This question paper contains 4 printed pages]

Your Roll No................

9666

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

MATHEMATICS—Paper XVII & XVIII (*i*)

(Number Theory)

Time : 2 Hours *Maximum Marks : 38*

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

Attempt any *two* parts from each question.

Marks are indicated against each question.

1. (*a*) Show that the linear congruence $ax \equiv b$ (mod, n) has a solution if and only if $d | b$ where d = g.c.d. (a, n). Further, show that if $d | b$ then it has d mutually incongruent solutions modulo n. 4

(*b*) Define a complete residue system modulo n. Show that if the set $\{a_1, a_2 \ldots\ldots\ldots\ldots a_n\}$ is a complete residue system modulo n and g.c.d.$(a, n) = 1$, then the set $\{aa_1, aa_2, \ldots\ldots\ldots\ldots aa_n\}$ is also a complete residue system modulo n. 4

(c) Find the least positive integer x such that : 4

$$2^2|x \quad 3^2|x+1 \text{ and } 5^2|x+2.$$

2. (a) Show that the quadratic congruence $x^2 + 1 \equiv 0 \pmod p$ where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod 4$. 5

(b) Show that for positive integers m and n : 5

$$\phi(m)\,\phi(n) = \phi(mn)\,\frac{\phi(d)}{d}$$

where d = g.c.d. (m, n).

Hence deduce that ϕ is multiplicative.

(c) In the language of Cryptography explain the terms : 5

(i) Plain text

(ii) Cipher text.

Decrypt the message WCPQ JZQO MX which was produced using the linear cipher :

$$C \equiv 3P + 4 \pmod{26}$$

where P is the digital equivalent of plain text better and C is the digital equivalent of the corresponding cipher text.

3. (a) Show that $\phi(n)$ is an even integer for $n > 2$ and hence prove that if g.c.d.$(m, n) = 1$ for integers m and n with $m > 2$, $n > 2$, then mn has no primitive roots. 5

(b) State Gauss lemma and show that if p is an odd prime, then : 5

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

(c) Solve the quadratic congruence : 5

$$x^2 \equiv 23 \pmod{7^3}.$$

4. (a) Define a perfect number and show that an even perfect number n ends in the digits 6 or 8. 5

(b) Show that if x, y, z is a primitive Pythagorean triple, then exactly one of x or y is even and the other is odd and 3 divides exactly one of x or y. Hence deduce that $12|xy$. 5

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

(ii) Prove that any positive multiple of 8 is sum of eight odd squares. 3+2