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

96

Question 1

(i) Prove by induction that the formula

$$1 + 6 + 15 + \cdots + n(2n-1) = \tfrac{1}{6}n(n+1)(4n-1)$$

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

(ii) Use the Euclidean Algorithm to determine the greatest common divisor of 238 and 140. [2]

(iii) For which integer values of c does the linear Diophantine equation

$$51x - 36y = c.$$

have solutions? Find the general solution of this equation, by any method, for the case when c takes the least positive value for which solutions exist. [5]

Question 2

(i) Prove that there are infinitely many primes of the form $4k + 3$. [5]

(ii) Consider the sequence of integers

$$5,\ 8,\ 13,\ 20,\ 29,\ \ldots,$$

whose nth term $a_n = n^2 - 4$. Consecutive terms of this sequence are either relatively prime or are both divisible by a certain prime p. Determine this prime p and prove that, for all $n \geq 1$, $\gcd(a_n, a_{n+1}) = 1$ or p. [6]

Question 3

(i) Suppose that a and b are integers, d and m are positive integers and that d is a divisor of m. For each of the following, decide whether it is true or false. If true, prove it from the definition of congruence alone; if false, give a counterexample.

(a) If $a \equiv b \pmod{d}$ then $a \equiv b \pmod{m}$.

(b) If, for some integer k, $ka \equiv kb \pmod{m}$ then $a \equiv b \pmod{m}$.

(c) If $da \equiv db \pmod{m}$ then $a \equiv b \left(\mathrm{mod}\ \frac{m}{d}\right)$.

(d) If $a \equiv db \pmod{m}$ then $a \equiv 0 \pmod{d}$. [6]

(ii) Find the least positive integer which satisfies each of the following linear congruences simultaneously.

$$x \equiv 0 \pmod{3}; \quad x \equiv 4 \pmod{5}; \quad x \equiv 8 \pmod{11}.$$ [5]

Question 4

N.B. **RESIT STUDENTS** should **NOT** attempt this question. An alternative question (Question 4R) is provided overleaf.

(i) Prove Fermat's Little Theorem (FLT): If p is a prime and a is any integer with $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. [6]

(ii) You are given that the recurring decimal of $\frac{1}{17}$ is

$$\frac{1}{17} = 0.(0588235294117647).$$

Answer the following, in each case giving brief justification of your answer.

(a) What is the order of 10 modulo 17?

(b) What is the value of 10^8 modulo 17?

(c) Write down the recurring decimal of $\frac{13}{17}$. [5]

Question 5

A positive integer n has the property that $2n + \sigma(n)$ is divisible by 3, where σ denotes the 'sum of the divisors' function. In what follows, p and q are distinct odd primes and r is a positive integer.

(i) Prove that n cannot be prime. [2]

(ii) Prove that if $n = p^2$, then $p \equiv 5 \pmod{6}$. [3]

(ii) Prove that if $n = 2p^r$, then $p = 3$. [3]

(iv) If $n = pq$, what can be deduced about p and q? [3]

Question 6

(i) Determine whether or not the quadratic congruence

$$x^2 + 7x + 5 \equiv 0 \pmod{43}$$

has solutions. [4]

(ii) Evaluate the Legendre symbol $(86/103)$. [Note that 103 is prime] [3]

(iii) Use Gauss' Lemma to show that 2 is quadratic non-residue of any prime p where $p \equiv 5 \pmod{8}$. [4]

Question 7

N.B. **RESIT STUDENTS** should **NOT** attempt this question. An alternative question (Question 7R) is provided overleaf.

(i) Determine the two simple finite continued fractions for $\frac{35}{13}$. [2]

(ii) Let $C_k = \frac{p_k}{q_k}$ be the kth convergent of an irrational number. Prove, using mathematical induction or otherwise, that for all $k \geq 2$,

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^k.$$ [3]

(iii) Determine the irrational number α whose continued fraction is $[1, (2, 3)]$. Write down the convergents C_1, C_2, C_3, C_4, C_5 and C_6 of this number and indicate (with brief justification) which is the first convergent accurate to within 0.002 of α. [6]

Question 8

(i) Determine the continued fraction of $\sqrt{12}$ and hence find two positive solutions of the Diophantine equation

$$x^2 - 12y^2 = 1.$$ [6]

(ii) For each of the numbers 560, 570 and 580 decide whether or not it can be expressed as a sum of two squares. For any which you claim cannot be so expressed, justify your answer. For any which can be so expressed, find two different expressions as a sum of two positive squares. [5]

The following two questions are for RESIT STUDENTS ONLY

Question 4R

(i) Prove Fermat's Little Theorem (FLT) If p is a prime and a is any integer with $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. [6]

(ii) Use Wilson's Theorem to:

(a) find the smallest prime divisor of $28! + 1$;

(b) prove that $n! + 1$ is composite for infinitely many values of n. [5]

Question 7R

(i) Determine the continued fraction of $2 + \sqrt{12}$. Write down the convergents C_0, C_1, C_2, C_3 and C_4 and estimate the accuracy $|C_3 - (2 + \sqrt{12})|$ of C_3. [6]

(ii) Determine the irrational number which has periodic continued fraction $[3; 1, \overline{1, 2}]$. [5]