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

$$\frac{1}{17} = 0.\langle 0588235294117647 \rangle.$$

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]

(iii) 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 $[1, \langle 2, 3 \rangle]$. 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]