Part IA

Numbers and Sets

Paper 4, Section I

1F Numbers and Sets

A *permutation* of the integers $\{1, \ldots, n\}$ is a bijection from this set to itself. The permutation σ is said to be *up-down* if $\sigma(1) < \sigma(2) > \sigma(3) < \sigma(4) > \ldots$; it is said to be *down-up* if, instead, $\sigma(1) > \sigma(2) < \sigma(3) > \sigma(4) < \ldots$.

(a) Define a bijection between the set of up-down and the set of down-up permutations of $\{1, \ldots, n\}$.

(b) Let A_n be the number of up-down permutations of $\{1, \ldots, n\}$ for $n \geqslant 1$, and define $A_0 = 1$. Show that these numbers satisfy the equation

$$2A_{n+1} = \sum_{k=0}^{n} \binom{n}{k} A_k A_{n-k} \quad \text{for } n \geqslant 1\,.$$

[*Hint: Consider the possible up-down or down-up permutations for which a given element of* $\{1, \ldots, n+1\}$ *maps to* $n+1$.]

Paper 4, Section I

2E Numbers and Sets

State and prove the Chinese remainder theorem.

Find all solutions x of the simultaneous congruences

$$\begin{cases} x \equiv 4 \mod 6\,, \\ x \equiv 2 \mod 8\,. \end{cases}$$

Prove that for every positive integer d there exist integers a and b such that $4a^2 + 9b^2 - 1$ is divisible by d.

Paper 4, Section II

5F Numbers and Sets

The Chebyshev polynomials are defined for $x \in \mathbb{R}$ by the recurrence relation

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_{n+1}(x) &= 2xT_n(x) - T_{n-1}(x) \qquad \text{for } n \geqslant 1. \end{aligned}$$

(a) Prove that $T_n\big(\cos(y)\big) = \cos(ny)$ for all integers $n \geqslant 0$.

(b) Prove that $\cos(\pi/n)$ is algebraic for all integers $n \geqslant 1$.

(c) For each integer $n \geqslant 1$, determine whether $\cos(\pi/n)$ is rational or not. [*Hint: After stating the known answers for small n, it is useful to consider the form of $T_n(x)$ for odd n.*]

(d) In each of the following cases, prove that the sequence (a_n) is bounded and determine whether it has a limit:

(i) $a_n = \sum_{k=1}^{n} \big(1 - \cos(\pi/k)\big)$,

(ii) $a_n = \sum_{k=0}^{n} \cos(ky)$, with $\cos(y) \neq 1$.

Paper 4, Section II

6E Numbers and Sets

If p is a prime number, prove that $(p-1)! \equiv -1 \mod p$.

If $n > 4$ is a composite number, prove that $(n-1)! \equiv 0 \mod n$.

State the Fermat–Euler theorem and deduce from it Fermat's little theorem.

If p is any prime, prove that if $a \equiv b \mod p$, then $a^{p^n} \equiv b^{p^n} \mod p^{n+1}$ for all integers $n \geqslant 1$.

Let $a > 1$ be an integer. A *pseudo-prime of base a* is a composite number $n > 1$ satisfying $a^{n-1} \equiv 1 \mod n$. By considering the numbers $\dfrac{a^{2p}-1}{a^2-1}$, where p is prime, or otherwise, prove that for each a there are infinitely many pseudo-primes of base a.

Paper 4, Section II

7D Numbers & Sets

(a) Let X be a set and let $f : X \to X$ be an injective function. Show that $f^n : X \to X$ is injective, where f^n denotes the n-fold composite of f with itself.

The image of f is given by $\{f(x) : x \in X\}$ and denoted $f(X)$. Show that

$$X \supseteq f(X) \supseteq f^2(X) \supseteq f^3(X) \supseteq \cdots$$

Suppose there exists $k \in \mathbb{N}$ such that $f^k(X) = f^{k+1}(X)$. Show that $f^k(X) = f^{k+m}(X)$ for all $m \in \mathbb{N}$. Hence, or otherwise, find a subset A of X such that $f : A \to A$ is bijective.

(b) Let $X = \{x_1, x_2, \ldots, x_n\}$ and let W_k be the set of words in elements of X of length k, that is $W_k = \{w_1 \ldots w_k : w_i \in X \text{ for } 1 \leqslant i \leqslant k\}$. Let P_n be the set of bijections $f : X \to X$. We define a relation $\sim$ on W_k as follows. Suppose $w, z \in W_k$, then $w \sim z$ if and only if there exists $f \in P_n$ such that $w_1 \ldots w_k = f(z_1) \ldots f(z_k)$, where $w = w_1 \ldots w_k$ and $z = z_1 \ldots z_k$. Show that $\sim$ defines an equivalence relation on W_k.

List the equivalence classes of W_3 for each $n \in \mathbb{N}$.

List the equivalence classes of W_4 when $n = 3$.

Let $n = 4$ and $g \in P_4$ be such that

$$g : x_1 \mapsto x_2,\ x_2 \mapsto x_3,\ x_3 \mapsto x_4 \text{ and } x_4 \mapsto x_1.$$

Let $F = \{g, g^2, g^3, g^4\}$. We define a new equivalence relation $\underset{F}{\sim}$ on W_k. Suppose $w, z \in W_k$, then $w \underset{F}{\sim} z$ if and only if there exists $f \in F$ such that $w_1 \ldots w_k = f(z_1) \ldots f(z_k)$. Are the equivalence classes of W_3 under $\underset{F}{\sim}$ the same as the equivalence classes under $\sim$? Justify your answer. [You may assume that $\underset{F}{\sim}$ is an equivalence relation.]

Paper 4, Section II

8D Numbers & Sets

Prove that a countable union of countable sets is countable.

Infinite binary sequences are sequences of the form $a_1a_2a_3\ldots$, where $a_i \in \{0,1\}$ for $i \in \mathbb{N}$. Are the sets consisting of the following countable? Justify your answers.

(i) All infinite binary sequences.

(ii) Infinite binary sequences with either a finite number of $1s$ or a finite number of $0s$.

(iii) Infinite binary sequences with infinitely many $1s$ and infinitely many $0s$.

A function $f : \mathbb{Z} \to \mathbb{N}$ is called *periodic* if there exists a positive integer k such that $f(x+k) = f(x)$ for every $x \in \mathbb{Z}$. Is the set of periodic functions $f : \mathbb{Z} \to \mathbb{N}$ countable? Justify your answer.

Is the set of bijections from $\mathbb{N}$ to $\mathbb{N}$ countable? Justify your answer.

Paper 4, Section I
1E Numbers and Sets

By considering numbers of the form $3p_1 \dots p_k - 1$, show that there are infinitely many primes of the form $3n + 2$ with $n \in \mathbb{N}$.

For which primes p is the number $2p^2 + 1$ also prime? Justify your answer.

Paper 4, Section I
2D Numbers and Sets

Prove that $\sqrt[3]{2} + \sqrt[3]{3}$ is irrational.

Using the fact that the number $e - e^{-1}$ can be represented by a convergent series $2\sum_{n=0}^{\infty} \frac{1}{(2n+1)!}$, prove that $e - e^{-1}$ is irrational.

What is a *transcendental* number? Given that e is transcendental, show that $ae + be^{-1}$ is also transcendental for any integers a, b that are not both zero.

Paper 4, Section II
5E Numbers and Sets

State Bezout's theorem. Suppose that $p \in \mathbb{N}$ is prime and $a, b \in \mathbb{N}$. Show that if p divides ab then p divides a or p divides b.

Show that if $m, n \in \mathbb{N}$ are coprime then any pair of congruences of the form

$$x \equiv a \mod m \quad \text{and} \quad x \equiv b \mod n$$

has a unique simultaneous solution modulo mn.

Show that if p is an odd prime and $d \in \mathbb{N}$ then there are precisely 2 solutions of $x^2 \equiv 1$ modulo p^d. Deduce that if $n \geqslant 3$ is odd, then the number of solutions of $x^2 \equiv 1$ modulo n is equal to 2^k, where k denotes the number of distinct prime factors of n.

How many solutions of $x^2 \equiv 1$ modulo n are there when $n = 2^d$?

Paper 4, Section II
6D Numbers and Sets

(a) Define the binomial coefficient $\binom{n}{k}$ for $0 \leqslant k \leqslant n$. Show from your definition that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ holds when both sides are well-defined.

(b) Prove the following special case of the binomial theorem: $(1+t)^n = \sum_{k=0}^{n} \binom{n}{k} t^k$ for any real number t. By integrating this expression over a suitable range, or otherwise, evaluate $\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k}$ and $\sum_{k=0}^{n} \frac{(-1)^k}{k+1}\binom{n}{k}$.

Deduce that $\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k}\binom{n}{k} = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$.

(c) The Fibonacci numbers are defined by

$$F_1 = 1, \qquad F_2 = 1, \qquad F_{n+2} = F_{n+1} + F_n \quad \text{for } n \geqslant 1.$$

By using induction, or otherwise, prove that

$$F_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-k-1}{k}$$

for all $n \geqslant 1$, where $\lfloor \frac{n-1}{2} \rfloor$ denotes the largest integer less than or equal to $\frac{n-1}{2}$.

Paper 4, Section II
7F Numbers and Sets

For a given natural number $n \geqslant 2$, let S be the set of ordered real n-tuples $x = (x_1, \ldots, x_n)$ where $x_i \geqslant 0$ for $1 \leqslant i \leqslant n$. For $x \in S$, let

$$P(x) = \{i : x_i > 0\}.$$

Define the relation $\preceq$ by

$$x \preceq y \text{ if and only if } P(x) \subseteq P(y).$$

(a) Is the relation $\preceq$ reflexive? Is it transitive? Is it symmetric? Justify your answers.

(b) Show that $x \preceq y$ if and only if there exists $z \in S$ such that $x_i = y_i z_i$ for all $1 \leqslant i \leqslant n$.

(c) Define the relation $\sim$ by

$$x \sim y \text{ if and only if } x \preceq y \text{ and } y \preceq x.$$

Show that $\sim$ defines an equivalence relation on S. Into how many equivalence classes does $\sim$ partition S?

(d) Define the relation $\perp$ by

$$x \perp y \text{ if and only if } P(x) \cap P(y) = \emptyset.$$

Given $s \in S$, show that for every $x \in S$ there exist unique $y, z \in S$ such that $x = y + z$ where $y \preceq s$ and $z \perp s$.

Paper 4, Section II
8F Numbers and Sets

(a) What does it mean to say a set is *countable*?

(b) Show from first principles that the following sets are countable:

(i) the Cartesian product $\mathbb{N} \times \mathbb{N}$, where $\mathbb{N} = \{1, 2, \ldots\}$ is the set of natural numbers,

(ii) the rational numbers,

(iii) the points of discontinuity of an increasing function $F : \mathbb{R} \to \mathbb{R}$.

(c) Let $A_1, A_2, \ldots$ be a collection of non-empty countable sets and consider the Cartesian product

$$B = A_1 \times A_2 \times \cdots.$$

Show from first principles that B is countable if and only if there exists a natural number N such that $|A_n| = 1$ for all $n > N$.

Paper 4, Section I
1E Numbers and Sets

Consider functions $f : X \to Y$ and $g : Y \to X$. Which of the following statements are always true, and which can be false? Give proofs or counterexamples as appropriate.

(i) If $g \circ f$ is surjective then f is surjective.

(ii) If $g \circ f$ is injective then f is injective.

(iii) If $g \circ f$ is injective then g is injective.

If $X = \{1, \ldots, m\}$ and $Y = \{1, \ldots, n\}$ with $m < n$, and $g \circ f$ is the identity on X, then how many possibilities are there for the pair of functions f and g?

Paper 4, Section I
2E Numbers and Sets

The *Fibonacci numbers* F_n are defined by $F_1 = 1$, $F_2 = 1$, $F_{n+2} = F_{n+1} + F_n$ $(n \geqslant 1)$. Let $a_n = F_{n+1}/F_n$ be the ratio of successive Fibonacci numbers.

(i) Show that $a_{n+1} = 1 + 1/a_n$. Hence prove by induction that

$$(-1)^n a_{n+2} \leqslant (-1)^n a_n$$

for all $n \geqslant 1$. Deduce that the sequence a_{2n} is monotonically decreasing.

(ii) Prove that

$$F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$$

for all $n \geqslant 1$. Hence show that $a_{n+1} - a_n \to 0$ as $n \to \infty$.

(iii) Explain without detailed justification why the sequence a_n has a limit.

Paper 4, Section II

5E Numbers and Sets

(a) Let S be the set of all functions $f : \mathbb{N} \to \mathbb{R}$. Define $\delta : S \to S$ by

$$(\delta f)(n) = f(n+1) - f(n)\,.$$

(i) Define the binomial coefficient $\binom{n}{r}$ for $0 \leqslant r \leqslant n$. Setting $\binom{n}{r} = 0$ when $r > n$, prove from your definition that if $f_r(n) = \binom{n}{r}$ then $\delta f_r = f_{r-1}$.

(ii) Show that if $f \in S$ is integer-valued and $\delta^{k+1} f = 0$, then

$$f(n) = c_0 \binom{n}{k} + c_1 \binom{n}{k-1} + \cdots + c_{k-1} \binom{n}{1} + c_k$$

for some integers $c_0, \ldots, c_k$.

(b) State the binomial theorem. Show that

$$\sum_{r=0}^{n} (-1)^r \binom{n}{r}^2 = \begin{cases} 0 & \text{if } n \text{ is odd} \\ (-1)^{n/2} \binom{n}{n/2} & \text{if } n \text{ is even} \end{cases}\,.$$

Paper 4, Section II

6E Numbers and Sets

(a) (i) By considering Euclid's algorithm, show that the highest common factor of two positive integers a and b can be written in the form $\alpha a+\beta b$ for suitable integers α and β. Find an integer solution of

$$15x + 21y + 35z = 1\,.$$

Is your solution unique?

(ii) Suppose that n and m are coprime. Show that the simultaneous congruences

$$\begin{aligned} x &\equiv a \pmod{n}\,, \\ x &\equiv b \pmod{m} \end{aligned}$$

have the same set of solutions as $x \equiv c \pmod{mn}$ for some $c \in \mathbb{N}$. Hence solve (i.e. find all solutions of) the simultaneous congruences

$$\begin{aligned} 3x &\equiv 1 \pmod{5}\,, \\ 5x &\equiv 1 \pmod{7}\,, \\ 7x &\equiv 1 \pmod{3}\,. \end{aligned}$$

(b) State the inclusion–exclusion principle.

For integers $r, n \geqslant 1$, denote by $\phi_r(n)$ the number of ordered r-tuples $(x_1, \ldots, x_r)$ of integers x_i satisfying $1 \leqslant x_i \leqslant n$ for $i = 1, \ldots, r$ and such that the greatest common divisor of $\{n, x_1, \ldots, x_r\}$ is 1. Show that

$$\phi_r(n) = n^r \prod_{p|n} (1 - \frac{1}{p^r})$$

where the product is over all prime numbers p dividing n.

Paper 4, Section II

7E Numbers and Sets

(a) Prove that every real number $\alpha \in (0,1]$ can be written in the form $\alpha = \sum_{n=1}^{\infty} 2^{-b_n}$ where (b_n) is a strictly increasing sequence of positive integers.

Are such expressions unique?

(b) Let $\theta \in \mathbb{R}$ be a root of $f(x) = \alpha_d x^d + \cdots + \alpha_1 x + \alpha_0$, where $\alpha_0, \ldots, \alpha_d \in \mathbb{Z}$. Suppose that f has no rational roots, except possibly θ.

(i) Show that if $s, t \in \mathbb{R}$ then

$$|f(s) - f(t)| \leqslant A(\max\{|s|, |t|, 1\})^{d-1}|s-t|\,.$$

where A is a constant depending only on f.

(ii) Deduce that if $p, q \in \mathbb{Z}$ with $q > 0$ and $0 < \left|\theta - \frac{p}{q}\right| < 1$ then

$$\left|\theta - \frac{p}{q}\right| \geqslant \frac{1}{A}\left(\frac{1}{|\theta|+1}\right)^{d-1} \frac{1}{q^d}\,.$$

(c) Prove that $\alpha = \sum_{n=1}^{\infty} 2^{-n!}$ is transcendental.

(d) Let β and γ be transcendental numbers. What of the following statements are always true and which can be false? Briefly justify your answers.

(i) $\beta\gamma$ is transcendental.

(ii) β^n is transcendental for every $n \in \mathbb{N}$.

Paper 4, Section II

8E Numbers and Sets

(a) Prove that a countable union of countable sets is countable.

(b) (i) Show that the set $\mathbb{N}^{\mathbb{N}}$ of all functions $\mathbb{N} \to \mathbb{N}$ is uncountable.

(ii) Determine the countability or otherwise of each of the two sets

$$A = \{f \in \mathbb{N}^{\mathbb{N}} : f(n) \leqslant f(n+1) \text{ for all } n \in \mathbb{N}\},$$
$$B = \{f \in \mathbb{N}^{\mathbb{N}} : f(n) \geqslant f(n+1) \text{ for all } n \in \mathbb{N}\}.$$

Justify your answers.

(c) A *permutation* σ of the natural numbers $\mathbb{N}$ is a mapping $\sigma \in \mathbb{N}^{\mathbb{N}}$ that is bijective. Determine the countability or otherwise of each of the two sets C and D of permutations, justifying your answers:

(i) C is the set of all permutations σ of $\mathbb{N}$ such that $\sigma(j) = j$ for all sufficiently large j.

(ii) D is the set all permutations σ of $\mathbb{N}$ such that

$$\sigma(j) = j - 1 \text{ or } j \text{ or } j + 1$$

for each j.

Paper 2, Section I

2D Numbers and Sets

Define an *equivalence relation*. Which of the following is an equivalence relation on the set of non-zero complex numbers? Justify your answers.

(i) $x \sim y$ if $|x-y|^2 < |x|^2 + |y|^2$.

(ii) $x \sim y$ if $|x+y| = |x| + |y|$.

(iii) $x \sim y$ if $\left|\dfrac{x}{y^n}\right|$ is rational for some integer $n \geqslant 1$.

(iv) $x \sim y$ if $|x^3 - x| = |y^3 - y|$.

Paper 2, Section II

7D Numbers and Sets

(a) Define the *Euler function* $\phi(n)$. State the Chinese remainder theorem, and use it to derive a formula for $\phi(n)$ when $n = p_1 p_2 \ldots p_r$ is a product of distinct primes. Show that there are at least ten odd numbers n with $\phi(n)$ a power of 2.

(b) State and prove the Fermat–Euler theorem.

(c) In the RSA cryptosystem a message $m \in \{1, 2, \ldots, N-1\}$ is encrypted as $c = m^e \pmod{N}$. Explain how N and e should be chosen, and how (given a factorisation of N) to compute the decryption exponent d. Prove that your choice of d works, subject to reasonable assumptions on m. If $N = 187$ and $e = 13$ then what is d?

Paper 2, Section II

8D Numbers and Sets

(a) Define what it means for a set to be *countable*. Prove that $\mathbb{N} \times \mathbb{Z}$ is countable, and that the power set of $\mathbb{N}$ is uncountable.

(b) Let $\sigma : X \to Y$ be a bijection. Show that if $f : X \to X$ and $g : Y \to Y$ are related by $g = \sigma f \sigma^{-1}$ then they have the same number of fixed points.

[A *fixed point* of f is an element $x \in X$ such that $f(x) = x$.]

(c) Let T be the set of bijections $f : \mathbb{N} \to \mathbb{N}$ with the property that no iterate of f has a fixed point.

[The k^{th} *iterate* of f is the map obtained by k successive applications of f.]

(i) Write down an explicit element of T.

(ii) Determine whether T is countable or uncountable.

Paper 4, Section I

1E Numbers and Sets

Find all solutions to the simultaneous congruences

$$4x \equiv 1 \pmod{21} \qquad \text{and} \qquad 2x \equiv 5 \pmod{45}.$$

Paper 4, Section I

2E Numbers and Sets

Show that the series

$$\sum_{n=1}^{\infty} \frac{1}{n^2+n} \qquad \text{and} \qquad \sum_{n=1}^{\infty} \frac{1}{(2n-1)!}$$

converge. Determine in each case whether the limit is a rational number. Justify your answers.

Paper 4, Section II

5E Numbers and Sets

(a) State and prove Fermat's theorem. Use it to compute $3^{803} \pmod{17}$.

(b) The *Fibonacci numbers* $F_0, F_1, F_2, \ldots$ are defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for all $n \geqslant 2$. Prove by induction that for all $n \geqslant 1$ we have

$$F_{2n} = F_n(F_{n-1} + F_{n+1}) \qquad \text{and} \qquad F_{2n+1} = F_n^2 + F_{n+1}^2.$$

(c) Let $m \geqslant 1$ and let p be an odd prime dividing F_m. Which of the following statements are true, and which can be false? Justify your answers.

(i) If m is odd then $p \equiv 1 \pmod 4$.

(ii) If m is even then $p \equiv 3 \pmod 4$.

Paper 4, Section II

6E Numbers and Sets

State the inclusion-exclusion principle.

Let $n \geqslant 2$ be an integer. Let $X = \{0, 1, 2, \ldots, n-1\}$ and

$$Y = \{(a, b) \in X^2 \,|\, \gcd(a, b, n) = 1\}$$

where $\gcd(x_1, \ldots, x_k)$ is the largest number dividing all of $x_1, \ldots, x_k$. Let R be the relation on Y where $(a, b)R(c, d)$ if $ad - bc \equiv 0 \pmod{n}$.

(a) Show that

$$|Y| = n^2 \prod_{p|n} \left(1 - \frac{1}{p^2}\right)$$

where the product is over all primes p dividing n.

(b) Show that if $\gcd(a, b, n) = 1$ then there exist integers r, s, t with $ra + sb + tn = 1$.

(c) Show that if $(a, b)R(c, d)$ then there exists an integer λ with $\lambda a \equiv c \pmod{n}$ and $\lambda b \equiv d \pmod{n}$. [*Hint: Consider $\lambda = rc + sd$, where r, s are as in part (b).*] Deduce that R is an equivalence relation.

(d) What is the size of the equivalence class containing $(1, 1)$? Show that all equivalence classes have the same size, and deduce that the number of equivalence classes is

$$n \prod_{p|n} \left(1 + \frac{1}{p}\right).$$

Paper 4, Section II

7E Numbers and Sets

(a) Let $f : X \to Y$ be a function. Show that the following statements are equivalent.

(i) f is injective.

(ii) For every subset $A \subset X$ we have $f^{-1}(f(A)) = A$.

(iii) For every pair of subsets $A, B \subset X$ we have $f(A \cap B) = f(A) \cap f(B)$.

(b) Let $f : X \to X$ be an injection. Show that $X = A \cup B$ for some subsets $A, B \subset X$ such that

$$\bigcap_{n=1}^{\infty} f^n(A) = \emptyset \qquad \text{and} \qquad f(B) = B.$$

[*Here f^n denotes the n-fold composite of f with itself.*]

Paper 4, Section II

8E Numbers and Sets

(a) What is a *countable set*? Let X, A, B be sets with A, B countable. Show that if $f : X \to A \times B$ is an injection then X is countable. Deduce that $\mathbb{Z}$ and $\mathbb{Q}$ are countable. Show too that a countable union of countable sets is countable.

(b) Show that, in the plane, any collection of pairwise disjoint circles with rational radius is countable.

(c) A *lollipop* is any subset of the plane obtained by translating, rotating and scaling (by any factor $\lambda > 0$) the set

$$\{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\} \cup \{(0, y) \in \mathbb{R}^2 | -3 \leqslant y \leqslant -1\}.$$

What happens if in part (b) we replace 'circles with rational radius' by 'lollipops'?

Paper 4, Section I

1E Numbers and Sets

State Fermat's theorem.

Let p be a prime such that $p \equiv 3 \pmod 4$. Prove that there is no solution to $x^2 \equiv -1 \pmod p$.

Show that there are infinitely many primes congruent to $1 \pmod 4$.

Paper 4, Section I

2E Numbers and Sets

Given $n \in \mathbb{N}$, show that $\sqrt{n}$ is either an integer or irrational.

Let α and β be irrational numbers and q be rational. Which of $\alpha + q$, $\alpha + \beta$, $\alpha\beta$, α^q and α^β *must* be irrational? Justify your answers. [*Hint: For the last part consider* $\sqrt{2}^{\sqrt{2}}$.]

Paper 4, Section II

5E Numbers and Sets

Let n be a positive integer. Show that for any a coprime to n, there is a unique $b \pmod n$ such that $ab \equiv 1 \pmod n$. Show also that if a and b are integers coprime to n, then ab is also coprime to n. [Any version of Bezout's theorem may be used without proof provided it is clearly stated.]

State and prove Wilson's theorem.

Let n be a positive integer and p be a prime. Show that the exponent of p in the prime factorisation of $n!$ is given by $\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$ where $\lfloor x \rfloor$ denotes the integer part of x.

Evaluate $20! \pmod{23}$ and $1000! \pmod{10^{249}}$.

Let p be a prime and $0 < k < p^m$. Let ℓ be the exponent of p in the prime factorisation of k. Find the exponent of p in the prime factorisation of $\binom{p^m}{k}$, in terms of m and ℓ.

Paper 4, Section II

6E Numbers and Sets

For $n \in \mathbb{N}$ let $Q_n = \{0,1\}^n$ denote the set of all 0-1 sequences of length n. We define the *distance* $d(x,y)$ between two elements x and y of Q_n to be the number of coordinates in which they differ. Show that $d(x,z) \leqslant d(x,y) + d(y,z)$ for all $x,y,z \in Q_n$.

For $x \in Q_n$ and $1 \leqslant j \leqslant n$ let $B(x,j) = \{y \in Q_n : d(y,x) \leqslant j\}$. Show that $|B(x,j)| = \sum_{i=0}^{j} \binom{n}{i}$.

A subset C of Q_n is called a *k-code* if $d(x,y) \geqslant 2k+1$ for all $x,y \in C$ with $x \neq y$. Let $M(n,k)$ be the maximum possible value of $|C|$ for a k-code C in Q_n. Show that

$$2^n \left(\sum_{i=0}^{2k} \binom{n}{i} \right)^{-1} \leqslant M(n,k) \leqslant 2^n \left(\sum_{i=0}^{k} \binom{n}{i} \right)^{-1} .$$

Find $M(4,1)$, carefully justifying your answer.

Paper 4, Section II

7E Numbers and Sets

Let $n \in \mathbb{N}$ and $A_1, \ldots, A_n$ be subsets of a finite set X. Let $0 \leqslant t \leqslant n$. Show that if $x \in X$ belongs to A_i for exactly m values of i, then

$$\sum_{S \subset \{1,\ldots,n\}} \binom{|S|}{t} (-1)^{|S|-t} \mathbf{1}_{A_S}(x) = \begin{cases} 0 & \text{if } m \neq t \\ 1 & \text{if } m = t \end{cases}$$

where $A_S = \bigcap_{i \in S} A_i$ with the convention that $A_\emptyset = X$, and $\mathbf{1}_{A_S}$ denotes the indicator function of A_S. [*Hint: Set $M = \{i : x \in A_i\}$ and consider for which $S \subset \{1,\ldots,n\}$ one has $\mathbf{1}_{A_S}(x) = 1$.*]

Use this to show that the number of elements of X that belong to A_i for exactly t values of i is

$$\sum_{S \subset \{1,\ldots,n\}} \binom{|S|}{t} (-1)^{|S|-t} |A_S| .$$

Deduce the Inclusion-Exclusion Principle.

Using the Inclusion-Exclusion Principle, prove a formula for the Euler totient function $\varphi(N)$ in terms of the distinct prime factors of N.

A *Carmichael number* is a composite number n such that $x^{n-1} \equiv 1 \pmod{n}$ for every integer x coprime to n. Show that if $n = q_1 q_2 \ldots q_k$ is the product of $k \geqslant 2$ distinct primes $q_1, \ldots, q_k$ satisfying $q_j - 1 \mid n - 1$ for $j = 1, \ldots, k$, then n is a Carmichael number.

Paper 4, Section II

8E Numbers and Sets

Define what it means for a set to be *countable*.

Show that for any set X, there is no surjection from X onto the power set $\mathcal{P}(X)$. Deduce that the set $\{0,1\}^{\mathbb{N}}$ of all infinite 0-1 sequences is uncountable.

Let $\mathcal{L}$ be the set of sequences $(F_n)_{n=0}^{\infty}$ of subsets $F_0 \subset F_1 \subset F_2 \subset \ldots$ of $\mathbb{N}$ such that $|F_n| = n$ for all $n \in \mathbb{N}$ and $\bigcup_n F_n = \mathbb{N}$. Let $\mathcal{L}_0$ consist of all members $(F_n)_{n=0}^{\infty}$ of $\mathcal{L}$ for which $n \in F_n$ for all but finitely many $n \in \mathbb{N}$. Let $\mathcal{L}_1$ consist of all members $(F_n)_{n=0}^{\infty}$ of $\mathcal{L}$ for which $n \in F_{n+1}$ for all but finitely many $n \in \mathbb{N}$. For each of $\mathcal{L}_0$ and $\mathcal{L}_1$ determine whether it is countable or uncountable. Justify your answers.

Paper 4, Section I
1D Numbers and Sets

(a) Show that for all positive integers z and n, either $z^{2n} \equiv 0 \pmod 3$ or $z^{2n} \equiv 1 \pmod 3$.

(b) If the positive integers x, y, z satisfy $x^2 + y^2 = z^2$, show that at least one of x and y must be divisible by 3. Can both x and y be odd?

Paper 4, Section I
2D Numbers and Sets

(a) Give the definitions of *relation* and *equivalence relation* on a set S.

(b) Let Σ be the set of ordered pairs (A, f) where A is a non-empty subset of $\mathbb{R}$ and $f : A \to \mathbb{R}$. Let $\mathcal{R}$ be the relation on Σ defined by requiring $(A, f)\, \mathcal{R}\, (B, g)$ if the following two conditions hold:

(i) $(A \setminus B) \cup (B \setminus A)$ is finite and

(ii) there is a finite set $F \subset A \cap B$ such that $f(x) = g(x)$ for all $x \in A \cap B \setminus F$.

Show that $\mathcal{R}$ is an equivalence relation on Σ.

Paper 4, Section II
5D Numbers and Sets

(a) State and prove the Fermat–Euler Theorem. Deduce Fermat's Little Theorem. State Wilson's Theorem.

(b) Let p be an odd prime. Prove that $X^2 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{4}$.

(c) Let p be prime. If h and k are non-negative integers with $h + k = p - 1$, prove that $h!k! + (-1)^h \equiv 0 \pmod{p}$.

Paper 4, Section II
6D Numbers and Sets

(a) Define what it means for a set to be *countable*.

(b) Let A be an infinite subset of the set of natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$. Prove that there is a bijection $f : \mathbb{N} \to A$.

(c) Let A_n be the set of natural numbers whose decimal representation ends with exactly $n - 1$ zeros. For example, $71 \in A_1$, $70 \in A_2$ and $15000 \in A_4$. By applying the result of part (b) with $A = A_n$, construct a bijection $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Deduce that the set of rationals is countable.

(d) Let A be an infinite set of positive real numbers. If every sequence $(a_j)_{j=1}^{\infty}$ of distinct elements with $a_j \in A$ for each j has the property that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} a_j = 0,$$

prove that A is countable.

[*You may assume without proof that a countable union of countable sets is countable.*]

Paper 4, Section II

7D Numbers and Sets

(a) For positive integers n, m, k with $k \leqslant n$, show that

$$\binom{n}{k}\left(\frac{k}{n}\right)^m = \binom{n-1}{k-1}\sum_{\ell=0}^{m-1} a_{n,m,\ell}\left(\frac{k-1}{n-1}\right)^{m-1-\ell}$$

giving an explicit formula for $a_{n,m,\ell}$. [You may wish to consider the expansion of $\left(\frac{k-1}{n-1}+\frac{1}{n-1}\right)^{m-1}$.]

(b) For a function $f : [0,1] \to \mathbb{R}$ and each integer $n \geqslant 1$, the function $B_n(f) : [0,1] \to \mathbb{R}$ is defined by

$$B_n(f)(x) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k}x^k(1-x)^{n-k}.$$

For any integer $m \geqslant 0$ let $f_m(x) = x^m$. Show that $B_n(f_0)(x) = 1$ and $B_n(f_1)(x) = x$ for all $n \geqslant 1$ and $x \in [0,1]$.

Show that for each integer $m \geqslant 0$ and each $x \in [0,1]$,

$$B_n(f_m)(x) \to f_m(x) \quad \text{as} \quad n \to \infty\,.$$

Deduce that for each integer $m \geqslant 0$,

$$\lim_{n\to\infty} \frac{1}{4^n}\sum_{k=0}^{2n}\left(\frac{k}{n}\right)^m\binom{2n}{k} = 1.$$

Paper 4, Section II

8D Numbers and Sets

Let $(a_k)_{k=1}^{\infty}$ be a sequence of real numbers.

(a) Define what it means for $(a_k)_{k=1}^{\infty}$ to converge. Define what it means for the series $\sum_{k=1}^{\infty} a_k$ to converge.

Show that if $\sum_{k=1}^{\infty} a_k$ converges, then $(a_k)_{k=1}^{\infty}$ converges to 0.

If $(a_k)_{k=1}^{\infty}$ converges to $a \in \mathbb{R}$, show that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} a_k = a\,.$$

(b) Suppose $a_k > 0$ for every k. Let $u_n = \displaystyle\sum_{k=1}^{n} \left(a_k + \frac{1}{a_k}\right)$ and $v_n = \displaystyle\sum_{k=1}^{n} \left(a_k - \frac{1}{a_k}\right)$.

Show that $(u_n)_{n=1}^{\infty}$ does not converge.

Give an example of a sequence $(a_k)_{k=1}^{\infty}$ with $a_k > 0$ and $a_k \neq 1$ for every k such that $(v_n)_{n=1}^{\infty}$ converges.

If $(v_n)_{n=1}^{\infty}$ converges, show that $\dfrac{u_n}{n} \to 2$.

Paper 4, Section I
1E Numbers and Sets

Find a pair of integers x and y satisfying $17x + 29y = 1$. What is the smallest positive integer congruent to 17^{138} modulo 29?

Paper 4, Section I
2E Numbers and Sets

Explain the meaning of the phrase *least upper bound;* state the least upper bound property of the real numbers. Use the least upper bound property to show that a bounded, increasing sequence of real numbers converges.

Suppose that $a_n, b_n \in \mathbb{R}$ and that $a_n \geqslant b_n > 0$ for all n. If $\sum_{n=1}^{\infty} a_n$ converges, show that $\sum_{n=1}^{\infty} b_n$ converges.

Paper 4, Section II
5E Numbers and Sets

(a) Let S be a set. Show that there is no bijective map from S to the power set of S. Let $\mathcal{T} = \{(x_n) \,|\, x_i \in \{0,1\} \text{ for all } i \in \mathbb{N}\}$ be the set of sequences with entries in $\{0,1\}$. Show that $\mathcal{T}$ is uncountable.

(b) Let A be a finite set with more than one element, and let B be a countably infinite set. Determine whether each of the following sets is countable. Justify your answers.

(i) $S_1 = \{f : A \to B \,|\, f \text{ is injective}\}$.

(ii) $S_2 = \{g : B \to A \,|\, g \text{ is surjective}\}$.

(iii) $S_3 = \{h : B \to B \,|\, h \text{ is bijective}\}$.

Paper 4, Section II
6E Numbers and Sets

Suppose that $a, b \in \mathbb{Z}$ and that $b = b_1 b_2$, where b_1 and b_2 are relatively prime and greater than 1. Show that there exist unique integers $a_1, a_2, n \in \mathbb{Z}$ such that $0 \leqslant a_i < b_i$ and

$$\frac{a}{b} = \frac{a_1}{b_1} + \frac{a_2}{b_2} + n.$$

Now let $b = p_1^{n_1} \dots p_k^{n_k}$ be the prime factorization of b. Deduce that $\frac{a}{b}$ can be written uniquely in the form

$$\frac{a}{b} = \frac{q_1}{p_1^{n_1}} + \cdots + \frac{q_k}{p_k^{n_k}} + n\,,$$

where $0 \leqslant q_i < p_i^{n_i}$ and $n \in \mathbb{Z}$. Express $\frac{a}{b} = \frac{1}{315}$ in this form.

Paper 4, Section II
7E Numbers and Sets

State the inclusion-exclusion principle.

Let $A = (a_1, a_2, \dots, a_n)$ be a string of n digits, where $a_i \in \{0, 1, \dots, 9\}$. We say that the string A has a run of length k if there is some $j \leqslant n - k + 1$ such that either $a_{j+i} \equiv a_j + i \pmod{10}$ for all $0 \leqslant i < k$ or $a_{j+i} \equiv a_j - i \pmod{10}$ for all $0 \leqslant i < k$. For example, the strings

$$(\underline{0, 1, 2}, 8, 4, 9),\ (3, \underline{9, 8, 7}, 4, 8) \text{ and } (3, \underline{1, 0, 9}, 4, 5)$$

all have runs of length 3 (underlined), but no run in $(3, 1, 2, 1, 1, 2)$ has length > 2. How many strings of length 6 have a run of length $\geqslant 3$?

Paper 4, Section II

8E Numbers and Sets

Define the binomial coefficient $\binom{n}{m}$. Prove directly from your definition that

$$(1+z)^n = \sum_{m=0}^{n} \binom{n}{m} z^m$$

for any complex number z.

(a) Using this formula, or otherwise, show that

$$\sum_{k=0}^{3n} (-3)^k \binom{6n}{2k} = 2^{6n}.$$

(b) By differentiating, or otherwise, evaluate $\displaystyle\sum_{m=0}^{n} m \binom{n}{m}$.

Let $S_r(n) = \displaystyle\sum_{m=0}^{n} (-1)^m m^r \binom{n}{m}$, where r is a non-negative integer. Show that $S_r(n) = 0$ for $r < n$. Evaluate $S_n(n)$.

Paper 4, Section I

1E Numbers and Sets

(a) Find all integers x and y such that

$$6x + 2y \equiv 3 \pmod{53} \qquad \text{and} \qquad 17x + 4y \equiv 7 \pmod{53}.$$

(b) Show that if an integer $n > 4$ is composite then $(n-1)! \equiv 0 \pmod{n}$.

Paper 4, Section I

2E Numbers and Sets

State the Chinese remainder theorem and Fermat's theorem. Prove that

$$p^4 \equiv 1 \pmod{240}$$

for any prime $p > 5$.

Paper 4, Section II

5E Numbers and Sets

(i) Let $\sim$ be an equivalence relation on a set X. What is an *equivalence class* of $\sim$? What is a *partition* of X? Prove that the equivalence classes of $\sim$ form a partition of X.

(ii) Let $\sim$ be the relation on the natural numbers defined by

$$m \sim n \iff \exists\, a, b \in \mathbb{N} \text{ such that } m \text{ divides } n^a \text{ and } n \text{ divides } m^b.$$

Show that $\sim$ is an equivalence relation, and show that it has infinitely many equivalence classes, all but one of which are infinite.

Paper 4, Section II

6E Numbers and Sets

Let p be a prime. A *base p expansion* of an integer k is an expression

$$k = k_0 + p \cdot k_1 + p^2 \cdot k_2 + \cdots + p^\ell \cdot k_\ell$$

for some natural number ℓ, with $0 \leqslant k_i < p$ for $i = 0, 1, \ldots, \ell$.

(i) Show that the sequence of coefficients $k_0, k_1, k_2, \ldots, k_\ell$ appearing in a base p expansion of k is unique, up to extending the sequence by zeroes.

(ii) Show that

$$\binom{p}{j} \equiv 0 \pmod{p}, \quad 0 < j < p,$$

and hence, by considering the polynomial $(1+x)^p$ or otherwise, deduce that

$$\binom{p^i}{j} \equiv 0 \pmod{p}, \quad 0 < j < p^i.$$

(iii) If $n_0 + p \cdot n_1 + p^2 \cdot n_2 + \cdots + p^\ell \cdot n_\ell$ is a base p expansion of n, then, by considering the polynomial $(1+x)^n$ or otherwise, show that

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1} \cdots \binom{n_\ell}{k_\ell} \pmod{p}.$$

Paper 4, Section II

7E Numbers and Sets

State the inclusion–exclusion principle.

Let $n \in \mathbb{N}$. A permutation σ of the set $\{1, 2, 3, \ldots, n\}$ is said to *contain a transposition* if there exist i, j with $1 \leqslant i < j \leqslant n$ such that $\sigma(i) = j$ and $\sigma(j) = i$. Derive a formula for the number, $f(n)$, of permutations which do not contain a transposition, and show that

$$\lim_{n \to \infty} \frac{f(n)}{n!} = e^{-\frac{1}{2}}.$$

Paper 4, Section II

8E Numbers and Sets

What does it mean for a set to be *countable*? Prove that

(a) if B is countable and $f\colon A \to B$ is injective, then A is countable;

(b) if A is countable and $f\colon A \to B$ is surjective, then B is countable.

Prove that $\mathbb{N} \times \mathbb{N}$ is countable, and deduce that

(i) if X and Y are countable, then so is $X \times Y$;

(ii) $\mathbb{Q}$ is countable.

Let $\mathcal{C}$ be a collection of circles in the plane such that for each point a on the x-axis, there is a circle in $\mathcal{C}$ passing through the point a which has the x-axis tangent to the circle at a. Show that $\mathcal{C}$ contains a pair of circles that intersect.

Paper 4, Section I

1E Numbers and Sets

Use Euclid's algorithm to determine d, the greatest common divisor of 203 and 147, and to express it in the form $203x + 147y$ for integers x, y. Hence find all solutions in integers x, y of the equation $203x + 147y = d$.

How many integers n are there with $1 \leqslant n \leqslant 2014$ and $21n \equiv 25 \pmod{29}$?

Paper 4, Section I

2E Numbers and Sets

Define the binomial coefficients $\binom{n}{k}$, for integers n, k satisfying $n \geqslant k \geqslant 0$. Prove directly from your definition that if $n > k \geqslant 0$ then

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

and that for every $m \geqslant 0$ and $n \geqslant 0$,

$$\sum_{k=0}^{m} \binom{n+k}{k} = \binom{n+m+1}{m}.$$

Paper 4, Section II

5E Numbers and Sets

What does it mean to say that the sequence of real numbers (x_n) converges to the limit x? What does it mean to say that the series $\sum_{n=1}^{\infty} x_n$ converges to s?

Let $\sum_{n=1}^{\infty} a_n$ and $\sum_{n=1}^{\infty} b_n$ be convergent series of positive real numbers. Suppose that (x_n) is a sequence of positive real numbers such that for every $n \geqslant 1$, either $x_n \leqslant a_n$ or $x_n \leqslant b_n$. Show that $\sum_{n=1}^{\infty} x_n$ is convergent.

Show that $\sum_{n=1}^{\infty} 1/n^2$ is convergent, and that $\sum_{n=1}^{\infty} 1/n^{\alpha}$ is divergent if $\alpha \leqslant 1$.

Let (x_n) be a sequence of positive real numbers such that $\sum_{n=1}^{\infty} n^2 x_n^2$ is convergent. Show that $\sum_{n=1}^{\infty} x_n$ is convergent. Determine (with proof or counterexample) whether or not the converse statement holds.

Paper 4, Section II

6E Numbers and Sets

(i) State and prove the Fermat–Euler Theorem.

(ii) Let p be an odd prime number, and x an integer coprime to p. Show that $x^{(p-1)/2} \equiv \pm 1 \pmod{p}$, and that if the congruence $y^2 \equiv x \pmod{p}$ has a solution then $x^{(p-1)/2} \equiv 1 \pmod{p}$.

(iii) By arranging the residue classes coprime to p into pairs $\{a, bx\}$ with $ab \equiv 1 \pmod{p}$, or otherwise, show that if the congruence $y^2 \equiv x \pmod{p}$ has no solution then $x^{(p-1)/2} \equiv -1 \pmod{p}$.

(iv) Show that $5^{5^5} \equiv 5 \pmod{23}$.

Paper 4, Section II

7E Numbers and Sets

(i) What does it mean to say that a set X is countable? Show directly that the set of sequences $(x_n)_{n\in\mathbb{N}}$, with $x_n \in \{0,1\}$ for all n, is uncountable.

(ii) Let S be any subset of $\mathbb{N}$. Show that there exists a bijection $f\colon \mathbb{N} \to \mathbb{N}$ such that $f(S) = 2\mathbb{N}$ (the set of even natural numbers) if and only if both S and its complement are infinite.

(iii) Let $\sqrt{2} = 1{\cdot}a_1a_2a_3\ldots$ be the binary expansion of $\sqrt{2}$. Let X be the set of all sequences (x_n) with $x_n \in \{0,1\}$ such that for infinitely many n, $x_n = 0$. Let Y be the set of all $(x_n) \in X$ such that for infinitely many n, $x_n = a_n$. Show that Y is uncountable.

Paper 4, Section II

8E Numbers and Sets

(i) State and prove the Inclusion–Exclusion Principle.

(ii) Let $n > 1$ be an integer. Denote by $\mathbb{Z}/n\mathbb{Z}$ the integers modulo n. Let X be the set of all functions $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that for every $j \in \mathbb{Z}/n\mathbb{Z}$, $f(j) - f(j-1) \not\equiv j \pmod{n}$. Show that

$$|X| = \begin{cases} (n-1)^n + 1 - n & \text{if } n \text{ is odd,} \\ (n-1)^n - 1 & \text{if } n \text{ is even.} \end{cases}$$

Paper 4, Section I

1E Numbers and Sets

Let m and n be positive integers. State what is meant by the *greatest common divisor* $\gcd(m,n)$ of m and n, and show that there exist integers a and b such that $\gcd(m,n) = am + bn$. Deduce that an integer k divides both m and n only if k divides $\gcd(m,n)$.

Prove (without using the Fundamental Theorem of Arithmetic) that for any positive integer k, $\gcd(km, kn) = k\gcd(m,n)$.

Paper 4, Section I

2E Numbers and Sets

Let $(x_n)_{n=1}^{\infty}$ be a sequence of real numbers. What does it mean to say that the sequence (x_n) is convergent? What does it mean to say the series $\sum x_n$ is convergent? Show that if $\sum x_n$ is convergent, then the sequence (x_n) converges to zero. Show that the converse is not necessarily true.

Paper 4, Section II

5E Numbers and Sets

(i) What does it mean to say that a function $f\colon X \to Y$ is *injective*? What does it mean to say that f is *surjective*? Let $g\colon Y \to Z$ be a function. Show that if $g \circ f$ is injective, then so is f, and that if $g \circ f$ is surjective, then so is g.

(ii) Let X_1, X_2 be two sets. Their *product* $X_1 \times X_2$ is the set of ordered pairs (x_1, x_2) with $x_i \in X_i$ ($i = 1, 2$). Let p_i (for $i = 1, 2$) be the function

$$p_i\colon X_1 \times X_2 \to X_i, \quad p_i(x_1, x_2) = x_i.$$

When is p_i surjective? When is p_i injective?

(iii) Now let Y be any set, and let $f_1\colon Y \to X_1$, $f_2\colon Y \to X_2$ be functions. Show that there exists a unique $g\colon Y \to X_1 \times X_2$ such that $f_1 = p_1 \circ g$ and $f_2 = p_2 \circ g$.

Show that if f_1 or f_2 is injective, then g is injective. Is the converse true? Justify your answer.

Show that if g is surjective then both f_1 and f_2 are surjective. Is the converse true? Justify your answer.

Paper 4, Section II
6E Numbers and Sets

(i) Let N and r be integers with $N \geqslant 0$, $r \geqslant 1$. Let S be the set of $(r+1)$-tuples $(n_0, n_1, \ldots, n_r)$ of non-negative integers satisfying the equation $n_0 + \cdots + n_r = N$. By mapping elements of S to suitable subsets of $\{1, \ldots, N+r\}$ of size r, or otherwise, show that the number of elements of S equals

$$\binom{N+r}{r}.$$

(ii) State the Inclusion–Exclusion principle.

(iii) Let $a_0, \ldots, a_r$ be positive integers. Show that the number of $(r+1)$-tuples (n_i) of integers satisfying

$$n_0 + \cdots + n_r = N, \quad 0 \leqslant n_i < a_i \text{ for all } i$$

is

$$\binom{N+r}{r} - \sum_{0 \leqslant i \leqslant r} \binom{N+r-a_i}{r} + \sum_{0 \leqslant i < j \leqslant r} \binom{N+r-a_i-a_j}{r} - \sum_{0 \leqslant i < j < k \leqslant r} \binom{N+r-a_i-a_j-a_k}{r} + \cdots$$

where the binomial coefficient $\binom{m}{r}$ is defined to be zero if $m < r$.

Paper 4, Section II
7E Numbers and Sets

(i) What does it mean to say that a set is *countable*? Show directly from your definition that any subset of a countable set is countable, and that a countable union of countable sets is countable.

(ii) Let X be either $\mathbb{Z}$ or $\mathbb{Q}$. A function $f\colon X \to \mathbb{Z}$ is said to be *periodic* if there exists a positive integer n such that for every $x \in X$, $f(x+n) = f(x)$. Show that the set of periodic functions from $\mathbb{Z}$ to itself is countable. Is the set of periodic functions $f\colon \mathbb{Q} \to \mathbb{Z}$ countable? Justify your answer.

(iii) Show that $\mathbb{R}^2$ is not the union of a countable collection of lines.

[You may assume that $\mathbb{R}$ and the power set of $\mathbb{N}$ are uncountable.]

Paper 4, Section II

8E Numbers and Sets

Let p be a prime number, and x, n integers with $n \geqslant 1$.

(i) Prove Fermat's Little Theorem: for any integer x, $x^p \equiv x \pmod{p}$.

(ii) Show that if y is an integer such that $x \equiv y \pmod{p^n}$, then for every integer $r \geqslant 0$,

$$x^{p^r} \equiv y^{p^r} \pmod{p^{n+r}}.$$

Deduce that $x^{p^n} \equiv x^{p^{n-1}} \pmod{p^n}$.

(iii) Show that there exists a unique integer $y \in \{0, 1, \ldots, p^n - 1\}$ such that

$$y \equiv x \pmod{p} \quad \text{and} \quad y^p \equiv y \pmod{p^n}.$$

Paper 4, Section I

1D Numbers and Sets

(i) Find integers x and y such that $18x + 23y = 101$.

(ii) Find an integer x such that $x \equiv 3 \pmod{18}$ and $x \equiv 2 \pmod{23}$.

Paper 4, Section I

2D Numbers and Sets

What is an *equivalence relation* on a set X? If R is an equivalence relation on X, what is an *equivalence class* of R? Prove that the equivalence classes of R form a partition of X.

Let R and S be equivalence relations on a set X. Which of the following are always equivalence relations? Give proofs or counterexamples as appropriate.

(i) The relation V on X given by xVy if both xRy and xSy.

(ii) The relation W on X given by xWy if xRy or xSy.

Paper 4, Section II

5D Numbers and Sets

Let X be a set, and let f and g be functions from X to X. Which of the following are always true and which can be false? Give proofs or counterexamples as appropriate.

(i) If fg is the identity map then gf is the identity map.

(ii) If $fg = g$ then f is the identity map.

(iii) If $fg = f$ then g is the identity map.

How (if at all) do your answers change if we are given that X is finite?

Determine which sets X have the following property: if f is a function from X to X such that for every $x \in X$ there exists a positive integer n with $f^n(x) = x$, then there exists a positive integer n such that f^n is the identity map. [Here f^n denotes the n-fold composition of f with itself.]

Paper 4, Section II

6D Numbers and Sets

State Fermat's Theorem and Wilson's Theorem.

For which prime numbers p does the equation $x^2 \equiv -1 \pmod{p}$ have a solution? Justify your answer.

For a prime number p, and an integer x that is not a multiple of p, the *order* of $x \pmod{p}$ is the least positive integer d such that $x^d \equiv 1 \pmod{p}$. Show that if x has order d and also $x^k \equiv 1 \pmod{p}$ then d must divide k.

For a positive integer n, let $F_n = 2^{2^n} + 1$. If p is a prime factor of F_n, determine the order of $2 \pmod{p}$. Hence show that the F_n are pairwise coprime.

Show that if p is a prime of the form $4k+3$ then p cannot be a factor of any F_n. Give, with justification, a prime p of the form $4k+1$ such that p is not a factor of any F_n.

Paper 4, Section II

7D Numbers and Sets

Prove that each of the following numbers is irrational:

(i) $\sqrt{2} + \sqrt{3}$

(ii) e

(iii) The real root of the equation $x^3 + 4x - 7 = 0$

(iv) $\log_2 3$.

Paper 4, Section II

8D Numbers and Sets

Show that there is no injection from the power-set of $\mathbb{R}$ to $\mathbb{R}$. Show also that there *is* an injection from $\mathbb{R}^2$ to $\mathbb{R}$.

Let X be the set of all functions f from $\mathbb{R}$ to $\mathbb{R}$ such that $f(x) = x$ for all but finitely many x. Determine whether or not there exists an injection from X to $\mathbb{R}$.

Paper 4, Section I

1E Numbers and Sets

What does it mean to say that a function $f : X \to Y$ has an inverse? Show that a function has an inverse if and only if it is a bijection.

Let f and g be functions from a set X to itself. Which of the following are always true, and which can be false? Give proofs or counterexamples as appropriate.

(i) If f and g are bijections then $f \circ g$ is a bijection.

(ii) If $f \circ g$ is a bijection then f and g are bijections.

Paper 4, Section I

2E Numbers and Sets

What is an *equivalence relation* on a set X? If $\sim$ is an equivalence relation on X, what is an *equivalence class* of $\sim$? Prove that the equivalence classes of $\sim$ form a partition of X.

Let $\sim$ be the relation on the positive integers defined by $x \sim y$ if either x divides y or y divides x. Is $\sim$ an equivalence relation? Justify your answer.

Write down an equivalence relation on the positive integers that has exactly four equivalence classes, of which two are infinite and two are finite.

Paper 4, Section II

5E Numbers and Sets

(a) What is the *highest common factor* of two positive integers a and b? Show that the highest common factor may always be expressed in the form $\lambda a + \mu b$, where λ and μ are integers.

Which positive integers n have the property that, for any positive integers a and b, if n divides ab then n divides a or n divides b? Justify your answer.

Let a, b, c, d be distinct prime numbers. Explain carefully why ab cannot equal cd.

[*No form of the Fundamental Theorem of Arithmetic may be assumed without proof.*]

(b) Now let S be the set of positive integers that are congruent to 1 mod 10. We say that $x \in S$ is *irreducible* if $x > 1$ and whenever $a, b \in S$ satisfy $ab = x$ then $a = 1$ or $b = 1$. Do there exist distinct irreducibles a, b, c, d with $ab = cd$?

Paper 4, Section II

6E Numbers and Sets

State Fermat's Theorem and Wilson's Theorem.

Let p be a prime.

(a) Show that if $p \equiv 3 \pmod 4$ then the equation $x^2 \equiv -1 \pmod p$ has no solution.

(b) By considering $\left(\frac{p-1}{2}\right)!$, or otherwise, show that if $p \equiv 1 \pmod 4$ then the equation $x^2 \equiv -1 \pmod p$ does have a solution.

(c) Show that if $p \equiv 2 \pmod 3$ then the equation $x^3 \equiv -1 \pmod p$ has no solution other than $-1 \pmod p$.

(d) Using the fact that $14^2 \equiv -3 \pmod{199}$, find a solution of $x^3 \equiv -1 \pmod{199}$ that is not $-1 \pmod{199}$.

[*Hint: how are the complex numbers* $\sqrt{-3}$ *and* $\sqrt[3]{-1}$ *related?*]

Paper 4, Section II

7E Numbers and Sets

Define the binomial coefficient $\binom{n}{i}$, where n is a positive integer and i is an integer with $0 \leqslant i \leqslant n$. Arguing from your definition, show that $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

Prove the binomial theorem, that $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$ for any real number x.

By differentiating this expression, or otherwise, evaluate $\sum_{i=0}^{n} i\binom{n}{i}$ and $\sum_{i=0}^{n} i^2\binom{n}{i}$.

By considering the identity $(1+x)^n(1+x)^n = (1+x)^{2n}$, or otherwise, show that

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}.$$

Show that $\sum_{i=0}^{n} i\binom{n}{i}^2 = \frac{n}{2}\binom{2n}{n}$.

Paper 4, Section II

8E Numbers and Sets

Show that, for any set X, there is no surjection from X to the power-set of X.

Show that there exists an injection from $\mathbb{R}^2$ to $\mathbb{R}$.

Let A be a subset of $\mathbb{R}^2$. A *section* of A is a subset of $\mathbb{R}$ of the form

$$\{t \in \mathbb{R} : \; a + tb \in A\},$$

where $a \in \mathbb{R}^2$ and $b \in \mathbb{R}^2$ with $b \neq 0$. Prove that there does not exist a set $A \subset \mathbb{R}^2$ such that every set $S \subset \mathbb{R}$ is a section of A.

Does there exist a set $A \subset \mathbb{R}^2$ such that every countable set $S \subset \mathbb{R}$ is a section of A? [*There is no requirement that every section of A should be countable.*] Justify your answer.

Paper 4, Section I

1E Numbers and Sets

(a) Find the smallest residue x which equals $28!\,13^{28} \pmod{31}$.

[*You may use any standard theorems provided you state them correctly.*]

(b) Find all integers x which satisfy the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{2}, \\ 2x &\equiv 1 \pmod{3}, \\ 2x &\equiv 4 \pmod{10}, \\ x &\equiv 10 \pmod{67}. \end{aligned}$$

Paper 4, Section I

2E Numbers and Sets

(a) Let r be a real root of the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, with integer coefficients a_i and leading coefficient 1. Show that if r is rational, then r is an integer.

(b) Write down a series for e. By considering $q!e$ for every natural number q, show that e is irrational.

Paper 4, Section II
5E Numbers and Sets

The Fibonacci numbers F_n are defined for all natural numbers n by the rules

$$F_1 = 1\,, \qquad F_2 = 1\,, \qquad F_n = F_{n-1} + F_{n-2} \quad \text{for } \; n \geqslant 3\,.$$

Prove by induction on k that, for any n,

$$F_{n+k} = F_k\,F_{n+1} + F_{k-1}\,F_n \quad \text{for all } \; k \geqslant 2\,.$$

Deduce that

$$F_{2n} = F_n(F_{n+1} + F_{n-1}) \qquad \text{for all } \; n \geqslant 2\,.$$

Put $L_1 = 1$ and $L_n = F_{n+1} + F_{n-1}$ for $n > 1$. Show that these (Lucas) numbers L_n satisfy

$$L_1 = 1\,, \qquad L_2 = 3\,, \qquad L_n = L_{n-1} + L_{n-2} \quad \text{for } \; n \geqslant 3\,.$$

Show also that, for all n, the greatest common divisor (F_n, F_{n+1}) is 1, and that the greatest common divisor (F_n, L_n) is at most 2.

Paper 4, Section II
6E Numbers and Sets

State and prove Fermat's Little Theorem.

Let p be an odd prime. If $p \neq 5$, show that p divides $10^n - 1$ for infinitely many natural numbers n.

Hence show that p divides infinitely many of the integers

$$5\,, \qquad 55\,, \qquad 555\,, \qquad 5555\,, \qquad \ldots \quad .$$

Paper 4, Section II
7E Numbers and Sets

(a) Let A, B be finite non–empty sets, with $|A| = a,\ |B| = b$. Show that there are b^a mappings from A to B. How many of these are injective ?

(b) State the Inclusion–Exclusion principle.

(c) Prove that the number of surjective mappings from a set of size n onto a set of size k is

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n \qquad \text{for } n \geqslant k \geqslant 1\,.$$

Deduce that

$$n! = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^n\,.$$

Paper 4, Section II
8E Numbers and Sets

What does it mean for a set to be countable ?

Show that $\mathbb{Q}$ is countable, but $\mathbb{R}$ is not. Show also that the union of two countable sets is countable.

A subset A of $\mathbb{R}$ has the property that, given $\epsilon > 0$ and $x \in \mathbb{R}$, there exist reals a, b with $a \in A$ and $b \notin A$ with $|x-a| < \epsilon$ and $|x-b| < \epsilon$. Can A be countable ? Can A be uncountable ? Justify your answers.

A subset B of $\mathbb{R}$ has the property that given $b \in B$ there exists $\epsilon > 0$ such that if $0 < |b-x| < \epsilon$ for some $x \in \mathbb{R}$, then $x \notin B$. Is B countable ? Justify your answer.

Paper 4, Section I

1E Numbers and Sets

Let R_1 and R_2 be relations on a set A. Let us say that R_2 *extends* R_1 if xR_1y implies that xR_2y. If R_2 extends R_1, then let us call R_2 an *extension* of R_1.

Let Q be a relation on a set A. Let R be the extension of Q defined by taking xRy if and only if xQy or $x = y$. Let S be the extension of R defined by taking xSy if and only if xRy or yRx. Finally, let T be the extension of S defined by taking xTy if and only if there is a positive integer n and a sequence $(x_0, x_1, \ldots, x_n)$ such that $x_0 = x$, $x_n = y$, and $x_{i-1}Sx_i$ for each i from 1 to n.

Prove that R is reflexive, S is reflexive and symmetric, and T is an equivalence relation.

Let E be any equivalence relation that extends Q. Prove that E extends T.

Paper 4, Section I

2E Numbers and Sets

(a) Find integers x and y such that

$$9x + 12y \equiv 4 \pmod{47} \qquad \text{and} \qquad 6x + 7y \equiv 14 \pmod{47}.$$

(b) Calculate $43^{135} \pmod{137}$.

Paper 4, Section II

5E Numbers and Sets

(a) Let A and B be non-empty sets and let $f : A \to B$.

Prove that f is an injection if and only if f has a left inverse.

Prove that f is a surjection if and only if f has a right inverse.

(b) Let A, B and C be sets and let $f : B \to A$ and $g : B \to C$ be functions. Suppose that f is a surjection. Prove that there is a function $h : A \to C$ such that for every $a \in A$ there exists $b \in B$ with $f(b) = a$ and $g(b) = h(a)$.

Prove that h is unique if and only if $g(b) = g(b')$ whenever $f(b) = f(b')$.

Paper 4, Section II

6E Numbers and Sets

(a) State and prove the inclusion–exclusion formula.

(b) Let k and m be positive integers, let $n = km$, let $A_1, \ldots, A_k$ be disjoint sets of size m, and let $A = A_1 \cup \ldots \cup A_k$. Let $\mathcal{B}$ be the collection of all subsets $B \subset A$ with the following two properties:

(i) $|B| = k$;

(ii) there is at least one i such that $|B \cap A_i| = 3$.

Prove that the number of sets in $\mathcal{B}$ is given by the formula

$$\sum_{r=1}^{\lfloor k/3 \rfloor} (-1)^{r-1} \binom{k}{r} \binom{m}{3}^r \binom{n-rm}{k-3r}.$$

Paper 4, Section II

7E Numbers and Sets

Let p be a prime number and let $\mathbb{Z}_p$ denote the set of integers modulo p. Let k be an integer with $0 \leqslant k \leqslant p$ and let A be a subset of $\mathbb{Z}_p$ of size k.

Let t be a non-zero element of $\mathbb{Z}_p$. Show that if $a + t \in A$ whenever $a \in A$ then $k = 0$ or $k = p$. Deduce that if $1 \leqslant k \leqslant p - 1$, then the sets $A, A + 1, \ldots, A + p - 1$ are all distinct, where $A + t$ denotes the set $\{a + t : a \in A\}$. Deduce from this that $\binom{p}{k}$ is a multiple of p whenever $1 \leqslant k \leqslant p - 1$.

Now prove that $(a + 1)^p = a^p + 1$ for any $a \in \mathbb{Z}_p$, and use this to prove Fermat's little theorem. Prove further that if $Q(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ is a polynomial in x with coefficients in $\mathbb{Z}_p$, then the polynomial $(Q(x))^p$ is equal to $a_n x^{pn} + a_{n-1} x^{p(n-1)} + \ldots + a_1 x^p + a_0$.

Paper 4, Section II

8E Numbers and Sets

Prove that the set of all infinite sequences $(\epsilon_1, \epsilon_2, \ldots)$ with every ϵ_i equal to 0 or 1 is uncountable. Deduce that the closed interval $[0, 1]$ is uncountable.

For an ordered set X let $\Sigma(X)$ denote the set of increasing (but not necessarily strictly increasing) sequences in X that are bounded above. For each of $\Sigma(\mathbb{Z})$, $\Sigma(\mathbb{Q})$ and $\Sigma(\mathbb{R})$, determine (with proof) whether it is uncountable.

4/I/1D **Numbers and Sets**

Let A, B and C be non-empty sets and let $f : A \to B$ and $g : B \to C$ be two functions. For each of the following statements, give either a brief justification or a counterexample.

(i) If f is an injection and g is a surjection, then $g \circ f$ is a surjection.

(ii) If f is an injection and g is an injection, then there exists a function $h : C \to A$ such that $h \circ g \circ f$ is equal to the identity function on A.

(iii) If X and Y are subsets of A then $f(X \cap Y) = f(X) \cap f(Y)$.

(iv) If Z and W are subsets of B then $f^{-1}(Z \cap W) = f^{-1}(Z) \cap f^{-1}(W)$.

4/I/2D **Numbers and Sets**

(a) Let $\sim$ be an equivalence relation on a set X. What is an *equivalence class* of $\sim$? Prove that the equivalence classes of $\sim$ form a partition of X.

(b) Let $\mathbb{Z}^+$ be the set of all positive integers. Let a relation $\sim$ be defined on $\mathbb{Z}^+$ by setting $m \sim n$ if and only if $m/n = 2^k$ for some (not necessarily positive) integer k. Prove that $\sim$ is an equivalence relation, and give an example of a set $A \subset \mathbb{Z}^+$ that contains precisely one element of each equivalence class.

4/II/5D **Numbers and Sets**

(a) Define the notion of a *countable set*, and prove that the set $\mathbb{N} \times \mathbb{N}$ is countable. Deduce that if X and Y are countable sets then $X \times Y$ is countable, and also that a countable union of countable sets is countable.

(b) If A is any set of real numbers, define $\phi(A)$ to be the set of all real roots of non-zero polynomials that have coefficients in A. Now suppose that A_0 is a countable set of real numbers and define a sequence $A_1, A_2, A_3, \ldots$ by letting each A_n be equal to $\phi(A_{n-1})$. Prove that the union $\bigcup_{n=1}^{\infty} A_n$ is countable.

(c) Deduce that there is a countable set X that contains the real numbers 1 and π and has the further property that if P is any non-zero polynomial with coefficients in X, then all real roots of P belong to X.

4/II/6D **Numbers and Sets**

(a) Let a and m be integers with $1 \leqslant a < m$ and let $d = (a, m)$ be their highest common factor. For any integer b, prove that b is a multiple of d if and only if there exists an integer r satisfying the equation $ar \equiv b \pmod{m}$, and show that in this case there are exactly d solutions to the equation that are distinct mod m.

Deduce that the equation $ar \equiv b \pmod{m}$ has a solution if and only if $b(m/d) \equiv 0 \pmod{m}$.

(b) Let p be a prime and let $\mathbb{Z}_p^*$ be the multiplicative group of non-zero integers mod p. An element x of $\mathbb{Z}_p^*$ is called a *kth power* (mod p) if $x \equiv y^k \pmod{p}$ for some integer y. It can be shown that $\mathbb{Z}_p^*$ has a *generator* : that is, an element u such that every element of $\mathbb{Z}_p^*$ is a power of u. Assuming this result, deduce that an element x of $\mathbb{Z}_p^*$ is a kth power (mod p) if and only if $x^{(p-1)/d} \equiv 1 \pmod{p}$, where d is now the highest common factor of k and $p-1$.

(c) How many 437th powers are there mod 1013? [*You may assume that* 1013 *is a prime number.*]

4/II/7D **Numbers and Sets**

(a) Let $\mathbb{F}$ be a field such that the equation $x^2 = -1$ has no solution in $\mathbb{F}$. Prove that if x and y are elements of $\mathbb{F}$ such that $x^2 + y^2 = 0$, then both x and y must equal 0.

Prove that $\mathbb{F}^2$ can be made into a field, with operations

$$(x, y) + (z, w) \;=\; (x + z, y + w)$$

and

$$(x, y) \cdot (z, w) \;=\; (xz - yw, xw + yz)\,.$$

(b) Let p be a prime of the form $4m + 3$. Prove that -1 is not a square (mod p), and deduce that there exists a field with exactly p^2 elements.

4/II/8D **Numbers and Sets**

Let q be a positive integer. For every positive integer k, define a number c_k by the formula

$$c_k = (q+k-1)\frac{q!}{(q+k)!}\,.$$

Prove by induction that

$$\sum_{k=1}^{n} c_k \;=\; 1 - \frac{q!}{(q+n)!}$$

for every $n \geqslant 1$, and hence evaluate the infinite sum $\sum_{k=1}^{\infty} c_k$.

Let $a_1, a_2, a_3, \ldots$ be a sequence of integers satisfying the inequality $0 \leqslant a_n < n$ for every n. Prove that the series $\sum_{n=1}^{\infty} a_n/n!$ is convergent. Prove also that its limit is irrational if and only if $a_n \leqslant n-2$ for infinitely many n and $a_m > 0$ for infinitely many m.

4/I/1E **Numbers and Sets**

(i) Use Euclid's algorithm to find all pairs of integers x and y such that

$$7x + 18y = 1\,.$$

(ii) Show that, if n is odd, then $n^3 - n$ is divisible by 24.

4/I/2E **Numbers and Sets**

For integers k and n with $0 \leqslant k \leqslant n$, define $\binom{n}{k}$. Arguing from your definition, show that

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$$

for all integers k and n with $1 \leqslant k \leqslant n-1$.

Use induction on k to prove that

$$\sum_{j=0}^{k} \binom{n+j}{j} = \binom{n+k+1}{k}$$

for all non-negative integers k and n.

4/II/5E **Numbers and Sets**

State and prove the Inclusion–Exclusion principle.

The keypad on a cash dispenser is broken. To withdraw money, a customer is required to key in a 4-digit number. However, the key numbered 0 will only function if either the immediately preceding two keypresses were both 1, or the very first key pressed was 2. Explaining your reasoning clearly, use the Inclusion–Exclusion Principle to find the number of 4-digit codes which can be entered.

4/II/6E **Numbers and Sets**

Stating carefully any results about countability you use, show that for any $d \geq 1$ the set $\mathbb{Z}[X_1, \ldots, X_d]$ of polynomials with integer coefficients in d variables is countable. By taking $d = 1$, deduce that there exist uncountably many transcendental numbers.

Show that there exists a sequence $x_1, x_2, \ldots$ of real numbers with the property that $f(x_1, \ldots, x_d) \neq 0$ for every $d \geq 1$ and for every non-zero polynomial $f \in \mathbb{Z}[X_1, \ldots, X_d]$.

[*You may assume without proof that* $\mathbb{R}$ *is uncountable.*]

4/II/7E **Numbers and Sets**

Let x_n $(n = 1, 2, \ldots)$ be real numbers.

What does it mean to say that the sequence $(x_n)_{n=1}^{\infty}$ converges?

What does it mean to say that the series $\sum_{n=1}^{\infty} x_n$ converges?

Show that if $\sum_{n=1}^{\infty} x_n$ is convergent, then $x_n \to 0$. Show that the converse can be false.

Sequences of positive real numbers x_n, y_n $(n \geq 1)$ are given, such that the inequality

$$y_{n+1} \leq y_n - \frac{1}{2}\min(x_n, y_n)$$

holds for all $n \geq 1$. Show that, if $\sum_{n=1}^{\infty} x_n$ diverges, then $y_n \to 0$.

4/II/8E **Numbers and Sets**

(i) Let p be a prime number, and let x and y be integers such that p divides xy. Show that at least one of x and y is divisible by p. Explain how this enables one to prove the Fundamental Theorem of Arithmetic.

[*Standard properties of highest common factors may be assumed without proof.*]

(ii) State and prove the Fermat-Euler Theorem.

Let $1/359$ have decimal expansion $0 \cdot a_1 a_2 \ldots$ with $a_n \in \{0, 1, \ldots, 9\}$. Use the fact that $60^2 \equiv 10 \pmod{359}$ to show that, for every n, $a_n = a_{n+179}$.

4/I/1E Numbers and Sets

Explain what is meant by a prime number.

By considering numbers of the form $6p_1p_2\cdots p_n - 1$, show that there are infinitely many prime numbers of the form $6k-1$.

By considering numbers of the form $(2p_1p_2\cdots p_n)^2+3$, show that there are infinitely many prime numbers of the form $6k+1$. [*You may assume the result that, for a prime* $p > 3$, *the congruence* $x^2 \equiv -3 \pmod{p}$ *is soluble only if* $p \equiv 1 \pmod{6}$.]

4/I/2E Numbers and Sets

Define the binomial coefficient $\binom{n}{r}$ and prove that

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1} \qquad \text{for } 0 < r \leqslant n.$$

Show also that if p is prime then $\binom{p}{r}$ is divisible by p for $0 < r < p$.

Deduce that if $0 \leqslant k < p$ and $0 \leqslant r \leqslant k$ then

$$\binom{p+k}{r} \equiv \binom{k}{r} \qquad \pmod{p}.$$

4/II/5E Numbers and Sets

Explain what is meant by an *equivalence relation* on a set A.

If R and S are two equivalence relations on the same set A, we define

$$R \circ S = \{(x,z) \in A \times A : \text{there exists } y \in A \text{ such that } (x,y) \in R \text{ and } (y,z) \in S\}.$$

Show that the following conditions are equivalent:

(i) $R \circ S$ is a symmetric relation on A;

(ii) $R \circ S$ is a transitive relation on A;

(iii) $S \circ R \subseteq R \circ S$;

(iv) $R \circ S$ is the unique smallest equivalence relation on A containing both R and S.

Show also that these conditions hold if $A = \mathbb{Z}$ and R and S are the relations of congruence modulo m and modulo n, for some positive integers m and n.

4/II/6E **Numbers and Sets**

State and prove the Inclusion–Exclusion Principle.

A permutation σ of $\{1, 2, \ldots, n\}$ is called a *derangement* if $\sigma(j) \neq j$ for every $j \leqslant n$. Use the Inclusion–Exclusion Principle to find a formula for the number $f(n)$ of derangements of $\{1, 2, \ldots, n\}$. Show also that $f(n)/n!$ converges to $1/e$ as $n \to \infty$.

4/II/7E **Numbers and Sets**

State and prove Fermat's Little Theorem.

An odd number n is called a *Carmichael number* if it is not prime, but every positive integer a satisfies $a^n \equiv a \pmod{n}$. Show that a Carmichael number cannot be divisible by the square of a prime. Show also that a product of two distinct odd primes cannot be a Carmichael number, and that a product of three distinct odd primes p, q, r is a Carmichael number if and only if $p-1$ divides $qr-1$, $q-1$ divides $pr-1$ and $r-1$ divides $pq-1$. Deduce that 1729 is a Carmichael number.

[*You may assume the result that, for any prime p, there exists a number g prime to p such that the congruence $g^d \equiv 1 \pmod{p}$ holds only when d is a multiple of $p-1$. The prime factors of* 1729 *are* 7, 13 *and* 19.]

4/II/8E **Numbers and Sets**

Explain what it means for a set to be countable. Prove that a countable union of countable sets is countable, and that the set of all subsets of $\mathbb{N}$ is uncountable.

A function $f : \mathbb{N} \to \mathbb{N}$ is said to be increasing if $f(m) \leqslant f(n)$ whenever $m \leqslant n$, and decreasing if $f(m) \geqslant f(n)$ whenever $m \leqslant n$. Show that the set of all increasing functions $\mathbb{N} \to \mathbb{N}$ is uncountable, but that the set of decreasing functions is countable.

[*Standard results on countability, other than those you are asked to prove, may be assumed.*]

4/I/1E **Numbers and Sets**

Find the unique positive integer a with $a \leq 19$, for which

$$17! \cdot 3^{16} \equiv a \pmod{19}.$$

Results used should be stated but need not be proved.

Solve the system of simultaneous congruences

$$\begin{aligned} x &\equiv 1 \pmod{2}, \\ x &\equiv 1 \pmod{3}, \\ x &\equiv 3 \pmod{4}, \\ x &\equiv 4 \pmod{5}. \end{aligned}$$

Explain very briefly your reasoning.

4/I/2E **Numbers and Sets**

Give a combinatorial definition of the binomial coefficient $\binom{n}{m}$ for any non-negative integers n, m.

Prove that $\binom{n}{m} = \binom{n}{n-m}$ for $0 \leq m \leq n$.

Prove the identities

$$\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l}$$

and

$$\sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} = \binom{n+m}{k}.$$

4/II/5E **Numbers and Sets**

What does it mean for a set to be countable? Show that $\mathbb{Q} \times \mathbb{Q}$ is countable, and $\mathbb{R}$ is not countable.

Let D be any set of non-trivial discs in a plane, any two discs being disjoint. Show that D is countable.

Give an example of a set C of non-trivial circles in a plane, any two circles being disjoint, which is not countable.

4/II/6E **Numbers and Sets**

Let R be a relation on the set S. What does it mean for R to be an equivalence relation on S? Show that if R is an equivalence relation on S, the set of equivalence classes forms a partition of S.

Let G be a group, and let H be a subgroup of G. Define a relation R on G by $a\ R\ b$ if $a^{-1}b \in H$. Show that R is an equivalence relation on G, and that the equivalence classes are precisely the left cosets gH of H in G. Find a bijection from H to any other coset gH. Deduce that if G is finite then the order of H divides the order of G.

Let g be an element of the finite group G. The order $o(g)$ of g is the least positive integer n for which $g^n = 1$, the identity of G. If $o(g) = n$, then G has a subgroup of order n; deduce that $g^{|G|} = 1$ for all $g \in G$.

Let m be a natural number. Show that the set of integers in $\{1, 2, \ldots, m\}$ which are prime to m is a group under multiplication modulo m. [*You may use any properties of multiplication and divisibility of integers without proof, provided you state them clearly.*]

Deduce that if a is any integer prime to m then $a^{\phi(m)} \equiv 1 \pmod{m}$, where ϕ is the Euler totient function.

4/II/7E **Numbers and Sets**

State and prove the Principle of Inclusion and Exclusion.

Use the Principle to show that the Euler totient function ϕ satisfies

$$\phi(p_1^{c_1} \cdots p_r^{c_r}) = p_1^{c_1-1}(p_1 - 1) \cdots p_r^{c_r-1}(p_r - 1).$$

Deduce that if a and b are coprime integers, then $\phi(ab) = \phi(a)\phi(b)$, and more generally, that if d is any divisor of n then $\phi(d)$ divides $\phi(n)$.

Show that if $\phi(n)$ divides n then $n = 2^c 3^d$ for some non-negative integers c, d.

4/II/8E **Numbers and Sets**

The Fibonacci numbers are defined by the equations $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for any positive integer n. Show that the highest common factor (F_{n+1}, F_n) is 1.

Let n be a natural number. Prove by induction on k that for all positive integers k,

$$F_{n+k} = F_k F_{n+1} + F_{k-1} F_n.$$

Deduce that F_n divides F_{nl} for all positive integers l. Deduce also that if $m \geq n$ then

$$(F_m, F_n) = (F_{m-n}, F_n).$$

4/I/1E **Numbers and Sets**

(a) Use Euclid's algorithm to find positive integers m, n such that $79m - 100n = 1$.

(b) Determine all integer solutions of the congruence

$$237x \equiv 21 \pmod{300}.$$

(c) Find the set of all integers x satisfying the simultaneous congruences

$$x \equiv 8 \pmod{79}$$
$$x \equiv 11 \pmod{100}.$$

4/I/2E **Numbers and Sets**

Prove by induction the following statements:

i) For every integer $n \geq 1$,

$$1^2 + 3^2 + \cdots + (2n-1)^2 = \frac{1}{3}(4n^3 - n).$$

ii) For every integer $n \geq 1$, $n^3 + 5n$ is divisible by 6.

4/II/5E **Numbers and Sets**

Show that the set of all subsets of $\mathbb{N}$ is uncountable, and that the set of all finite subsets of $\mathbb{N}$ is countable.

Let X be the set of all bijections from $\mathbb{N}$ to $\mathbb{N}$, and let $Y \subset X$ be the set

$$Y = \{f \in X \mid \text{for all but finitely many } n \in \mathbb{N},\ f(n) = n\}.$$

Show that X is uncountable, but that Y is countable.

4/II/6E **Numbers and Sets**

Prove Fermat's Theorem: if p is prime and $(x,p)=1$ then $x^{p-1} \equiv 1 \pmod{p}$.

Let n and x be positive integers with $(x,n)=1$. Show that if $n=mp$ where p is prime and $(m,p)=1$, then

$$x^{n-1} \equiv 1 \pmod{p} \quad \text{if and only if} \quad x^{m-1} \equiv 1 \pmod{p}.$$

Now assume that n is a product of distinct primes. Show that $x^{n-1} \equiv 1 \pmod{n}$ if and only if, for every prime divisor p of n,

$$x^{(n/p)-1} \equiv 1 \pmod{p}.$$

Deduce that if every prime divisor p of n satisfies $(p-1)|(n-1)$, then for every x with $(x,n)=1$, the congruence

$$x^{n-1} \equiv 1 \pmod{n}$$

holds.

4/II/7E **Numbers and Sets**

Polynomials $P_r(X)$ for $r \geq 0$ are defined by

$$P_0(X) = 1$$
$$P_r(X) = \frac{X(X-1)\cdots(X-r+1)}{r!} = \prod_{i=1}^{r} \frac{X-i+1}{i} \qquad \text{for } r \geq 1.$$

Show that $P_r(n) \in \mathbb{Z}$ for every $n \in \mathbb{Z}$, and that if $r \geq 1$ then $P_r(X) - P_r(X-1) = P_{r-1}(X-1)$.

Prove that if F is any polynomial of degree d with rational coefficients, then there are unique rational numbers $c_r(F)$ $(0 \leq r \leq d)$ for which

$$F(X) = \sum_{r=0}^{d} c_r(F) P_r(X).$$

Let $\Delta F(X) = F(X+1) - F(X)$. Show that

$$\Delta F(X) = \sum_{r=0}^{d-1} c_{r+1}(F) P_r(X).$$

Show also that, if F and G are polynomials such that $\Delta F = \Delta G$, then $F - G$ is a constant.

By induction on the degree of F, or otherwise, show that if $F(n) \in \mathbb{Z}$ for every $n \in \mathbb{Z}$, then $c_r(F) \in \mathbb{Z}$ for all r.

4/II/8E **Numbers and Sets**

Let X be a finite set, $X_1, \ldots, X_m$ subsets of X and $Y = X \setminus \bigcup X_i$. Let g_i be the characteristic function of X_i, so that

$$g_i(x) = \begin{cases} 1 & \text{if } x \in X_i \\ 0 & \text{otherwise.} \end{cases}$$

Let $f\colon X \to \mathbb{R}$ be any function. By considering the expression

$$\sum_{x \in X} f(x) \prod_{i=1}^{m} (1 - g_i(x))\,,$$

or otherwise, prove the Inclusion–Exclusion Principle in the form

$$\sum_{x \in Y} f(x) = \sum_{r \geq 0} (-1)^r \sum_{i_1 < \cdots < i_r} \Biggl(\sum_{x \in X_{i_1} \cap \cdots \cap X_{i_r}} f(x) \Biggr).$$

Let $n > 1$ be an integer. For an integer m dividing n let

$$X_m = \{0 \leq x < n \mid x \equiv 0 \pmod{m}\}.$$

By considering the sets X_p for prime divisors p of n, show that

$$\phi(n) = n \prod_{p \mid n} \Bigl(1 - \frac{1}{p}\Bigr)$$

(where ϕ is Euler's function) and

$$\sum_{\substack{0 < x < n \\ (x,n)=1}} x = \frac{n^2}{2} \prod_{p \mid n} \Bigl(1 - \frac{1}{p}\Bigr).$$

4/I/1C Numbers and Sets

(i) Prove by induction or otherwise that for every $n \geqslant 1$,

$$\sum_{r=1}^{n} r^3 = \left(\sum_{r=1}^{n} r \right)^2 .$$

(ii) Show that the sum of the first n positive cubes is divisible by 4 if and only if $n \equiv 0$ or $3 \pmod 4$.

4/I/2C Numbers and Sets

What is an *equivalence relation*? For each of the following pairs $(X, \sim)$, determine whether or not $\sim$ is an equivalence relation on X:

(i) $X = \mathbb{R}$, $x \sim y$ iff $x - y$ is an even integer;

(ii) $X = \mathbb{C} \setminus \{0\}$, $x \sim y$ iff $x\bar{y} \in \mathbb{R}$;

(iii) $X = \mathbb{C} \setminus \{0\}$, $x \sim y$ iff $x\bar{y} \in \mathbb{Z}$;

(iv) $X = \mathbb{Z} \setminus \{0\}$, $x \sim y$ iff $x^2 - y^2$ is ± 1 times a perfect square.

4/II/5C Numbers and Sets

Define what is meant by the term *countable*. Show directly from your definition that if X is countable, then so is any subset of X.

Show that $\mathbb{N} \times \mathbb{N}$ is countable. Hence or otherwise, show that a countable union of countable sets is countable. Show also that for any $n \geqslant 1$, $\mathbb{N}^n$ is countable.

A function $f : \mathbb{Z} \to \mathbb{N}$ is *periodic* if there exists a positive integer m such that, for every $x \in \mathbb{Z}$, $f(x + m) = f(x)$. Show that the set of periodic functions $f : \mathbb{Z} \to \mathbb{N}$ is countable.

4/II/6C Numbers and Sets

(i) Prove Wilson's theorem: if p is prime then $(p-1)! \equiv -1 \pmod p$.

Deduce that if $p \equiv 1 \pmod 4$ then

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p.$$

(ii) Suppose that p is a prime of the form $4k+3$. Show that if $x^4 \equiv 1 \pmod p$ then $x^2 \equiv 1 \pmod p$.

(iii) Deduce that if p is an odd prime, then the congruence

$$x^2 \equiv -1 \pmod p$$

has exactly two solutions (modulo p) if $p \equiv 1 \pmod 4$, and none otherwise.

4/II/7C Numbers and Sets

Let m, n be integers. Explain what is their *greatest common divisor* (m,n). Show from your definition that, for any integer k, $(m,n) = (m+kn, n)$.

State Bezout's theorem, and use it to show that if p is prime and p divides mn, then p divides at least one of m and n.

The Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, ... is defined by $x_0 = 0$, $x_1 = 1$ and $x_{n+1} = x_n + x_{n-1}$ for $n \geqslant 1$. Prove:

(i) $(x_{n+1}, x_n) = 1$ and $(x_{n+2}, x_n) = 1$ for every $n \geqslant 0$;

(ii) $x_{n+3} \equiv x_n \pmod 2$ and $x_{n+8} \equiv x_n \pmod 3$ for every $n \geqslant 0$;

(iii) if $n \equiv 0 \pmod 5$ then $x_n \equiv 0 \pmod 5$.

4/II/8C Numbers and Sets

Let X be a finite set with n elements. How many functions are there from X to X? How many relations are there on X?

Show that the number of relations R on X such that, for each $y \in X$, there exists at least one $x \in X$ with xRy, is $(2^n-1)^n$.

Using the inclusion–exclusion principle or otherwise, deduce that the number of such relations R for which, in addition, for each $x \in X$, there exists at least one $y \in X$ with xRy, is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (2^{n-k}-1)^n.$$

4/I/1C **Numbers and Sets**

What does it mean to say that a function $f : A \to B$ is injective? What does it mean to say that a function $g : A \to B$ is surjective?

Consider the functions $f : A \to B$, $g : B \to C$ and their composition $g \circ f : A \to C$ given by $g \circ f(a) = g(f(a))$. Prove the following results.

(i) If f and g are surjective, then so is $g \circ f$.

(ii) If f and g are injective, then so is $g \circ f$.

(iii) If $g \circ f$ is injective, then so is f.

(iv) If $g \circ f$ is surjective, then so is g.

Give an example where $g \circ f$ is injective and surjective but f is not surjective and g is not injective.

4/I/2C **Numbers and Sets**

If f, $g : \mathbb{R} \to \mathbb{R}$ are infinitely differentiable, Leibniz's rule states that, if $n \geqslant 1$,

$$\frac{d^n}{dx^n}\big(f(x)g(x)\big) = \sum_{r=0}^{n} \binom{n}{r} f^{(n-r)}(x)g^{(r)}(x).$$

Prove this result by induction. (You should prove any results on binomial coefficients that you need.)

4/II/5F **Numbers and Sets**

What is meant by saying that a set is countable?

Prove that the union of countably many countable sets is itself countable.

Let $\{J_i : i \in I\}$ be a collection of disjoint intervals of the real line, each having strictly positive length. Prove that the index set I is countable.

4/II/6F Numbers and Sets

(a) Let S be a finite set, and let $\mathbb{P}(S)$ be the power set of S, that is, the set of all subsets of S. Let $f : \mathbb{P}(S) \to \mathbb{R}$ be additive in the sense that $f(A \cup B) = f(A) + f(B)$ whenever $A \cap B = \varnothing$. Show that, for $A_1, A_2, \ldots, A_n \in \mathbb{P}(S)$,

$$f\left(\bigcup_i A_i\right) = \sum_i f(A_i) - \sum_{i<j} f(A_i \cap A_j) + \sum_{i<j<k} f(A_i \cap A_j \cap A_k) - \cdots + (-1)^{n+1} f\left(\bigcap_i A_i\right).$$

(b) Let $A_1, A_2, \ldots, A_n$ be finite sets. Deduce from part (a) the inclusion–exclusion formula for the size (or cardinality) of $\bigcup_i A_i$.

(c) A *derangement* of the set $S = \{1, 2, \ldots, n\}$ is a permutation π (that is, a bijection from S to itself) in which no member of the set is fixed (that is, $\pi(i) \neq i$ for all i). Using the inclusion–exclusion formula, show that the number d_n of derangements satisfies $d_n/n! \to e^{-1}$ as $n \to \infty$.

4/II/7B Numbers and Sets

(a) Suppose that p is an odd prime. Find $1^p + 2^p + \ldots + (p-1)^p$ modulo p.

(b) Find $(p-1)!$ modulo $(1 + 2 + \ldots + (p-1))$, when p is an odd prime.

4/II/8B Numbers and Sets

Suppose that a, b are coprime positive integers. Write down an integer $d > 0$ such that $a^d \equiv 1$ modulo b. The least such d is the *order* of a modulo b. Show that if the order of a modulo b is y, and $a^x \equiv 1$ modulo b, then y divides x.

Let $n \geqslant 2$ and $F_n = 2^{2^n} + 1$. Suppose that p is a prime factor of F_n. Find the order of 2 modulo p, and show that $p \equiv 1$ modulo 2^{n+1}.

4/I/1E **Numbers and Sets**

(a) Show that, given a set X, there is no bijection between X and its power set.

(b) Does there exist a set whose members are precisely those sets that are not members of themselves? Justify your answer.

4/I/2E **Numbers and Sets**

Prove, by induction or otherwise, that

$$\binom{n}{0}+\binom{n+1}{1}+\cdots+\binom{n+m}{m}=\binom{n+m+1}{m}.$$

Find the number of sequences consisting of zeroes and ones that contain exactly n zeroes and at most m ones.

4/II/5E **Numbers and Sets**

(a) Prove Wilson's theorem, that $(p-1)! \equiv -1 \pmod{p}$, where p is prime.

(b) Suppose that p is an odd prime. Express $1^2.3^2.5^2.\ldots.(p-2)^2 \pmod{p}$ as a power of -1.

[*Hint:* $k \equiv -(p-k) \pmod{p}$.]

4/II/6E **Numbers and Sets**

State and prove the principle of inclusion-exclusion. Use it to calculate $\phi(4199)$, where ϕ is Euler's ϕ-function.

In a certain large college, a survey revealed that 90% of the fellows detest at least one of the pop stars Hairy, Dirty and Screamer. 45% detest Hairy, 28% detest Dirty and 46% detest Screamer. If 27% detest only Screamer and 6% detest all three, what proportion detest Hairy and Dirty but not Screamer?

4/II/7E **Numbers and Sets**

(a) Prove that, if p is prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$.

(b) The *order* of $a \pmod{p}$ is the least positive integer d such that $a^d \equiv 1 \pmod{p}$. Suppose now that $a^x \equiv 1 \pmod{p}$; what can you say about x in terms of d? Show that $p \equiv 1 \pmod{d}$.

(c) Suppose that p is an odd prime. What is the order of $x \pmod{p}$ if $x^2 \equiv -1 \pmod{p}$? Find a condition on $p \pmod{4}$ that is equivalent to the existence of an integer x with $x^2 \equiv -1 \pmod{p}$.

4/II/8E **Numbers and Sets**

What is the Principle of Mathematical Induction? Derive it from the statement that every non-empty set of positive integers has a least element.

Prove, by induction on n, that $9^n \equiv 2^n \pmod{7}$ for all $n \geq 1$.

What is wrong with the following argument?

"Theorem: $\sum_{i=1}^{n} i = n(n+1)/2 + 126$.

Proof: Assume that $m \geq 1$ and $\sum_{i=1}^{m} i = m(m+1)/2 + 126$. Add $m+1$ to both sides to get

$$\sum_{i=1}^{m+1} i \;=\; m(m+1)/2 + m + 1 + 126 \;=\; (m+1)(m+2)/2 + 126.$$

So, by induction, the theorem is proved."