

4/I/1D Numbers and Sets

Let A , B and C be non-empty sets and let $f : A \rightarrow B$ and $g : B \rightarrow C$ 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 $h : C \rightarrow A$ 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, \dots 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 $1 \leq a < m$ 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 k th 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 k th 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 $n \geq 1$, and hence evaluate the infinite sum $\sum_{k=1}^{\infty} c_k$.

Let a_1, a_2, a_3, \dots be a sequence of integers satisfying the inequality $0 \leq a_n < n$ 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 $a_n \leq n - 2$ for infinitely many n and $a_m > 0$ for infinitely many m .