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

(i) Show that the largest power of a prime p dividing $n!$ is

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots,$$

the sum being continued until the terms become zero.

Give an example to show that this may not be the correct power of p dividing $n!$ when p is not prime.

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

(iii) Find the number of zeros at the end of $70!$, explaining how you get your answer.

(iv) Reading the decimal digits of $n!$ $(n > 1)$ from left to right, show (using (ii) or otherwise) that the last nonzero digit is always even.

2.

(i) Explain why

$$x^2 \equiv x \bmod 225 \iff x^2 \equiv x \bmod 9 \text{ and mod } 25.$$

Find all the solutions of the congruence $x^2 \equiv x \bmod 225$, stating carefully any general results on congruences you use in your solution.

(ii) State and prove Fermat's theorem. Use it to show that, if n is an integer, then it is not possible to have $n^2 \equiv -1 \bmod 7$. Show more generally that if n is an integer and p is a prime of the form $p = 4k + 3$, then p does not divide $n^2 + 1$.

3. Let n be odd and $(b, n) = 1$. Describe Miller's test with base b as applied to n.

Let $n = 257 = 2^8 + 1$. Use $2^8 \equiv -1 \bmod 257$ to write down the effect of applying Miller's test with base 2 to 257.

Now suppose an odd number n passes Miller's test with base 2.

(i) Suppose that the last step of the test with base 2 has the form

$$2^r \equiv \pm 1 \bmod n$$

for an *odd* value of r. Show that n also passes Miller's test with base 4 in the same number of steps as with base 2. [Hint: Show that, for any k,
$2^k \equiv \pm 1 \bmod n \Longrightarrow 4^k \equiv 1 \bmod n$.]

(ii) Suppose that the last step of the test with base 2 has the form

$$2^r \equiv -1 \bmod n$$

with r *even*. Show that n also passes Miller's test with base 4, in one more step than it passes in base 2.

Do (i) and (ii) show that every odd n which passes Miller's test with base 2 also passes with base 4?

4. Define Euler's ϕ function and show that, for a prime p and $a \geq 1$, $\phi(p^a) = p^{a-1}(p-1)$. Write down a general formula for $\phi(n)$.

(i) Make a table of values of $\phi(p^a)$ for small primes p and integers $a \geq 1$, and find all values of n for which $\phi(n) = 16$.

(ii) Let p be a prime such that $p \equiv -1 \bmod 12$ and let a be even. Show that
$\phi(p^a) \equiv 2 \bmod 12$.

(iii) Let p be a prime such that $p \equiv 5 \bmod 12$ and let $b \geq 1$. Assume $\phi(p^b) \equiv 2 \bmod 12$ and deduce that $5^{b-1} \cdot 2 \equiv 1 \bmod 6$. Why is this a contradiction?

(iv) Show similarly that if p is a prime congruent to 7 or 1 mod 12, and $b \geq 1$, then $\phi(p^b) \equiv 2 \bmod 12$ is impossible.

5. Define the term *primitive root* mod m.

(i) Given that g is a primitive root mod m, show that

$$g^a \equiv g^b \bmod m \iff a \equiv b \bmod \phi(m).$$

[You may assume the standard result that, for any c coprime to m, $c^k \equiv 1 \bmod m \iff \mathrm{ord}_m c | k$.] Verify that 2 is a primitive root mod 25. Hence or otherwise solve the congruence

$$11^x \equiv 21 \bmod 25$$

and show that the congruence $y^{12} \equiv -1 \bmod 25$ has no solutions.

(ii) Suppose that g is a primitive root mod m, where $m > 2$, and suppose that x is such that $x^2 \equiv 1 \bmod m$. Why is it true that $x \equiv g^k \bmod m$ for some k? (State any general result you use.) Deduce or prove otherwise that

$$x^2 \equiv 1 \bmod m$$

has exactly two solutions mod m, and hence that the only solutions are $x \equiv \pm 1 \bmod m$.

6. Define the function σ and show that for any prime p and integer $a \geq 1$, $\sigma(p^a) = \frac{p^{a+1}-1}{p-1}$.

(i) Let $n = 2^{m-1}(2^m - 1)$ where $2^m - 1$ is prime. Show that $\sigma(n) = 2n$. State clearly any properties of σ which you use. Use this formula to give *three* examples of numbers n for which $\sigma(n) = 2n$.

(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 $\sigma(n) < 2n$.

7.

(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 p be prime and let $n = 6p + 1$. Suppose that $2^p \equiv -1 \bmod n$. Let q be a prime factor of n. Show that $2^{2p} \equiv 1 \bmod q$ and that $\text{ord}_q 2 = 2p$. Deduce that $2p|(q-1)$ and hence that $q > \sqrt{n}$. Why does it follow that n is prime?

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) Suppose that $Q_k = 1$ for some $k \geq 1$. Show that $P_1 = a_0$ and $Q_1 = n - a_0^2$. Show also that $P_{k+1} = P_1$, $Q_{k+1} = Q_1$, and 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

$$x^2 - 30y^2 = 1.$$