1. Let α, β, k, m be integers, and let n be a positive integer.

(i) Show that $(\alpha, \beta) = (\alpha + k\beta, \beta) = (\alpha, \beta + k\alpha)$.

(ii) Find $(m^2 - 3, m^3 - 2m + 2)$. Find $(n! + 2, (n+1)! + n + 2)$.

(iii) Solve the following simultaneous congruences for x.

$$4x \equiv 6 \pmod{10}, \quad 2x \equiv 13 \pmod{17}.$$

(iv) Solve the following simultaneous congruences for x.

$$x \equiv 2 \pmod{m^2 - 3}, \quad x \equiv 4 \pmod{m^3 - 2m + 2}.$$

(v) Solve the following simultaneous congruences for x.

$$(n! + 2)x \equiv 3 \pmod{(n+1)! + n + 2}, \quad 2x \equiv 5 \pmod{n+1}.$$

2. (i) Define Euler's ϕ function. Prove Euler's Theorem, that if $(b, n) = 1$ then $b^{\phi(n)} \equiv 1 \pmod{n}$. Use it to show that $51 | (2 \times 5^{130} + 1)$.

(ii) Write down a general formula for $\phi(n)$. Show that if p is prime and $p|n$ then $(p-1)|\phi(n)$. Make a table of $\phi(p^a)$ for small primes p and integers $a \geq 1$, in order to find all values of n for which $\phi(n) = 16$. Show that there is no n for which $\phi(n) = 26$.

(iii) If $\phi(n)$ is divisible by 2 but not by 4, show that $n = 4$ or p^a or $2p^a$ for some prime $p \equiv 3 \pmod 4$ and some positive integer a. Show that there is no n for which $\phi(n) = 2 \times 5^{130}$.

3. (i) Define the term *Carmichael number.* Let $n = q_1 q_2 \ldots q_k$ where the q_i are distinct primes and $k \geq 2$. Suppose that, for each $i = 1, \ldots, k$, we have $(q_i - 1)|(n-1)$. Prove that n is a Carmichael number.

(ii) Suppose that p, $2p-1$, $3p-2$ are all primes, with $p > 3$. Prove that $p(2p-1)(3p-2)$ is a Carmichael number. Find the smallest Carmichael number of this form.

(iii) Let $n = pqr$, where p, q, r are distinct primes. Suppose also that $(p-1)|(qr-1)$ and $(q-1)|(pr-1)$ and $(r-1)|(pq-1)$. Prove that n is a Carmichael number. Show that $601 \times 1201 \times 1801$ is a Carmichael number (you may assume that 601, 1201 and 1801 are prime).

4. Let $m > 1$ be an integer not divisible by 2 or 5. Consider the standard equations which occur in the calculation of the decimal expansion of $\frac{1}{m}$:

$$\begin{aligned} 1 &= r_1, \\ 10r_1 &= mq_1 + r_2, \\ 10r_2 &= mq_2 + r_3, \text{ etc.,} \end{aligned}$$

where $0 < r_i < m$ and $0 \leq q_i \leq 9$ for each i so that the q_i are the decimal digits. Prove that, for $j \geq 0$, $r_{j+1} \equiv 10^j \bmod m$, and that the length of the period of $1/m$ in decimal notation is the order of 10 mod m.

Suppose now that $m = p$ is *prime* (not equal to 2 or 5), and assume that

$$\frac{1}{p} = 0 \cdot \overline{q_1 q_2 \ldots q_{2k}}$$

has even period length $2k$. Show that $10^k \equiv -1 \pmod p$ and deduce that $r_{k+1} = p - 1$.

Show further that the sums $r_2 + r_{k+2}, r_3 + r_{k+3}$, etc., are all equal to p, and that the sums $q_1 + q_{k+1}, q_2 + q_{k+2}, q_3 + q_{k+3}$, etc., are all equal to 9.

5. (i) Define the function $\sigma(n)$. Show that for a prime p and integer $a \geq 1$, $\sigma(p^a) = 1 + p + p^2 + \ldots + p^a = \frac{p^{a+1}-1}{p-1}$. Write down a general formula for $\sigma(n)$. Show that if p is odd and a is odd then $\sigma(p^a)$ is even. Show that if p is odd and a is even then $\sigma(p^a)$ is odd.

(ii) Show that, if $2^{s+1} - 1$ is prime, then $n = 2^s(2^{s+1} - 1)$ is a perfect number. Write down three even perfect numbers.

(iii) Use the formula for $\sigma(p^a)$ to show that

$$\sigma(p^a) < p^a \left(\frac{p}{p-1} \right).$$

Now suppose that $n = p^a q^b$ where $p \geq 3$ and $q \geq 5$ are distinct odd primes and $a \geq 1, b \geq 1$. Show that

$$\frac{\sigma(p^a)}{p^a} < \frac{3}{2}, \quad \frac{\sigma(q^b)}{q^b} < \frac{5}{4}.$$

Deduce that $\sigma(n) < 2n$ and that n is not a perfect number.

[Hint: You may find it helpful first to show the identity $\frac{p}{p-1} = 1 + \frac{1}{p-1}$]

(iv) Let $n = p_1^{n_1} p_2^{n_2} p_3^{n_3} p_4^{n_4} p_5^{n_5} p_6^{n_6}$, where $p_1, \ldots, p_6$ are distinct odd primes. Show that if n is a perfect number then $3|n$ and exactly one of $n_1, \ldots, n_6$ is odd.

6. (i) Describe Miller's Test to base b for the primality of an odd integer n with $(b, n) = 1$. Explain why, if n is prime, then it always passes Miller's Test.

(ii) For each of the following values of n and b apply Miller's Test to n base b. In each case, decide whether n is a pseudoprime to base b and decide whether n is a strong pseudoprime to base b.

(a) $b = 6$, $n = 217$. (b) $b = 8$, $n = 65$. (c) $b = 2$, $n = 129$.

[You may wish first to compute $6^3 \pmod{217}$, $8^2 \pmod{65}$ and $2^7 \pmod{129}$.]

(iii) Let $k \geq 1$. Show that $n = 2^{2^k} + 1$ always passes Miller's Test to the base 2.

7. For the continued fraction expansion $[a_0, a_1, a_2, \ldots]$ of $x_0 = \sqrt{n}$ where n is not a square, you may assume the standard formulae:

$$P_0 = 0, Q_0 = 1,\ x_k = \frac{P_k + \sqrt{n}}{Q_k},\ a_k = [x_k],\ P_{k+1} = a_k Q_k - P_k,\ Q_{k+1} = \frac{(n - P_{k+1}^2)}{Q_k}.$$

(i) Show that $P_1 = a_0$ and $Q_1 = n - a_0^2$. Now suppose that $Q_k = 1$ for some $k \geq 1$. Show that $P_{k+1} = P_1$, $Q_{k+1} = Q_1$, and that the continued fraction recurs: $[a_0, \overline{a_1, \ldots, a_k}]$.

(ii) For the case $n = 9d^2 + 6d$ $(d \geq 1)$, show that the continued fraction expansion of $\sqrt{n}$ is $[3d, \overline{1, 6d}]$.

(iii) Find three solutions in integers $x > 0, y > 0$ to the equation

$$x^2 - 48y^2 = 1.$$

8. Let p denote an odd prime.

(i) State Euler's Criterion for quadratic residues.

(ii) Deduce from Euler's criterion that $(\frac{-1}{p}) = 1$ if and only if $p \equiv 1 \pmod 4$.

(iii) State Gauss' Law of Quadratic Reciprocity. Evaluate $(\frac{-19}{193})$. Show that $(\frac{3}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

(iv) Let $p_1, p_2, \ldots, p_k$ be primes, all congruent to $-1 \pmod{12}$, and define n by: $n = 3(2p_1p_2 \ldots p_k)^2 - 1$. Show that $n \equiv -1 \pmod{12}$. Now, let p be prime and $p|n$. Use the definition of n to show that $(\frac{3}{p}) = 1$. Deduce that $p \equiv \pm 1 \pmod{12}$. Show that at least one such prime factor p of n must be congruent to $-1 \pmod{12}$ and hence show that there must be infinitely many primes congruent to $-1 \pmod{12}$.