Lecture 5: Proof methods

Password : proof

Table of contents

Basic number theory

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

  Two integers m and n have the **same parity** if they are both even or both odd.

Basic number theory

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

  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 (or a **multiple** of) another integer d if

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

Remark: The number of multiples of d in $\{1, \ldots, n\}$ is $\lfloor \frac{n}{d} \rfloor$.

Fundamental theorem of arithmetic

- 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 $\gcd(120, 500)$.

$120 = 2 \times 60 = 2^2 \times 30 = 2^3 \times 15 = 2^3 \times 2 \times 5$

$500 = 2^2 \times 125 = 2^2 \times 5^3$

$\gcd(120, 500) = 2^2 \times 5 = 20$

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

$124 = 2^2 \times 31$

$96 = 2^5 \times 3$

$\gcd(124, 96) = 2^2 = 4$.

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

(a) $\text{lcm}(2^3 3^5 5^7, 2^4 3^3) = 2^4 3^5 5^7$

(b) $1004 = 2^2 \times 251$

$256 = 2^8$

$\text{lcm}(1004, 256) = 2^8 \times 251$

Relation between gcd and lcm

Lemma 1

Let a and b be positive integers. Then

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

Proof. Optional. See textbook.

Example. Verify that

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

$1004 = 2^2 \times 251$

$256 = 2^8$

$\Rightarrow \gcd(1004, 256) = 2^2$

$$\operatorname{lcm}(1004, 256) = 2^8 \times 251 = \frac{1004 \cdot 256}{\gcd(1004, 256)} = \frac{2^{10} \times 251}{2^2}$$

Proof of a proposition

- Let p be a proposition.
- **Prove p** (**or show p**) means proving (or showing) that p is true. Equivalently, 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 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 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.

Since n is odd, $n = 2k+1$ for some $k \in \mathbb{Z}$.

We have

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1$$

$$m = 2k^2 + 2k$$

$$= 2m + 1$$

$\therefore$ 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.

Since $5^2 = 3^2 + 4^2$, the statement is true.

Example 5 (Proof by counterexample)

Disprove the following proposition:

For any two real numbers a, b

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

Consider $a = -2$, $b = 1$. We have

$a < b$, but $a^2 = 4 > b^2 = 1$

$\therefore$ The statement is false.

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.

since $0 > 1$ is false, the statement

$P(0)$: If $0 > 1$, then $0^2 > 0$

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.

Since there is no integer in $\{10, \ldots, 15\}$ is a perfect square, the steament is true.

Proof by contraposition

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

$$p \to q \equiv \neg q \to \neg p.$$

In the proof by contraposition for $p \to q$, we do the following

Proof by contraposition

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

$$p \to q \equiv \neg q \to \neg p.$$

In the proof by contraposition for $p \to q$, we do the following

1. Assume that $\neg q$ is true.
2. Show that $\neg p$ is true.

Example 7

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

$p \longrightarrow q$

Assume that n is even:

$n = 2k$ for some $k \in \mathbb{Z}$

Now $n^2 = 4k^2$ is even. (contradicting to the assumption that n^2 is odd)

$\therefore$ The statement is proved by contraposition.

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.

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.
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 $a, b \in \mathbb{Z}$ and $b \neq 0$.

Assume that $\sqrt{2}$ is a rational number:

$\sqrt{2} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ and $b \neq 0$ and $\gcd(a,b) = 1$ (1)

↓ a and b have no common divisor in the prime factorizations.

$a = \sqrt{2}\, b \Rightarrow a^2 = 2b^2$ (*)

Hence a^2 is even $\Rightarrow a$ is even. Hence

$a = 2a_1$ for $a_1 \in \mathbb{Z}$ (2)

By (*), $(2a_1)^2 = 2b^2 \Rightarrow 2b^2 = 4a_1^2 \Rightarrow b^2 = 2a_1^2$.

Hence b^2 is even $\Rightarrow b$ is even. So

$b = 2b_1$ for some $b_1 \in \mathbb{Z}$ (3)

By (2) & (3), 2 is a common divisor of a & $b \Rightarrow$ contradict (1).

$\therefore \sqrt{2}$ is an irrational number.

Proof by contraposition vs proof by contradiction

	Proof by contraposition	Proof by contradiction
When to use?	When proving a conditional statement $p \to q$	Use it for proving any statement: Prove p
How to start?	($p \to q \equiv \neg q \to \neg p$) Assume $\neg q$.	Assume $\neg p$
Conclusion?	$p \to q$	p is true

Proof of equivalence

- Biconditional statement is the conjunction of 2 conditional statements

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

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.

$p \quad \longleftrightarrow \quad q$

We prove 2 things:

(1) If n is odd, then n^2 is odd

proved in Example 3.

(2) If n^2 is odd, then n is odd

proved in Example 7.

Mathematical induction (weak induction)

$\forall n \geq n_0 \; P(n)$

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

(2) $P(k) \to P(k+1)$ for $k \geq n_0$

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.

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 $n \geq n_0$.

$P(n_0), P(n_0+1), P(n_0+2), \ldots$

Example 9

Use mathematical induction to prove the following propositions

$P(n) : 1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$ 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 $k \geq 1$:

$P(k) \rightarrow P(k+1)$

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

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 $P(k+1)$.

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

$P(n): 1+2+\cdots+n = \frac{n(n+1)}{2}$ 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 $P(k+1)$.

- 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

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

Basis step: $P(1)$ is true because $a + ar = \frac{a(1-r^2)}{1-r}$

Inductive step: Assume $P(k)$ is true for some $k \geq 1$:

$$a + ar + \ldots + ar^k = \frac{a(1-r^{k+1})}{1-r} \quad (*)$$

Need to prove $P(k+1)$: $a + ar + \ldots + ar^k + ar^{k+1} = \frac{a(1-r^{k+2})}{1-r}$.

Add ar^{k+1} to both sides of $(*)$:

$$a + ar + \ldots + ar^k + ar^{k+1} = \frac{a(1-r^{k+1})}{1-r} + ar^{k+1}$$

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

(a) $a + ar + \ldots + ar^k + ar^{k+1} = \frac{a(1-r^{k+1})}{1-r} + ar^{k+1}$

$= a\left(\frac{1-r^{k+1}}{1-r} + r^{k+1}\right) = a\,\frac{(1-r^{k+1}) + r^{k+1}(1-r)}{1-r}$

$= a\,\frac{1 - r^{k+1} + r^{k+1} - r^{k+2}}{1-r} = \frac{a(1-r^{k+2})}{1-r}$,

proving P(k+1).

$\therefore$ $a + ar + \ldots + ar^n = \frac{a(1-r^{n+1})}{1-r}$ for any $n \geq 1$.

(b) Apply (a) for $a = 1$, $r = \frac{1}{2}$:

If $\frac{1}{2} + \ldots + \left(\frac{1}{2}\right)^{n-1} = \frac{1 - \left(\frac{1}{2}\right)^n}{1 - 1/2} = 2\left(1 - \frac{1}{2^n}\right) < 2 \times 1 = 2$

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

For any $k \geq n_0$:

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

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 $\rightarrow P(n_0+1)$ 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.

  .....

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.

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

  .....

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

Example 11

The Fibonacci sequence $\{F_n\}_{n=1}^{\infty}$ is defined by

$$F_1 = F_2 = 1, \qquad 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

$$F_n = F_{n-1} + F_{n-2} \text{ for any } n \geq 3.$$

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 $n = 2$

$$F_1 = \frac{1}{2}\left(\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right) = 1$$

$$F_2 = \frac{1}{2}\left(\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right) = 1$$

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 $n \in \{1, \ldots, k\}$ } with $k \geq 2$

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

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

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

$F_{k+1} = F_k + F_{k-1}$ for $k \geq 2$

$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$, $\left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{3-\sqrt{5}}{2}$

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

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

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\frac{3+\sqrt{5}}{2} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\frac{3-\sqrt{5}}{2}$$

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

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

Exercise 2

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

Solution. Define

$P(n)$: n 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

$P(k+1)$: $k+1$ 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 $m \in \{2, \ldots, k\}$, 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

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

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.

a) $a_1 = 3, a_2 = 15, a_3 = 63, a_4 = 255, a_5 = 1023$

Guess: $a_n = 4^n - 1$

b) By strong induction, we prove

$P(n): a_n = 4^n - 1$ for any $n \geq 1$

Basis step:

It's clear that both $P(1): a_1 = 4^1 - 1$ and $P(2): a_2 = 4^2 - 1$ are true.

Inductive step: Assume $P(1), \ldots, P(k)$ are all true for some $k \geq 2$, that is,

$$a_n = 4^n - 1 \text{ for any } n \in \{1, \ldots, k\}$$

We prove $P(k+1)$: $a_{k+1} = 4^{k+1} - 1$. We have

$$\begin{aligned} a_{k+1} &= 5a_k - 4a_{k-1} \\ &= 5(4^k - 1) - 4(4^{k-1} - 1) \\ &= 4^{k-1}(5 \cdot 4 - 4) - 1 = 4^{k+1} - 1. \end{aligned}$$

$\therefore$ $a_n = 4^n - 1$ for any $n \geq 1$.