Bachelor of Science Examination, 2017

(3rd Year, 1st Semester)

MATHEMATICS (Honours)

Unit - 5.5 (b)

[Number Theory]

Full Marks : 50 Time : Two Hours

The figures in the margin indicate full marks.

Answer Question No. 1 and any *four* from the rest.

1. Answer any *ten* : 1×10

(a) What is the remainder on division of 2^{1000} by 13 ?

(b) Using unique factorisation of positive integers into primes prove that $\log_6 9$ is irrational.

(c) Determine the smallest positive integer having only 10 positive divisors.

(d) Determine the possible gcd's of a and $a + 10$ for any positive integer a.

[*Turn over*]

(e) Determine the integers n such that the congruence $x^2 \equiv n \pmod 3$ has solution.

(f) The congruence $x^3 + x^2 + 1 \equiv 0 \pmod{90}$ has no solution — Justify.

(g) $x^2 + y^2 = 43$ cannot have any integral solution — Explain.

(h) Suppose $m > 2$ is any integer. Then $1^2, 2^2, \ldots, m^2$ cannot be a complete residue system modulo m — Explain.

(i) Find the number of positive integers $x(<13)$ such that $x^{12} = 1$ but $x^m \neq 1$ for any $1 < m < 12$.

(j) That the congruences $x^2 \equiv -2 \pmod{71}$ and $x^2 \equiv -2 \pmod{79}$ have no solution — can be explained by a single argument — Explain.

(k) 242 cannot divide $|\underline{241} + 1$ — Explain.

2. (a) Suppose p is a prime. Prove that $x^2 \equiv -1 \pmod p$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

(b) Find the least positive integer x such that $2x \equiv 3 \pmod{7}$, $5x \equiv 2 \pmod{11}$, $6x \equiv 5 \pmod{13}$.

(c) Show that $n^2 + 1$ is not divisible by 23 for any integer n. 4+5+1=10

3. (a) (i) Define Euler's phi function.

(ii) Suppose n is a positive integer. Prove that the set $\{a : a \text{ is a solution of } \varphi(x) = n\}$ has a lower bound as well as an upper bound.

Hence conclude that $\varphi(x) = n$ has atmost a finite number of solutions.

(b) Prove that $\varphi(x) = 14$ has no solution. (1+6)+3=10

4. (a) (i) Define Mersenne number M_x for any prime number x.

(ii) Suppose n is a positive integer such that $p = 4n + 3$, $q = 8n + 7$ are primes. Prove that q divides the Mersenne number M_p. Hence provide two composite Mersenne numbers.

(b) State the Gaussian quadratic reciprocity law. What does it say about the solvability of the congruences $x^2 \equiv p(\mathrm{mod}\, q)$, $x^2 \equiv q(\mathrm{mod}\, p)$ for distinct odd primes p and q ? (1+6)+(1+2)=10

5. (a) (i) Define Legendre symbol $\left(\frac{a}{p}\right)$.

(ii) Prove that for an odd prime p,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p) \text{ and } \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

(b) Suppose a is a primitive root of an odd prime p. Show that

(i) any even power of a is a quadratic residue modulo p,

(ii) any odd power of a is quadratic nonresidue modulo p. (2+4)+(2+2)=10

6. (a) Suppose p is a prime and n is a positive integer such that $p > n$. Use Wilson's theorem to prove that $(n-1)!(p-n)! \equiv (-1)^n (\mathrm{mod}\, p)$.

[*Turn over*]

(b) Solve $x^3 - 2x + 6 \equiv 0 \pmod{125}$.

(c) Reduce the congruence $x^{15} - x^{10} + 4x - 3 \equiv 0 \pmod{7}$ to a congruence of degree ≤ 6. 4+4+2=10

7\. (a) Find all primes p such that $x^2 \equiv 13 \pmod{p}$ has a solution.

(b) Find a system of congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

with $(m_i,\ m_j) = 1$ for all $i \neq j$ $(1 \leq i,\ j \leq 3)$ such that it is equivalent to the following system of congruences.

$$x \equiv -2 \pmod{12}$$

$$x \equiv 6 \pmod{10}$$

$$x \equiv 1 \pmod{15}$$

7+3=10
