Lecture 5: Proof methods

Table of contents

Basic number theory

- An integer n is
  - **even** if there is an integer k such that $n = 2m$,
  - **odd** if there is an integer m such that $n = 2m + 1$

  Two integers m and n have the **same parity** if they are both even or both odd.
- In general, an integer n is called **divisible** by another integer d if

$$n = dm \text{ for some integer } m.$$

  We also call n a multiple of d.

Fundamental theorem of arithmetic

Prime Factorization

Any integer $n \geq 2$ can be expressed uniquely as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \tag{1}$$

where $e_1, \ldots, e_k \in \mathbb{Z}^+$ and $p_1 < p_2 < \cdots < p_k$ are primes.
The equation (1) is called the **prime factorization** of n.

Greatest common divisor

$\gcd(a,b)=$ *largest positive integer* d that divides both a and b.

1. Factorize a and b.

Greatest common divisor

$\gcd(a, b)$= *largest positive integer* d that divides both a and b.

1. Factorize a and b.
2. Find *common prime factors* of a and b, say $p_1, \ldots, p_k$
   - Assume $p_1^{a_1} \cdots p_k^{a_k}$ is the part of a containing $p_1, \ldots, p_k$
   - Assume $p_1^{b_1} \ldots p_k^{b_k}$ is the part of b containing $p_1, \ldots, p_k$.

Greatest common divisor

$\gcd(a,b)$= *largest positive integer* d that divides both a and b.

1. Factorize a and b.
2. Find *common prime factors* of a and b, say $p_1, \ldots, p_k$
   - Assume $p_1^{a_1} \cdots p_k^{a_k}$ is the part of a containing $p_1, \ldots, p_k$
   - Assume $p_1^{b_1} \ldots p_k^{b_k}$ is the part of b containing $p_1, \ldots, p_k$.
3. Put $c_i = \min\{a_i, b_i\}$ for $i = 1, \ldots, k$. Then

$$\gcd(a,b) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}.$$

Example 1

(a) Find $\gcd(120, 500)$.

(b) Find $\gcd(124, 96)$.

Least common multiple

$\mathrm{lcm}(\mathbf{a}, \mathbf{b})$ = smallest positive integer l that is divisible by both a and b

1. Factorize a and b.

Least common multiple

$\mathrm{lcm}(\mathbf{a}, \mathbf{b})$ = smallest positive integer l that is divisible by both a and b

1. Factorize a and b.
2. Let $p_1, \ldots, p_n$ be *all primes* occurring in the prime factorization of either a or b. Assume

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \; b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where the $a_i, b_i \geq 0$ for all i.

Least common multiple

$\mathrm{lcm}(\mathbf{a}, \mathbf{b})$ = smallest positive integer l that is divisible by both a and b

1. Factorize a and b.
2. Let $p_1, \ldots, p_n$ be *all primes* occurring in the prime factorization of either a or b. Assume

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \;\; b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

   where the $a_i, b_i \geq 0$ for all i.

3. Conclusion

$$\mathrm{lcm}(a, b) = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}.$$

Example 2

Find $\operatorname{lcm}(2^3 3^5 5^7, 2^4 3^3)$ and $\operatorname{lcm}(1004, 256)$.

Relation between gcd and lcm

Lemma 1

Let a and b be positive integers. Then

$$\mathrm{lcm}(a,b) = \frac{ab}{\gcd(a,b)}.$$

Proof. Optional. See textbook.

Example. Verify that

$$\mathrm{lcm}(1004, 256) = \frac{1004 \cdot 256}{\gcd(1004, 256)}$$

Proof of a proposition

- Let p be a proposition.
- **Prove $\mathbf{p}$ (or show $\mathbf{p}$)** means proving (or showing) that the truth value of p is 1.

Direct proof

- A **direct proof** of a conditional statement $p \to q$ is done in the following steps
  1. Assume that p is true.
  2. Show that q is also true.

Direct proof

- A **direct proof** of a conditional statement $p \to q$ is done in the following steps
  1. Assume that p is true.
  2. Show that q is also true.
- Other forms of direct proofs: **constructive proof**, **exhaustive proof**, **proof by counterexample**.

Example 3 (Direct proof of conditional statement)

Prove that if n is an odd integer, then n^2 is odd.

Example 4 (Constructive proof)

An integer n is called a perfect square if it can be written as the square of an integer, say $n = k^2$.

Show that there exists a perfect square which can be written as the sum of two perfect squares.

Example 5 (Proof by counterexample)

Disprove the following proposition:

For any two real numbers a, b

$$\text{If } a < b, \text{ then } a^2 < b^2.$$

Vacuous proof

- $p \to q$ is true whenever p is false.
- If we can show that p is false, then we have a proof for $p \to q$. This type of proof is called **vacuous proof**.

Example 6

(a) Let $P(n)$ be the predicate "If $n > 1$, then $n^2 > n$" defined the domain of integers. Show that $P(0)$ is true.

(b) Prove that if n is an integer with $10 \leq n \leq 15$ which is a perfect square, then n is also a perfect cube.

Proof by contraposition

- **Proof by contraposition** uses the equivalence between a conditional proposition and its contrapositive

$$p \rightarrow q \equiv \neg q \rightarrow \neg p.$$

- In the proof by contraposition for $p \rightarrow q$, we do the following
  1. Assume that $\neg q$ is true.
  2. Show that $\neg p$ follows.

Example 7

Let n be an integer. Prove that if n^2 is odd, then n is odd.

Proof by contradiction

Assume we want to prove a proposition p.

In the method of **proof by contradiction**, we show that $\neg p \to \mathbf{F}$.

1. Suppose that p is false.

Proof by contradiction

Assume we want to prove a proposition p.

In the method of **proof by contradiction**, we show that $\neg p \rightarrow \mathbf{F}$.

1. Suppose that p is false.
2. Draw a contradiction upon the assumption given by the problem and the assumption that p is false.

Exercise 1

Prove that $\sqrt{2}$ is an irrational number.

Hint. Any rational number can be written as $\frac{a}{b}$ with $a, b \in \mathbb{Z}$.

Proof of equivalence

- Biconditional statement is the conjunction of 2 conditional statements

$$p \leftrightarrow q \equiv (p \to q) \land (q \to p).$$

Proof of equivalence

- Biconditional statement is the conjunction of 2 conditional statements

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p).$$

- To prove $p \leftrightarrow q$, we need to show
  1. $p \rightarrow q$ and
  2. $q \rightarrow p$.

Example 8

Prove that n is odd if and only if n^2 is odd.

Mathematical induction (weak induction)

Assume we want to prove $P(n)$ for all integers $n \geq n_0$.

There are two main steps in **mathematical induction**.

Mathematical induction (weak induction)

Assume we want to prove $P(n)$ for all integers $n \geq n_0$.

There are two main steps in **mathematical induction**.

1. **Basis step**: Show that $P(n_0)$ is true.
2. **Inductive step**: Prove $P(k) \to P(k+1)$ for any $k \geq n_0$.
   - Assume that $P(k)$ is true.
   - Prove $P(k+1)$.

Rationale of mathematical induction

1. By the basis step: $P(n_0)$ is true.

Rationale of mathematical induction

1. By the basis step: $P(n_0)$ is true.
2. By the inductive step

   For any $k \geq n_0$, $P(k+1)$ is true whenever $P(k)$ is true.

   So the following propositions are true:

$$P(n_0), P(n_0+1), \ldots, P(k), P(k+1), \ldots$$

$\therefore P(n)$ is true for any $n \geq n_0$.

Example 9

Use mathematical induction to prove the following propositions

$$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ for any } n \geq 1.$$

Example 9

Use mathematical induction to prove the following propositions

$$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ for any } n \geq 1.$$

1. **Basis step.** $P(1)$ is true because $1 = \frac{1 \times (1+1)}{2}$.

Example 9

Use mathematical induction to prove the following propositions

$$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ for any } n \geq 1.$$

1. **Basis step.** $P(1)$ is true because $1 = \frac{1\times(1+1)}{2}$.
2. **Inductive step.** Assume that $P(k)$ is true for some $k \geq 1$:

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}. \tag{2}$$

We need to prove $P(k+1)$:

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for any $n \geq 1$

- Adding $k + 1$ to both sides of (2), we obtain

$$1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2}+(k+1) = \frac{(k+1)(k+2)}{2},$$

proving $P(k + 1)$.

$P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for any $n \geq 1$

- Adding $k + 1$ to both sides of (2), we obtain

  $$1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2},$$

  proving $P(k + 1)$.
- Therefore, we proved $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for any $n \geq 1$ by mathematical induction.

Example 10: Geometric sum

(a) Let $r \neq 1$ be a real number, prove

$$P(n) : \sum_{k=0}^{n} ar^k = a + ar + \cdots + ar^n = \frac{a(1 - r^{n+1})}{1 - r} \text{ for any } n \geq 1.$$

(b) Use (a) to show that $1 + \frac{1}{2} + \cdots + \frac{1}{2^{n-1}} \leq 2$ for any $n \geq 1$.

Strong induction

Assume we want to prove $P(n)$ for all integers $n \geq n_0$.

There are two main steps in **strong induction**.

Strong induction

Assume we want to prove $P(n)$ for all integers $n \geq n_0$.

There are two main steps in **strong induction**.

1. **Basis step.** Show that $P(n_0)$ is true.
2. **Inductive step.** Prove the following for any $k \geq n_0$

$$(P(n_0) \wedge P(n_0 + 1) \wedge \cdots \wedge P(k)) \rightarrow P(k+1)$$

- Assume $P(n_0), \cdots, P(k)$ are true for some $k \geq n_0$.
- Prove that $P(k+1)$ is true.

Rationale of strong induction

By the basis step, $P(n_0)$ is true.

By the inductive step,

- $P(n_0)$ is true $\rightarrow P(n_0 + 1)$ is true.

Rationale of strong induction

By the basis step, $P(n_0)$ is true.

By the inductive step,

- $P(n_0)$ is true $\rightarrow P(n_0 + 1)$ is true.
- $P(n_0)$ and $P(n_0 + 1)$ are true $\rightarrow P(n_0 + 2)$ is true.

Rationale of strong induction

By the basis step, $P(n_0)$ is true.

By the inductive step,

- $P(n_0)$ is true $\to P(n_0+1)$ is true.
- $P(n_0)$ and $P(n_0+1)$ are true $\to P(n_0+2)$ is true.
- $P(n_0), P(n_0+1)$ and $P(n_0+2)$ are true $\to P(n_0+3)$ is true.

  ....

Rationale of strong induction

By the basis step, $P(n_0)$ is true.

By the inductive step,

- $P(n_0)$ is true $\rightarrow P(n_0+1)$ is true.
- $P(n_0)$ and $P(n_0+1)$ are true $\rightarrow P(n_0+2)$ is true.
- $P(n_0), P(n_0+1)$ and $P(n_0+2)$ are true $\rightarrow P(n_0+3)$ is true.

  $\dots\dots\dots\dots\dots\dots$
- $P(n_0), P(n_0+1), \dots, P(k)$ are true $\rightarrow P(k+1)$ is true.

  $\dots\dots\dots\dots\dots\dots$

  Therefore, $P(n)$ is true for any $n \geq n_0$.

Example 11

The Fibonacci sequence $\{F_n\}$ is defined by

$$\begin{aligned} F_1 &= F_2 = 1, \\ F_n &= F_{n-1} + F_{n-2} \text{ for any } n \geq 3. \end{aligned}$$

Prove that $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ for any $n \geq 1$.

Solution. Let's first try the usual induction.

Example 11

The Fibonacci sequence $\{F_n\}$ is defined by

$$\begin{aligned} F_1 &= F_2 = 1, \\ F_n &= F_{n-1} + F_{n-2} \text{ for any } n \geq 3. \end{aligned}$$

Prove that $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ for any $n \geq 1$.

Solution. Let's first try the usual induction.

1. Basis step: It's clear that $F_1 = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right)$
2. Inductive step: Assume that $F_k = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right)$.

   We need to prove $F_{k+1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right)$.

   We need to use $F_{k+1} = F_k + F_{k-1}$. But what is F_{k-1}?

Example 12: Strong induction

1. Basis step: It's clear that the claim is true for $n = 1$ and $n = 2$

Example 12: Strong induction

1. Basis step: It's clear that the claim is true for $n = 1$ and $n = 2$
2. Inductive step: Assume that the claim holds for any $n \in \{1, \ldots, k\}$

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \text{ for any } n \in \{1, \ldots, k\}$$

We need to prove that the claim holds for $n = k + 1$, that is,

$$F_{k+1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right).$$

Exercise 2

Show that if $n \geq 2$ is an integer, then n can be written as a product of primes.

Solution. Define

$$P(n)\text{: } n \text{ can be written as the product of primes.}$$

We need to prove $P(n)$ for any integer $n \geq 2$.

Exercise 2

Show that if $n \geq 2$ is an integer, then n can be written as a product of primes.

Solution. Define

$$P(n)\text{: } n \text{ can be written as the product of primes.}$$

We need to prove $P(n)$ for any integer $n \geq 2$.

Basis step.

$P(2)$ is true because 2 is a prime itself.

Inductive step

Inductive step.

Assume $P(2), P(3), \ldots, P(k)$ are true for some $k \geq 2$. We need to prove

$$P(k+1)\text{: } k+1 \text{ can be written as a product of primes.}$$

Consider two cases concerning the primality of $k+1$.

1. **Cases 1**: $k+1$ is a prime
   In this case, it is clear that $k+1$ is a product of primes.
2. **Case 2**: $k+1$ is a composite.
   There exists a prime p which is a divisor of $k+1$. Write

$$k+1 = pm \text{ for some integer } m.$$

Case 2: $k+1 = pm$ for some integer m

Idea: Use inductive assumption to write m as a product of primes.
All that left is to guarantee that $m \in \{2, \ldots, k\}$, that is, $2 \leq m \leq k$.

Case 2: $k+1 = pm$ for some integer m

Idea: Use inductive assumption to write m as a product of primes.
All that left is to guarantee that $m \in \{2, \dots, k\}$, that is, $2 \le m \le k$.

- Note that $m > 1$ because if $m = 1$, then $k+1 = p$ is a prime, a contradiction.
- Further, $m = \frac{k+1}{p} \le \frac{k+1}{2} < k+1$. So

$$2 \le m \le k.$$

Case 2: $k+1 = pm$ for some integer m

Idea: Use inductive assumption to write m as a product of primes.
All that left is to guarantee that $m \in \{2, \ldots, k\}$, that is, $2 \leq m \leq k$.

- Note that $m > 1$ because if $m = 1$, then $k+1 = p$ is a prime, a contradiction.
- Further, $m = \frac{k+1}{p} \leq \frac{k+1}{2} < k+1$. So

$$2 \leq m \leq k.$$

- By the inductive assumption, $P(m)$ is true $\Rightarrow$ m is a product of primes. Thus, $k+1 = pm$ is a product of primes.

$\therefore$ Any $n \geq 2$ is a product of primes.

Exercise 3

Let the sequence $\{a_n\}_{n=1}^{\infty}$ be defined by

$$a_1 = 3, a_2 = 15, \ a_{n+1} = 5a_n - 4a_{n-1} \text{ for any } n \geq 2$$

(a) Find a_1, a_2, a_3, a_4, a_5. Could you guess a formula for a_n?

(b) Using the correct type of induction, prove your guess in part a.

Exercise 4