[This question paper contains 4 printed pages.]

2144 *Your Roll No.* ....

B.Sc. (Hons.) / III **C**

MATHEMATICS – Paper XII (*iv*)

(Number Theory and Cryptography)

(Admissions of 2009 and onwards)

Time : 3 Hours *Maximum Marks : 75*

(Write your Roll No. on the top immediately on receipt of this question paper.)

Attempt any **two** *parts from each question.* **All** *questions are compulsory.*

1\. (a) A customer bought a dozen pieces of fruit, apples and oranges, for Rs. 132/- . If an apple costs 3 rupees more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought ? (5)

(b) Prove that the linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$ where $d = gcd(a, n)$. Also show that if $d \mid b$, then it has d mutually incongruent solutions modulo n. (5)

(c) What is the remainder when the following sum is divided by 4 ?

$1^5 + 2^5 + 3^5 + \ldots\ldots + 99^5 + 100^5$ (5)

2. (a) Verify that 0, 1, 2, 2^2, 2^3, 2^4, ... 2^9 form a complete set of residues modulo 11 but that 0, 1^2, 2^2, 3^2, ..., 10^2 do not. (6½)

(b) State and prove Wilson theorem and also comment on converse of it. (6½)

(c) (i) Using Wilson's theorem, prove that for any odd prime p,

$$1^2.3^2.5^2.7^2 \ldots\ldots (p-2)^2 \equiv (-1)^{(p-1)/2} \pmod{p}.$$

(4)

(ii) Find the remainder when 15! is divided by 17. (2½)

3. (a) Define Möbius function and prove that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 : & if\ n = 1 \\ 0 : & if\ n > 1 \end{cases}$$ (1+5½)

(b) (i) If m and n are relatively prime positive integers, prove that

$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

(ii) Show that if gcd (a, n) = gcd $(a-1, n) = 1$, then

$$1 + a + a^2 + \ldots + a^{\phi(n) - 1} \equiv 0 \pmod{n}.$$

(3½+3)

(c) If the integer a has order k modulo n and h > 0, then prove that a^h has order $k/\gcd(h, k)$ modulo n. Further prove that if r is a primitive root of an integer n and gcd $(k, \phi(n)) = 1$, then r^k is also a primitive root of n. (5+1½)

4. (a) If $\gcd(m, n) = 1$, where $m > 2$ and $n > 2$, then prove that the integer mn has no primitive roots. (6½)

(b) If p is an odd prime, then prove that

$$\sum_{a=1}^{p-1} (a/p) = 0$$ (6½)

(c) Show that 7 and 18 are the only incongruent solutions of $x^2 \equiv -1 \pmod{5^2}$. (6½)

5. (a) The ciphertext ALXWU VADCOJO has been enciphered with the cipher

$$C_1 \equiv 4P_1 + 11P_2 \pmod{26}$$
$$C_2 \equiv 3P_1 + 8P_2 \pmod{26}$$

derive the plaintext. (6½)

(b) (i) A user of knapsack cryptosystem has the sequence 49, 32, 30, 43 as a listed encryption key. If the user's private key involves the modulus $m = 50$ and multiplier $a = 33$, determine the secret superincreasing sequence. (3)

(ii) Find the unique solution of the following superincreasing knapsack problem :

$51 = 3x_1 + 5x_2 + 9x_3 + 18x_4 + 37x_5$ (3½)

(c) If u_n is the n^{th} Fibonacci number then prove the following

(i) $\mu_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$; $n \geq 1$. where $\alpha = \left(\dfrac{1+\sqrt{5}}{2}\right)$ and $\beta = \left(\dfrac{1-\sqrt{5}}{2}\right)$. (3)

(ii) $\mu_{2n+1}\mu_{2n-1} - 1 = \mu_{2n}^2$ (3½)

6. (a) Prove that for $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$ (6½)

(b) Prove that in a primitive Pythagorean triple x, y, z, the product xy is divisible by 12, hence $60 \mid xyz$. (6½)

(c) (i) Prove that every integer $n \geq 170$ is a sum of five squares, none of which are equal to zero. (3½)

(ii) Prove that a positive integer n can be represented as the difference of two squares if and only if n is not of the form $4k + 2$. (3)