Discrete Mathematics

Discrete mathematics deals with finite or countably infinite sets, this includes integers and related concepts.

Definitions

Keyword	Definition
Statement	Something that is either true or false.
Predicate	A statement whose truth depends on one or more variables.
Theorem	An important true statement.
Proposition	A less important true statement.
Lemma	A statement used to prove other true statements.
Corollary	A true statement that is a simple deduction from a theorem or proposition.
Conjecture	A statement believed to be true, but not proved yet.
Proof	A way to show a statement is true.
Logic	The study of methods and principles used to distinguish correct reasoning from incorrect reasoning.
Axiom	A basic assumption about a mathematical situation.
Definition	An explaination of the mathematical meaning of a word.
Simple statement	A simple statement cannot be broken down.
Composite statement	A compisite statement is built using several other statements connected by logical expressions.

Proof Structure

Definitions

Keyword	Definition
Assumptions	Statements that may be used for deduction.
Goals	Statements to be established.

Start by listing out assumptions and write down the goal.

Implication

$$\text{collection of hypotheses} \implies \text{some conclusion}$$

To prove $P \implies Q$

- Add P to the list of assumptions.
- Replace $P \implies Q$ in goal with Q.

Types of Real Numbers

Definitions

Keyword	Definition
Rational	A number is rational if it is in form m/n for some integer m, n, otherwise it is irrational.
Positive	A number is positive if it is greater than 0, otherwise it is nonpositive.
Negative	A number is negative if it is less than 0, otherwise it is nonnegative.
Natural	A number is natural if it is a nonnegative integer.

Modus Ponens (Implication Elimination)

The main rule for logical deduction is

- From statements P and $P \implies Q$.
- Q follows.

$$\frac{P \quad P \implies Q}{Q}$$

Bi-implications

Some theorems are in form $P \iff Q$, to prove it

- Prove $P \implies Q$
- Prove $Q \implies P$

Quantifiers

Universal Quantifications

Definition

$(\forall x)\ P(x)$ means: for all individuals x of the universe of the discourse, the property $P(x)$ holds.

Universal instantiation allows any a to be plugged in to $(\forall x)\ P(x)$ and conclude that $P(a)$ is true.

Proof: Statement involving universal quantification

Assumptions	Goals
	G1: $(\forall x)\ P(x)$

We can rewrite as

Proof: Statement involving universal quantification

Assumptions	Goals
A1: x stands for an arbitrary individual.	~~G1: $(\forall x)\ P(x)$~~
	G2: $P(x)$

Divisibility and Congruence

Definition

Let d and n be integers. If d divides n, we write $d \mid n$.

$$(\exists k)\ n = k \cdot d \iff d \mid n$$

Definition

For integers a and b, and positive integer m.

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

We can prove that

- If n is odd, then $n \equiv 1 \pmod{2}$
- If n is even, then $n \equiv 0 \pmod{2}$

Example: Congruence Result

Let m and n be positive integers, and a and b be arbitrary integers.

We want to prove the statement $(\forall n)$

Proof: Multiplied Congruence

Assumptions	Goals
A1: $m, n, a, b \in \mathbb{Z}$	G1: $(\forall n)\ a \equiv b \pmod{m} \implies na \equiv nb \pmod{nm}$
A2: $a, b > 0$	

Rewriting the target

Proof: Multiplied Congruence

Assumptions	Goals
A1: $m, n, a, b \in \mathbb{Z}$	G1: $\cancel{(\forall n)\ a \equiv b \pmod{m} \implies na \equiv nb \pmod{nm}}$
A2: $a, b > 0$	G2: $na \equiv nb \pmod{nm}$
A3: $a \equiv b \pmod{m}$	

Then rewrite A3

$$\begin{aligned}
&\implies a \equiv b \pmod{m} \\
&\implies (\exists k)\ (a - b) = k \cdot m \\
&\implies (\exists k)\ n(a - b) = k \cdot m \cdot n \\
&\implies na \equiv nb \pmod{nm}
\end{aligned}$$

Which is the goal.

To prove $(\forall n)\ (na, nb, nm) \implies a \equiv b \pmod{m}$, plug $n = 1$ and we have the goal.

Equality

Definition

The axioms for **equality** are

- $(\forall x)\ x = x$
- $(\forall x, y)\ (x = y) \implies (P(x) \iff P(y))$

Conjunction

To prove a conjunction $P \land Q$, we need to prove both P and Q.

Definition

$(P \iff Q) \iff (P \implies Q \land Q \implies P)$

Example: $(\forall n)\ (6 \mid n \iff 3 \mid n \land 2 \mid n)$

Let n be an arbitrary value.

$$\begin{aligned} 6 \mid n &\iff (\exists i)\ n = 6i \\ &\iff (\exists i)\ n = 2 \cdot 3 \cdot i \\ &\implies (\exists j{,}k)\ n = 2j \land n = 3k \\ &\iff 2 \mid n \land 3 \mid n \end{aligned}$$

And the reverse direction

$$\begin{aligned} 2 \mid n \land 3 \mid n &\iff (\exists i{,}j)\ n = 2i \land n = 3j \\ &\iff (\exists i{,}j)\ 3n = 6i \land 2n = 6j \\ &\iff (\exists i{,}j)\ n = 6(i - j) \\ &\implies (\exists k)\ n = 6k \\ &\iff 6 \mid n \end{aligned}$$

Existential Quantifier

Definition

$(\exists x)\ P(x)$: there exists an individual x in the universe of the discourse which $P(x)$ holds.

Proving an Existential Quantifier

Find a witness w so $P(w)$ is true.

Target: $(\forall n)\ (\exists i{,}j)\ 4n = i^2 - j^2$

- Let $i = n + 1$
- Let $j = n - 1$

It is true that $4n = i^2 - j^2$.

Using an Existential Quantifier

Introduce a variable w and assume $P(w)$ to be true.

Unique Existence

Definition

$(\exists! x)\ P(x) \iff ((\exists x)\ P(x) \land ((\forall y{,}z)\ P(y) \land P(z) \implies y = z))$

To prove $(\forall x)\ (\exists! y)\ P(x, y)$

1. Find a **unique** witness w so that $P(w, f(w))$ is true.
2. Show that $(\forall x)\ P(x, y) \implies y = f(x)$

Disjunction

$P \lor Q$ can be proved by showing P or Q.

To use disjunction, e.g. $P_1 \lor P_2 \implies Q$, we need to show $P_1 \implies Q \land P_2 \implies Q$.

Proving Fermat's Little Theorem

Step 1: Lemma 1 for Fermat's Little Theorem

Required to prove:

$$(\forall m, n \in \mathbb{N})\ m = 0 \lor m = n \implies \binom{n}{m} \equiv 1 \pmod{n}$$

Proof: Lemma 1 for Fermat's Little Theorem

Assumptions	Goals
A1: $m, n \in \mathbb{Z}$	G1: $\binom{n}{m} \equiv 1 \pmod{n}$
A2: $m = 0 \lor m = n$	

$$m = 0 \implies \binom{n}{0} = 1 \implies \binom{n}{m} \equiv 1 \pmod{p}$$
$$m = n \implies \binom{n}{n} = 1 \implies \binom{n}{m} \equiv 1 \pmod{p}$$

Therefore proved.

Step 2: Lemma 2 for Fermat's Little Theorem

Lemma: Euclid's Lemma

This is provided without proof. If p is prime

$$p \mid (a \cdot b) \implies p \mid a \lor p \mid b$$

Required to prove:

$$(\forall p, m \in \mathbb{N})\ p \text{ is prime} \land 0 < m < p \implies \binom{p}{m} \equiv 0 \pmod{p}$$

Proof: Lemma 2 for Fermat's Little Theorem

Assumptions	Goals
A1: $p, m \in \mathbb{N}$	G1: $\binom{p}{m} \equiv 0 \pmod{p}$
A2: p is prime	
A3: $0 < m < p$	

$$\binom{p}{m} = \frac{p!}{m!(p-m)!}$$

$$\text{since none of } m, m-1, \ldots \text{ or } p-m, p-m-1, \ldots \text{ divides } p$$

$$= p\left(\frac{(p-1)!}{m!(p-m)!}\right)$$

$$\text{where } \frac{(p-1)!}{m!(p-m)!} \text{ is an integer}$$

Therefore $\binom{p}{m} \equiv 0 \pmod{p}$.

> **Note**
> This is a pretty bad proof, especially we haven't define prime numbers yet.

Step 3: Freshman's Dream

> **Theorem: Binomial Theorem**
> $$(m+n)^p = \sum_{k=0}^{p} \binom{p}{k} m^{p-k} n^p$$

> **Properites of Congruence**
> If $a \equiv b \pmod{m} \land x \equiv y \pmod{m}$, then
> - $a + x \equiv b + y \pmod{m}$
> - $ia \equiv ib \pmod{m}$ where i is an integer

Required to prove:

$$(\forall p \text{ is prime})\ (m+n)^p \equiv m^p + n^p \pmod{p}$$

Proof: Freshman's Dream

Assumptions	Goals
A1: p is prime	G1: $(m+n)^p \equiv m^p + n^p \pmod{p}$

By bimonial theorem

$$(m+n)^p = \sum_{k=0}^{p} \binom{p}{k} m^{p-k} n^p$$

$$= m^p + n^p \quad \text{cancel terms using lemma 2}$$

Therefore $(m+n)^p \equiv m^p + n^p \pmod{p}$

Step 4: Dropout Lemma

When $n = 1$ for Freshman's dream.

$$(m+1)^p \equiv m^p + 1 \pmod{p}$$

Step 5: Many Dropout Lemma

$$\begin{aligned}(m+i)^p &= \Big(m + \underbrace{1+1+\ldots+1}_{i \text{ times}}\Big)^p \\ &= \Big(m + \underbrace{1+1+\ldots+1}_{i-1 \text{ times}}\Big)^p + 1 \\ &= m^p + i \quad \text{after applying dropout lemma } i \text{ times}\end{aligned}$$

So $(m+i)^p \equiv m^p + i \pmod p$.

Step 6: Fermat's Little Theorem, Cause 1
When $m = 0$ for many dropout lemma.

$$(\forall p \text{ is prime})\ i^p \equiv i \pmod m$$

Proposition
$(\forall i \in \mathbb{N} \text{ not a multiple of } p) \quad i \cdot i^{p-2} \equiv 1 \pmod p$

Definition
i^{p-2} is the reciprocal moduluo of p.

Logical Equivalents

$$\begin{aligned}\neg(P \implies Q) &\iff P \wedge \neg Q \\ \neg(P \iff Q) &\iff (P \iff \neg Q) \quad \text{how tf is this true?} \\ \neg((\forall x)\ P(x)) &\iff (\exists x)\ \neg P(x) \\ \neg(P \wedge Q) &\iff (\neg P) \vee (\neg Q) \\ \neg((\exists x)\ P(x)) &\iff (\forall x)\ \neg P(x) \\ \neg(P \vee Q) &\iff \neg P \wedge \neg Q \\ \neg(\neg P) &\iff P\end{aligned}$$

Definition
$\neg P \iff (P \implies \text{false})$
false $\iff$ some absurd statement

Prove by Contradiction
Instead of showing P, show $\neg P \implies$ false.

$$(\neg P \implies \text{false}) \iff \neg(\neg P) \iff P$$

Prove by Contrapositive
Required to prove:

$$(\neg Q \implies \neg P) \iff (P \implies Q)$$

Proof: Contrapositive

Assumptions	Goals
A1: $\neg Q \Longrightarrow \neg P$	G1: Q
A2: P	

Suppose A3: $\neg Q$.
A4. $\neg P$ by A1 and A3.
A5. false by A2 and A4.

This is a contradiction, therefore Q must be true.

Numbers

Natural numbers are constructed from zero by the successor relation.

```
type N =
  | zero
  | succ of N
```

Definition

A **monoid** is an algebraic structure with
- A neutral element e
- A binary operation $\cdot$

Monoid Laws
- Neutral element $e \cdot x = x = x \cdot e$
- Associative $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

A monoid is **commutative** if $x \cdot y = y \cdot x$.

Addition $(\mathbb{N}, 0, +)$ and **multiplication** $(\mathbb{N}, 1, \times)$ satisfies monoid laws and commutative laws.

Rings

Definition

A **semiring** $(\mathbb{N}, 0, \oplus, 1, \otimes)$ is an algebraic structure with
- A commutative monoid structure $(\mathbb{N}, 0, \oplus)$
- A monoid structure $(\mathbb{N}, 1, \otimes)$

And satisfies the distributive laws $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$.

A semiring is **commutative** if $\otimes$ is.

Cancellation

The additive and multiplicative structures of natural numbers allows for
- Additive cancellation: $k + m = k + n \Longrightarrow m = n$
- Multiplicative cancellation: if $k \neq 0$, then $k \times m = k \times n \Longrightarrow m = n$

Inverses

For a monoid with neutral element e and binary operation $\oplus$.
- x admits an inverse on the left if $(\exists l)\ l \oplus x = e$

- x admits an inverse on the right if $(\exists r)\ x \oplus r = e$
- x admits an inverse if l and r both exists.

Proposition

If l and r both exists, $l = r$.

$$\begin{aligned} e \oplus r &= r \\ \Longleftrightarrow (l \oplus x) \oplus r &= r \\ \Longleftrightarrow l \oplus (x \oplus r) &= r \\ \Longleftrightarrow l &= r \end{aligned}$$

Definitions

- A **group** is a monoid in which every element has an inverse.
- An **Abelian group** is a group where the monoid is commutative.

- x admits an additive inverse if $(\exists y)\ x + y = 0$
- x admits an multiplicative inverse if $(\exists y)\ x \times y = 1$

The natural numbers can be extended to include all additive inverses to give the set of **integers**.

Definitions

- A **ring** is a semiring $(\mathbb{Z}, 0, \oplus, 1, \otimes)$ where $(\mathbb{Z}, 0, \oplus)$ is a group.
  A ring is commutative if $(\mathbb{Z}, \otimes, 1)$ is.
- A **field** is a commutative ring in which every element besides 0 has a **reciprocal** (inverse with respect to $\otimes$).

Division Theorem

Required to prove:

$$(\forall m \in \mathbb{N}, n \in \mathbb{N}^{+})\ (\exists! q, !r)\ (q \geq 0) \land (0 \leq r < m) \land (m = qn + r)$$

We need to prove if (q, r) and (q', r') both satisfies the conditon, then $(q, r) = (q', r')$.

Proof: Division theorem

Assumptions	Goals
A1: $(q \geq 0) \land (0 \leq r < n) \land (m = qn + r)$	G1: $q = q'$
A2: $(q' \geq 0) \land (0 \leq r' < n) \land (m = q'n + r')$	G2: $r = r'$

Because $m - r = qn$, similar for (q', r')

$$m \equiv r \pmod{n}$$
$$m \equiv r' \pmod{n}$$

We have proved that congruence is transitive

$$r \equiv r' \pmod{n}$$

As $0 \leq r, r' < n$, therefore $r = r'$. And by cancellation, $q = q'$.

Proving the Division Algorithm

```
let divalg m n =
  let diviter q r =
    if r < n then (q, r)
    else diviter (q + 1, r - n)
  in diviter 0 m
```

Required to prove:

1. Partial correctness
   $(\forall m \in \mathbb{N}, n \in \mathbb{N}^{+})$ $\;$ divalg(m, n) terminates with $(q_0, r_0) \implies (r_0 < n \wedge m = q_0 n + r_0)$
2. Total correctness.
   $(\forall m \in \mathbb{N}, n \in \mathbb{N}^{+})$ $\;$ divalg(m, n) terminates

We can prove partial correctness by induction:

- If `divalg` exits then $r_0 < n$
- Prove at each point of the computation $m = qn + r$

To prove total correctness:

- m decreases in natural number at every step.
- m cannot decreate forever (all natural numbers comes from applying the successor function a finite number of times to 0).