09/15/22

Divisibility:-

$n \mid a \rightarrow n$ perfectly divides 'a'.
$n / a \rightarrow n$ divides 'a'.

$\boxed{a = qn + r}$, and $0 \le r < n$, where $\boxed{q = \lfloor a/n \rfloor}$

q = quotient, r = reminder, a = dividend ; n = divisor.

GCD:-

→ The smallest GCD for 2 numbers is '1'.

→ If the value of one number is '0' then take the GCD of another number and take the absolute value

Modular Arithmetic Congruence :-

If $(a \bmod n) = (b \bmod n)$ then a and b are congruence to the divisor 'n'.

Modular Arithmetic properties:-

Multiplicative inverse modulo n:

→ Consider Z_p, $P = 7$; $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

Definition:- For each element $(w) = Z_p$; $w \neq 0$, there exists a $z \in Z_p$, such that $\boxed{w \cdot z \equiv 1 \pmod{P}}$

w	z
0	Doesn't Exist
1	1
2	4
3	5
4	2
5	3

6 | 0

Ex:- $a = 2, b = 5, n = 7$

$\frac{2}{5} \pmod 7$

$= 2 \cdot 5^{-1} \pmod 7$

$= 2 \cdot 3 \bmod 7$

$= 6.$

GCD using Euclidean Algorithm:-

Find $\gcd(a, b)$

1.) $r_1 = a \bmod b.$

$r_2 = b \bmod r_1.$

$r_3 = r_1 \bmod r_2$

$\vdots$

$r_n = r_{n-2} \bmod r_{n-1}$

If $r_n = 0$, set $r_{n-1} = \gcd(a, b)$

If $\gcd(a, b) = 1$, a, b, are co-primes

$a, b \geq 0.$

Ex:- $\gcd(48, 25)$

$r_1 = 48 \bmod 25 = 23.$

$r_2 = 25 \bmod 23 = 2.$

$r_3 = 23 \bmod 2 = 1.$

$r_4 = 2 \bmod 1 = 0.$

$\therefore \gcd(48, 25) = 1,$ co-prime

9/20/22: Extended Euclidean Algorithm (Bezouté lemma)

If $a, b > 0$, and $\gcd(a,b) = d$; $d \geq 1$, then $\exists x, y \in \mathbb{Z}$

such that $\boxed{x \cdot a + y \cdot b = d}$ x & y are not unique.

$x \cdot a \pmod{b} = 1$.

and

$y \cdot b \pmod{a} = 1$.

Ex1:- Find (x, y)

For $a = 84$, $b = 33$

sol:- First find $\gcd(a,b) = d$

$r_1 = 84 \bmod 33 = 18$	$q_1 = 2$
$r_2 = 33 \bmod 18 = 15$	$q_2 = 1$
$r_3 = 18 \bmod 15 = 3$ gcd	$q_3 = 1$
$r_4 = 15 \bmod 3 = 0$	$q_4 = 5$

$\therefore \gcd(84, 33) = 3 = d$.

Find x, y, such that;

$x \cdot 84 + y \cdot 33 = 3$. → (by Extended Euclidean)

$\boxed{\text{dividend} = \text{divisor} \cdot q + r}$

$\boxed{r = \text{dividend} - q \cdot \text{divisor}}$

$3 = 18 - 1 \cdot 15$

$= 18 - 1(33 - 1 \cdot 18)$

$= 18 \cdot 1 - 1(33 - 18 \cdot 1)$

$$= 2(18) - (33)\cdot 1$$

$$= 2(84 - 2\cdot 33) - 1(33)$$

$$3 = 2(84) - 3(33)$$

$$x = 2 \; ; \; y = -5.$$

Ex2:- Find (x, y) for $(210, 45)$

Sol:- set $a = 210$; $b = 45$.

Find the $\gcd(210, 45) = d$.

$r_1 = 210 \mod 45 = 30$		$q_1 = 4$
$r_2 = 45 \mod 30 = 15$ gcd		$q_2 = 1$
$r_3 = 30 \mod 15 = 0$		$q_3 = 2$

$\therefore d = 15.$

$\therefore \gcd(210, 45) = 15.$

Now Find (x, y); such that;

$$x \cdot a + y \cdot b = d$$

$$210x + 45y = 15. \rightarrow \text{(by Extended Euclidean)}$$

we know that, $\boxed{\text{dividend} = \text{divisor} \cdot q + r}$

$$r = \text{dividend} - q \cdot \text{divisor}$$

$$15 = 45 - 1(30)$$

$$15 = (45)1 - 1(210 - 45 \cdot 4)$$

$$15 = (45)1 - (210)1 + (45)4$$

$$15 = (45)5 - (210)1$$

$$15 = -(210)1 + (45)5.$$

$$\therefore x = -1 \; ; \; y = 5.$$

GF(P): Galois Field.

$$GF(P) = \mathbb{Z}_P = \{0, \dots, P-1\}$$

$GF(P^n)$, P is prime, $n > 0$ has exactly P^n polynomials.

$$f(x) = a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \dots + a_1 x + a_0$$

$$f(x) = \sum_{i=0}^{n-1} a_i \dots x^i.$$

$$a_i \in \{0, \dots, P-1\}$$

degree of $f(x)$ is $(n-1)$.

Ex1:- Let $P = 2$; $n = 3$ Find set of all polynomials in $GF(2^3)$.

Sol:- $a_i \in \{0, 1\}$

$$f(x) = \sum_{i=0}^{2} a_i \cdot x^i$$

$\underline{i=0:}$ $f(x) = a_0 \cdot x^0$.

$S_0 = \{0, 1\}$

$\underline{i=1:}$ $f(x) = a_0 x^0 + a_1 x^1$

$S_1 = \{ \overset{(0,0)}{0} ; \overset{(0,1)}{x} ; \overset{(1,0)}{1} ; \overset{(1,1)}{1+x} \}$

$\underline{i=2:}$ $f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2$

$S_2 = \{ 000, 001, 010, 011, 100, 101, 110, 111 \} \rightarrow$ (set of Possible Combinations)

$\therefore S_2 = \{ 0, 1, x^2, x, x+x^2, x^2+1, x+1, x^2+x+1 \}$

$\therefore S = S_1 \cup S_2 \cup S_3$

$S = \{ 0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1 \}$

$\underline{\text{Ex 2:-}}$ Find set of Polynomials in $GF(3^2)$

$f(x) = \sum_{i=0}^{1} a_i \cdot x^i ; a_i \in \{0, 1, 2\}$

$\underline{i=0:}$ $f(x) = a_0 x^0$,

$S_0 = \{0, 1, 2\}$

$\underline{i=1:}$ $f(x) = a_0 x^0 + a_1 x^2$.

$f(x) = a_0 + a_1 x$

No of Combinations Possible $= \{ 00, 01, 10, 11, 02, 20, 22, 12, 21 \}$

$S_1 = \{0, 1, 2, x, x+1, 2x+1, x+2, 2x, 2x+2\}$

$\therefore S = S_0 \cup S_1$

$\therefore S = \{0, 1, 2, x, x+1, 2x+1, x+2, 2x, 2x+2\}.$