($2\frac{1}{2}$ Hours) REVISED COURSE [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>1 is prime if and only if (n-2)!≡ 1(modn). (08)

(ii) Prove that a linear congruence ax≡ $b(modn)$ has solution if and only if d/b where d=gcd(a,n). If d/b then prove that it has d mutually incongruent solutions modulo n. Find solutions of 24x≡ 15 (mod21). (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 is an odd prime, $1^p + 2^p + 3^p + \ldots\ldots\ldots + (p-1)^p \equiv 0$(mod p). Also prove that if p and q are distinct primes then (06)

$p^{\ q-1} + q^{p-1} \equiv 1$(mod pq)

(iii) Define function φ(n).Prove that for n≥ 1,$\sum_{d/n} \varphi(d)$=n. (06)

(iv) Solve the system linear congruences (06)
x ≡ 2(mod5), x≡ $3(mod7)\ and\ x \equiv 4(mod9)$.

Q2 (a) Attempt any **ONE** question: (08)

(i) Show that the equation $x^4 + y^4 = z^4$ has no solution in positive integers.

(ii) Show that a positive integer n is representable as the sum of two squares if and only if each of its prime factors of the form 4k+3 occurs to an even power. (08)

(b) Solve any **TWO** of the following.

(i) Determine all solutions in positive integers of the Diophantine equation 5x+3y=52. (06)

(ii) Show that the equation $x^2 + y^2 = 9z + 3$ has no integral solution. (06)

(iii) Show that the area of a Pythagorean triangle can never be equal to a perfect (integral) square. (06)

(iv) Let p be an odd prime. If p|$a^2 + b^2$, where gcd(a, b) =1, prove that the prime $p \equiv 1\ (mod\ 4)$. (06)

Q3 (a) Attempt any **ONE** question:

(i) Explain RSA cryptosystem. Also write RSA algorithm. (08)

(ii) Define the term primitive root of integer n .Prove that if n has primitive root then it has exactly $\varphi(\varphi(n))$ primitive roots. Hence find number of primitive roots of n=31. (08)

(b) Solve any **TWO** of the following.

(i) Prove that if the integer a has order k modulo n and h>0, then a^h has order $k/\gcd(h,k)$ modulo n. (06)

(ii) Explain Hill's cipher with blocks of two letters. Encipher message WAKEUP using matrix $\begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix}$(mod26). (06)

(iii) Encipher message RETURN HOME using Vigenere's cipher with seed Q. Also decipher BS FMX KFSGR obtained by applying keyword YES. (06)

(iv) If affine transformation f(x)=ax+b(mod 26) enciphers GI to WC , find a, b. Also find deciphering transformation and use it to decipher MX. (06)

Q4 Solve any **THREE:**

(i) Use Kraitchik's method to factor the number 20437. Explain the method. (05)

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

a) If n is an odd integer , then $\varphi(2n) = \varphi(n)$.

b) If n is an even integer , then $\varphi(2n) = 2\varphi(n)$

(iii) Prove that $\boldsymbol{ax + by = a + c}$ is solvable if and only if $\boldsymbol{ax + by = c}$ is solvable. (05)

(iv) Show that the representation of a given prime p as the difference of two squares is unique. Does this result hold for any arbitrary positive integer that is neither prime nor of the form 4k+2? (05)

(v) Given that a has order 3 modulo p, where p is an odd prime , show that a+1 must have order 6 modulo p.

(vi) Decrypt the message **fwmdiq.** Suppose the message is encrypted by Hill cipher with the encrypting matrix K=$\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$ (05)
