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 Mathematical Induction to prove that

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$$

is true for all positive integers n. [4]

(ii) Use the Euclidean Algorithm to determine the greatest common divisor of 323 and 532 and hence find integers x and y such that

$$\gcd(323, 532) = 323x - 532y.$$ [3]

(iii) Prove that, for all integers n,

$$\gcd(2n^2 + 2n + 1, 2n + 1) = 1.$$ [4]

Question 2

(i) Assuming Euclid's Lemma, i.e. if a divides bc, with $\gcd(a, b) = 1$, then a divides c, prove that if p divides the product $a_1 a_2 \ldots a_n$, where p is prime and $a_1, a_2, \ldots, a_n$ are integers, then p divides a_k for some $1 \leq k \leq n$. [5]

(ii) Prove that every positive integer of the form $3n + 2$ has a prime divisor of this same form. [3]

(iii) Prove that $p = 5$ is the only prime for which $3p + 1$ is a square. [3]

Question 3

(i) From the definition of congruence alone, prove the following, for integers a, b, c, d, k and n with $n > 1$.

(a) If $a \equiv b \pmod{n}$ then $ka + c \equiv kb + c \pmod{n}$.

(b) If $ka \equiv b \pmod{n}$ and $kc \equiv d \pmod{n}$ then $ad \equiv bc \pmod{n}$. [4]

(ii) Find the least positive integer which satisfies the following system of simultaneous linear congruences.

$$5x \equiv 1 \pmod{13}; \quad 7x \equiv 10 \pmod{11}; \quad 31x \equiv 6 \pmod{7}.$$ [7]

Question 4

(i) Prove Wilson's Theorem: If p is prime then $(p-1)! \equiv -1 \pmod{p}$. [6]

(ii) Deduce from Wilson's Theorem that, for any odd prime p,

$$2(p-3)! + 1 \equiv 0 \pmod{p}.$$ [2]

(iii) Determine the remainder when 41^{41} is divided by 17. [3]