Q.P.Code:. 016022

(3 hours) **Total Marks: 100**

N.B: (1) All questions are compulsory
(2) Attempt any two sub-questions from part (a), part (b) and part(c)
(3) Figures to the right indicate marks for respective sub-questions.

Q1.a) i) Determine all solutions in integers of the Diophantine equation:56x+72y=40 (5)

ii) Assuming that p_n is the n[th] prime number, establish that , none of the integers $P_n = p_1p_2p_3 \ldots \ldots . p_n + 1$ is a perfect square. (5)

b) i) Prove that if the irrational $x > 1$ is represented by the infinite continued fraction $[a_{0;}\ a_1\ ,a_2, \ldots\ldots]$ then $\frac{1}{x}$ has the expansion $[0;\ a_{0;}\ a_1\ ,a_2, \ldots\ldots]$ (5)

ii) Show that there are infinitely many primes of the form 4k+1. (5)

c) i) Encipher message GOODLUCK by using Caesar cipher . (5)

ii) Find all solutions of $x^2 \equiv 23(mod\ 7^2)$ (5)

Q2.a) Prove that the linear Diophantine equation ax+by=c has a solution if and only if d|c, where d = gcd(a.b). Also , if $x_0\ ,y_0$ is any particular solution of this equation, then all other solutions are given by x=x_0 + $\left(\frac{b}{d}\right)$t , y = y_0 -$\left(\frac{a}{d}\right)$t , where t is an arbitrary integer. (10)

b) i) State and Euler's generalization of Fermat's theorem. (6)

ii) Confirm that for any integer n ≥ 0, $51 | 10^{32n+9} - 7$ (4)

c) i) Prove that the quadratic congruence x^2+1 ≡ 0 (mod p) , where p is an odd prime, has a solution if and only if p≡ 1 (mod 4) (6)

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

Q3.a) For an odd prime p , define the Legendre symbol $\left(\frac{a}{p}\right)$ where a ε ℤ .State the quadratic reciprocity law. Hence show that (10)

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & if\ p\ or\ q\ \equiv 1(mod\ 4) \\ -\left(\frac{q}{p}\right) & if\ p\ and\ q \equiv 3(mod\ 4) \end{cases}$$

b) i) Define Jacobi symbol $\left(\frac{P}{Q}\right)$ where Q is odd and positive. Show that $\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}\left(\frac{Q}{P}\right)$ (6)

TURNOVER

	ii)	Evaluate $\tau(n)$ *and* $\sigma(n)$ for n=720, where τ *and* σ are arithmetic functions.	(4)
c)	i)	Define *Möbius* function μ. Prove that μ is multiplicative function. Also prove that , if n is a positive integer, $\sum_{d\mid n}\mu(d)=\begin{cases}1 \text{ if } n=1\\ 0 \text{ if } n>1\end{cases}$	(6)
	ii)	Show that the Fermat number F_5 is divisible by 641.	(4)
Q4.a)		Prove that every simple infinite continued fraction represents an irrational number and conversely every irrational number represents an infinite continued fraction. Represent $\sqrt{2}$ as a simple infinite continued fraction.	(10)
b)	i)	If $C_k=\frac{p_k}{q_k}$ is the k^{th} convergent of the finite simple continued fraction $[a_0; a_1, a_2, \_,\_,\_, a_n]$; then show that the convergents with even subscripts form a strictly increasing sequence.	(6)
	ii)	For any positive integer n , Show that $\sqrt{(n^2+1)}$ = [n; $\overline{2n}$]	(4)
c)	i)	Find the fundamental solution of x^2-41y^2=1	(6)
	ii)	If d is divisible by a prime $p \equiv 3(mod\ 4)$, show that the equation of x^2-dy^2= -1 has no solution.	(4)
Q5.a)		Define Carmichael number. Show that n is Carmichael number if and only if it is odd and for every prime p dividing n, p-1|n-1.	(10)
b)	i)	Explain Hill cipher with block of two letters stating enciphering and deciphering function.	(6)
	ii)	Use affine transformation f(x) =2x+1(mod 26) to encipher message "MATHS"	(4)
c)	i)	If n is pseudoprime to bases b_1 *and* b_2, then prove that n is pseudoprime to bases $b_1\, b_2$ and $b_1 b_2^{-1}$.	(6)
	ii)	If $n=2^{2^k}+1$ is composite then show that n is pseudoprime to base 2 where k > 0.	(4)
