1. (i) Use Euclid's algorithm to calculate $(34, 21)$ and $(89, 55)$. Find integers s and t such that $34s + 21t = (34, 21)$. [7 marks]

(ii) The *Fibonacci numbers* are a sequence of numbers F_n defined as follows:

$$F_0 = F_1 = 1, \qquad F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

So the first few Fibonacci numbers are 1, 1, 2, 3, 5, 8, ... Explain why $(F_n, F_{n-1}) = (F_{n-1}, F_{n-2})$ for all $n \geq 2$ and hence show that any two consecutive Fibonacci numbers are coprime: that is, $(F_n, F_{n-1}) = 1$ for all $n \geq 1$. [6 marks]

(iii) Suppose that a and b are two positive integers with $a > b$ such that Euclid's algorithm applied to a and b takes precisely n steps. In other words, the steps of Euclid's algorithm are as follows (after setting $r_0 = a$ and $r_1 = b$):

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_n r_n. \end{aligned}$$

where $r_n \neq 0$. Show that $a \geq F_n$. Deduce that, to compute the GCD of any two numbers both smaller than F_n, Euclid's algorithm takes no more than $n - 1$ steps. [7 marks]

2. (i) State Fermat's theorem. Explain how to deduce that, if n is any integer, then $n^4 \equiv 0$ or $1 \pmod 5$. Show that there do not exist integers x and y satisfying the equation

$$x^4 + y^4 = 2^{2006}.$$

[8 marks]

(ii) Show that $(x + 4)^4 \equiv x^4 \pmod{16}$. If n is an integer, what are the possible values of $n^4 \pmod{16}$? [6 marks]

(iii) If n is an integer, what are the possible values of $n^4 \pmod{80}$? Justify your answer. [6 marks]

3. (i) Describe Miller's test to base b for the primality of an integer n with $(b, n) = 1$. Explain why, if n is prime, then it always passes Miller's test.

[5 marks]

(ii) For each of the following values of n and b, apply Miller's test to n, with base b. In each case, decide whether n is a pseudoprime to base b and whether n is a strong pseudoprime to base b. Also state whether n is prime.

(a) n=341, b=2; (b) n=121, b=3; (c) n=221, b=2.

[You may wish first to compute $2^{10} \pmod{341}$, $3^5 \pmod{121}$ and $2^{24} \pmod{221}$.]

[9 marks]

(iii) Suppose that n is a pseudoprime to the base b but fails Miller's test: that is, there exists an integer r such that $b^{2r} \equiv 1 \pmod{n}$ but $b^r \not\equiv \pm 1 \pmod{n}$. Show that $(b^r - 1, n)$ is a proper factor of n (i.e., a factor of n which is neither 1 nor n). Apply this in case (a) to find a proper factor of 341. [6 marks]

4. (i) Let p be prime and m a positive integer. Explain why the largest power of p which divides $m!$ is p^a, where

$$a = \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \left[\frac{m}{p^3}\right] + \cdots .$$

Find the number of zeroes at the end of 2006!. Find the number of zeroes at the end of the binomial coefficient

$$\binom{28}{8} = \frac{28!}{20!8!}.$$

[8 marks]

(ii) Define Euler's function $\phi(n)$ and explain why $\phi(p^r) = p^{r-1}(p-1)$. If the prime factorisation of n is $n = p_1^{r_1} \times \cdots \times p_k^{r_k}$, write down a formula for $\phi(n)$.

[5 marks]

(iii) Using your formula from (ii), compute the number of zeroes at the end of $\phi(100!)$. [You may assume that 2 divides $\phi(100!)$ to a higher power than 5 does.]

[7 marks]

5. (i) Let $m > 1$ be an integer not divisible by 2 or 5. Consider the standard equations which occur in the calculation of the decimal expansion of $\frac{1}{m}$:

$$\begin{aligned} 1 &= r_1, \\ 10r_1 &= mq_1 + r_2, \\ 10r_2 &= mq_2 + r_3, \\ &\vdots \end{aligned}$$

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 $j \geq 0$, $r_{j+1} \equiv 10^j \pmod{m}$, that the length of the period of $\frac{1}{m}$ in decimal notation is the order of 10 modulo m, and that the period begins immediately after the decimal point. [7 marks]

(ii) Find the lengths of the decimal periods for the fractions

$$\frac{1}{7}, \quad \frac{1}{13}, \quad \frac{1}{17} \quad .$$

[You may like to know that $10^8 + 1 = 17 \times 5882353$.] [7 marks]

(iii) Suppose now that p is prime. Complete the sentence "The length of the period is $p - 1$ if and only if 10 is a ______ ______ modulo p", define any terms you have used and show that it is true. [6 marks]

6. (i) Define the functions $d(n)$ and $\sigma(n)$. Show that, if p is prime and $a \geq 1$, then $\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1}-1}{p-1}$. Explain what it means to say that σ is *multiplicative* and prove that this is so. If the prime factorisation of an integer n is $n = p_1^{n_1} \times \cdots \times p_k^{n_k}$, write down a general formula for $\sigma(n)$. [9 marks]

(ii) Make a table of $\sigma(p^a)$ for small p and a and use it to find all positive integers n such that $\sigma(n) = 60$. [5 marks]

(iii) Define a *perfect number*. Show that, if $s \geq 1$ is an integer such that $2^{s+1} - 1$ is prime, then $2^s(2^{s+1} - 1)$ is a perfect number. Write down three perfect numbers. [6 marks]

7. (i) If the continued fraction of a real number x_0 is $x_0 = [a_0, a_1, a_2, \ldots]$, explain what the *convergents* of x_0 are. Using your calculator, find the first four terms in the continued fraction of π. Find the first four convergents of π.

[6 marks]

For the continued fraction expansion of $x_0 = \sqrt{n}$ where n is not a square, you may assume the standard formulae:

$$P_0 = 0, \qquad Q_0 = 1, \qquad x_k = \frac{P_k + \sqrt{n}}{Q_k}, \qquad a_k = [x_k],$$

$$P_{k+1} = a_k Q_k - P_k, \qquad Q_{k+1} = \frac{(n - P_{k+1}^2)}{Q_k}.$$

(ii) 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: $\sqrt{n} = [a_0, \overline{a_1, \ldots, a_k}]$. [6 marks]

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

$$x^2 - 18y^2 = 1.$$

[8 marks]

8. (i) Let p be an odd prime. Explain what it means for an integer n to be a *quadratic residue* modulo p. Show directly that -1 is a quadratic residue modulo 37. State a result relating $\left(\frac{-1}{p}\right)$ to the value of p modulo 4 and comment on how it relates to your previous answer. [7 marks]

(ii) State Gauss' law of quadratic reciprocity. Show that, if p is an odd prime not equal to 5, then 5 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod 5$. [5 marks]

(iii) Consider the function $q(x, y) = x^2 - 5y^2$. We are interested in what values this function can take when x and y are coprime integers.

Suppose there is an odd prime $p \neq 5$ such that $p \mid x^2 - 5y^2$ for some coprime integers x and y. Show that if $p \mid x$ then $p \mid y$ as well, and deduce that p does not divide x. Similarly show that $p \nmid y$. Show that y has an inverse modulo p and hence that 5 is a quadratic residue modulo p.

Deduce that, apart from maybe 5, the only odd primes which can divide $q(x, y)$, for x and y coprime, are those congruent to $\pm 1 \pmod 5$. [8 marks]