Ex./FM/5.5B/39/2019

BACHELOR OF SCIENCE EXAMINATION, 2019

(3rd Year, 1st Semester)

MATHEMATICS (Honours)

Paper - 5.5B

Number Theory

Time : Two hours Full Marks : 50

Symbols have usual meanings, if not mentioned otherwise.
Answer ***Q. No. 1*** and any ***four*** from the rest.

1. (a) Prove that (a,b) = (b,a) = (a, –b) = (a ,b + ax) where x is an arbitrary integer.

 (b) Prove that $42|n^7 - n$ for any integer n.

 (c) Reduce the congruence $x^{15} - x^{10} + 4x - 3 \equiv 0 \bmod 7$ to an equivalent congruence having degree without exceeding 6. 4+3+3=10

2. (a) Given integers a, b, and m > 0, prove that the congruence $ax \equiv b \bmod m$ has a solution if and only if g|b where g = (a , m). If this condition is met, then the solutions form an arithmetic progression with common difference form an arithmetic progression with common difference m/g, giving g solutions.

(Turn over)

(b) Find the values of x for which both $x \equiv 29 \bmod 52$ and $x \equiv 19 \bmod 72$ simultaneously hold. Justify your answer. 6+4=10

3. State Hensel's lemma. Using this lemma, solve the congruence $x^2 + 5x + 24 \equiv 0 \bmod 36$. 2+8=10

4. (a) Given a polynomial f(x) with integer coefficients and a prime number p, prove that the congruence $f(x) \equiv 0 \bmod p$ has at most n solutions, where n is the degree of the congruence.

(b) If $d|(p-1)$ for a prime number p, then prove that $x^d \equiv 1 \bmod p$ has exactly d solutions. 6+4=10

5. Let $m = 1, 2, 4, p^\alpha, \text{or} 2p^\alpha$ where p is an odd prime. If (a,m) = 1 then prove that the congruence $x^n \equiv a \bmod m$ has $(n, \phi(m))$ solutions or no solution according as

$$\alpha^{\phi(m)/(n,\phi(m))} \equiv 1 \bmod m$$

or not. Hence determine the number of solutions of the congruence $x^4 \equiv 61 \bmod 117$. 5+5=10

6. (a) Given $(a, p) = 1$ for an arbitrary odd prime p, consider a, 2a, 3a, ..., $\{(p-1)/2\}a$ and their least positive residues modulo p. If n denotes the number of these residues which exceed p/2, then prove that

$$\left(\frac{a}{q}\right) = (-1)^n$$

(b) Show that 3 is a quadratic residue of 13, but a quadratic nonresidue of 7. 6+4=10

7. If P and Q are odd and positive such that (P,Q) = 1, then prove that

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\{(P-1)/2\}\{(Q-1)/2\}}$$

Decide whether the congruence $x^4 \equiv 25 \bmod 1013$ is solvable, given 1013 is prime. 5+5=10

—— X ——