1. Let $[x]$ denote, as usual, the greatest integer $\leq x$.

(i) 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.

(ii) Find the number of zeros at the end of the decimal expression of 60!

(iii) Show that, for all real numbers x, y and z, $[x] + [y] + [z] \leq [x + y + z]$.

(iv) Show that, for any positive integers a, b, c,

$$\frac{(a+b+c)!}{a!b!c!}$$

is an integer. Find the number of zeros at the end of the decimal expression of

$$\frac{60!}{10!20!30!}.$$

2. (i) State and prove Fermat's theorem.

(ii) Define the term *pseudoprime*. Using Fermat's theorem, or otherwise, find 3^{670} mod 11 and 3^{660} mod 61; also find 3^{670} mod 61. Hence or otherwise show that 671 is a pseudoprime to base 3.

(iii) Let n be a pseudoprime to base b. Show that n is also a pseudoprime to base b^2.

(iv) Show that 15 is a pseudoprime to base 4, but is not a pseudoprime to base 2. For any odd integer $b \geq 3$, show that $n = b^2 - 1$ is a pseudoprime to base b^2, but is not a pseudoprime to base b.

3. (i) Describe Miller's test to base b for the primality of an odd integer n with $(b, n) = 1$. Does 25 pass Miller's test to base 7? Does 217 pass Miller's test to base 5? [You may wish first to compute $7^4 \pmod{25}$ and $5^6 \pmod{217}$.]

(ii) Suppose, for some integer b and odd integer n, that $b^{n-1} \equiv 1 \pmod{n}$ and $b^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$. Does n pass or fail Miller's test to base b? Show that $c = (b^{(n-1)/2} - 1, n)$ is a proper factor of n [that is: $c|n$ and $c \neq 1, c \neq n$].

4. Let m 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. 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 $\sigma(n)$.

(i) Make a table of values of $\sigma(p^a)$ for small p and a in order to find all n for which $\sigma(n) = 42$. Does there exist n such that $\sigma(n) = 21$?

(ii) 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

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

and deduce that $\sigma(n) < 2n$.

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

6. (i) Define the term *primitive root* mod n.

(ii) Let $n = ab$ where $a > 2, b > 2$ and $(a, b) = 1$. Show that $\phi(a), \phi(b)$ are both even. Show, using Euler's theorem or otherwise, that, for any g with $(g, n) = 1$,

$$g^{\frac{\phi(n)}{2}} \equiv 1 \pmod{n}.$$

[Hint: First use $\phi(n) = \phi(a)\phi(b)$ and the fact that $\phi(a), \phi(b)$ are both even to show that the given congruence holds mod a and mod b.]

Deduce that n has no primitive roots.

(iii) Verify that 5 is a primitive root mod 34 and hence or otherwise solve the equations: (a) $23^x \equiv 15 \pmod{34}$; (b) $y^4 \equiv 21 \pmod{34}$.

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

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

$$x^2 - 35y^2 = 1.$$

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. Let p be an odd prime. Show that $(\frac{5}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod{5}$.

(iv) Let $p_1, p_2, \ldots, p_k$ be primes, all congruent to $-1 \pmod{5}$, and define n by: $n = 4(p_1 p_2 \ldots p_k)^2 - 5$. Show that $n \equiv -1 \pmod{5}$. Now, let p be prime and $p|n$. Use the definition of n to show that $(\frac{5}{p}) = 1$. Deduce that $p \equiv \pm 1 \pmod{5}$. Show that at least one such prime factor p of n must be congruent to $-1 \pmod{5}$ and hence show that there must be infinitely many primes congruent to $-1 \pmod{5}$.