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 option. All questions carry equal marks.

PART I NUMBER THEORY (M381, M382, M383)

Question 1

(i) Use the Euclidean Algorithm to find the greatest common divisor of 138 and 210. Hence find integers x and y such that

$$\gcd(138, 210) = 138x + 210y.$$ [4]

(ii) The Fibonacci sequence is defined by

$$u_1 = u_2 = 1,$$
$$u_{n+2} = u_{n+1} + u_n, \quad \text{for all } n \geq 1.$$

Prove, by induction, that

$$u_{n-1}u_{n+1} - u_n^2 = (-1)^n, \quad \text{for all } n \geq 2.$$ [4]

(iii) m and n are positive integers such that n has remainder 4 on division by 9 and $m = 5n + 3$. Prove that $\gcd(m, n) = 1$. [3]

Question 2

(i) Prove by any method that there are infinitely many primes. [3]

(ii) Let n be a positive integer which is congruent to 3 (modulo 4). Prove that n must have a prime divisor which is also congruent to 3 (modulo 4). [4]

(iii) If m and n are integers such that $\gcd(m, 3) = 1$ and $\gcd(n, 3) = 1$, prove that $m^2 + n^2$ cannot be a perfect square. [4]

Question 3

(i) From the definition of congruence alone, prove that if $ka \equiv b \pmod{n}$ and $kc \equiv d \pmod{n}$ then $ad \equiv bc \pmod{n}$. [3]

(ii) Solve the linear congruence $13x \equiv 17 \pmod{49}$. [3]

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

$$x \equiv 1 \pmod{3}; \quad 3x \equiv 4 \pmod{7}; \quad 3x \equiv 5 \pmod{11}.$$ [5]

Question 4

(i) Determine the least positive remainder when 7^{30} is divided by 145. [6]

(ii) Suppose that $p = 4n + 1$ is prime. Use Wilson's Theorem to prove that $[(2n)!]^2 \equiv -1 \pmod{p}$. [5]

Question 5

(i) (a) Prove the formula

$$\tau(p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}) = (k_1+1)(k_2+1)\ldots(k_r+1).$$

[You may assume that the τ-function is multiplicative.] [4]

(b) Find the least positive integer n for which $\tau(n) = 18$. [3]

(ii) Supose that p is a prime. Prove that $n = 2^{p-1}(2^p - 1)$ is perfect if and only if $2^p - 1$ is prime. [4]