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.