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.*

PART I NUMBER THEORY

Question 1

(i) Use the Euclidean Algorithm to determine the greatest common divisor of 87 and 126, and hence find positive integers x and y such that

$$\gcd(87, 126) = 87x - 126y. \qquad [4]$$

(ii) Use Mathematical Induction to prove that the formula

$$1 + 5 + 12 + 22 + \cdots + \tfrac{1}{2}n(3n-1) = \tfrac{1}{2}n^2(n+1)$$

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

8

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

Question 2

(i) If integers $p_1, p_2, \ldots, p_r$ are all of the form $3k+2$, where k is an integer, prove that $(p_1 p_2 \ldots p_r)^2$ is of the form $3k+1$. [3]

(ii) Prove that any positive number of the form $3k+2$ must have a prime divisor of this same form. [3]

11

(iii) Prove that there are infinitely many primes of the form $3k+2$ by the following method. Suppose that $p_1, p_2, \ldots, p_r$ are all the primes of the form $3k+2$. Construct from this list of primes a number of the form $3k+2$ which is not divisible by any prime in this list and explain why this proves the assertion. [5]

Question 3

(i) Suppose that $n \equiv 4 \pmod 6$. Find the least positive residue of $12n + 5$

(a) modulo 8;

(b) modulo 9. [2]

(ii) Let p be an odd prime and a be such that $\gcd(a, p) = 1$. Prove that

$$2,\ 2+a,\ 2+2a,\ 2+3a, \ldots,\ 2+(p-1)a$$

forms a complete set of residues modulo p. [3]

(iii) Find the least positive integer which satisfies each of the following linear congruences simultaneously:

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