CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Aug 08, 2024

Lecture 06 – Strong Induction

Recap

Last week

- What are discrete structures?
- Course outline
- Chapter 1: Proofs and structures
  - Propositions: statements that can be assigned a truth value
  - Predicates: propositions with variables
  - Quantifiers
  - Theorems and different types of proofs

This week

- Induction
- Well-ordering principle
- Today: Strong Induction

Application of WOP to prove theorems (Last class)

– Proving one part of the fundamental theorem of arithmetic.

Application of WOP to prove theorems (Last class)

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of (one or more) primes

Application of WOP to prove theorems (Last class)

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of (one or more) primes

Proof by contradiction using WOP!:

- Let S be the set of all integers greater than 1 that cannot be written as a product of (one or more) primes.

Application of WOP to prove theorems (Last class)

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of (one or more) primes

Proof by contradiction using WOP!:

- Let S be the set of all integers greater than 1 that cannot be written as a product of (one or more) primes.
- If S is non-empty, there is a least element in it by WOP.

Application of WOP to prove theorems (Last class)

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of (one or more) primes

Proof by contradiction using WOP!:

- Let S be the set of all integers greater than 1 that cannot be written as a product of (one or more) primes.
- If S is non-empty, there is a least element in it by WOP.
- Call this least number n. First, n can't be a prime (why?).
- So $n = a \cdot b$, where $n > a, b > 1$.

Application of WOP to prove theorems (Last class)

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of (one or more) primes

Proof by contradiction using WOP!:

- Let S be the set of all integers greater than 1 that cannot be written as a product of (one or more) primes.
- If S is non-empty, there is a least element in it by WOP.
- Call this least number n. First, n can't be a prime (why?).
- So $n = a \cdot b$, where $n > a, b > 1$.
- Since a and b are smaller than the smallest number in S, they can be written as a product of (one or more) primes.
- Let $a = p_1 \dots p_k$ and $b = q_1 \cdots q_l$, for $k, l \geq 1$. But then $n = p_1 \cdots p_k \cdot q_1 \cdots q_l$, which is a contradiction. □

Application of WOP to prove theorems (Last class)

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of (one or more) primes

Proof by contradiction using WOP!:

- Let S be the set of all integers greater than 1 that cannot be written as a product of (one or more) primes.
- If S is non-empty, there is a least element in it by WOP.
- Call this least number n. First, n can't be a prime (why?).
- So $n = a \cdot b$, where $n > a, b > 1$.
- Since a and b are smaller than the smallest number in S, they can be written as a product of (one or more) primes.
- Let $a = p_1 \dots p_k$ and $b = q_1 \cdots q_l$, for $k, l \geq 1$. But then $n = p_1 \cdots p_k \cdot q_1 \cdots q_l$, which is a contradiction. □

Qn: How do you show uniqueness?

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness?

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j. (else, if dividing by p_i would give a smaller elt in S)

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j.
4. Without loss of generality, assume $p_1 < q_1$.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j.
4. Without loss of generality, assume $p_1 < q_1$.
5. Then, $s = p_1 \cdot P = q_1 \cdot Q$ for some $Q < P$.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j.
4. Without loss of generality, assume $p_1 < q_1$.
5. Then, $s = p_1 \cdot P = q_1 \cdot Q$ for some $Q < P$.
6. $s - p_1 Q = (q_1 - p_1)Q = p_1(P - Q) < s$ which implies $p_1 < s$.
7. But by 2., p_1 must have a unique prime factorization, so it must occur in factorization of Q or $(q_1 - p_1)$.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j.
4. Without loss of generality, assume $p_1 < q_1$.
5. Then, $s = p_1 \cdot P = q_1 \cdot Q$ for some $Q < P$.
6. $s - p_1 Q = (q_1 - p_1)Q = p_1(P - Q) < s$ which implies $p_1 < s$.
7. But by 2., p_1 must have a unique prime factorization, so it must occur in factorization of Q or $(q_1 - p_1)$.
   - If p_1 occurs in factorization of Q, then $p_1 = q_j$ so violates 3.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j.
4. Without loss of generality, assume $p_1 < q_1$.
5. Then, $s = p_1 \cdot P = q_1 \cdot Q$ for some $Q < P$.
6. $s - p_1 Q = (q_1 - p_1)Q = p_1(P - Q) < s$ which implies $p_1 < s$.
7. But by 2., p_1 must have a unique prime factorization, so it must occur in factorization of Q or $(q_1 - p_1)$.
   - If p_1 occurs in factorization of Q, then $p_1 = q_j$ so violates 3.
   - If p_1 occurs in factorization of $q_1 - p_1$ then p_1 must divide $q_1 - p_1$ and hence also q_1, which is impossible since p_1, q_1 are primes.

Fundamental theorem of arithmetic (Uniqueness)

Any integer > 1 can be written as a unique product of one or more primes

How do we show uniqueness? Proof by contradiction!

1. Let $S \neq \emptyset$ be the set integers > 1 that can be written has product of one or more primes in two ways.
2. By WOP, let s be the smallest integer in S.
3. Then $s = p_1, \ldots p_m = q_1 \ldots q_n$ where each p_i is distinct from each q_j.
4. Without loss of generality, assume $p_1 < q_1$.
5. Then, $s = p_1 \cdot P = q_1 \cdot Q$ for some $Q < P$.
6. $s - p_1 Q = (q_1 - p_1)Q = p_1(P - Q) < s$ which implies $p_1 < s$.
7. But by 2., p_1 must have a unique prime factorization, so it must occur in factorization of Q or $(q_1 - p_1)$.
   - If p_1 occurs in factorization of Q, then $p_1 = q_j$ so violates 3.
   - If p_1 occurs in factorization of $q_1 - p_1$ then p_1 must divide $q_1 - p_1$ and hence also q_1, which is impossible since p_1, q_1 are primes.
8. Hence we have a contradiction, and we conclude $S = \emptyset$. $\square$

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.
- But now it may be that $p, q \neq k$, so we can't use induction hypothesis.
  - For example, if $k + 1 = 21$, then $21 = 7 \cdot 3$, but $k = 20$, we need $P(7), P(3)$ to hold!

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.
- But now it may be that $p, q \neq k$, so we can't use induction hypothesis.
  - For example, if $k + 1 = 21$, then $21 = 7 \cdot 3$, but $k = 20$, we need $P(7), P(3)$ to hold!
- Let us strengthen our induction hypothesis. That is...

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume strong induction hypothesis, i.e., for all $1 \leq r \leq k$, $k = p_1 \cdots p_m$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume strong induction hypothesis, i.e., for all $1 \leq r \leq k$, $k = p_1 \cdots p_m$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.
- By the stronger hypothesis, we can write $p = p_1 \ldots p_k$ and $q = q_1 \cdots q_l$.
- Therefore $k + 1 = p_1 \cdots p_k \cdot q_1 \cdots q_k$.
- Thus, the statement holds for all $n > 1$. □

Strong Induction

Strong Induction

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $(P(0) \wedge P(1) \wedge \cdots \wedge P(k)) \implies P(k+1)$ then $P(n)$ is true for all $n \in \mathbb{N}$. (Induction Step)

Strong Induction

Strong Induction

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $(P(0) \wedge P(1) \wedge \cdots \wedge P(k)) \implies P(k+1)$ then $P(n)$ is true for all $n \in \mathbb{N}$. (Induction Step)

Induction

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

Theorem: Strong Induction iff Induction iff WOP

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.
- Base case: n=1.

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.
- Base case: n=1.
- Assume for groups of $2k+1$ students. Now consider a group of $2k+3$ students.

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.
- Base case: n=1.
- Assume for groups of $2k+1$ students. Now consider a group of $2k+3$ students.
- Consider the closest pair A-B and divide into two cases based on whether someone threw rocket at them.

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r $(q, r \in \mathbb{N})$, such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r $(q, r \in \mathbb{N})$, such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on k'.

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on k'.
5. By Ind Hyp, $k' = q'm + r'$ for some q', $0 \leq r' < m$.

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r $(q, r \in \mathbb{N})$, such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k+1 = q^*m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on k'.
5. By Ind Hyp, $k' = q'm + r'$ for some q', $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r $(q, r \in \mathbb{N})$, such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k+1 = q^*m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on k'.
5. By Ind Hyp, $k' = q'm + r'$ for some q', $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$
7. Then, $q^*m + r^* = (q'+1)m + r' = q'm + r' + m = k' + m = ((k+1) - m) + m = k + 1$. □

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r $(q, r \in \mathbb{N})$, such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k+1 = q^*m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on k'.
5. By Ind Hyp, $k' = q'm + r'$ for some q', $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$
7. Then, $q^*m + r^* = (q'+1)m + r' = q'm + r' + m = k' + m = ((k+1) - m) + m = k + 1$. □

Qns: Show uniqueness (H.W).

Another exercise by Strong Induction

Quotient-Remainder Theorem

For any $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient q and remainder r $(q, r \in \mathbb{N})$, such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on n.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should q and r be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k+1 = q^*m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on k'.
5. By Ind Hyp, $k' = q'm + r'$ for some q', $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$
7. Then, $q^*m + r^* = (q'+1)m + r' = q'm + r' + m = k' + m = ((k+1) - m) + m = k + 1$. □

Qns: Show uniqueness (H.W). Also, what if $m, n \in \mathbb{Z}, m \neq 0$?