1. Let $[x]$ denote, as usual, the greatest integer less than or equal to 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 for each of $80!$ and the binomial coefficient $\begin{pmatrix} 80 \\ 35 \end{pmatrix}$, explaining your reasoning.

(iii) Explain why the largest power of 2 dividing $n!$ is, for $n > 1$, always greater than the largest power of 5 dividing $n!$.

(iv) Reading the decimal digits of $n!$ (for $n > 1$) from left to right, show (using (iii) or otherwise) that the last nonzero digit is always even. Show that the number of zeros at the end of the decimal expression for $(5n)!$ is n more than the number of zeros at the end of the decimal expression for $n!$.

2. (i) State and prove Fermat's Theorem. Use it to prove that $2^{75} + 3^{75}$ is divisible by 5.

(ii) Let $n = r^4 + 1$, where r is an integer. Use Fermat's Theorem to show that, if 5 does not divide r, then $n \equiv 2 \pmod 5$. Find also what n is congruent to (mod 5) when 5 does divide r. Deduce that n is never a multiple of 5 for any value of r. Show also that n is never a multiple of 13. Let p be a prime of the form $p = 4m + 3$. Show that n is never a multiple of p.

(iii) Let $n = r^{2k} + 1$, where r, k are positive integers, and let p be a prime of the form $p = 4km + 2k + 1$. Show that n is never a multiple of p.

3. (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) $b = 19$, $n = 169$. (b) $b = 5$, $n = 217$. (c) $b = 2$, $n = 105$.

[You may wish first to compute $19^6 \pmod{169}$, $5^6 \pmod{217}$, $2^{12} \pmod{105}$.]

(iii) Show that if n passes Miller's Test to base b then n passes Miller's Test to base $n - b$.

4. (i) 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 $j \geq 0$, $r_{j+1} \equiv 10^j \bmod m$, that the length of the period of $1/m$ in decimal notation 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 for the fractions

$$\frac{1}{7}, \ \frac{1}{31}, \ \frac{1}{217}.$$

(iv) Let (a, b) denote the greatest common divisor of a and b, and let $[a, b]$ denote the least common multiple of a and b. For any integers a, b, show that $ab = (a, b)[a, b]$.

(v) For distinct primes p, q (with $p \neq 2, 5$ and $q \neq 2, 5$), show that the decimal period of $\frac{1}{pq}$ has length at most $(p-1)(q-1)/2$.

5. (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 3 is a primitive root mod 38 and hence or otherwise solve the equations:

$$\text{(a)} \ \ 7^x \equiv 25 \pmod{38}; \quad \text{(b)} \ \ y^4 \equiv 23 \pmod{38}.$$

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

(ii) Make a table of values of $\sigma(p^a)$ for small p and a in order to find all n for which $\sigma(n) = 48$.

(iii) Find the smallest n for which $d(n) = 27$.

(iv) Show that there is no perfect number of the form $15 \cdot 2^k$.

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 $n = d^2 + d$ $(d \geq 1)$, 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

$$x^2 - 42y^2 = 1.$$

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) Deduce from Euler's criterion that $(\frac{2}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod 8$.

(iv) State Gauss' Law of Quadratic Reciprocity. Evaulate $(\frac{14}{71})$ and $(\frac{-3}{71})$. Show that $(\frac{10}{p}) = 1$ if and only if $p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$.