1. (i) Let a, b and k be positive integers. Prove that the common divisors of a and b coincide with the common divisors of $a + bk$ and b. Deduce that the greatest common divisors coincide: $(a, b) = (a + bk, b)$.

Let n be an integer ≥ 2. Show that $(n!, (n+1)! + 2) = 2$.

Let x be an integer. Show that

$$(x^3 + 2x - 1, x^2 + 1) = \begin{cases} 2 & \text{if } x \text{ is odd,} \\ 1 & \text{if } x \text{ is even.} \end{cases}$$

(ii) State the fundamental theorem of arithmetic.

Let a and b be positive integers expressed in the usual way as

$$a = p_1^{a_1} \dots p_k^{a_k}, \quad b = p_1^{b_1} \dots p_k^{b_k},$$

where the a_i and b_i are ≥ 0 and, for each i, at least one of a_i, b_i is > 0.

Suppose that, for some *coprime* positive integers m and n we have $a^m = b^n$. State why $ma_i = nb_i$ for each i and deduce $n|a_i$ and $m|b_i$ for all i. Deduce that $a = x^n, b = x^m$ for a positive integer x.

2. (i) Explain why

$$x^2 \equiv x \mod 196 \iff x^2 \equiv x \mod 4 \text{ and mod } 49.$$

Find all the solutions of the congruence $x^2 \equiv x \mod 196$, stating clearly any general results you use in your solution.

(ii) Let b be an integer ≥ 2. Define *pseudoprime to base b*. Prove that, if n is a pseudoprime to base 2 then it is a pseudoprime to base 4. Find a number $n > 4$ which is a pseudoprime to base 4 but not to base 2. (There is such an $n < 10$.)

Verify that 91 is a pseudoprime to base 3, stating clearly any results you use in your argument.

3. (i) State Fermat's theorem.

Let $n = x^6 + 1$ where x is an integer ≥ 1.

Use Fermat's theorem to show that $n \equiv 2 \bmod 7$ if x is not a multiple of 7. Deduce that n can never be $\equiv 0 \bmod 7$, i.e. can never be a multiple of 7.

Show more generally that, if p is a prime of the form $p = 12k+7$ $(k \geq 0)$ then n can never be a multiple of p.

(ii) Describe Miller's test as applied to an odd positive integer n, with base b where $(b, n) = 1$.

Let b be even and let $n = b + 1$. Show that n always passes Miller's test to base b. [Hint: $b \equiv -1 \bmod n$.] Illustrate by applying Miller's test with base $b = 8$ to $n = 9$.

4. Define the term *Carmichael number.*

(i) Suppose $n = q_1 q_2 \ldots q_k$, where $k \geq 2$, the q_i are distinct primes and $(q_i - 1)|(n - 1)$ for all i. Prove that n is a Carmichael number, stating clearly any general results on congruences which you use.

(ii) Suppose $q_1 = p, q_2 = 2p - 1$ and $q_3 = 3p - 2$ are all prime, and let $n = q_1 q_2 q_3$. Show that

$$n - 1 = (p - 1)(6p^2 - p + 1),$$

and deduce that n is a Carmichael number provided $p \equiv 1 \bmod 6$. Hence find an example of a Carmichael number.

(iii) Let $n = ab$ where $1 < a < b$. Writing

$$ab - 1 = a(b - 1) + (a - 1),$$

or otherwise, show that it is impossible to have $(b - 1)|(n - 1)$. Deduce that the smallest value of k in (i) which yields a Carmichael number is $k = 3$.

5. Define Euler's ϕ function. Write down a general formula for $\phi(n)$ and find all n for which $\phi(n) = 4$.

State and prove Euler's theorem.

Let p be a prime > 5. Show that $10^{6p-6} \equiv 1 \bmod 9p$, making it clear where you assume $p > 5$.

Define $r_n = \frac{10^n - 1}{9}$. Explain why is r_n an integer and write down its expression in decimal notation. Show that, with p as above, $p | r_{6p-6}$.

6. (i) Define the term *order of* g mod m and *primitive root* mod m. Find the smallest positive primitive root mod 18.

Show that the equation $13^x \equiv 11 \bmod 18$ has no solutions and find all solutions to $13^x \equiv 7 \bmod 18$. State clearly any general results you use about primitive roots.

(ii) Let p be an odd prime and let $n = 4p + 1$. Assume that $2^p \equiv 1 \bmod n$. Suppose that q is a prime, $q|n$. Show that the order of 2 mod q is p and deduce that $p|(q-1)$. Deduce that $q > \sqrt{n}$ and that n is prime.

7. Define the functions d and σ. Show that, for a prime p and $a \geq 1$,

$$d(p^a) = a + 1, \quad \sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}.$$

Write down general formulae for d and σ.

Find the smallest n for which $d(n) = 12$. Make a table of values of $\sigma(p^a)$ for small values of p and a, in order to find all n for which $\sigma(n) = 42$.

A number is called *3-perfect* if $\sigma(n) = 3n$. Find all 3-perfect numbers of the form $n = 2^k.15$.

8. (i) Let $n = 9d^2 + 3$ where $d \geq 1$. Show that $[\sqrt{n}] = 3d$. Show that the continued fraction expansion of $\sqrt{n}$ is $[3d, \overline{2d, 6d}]$. 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 $\sqrt{39}$ to find *three* solutions $x > 0, y > 0$ to the equation

$$x^2 - 39y^2 = 1.$$

(ii) Show that the continued fraction expansion of $\sqrt{n}$ recurs after *one* term if and only if n is of the form $r^2 + 1$, and that the expansion is then $[r, \overline{2r}]$. [You may assume that recurrence after one term is equivalent to $Q_1 = 1$.]