M.A.E.E.R.'S

MAHARASHTRA INSTITUTE OF TECHNOLOGY,

S. No. 124, Paud Road, Kothrud, Pune - 411 038.

F.E. : MID TERM EXAMINATION - 2007 - 08

Student's Name : _____

Subject : _____ **Div. :** _____ **Roll No. :** _____

Ques.							Total	
Marks								Sign.

Number Theory

Topics - Divisibility, Modular arithmetic, properties Euclidean algorithm, solving congruence eqn Chinese remainder thm, Fermat's thm.

Number Theory - study of set of integers & their properties.

Divisibility & modular Arithmetic -

Modular arithmetic - division of an integer by an +ve integer produces a quotient and a remainder. Working with these remainder ~~gives~~ leads to modular arithmetic which is imp in computer Science.

Def^n:- Let $a, b \in \mathbb{Z}$, $a \neq 0$.
a **divides** b if $\exists\ c \in \mathbb{Z}$ s.t, $b = ac$.
Notation - $a|b$

Thm :- Let $a, b, c \in \mathbb{Z}$ where $a \neq 0$ then
(i) If $a|b$ & $a|c \Rightarrow a|(b+c)$
(ii) If $a|b$ then $a|bc$ for all integers c
(iii) If $a|b$ & $b|c$ then $a|c$.

Corollary — If a, b, c are integers where $a \neq 0$ such that $a|b$ and $a|c$ then $a|(mb+nc)$ whenever m, n are integers.

The division algorithm

Let a be an integer and d be a +ve integer then there are unique integers q & r with $0 \leq r < d$ such that $a = dq + r$.

$d \Rightarrow$ divisor r = remainder, q = quotient.

Ex:- What are the quotient & remainder when 101 is divided by 10?

→ $101 = (10)(10) + 1$

Remainder = 1 & $q = 10$

In some cases:- What time it will be 50 hours from now?

Here we think about remainder after dividing 50 by 24 hours.

Def' If a & b are integers & m is a +ve integer, $a \equiv b \pmod m$ if $m|(a-b)$

Thm — Let m be a +ve integer. The integers a & b are congruent modulo m iff $\exists\ k$ such that $a = b + km$.

Ex:- $7 \equiv 2 \pmod 5$

Thm — Let m be a +ve integer.
If $a \equiv b \pmod m$ & $c \equiv d \pmod m$ then
$a+c \equiv (b+d) \pmod m$
$ac \equiv bd \pmod m$

Ex — $7 \equiv 2 \pmod 5$ & $11 \equiv 1 \pmod 5$

$\Rightarrow 18 \equiv (2+1) \pmod 5$
$\equiv 3 \pmod 5$
i/y $77 \equiv 2 \pmod 5$

Arithmetic modulo m

We define arithmetic operations on $\mathbb{Z}_m$ i.e, $\{0, 1, \ldots, m-1\}$ set of non-ve integers less than m

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

Ex:- Evaluate $7 +_{11} 9$ & $7 \cdot_{11} 9$

$7 +_{11} 9 = (7+9) \pmod{11}$
$= 16 \pmod{11}$
$= 5.$

$7 \cdot_{11} 9 = (7 \times 9) \pmod{11}$
$= 63 \pmod{11}$
$= 8$

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition & multiplicⁿ of integers.

① closure – If $a, b \in Z_m$ then $a +_m b$ & $a \cdot_m b$ belongs to Z_m

② Associative –

$$(a +_m b) +_m c = a +_m (b +_m c)$$
$$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$$

③ Commutativity:- If $a, b \in Z_m$ $a +_m b = b +_m a$
$a \cdot_m b = b \cdot_m a$

④ Identity element

$$a +_m 0 = 0 +_m a = a$$
$$a \cdot_m 1 = 1 \cdot_m a = a$$

⑤ Additive inverse:-
If $a \neq 0 \in Z_m$ then $(m-a)$ is additive inverse of a
i.e, $a +_m (m-a) = 0$
$0 +_m 0 = 0$

⑥ Distributivity – $a \cdot_m (b +_m c) = (a \cdot_m b) + (a \cdot_m c)$

Note:- Z_m with this modular addition is said to be commutative group & with all operations above called commutative ring.

Primes & g.c.d

Prime – An integer p greater than 1 is called **prime** if the only +ve factors of p are 1 & p.

If a number is not prime it is called **composite**

Ex:– 7 is a prime but 6 is not prime

Thm – Fundamental thm of arithmetic

Every integer > 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of ~~der~~ nondecreasing size.

Ex] $100 = 2 \times 50$

$= 2 \times 5 \times 10$

$= 2 \times 5 \times 5 \times 2$

$= 2^2 5^2$

GCD

Def^n:– Let $a, b \in \mathbb{Z}$ both are nonzerse

The largest integer d such that $d|a$ & $d|b$ is called g.c.d of a & b.

$d = \gcd(a, b)$

Def^n:– relatively prime:– a & b said to be relatively prime if $\gcd(a, b) = 1$

Euclidean Algorithm

Find gcd (91, 287)

divide 287 by 91

$$287 = (91)(3) + 14$$
$$91 = (14)(6) + 7$$
$$14 = 7 \times 2 + 0.$$

$\therefore$ gcd (14, 7) = 7

further gcd (287, 91) = 7

$$\begin{array}{r} 3 \\ 91 \overline{)\,287} \\ -273 \\ \hline 14 \end{array} \qquad \begin{array}{r} 6 \\ 14 \overline{)\,91} \\ 84 \\ \hline 7 \end{array}$$

Lemma – Let $a = bq + r$, a, b, q & r are integers.
then gcd (a, b) = gcd (b, r)

Find gcd of 414 & 662 by Eulidean algo.

→

$$662 = 441(1) + 248$$
$$441 = 248(1) + 166$$
$$248 = 166(1) + 82$$
$$166 = 82(2) + 2$$
$$82 = 2(41)$$

$\therefore$ gcd (414, 662) = 2 ∵ 2 is the last nonzero remainder

Algorithm:–

```
x = a
y = b
While y ≠ 0
    r = x mod y
    x = y
    y = r
return x {gcd (a, b) is x}
```

Bezout's thm — gcd as a linear combination

Thm – If a & b are +ve integers then $\exists$ s & t s.t $\gcd(a,b) = sa+tb$

Ex:- Express $\gcd(252, 198) = 18$ as a linear combination of 252 & 198.

→

$$252 = 198(1) + 54 \quad \text{—— (1)}$$
$$198 = 54(3) + 36 \quad \text{—— (2)}$$
$$54 = 36(1) + 18 \quad \text{—— (3)}$$
$$36 = (2)18$$

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

$$18 = 54 - 36(1)$$
$$= 54 - (198 - (54)(3))(1)$$
$$= 54 \times 1 - 198 \times 1 + 54 \times 3$$
$$= 54 \times 4 - 198 \times 1$$
$$= (252 - 198 \times 1) \times 4 - 198 \times 1$$
$$= 252 \times 4 - 198 \times 4 - 198 \times 1$$
$$= 252 \times 4 - 198 \times 5.$$

$$\therefore \boxed{18 = 4(252) - 5(198)}$$

Lemma If a, b, c are +ve integers s.t $\gcd(a,b) = 1$ & $a \mid bc$ then $a \mid c$

Lemma – If p is a prime & $p \mid a_1 a_2 \cdots a_n$ where each a_i is an integer then $p \mid a_i$ for some i

Use Euclidean algorithm to find

1. 1001, 1331
2. 9888, 6060
3. 111, 201
4. 123, 277.

Express gcd of each pair of integers as a lin comb^{n} of these integers.

1. 33, 44
2. 124, 323
3. 117, 213
4. 3457, 4669.

Lemma — If a, b, c are +ve integers s.t. $\gcd(a, b) = 1$ & $a \mid bc$ then $a \mid c$.

* If p is a prime & $p \mid a_1 a_2 \cdots a_n$ where each a_i is an integer then $p \mid a_i$ for some i

Thm:- Let m be a +ve integer & let a, b, c be integers.

If $ac \equiv bc \pmod{m}$ & $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

Linear congruence — A congruence of the form

$ax \equiv b \pmod{m}$

where m is +ve integer

a & b are integers & x is a variable

is called Linear congruence.

Thm:- If a & m are relatively prime integers & $m > 1$ then an inverse of a modulo m exists.

Furthermore the inverse is unique.

Find all solutions of linear congruence.

$3x \equiv 4 \pmod{7}$

$\rightarrow$

$3 \pmod{7}$ -2 $3x \equiv -2 \times 4 \pmod{7}$

$-6x \equiv -8 \pmod{7}$

Chinese remainder thm. (Sun-Tsu puzzle)

Q^n:- There are certain things whose no is unknown. When divided by 3 remainder is 2
" " 5 " " 3
" " 7 " " 2
What will be such no?

Ex:

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

∴ Chinese remainder thm:-

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime +ve integers greater than one & $a_1, a_2, \ldots, a_n$ any arbitrary integers. Then the system

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
⋮
$x \equiv a_n \pmod{m_n}$ has a unique soln modulo $m = m_1 m_2 \cdots m_n$

Soln is:-

$$x \equiv a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}$$

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

& $M_k M_k^{-1} \equiv 1 \pmod{m_k}$

Soln:- $a_1 = 2,\ a_2 = 3,\ a_3 = 2$

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

$m = 3 \times 5 \times 7 = 105$

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

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

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

$M_k M_k^{-1} \equiv 1 \pmod{m_k}$

$M_1 M_1^{-1} \equiv 1 \pmod{m_1}$

$35 M_1^{-1} \equiv 1 \pmod{3}$

$35 \times 1 = 35 \div 3 = 2 \neq 1$

$35 \times 2 = 70 \div 3 =$ quotient 23 remainder $= 1$

$\therefore \boxed{M_1^{-1} = 2}$

Ily $M_2^{-1} \Rightarrow \quad M_2 M_2^{-1} \equiv 1 \pmod{m_2}$

$21(\_) \equiv 1 \pmod{5}$

$21 \times 1 \div 5 \Rightarrow$ rem $= 1$

$\boxed{M_2^{-1} = 1}$

Ily $M_3^{-1} \Rightarrow \quad 15 \times M_3^{-1} \equiv 1 \pmod{7}$

$\boxed{M_3^{-1} = 1}$

$\therefore$ Soln:- $x \equiv$

$\left(2(35)(2) + 21(3) + 2(15 \times 1)\right) \bmod 105$

$\Rightarrow 140 + 63 + 30$

$\Rightarrow 233 \bmod 105$

$\equiv 23 \pmod{m}$

$105 \overline{)233}\ (2$

210

23

$\boxed{x = 23}$ smallest +ve.