Number theory

The division algorithm:- let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$ such that $a = dq + r$

Here, d is called divisor, a is called the dividend q is called the quotient, r is called the remainder

$q = a \text{ div } d$, $r = a \bmod d$

1. what are the quotient and remainder when 101 is divided by 11 and -11 divided by 3?

sol^n:- we have $101 = 11 \cdot 9 + 2$

$d = 11$, $q = 9$, $r = 2$.

$-11 = 3 \cdot (-4) + 1$

$d = 3$, $q = -4$, $r = 1$

Modular arithmatic:-

Def^n:- If a and b are integers and m, is a positive integer, then a is congruent to b modulo m if m divides $a-b$. we use the notation $a \equiv b \pmod m$ to indicate that a is congruent to b modulo m. If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$

Theorem:- let a and b integers, and m be a positive integer, then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

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

soln: 6 divides so, $17 - 5 = 12$ Now $17 \equiv 5 \pmod{6}$

but $24 - 14 = 10$ which is not divisible by 6 so, $24 \not\equiv 14 \pmod{6}$.

Theorem:- let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

soln: If $a \equiv b \pmod{m}$ then $m \mid (a-b)$. This means that there is an integer k such that $a - b = km$ so that $a = b + km$. Conversely there is an integer k such that $a = b + km$ $\therefore km = a - b$ Here m divides $a - b$ so that $a \equiv b \pmod{m}$

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 $ac \equiv bd \pmod m$

proof:- Because $a \equiv b \pmod m$ and $c \equiv d \pmod m$ there are integers s and t with $b = a + sm$ and $d = c + tm$

$$b+d = a + sm + c + tm$$

$$= (a+c) + m(s+t)$$

$$\therefore a+c \equiv (b+d) \pmod m$$

$$bd = (a+sm)(c+tm)$$

$$= ac + m(at + cs + stm)$$

$$\therefore ac \equiv bd \pmod m$$

Cryptology:

1. what letter replace the letter K when the function $f(p) = (7p+3) \bmod 26$ is used for encryption?

Solⁿ:- K represents 10 so that,

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

$$= 21$$

which represents V so K is replace by V.

Scanned by CamScanner

2. What is the Least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Soln:- We have, $lcm = 2^{max(3,4)} \cdot 3^{max(5,3)} \cdot 7^{max(2,0)}$

$= 2^4 3^5 7^2$

* Euclidean algorithm:-

procedure: gcd (a, b)

x: = a

y: = b

while $y \neq 0$

begin

r: = x mod y

x: = y

y: = r

end [gcd (a,b) is x]

* If $a = bq + r$ and a, b, q and r are integers, Then gcd (a,b) = gcd (b,r)

*
$$a = bq_1 + r_1 \quad 0 \leq r_1 < b$$
$$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \quad 0 \leq r_{n-1} \leq r_{n-2}$$

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

1. Determine whether the integers 10, 17, 21 are pairwise relatively prime and whether the integers 10, 19, 24 are pairwise relatively prime?

Sol^n:- $\gcd(10, 17) = 1$

$\gcd(10, 21) = 1$

$\gcd(17, 21) = 1$

they are pairwise relatively prime.

$\gcd(10, 24) = 2 > 1$

they are not pairwise relatively prime.

1. Using prime factorizations the gcd of 120 and 500?

Sol^n:- Here, $120 = 2^3 \cdot 3 \cdot 5$

$500 = 2^2 \cdot 5^3$

$\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$

$= 2^2 \cdot 3^0 \cdot 5^1$

$= 20$

Scanned by CamScanner

of Because $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$ it follows the theorem that

$18 = 7 + 11 \equiv 2 + 1 \equiv 3 \pmod 5$

and

$77 = 7 \cdot 11 \equiv 2 \cdot 1 \equiv 2 \pmod 5$

Theorem 1:- Let a, b and c are integers then

(i) $a|b$ and $a|c$ then $a|b+c$

proof:- if $a|b$ and $a|c$ then defn of divisibility there are integers s and t $b = as$, $c = at$

$\therefore$ $b + c = as + at = a(s+t)$

$\therefore$ a divides $b+c$ so that $a|(b+c)$

GCD and LCM

1. What is the greatest common divisor of 24 and 36?

Soln: gcd $(24, 36) = 12$

2. What is the greatest common divisor of 17 and 22?

Soln: gcd $(17, 22) = 1$

Defn:- The integers are relatively prime if their gcd $= 1$

$r_{n-2} = r_{n-1} a_n + r_n$, $0 \le r_n < r_{n-1}$

when $r_n = 0$. then $\gcd(a,b) = r_{n-1}$

※ If $a = 37$, $b = 8$ then $\gcd(a,b) = ?$

$37 = 8 \times 4 + 5$

$8 = 5 \times 1 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

$\therefore \gcd(a,b) = 1$

$37 = 8 \times 5 - 3$

$8 = 3 \times 3 - 1$

$3 = 1 \times 3 - 0$

$\gcd(a,b) = 1$

it is called minimal remainder.

※ Lame's theorem: Let $a > b$, both positive and let n be the number of division in Euclidean's algorithm. for a and b, then $n \le 5t$, where t is the number of digits in b.

EX:- If $a = 13$, $b = 8$, Here $a > b$ and $t = 1$

$n = 5$, $n = 5t = 5 \times 1 = 5$

$13 = 8\times1 + 5$

$8 = 5\times1 + 3$

$5 = 3\times1 + 2$

$3 = 2\times1 + 1$

$2 = 1\times2 + 0$

$\therefore n = 5$

$\gcd(13, 8) = 1$

* Kronecker's theorem:- $M(a, b) \leq E(a, b)$

* Theorem: The gcd is unique.

$\gcd(a, b) = d_1$

$\gcd(a, b) = d_2$

$\therefore d_1 = d_2$

* Theorem:- Let $a_1, a_2 \cdots a_n$ be any non-zero integer's whose gcd is d, then there exists integers $x_1, x_2, \cdots x_n$ such that,

$a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$

* If $\gcd(252, 198) = 18$ find Linear combination of 252 and 198?

$252x_1 + 198x_2 = 18$

$252 = 198\times1 + 54$ —(i)

$198 = 54\times3 + 36$ —(ii)

$54 = 36\times1 + 18$ —(iii)

$36 = 18 \times 2 + 0$ —— (iv)

(i) $54 = 252 - 198 \times 1$

(ii) $36 = 198 - 54 \times 3$

$= 198 - (252 - 198 \times 1) \times 3$

$= 4 \times 198 - 252 \times 3$

(iii) $18 = 54 - 36 \times 1$

$= 54 - (4 \times 198 - 252 \times 3)$

$= (252 - 198 \times 1) - (4 \times 198 - 252 \times 3)$

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

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

$\therefore x_1 = 4,\ x_2 = -5$

※ Theorem:- If a, b and c are positive integer such that $\gcd(a, b) = 1$ and $a | bc$ then $a | c$.

※ 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.

※ Theorem:- Let m be a positive integer and Let a, b, and c be integers,

if $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$

then $a \equiv b \pmod{m}$

※ $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

$m = 3 \times 5 \times 7$

$= 105$

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

$M_2 = 21, \quad M_3 = 15$

y_1 = inverse of M_1 mod m_1

= " " 35 " 3

$S = \{0, 1, 2\}$

$35x \bmod 3 = 1 \longrightarrow 35x \equiv 1 \pmod 3$

$\therefore 35x \bmod 3 = 1 \bmod 3$

$= 1$

$x = 0, \quad 35 \cdot 0 = 0 \bmod 3 = 0$

$x = 1 \quad 35 \cdot 1 = 35 \bmod 3 = 2$

$x = 2, \quad 35 \cdot 2 = 70 \bmod 3 = 1$

$\therefore y_1 = 2$

$y_2 = 1, \ y_3 = 1$

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

$= 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233$

Theorem:- If a and m are relatively prime integer and $m > 1$ then inverse of a mod m exist.

$\gcd(a, m) = 1$

$\gcd(3, 7) = 1$

※ **The chines remainder theorem:-** Let $m_1, m_2 \cdots m_n$ be pairwise prime positive integer and $a_1, a_2 \cdots a_n$ arbitrary integers. then the system.

$$x = a_1 \pmod{m_1}$$

$$x = a_2 \pmod{m_2}$$

$$\vdots$$

$$x = a_n \pmod{m_n}$$

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

$$m = m_1 m_2 \cdots m_n$$

$$M_k = \frac{m}{m_k}$$

i.e $M_1 = \frac{m}{m_1}$, $M_2 = \frac{m}{m_2}$

$$\gcd(M_k, m_k) = 1$$

$$M_k y_k \equiv 1 \pmod{m_k}$$

$\downarrow$

inverse of M_k mod m_k

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + \cdots + a_n M_n y_n$$

proof :- Given that, $ac \equiv bc \pmod m$

$m | ac - bc$

$m | c(a-b)$

Here, $\gcd(c,m) = 1$, and $m | c(a,b)$ so

$m | (a-b)$ [Euclid's first theorem]

by def^n $a \equiv b \pmod m$

※ Linear Congruence :- $ax \equiv b \pmod m$ where m is a positive integers and a and b are integers, and x is a variable, is called linear congruence.

※ $3x \equiv 4 \pmod 7$ find $x = ?$

Soln:- $3x \equiv 4 \pmod 7$

$3x \bmod 7 = 4 \bmod 7$

$= 4$

Here, $S = \{0, 1, 2, 3, 4, 5, 6\}$

$x = 0$, $3x = 0$, $0 \bmod 7 = 0$

$x = 1$, $3 \cdot 1 = 3$, $3 \bmod 7 = 3$

⋮

$x = 6$, $3 \cdot 6 = 18$, $18 \bmod 7 = 4$

$\therefore x = 6$ (Ans:)

$\therefore x = 233 \bmod 105 = 23$ (Ans)

FERMET'S LITTLE THEOREM:- If p is a prime and a is an integer not divisible then;

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

$\gcd(p,a) = 1$

$p = 341,\ a = 2$

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

Let b be a positive integer if n is a composite positive number and $b^{n-1} \equiv 1 \pmod{n}$ then n is called pseudoprime to the base b.

A composite integer that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all positive integer b with $\gcd(b,n) = 1$ is called carmichael number.

Example:- The integer 561 is a carmichael number because 561 is composite $561 = 3 \cdot 11 \cdot 17$

if $\gcd(b, 561) = 1$ then,

$\gcd(b, 3) = 1$

$\gcd(b, 11) = 1$

$\gcd(b, 17) = 1$

Now, $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$

it follows that. $b^{560} = (b^2)^{280} \equiv 1 \pmod 3$

$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$$

$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$$

Now. $b^{560} \equiv 1 \pmod{561}$ so that $\gcd(b, 561) = 1$ so it is an carmichael number.

※ public key and private key :-

Encryption :- $C = (P+K) \bmod 26$

$$K \downarrow \text{key} = 3$$

$$C = (A+3) \bmod 26$$

$$= (1+3) \bmod 26$$

$$= 4$$

$\therefore C = \text{'D'}$

Decryption :- $P = (C-K) \bmod 26$

$$= (4-3) \bmod 26$$

$$= 1 \bmod 26$$

$$= 1$$

$$P = \text{'A'}$$

RSA algorithm:-

1. Select p, q
2. $n = pq$
3. $\varphi(n) = (p-1)(q-1)$
4. select e, $\gcd(e, \varphi(n)) = 1$

   $1 < e < \varphi(n)$

5. Calculate $de \equiv 1 \pmod{\varphi(n)}$
6. public key $\{e, n\}$

※ **Ex:-** 1. $p = 17,\ q = 11$

2. $n = 17 \times 11$
   $= 187$

3. $\varphi(n) = 16 \times 10 = 160$

4. $e = 7.\quad \gcd(7, 160) = 1$

5. $d = 23 \quad de \equiv 1 \pmod{160}$

   $d \cdot 7 \equiv 1 \pmod{160}$

6. public key $\{7, 187\}$

   private key $\{23, 187\}$

plain text 88 $\longrightarrow 88^7 \bmod 187 = 11$

" " 88 $\longrightarrow 11^{23} \bmod 187 = 88$