CLASS TEST SHEET

Date of Test

Roll No. Reg. No. Course Code Section Test No.

Unit-6 Number theory and its application in cryptography

1. Divisibility Defn & its properties,
2. Division Algorithm
3. Modular Arithmetic

(1)

4. Primes
5. fundamental theorem of arithmetic
6. GCD, LCM & Euclidean algorithm. (find GCD using EA / Linear congruence
7. Bezout's theorem of GCD (GCD of positive integers as LC) find the Bezout's coefficients of positive integers using EA.
8. Inverse (of (modulo m), soln of linear congruence's and proper (find the inverse using Bezout's thm and use it to solve linear congruence's). Chinese remainder theorem

9. Encryption and description by Ceasar cipher and affine transformation.
(decode and encode the messages by Ceasar cipher and affine transformation, Fermat's little theorem.

Defn. If p and q are integers with $p \neq 0$, we say that p divides q if $\exists$ an integer r such that $q = pr$.

$p | q \rightarrow$ notation.

Ex:- $3 \nmid 7$ but $3 | 12 \Rightarrow 12 = 3 \cdot 4$

Thm. Let p, q and r be integers, where $p \neq 0$. Then

i) if $p | q$ and $p | r$, then $p | (q+r)$.

ii) if $p | q$, then $p | qr$ for all integers r

iii) if $p | q$ and $q | r$, then $p | r$

$p | q \Rightarrow q = a \cdot p$, $p | r \Rightarrow r = bp$

Now $(q + r) = ap + bp = \underbrace{(a+b)}_{\text{integr}} p = cp$

$\Rightarrow p | (q+r)$

$p | q \Rightarrow q = ap$, $q | r \Rightarrow r = bq$

$r = bq = b \cdot (ap) = bap = cp$

$\Rightarrow p | r$.

Corollary ① If p, q and r are integers, where $p \neq 0$, such that $p | q$, & $p | r$, then $p | mq + nr$ where m & n are integer.

(from (ii) & (i) we proof this)

<u>The Division Algorithm</u>:- Let p be an integer and s a positive integer. Then $\exists$ a unique integers a and r, with $\underline{0 \leq r < s}$, such that $p = sa + r$.

Here $s \to$ divisor $\qquad a = dq + r$

$p \to$ dividend $\qquad p = sa + r$

$a \to$ quotient

$r \to$ remainder $\to$ we can write $\qquad$ divisor $\qquad$ 14-divident

$$3 \overline{)\,14\,(}\,4 \quad 4 \to \text{quotient}$$
$$\underline{12}$$
$$2 \to \text{remainder}$$

we can express the quotient and remainder as

$a = p \text{ div } s$, $r = p \bmod s$. $\Rightarrow s \mid p - r$

& $p \text{ div } s = \lfloor p/s \rfloor$

Ex: ① What are the quotient and remainder when 93 divided by 10 ?

Soln:

$93 = 10 \cdot 9 + 3 = sa + r$

quotient, $a = 9$, $r = 3$

i.e $9 = 93 \text{ div } 10$

and $3 = 93 \bmod 10$ (i.e 10 divides $(93-3)$) $10 \mid 93-3$

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

Soln:

$p = -13$, $s = 4$ $\qquad -16+3 = -13$

$-13 = 4(-4) + 3 \to$ bez $0 \le r < s \to$ positive integer

any integer

quotient, $a = -4$, $r = 3$

$3 = -13 \bmod 4$ & $-4 = -13 \text{ div } 4$

Theorem :- Let m be a positive integer. The integers a and b are congruent modulo m iff $\exists$ an integer k such that $a = b + km$.

(2) Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$a + c = b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Ex:- $8 \equiv 3 \pmod{5}$ and $11 = 1 \pmod{5}$

$8 + 11 = 3 + 1 \pmod{5}$

i.e $19 \equiv 4 \pmod{5}$

$\therefore 19 \equiv 4 \pmod{5}$

$8 \cdot 11 = 3 \cdot 1 \pmod{5}$

$88 = 3 \pmod{5}$

19
15
4

$5)19($

$5)88|17$
5
3

Let m be a positive integer and let a and b be integers. Then

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

and $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

$\longrightarrow$ after modulo