1. Let α, β, k, x be integers, and let a, b, n, q, r be positive integers.

(i) Show that $(\alpha, \beta) = (\alpha + k\beta, \beta) = (\alpha, \beta + k\alpha)$.

(ii) Find $(x^3 - 2, x^2 + 1)$.

(iii) Show that $(x^n - 1)/(x - 1)$ is an integer. Show that

$$((x^n - 1)/(x - 1), x - 1) = (n, x - 1).$$

[Hint: first find a polynomial $f(x)$ such that $x^n - 1 = (x-1)f(x)$, then divide $f(x)$ by $x - 1$ to find a polynomial $g(x)$ such that $(x^n - 1)/(x - 1) = (x - 1)g(x) + n$.]

(iv) Let $a = bq + r$, with $0 \leq r < b$, and $A = n^a - 1, B = n^b - 1, R = n^r - 1$. Find Q, a polynomial in n, such that $A = BQ + R$. Hence or otherwise show that $(n^a - 1, n^b - 1) = n^{(a,b)} - 1$. Compute $(3^{87} - 1, 3^{69} - 1)$.

2. (i) Explain why

$$x^2 \equiv x \pmod{216} \iff x^2 \equiv x \text{ (mod 8 and mod 27)}.$$

Find all solutions to $x^2 \equiv x \pmod{216}$, stating clearly any general results on congruences which you use in your solution.

(ii) State and prove Fermat's theorem. Use it to show that, if n is an integer, then 7 does not divide $n^2 + 1$. Show also that if n is an integer and p is a prime of the form $p = 8\ell + 5$, then p does not divide $n^4 + 1$.

3. 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 $\phi(p^a)$ for small primes p and integers $a \geq 1$, in order to find all values of n for which $\phi(n) = 20$. Show that there does not exist n for which $\phi(n) = 14$.

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

(iii) Let $p > 3$ be prime. What can p be congruent to modulo 12? Let $b \geq 3$ be odd. Show that $\phi(p^b) \not\equiv 2 \pmod{12}$.

4. (i) Describe Miller's test to base b for the primality of an odd integer n with $(b,n)=1$. Apply Miller's test to $n=85$, using:

(a) base 2. (b) base 4. (c) base 13.

Decide, giving reasons, whether 85 is a pseudoprime or strong pseudoprime to each of these bases.

[You may find it helpful first to compute 2^8 and $13^2 \pmod{85}$]

(ii) Let $n \geq 3$ be an odd integer. Show that n always passes Miller's test to base $b = n-1$. [You may find it helpful first to show that $b \equiv -1 \pmod{n}$].

(iii) Let $m \geq 2$ be an even integer. Show that $n = m^m + 1$ always passes Miller's test to base m.

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

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

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.

6. (i) Define $\sigma(n)$ and show, for prime p, that $\sigma(p^a) = 1 + p + p^2 + \ldots + p^a$. Prove that, if $\sigma(p^a)$ is odd and $p \neq 2$, then a is even. Write down a general formula for $\sigma(n)$. Prove that, if $\sigma(n)$ is odd, then n is either m^2 or $2m^2$ for some integer m.

(ii) Show that every even perfect number n satisfies $n \equiv 6$ or $8 \pmod{10}$, and so has last digit 6 or 8 when written in base 10.

[You may assume without proof the result from lectures that any even perfect number n is of the form $n = 2^s(2^{s+1} - 1)$ with $2^{s+1} - 1$ a prime number.]

(iii) Show that every even perfect number > 6 is the sum of consecutive odd cubes. Find the first three even perfect numbers > 6 and write each as a sum of consecutive odd cubes.

[You may use without proof the identity $1^3 + 3^3 + \ldots + (2k-1)^3 = k^2(2k^2 - 1)$.]

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 $n = 4d^2 + d$ $(d \geq 2)$, show that the continued fraction expansion of $\sqrt{n}$ is $[2d, \overline{4, 4d}]$.

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

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

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) Show that $(\frac{-2}{p}) = 1$ if and only if $p \equiv 1$ or $3 \pmod 8$.

(v) Let $p_1, p_2, \ldots, p_k$ be primes, all congruent to $3 \pmod 8$, and define n by: $n = (p_1 p_2 \ldots p_k)^2 + 2$. Show that $n \equiv 3 \pmod 8$. Now, let $p | n$. Use the definition of n to show that $(\frac{-2}{p}) = 1$, and deduce that $p \equiv 1$ or $3 \pmod 8$. Show that at least one such prime factor p of n must be congruent to $3 \pmod 8$ and hence show that there must be infinitely many primes congruent to $3 \pmod 8$.