1. (i) Given that $x \equiv 1 \bmod 4$, what are the possible values of $x \bmod 12$? Show that every positive integer satisfies at least one of the congruences

$$x \equiv 0 \pmod 2, x \equiv 0 \pmod 3, x \equiv 1 \pmod 4, x \equiv 5 \pmod 6, x \equiv 7 \pmod{12}.$$

(ii) Show that, if p is an odd prime, then $p^n | x(x-2)$ if and only if $p^n | x$ or $p^n | (x-2)$. Find all solutions to the congruence

$$x^2 \equiv 2x \pmod{225}.$$

2. (i) Show that, if n is composite, then $2^n - 1$ is composite.

(ii) Define the term *pseudoprime to base* 2. Using Fermat's theorem, or otherwise, write down $2^{340} \bmod 11$ and $2^{330} \bmod 31$; also find $2^{340} \bmod 31$. Hence or otherwise show that 341 is a pseudoprime to base 2.

(iii) Now let n be a pseudoprime to base 2 and let $m = 2^n - 1$. Show that $n | (m-1)$ and deduce that $(2^n - 1) | (2^{m-1} - 1)$. Deduce that m is also a pseudoprime to base 2.

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 35 pass Miller's test to base 6?

(ii) Let p be an odd prime and $n = 4p + 1$. Suppose that $2^p \equiv 1 \pmod n$. Does n pass Miller's test to base 2?

4. (i) Define Euler's ϕ-function and write down a formula for $\phi(n)$. Compute $\phi(2 \times 7^2)$, $\phi(2 \times 5 \times 17)$, $\phi(2^4 \times 5 \times 257^5)$, giving your answers in factorized form.

Use the formula to show that, if p is prime and $p^2 | n$, then $p | \phi(n)$. Deduce that, if $\phi(n) = 2^k$, then n must be of the form

$$n = 2^s q_1 q_2 \dots q_m$$

where $q_1, \dots, q_m$ are distinct odd primes of the form $2^r + 1$.

(ii) Find an odd number n with $\phi(n) = 2^{31}$. (It is enough to give n in a factorized form.) Find *three* even numbers n with $\phi(n) = 2^{32}$.

[You may assume throughout the question the fact that: $2^1 + 1$, $2^2 + 1$, $2^4 + 1$, $2^8 + 1$ and $2^{16} + 1$ are all prime.]

5. 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

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

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.

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 7 is a primitive root mod 22 and hence or otherwise solve the equations

$$\text{(a)} \quad 19^x \equiv 17 \pmod{22}; \quad \text{(b)} \quad y^5 \equiv -1 \pmod{22}.$$

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

(ii) Find the smallest n for which $d(n) = 15$. Make a table of values of $\sigma(p^a)$ for small p and a and find all n for which $\sigma(n) = 72$.

(iii) Let $n = 2^3 \cdot p \cdot q$, where p and q are odd primes with $p < q$. Suppose that $\sigma(n) = 3n$. Show that this implies

$$3pq = 5(p + q + 1).$$

Find primes p and q which satisfy this equation and show that they are the only ones possible.

8. (i) Let $n = d^2 + 2$ where $d \geq 1$. Show that $[\sqrt{n}] = d$. Show that the continued fraction expansion of $\sqrt{n}$ is $[d, \overline{d, 2d}]$. You may assume the usual formulae, given below.

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

Write down formulae for the convergents p_k/q_k of a continued fraction $[a_0, a_1, a_2, \ldots]$.

Find enough convergents of the continued fraction of $\sqrt{27}$ to find *two* solutions $x > 0, y > 0$ to the equation

$$x^2 - 27y^2 = 1.$$

(ii) Let $m = d^2 - 1$ where $d \geq 2$. Show that the continued fraction expansion of $\sqrt{m}$ is $[d-1, \overline{1, 2d-2}]$.