Numbers & Sets - Definitions & Methods

Lectured by Prof Imre Leader

Michaelmas 2013

1 Elementary Number Theory

Method 1 (Strong Induction)**.** If $P(1)$, and for all n: $P(m)\ \forall m < n \implies P(n)$, then $P(n)\ \forall n$.

Definition 1 (Highest Common Factor)**.** A natural number c is the *highest common factor* of a and b if:

1. $c \mid a$ and $c \mid b$
2. For any natural number d, if $d \mid a$ and $d \mid b$, then $d \mid c$.

1.1 Modular Arithmetic

Definition 2 (Integers Modulo n)**.** Let $n \geq 2$ be a natural number. Then integers mod n, written $\mathbb{Z}_n$, consists of the integers, where two numbers a, b are regarded as the same if they differ by a multiple of n, and we say that $a \equiv b \pmod{n}$, or 'a is congruent to b mod n'.

Definition 3 (Invertible)**.** Say that an integer a is *invertible* (or a *unit*) mod n if there exists an integer b with $ab \equiv 1\ (n)$.

Method 2 (Solving Congruences)**.** Use Euclid's algorithm, or spot an inverse. You can write in equation form (i.e. $a + xn = b$) to reduce if a, b, n share a common factor.

For multiple congruences, use the Chinese Remainder Theorem. For m, n coprime, $x \equiv a\ (m)$ and $x \equiv b\ (n)$, have $ms + nt = 1$, and so $x \equiv a(nt) + b(ms)\ (mn)$ is the solution.

Method 3 (RSA Encryption)**.** Choose two primes p and q, and set $n = pq$. Choose an encoding exponent e. Encode a message x as x^e in $\mathbb{Z}_n$.

To decode this, need a decoding exponent d, such that $(x^e)^d = x$. Have $x^{\phi(n)} = 1$ by Fermat-Euler (assuming x coprime to n), so $x^{k\phi(n)} = 1$, so $x^{k\phi(n)+1} = x$. Thus sufficient to have d with de of form $k\phi(n) + 1$, i.e. $de \equiv 1\ (\phi(n))$, which can be found by running Euclid on e and $\phi(n)$. (N.B. $\phi(n) = n - p - q + 1$.)

2 The Reals

Definition 4 (Bounded above)**.** A set S is *bounded above* if $\exists x \in \mathbb{R}$ with $x \geq y \; \forall y \in S$. We call such an x an *upper bound* for S.

Definition 5 (Least Upper Bound)**.** Say that x is a *least upper bound*, or *supremum* for a set S if x is an upper bound for S and no $x' < x$ is an upper bound for S.

Definition 6 (Open / Closed Interval)**.** The closed interval $[a, b]$ consists of all reals x with $a \leq x \leq b$.

The open interval (a, b) consists of all reals x with $a < x < b$.

Definition 7 (Convergence)**.** Say that (x_n) *tends* to c if $\forall \epsilon > 0 \;\; \exists N$ such that $\forall n \geq N$: $c - \epsilon < x_n < c + \epsilon$. We can also say that (a_n) *converges* to a, or a is the *limit* of (a_n), and write $\lim_{n\to\infty} a_n = a$, or $a_n \to a$.

Definition 8 (Monotone)**.** A sequence (x_n) is *monotone* if it is decreasing ($x_n \leq x_{n-1} \; \forall n$) or increasing ($x_n \geq x_{n-1} \; \forall n$).

Definition 9 (Algebraic)**.** Say $x \in \mathbb{R}$ is *algebraic* if it is a root of some (non-zero) integer polynomial. A non-algebraic number is known as *transcendental*.

3 Sets

Definition 10 (Set)**.** A *set* is any (except Russel's paradox-like) collection of (mathematical) objects.

Definition 11 (Subset)**.** For sets A, B, say A is a *subset* of B written $A \subset B$, if every member of A is a member of B.

For any set A, and any property $p(x)$, we can form the subset $\{x \in A : p(x)\}$ - this is known as *subset selection*.

Definition 12 (Union and Intersection)**.** For sets A, B can form the *union* $A \cup B = \{x : x \in A \text{ or } x \in B\}$, and the *intersection* $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

Definition 13 (Disjoint)**.** Say sets A, B are *disjoint* if $A \cap B = \emptyset$, where $\emptyset$ is the empty set.

Method 4 (Identities about sets)**.** To prove an identity relating different sets, either:

Suppose $x \in$ LHS and show that $x \in$ RHS, and vice versa.

Use indicator functions.

Definition 14 (Power set)**.** For any set A, the *power set* of A, written $\mathcal{P}(A)$ is $\{B : B \subset A\}$, the set of all subsets of A.

Definition 15 (Binomial Coefficient)**.** For $N \in \mathbb{N}$ and $0 \leq k \leq n$, the *binomial coefficient* $\binom{n}{k}$ is the number of subsets of $\{1, \ldots, n\}$ of size k.

4 Functions

Definition 16 (Function)**.** Let A, B be sets. A *function* f is a rule that assigns to each point $a \in A$ a *unique* point $f(a) \in B$. (More precisely, a function is a subset of $A \times B$ such that $\forall a \in A$ $\exists$ unique $b \in B$ with $(a, b) \in f$.)

Definition 17 (Injective)**.** Say $f : A \to B$ is *injective* if $\forall a, a' \in A$, $a \neq a' \implies f(a) \neq f(a')$ ('different points stay different'). Equivalently, $f(a) = f(a') \implies a = a'$.

Definition 18 (Surjective)**.** Say $f : A \to B$ is *surjective* if $\forall b \in B$ $\exists a \in A$ with $f(a) = b$ ('everything in B is hit').

Definition 19 (Bijective)**.** Say $f : A \to B$ is *bijective* if it is injective and surjective.

Definition 20 (Domain, Range and Image)**.** For $f : A \to B$, the *domain* of f is A, the *range* of f is B, and the *image* of f is $\{f(a) : a \in A\}$.

Definition 21 (Characteristic Function)**.** For $A \subset X$, we have the *characteristic function* or *indicator function*

$$\chi_A : X \to \{0, 1\} : x \mapsto \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

Definition 22 (Relation)**.** A *relation* R on a set X is a subset R of $X \times X$ (ordered pairs of X). We write aRb for $(a, b) \in R$.

Definition 23 (Equivalence Relation)**.** We say that R is an *equivalence relation* if R is:

- Reflexive: $\forall x \in X : xRx$
- Symmetric: $\forall x, y \in X : xRy \implies yRx$
- Transitive: $\forall x, y, z \in X : xRy, yRz \implies xRz$

Definition 24 (Equivalence Class)**.** Given an equivalence relation R on a set X and an element $x \in X$, the equivalence class of x is $[x] = \{y \in X : yRx\}$.

Definition 25 (Quotient)**.** The set of equivalence classes of R is called the *quotient* of X by R, written X/R.

The function $q : X \to X/R : x \mapsto [x]$ is called the *quotient map.*

5 Countability

Definition 26 (Countable)**.** Say X is *countable* if X bijects with $\mathbb{N}$, or X is finite. Equivalently, if we can list X as $a_1, a_2, \ldots$ (might terminate).

If X is not countable, we say that it is *uncountable.*

Method 5 (Show set uncountable)**.**

1. Copy diagonal argument
2. Inject your favourite uncountable set

Method 6 (Show set countable)**.**

1. List it
2. Inject it into $\mathbb{N}$
3. Use 'countable union of countable sets is countable'
4. If in/near $\mathbb{R}$, try to use '$\mathbb{Q}$ is countable'