Discrete Mathematics

Lecture 4: Properties of Integers: Mathematical Induction

Murat Ak

Akdeniz University

First Created: November 7, 2016,
Last Modified: October 25, 2024

Table of contents

1. Well-Ordering Principle: Mathematical Induction
2. Recursive Definitions
3. The Division Algorithm: Prime Numbers
4. The Greatest Common Divisor: The Euclidean Algorithm
5. Fundamental Theorem of Arithmetic
6. Summary

Well Ordering Principle

It is possible to define positive integers as:

$$\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\} = \{x \in \mathbb{Z} \mid x \geq 1\}$$

However, if we try to do likewise for rational and real numbers,

$$\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x > 0\} \text{ and } \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$$

but we cannot represent $\mathbb{Q}^+$ and $\mathbb{R}^+$ as we did for $\mathbb{Z}^+$. Why?

Well ordering principle

Every nonempty subset of $\mathbb{Z}^+$ contains a smallest element.
Hence we say $\mathbb{Z}^+$ is well-ordered.

Mathematical Induction

Mathematical Induction

Let $S(n)$ denote an open statement that involves one or more occurrences of the variable n which represents a positive integer.

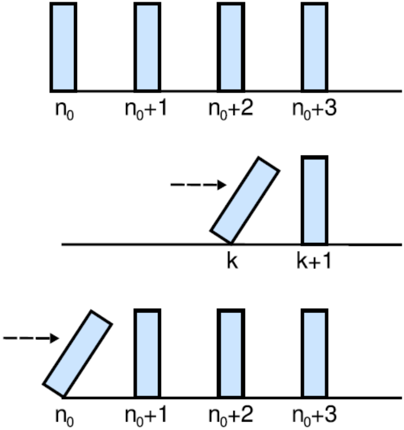
1. If $S(1)$ is true, and
2. If whenever $S(k)$ is true for some particular but arbitrarily chosen $k \in \mathbb{Z}^+$, then $S(k+1)$ is true;

then $S(n)$ is true for all $n \in \mathbb{Z}^+$

Simple Proof.

This is just an application of Modus Ponens continuously. □

Proof of Mathematical Induction



Example

Example

Prove the following for $n \in \mathbb{Z}^+$

$$S(n) : \sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n = \frac{n^2 + n}{2}$$

Step 1: Obviously, $S(1)$ is true because $1 = (1^2 + 1)/2$.
Step 2: Let's assume this holds for an arbitrary k and show the same holds for $k + 1$ i.e. $(S(k) \Rightarrow S(k + 1))$.

Example

Example

Assume that the following holds for some $k \in \mathbb{Z}^+$:

$$S(k) : \sum_{i=1}^{k} i = 1 + 2 + 3 + \ldots + k = \frac{k^2 + k}{2}$$

We need to show that

$$S(k+1) : \sum_{i=1}^{k+1} i = 1+2+3+\ldots+k+1 = \frac{(k+1)^2 + (k+1)}{2}$$

Example

Example

$$S(k+1): \sum_{i=1}^{k+1} i = 1+2+3+\ldots+k+(k+1) = \sum_{i=1}^{k} i + (k+1)$$

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

$$= \frac{k^2+3k+2}{2} = \frac{(k+1)^2+(k+1)}{2}$$

and this concludes the proof.

Example

Example 4.6

Prove the following for $n \in \mathbb{Z}^+$

$$S(n) : \sum_{i=1}^{n} i = 1 + 2 + 3 + \ldots + n = \frac{n^2 + n + 2}{2}$$

Let's assume this holds for an arbitrary k and show the same holds for $k + 1$.

Example

Example 4.6

Assume that the following holds for some $k \in \mathbb{Z}^+$:

$$S(k) : \sum_{i=1}^{k} i = 1 + 2 + 3 + \ldots + k = \frac{k^2 + k + 2}{2}$$

We need to show that

$$S(k+1) : \sum_{i=1}^{k+1} i = 1+2+3+\ldots+k+1 = \frac{(k+1)^2 + (k+1) + 2}{2}$$

Example

Example 4.6

$$S(k+1) : \sum_{i=1}^{k+1} i = 1+2+3+\ldots+k+(k+1) = \sum_{i=1}^{k} i+(k+1)$$

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

$$= \frac{k^2+3k+4}{2}$$

Check this with an example. Say 3. What's wrong?

Example

Theorem

$\forall n \in \mathbb{Z}^+ [1 + 3 + 5 + \cdots + (2n - 1) = n^2]$

Proof.

- $n = 1 : \; 1 = 1^2$
- $n = k : \;$ Assume $[1 + 3 + 5 + \cdots + (2k - 1) = k^2]$
- $n = k + 1 :$
  $[1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + 2k + 1]$
  $= (k + 1)^2$

□

Example

Theorem

$\forall n \in \mathbb{Z}^+, n \geq 4 \; [2^n < n!]$

Proof.

- $n = 4 : \; 2^4 = 16 < 24 = 4!$
- $n = k : \;$ Assume $[2^k < k!]$
- $n = k + 1 :$
  $2^{k+1} = 2 \cdot 2^k < 2 \cdot k! < (k+1) \cdot k! = (k+1)!$

□

Example

Theorem

$\forall n \in \mathbb{Z}^+, n \geq 14 \ \exists i, j \in \mathbb{N} \ [n = 3i + 8j]$

Proof.

- $n = 14$: $14 = 3 \cdot 2 + 8 \cdot 1$
- $n = k$: Assume $[k = 3a + 8b]$ (So, $i = a, j = b$)
- $n = k + 1$: Since we assumed $[k = 3a + 8b]$, where $k \geq 14$, note that either $a \geq 5$ or $b \geq 1$.
  - If $b \geq 1$, then $k + 1 = k - 8 + 3 \cdot 3 = 3(a + 3) + 8(b - 1)$
  - If $a \geq 5$, then $k + 1 = k - 5 \cdot 3 + 2 \cdot 8 = 3(a - 5) + 8(b + 2)$

□

Strong Induction (Alternative Form)

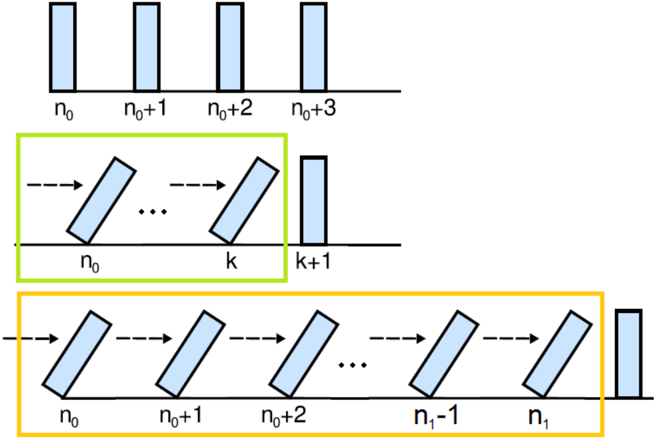
Mathematical Induction Strong Form

Let $S(n)$ denote an open statement that involves one or more occurrences of the variable n which represents a positive integer. Also let $n_0, n_1 \in \mathbb{Z}^+$ with $n_0 \leq n_1$.

1. If $S(n_0), S(n_0+1), S(n_0+2), \cdots, S(n_1-1)$ and $S(n_1)$ are true, and
2. If whenever $S(n_0), S(n_0+1), S(n_0+2), \cdots, S(k-1)$ and $S(k)$ are true for some particular but arbitrarily chosen $k \in \mathbb{Z}^+$ where $k \geq n_1$, then the statement $S(k+1)$ is true;

then $S(n)$ is true for all $n \geq n_0$.

Proof of Mathematical Induction



Strong Induction (Alternative Form)

Theorem

$\forall n \in \mathbb{Z}^+$, $n \geq 2$ n can be written as the product of prime numbers.

Proof.

- $n = 2$: $2 = 2$
- assume that the theorem is true for $\forall i \leq k$
- $n = k + 1$:
  - if prime: $n = n$
  - if not prime: $n = u \cdot v$ and $u < k \wedge v < k \Rightarrow$ both u and v can be written as the product of prime numbers

□

Strong Induction (Alternative Form)

Strong induction = induction

Strong induction and classical induction are equivalently powerful (i.e. if we can prove a proposition with one, we can also prove it using the other.) But sometimes it is much easier to prove propositions using strong induction while it becomes much more tricky to do so using classical induction (as in the previous example).

Recursive Definitions

- When we have an integer sequence $b_n = b_0, b_1, b_2, \ldots$, where $b_n = 2n$ for all $n \in \mathbb{N}$, given its index, we can immediately find any term in this series. For example, $b_{100} = 200$. Because we have an explicit formula for terms.
- However, there may be cases where we cannot express a series with an explicit formula. We may rather express every other term by using previous terms:

$$a_0 = 1, a_1 = 2, a_2 = 3,$$

$$a_n = a_{n-1} + a_{n-2} + a_{n-3}, n \geq 3.$$

Recursive Definitions

$$a_0 = 1, a_1 = 2, a_2 = 3,$$

$$a_n = a_{n-1} + a_{n-2} + a_{n-3}, n \geq 3.$$

Here we have a recursive definition of a series where the first three terms are directly assigned and the terms for the rest of the series is defined as the sum of three previous terms. For instance, $a_3 = a_2 + a_1 + a_0 = 3 + 2 + 1 = 6$.

Equivalent explicit and recursive formulas

- Sometimes, it is easy to find an explicit formula for a given recursive one. For example, the following two formulas are the same:
    - $b_n = 2n, \forall n \in \mathbb{N}$
    - $b_0 = 0, b_n = b_{n-1} + 2$
    - They both result in $0, 2, 4, 6, 8, \ldots$
- Sometimes, it is not so obvious.
    - $$a_0 = 1, a_1 = 2, a_2 = 3,$$ $$a_n = a_{n-1} + a_{n-2} + a_{n-3}, n \geq 3.$$
    - $1, 2, 3, 6, 11, 20, 37, 68, \ldots$

Significance in Computer Science

- Recursive formulas are very important in computer science because
  - Many algorithms use approaches like divide-and-conquer which uses recursion idea
  - These algorithms find the solution by finding solutions for sub-problems
  - So, complexity of an algorithm may be defined as a recursive formula

Example Algorithm: Towers of Hanoi

1. Only one disk can be moved at a time.

2. Valid moves: Take the *uppermost* disk from one of the stacks, and place it on top of another stack.

3. No disk may be placed on top of a smaller disk.

Example Algorithm: Towers of Hanoi

- One possible solution (for n disks) is a recursive one.
- Let's name the stacks A, B, and C, where we move disks from A to C.
- To move n disks from A to C:
    1. move $n-1$ disks from A to B.
    2. move disk n from A to C
    3. move $n-1$ disks from B to C so they sit on disk n
- Note that the 1st and 3rd steps are smaller versions of the same problem.

Example Algorithm: Towers of Hanoi

- So, time complexity for moving n disks can be expressed using a recursive formula:
- $T(n) = T(n-1) + 1 + T(n-1),\ T(1) = 1$
- $T(n) = 2T(n-1) + 1,\ T(1) = 1$
- So, what is $T(100)$? (When we have 100 disks to move)
- Do we have to find all $T(i)$ for all $1 \leq i \leq 100$?

Example Algorithm: Towers of Hanoi

- Fortunately, we can express the same series with an explicit formula:
- $T(n) = T(n-1) + 1 + T(n-1),\ T(1) = 1$
- $T(n) = 2^n - 1$
- This equivalence can be proven using mathematical induction.

Example Algorithm: Towers of Hanoi

Theorem (Towers of Hanoi, recursive solution time complexity)

$T(n) = 2^n - 1$

Proof.

1. Basis step: For $n = 1$, we have $2^1 - 1 = 1$ which is true.
2. Inductive hypothesis: we assume that the equality holds for arbitrary $k \geq 1$: $T(k) = 2^k - 1$.
3. For $k + 1$, according to the recursive formula we have $T(k+1) = 2T(k) + 1$. Since $T(k)$ is assumed to be $2^k - 1$, we conclude that $T(k+1) = 2(2^k - 1) + 1$. Then, $T(k+1) \overset{conc}{=} 2^{k+1} - 1 \overset{thm}{=} T(k+1)$.

□

Towers of Hanoi Example, Conclusion

- Some questions are solved recursively
- We want to calculate the time complexity of these algorithms
- Then we have to deal with recursive formulas
- We can use mathematical proof techniques such as induction to prove time complexities of these algorithms

Induction Examples

Definition: Harmonic Numbers

$$H_1 = 1$$

$$H_2 = 1 + \frac{1}{2}$$

$$H_3 = 1 + \frac{1}{2} + \frac{1}{3}$$

Sum of Harmonic Numbers

Prove that

$$\forall n \in \mathbb{Z}^+, \sum_{j=1}^{n} H_j = (n+1)H_n - n$$

Induction Examples

Harmonic Number Exercises

For all $n \in \mathbb{N}$, prove that $1 + \left(\frac{n}{2}\right) \leq H_{2^n}$

Harmonic Number Exercises

For all $n \in \mathbb{Z}^+$, prove that

$$\sum_{j=1}^{n} jH_j = \left[\frac{n(n+1)}{2}\right] H_{n+1} - \left[\frac{n(n+1)}{4}\right]$$

Induction Examples

Binary search

For all $n \geq 0$, let $A_n \subset \mathbb{R}$, where $|A_n| = 2^n$ and the elements of A_n are listed in ascending order. If $r \in \mathbb{R}$, prove that in order to determine whether $r \in A_n$, we must compare r with no more than $n + 1$ elements in A_n.

Induction Examples

Definition: Fibonacci Numbers

$$F_0 = 0$$

$$F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2}$$

Sum of Squares of Fibonacci Numbers

Find (conjecture) a formula for

$$\sum_{i=0}^{n} F_i^2$$

and prove your conjecture.

Induction Examples

Definition: Lucas Numbers

$$L_0 = 2$$

$$L_1 = 1$$

$$L_n = L_{n-1} + L_{n-2}$$

Lucas Fibonacci Relation

Prove that

$$\forall n \in \mathbb{Z}^+ L_n = F_{n-1} + F_{n+1}$$

Division

Definition (divisor, multiple)

If $a, b \in \mathbb{Z}$ and $b \neq 0$, we say that b divides a, and write $b|a$, if there is an integer such that $a = bn$. When this occurs, we say that b is a divisor of a, or a is a multiple of b.

Divison Properties

For all $a, b, c \in \mathbb{Z}$:

- $1|a$ and $a|0$
- $(a|b \wedge b|a) \Rightarrow a = \pm b$
- $(a|b \wedge b|c) \Rightarrow a|c$
- $(a|b) \Rightarrow \forall x \in \mathbb{Z}[a|bx]$
- $x = y + z \Rightarrow$ if b divides any two of x, y, z, then b divides the other as well.

- $(a|b \wedge a|c) \Rightarrow \forall x, y \in \mathbb{Z}[a|(bx + cy)]$ (The expression $bx + cy$ is called a linear combination of b and c)
- If for $1 \leq i \leq n$, $c_i \in \mathbb{Z}$, and $a|c_i$, then $[a|(c_1x_1 + c_2x_2 + \ldots + c_nx_n)]$ where $x_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.

Infinitely many primes

Lemma

If $n \in \mathbb{Z}^+$ and n is composite, then there exists a prime p such that $p|n$.

Theorem

There are infinitely many primes.

Euclid's proof.

Suppose there are finitely many primes: $p_1, p_2, \ldots, p_k$. Let $x = p_1 p_2 p_3 \ldots p_k + 1$. Then for all i, $x > p_i$ (so it cannot be a prime because it is not in the finite list) and $p_i \nmid x$ (so it must be a new prime due to the lemma above) → contradiction. So, there must be infinitely many primes. □

The Division Algorithm

Theorem (Division Algorithm)

If $a, b \in \mathbb{Z}$*, with* $b > 0$*, then there exists a unique* $q, r \in \mathbb{Z}$ *with* $a = qb + r, 0 \leq r < b$*.*

Proof.

Left as an exercise. □

Greatest Common Divisor

Definition (Common divisor)

For $a, b \in \mathbb{Z}$, a positive integer c is said to be a common divisor of a and b if $c|a \wedge c|b$.

Definition (GCD)

For $a, b \in \mathbb{Z}$, a positive integer c is said to be the greatest common divisor of a and b if c is a common divisor and it is the greatest such number, and denoted $gcd(a, b)$.

Theorem (Uniqueness of GCD)

For all $a, b \in \mathbb{Z}$, there exists a unique positive integer c that is the greatest common divisor of a and b.

Properties of the Greatest Common Divisor

- For all $a, b \in \mathbb{Z}^+$, the GCD of a, b exists and it is unique.
- $gcd(a, b) = gcd(b, a)$
- $gcd(-a, b) = gcd(a, -b) = gcd(-a, -b) = gcd(a, b)$

Finding the GCD of Two Integers

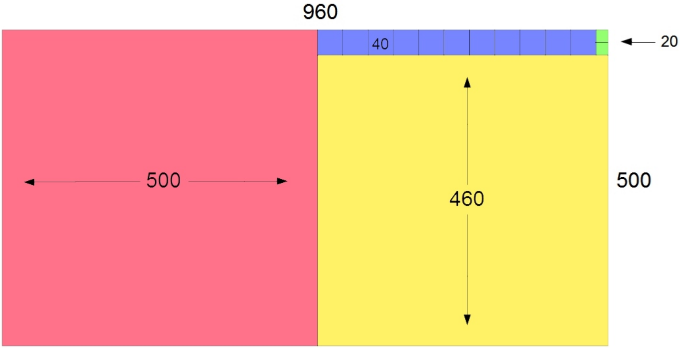
Theorem (Euclidean Algorithm)

Let $a, b \in \mathbb{Z}^+$, set $r_0 = a$ and $r_1 = b$ and apply the division algorithm until r_n is the last non-zero remainder:

$$
\begin{array}{ll}
r_0 = q_1 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_2 r_2 + r_3 & 0 < r_3 < r_2 \\
r_2 = q_3 r_3 + r_4 & 0 < r_4 < r_3 \\
\ldots & \ldots \\
r_i = q_{i+1} r_{i+1} + r_{i+2} & 0 < r_{i+2} < r_{i+1} \\
\ldots & \ldots \\
r_{n-2} = q_{n-1} r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} = q_n r_n &
\end{array}
$$

Euclidean Algorithm Visualization

Start with a rectangle with side lengths *a* and *b* and repeatedly remove maximal squares from the remaining rectangular area



Extended Euclidean Algorithm to Find Coefficients

Find two integers a and b such that $1914a + 899b = gcd(1914, 899)$.
First use Euclid's algorithm to find the GCD:

$$
\begin{aligned}
1914 &= 2 \times 899 + 116 && (1)\\
899 &= 7 \times 116 + 87 && (2)\\
116 &= 1 \times 87 + 29 && (3)\\
87 &= 3 \times 29 + 0 && (4)
\end{aligned}
$$

Extended Euclidean Algorithm to Find Coefficients

From this, the last non-zero remainder GCD is 29. Now we use the extended algorithm:

$$29 = 116 + (-1) \times 87 \tag{5}$$

$$87 = 899 + (-7) \times 116 \tag{6}$$

Extended Euclidean Algorithm to Find Coefficients

Substituting for 87 in the first equation, we have

$$\begin{aligned} 29 &= 116 + (-1) \times (899 + (-7) \times 116) && (7)\\ &= (-1) \times 899 + 8 \times 116 && (8)\\ &= (-1) \times 899 + 8 \times (1914 + (-2) \times 899) && (9)\\ &= 8 \times 1914 + (-17) \times 899 && (10)\\ &= 8 \times 1914 - 17 \times 899 && (11) \end{aligned}$$

Since we now wrote the GCD as a linear combination of two integers, we terminate the algorithm and conclude
$a = 8, b = -17$

Coprimeness

Definition (Relatively prime (Co-prime))

Integers a and b are relatively prime if $gcd(a, b) = 1$.

Theorem

If $a, b, c \in \mathbb{Z}^+$, the Diophantine equation $ax + by = c$ has an integer solution $x = x_0, y = y_0$ if and only if $gcd(a, b)|c$.

Corollary

$gcd(a, b)$ is the smallest positive integer we can write as a linear combination of a and b.

$gcd(42, 70) = 14 \rightarrow 42x + 70y = 14$ (Here, 14 is the smallest positive integer for which we can have integer solutions)

Least Common Multiple

Definition (Common Multiple)

For $a, b \in \mathbb{Z}$, a positive integer c is said to be a common multiple of a and b if $a|c \wedge b|c$.

Definition (LCM)

For $a, b \in \mathbb{Z}$, a positive integer c is said to be the least common multiple of a and b if c is a common multiple and it is the smallest such number, and denoted $lcm(a, b)$.

Theorem (Uniqueness of LCM)

For all $a, b \in \mathbb{Z}$, there exists a unique positive integer c that is the least common multiple of a and b.

Least Common Multiple

Suppose we have many rectangles of size lengths a, b. The smallest square area that can be tiled with these rectangles has side length $lcm(a, b)$.

Theorem (GCD and LCM)

For all $a, b \in \mathbb{Z}^+$, $ab = lcm(a, b) \cdot gcd(a, b)$.

Fundamental Theorem of Arithmetic

Lemma

If $a, b \in \mathbb{Z}^+$, and p is prime, then $p|ab \Rightarrow (p|a \vee p|b)$.

Lemma

If $a_i \in \mathbb{Z}^+$ for all $1 \leq i \leq n$, and p is prime, then $p|a_1a_2 \ldots a_n \Rightarrow p|a_i$ for some $1 \leq i \leq n$.

Theorem (The Fundamental Theorem of Arithmetic)

Every integer $n > 1$ can be written as a product of primes uniquely.

Using The Fundamental Theorem of Arithmetic

Example 4.41: $\sqrt{2}$ is irrational

Prove that $\sqrt{2}$ is irrational ($\sqrt{2} \notin \mathbb{Q}$)

Proof.

Assume that $\sqrt{2} \in \mathbb{Q}$. Then we can write $\sqrt{2} = a/b$ for some $a, b \in \mathbb{Z}^+$ and $gcd(a, b) = 1$ (otherwise we cancel out common divisors). Then,
$2 = a^2/b^2 \Rightarrow 2b^2 = a^2 \Rightarrow 2|a^2 \Rightarrow 2|a$. Then we write $a = 2c$ for some $c \in \mathbb{Z}^+$. We get $2b^2 = (2c)^2 \Rightarrow b^2 = 2c^2$. Then $2|b^2 \Rightarrow 2|b$. Now, since 2 divides both a and b, we have a contradiction with $gcd(a, b) = 1$. Therefore $\sqrt{2} \notin \mathbb{Q}$. □

WHAT TO REMEMBER

You should learn the following from this section:

- In which circumstances you can use induction (and also which form) to make mathematical proofs
- How to apply mathematical induction *correctly*
    - Base step!
    - Inductive hypothesis
    - Show for the next one
- The distinction between explicit formulas and recursive formulas and
    - Why we encounter recursive formulas
    - Why we are trying to turn them into explicit ones

WHAT TO REMEMBER

You should learn the following from this section:

- That corresponding closed formulas of some recursive formulas have not been found.
- How to use mathematical induction to show prove recursive formulas
- Properties of integer division (Thm 4.3)
- The Division Algorithm (Thm 4.5)

WHAT TO REMEMBER

You should learn the following from this section:

- The famous Euclidean GCD Algorithm and how to use it
- How to show two numbers (or expressions) are relatively prime using Euclidean Algorithm. (Ex 4.35)
- How Euclidean Algorithm can be implemented
- Relation between EA and tiling a rectangle with maximum squares (graphical representation of it)

WHAT TO REMEMBER

You should learn the following from this section:

- Fundamental Theorem of Arithmetic and how it can be used in proofs
- Proving $\sqrt{2}$ is irrational
- How to find prime factors of an integer
- Integer factorization problem (product of two large primes)