$

$\gcd(17, 22) = 1$

★ Greatest common divisor (gcd) of 'b' and 'c' is defined for every pair of integers (b, c) except $b=0, c=0$

Euclidean Algorithm:- Suppose a and b are integers with $a \geq b > 0$

1) Apply the division algorithm $a = bq + r, \quad 0 \leq r < b$
2) Rename b as a & r as b and repeat until $r = 0$

★ The largest non-zero remainder is the gcd(a, b).

Algorithm: Apply division algorithm to a and b to get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

If $r_1 = 0$, then $b \mid a$

$\Rightarrow \gcd(a, b) = b$

If $r_1 \neq 0$ then divide b by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$ then $\gcd(r_1, b) = r_1$

If $r_2 \neq 0$ then we will continue the procedure as follows

$$\begin{cases} r_1 = q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots \\ r_{n-2} = q_n r_{n-1} + r_n \\ r_{n-1} = q_{n+1} r_n + 0 \end{cases}$$

$\therefore \gcd(a, b) = r_n$ (proof is based on following Lemma).

Lemma:- If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$

By this lemma, $\gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$

$\gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = r_n$

$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = g(r_2, r_3) \cdots = \gcd(r_{n-1}, r_n) = r_n$

Q1. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm [3]

Sol.
$662 = 414 \cdot 1 + 248$
$414 = 248 \cdot 1 + 166$
$248 = 166 \cdot 1 + 82$
$166 = 82 \cdot 2 + 2$
$82 = 2 \cdot 41 + 0$

Hence, $\gcd(414, 662) = 2$.

Q2. Find $\gcd(252, 198)$ using Euclidean algorithm

Sol.
$252 = 198 \cdot 1 + 54$
$198 = 54 \cdot 3 + 36$
$54 = 36 \cdot 1 + 18$
$36 = 18 \cdot 2 + 0$

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

gcd as linear combination

BEZOUT'S THEOREM:- If a and b are positive integers, then there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

Ex: Express gcds of Q1 and Q2 as a linear combination of the given numbers

For Q1: To show that $\gcd(662, 414) = 2 = 662x + 414y$

From fourth division, we have

$$2 = 166 - 82 \cdot 2$$

From third division, we have

$$82 = 248 - 166 \cdot 1$$

Substitute value of 82 in previous equation, we get

$$2 = 166 - (248 - 166 \cdot 1) \cdot 2$$
$$= 166 - 248 \cdot 2 + 166 \cdot 2$$
$$= 166 \cdot 3 - 248 \cdot 2$$

from second division, we have $166 = 414 - 248 \cdot 1$

$$\Rightarrow \therefore 2 = (414 - 248 \cdot 1) \cdot 3 - 248 \cdot 2$$
$$= 414 \cdot 3 - 248 \cdot 3 - 248 \cdot 2$$
$$= 414 \cdot 3 - 248 \cdot 5$$

from first division, we have $248 = 662 - 414 \cdot 1$

$$\therefore 2 = 414 \cdot 3 - (662 - 414 \cdot 1) \cdot 5$$
$$2 = 414 \cdot 8 - 662 \cdot 5$$

$\therefore$ value of $x = 8$ $\quad y = -5$

$$\boxed{2 = 414x + 662 \cdot y}$$

For Q2: To find x and y s.t.

$$\gcd(252, 198) = 18 = 252 \cdot x + 198 \cdot y$$

From third division, we have

$$18 = 54 - 1 \cdot 36$$
$$= 54 - 1 \cdot (198 - 3 \cdot 54) \quad (\text{from } 2^{nd} \text{ div})$$
$$18 = 4 \cdot 54 - 1 \cdot 198$$
$$= 4(252 - 1 \cdot 198) - 1 \cdot 198 \quad (\text{from } 1st \text{ divi})$$
$$18 = 4 \cdot 252 - 5 \cdot 198$$

$\therefore x = 4$
$y = -5$

Result:

1) For any integer $m > 0$,
$$\gcd(ma, mb) = m(a, b)$$
For any integer $k \neq 0$
$$\gcd(ka, kb) = |k| \gcd(a, b)$$

2) If $\gcd(a, b) = g$ and $g|a$, $g|b$, then
$$\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

3) If $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, then $(ab, m) = 1$

Primes:- 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.

Remark:- The integer n is composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.

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

Example: The prime factorization of

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$$
$$641 = 641$$
$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

* One procedure for showing that an integer is prime is based on the following observation

Theorem 1:- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Example: Show that 101 is prime.

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5 and 7. Because 101 is not divisible by 2, 3, 5 or 7, it follows that 101 is prime.

Example: Find primes not exceeding 100.

We can use above mentioned theorem, to find the primes not exceeding 100. By theorem 1, the composite integers not exceeding 100 must have a prime factor not exceeding 10. The only primes less than 10 are 2, 3, 5 and 7. Delete the numbers divisible by 2, 3, 5 and 7 from 1 to 100 yields the primes not exceeding 100.

Ans: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 and 97.

Theorem 2: There are infinitely many primes

Mersenne primes:-

The largest prime known has been an integer of the special form $2^p - 1$, where p is also prime. Such prime are called Mersenne primes

Note that, every integer of $2^p - 1$ form is not a prime.

Example:

$2^2 - 1 = 3$
$2^3 - 1 = 7$
$2^5 - 1 = 31$
$2^7 - 1 = 127$

} Mersenne primes

$2^{11} - 1 = 2047 = 23 \cdot 89$ (Not a Mersenne prime)

Note that, $2^n - 1$ cannot be prime when n is not prime.

Twin Prime Conjecture:

Definition: Twin Prime: are pairs of primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, 4967 and 4969...

The twin prime conjecture asserts that there are infinite many twin prime.

* The world's record for twin primes, as of mid 2011, consists of the numbers $65,516,468,355 \cdot 2^{333,333} \pm 1$, which have 100,355 decimal digits.

Goldbach's conjecture:

Every even integer n, $n>2$, is the sum of two primes

We can check this conjecture for every small even nos

Eg:
$4 = 2+2$
$6 = 3+3$
$8 = 5+3$
$10 = 7+3$
$12 = 7+5$...

* As of mid 2011, the conjecture has been checked for all positive even integer upto 1.6×10^{18}.

Definition: The integers a and b are relatively prime if their gcd is 1.

Eg: 17 and 22 are relatively prime.

Definition: The integers $a_1, a_2, \ldots, a_n$ are pairwise relative prime if $\gcd(a_i, a_j) = 1$ whenever $1 \le i < j \le n$.

Example:- 10, 17, 21 are relatively prime
↓ pairwise

but 10, 19 and 24 are not pairwise relatively prime.

Theorem:- If p is a prime and $p \mid ab$ then either $p \mid a$ or $p \mid b$

Least common multiple (Lcm):-

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

Theorem:- Let a and b be positive integers. Then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b).$$

*** Theorem:-** If p_n is the nth prime number then

$$p_n \leq 2^{2^{n-1}}$$

Eg: $p_1 \leq 2^{2^{1-1}} = 2^1 = 2$

$p_2 \leq 2^{2^{2-1}} = 4$

Theorem Let p_n denotes nth prime number in their natural order then

$$p_n \leq p_1 p_2 \cdots p_{n-1} + 1$$

CONGRUENCE:-

Let n be a fixed positive integer given any two numbers (Integers) a and b

then $a \equiv b \pmod n$

if $n \mid a-b$ {i.e. n divides (a-b)}

* $a \equiv b \pmod n$ read as "a is congruent to b modulo n".

* If a and b are not congruent modulo m, we write $a \not\equiv b \pmod m$.

Example: For $n = 7$

$3 \equiv 24 \pmod 7$

$-31 \equiv 11 \pmod 7$

$25 \not\equiv 12 \pmod 7$

Remark:- Given an integer 'a' when divided by 'b', gives some quotient and remainder

s.t. $a = bq + r \qquad 0 \leq r < b$

$a - r = bq$

$\Rightarrow a \equiv r \pmod b$

Example:

$6 \equiv 0 \pmod 3$

$7 \equiv 1 \pmod 3$

$8 \equiv 2 \pmod 3$

Given an integer 'a' when divided by 'n', gives some quotient and remainder such that

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

$$\Rightarrow a \equiv r \pmod{n} \quad ; \quad 0 \le r < n$$

$\therefore r$ has $(n-1)$ choices

i.e. $r = 0, 1, 2, \ldots, n-1$.

1) The set of integers $0, 1, 2, \ldots n-1$ is called least non-negative residue of modulo n. [Denoted $\mathbb{Z}_n$]

2) The set of integers $a_1, a_2, \ldots a_n$ is the complete system of residue modulo n.

Example :- Is it complete system of residue module 7

$-12, -4, 11, 13, 22, 82, 91$

Solution:

$-12 \equiv 2 \pmod 7$

$-4 \equiv 3 \pmod 7$

$11 \equiv 4 \pmod 7$

$13 \equiv 6 \pmod 7$

$22 \equiv 1 \pmod 7$

$82 \equiv 5 \pmod 7$

$91 \equiv 0 \pmod 7$

Least residue system :- $\{0, 1, 2, 3, 4, 5, 6\}$

Complete residue system :- $\{-12, -4, 11, 13, 22, 82, 91\}$

But if there is 97, then $97 \equiv 6 \pmod 7$

then $\{-12, -4, 11, 13, 22, 82, 91, 97\}$ is not complete res system.

Remark :- For arbitary integers a and b,

$a \equiv b \pmod n$

iff a and b leaves the same non-negative remainder when divided by n.

Eg: $24 \equiv 17 \pmod 7$

both have remainder 3.

Application of Congruence to divisibility

Q. Find the remainder when 2^{50} is divisibility by 7.

Solution:-

$2^0 = 1 \equiv 1 \pmod 7$
$2^1 = 2 \equiv 2 \pmod 7$
$2^2 = 4 \equiv 4 \pmod 7$
$2^3 = 8 \equiv 1 \pmod 7$
$2^4 = 16 \equiv 2 \pmod 7$
$2^5 = 32 = 4 \pmod 7$
$2^6 \equiv 64 \equiv 1 \pmod 7$

The pattern repeats with a period of 3.

$\therefore \quad 2^3 \equiv 1 \pmod 7$

$(2^3)^2 \equiv (1)^2 \pmod 7$

$\Rightarrow (2^3)^{16} \equiv (1)^{16} \pmod 7$

$\Rightarrow 2^{48} \equiv 1 \pmod 7$

$\Rightarrow 2^{48} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod 7$

$\Rightarrow 2^{50} \equiv 2^2 \pmod 7$

$\Rightarrow 2^{50} \equiv 4 \pmod 7$

$\therefore$ The remainder when 2^{50} is divisible by 7 is 4.

Fermat's Little Theorem:-

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

Furthermore, for every integer a, we have $a^p \equiv a \pmod p$

Properties of Congruence

1) Reflexive : $a \equiv a \pmod m$
2) Symmetry : $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$
3) Transitivity : if $a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$
4) If $a \equiv b \pmod m \Rightarrow ka = kb \pmod m$
5) If $a \equiv b \pmod m \Rightarrow a^n = b^n \pmod m$ n is any +ve integer
5) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a+c \equiv b+d \pmod m$ and $a \cdot c \equiv b \cdot d \pmod m$
6) If $ca \equiv cb \pmod n$ then $a \equiv b \pmod{n/d}$; $d = \gcd(n, c)$
7) If $ca \equiv cb \pmod n$ and $p \nmid c$ then $a \equiv b \pmod p$.

Example:- Find the remainder when 2^{402} is divided by 4.

$2^1 \equiv 2 \pmod 4$

$2^2 \equiv 0 \pmod 4$

$(2^2)^{201} \equiv (0)^{201} \pmod 4$

$2^{402} \equiv 0 \pmod 4$ $\therefore$ remainder is zero

Example:- Find remainder when 2^{354} is divided by 31.

Note that $32 = 2^5 \equiv 1 \pmod{31}$

$(2^5)^{70} \equiv (1)^{70} \pmod{31}$

$2^{350} \equiv 1 \pmod{31}$

Now, multiply by 2^4 on both sides, we get

$2^{354} \equiv 2^4 \pmod{31}$

$2^{354} \equiv 16 \pmod{31}$

$\therefore$ remainder when 2^{354} is divided by 31 is 16

Application2

Q:- Find the remainder obtained upon the dividing the sum $1! + 2! + 3! + \dots + 100!$ by 12.

$1! \equiv 1! \pmod{12}$

$2! \equiv 2 \pmod{12}$

$3! \equiv 6 \pmod{12}$

$4! = 24 \equiv 0 \pmod{12}$

$5! = 5 \cdot 4! \equiv 5 \cdot 0 \pmod{12} \Rightarrow 5! \equiv 0 \pmod{12}$

$\vdots$

$100! = \underbrace{100 \cdot 99 \cdots 5}_{K} \cdot 4! \equiv K \cdot 0 \pmod{12}$

$\Rightarrow 100! \equiv 0 \pmod{12}$

$\Rightarrow 1! + 2! + 3! + \dots 100! \equiv 1 + 2 + 6 + 0 + 0 + \dots + 0 \pmod{12}$

$\equiv 9 \pmod{12}$

Ans: Remainder is 9.

Arithmetic Modulo m

$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$
= Set of non negative integers less than m.

Addition of these integers, denoted by $+_m$ by

$$a +_m b = (a+b) \pmod m$$

Multiplication of integers, denoted by $\cdot_m$ by

$$a \cdot_m b = (a \cdot b) \pmod{(m)}$$

Q: Use the definition of addition and multiplication in $\mathbb{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$

Soln:- $7 +_{11} 9 = (7+9) \pmod{11} = 16 \bmod (11) = 5$

and $7 \cdot_{11} 9 = 7 \cdot 9 \pmod{11} = 63 \bmod 11 = 8$

Hence $7 +_{11} 9 = 5$

$7 \cdot_{11} 9 = 8$

Application 3: Find the last digit of the number 9^9 ⟹ modulo 10

$9^1 \equiv 9 \pmod{10}$

$9^2 = 9 \cdot 9 = 81 \equiv 1 \pmod{10}$

$(9^2)^4 \equiv (1)^4 \pmod{10}$

$9^8 \equiv 1 \pmod{10}$

$9^8 \cdot 9 \equiv 9 \pmod{10}$

∴ Last digit of no. $9^9 = 9$ Ans.

Applications:

ISBNs (International Standard Book Number).

- A 10-digit code $x_1 x_2 x_3 \ldots x_{10}$ assigned by the publisher as the identification for books.
- X - used to represent 10.

The check digit (x_{10}) is selected so that

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}$$

or equivalent $\Rightarrow \sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$

Q:- The first nine digits of the ISBN-10 of the sixth edition of this book are 007288008. What is the check digit?

$$x_{10} = \sum_{i=1}^{9} i x_i \pmod{11}$$

$$x_{10} = (1x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9) \pmod{11}$$

$$= 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$$

$$\equiv 189 \equiv 2 \pmod{11}$$

Hence $\boxed{x_{10} = 2}$

Q. Is 084930149X a valid ISBN-10?

$x_{10} = X = 10$

$x_{10} = 0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81$

$\equiv$

$= 199 \pmod{11}$

$199 = 18 \times 11 + 1$

$\Rightarrow x_{10} \equiv 1 \pmod{11}$

$\Rightarrow 10 \not\equiv 1 \pmod{11}$

$\because 10 - 1 = 9$ & $11 \nmid 9$

$\therefore$ Hence, 084930149X is not valid ISBN-10.

Q: The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is 0-321-500Q1-8, where Q is a digit. Find the value of Q.

UPCs : Universal Product Codes : UPC is a bar code that is found on retail products.

The most common form of a UPC has 12 decimal digits The first digit identifies the product category, the next five digits identify the manufacturer, the following five identify the particular product and the last digit is a check digit. The check digit is determined by the congruence

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

Q. Suppose that the first 11 digits of an UPC are 79357343104 what is the check digit ?

Solution:

$$3\cdot 7 + 9 + 3\cdot 3 + 5 + 3\cdot 7 + 3 + 3\cdot 4 + 3 + 3\cdot 1 + 0 + 3\cdot 4 + x_{12} \equiv 0 \pmod{10}$$

$$\Rightarrow \quad 98 + x_{12} \equiv 0 \pmod{10}$$

$$\Rightarrow \quad x_{12} \equiv -8 \pmod{10}$$

$$\Rightarrow \quad x_{12} = 2 \pmod{10}$$ } Add 10 both sides

So, the check digit is 2.

Is 041331021641 a valid UPC?

$$3(0) + 4 + 3(1) + 3 + 3(3) + 1 + 3(0) + 2 + 3(1) + 6 + 3(4) + 1$$

$$= 0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1$$

$$\equiv 4 \not\equiv 0 \pmod{10}$$

Hence 041331021641 is not a valid UPC.

Linear Congruences:-

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.

Example:- If $3x \equiv 0 \pmod 3$. find x.

Solution: $x = 1$

Theorem:- The linear congruence $ax \equiv b \pmod n$ has a solution iff $d \mid b$ where $d = \gcd(a, n)$.

- Suppose the above congruence is solvable and x_0 is any specific solution then, the other solution has form $\boxed{x = x_0 + \frac{n}{d}t}$ for some choice of t.

Example:- $18x \equiv 30 \pmod{42}$ → (1)

$d = \gcd(18, 42) = 6$

& $6 \mid 30 = 5$

(i) $x_0 = 4$ is one solution of (1) as $18 \times 4 \equiv 30 \pmod{42}$
$42 \mid -72 - 30$

(ii) $x_0 + \frac{n}{d} = 4 + \frac{42}{6} = 4 + 7 = 11$ (for $t = 1$)

(iii) $x_0 + \frac{2n}{d} = 4 + 14 = 18$

(iv) $x_0 + \frac{3n}{d} = 4 + 21 = 25$

(v) $x_0 + \frac{4n}{d} = 4 + 28 = 32$

(vi) $x_0 + \frac{5n}{d} = 4 + 35 = 39$

So, the solutions are 11, 18, 25, 32 and 39.

Chinese Remainder Theorem:-

Let $m_1, m_2, \ldots m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ an arbitrary integers Then the systems

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

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

Solution :-

$$\bar{x} = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

where, $M_K = \frac{m}{m_K}$

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

&

$$\bar{x} \equiv a_K \pmod{m}$$

↓ final answer

Q. Solve the system by chinese ~~Rest~~ remainder theorem

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Solution:- According to theorem,

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 2$

$m_1 = 3 \quad m_2 = 5 \quad m_3 = 7$

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

I $\quad m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$

II $\quad M_1 = \frac{m}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{m}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15$

III $\quad M_1 y_1 \equiv 1 \pmod{m_1}$

$35 y_1 \equiv 1 \pmod 3$

$3 \mid 35y_1 - 1 = \frac{35y_1 - 1}{3} \Rightarrow y_1 = 2$ Use Hit & Trial

$M_2 y_2 \equiv 1 \pmod{m_2}$

$21 y_2 \equiv 1 \pmod 5$

$5 \mid 21y_2 - 1 = \frac{21y_2 - 1}{5} \Rightarrow y_2 = 1$

$M_3 y_3 \equiv 1 \pmod 7$

$15 y_3 \equiv 1 \pmod 7$

$\boxed{y_3 = 1}$

Final solution

$$\bar{x} = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$
$$= 233$$

$$\bar{x} \equiv 233 \equiv 23 \pmod{105}$$

It follows that 23 is the smallest positive integer that is a simultaneous solution.

That is, 23 is smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

8. Find solutions x, if they exist, to the system of equivalences

$$2x \equiv 6 \pmod{14}$$
$$3x \equiv 9 \pmod{15}$$
$$5x \equiv 20 \pmod{60}$$

Solution $\gcd(2,14) = 2$, so we can cancel 2 form from all term from first equivalence and write it

$$x \equiv 3 \pmod 7$$

Similarly, for second equivalence, $\gcd(3,15) = 3$,

$$\therefore x \equiv 3 \pmod 5$$

for third equivalence, $\gcd(5,60) = 5$

$\Rightarrow$ we can write it as,

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

Now, using chinese remainder theorem, on

$$x \equiv 3 \pmod 7$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod{12}.$$

we have, $m = 7 \cdot 5 \cdot 12 = 420$

$M_1 = 60 \quad M_2 = 84 \quad M_3 = 35$

$M_1 y_1 \equiv 1 \pmod{m_1}$

$\Rightarrow 60 \cdot y_1 \equiv 1 \pmod 7$

$\Rightarrow 7 \mid 60y_1 - 1 \Rightarrow \frac{60y_1 - 1}{7} \Rightarrow y_1 = 2$

or

$4y_1 \equiv 1 \pmod 7$

$7 \mid 4y - 1 \Rightarrow \frac{4y-1}{7} \Rightarrow y =$

$M_2 y_2 \equiv 1 \pmod{m_2}$

$\Rightarrow 84 \cdot y_2 \equiv 1 \pmod 5$

$\Rightarrow 5 \mid 84y_2 - 1 \Rightarrow \frac{84y_2 - 1}{5} \Rightarrow y_2 = 4$

$M_3 y_3 \equiv 1 \pmod{m_3}$

$35 y_3 \equiv 1 \pmod{12}$

$11 y_3 \equiv 1 \pmod{12} \quad y_3 = 11$

Hence, we have

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

$= 2 \cdot 60 \cdot 3 + 4 \cdot 84 \cdot 3 + 11 \cdot 35 \cdot 4 \equiv 2908$

Hence, we have any solution $x \equiv 2908 \equiv 388 \pmod{4}$

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.

s is inverse of a modulo m

if $sa \equiv 1 \pmod m$

Question:- Find an inverse of 3 modulo 7

Soln: $s \cdot 3 \equiv 1 \pmod 7$

By Euclidean algorithm $7 = 2 \cdot 3 + 1$

$\Rightarrow 1 = 7 \cdot 1 - 2 \cdot 3$

∴ Bezout's coefficients are -2 and 1

-2 and 1 o

3 & 7.

Also, -2 is an inverse of 3 modulo 7.

Note that every integer congruent to -2 modulo 7 is also an inverse of 3 such as 5, -9, 12 and so on.

Q. Find an inverse of 101 modulo 4620.

For finding inverse, first check gcd(a,b) = 1 ?

If yes, then proceed further and find Bezout's coefficients x and y such that

$$101x + 4620y = 1.$$

~~Now, $101x \equiv 4620y \equiv 1$~~ ✗

It will follows that $a = 101$ has inverse 101 modulo 4620. because $4620y$ is exactly divisible by 4620.

Using Euclidean algorithm to find gcd(101, 4620):

$$4620 = 45 \cdot 101 + 75$$
$$101 = 1 \cdot 75 + 26$$
$$75 = 2 \cdot 26 + 23$$
$$26 = 1 \cdot 23 + 3$$
$$23 = 7 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1.$$

(·) → * (Multiplication) not decimal

Because the last non-zero remainder is 1, we know that gcd(101, 4620) = 1.

We can now find the Bezout coefficients for 101 and 4620 by working backwards through these steps, expressing gcd(101, 4620) = 1 in terms of each successive pair of remainder. In each step we eliminate the remainder by expressing it as a linear combination of the divisor and the dividend.

We obtain
$$1 = 3 - 1 \cdot 2$$
$$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$
$$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$
$$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$$
$$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$$

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

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

That $(-35)(4620) + (1601)(101)$ tells us that -35 and 1601 are Bezout coefficient of 4620 and 101 and 1601 is an inverse of 101 modulo 4620.

Q. What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$?

Solution:- (i) find inverse of 3 mod 7

$7 = 3 \cdot 2 + 1$

$7 - 3 \cdot 2 = 1$

$7 - 3 \cdot 2 \equiv 1 \pmod 7$

$\Rightarrow -3 \cdot 2 \equiv 1 \pmod 7$

$\therefore -2$ is inverse of 3

(ii) Multiply by (-2) on both sides

$(-2)3x \equiv 4 \times (-2) \pmod 7$

$1x \equiv -8 \pmod 7$

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

$\Rightarrow x \equiv -8$ is one of its solutions

and other solutions are $-1, -15, (-15 \pm 7), (-15 - 7 - 7), \ldots$

Examples:

Find inverse of 7 mod 26.

Find x, such that $7x \equiv 1 \pmod{26}$

$\gcd(26, 7) = 1$

$1 = 7x + 26y$

Using Euclidean algorithm,

$26 = 7 \times 3 + 5$

$7 = 5 \times 1 + 2$

$5 = 2 \times 2 + 1$

Now, $1 = 5 - 2 \times 2$

$= 5 - (7 - 5 \times 1)\, 2$

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

$1 = (26 - 7*3)*3 - 7*2$

$= 26*3 - 7*9 - 7*2$

$1 = 26*3 - 7*11$

$\Rightarrow 26*3 - 7*11 \equiv 1 \bmod(26)$

$\Rightarrow 0 - 7*11 \equiv 1 \bmod(26)$

$\Rightarrow -11$ is inverse of a 7 mod(26)

$\Rightarrow 26 - 11 = 15$ is also the inverse of 7 modulo 26

Q. Find inverse of 89 mod 232

Solution, Find x, such that $89x \equiv 1 \pmod{232}$

$\gcd(89, 232) = 1$

$89x + 232y = 1$

$232 = 89 \cdot 2 + 54$

$89 = 54 \cdot 1 + 35$

$54 = 35 \cdot 1 + 19$

$35 = 19 \cdot 1 + 16$

$19 = 16 \cdot 1 + 3$

$16 = 3 \cdot 5 + 1$

$5 = 1 \cdot 5 + 0$

$\gcd(89, 232) = 1$

$\therefore 1 = 16 - 3 \cdot 5$

$= 16 - (19 - 16 \cdot 1) \cdot 5 = 16*6 - 19*5$

$= (35 - 19 \cdot 1)\,6 - 19*5$

$= 35*6 - 19*11$

$= 35*6 - (54 - 35)*11$

$= 35*17 - 54*11$

$= (89 - 54)17 - 54*11$

$= 89*17 - 54*28$

$= 89*17 - (232 - 89*2)*28$

$= 89*73 - 232*28$

$\therefore 1 = 89*73 - 232*28$

With mod 232, (remainder with mod 232)

$1 \bmod(232) \equiv 89*73 + 0$

$\therefore$ 73 is inverse of 89 mod(232)

Cryptography

Number theory plays a key role in cryptography, to keep the message secret between sender and receiver from the third party.

- **Classical cryptography**

One of the earliest known uses of cryptograph was by Julius Caesar. He made message secret by shifting each letter forward by three letters in the alphabet (sending the last three letters of the alphabet to the first letters). This process is called encryption.

To express Caesar's encryption process mathematically, first replace each letter by an element of Z_{26} (integers from 0 to 25). and then represent it by function f s.t.

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

where integer $f(p)$ in the set $\{0, 1, 2, \ldots, 25\}$

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

Example : What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

Solution :- First replace the letters in the message with numbers.

This produce

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

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

Now replace each of the numbers p by $(p+3) \bmod 26$. This gives

$24+3 = 27 \equiv 1 \pmod{26}$

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

Translating this back to letters produce the encrypted message

"PHHW BRX LQ WKH SDUN".

* To recover the original message from a secret message encrypted by the Caesar cipher, the function f^{-1}, i.e. inverse of f, is used.
The process of determining the original message from the encrypted message is called decryption.
In this case, $f^{-1}(p) = (p-3) \bmod 26$.

The generalized form of Caesar cipher:
Instead of shifting the numerical equivalent of each letter by 3, we can shift the numerical equivalent of each letter by k, so that
$$f(p) = (p+k) \bmod 26.$$
Such a cipher is called a shift cipher.
• The decryption can be carried out using
$$f^{-1}(p) = (p-k) \bmod 26$$
• The integer k is called a key.

Example:- Encrypt the plaintext message "STOP GLOBAL WARMING" using the shift cipher with shift $k = 11$.

Solution:- To encrypt the message "STOP GLOBAL WARMING" we first translate each letter to the corresponding element of $\mathbb{Z}_{26}$. This produces the string
18 19 14 15 6, 11, 14, 1, 0, 11 22 0 17 12 8 13 6
We now apply the shift $f(p) = (p+11) \bmod 26$ to each number in this string. We obtain
3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.
Translating this last string back to letters, we obtain the cipher-text
"DEZA RWZMLW HLCXTYR".

Example:- Decrypt the ciphertext message
"LEWLYPLUJL PZ H NYLHA ALHJOLY"
that was encrypted with the shift cipher with shift $k=7$.

Soln: Translate the letters back to elements of $\mathbb{Z}_{26}$.

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0, 11, 7, 9, 14, 11, 24.

Next, shift each number by $-7 \bmod 26$;

4 23 15 4 17 8 4 13 24, 8 18, 0 6 17 4 0 19,
19 4 0 2 7 4 17,

Finally, we translate these numbers back to letters to obtain the plaintext. We obtain
"EXPERIENCE IS A GREAT TEACHER".

We can generalize shift ciphers further to slightly enchance security by using a function of the form.

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen so that f is a bijection. Such mapping is called a AFFINE TRANSFORMATION & resulting cipher is called AFFINE CIPHER

Definition of Bijection

The function $f(p) = (ap+b) \bmod 26$ is a bijection iff $\gcd(a, 26) = 1$.

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

Solution: Letter K represents 10.

$$\therefore f(10) = (7(10)+3) \bmod 26$$
$$= 21 \bmod 26$$

Now, Number 21 represent V,
$\therefore$ replace the letter K by V in the encrypted msg.