1. (i) Let x be a real number and n an integer. Show that

$$[x] \geq n \quad \Leftrightarrow \quad x \geq n.$$

[You may use the standard inequalities $x - 1 < [x] \leq x$.] Deduce that if a is an integer ≥ 0 and y is a real number, then $[ay] \geq a[y]$.

(ii) Let $n > 0$ be an integer. Let r be the largest power of a prime p dividing $n!$ (that is: p^r divides $n!$ but p^{r+1} does not divide $n!$). Show that

$$r = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots,$$

the sum being continued until the terms become zero. Use this to find the number of zeros at the end of the decimal expression for each of 50! and the binomial coefficient $\binom{50}{25}$, explaining your reasoning.

(iii) Using (i) and the formula in (ii), or otherwise, show that, if a and b are positive integers, then $(b!)^a$ divides $(ab)!$.

2. Define Euler's ϕ-function. Prove Euler's Theorem, that if $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Now, let $(a, b) = 1$. Show the following.

(i) If $a|bc$ then $a|c$.

(ii) If $a|c$ and $b|c$ then $ab|c$.

(iii) $\big(\, x \equiv y \pmod{a}$ and $x \equiv y \pmod{b} \,\big) \quad \Leftrightarrow \quad x \equiv y \pmod{ab}$.

(iv) $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

[For part (i) you may find it helpful to use that fact that, since $(a, b) = 1$, there exist integers s, t satisfying $as + bt = 1$.]

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) Suppose that n is as in (i) with $k = 2$, and suppose that $q_2 > q_1$. Show that $n - 1 \equiv q_1 - 1 \pmod{q_2 - 1}$. Show that this leads to a contradiction. What is the minimum possible value of k in (i)?

4. 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.

For each of the following values of b, apply Miller's test on 133 to base b. In each case, decide whether 133 is a pseudoprime to base b, and whether 133 is a strong pseudoprime to base b.

(i) $b = 12$, (ii) $b = 11$, (iii) $b = 8$, (iv) $b = 2$.

[You may find it helpful first to compute 12^3, 11^3, 8^3 and 8^6 (mod 133).]

5. (i) Define the term *primitive root* mod n. Given that g is a primitive root mod n, show that

$$g^a \equiv g^b \pmod{n} \iff a \equiv b \pmod{\phi(n)}.$$

(ii) Show that 3 is a primitive root mod 34. Hence or otherwise find all x for which $15^x \equiv 21 \pmod{34}$. Show that 13 is not a primitive root mod 34.

(iii) Suppose that g is a primitive root mod n, where $n > 2$. By writing $x \equiv g^k \pmod{n}$ or otherwise, show that $x^2 \equiv 1 \pmod{n}$ has exactly two solutions, and deduce that

$$x^2 \equiv 1 \pmod{n} \iff x \equiv \pm 1 \pmod{n}.$$

(iv) Let $n = 4h$ where $h > 1$, and let $x = 2h+1$. Show that $x^2 \equiv 1 \pmod{n}$ and deduce from (iii) (or otherwise) that there is no primitive root mod n.

6. (i) Let m be an integer with $(m, 10) = 1$. Show that the length of the decimal period of $\frac{1}{m}$ is the order of 10 mod m, and that the period begins immediately after the decimal point.

(ii) Let $(x, m) = (x, n) = (m, n) = 1$. Show that $\mathrm{ord}_{mn}x$ is the least common multiple of $\mathrm{ord}_m x$ and $\mathrm{ord}_n x$.

(iii) Find the lengths of the decimal periods of the fractions

$$\frac{1}{7}, \frac{1}{11}, \frac{1}{13}, \frac{1}{17}, \frac{1}{77}, \frac{1}{91}, \frac{1}{143}, \frac{1}{221}.$$

7. (i) Define the function $\sigma(n)$. Show that for a prime p and integer $a \geq 1$, $\sigma(p^a) = \frac{p^{a+1}-1}{p-1}$. Write down a general formula for $\sigma(n)$.

(ii) Make a table of values of $\sigma(p^a)$ for small p and a in order to find all n for which $\sigma(n) = 32$.

(iii) Show that, if $2^{s+1} - 1$ is prime, then $n = 2^s(2^{s+1} - 1)$ is a perfect number.

(iv) Let $s(n) = \sigma(n) - n$. What are $s(p)$ and $s(p^2)$ for p prime? Show that, if $n > 1$ is neither prime nor the square of a prime, then $s(n) \geq 1 + p + n/p$ for some prime p dividing n. Hence (or otherwise) find all n such that $s(n) = 7$.

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

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

$$x^2 - 20y^2 = 1.$$