($2\frac{1}{2}$ Hours) [Total Marks :75]

N.B.: (1) All questions are compulsory.

(2) Figures to the right indicate marks for respective sub questions.

Q1 (a) Attempt any one question.

(i) State and prove Wilson's Theorem. Also prove it's converse. Show that n=13 is prime using the converse. (08)

(ii) State and prove Euler's Generalization of Fermat's Theorem. Show that, for any integer n≥ 0,51 divides 10^{32n+9}-7. (08)

(b) Solve any two questions:

(i) Prove that $ax \equiv ay(mod\ m)$ if and only if $x \equiv y\ (mod\ \frac{m}{(a,m)})$. (06)

(ii) Prove that if p and p+2 are pair of twin primes, then 4((p-1)!+1)+p≡ 0 (modp(p+2)). (06)

(iii) If every prime that divides n also divides m, prove that (06)

$\phi(nm) = n\phi(m)$.

(iv) Solve system of simultaneous congruences: (06)

$$x \equiv 5(mod\ 11)\ ,\quad x \equiv 14(mod\ 29)\ ,\quad x \equiv 15(mod\ 31)$$

Q2 (A) Attempt any ONE: (08)

(i) Show that all the solutions of the Pythagorean equation $x^2 + y^2 = z^2$ satisfying the conditions gcd(x, y, z) =1 , 2 | x, x>0, y>0, z>0 are given by the formulae

x=2st , $y=s^2 - t^2$, $z=s^2 + t^2$ for integers s>t>0 such that

[TURN OVER

gcd(s, t)=1 and $s \not\equiv t \pmod 2$.

(ii) Prove that an odd prime p is expressible as a sum of two squares if and only if $p \equiv 1 \pmod 4$. (08)

(B) Solve any TWO of the following.

(i) Determine all solutions of the Diophantine equation $52x+72y=40$. (06)

(ii) If x, y and z is a primitive Pythagorean triple prove that x+y and x-y are congruent modulo 8 either to 1 or 7. (06)

(iii) Show that a positive integer n can be represented as the difference of two squares if and only if n is not of the form 4k+2. (06)

(iv) If n is the sum of two triangular numbers establish that 4n+1 is the sum of two squares. (06)

Q3 (A) Attempt any one question:

(i) If p is an odd prime and gcd(a,2p)=1 , then show that $\left(\frac{a}{p}\right)=(-1)^t$ where $t=\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right]$ and $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$. (08)

(ii) Define Jacobi symbol $\left(\frac{P}{Q}\right)$ for Q odd and positive. (08)

Show that $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$ and $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$

(B) Solve any two of the following.

(i) Prove that if p and q are odd primes and $p = q + 4a$ for some a then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. (06)

(ii) Show that there are infinitely many primes of the form 6k+1. (06)

(iii) Show that $\left(\frac{3}{p}\right) = 1$ if $p \equiv 1$ or 11 (mod 12). (06)

(iv) Find solutions of the quadratic congruence $x^2 \equiv 14 \ (mod\ 5^3)$. (06)

Q4 Solve any THREE:

(i) Employ Fermat's theorem to prove that, if p is an odd prime then (05)

$1^{p-1} + 2^{p-1} + \text{--------} (p-1)^{p-1} \equiv -1 (\text{mod } p)$.

(ii) Establish each of the assertions: (05)

a) $\Phi(3n) = 3\,\Phi(n)$ if and only if 3 divides n

b) $\Phi(3n) = 2\,\Phi(n)$ if and only if 3 does not divide n.

(iii) Show that if $n \equiv 3$ or 6 (mod 9), then n cannot be represented as a sum of two squares. (05)

(iv) A certain number of sixes and nines is added to give a sum of 126; if the number of sixes and nines is interchanged, the new sum is 114. How many of each were there originally? (05)

(v) If the prime $p > 3$, show that p divides the sum of its quadratic residues. (05)

(vi) Prove that the quadratic congruence $6x^2 + 5x + 1 \equiv 0 (\text{mod } p)$ has a solution for every prime p, even though the equation $6x^2 + 5x + 1 = 0$ has no solution in integers. (05)

....