NUMBER THEORY AND CRYPTOGRAPHY

CHAPTER - 4

WEEK - 7

DIVISION:- If a and b are integers and $a \neq 0$. we say that a divides b written as $a|b$ (or) $\frac{b}{a}$ if there is an integer c such that $b = ac$.

When a divides b, then a is a factor or divisor of b and b is a multiple of a.

Eg: $4|12$, $3|9$, $2 \nmid 9$, $5 \nmid 24$.

NOTE
1) If $a|b$ and $a|c$, then $a|(b+c)$ and $a|(mb+nc)$
2) If $a|b$, then $a|bc$ for all c
3) If $a|b$ and $b|c$ then $a|c$

DIVISION ALGORITHM:- If a is an integer and d is a positive integer, then there exists unique integers q and r such that $a = dq + r$ where $0 \leq r < d$.

$$d\,)\,a\,(\,q$$

r

DIVIDEND, DIVISOR, QUOTIENT, REMAINDER.

NOTE
$q = \lfloor a/d \rfloor$ (Floor function)

$r = a - d\lfloor a/d \rfloor$

Eg ① Find the quotient and remainder when 123 is divided by 5

Sol

$$5\,\overline{)\,123\,}\,(24$$
$$\underline{120}$$
$$\underline{3}$$

quotient = 24
remainder = 3.

$123 = (5)(24) + 3.$

Eg ② What is the quotient and remainder when -13 is divided by 4

Sol

$$4\,\overline{)\,-13\,}\,(-4$$
$$\underline{-16}$$
$$\underline{3}$$

$-13 = 4(-4) + 3.$

$$4\,\overline{)\,-13\,}\,(-3$$
$$\underline{-12}$$
$$\underline{-1}$$

$-13 = 4(-3) + (-1)$
This is not correct as r must be positive and does not satisfy $0 \le r < d$.

CONGRUENCE :- 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 write this as $a \equiv b \pmod{m}$.

Eg

$15 \equiv 3 \pmod{2}$
$15 \equiv 3 \pmod{4}$
$15 \equiv 3 \pmod{6}$
$21 \equiv 6 \pmod{5}$
$47 \not\equiv 2 \pmod{6}$.
$24 \not\equiv 14 \pmod{6}$

NOTE 1) When $a \equiv b \pmod{m}$, then the remainder is zero and $\frac{a-b}{m} = K$ where K is an integer

(or) $a = b + mK$

(2) If $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then

(i) $a + c \equiv b + c \pmod{m}$

(ii) $ac \equiv bc \pmod{m}$.

Eg: $9 \equiv 2 \pmod{7}$ and $15 \equiv 1 \pmod{7}$.

$\Rightarrow 9 + 15 \equiv 2 + 1 \pmod{7}$ i.e., $24 \equiv 3 \pmod{7}$

and $(9)(15) \equiv (2)(1) \pmod{7}$ i.e., $135 \equiv 2 \pmod{7}$

ARITHMETIC MODULO m

If a, b are non negative integers less than m, then

$a +_m b$ = The remainder when $(a+b)$ is divided by m.

Eg: $3 +_8 6 = 1$ $\qquad \frac{3+6}{8} = \frac{9}{8}$ $\quad 8)9(1$, $\frac{8}{1}$

$5 +_{11} 10 = 4$ $\qquad \frac{5+10}{11} = \frac{15}{11}$ $\quad 11)15(1$, $\frac{11}{4}$.

MULTIPLICATION MODULO m

$a \cdot_m b$ = The remainder then $a \cdot b$ is divided by m

Eg: $3 \cdot_6 5 = 3$. $\qquad \frac{3 \times 5}{6} = \frac{15}{6}$ $\quad 6)15(2$, $\frac{12}{3}$

$5 \cdot_{11} 10 = 6$. $\qquad \frac{5 \times 10}{11} = \frac{50}{11}$ $\quad 11)50(4$, $\frac{44}{6}$

Eg: $4 +_7 3 = 0$. $\qquad 3 \cdot_{11} 7 = 10$.

$5 +_8 6 = 3$. $\qquad 8 \cdot_{12} 9 = 0$.

Binary expansions – base is 2 – Each digit is either a 0 or 1

Octal expansion – base is 8.
Decimal expansion – base is 10.
Hexa Decimal expansion – base is 16. – 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
A = 10, B = 11, C = 12, D = 13, E = 14
F = 15

Binary to Decimal

$$(101010101)_2 = 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0.$$

$$= 256 + 0 + 64 + 0 + 16 + 0 + 4 + 0 + 1$$

$$= (341)_{10}.$$

$$(101011111)_2 = 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0$$

$$= 256 + 0 + 64 + 0 + 16 + 8 + 4 + 2 + 1$$

$$= (351)_{10}.$$

Octal to Decimal

$$(7016)_8 = 7\cdot 8^3 + 0\cdot 8^2 + 1\cdot 8^1 + 6\cdot 8^0$$

$$= 3584 + 0 + 8 + 6$$

$$= (3598)_{10}.$$

$$(572)_8 = 5\times 8^2 + 7\times 8^1 + 2\times 8^0$$

$$= 320 + 56 + 2$$

$$= (378)_{10}.$$

Hexa Decimal to Decimal

$(2AE0B)_{16} = 2\times16^4 + 10\times16^3 + 14\times16^2 + 0\times16^1 + 11\times16^0$

$= (175627)_{10}$

$(80E)_{16} = 8\times16^2 + 0\times16^1 + 14\times16^0$

$= 2048 + 0 + 224$

$= (2272)_{10}$.

Decimal to octal

$(12345)_{10}$ = Write the Remainders in reverse order.

$= (30071)_8$.

$$\boxed{\begin{aligned} 12345 &= 8\cdot1543+1 \\ 1543 &= 8\cdot192+7 \\ 192 &= 8\cdot24+0 \\ 24 &= 8\cdot3+0 \\ 3 &= 8\cdot0+3 \end{aligned}}$$

$8) 12345 (1543$
12344
1

$8) 1543 (192$
1536
7

$8) 192 (24$
192
0

$8) 24 (3$
24
0

$8) 3 (0$
0
3

Go on dividing until you get 0 as quotient.

$(4532)_{10} = (10664)_8$

$$\boxed{\begin{aligned} 4532 &= 8\cdot 566 + 4 \\ 566 &= 8\cdot 70 + 6 \\ 70 &= 8\cdot 8 + 6 \\ 8 &= 8\cdot 1 + 0 \\ 1 &= 8\cdot 0 + 1 \end{aligned}}$$

$8)\,4532\,(566$
4528
4

$8)\,566\,(70$
560
6

$8)\,70\,(8$
64
6

$8)\,8\,(1$
8
0

$8)\,1\,(0$
0
1

Decimal to hexadecimal

$(177130)_{10} = (2B3EA)_{16}$

$$\boxed{\begin{aligned} 177130 &= 16\cdot 11070 + 10 \\ 11070 &= 16\cdot 691 + 14 \\ 691 &= 16\cdot 43 + 3 \\ 43 &= 16\cdot 2 + 11 \\ 2 &= 16\cdot 0 + 2 \end{aligned}}$$

$16)\,177130\,(11070$
177120
$10 \to A$

$16)\,11070\,(691$
11056
$14 \to E$

$16)\,691\,(43$
688
3

$16)\,43\,(2$
32
$11 \to B$

$16)\,2\,(0$
0
2

$(100632)_{10} = (18918)_{16}$

$$\boxed{\begin{aligned} 110632 &= 16\cdot 6289 + 8 \\ 6289 &= 16\cdot 393 + 1 \\ 393 &= 16\cdot 24 + 9 \\ 24 &= 16\cdot 1 + 8 \\ 1 &= 16\cdot 0 + 1 \end{aligned}}$$

$16)\,100632\,(6289$
100624
8

$16)\,6289\,(393$
6288
1

$16)\,393\,(24$
384
9

$16)\,24\,(1$
16
8

$16)\,1\,(0$
0
1

Decimal to binary

$(241)_{10} = (11110001)_2$

$(231)_{10} = (11100111)_2$

$$
\begin{array}{l}
2)\underline{231}\ (115 \\
\quad \underline{230} \\
\quad\ \ 1 \\
2)\underline{115}\ (57 \\
\quad \underline{114} \\
\quad\ \ 1 \\
2)\underline{57}\ (28 \\
\quad \underline{56} \\
\quad\ 1 \\
2)\underline{28}\ (14 \\
\quad \underline{28} \\
\quad\ 0 \\
2)\underline{14}\ (7 \\
\quad \underline{14} \\
\quad\ 0 \\
2)\underline{7}\ (3 \\
\quad \underline{6} \\
\quad 1 \\
2)\underline{3}\ (1 \\
\quad \underline{2} \\
\quad 1 \\
2)\underline{1}\ (0 \\
\quad \underline{0} \\
\quad 1
\end{array}
$$

$$
\boxed{
\begin{array}{l}
231 = 2\cdot 115+1 \\
115 = 2\cdot 57+1 \\
57 = 2\cdot 28+1 \\
28 = 2\cdot 14+0 \\
14 = 2\cdot 7+0 \\
7 = 2\cdot 3+1 \\
3 = 2\cdot 1+1 \\
1 = 2\cdot 0+1
\end{array}
}
$$

$$
\begin{array}{l}
2)\underline{241}\ (120 \\
\quad \underline{240} \\
\quad\ \ 1 \\
2)\underline{120}\ (60 \\
\quad \underline{120} \\
\quad\ \ 0 \\
2)\underline{60}\ (30 \\
\quad \underline{60} \\
\quad\ 0 \\
2)\underline{30}\ (15 \\
\quad \underline{30} \\
\quad\ 0 \\
2)\underline{15}\ (7 \\
\quad \underline{14} \\
\quad\ 1 \\
2)\underline{7}\ (3 \\
\quad \underline{6} \\
\quad 1 \\
2)\underline{3}\ (1 \\
\quad \underline{2} \\
\quad 1 \\
2)\underline{1}\ (0 \\
\quad \underline{0} \\
\quad 1
\end{array}
$$

$$
\boxed{
\begin{array}{l}
241 = 2\cdot 120+1 \\
120 = 2\cdot 60+0 \\
60 = 2\cdot 30+0 \\
30 = 2\cdot 15+0 \\
15 = 2\cdot 7+1 \\
7 = 2\cdot 3+1 \\
3 = 2\cdot 1+1 \\
1 = 2\cdot 0+1
\end{array}
}
$$

Binary to octal

(Group the binary digits into a block of three binary digits. ~~from left to right~~ if necessary add zeros at the beginning)

$$
\begin{aligned}
(11\,1110\,1011\,1100)_2 &= (011\ 111\ 010\ 111\ 100)_2 \\
&= (3\quad 7\quad 2\quad 7\quad 4)_8 \\
&= (37274)_8.
\end{aligned}
$$

Binary to Hexadecimal :- Group the binary digits into blocks of four and if necessary add zero's at the beginning.

$$(11111010111100)_2 = (0011 \;\; 1110 \;\; 1011 \;\; 1100)$$

$$= (3 \;\; 14 \;\; 11 \;\; 12)_{16}$$

$$= (3 \;\; E \;\; B \;\; C)_{16}$$

Octal to Binary :- Replace each octal digit by a block of three binary digits.

$$(765)_8 = (111 \;\; 110 \;\; 101)_2$$

$$(16175)_8 = (001 \;\; 110 \;\; 001 \;\; 111 \;\; 101)_2$$

Hexa Decimal to Binary : Replace each ~~oct~~ hexadecimal digit by a block of four binary digits.

$$(A8D)_{16} = (1010 \;\; 1000 \;\; 1101)_2$$

$$(BD2F)_{16} = (1011 \;\; 1101 \;\; 0010 \;\; 1111)_2$$

Try: Octal to Hexa Decimal.

Hexa Decimal to Octal.

PRIME NUMBER:- An integer $P > 1$ is said to be a prime number if the divisors of p are 1 and p itself.

(EG) 2, 3, 5, 7, 11, 13, 17, ...

PRIME FACTORIZATION:- Every integer greater than 1 can be written as a product of prime numbers.

Examples:-

$$100 = 2 \times 50 = 2 \times 2 \times 25 = 2 \times 2 \times 5 \times 5 = 2^2 5^2$$

$$372 = 2 \times 186 = 2 \times 2 \times 93 = 2 \times 2 \times 3 \times 31 = 2^2 \cdot 3^1 \cdot 31^1$$

$$745 = 5 \times 149$$

$$7007 = 7 \times 1001 = 7 \times 7 \times 143 = 7 \times 7 \times 11 \times 13 = 7^2 \cdot 11^1 \cdot 13^1$$

GREATEST COMMON DIVISOR (GCD):- If a and b are integers, then the largest integer d such that $d|a$ and $d|a$ is called the $gcd(a,b)$.

Example $gcd(24, 36)$

Divisors of 24 = 1, 2, 3, 4, 6, 12, 24

Divisors of 36 = 1, 2, 3, 4, 6, 9, 12, 18, 36.

Common divisors = 1, 2, 3, 4, 6, 12

Greatest Common divisor = 12 $\Rightarrow gcd(24, 36) = 12$

2) gcd (9, 16)

Divisors of 9 = 1, 3, 9

divisors of 16 = 1, 2, 4, 8, 16.

Common divisors = 1

gcd (9, 16) = 1

RELATIVELY PRIME NUMBERS:- Two integers are said to be relatively prime if their gcd is 1

Eg 17 and 22 are relatively prime.

II. method to find gcd (a, b) using Prime factorization

Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$

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

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

Eg gcd (45, 120)

$45 = 3 \times 15$
$= 3 \times 3 \times 5$
$= 2^0 . 3^2 . 5^1$

$120 = 2 \times 60$
$= 2 \times 2 \times 30$
$= 2 \times 2 \times \cancel{2} \times 15$
$= 2 \times 2 \times 2 \times 3 \times 5$
$= 2^3 . 3^1 . 5^1$

$gcd(45,120) = 2^{\min(0,3)} 3^{\min(2,1)} 5^{\min(1,1)}$
$= 2^0 . 3^1 . 5^1$
$= 15$

~~GCD BASE~~ NOTE :- If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$

EUCLIDEAN ALGORITHM :-

If a and b are positive integers with $a \geq b$.

Let $r_0 = a$ and $r_1 = b$. By division algorithm.

$r_1 = b) \overset{r_0}{a} (q_1$

$\overline{r_2}$

$r_2) r_1 (q_2$

$\overline{r_3}$

$r_3) r_2 (q_3$

$\overline{q_4}$

$$r_0 = r_1 q_1 + r_2$$
$$r_1 = r_2 q_2 + r_3.$$
$$r_2 = r_3 q_3 + r_4$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n.$$
$$r_{n-1} = r_n q_n + 0.$$

Now
$$\begin{aligned}
\gcd(a,b) &= \gcd(r_0, r_1) \\
&= \gcd(r_1, r_2) \\
&= \gcd(r_2, r_3) \\
&\ \vdots \\
&= \gcd(r_{n-2}, r_{n-1}) \\
&= \gcd(r_{n-1}, r_n) \\
&= \gcd(r_n, 0) \\
&= r_n.
\end{aligned}$$

Hence the gcd is the LAST NON ZERO REMAINDER in the sequence of divisions.

Example 1 Find the gcd (414, 662) using Euclidean algorithm.

Sol.

$$
\begin{array}{l}
414)\,662\,(1 \\
\quad\;\; 414 \\
\quad\;\; \overline{248)\,414\,(1} \\
\qquad\qquad 248 \\
\qquad\qquad \overline{166)\,248\,(1} \\
\qquad\qquad\qquad 166 \\
\qquad\qquad\qquad \overline{82)\,166\,(2} \\
\qquad\qquad\qquad\quad 164 \\
\qquad\qquad\qquad\quad \overline{2)\,82\,(41} \\
\qquad\qquad\qquad\qquad 82 \\
\qquad\qquad\qquad\qquad \overline{0}
\end{array}
$$

$$
\boxed{
\begin{aligned}
662 &= 414\cdot 1 + 248 \\
414 &= 248\cdot 1 + 166 \\
248 &= 166\cdot 1 + 82 \\
166 &= 82\cdot 2 + 2 \\
82 &= 2\cdot 41 + 0
\end{aligned}
}
$$

gcd (414, 662) = Last non zero remainder

= 2.

Example 2 Find the gcd (91, 287) by Euclidean Algorithm

Sol.

$$
\begin{array}{l}
91)\,287\,(3 \\
\quad\;\; 273 \\
\quad\;\; \overline{14)\,91\,(6} \\
\qquad\quad 84 \\
\qquad\quad \overline{7)\,14\,(2} \\
\qquad\qquad 14 \\
\qquad\qquad \overline{0}
\end{array}
$$

$$
\begin{aligned}
287 &= 91\cdot 3 + 14 \\
91 &= 14\cdot 6 + 7 \\
14 &= 7\cdot 2 + 0.
\end{aligned}
$$

gcd (91, 287) = Last nonzero remainder

= 7

LEAST COMMON MULTIPLE (LCM), If a and b are integers, then the smallest integer that is divisible by both a and b is called lcm(a,b).

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

Example:- lcm (120, 500).

$$120 = 2\times 60 = 2\times 2\times 30 = 2\times2\times2\times15 = 2^3\cdot 3^1\cdot 5^1$$

$$500 = 2\times 250 = 2\times 2\times 125 = 2\times2\times5\times25 = 2\times2\times5\times5\times5 = 2^2\cdot 3^0\cdot 5^3$$

$$\operatorname{lcm}(120,500) = 2^{\max(3,2)}\, 3^{\max(1,0)}\, 5^{\max(1,3)} = 2^3\cdot 3^1\cdot 5^3 = 8\times3\times125 = 3000$$

Relation between gcd & lcm

* NOTE: $\gcd(a,b)\times \operatorname{lcm}(a,b) = a\cdot b$.

Example Let $a=120$, $b=500$

$$\gcd(120,500) = 2^{\min(3,2)}\cdot 3^{\min(1,0)}\cdot 5^{\min(1,3)} = 2^2\cdot 3^0\cdot 5^1 = 20$$

$$\operatorname{lcm}(120,500) = 2^{\max(3,2)}\cdot 3^{\max(1,0)}\cdot 5^{\max(1,3)} = 2^3\cdot 3^1\cdot 5^3 = 3000.$$

Now $\gcd(120,500)\times \operatorname{lcm}(120,500) = 20\times 3000 = 60\,000$.

and $a\cdot b = 120\times 500 = 60000$

Therefore $\gcd(a,b)\times\operatorname{lcm}(a,b) = a\cdot b$.