1. (i) Explain why

$$x^2 \equiv x \pmod{1000} \iff x^2 \equiv x \pmod{8 \text{ and } 125}.$$

Find all solutions of $x^2 \equiv x \pmod{1000}$, stating clearly any general results on congruences which you use in your solution.

(ii) Show that $x^3 \equiv 0, 1$ or $-1 \pmod{9}$ for any integer x. Deduce that it is impossible to write an integer of the form $9m + 4$ as the sum of three cubes $x^3 + y^3 + z^3$ for integers x, y, z.

(iii) Show that if $x^2 + y^2 \equiv 0 \pmod{7}$ then $x \equiv 0$ and $y \equiv 0 \pmod{7}$. Deduce that no integer of the form $7(7m + 1)$ can be written as the sum of two squares $x^2 + y^2$ for integers x, y.

2. (i) State and prove Fermat's Theorem. Use it to prove that $3^{50} + 5^{50}$ is divisible by 17.

(ii) Let $n = r^6 + 1$, where r is an integer. Use Fermat's Theorem to show that, if 7 does not divide r, then $n \equiv 2 \pmod{7}$. Find also what n is congruent to (mod 7) when 7 does divide r. Deduce that n is never a multiple of 7 for any value of r. Show also that n is never a multiple of 3 or 11. Let p be a prime of the form $p = 12m + 7$. Show that n is never a multiple of p.

3. (i) 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 $\phi(n)$. Show that if p is prime and $p|n$ then $(p-1)|\phi(n)$. Show that if p is prime and $p^2|n$ then $p|\phi(n)$.

(ii) Find the prime-power decomposition of 10! (that is, write 10! as the product of powers of distinct primes). Compute $\phi(10!)$. Compute $\phi(a)$ where a is the binomial coefficient

$$\begin{pmatrix} 25 \\ 5 \end{pmatrix} = \frac{25!}{5!20!}.$$

(iii) Show that there do not exist integers $n, k \geq 1$ such that $\phi(n) = 3^k$. Find three odd primes p such that $\phi(p)$ is a power of 2. Find three odd composite integers n such that $\phi(n)$ is a power of 6.

4. (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) Define what it means for n to be a *pseudoprime* to base b. Define what it means for n to be a *strong pseudoprime* to base b.

(iii) 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) $b = 2$, $n = 645$. (b) $b = 3$, $n = 121$. (c) $b = 2$, $n = 33$.

[You may wish first to compute $2^{28} \pmod{645}$, $3^5 \pmod{121}$ and $2^5 \pmod{33}$.]

(iv) Let $(a, n) = 1$. Show that if n is a pseudoprime to base a and base ab then n is also a pseudoprime to base b.

5. (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

$$\frac{1}{7}, \ \frac{1}{23}, \ \frac{1}{161}.$$

(iv) For any prime $p > 7$, show that the decimal period of $\frac{1}{7p}$ has length at most $3(p-1)$.

[Hint. For the last part, you may find it helpful to use the result from lectures that $ab = (a, b)[a, b]$, for any integers a, b.]

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 $\sigma(n) = 96$.

(iii) Find the smallest n for which $d(n) = 14$.

(iv) Let $n = 2^5 3^3 pq$, where p and q are primes and $3 < p < q$. Suppose that $\sigma(n) = 4n$. Show that this implies

$$35(p+1)(q+1) = 48pq.$$

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

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 $n = 4d^2 + 2d$ $(d \geq 1)$, show that the continued fraction expansion of $\sqrt{n}$ is $[2d, \overline{2, 4d}]$.

(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 $(\frac{6}{79})$ and $(\frac{-11}{151})$. Show that $(\frac{-3}{p}) = 1$ if and only if $p \equiv 1 \pmod 3$.