1. Show that, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Let $m = 4 \cdot 10^k + 367$ where k is an integer ≥ 0.

(i) Show that $k \equiv 1 \pmod{2} \Rightarrow m \equiv 0 \pmod{11}$.

(ii) Show that $k \equiv 1 \pmod{3} \Rightarrow m \equiv 0 \pmod{37}$.

(iii) Find a number $n_1 > 1$ such that $k \equiv 0 \pmod{6} \Rightarrow m \equiv 0 \pmod{n_1}$.

(iv) Find a number $n_2 > 1$ such that $k \equiv 2 \pmod{6} \Rightarrow m \equiv 0 \pmod{n_2}$.

Deduce that m is composite for every k.

2. State Fermat's Theorem. Define the term *pseudoprime*.

Let a be an integer > 1 and let p be an odd prime such that p does not divide a, and p does not divide $a^2 - 1$. Let

$$n = \frac{a^{2p} - 1}{a^2 - 1} = a^{2p-2} + a^{2p-4} + \ldots + a^2 + 1.$$

(i) Show that $(a, n) = 1$ and that $n - 1$ is even.

(ii) Show that $a^{2p} \equiv 1 \pmod{n}$.

(iii) Show that $(n-1)(a^2-1) = a^2(a^{2p-2} - 1)$ and deduce from Fermat's Theorem that $p \mid n - 1$. Deduce from (i) that $2p \mid n - 1$.

(iv) Deduce from (ii) and (iii) that $a^{n-1} \equiv 1 \pmod{n}$.

(v) Taking $a = 3$ and the smallest allowable value of p, find a pseudoprime to the base 3.

3. Define Euler's ϕ-function. Prove Euler's Theorem, that if $(b, n) = 1$ then $b^{\phi(n)} \equiv 1 \pmod{n}$.

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) Show that $m^{100} \equiv 1 \pmod{8}$ and $m^{100} \equiv 1 \pmod{125}$ for any integer m satisfying $(m, 10) = 1$. What are the last 3 digits of $37^{100} - 21^{100}$?

(ii) Show that $\phi(n)$ is even for all $n > 2$.

(iii) Describe all n such that $\phi(n) \equiv 2 \pmod{4}$.

4. 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.

For each of the following values of b, apply Miller's test on 325 to base b. In each case, decide whether 325 is a pseudoprime to base b, and whether 325 is a strong pseudoprime to base b.

(i) $b = 2$, (ii) $b = 7$, (iii) $b = 24$, (iv) $b = 126$.

[You may find it helpful first to compute 2^{60}, 7^{12}, 24^{12} and $126^3 \pmod{325}$.]

5. Define what is meant by $\mathrm{ord}_n a$, the *order* of a mod n. Define what it means for a to be a *primitive root* mod n.

(i) Suppose that p is prime and $p \mid F_k$, where $F_k = 2^{2^k} + 1$. Show that $\mathrm{ord}_p 2 = 2^{k+1}$ and deduce that $2^{k+1} \mid p - 1$. Show that F_5 has no prime factor $p \leq 100$.

(ii) Verify that 3 is a primitive root mod 17. Hence find all solutions x to $4^x \equiv 8 \pmod{17}$. Solve also $y^{10} \equiv 2 \pmod{17}$.

6. Define the function $\sigma(n)$. Show that for a prime p and integer $a \geq 1$, $\sigma(p^a) = \frac{p^{a+1}-1}{p-1}$. Write down a general formula for $\sigma(n)$.

(i) Make a table of values of $\sigma(p^a)$ for small p and a in order to find all n for which $\sigma(n) = 32$.

(ii) Show that, if $2^{s+1} - 1$ is prime, then $n = 2^s(2^{s+1} - 1)$ is a perfect number.

(iii) Show that, if n is an even perfect number, then there exists an integer s such that $2^{s+1} - 1$ is prime and $n = 2^s(2^{s+1} - 1)$.

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 $n = d^2 - 2$ $(d \geq 3)$, show that the continued fraction expansion of $\sqrt{n}$ is $[d-1, \overline{1, d-2, 1, 2d-2}]$.

(iii) Find a solution in integers $x > 0, y > 0$ to the equation

$$x^2 - 23y^2 = 1.$$

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) Let $p_1, p_2, \ldots, p_k$ be primes, all congruent to 5 (mod 8), and define n by: $n = (p_1 p_2 \ldots p_k)^2 + 4$. Show that $n \equiv 5 \pmod 8$. Now, let p be prime and $p|n$. Use the definition of n to show that $(\frac{-4}{p}) = 1$, and deduce that $(\frac{-1}{p}) = 1$. Deduce that $p \equiv 1$ or $5 \pmod 8$. Show that at least one such prime factor p of n must be congruent to 5 (mod 8) and hence show that there must be infinitely many primes congruent to 5 (mod 8).