Answer as many questions as you wish. Full marks may be obtained by complete answers to **NINE** *questions, provided that no more than* **SIX** *questions have been selected from any one part. All questions carry equal marks.*

95

PART I NUMBER THEORY

Question 1

(i) Prove by induction that the formula

$$1 + 3 + 6 + 10 + \cdots + \frac{1}{2}n(n+1) = \frac{1}{6}n(n+1)(n+2)$$

holds for all integers $n \geq 1$. [4]

(ii) Use the Euclidean Algorithm to find the greatest common divisor of 157 and 117. Hence find integers x and y such that

$$\gcd(157, 117) = 157x + 117y.$$ [4]

(iii) Suppose that m and n are positive integers such that n has remainder 7 when divided by 8, and $m = 9n + 4$. Prove that $\gcd(m, n) = 1$. [3]

Question 2

(i) Prove that there are infinitely many primes of the form $4k + 3$. [7]

(ii) Prove that for any prime p it is not possible for both $8p - 1$ and $8p + 1$ to be prime. [4]

Question 3

(i) For each of the following statements decide whether or not it is generally true. If you believe it to be true, prove it; otherwise give a counter-example. Throughout a, b, k and n are positive integers.

(a) If $a \equiv b \pmod{n}$ then $k(a+1) \equiv k(b+1) \pmod{n}$;

(b) if $ka \equiv kb \pmod{n}$ then $a \equiv b \pmod{n}$;

(c) if $a^2 \equiv b^2 \pmod{n}$ then either $a \equiv b \pmod{n}$ or $a \equiv -b \pmod{n}$. [6]

(ii) Find the least positive integer x which simultaneously satisfies all three of the following linear congruences:

$$x \equiv 1 \pmod{5}; \quad 3x \equiv 2 \pmod{7}; \quad 6x \equiv 2 \pmod{11}.$$ [5]

Question 4

(i) Use Fermat's Little Theorem in showing the following.

(a) $3^{50} + 5^{50}$ is divisible by 17.

(b) If p is an odd prime then each of the numbers $(p-1)2^{p-1} + 1$ and $(p-2)2^{p-2} + 1$ is divisible by p. [7]

(ii) Use Wilson's Theorem in showing that 13 is the smallest prime which divides $11! - 1$. [4]

Question 5

The respective parts of this question are concerned with Euler's phi-function, ϕ, and the sum of the positive divisors function, σ. You may assume that each of these functions is multiplicative.

(i) Prove the formula

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$ [5]

(ii) A positive integer n has the property that $n + 3\sigma(n)$ is divisible by 4. Prove that:

(a) if $n = p^2$ (for some prime p) then $p \equiv 3 \pmod{4}$;

(b) if $n = p^2 q$ (for distinct primes p and q) then $p = 2$. [6]

Question 6

(i) Determine whether or not the quadratic congruence

$$2x^2 + 7x + 1 \equiv 0 \pmod{17}$$

has solutions. [4]

(ii) Evaluate the Legendre symbol $(-47/73)$. [3]

(iii) Use Gauss's Lemma to show that 2 is a quadratic residue of any prime of the form $8k + 7$. [4]

Question 7

(i) The number x has continued fraction

$$x = [1; 1, 2, 2, 3, 3, 4, 4, \ldots].$$

Write down the convergents C_0, C_1, C_2, C_3, C_4, C_5 and C_6 of x. Estimate the accuracy of C_5 by obtaining an upper bound for $|x - C_5|$. [5]

(ii) Determine the irrational number which has periodic continued fraction $[0; 3, \overline{1, 2}]$. [6]

Question 8

(i) Given that the continued fraction of $\sqrt{7}$ is $[2; \overline{1, 1, 1, 4}]$, determine two solutions of Pell's equation

$$x^2 - 7y^2 = 1.$$ [4]

(ii) Of the numbers 240, 245 and 270, one can be written as a sum of two squares whilst the other two cannot. Identify which two cannot be written as the sum of two squares, justifying your answer, and express the third as a sum of two squares. [4]

(iii) Use the method of infinite descent to show that the equation

$$x^2 = 2y^2$$

has no solutions in positive integers. [3]