

Paper 4, Section I**1E Numbers and Sets**

What does it mean to say that a function $f : X \rightarrow Y$ 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 $0 \leq i \leq n$. 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.