

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

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

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

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

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

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

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 $f: \mathbb{N} \rightarrow \mathbb{N}$ is said to be increasing if $f(m) \leq f(n)$ whenever $m \leq n$, and decreasing if $f(m) \geq f(n)$ whenever $m \leq n$. Show that the set of all increasing functions $\mathbb{N} \rightarrow \mathbb{N}$ 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.]