📢

Chapters 4, 5, 6

[4] Elementary Number Theory and Methods of Proof

▼ [4.1] Direct Proof and Counterexample I: Introduction

- As a basis, number theory will be used for this chapter
- The three properties of equality (for all objects A, B, and C):
  1. $A = A$
  2. If $A = B$, then $B = A$
  3. If $A = B$ and $B = C$, then $A = C$
- If one object equals another, then they may act as substitutes for each other
- We assume that there is no integer between 0 and 1
- The set of all integers is closed under addition, subtraction, and multiplication, or in other words, those operations between integers will always yield integers

Even, Odd, Prime, and Composite Integers

$$\begin{aligned} n \text{ is even} &\iff n = 2k \text{ for some integer } k \\ n \text{ is odd} &\iff n = 2k+1 \text{ for some integer } k \end{aligned}$$

- Using these formal definitions, you can prove whether or not some numbers are even or odd
- 0 is even because $0 = 2 \cdot 0$

$$n \text{ is prime} \iff \begin{array}{l} \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \\ \text{then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1. \end{array}$$

$$n \text{ is composite} \iff \begin{array}{l} \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs \\ \text{and } 1 < r < n \text{ and } 1 < s < n. \end{array}$$

Proving Existential Statements

- Existential statement $\exists x \in D$ such that $Q(x)$ is true if, and only if, $Q(x)$ is true for at least one x in D
- **Constructive proofs of existence** are used to prove an existential statement
    - This includes finding an x in D that makes $Q(x)$ true or providing directions to reach such an x
- The main logical principle behind this is **existential generalization** since one example is needed to prove it
- The **nonconstructive proof of existence** is showing the existence of some value x that makes $Q(x)$ true through axioms are proved theorems or through assumptions that no x causes a contradiction
- Between constructive and nonconstructive proofs, the main advantage of constructive proofs is that they provide actual directions for reaching x

Disproving Universal Statements by Counterexample

- Universal statement $\forall x \in D$, if $P(x)$ then $Q(x)$ is true if, and only if $Q(x)$ is true for all x in D
- As stated in chapter 3, some value of x where $P(x)$ is true but $Q(x)$ is false is a **counterexample** to the statement
- Similar to proving existential statements, just one example is needed

Proving Universal Statements

- There are multiple methods for proving universal statements are true for all x in D
- **Method of exhaustion** is a brute force method where all examples are given, meaning that it is only viable for limited domains
- **Universal generalization** or **generalizing from the generic particular** is by showing that all elements of a set has a particular property
    - This can be done by choosing a *particular* yet *arbitrarily* chosen element
- The method of **direct proof** is when a universal generalization is applied to a property of the form: "If $P(x)$ then $Q(x)$"
    1. Express the statement to be proved in the form: "For every $x \in D$, if $P(x)$ then $Q(x)$"
        a. *Not a required step for the actual proof*

2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true
    1. Can be abbreviated to "Suppose $x \in D$ and $P(x)$"
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference

- Ex: Prove that the sum of any two even integers are even
    - Suppose m and n are any *particular but arbitrarily chosen* even integers
    - By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s
    - Thus,

$$\begin{aligned} m + n &= 2r + 2s && \text{(By substitution)} \\ &= 2(r + s) && \text{(By factoring out 2)} \end{aligned}$$

    - Let $t = r + s$
    - t is the sum integers, therefore it is also an integer

$$m + n = 2t \qquad \text{(By substitution)}$$

    - This follows the form of an even, $2 \cdot (\text{integer})$, thus $m + n$ is even
- Another basic law of logic is **existential instantiation** which says that if something exists, then it can be given a unique name

Getting Proofs Started

- The starting point of any proof is not dependent on the content, but rather the linguistic style
    - Thus, you do not have to understand a theorem completely to begin a proof
- Generally, it is very helpful to use variables and quantifiers
- For example: "Every complete bipartite graph is connected"
    - *Even when not knowing anything about them, it is still possible to set up a proof*
    - *Formally, this is "For every graph G, if G is completely bipartite, then G is connected"*
    - Suppose G is a *particular but arbitrarily chosen* graph such that G is a complete bipartite

. . .

- Therefore, G is connected

▼ [4.2] Direct Proof and Counterexample II: Writing Advice

Directions for Writing Proofs of Universal Statements

- There are multiple rules of style for the final versions of proofs, and the following are conventional for universal statements

1. Copy the statement of the theorem to be proved on your paper
   a. This allows it to be referenced
2. Clearly mark the beginning of your proof with the word: "proof"
   a. This separates discussion from the proof itself
3. Make your proof self-contained
   a. Every variable in the proof should be explained
4. Write your proof in complete, grammatically, correct sentences
   a. Symbols and shorthand abbreviations can still be helpful, but should be incorporated into sentences
5. Keep your reader informed about the status of each statement in your proof
   a. Statements should be properly prefaced so readers know if a statement is an assumption or established, for example
6. Give a reason for each assertion in your proof
   a. Assertions should have an obvious source, whether it be the hypothesis or from a definition of terms, and can be prefaced by stating such outright
7. Include the "little words and phrases" that make the logic of your arguments clear
   a. Transition words can be helpful for showing that a sentence follows from previous ones
8. Display equations and inequalities
   a. Specifically, they should be displayed on separate lines to increase readability

Variations among Proofs

- Even then, proofs by different people using the same logic and steps have variations

Common Mistakes

- **Arguing from examples**
    - A general statement cannot be proved just because it holds true for some individual cases
- **Using the same letter to refer to different things**
    - A good way to think about it is like using global variables in a programming language
- **Jumping to conclusions**
    - If steps are left out, truths can be alleged without proper proof
- **Assuming what is to be proved**
    - A variation of jumping to conclusions
    - An assumption made that is essentially just what the proof is trying to prove
- **Confusion between what is known and what is still to be shown**
    - Another variation of jumping to conclusions
    - Incorrect language may cause confusion by making something seem like a statement
- **Use of *any* when the correct word is *some***
    - These words do not mean the same thing in all contexts, as *any* could possibly represent a universal quantifier
- **Misuse of the word *if***
    - Using *if* in lieu of *because* does not always work because they do not mean the same thing in every context
    - For instance, *if* could unintentionally imply doubt in a statement
- For instance, here is a proof with a mistake attempting to prove that if n is any even integer, then $(-1)^n = 1$
    - Suppose n is any even integer
    - By definition of even, $n = 2a$ for some integer a
    - Thus,

$$\begin{aligned}(-1)^n &= (-1)^{2a} && \text{(By substitution)}\\ &= \left((-1)^a\right)^2 && \text{(By law of exponents)}\\ &= 1 && \text{(An squared number is nonnegative)}\end{aligned}$$

    - While this proof correctly shows that the result is 1, the proof is not valid because the last step jumps to a conclusion
        - *It is not sensible for it to claim that the square of $(-1)^a$ is 1*

Showing That an Existential Statement is False

- Given that the negation of an existential statement is universal, to prove an existential statement false, its negation must be proved
- Thus, it is very similar to proving a universal statement true
- Ex: There is a positive integer n such that $n^2 + 3n + 2$ is prime
    - *This is a false statement and can be proven false by negating it and proving the negation*
    - Suppose n is any *particular but arbitrarily chosen integer*
    - *Here, we are showing that all values of* n *are not prime*

$$n^2 + 3n + 2 = (n+1)(n+2) \qquad \text{(By factoring)}$$

    - $(n+1)$ and $(n+2)$ are both integers because they are sums of integers
    - $(n+1)$ and $(n+2)$ are both greater than 1 because $n \geq 1$
    - Therefore, $n^2 + 3n + 2$ is a product of two integers that are both greater than 1
    - By definition of prime, $n^2 + 3n + 2$ cannot be a prime

▼ [4.3] Direct Proof and Counterexample III: Rational Numbers

- A real number r is **rational**, if and only if, it can be expressed as a quotient of two integers with a nonzero denominator
    - Otherwise, it is an irrational number

$$r \text{ is rational} \iff \exists \text{ integers } a \text{ and } b \text{ such that } r = \tfrac{a}{b} \text{ and } b \neq 0.$$

- This definition can be used to prove the rationality of some numbers
    - 0 is a rational number

$$0 = \frac{0}{1}$$

    - 0.281 is a rational number

$$0.281 = \frac{281}{1000}$$

  - $\frac{2}{0}$ is not a rational number because it is not a real number
  - $0.\overline{12}$ is rational number even though the decimal is infinite and can be proved using algebra
    - This holds true for any endlessly repeating decimal as they can all be solved for in the following way

$$\begin{aligned} &\text{Let } x = 0.\overline{12} \\ x &= 0.\overline{12} && (1) \\ 100x &= 12.\overline{12} && (2) \\ 100x - x &= 12.\overline{12} - 0.\overline{12} && (3) \\ 99x &= 12 && (4) \\ x &= \frac{12}{99} && (5) \end{aligned}$$

- If m and n are integers and neither m nor n is zero, $\frac{m+n}{mn}$ is a rational number since operations between two integers always result in an integer, meaning $m+n$ and mn are integers
  - mn also does not equal zero due to the following property
- According to the **zero product property**, if neither of two real numbers are zero, then their product cannot be zero

More on Generalizing from the Generic Particular

- When claiming that a property holds true for all elements in a domain, there has to be a way to prove it for an arbitrarily chosen value
- While problems are generally stated informally, they can be easier to solve when written in formal language
- In a proof, saying that particular variables are any particular number from a particular domain is a **generalization from the generic particular**
- **Theorem 4.3.1:** Every integer is a rational number
  - Suppose m is a *particular but arbitrarily chosen* integer
  - Thus, $m = m \cdot 1$

$$\begin{aligned} m &= m \cdot 1 \\ \frac{m}{1} &= m \qquad\qquad \text{(Divide both sides by 1)} \end{aligned}$$

- m and 1 are both integers, and $1 \neq 0$, therefore m may be expressed as the quotient of two integers with a nonzero denominator
- m is rational

Proving Properties of Rational Numbers

- **Theorem 4.3.2: T**he sum of any two rational numbers is rational
  - *The first step for a proof should be formalizing the statement that needs to be proved*

$$\forall \text{ real numbers } r \text{ and } s, \\ \text{if } r \text{ and } s \text{ are rational then } r+s \text{ is rational.}$$

  - *Afterward, establish a starting point*
  - Suppose r and s are any particular but arbitrarily chosen real numbers such that r and s are rational
  - *Or even more simply, "Suppose r and s are any rational numbers"*
  - *After this, think of how it can be shown that $r + s$ is rational*

$$r = \tfrac{a}{b} \text{ and } s = \tfrac{c}{d} \text{ for some integers } a\ b, c, \text{ and } d \text{ where } b \neq 0 \text{ and } d \neq 0.$$

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} && \text{(By substitution)} \\ &= \frac{ad}{bd} + \frac{bc}{bd} && \text{(By common denominator)} \\ &= \frac{ad+bc}{bd} && \text{(By adding fractions with equal denominators)} \end{aligned}$$

  - Since the products and sum of integers are integers, $ad + bc$ and bd are both integers
  - Additionally, $bd \neq 0$ due to the zero product property
  - Thus, $\frac{ad+bc}{bd}$ and by extension $r + s$ is a rational number

Deriving New Mathematics from Old

- While fundamental definitions are common in proofs, new proofs can be derived from existing ones
- **Corollary 4.2.3:** The double of a rational number is rational
  - Suppose r is any *particular but arbitrarily chosen* rational number

- Then,

$$2r = r + r$$

- Thus, $2r$ is the sum of 2 rational numbers, so by Theorem 4.3.2, $2r$ is rational

▼ [4.4] Direct Proof and Counterexample IV: Divisibility

- The following is the definition if **divisibility**

$$\begin{gathered}\text{If } n \text{ and } d \text{ are integers then} \\ n \text{ is divisble by } d \iff n \text{ equals } d \\ \text{times some integer and } d \neq 0.\end{gathered}$$

- There are numerous ways to say “n is divisible by d”
  - n **is a multiple of** d
  - d **is a factor of** n
  - d **is a divisor of** n
  - d **divides** n
- The notation $d \mid n$ denotes “d divides n” or symbolically:

$$d \mid n \iff \exists \text{ an integer, say } k, \text{ such that } n = dk \text{ and } d \neq 0$$

- It should be noted that this is not an algebraic operator, but rather a logical one
- These definitions can be used to prove the divisibility of some numbers
  - 21 is divisible by 3

$$21 = 3 \cdot 7$$

  - $7 \mid 42$

$$42 = 7 \cdot 6$$

  - 32 is a multiple of -16

$$32 = (-16)(-2)$$

  - If k is any nonzero integer, k divides 0

$$0 = k \cdot 0$$

- $10km$ can be proven to be divisible by 5 using algebra

$$\begin{aligned} &10km = 5 \cdot (2km) && (1) \\ &2km \text{ is the product of the 3 integers, thus it is an integer.} && (2) \end{aligned}$$

- There are also 2 useful properties of divisibility for proofs
  - **Theorems 4.4.1** and **4.4.2**

$$\text{For all integers } a \text{ and } b\text{, if } a \text{ and } b \text{ are positive and } a \text{ divides } b \text{ then } a \leq b. \quad (1)$$

$$\text{The only divisors of 1 are 1 and } -1. \quad (2)$$

- To disprove the divisibility between two integers, the negation, a universal statement, may be used

$$\forall \text{ integers } n \text{ and } d\text{, } d \nmid n \iff \tfrac{n}{d} \text{ is not an integer.}$$

- For example, $4 \nmid 15$

$$\frac{15}{4} = 3.75$$

- Additionally, a second definition of prime and composite numbers can be obtained using divisibility

$$n \text{ is prime } \iff n > 1 \text{ and } \forall \text{ positive integer } r\text{, } r \nmid n \text{ when } r \neq 1 \text{ and } r \neq n.$$

Proving Properties of Divisibility

- **Theorem 4.4.3:** For all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$
  - Suppose a, b, and c are any *particular but arbitrarily chosen* integers such that a divides b and b divides c
  - By definition of divisibility, $b = ar$ and $c = bs$ for some integers r and s

$$\begin{aligned} c &= bs \\ &= (ar)s && \text{(By substitution)} \\ &= a(rs) && \text{(By associative laws)} \end{aligned}$$

  - (rs) is an integer because it is the product of integers
  - Thus, by definition of divisibility, a divides c
- **Theorem 4.4.4:** Any integer $n > 1$ is divisible by a prime number

    - Suppose n is a *particular but arbitrarily chosen* integer such that it is greater than 1
    - If n is prime, then $n \mid n$ by definition of divisibility
    - If n is not prime, then $n = r_0 s_0$ where r_0 and s_0 are integers such that $1 < r_0 < n$ and $1 < s_0 < n$
    - If r_0 or s_0 is prime, the theorem is proven by definition of transitivity for divisibility
    - If not, r_0 may be factored as $r_1 s_1$ which can be continuously factored until $r_k s_k$ where r_k is prime and the theorem succeeds, as the well-ordering principle states that there must be a least element in a finite decreasing sequence (which one of the factors should be)
-

Counterexamples and Divisibility

- An example of a false statement for divisibility is as follows:

$$\text{For all integers } a \text{ and } b, \text{ if } a \mid b \text{ and } b \mid a \text{ then a=b}$$

- To start:
    - Suppose a and b are integers such that $a \mid b$ and $b \mid a$.
- Using the definition of divisibility, this statement implies:

$$b = ap = (bq)p = (qp)b \text{ where } p \text{ and } q \text{ are both integers}$$

- By simplifying, it can be asserted that $qp = 1$. Thus, q and p are divisors of 1
- Using one of the previous properties of divisibility, either q and p are both 1 or both -1
- After narrowing it down, a counterexample can be found with $q = p = -1$

$$a \mid b \text{ so } b = -a$$
$$\therefore a \neq b$$

The Unique Factorization of Integers Theorem

- **Theorem 4.4.5:** All integers that are prime or composite has a unique product of solely prime numbers

$$\underline{\textbf{Unique Factorization of Integers Theorem}}$$
$$\text{Given any integer } n > 1 \text{, there exists a prime number } k\text{,}$$
$$\text{distinct prime numbers } p_1, p_2, \ \ldots \ , p_k \text{, and}$$
$$\text{positive integers } e_1, e_2, \ \ldots \ , e_k \text{ such that}$$

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$$

$$\text{where any other expression for } n \text{ as a product of}$$
$$\text{prime numbers is identical except for order.}$$

- The given form $n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$ is known as the **standard factored form**
  - The best method of finding it is to split n into all its factors and continuously split those factors into their factors until they are all prime numbers
- The important takeaway from this concept is that if 1 were to be a distinct prime number, there would be infinite permutations of the form n as a product of prime numbers
- Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10$$

  - Does 17 divide m?
  - By the unique factorization of integers theorem, the left-hand side of the equation may be expressed as a product prime numbers
  - 17 is a prime factor on the right-hand side of the equation equal to the left-hand side of the equation
  - 17 is not a prime factor of the left-hand side terms, 8, 7, 6, 5, 4, 3, 2, and 1, thus it must be a prime factor of m
  - Thus, $17 \mid m$

▼ [4.5] Direct Proof and Counterexample V: Division into Cases and the Quotient-Remainder Theorem

- **Theorem 4.5.1:**

$$\underline{\textbf{Quotient Remainder Theorem}}$$
$$\text{Given any integer } n \text{ and positive integer } d \text{, there exist}$$
$$\text{unique integers } q \text{ and } r \text{ such that } n = dq + r \text{ and } 0 \leq r < d.$$

- Here are some examples of the **quotient remainder theorem**

- $n = 54$ and $d = 4$

$$54 = 4 \cdot 13 + 2 \qquad \therefore q = 13 \text{ and } r = 2$$

- $n = -54$ and $d = 4$

$$-54 = 4 \cdot (-14) + 2 \qquad \therefore q = -14 \text{ and } r = 2$$

- $n = 54$ and $d = 70$

$$54 = 70 \cdot 0 + 54 \qquad \therefore q = 0 \text{ and } r = 54$$

- According to the quotient remainder theorem with a divisor of 2, every integer is either even or odd

$$n = 2q + r$$

  - Given $0 \leq r < d$, r is either 0 or 1, fitting the form of an even or odd integer

div and mod

- Given an integer n and a positive integer d
  - $n \operatorname{div} d$ is the integer quotient obtained when n is divided by d
  - $n \bmod d$ is the integer remainder obtained when n is divided by d
- Symbolically:

$$n \operatorname{div} d = q$$

$$n \bmod d = r \iff n = dq + r$$

- When applying integer division, simply floor the quotient obtained from normal division
- When applying modulo, subtract the integer quotient multiplied by the divisor from n

$$m \bmod d = n - d(n \operatorname{div} d)$$

Representations of Integers

- An integer's **parity** is a property that indicates whether it is even or odd
- **Theorem 4.5.2:** According to the **parity property**, any integer is either even or odd
  - Suppose that two *particular but arbitrarily chosen* consecutive integers are given, known as m and $+1$

- *Here, there are two different cases—either m is odd and $m+1$ is even or m is even and $m+1$ is odd*
- **Case 1:** m is odd
    - By definition of odd, $m = 2k+1$ for some integer k
    - Thus,

$$\begin{aligned} m+1 &= (2k+1)+1 && \text{(By substitution)} \\ &= 2k+2 \\ &= 2(k+1) && \text{(By factoring out 2)} \end{aligned}$$

    - $(k+1)$ is an integer because it is the sum of integers
    - Therefore, $m+1$ is an even number by definition of even
- **Case 2:** m is even
    - By definition of odd, $m = 2j$ for some integer j
    - Thus,

$$m+1 = 2j+1 \qquad \text{(By substitution)}$$

    - Therefore, $m+1$ is an odd number by definition of odd
- As a result, regardless of whether m is even or odd, $m+1$ will have opposite parity

- Theorem 4.5.2 is an example of proving something by division into cases, as it analyzes two distinct parities which m may be to prove that the property holds in any case
- **Theorem 4.5.3:** The square of any odd integer has the form $8m+1$ for some integer m
    - Suppose n is a *particular but arbitrarily chosen* odd integer
    - By the quotient remainder theorem with a divisor 4,

$$\begin{gathered} n = 4q+1 \quad \text{or} \quad 4q+3 \\ \text{for some integer } q \end{gathered}$$

    - The other expressions derived from the quotient remainder theorem with a divisor of 4, can be simplified such that

$$\begin{aligned} n &= 4q \\ &= 2(2q) \end{aligned}$$

$$\begin{aligned} n &= 4q + 2 \\ &= 2(2q + 1) \end{aligned}$$

    - $(2q)$ and $(2q + 1)$ are integers because the set of all integers is closed under addition and multiplication

  - **Case 1:** $n = 4q + 1$

$$\begin{aligned} n^2 &= (4q + 1)^2 && \text{(By substitution)} \\ &= 16q^2 + 8q + 1 && \text{(By multiplication)} \\ &= 8(2q^2 + q) + 1 && \text{(By factoring out 8)} \end{aligned}$$

    - $(2q^2 + q)$ is an integer because the set of all integers is closed under multiplication and addition
    - Thus, for $n = 4q + 1$, n^2 may be expressed in the form of $8 \cdot (\text{integer}) + 1$

  - **Case 2:** $n = 4q + 3$

$$\begin{aligned} n^2 &= (4q + 3)^2 && \text{(By substitution)} \\ &= 16q^2 + 24q + 9 && \text{(By multiplication)} \\ &= 16q^2 + 24q + 8 + 1 \\ &= 8(2q^2 + 3q + 1) + 1 && \text{(By factoring out 8)} \end{aligned}$$

    - $(2q^2 + 3q + 1)$ is an integer because the set of all integers is closed under multiplication and addition
    - Thus, for $n = 4q + 3$, n^2 may be expressed in the form of $8 \cdot (\text{integer}) + 1$

  - In both cases, n^2 can be expressed in the form $8 \cdot (\text{integer}) + 1$, so the theorem is proven

Absolute Value and the Triangle Inequality

- The **absolute value of x** is defined as:

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

- There are a few lemmas concerning them

- *Lemmas 4.5.3, 4.5.4, and 4.5.5*

$$\text{For every real number } r, \ -|r| \leq r \leq |r|. \tag{1}$$

$$\text{For every real number } r, |-r| = r. \tag{2}$$

$$\text{For all real numbers } x \text{ and } y, |x+y| \leq |x| + |y|. \tag{3}$$

▼ [4.6] Direct Proof and Counterexample VI: Floor and Ceiling

- The **floor** of a number is the integer to its immediate left

$$\text{If } x \text{ is a real number and } n \text{ is an integer,}$$
$$\text{then } \underline{\text{the floor of } x} \text{ is}$$

$$\lfloor x \rfloor = n \iff n \leq x < n+1$$

- The **roof** or **ceiling** of a number is the integer to its immediate right

$$\text{If } x \text{ is a real number and } n \text{ is an integer,}$$
$$\text{then } \underline{\text{the ceiling of } x} \text{ is}$$

$$\lceil x \rceil = n \iff n-1 < x \leq n$$

- Given this definition, the roofs and floors of numbers can be found
  - The floor and roof of $\frac{25}{4}$

$$\frac{25}{4} = 6.25 \qquad\qquad 6 < 6.25 < 7$$

$$\left\lfloor \frac{25}{4} \right\rfloor = 6 \qquad\qquad \left\lceil \frac{25}{4} \right\rceil = 7$$

  - The floor and roof of -2.01

$$-3 < -2.01 < -2$$

$$\lfloor -2.01 \rfloor = -3 \qquad\qquad \lceil -2.01 \rceil = -2$$

- For all real numbers x and y, $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ is a false statement. To arrive at a counterexample, the following methodology may be followed

- Suppose x and y are real numbers
- When imagining the quantities that they represent, it can be said:

$$\begin{aligned} x &= \lfloor x \rfloor + \text{fractional part of } x \\ y &= \lfloor y \rfloor + \text{fractional part of } y \\ \therefore x + y &= \lfloor x + y \rfloor + \text{fractional part of } (x+y) \end{aligned}$$

- Given this, it can seen that as long as the fractional part of $x + y$ is at least 1, then a counterexample may be found
- Thus, $x = \frac{1}{2}$ and $y = \frac{1}{2}$ are an obvious counterexample for fitting this line of reasoning

- **Theorem 4.6.2:** For any integer n

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

- Suppose n is a *particular but arbitrarily chosen* integer
- By the quotient remainder theorem, n is either even or odd
- **Case 1:** n is even
  - By definition of even, $n = 2k$ for some integer k

$$\begin{aligned} \left\lfloor \frac{n}{2} \right\rfloor &= \left\lfloor \frac{2k}{2} \right\rfloor && \text{(By definition of even)} \\ &= \lfloor k \rfloor \\ &= k \\ &= \frac{2k}{2} && \text{(i)} \\ &= \frac{n}{2} && (n \text{ is even}) \end{aligned}$$

    - (i) → Multiply by fraction equivalent to 1
  - This proves that if n is even, the floor of $\frac{n}{2}$ is $\frac{n}{2}$
- **Case 2:** n is odd
  - By definition of odd, $n = 2k + 1$ for some integer k

$$\begin{aligned}\left\lfloor \frac{n}{2} \right\rfloor &= \left\lfloor \frac{2k+1}{2} \right\rfloor && \text{(By definition of odd)} \\ &= \left\lfloor k + \frac{1}{2} \right\rfloor \\ &= k \\ &= \frac{2k}{2} && \text{(i)} \\ &= \frac{2k+1-1}{2} && \text{(ii)} \\ &= \frac{n-1}{2} && (n \text{ is odd})\end{aligned}$$

            - (i) → Multiply by fraction equivalent to 1
            - (ii) → Add a net total of 0 by adding 1 and subtracting 1
        - This proves that if n is odd, the floor of $\frac{n}{2}$ is $\frac{n-1}{2}$
    - Both cases covering whether n is even or odd are proven true, thus the theorem is true
- **Theorem 4.6.3:** If n is any integer and d is a positive integer, and if $q = \lfloor n \div d \rfloor$ and $r = n - d \cdot \lfloor n \div d \rfloor$, then

$$n = dq + r \quad \text{and} \quad 0 \leq r < d$$

    - Suppose n is any integer, and d is any positive integer such that $q = \lfloor n \div d \rfloor$ and $r = n - d \cdot \lfloor n \div d \rfloor$

$$\begin{aligned} dq + r &= d \cdot \lfloor n \div d \rfloor + n - d \cdot \lfloor n \div d \rfloor && \text{(By substitution)} \\ &= n \end{aligned}$$

    - Thus, $dq + r = n$
    - By definition of math floor, $q \leq n \div d < q + 1$

$$\begin{aligned} q \leq n \div d < q + 1 &= dq \leq n < dq + d && \text{(i)} \\ &= dq \leq dq + r < dq + d && \text{(ii)} \\ &= 0 \leq r < d && \text{(iii)} \end{aligned}$$

        - (i) → By multiplying all sections of the inequality by d
        - (ii) → By substitution
        - (iii) → By subtracting dq from all sections of the inequality

    - The statement is proven to be true

▼ [4.7] Indirect Argument: Contradiction and Contraposition

- It can be shown that assuming the existence of elements in a domain that satisfy just the hypothesis leads logically to a contradiction
- On the other hand, imagining elements in the domain that lead to a false conclusion and proving that they also do not satisfy the hypothesis is the basis of a **proof by contraposition**

Argument by Contradiction

- **Proof by contradiction:**
    1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true
        a. "Suppose $P(x)$" → **Negate** → "Suppose not. Suppose $\neg P(x)$"
    2. Show that this supposition leads logically to a contradiction
    3. Conclude that the statement to be proved is true
- Ex: There is no greatest integer
    - Suppose not. Suppose there is a greatest integer N
    - As a result, $N \geq n$ for every integer n
    - Let $M = N + 1$
    - M is an integer because it is the sum of integers
    - $M > N$ because it is equal to N plus another integer
    - Thus, N is both the greatest integer and not the greatest integer, meaning that there is a contradiction in the supposition
    - Therefore, the original statement is proven to be true
- **Theorem 4.7.2:** There is no integer that is both even and odd
    - Suppose not. That is, suppose there is at least one integer n that is both even and odd
    - By definition of even, $n = 2a$ for some integer a, and by definition of odd, $n = 2b + 1$ for some integer b

$$\begin{aligned} 2a &= 2b + 1 && \text{(By substitution)} \\ 2a - 2b &= 1 && \text{(By subtraction)} \\ 2(a - b) &= 1 && \text{(By distributive property)} \\ a - b &= \frac{1}{2} && \text{(By division)} \end{aligned}$$

- $a - b$ is the difference between two integers, so it is an integer
- $a - b = \frac{1}{2}$ and $\frac{1}{2}$ is not an integer, so $a - b$ is also not an integer
- This is a contradiction in the supposition, thus the theorem is true

- **Theorem 4.7.3:** The sum of any rational and any irrational number is irrational
  - Suppose not. That is, suppose there is some rational number r and some irrational number s such that their sum $r + s$ is rational
  - By definition of a rational number, $r = \frac{a}{b}$ and $r + s = \frac{c}{d}$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$

$$\begin{aligned} r + s &= \frac{c}{d} \\ \frac{a}{b} + s &= \frac{c}{d} && \text{(By Substitution)} \\ s &= \frac{c}{d} - \frac{a}{b} && \text{(By subtraction)} \\ s &= \frac{bc}{bd} - \frac{ad}{bd} && \text{(Common denominator)} \\ s &= \frac{bc - ad}{bd} && \text{(Combining like denominators)} \end{aligned}$$

  - $bc - ad$ and bd are integers because products and differences of integers are integers
  - $bd \neq 0$ by the zero product property
  - Thus, s may be expressed as the quotient of two integers with a nonzero denominator, meaning that s is rational
  - This contradicts the supposition that s is rational, thus the theorem is true

Argument by Contraposition

- This is the second form of indirect argument
- Take the contrapositive of the statement, then prove the contrapositive by direct proof
- **Proof by contraposition:**
  1. Express the statement to be proved in the form

    a. *Not a required written aspect of the proof*

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

2. Rewrite the statement in the contrapositive form

$$\forall x \text{ in } D, \text{ if } Q(x) \text{ is false then } P(x) \text{ is true.}$$

3. Prove the contrapositive by direct proof
    a. Suppose x is a particular but arbitrarily chosen element of D such that $Q(x)$ is false
    b. Show that $P(x)$ is false

- Prove that “for every integer n, if n^2 is even then n is even.”
    - **Contrapositive: “**For every integer n, if n is odd then n^2 is odd.”
        - *“Not even” may be expressed as “odd” due to the quotient-remainder theorem*
    - By definition of odd, $n = 2k + 1$ for some integer k

$$\begin{aligned} n^2 &= (2k+1)^2 && \text{(By substitution)} \\ &= 4k^2 + 4k + 1 && \text{(By multiplication)} \\ &= 2(2k^2 + 2k) + 1 && \text{(By distributive property)} \end{aligned}$$

    - Since $2k^2 + 2k$ is the sum of products of integers, it is an integer
    - Thus, $2(2k^2 + 2k) + 1$ is in the form of definition of an odd $\left(2 \cdot (\text{integer}) + 1\right)$
    - n^2 is odd
    - The contrapositive was proven to be true, so the given statement is true

Relation between Proof by Contradiction and Proof by Contraposition

- Proof by contraposition can be recast in the language of proof by contradiction
- In proof by contrapositive:

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

- Is proven by a direct proof for the equivalent:

$$\forall x \in D, \text{ if } \neg Q(x) \text{ then } \neg P(x)$$

- To do this, there should be an arbitrary element x in D such that $\neg Q(x)$ and then follow by showing $\neg P(x)$

- Meanwhile, in proof by contradiction, there is a supposition:

$$\exists x \in D \text{ such that } P(x) \text{ and } \neg Q(x).$$

- And showing $\neg P(x)$ shows a contradiction to the supposition
- These processes are similar, and proof by contraposition has the distinct advantage of not requiring a negation and are far more straightforward in their goal
- However, proof by contraposition only works with universal conditional statements
- For instance, the previous proof "for every integer n, if n^2 is even then n is even" can also be proven by contradiction (just like all other proof by contraposition problems)
  - **Negation:** "There exists an integer n such that n^2 is even and n is odd"
  - By definition of odd, $n = 2k + 1$ for some integer k

$$\begin{aligned} n^2 &= (2k+1)^2 && \text{(By substitution)} \\ &= 4k^2 + 4k + 1 && \text{(By multiplication)} \\ &= 2(2k^2 + 2k) + 1 && \text{(By distributive property)} \end{aligned}$$

  - Since $2k^2 + 2k$ is the sum of products of integers, it is an integer
  - Thus, $2(2k^2 + 2k) + 1$ is in the form of definition of an odd $\big(2 \cdot (\text{integer}) + 1\big)$
  - n^2 is odd
  - However, n^2 is also stated to be even, showing a contradiction in the supposition
- This is very similar to the proof by contraposition for the same statement
- Thus, it can be more efficient to use proof by contraposition instead if the statement is universal and conditional

Proof as a Problem-Solving Tool

- Direct proof, disproof by counterexample, proof by contradiction, and proof by contraposition are all tools that can be used interchangeable to determine the truth of statements
- Thus, it is valid to switch tactics if one method is unable to yield a clear answer
- If you feel like you can show that there are elements in a domain that only satisfy the hypothesis, then proof by contradiction is the most logical path
- If you feel like you could imagine elements in a domain where the conclusion and hypothesis are false, then there is a basis for a proof by contraposition

▼ [4.8] Indirect Argument: Two Famous Theorems

The Irrationality of $\sqrt{2}$

- The length of the diagonal of a unit square is:

$$\sqrt{1^2 + 1^2} = \sqrt{2}$$

- In ancient Greece, mathematicians believed that given any line segments A and B, a particular unit of length could be found such that A was exactly m units long and B was exactly n units long for some integers m and n

$$\frac{\text{length } A}{\text{length } B} = \frac{m}{n}$$

- This means that the ratio between them is rational
- However, applying this to the unit square:

$$\frac{\text{length (diagonal)}}{\text{length (side)}} = \frac{\sqrt{2}}{1} = \sqrt{2}$$
$$\therefore \sqrt{2} \text{ is rational}$$

- Intuitively, it is easy to tell that this is not true. In particular, this can be proved by contradiction
- **Theorem 4.8.1:** $\sqrt{2}$ is irrational
    - Suppose not. That is, suppose that $\sqrt{2}$ is rational
    - By definition of a rational number, there are integers n and m with no common factors such that $\sqrt{2} = \frac{m}{n}$

$$\begin{aligned} \sqrt{2} &= \frac{m}{n} \\ 2 &= \frac{m^2}{n^2} && \text{(By squaring both sides)} \\ m^2 &= 2n^2 && \text{(Multiplying by } n\text{)} \end{aligned}$$

    - n^2 is even because it is the product of integers, so m^2 is also even because it is in the even form $2 \cdot \text{(integer)}$
    - Thus $m = 2k$ for some integer k according to the previously proved preposition that if the square of any integer is even then the integer is even

$$\begin{aligned}(2k)^2 &= 2n^2 && \text{(By substitution)}\\ 4k^2 &= 2n^2 \\ n^2 &= 2k^2 && \text{(By dividing by 2)}\end{aligned}$$

  - k^2 is an integer because it is the product of two integers, thus $2k^2$ represents the form of an even number $2 \cdot (\text{integer})$ meaning that n^2 is also even
  - Referring to that proved preposition yet again, n must be even
  - However, if both m and n are even, they have a common factor of 2, leading to a contradiction in the supposition
  - Thus, $\sqrt{2}$ is irrational

Are There Infinitely Many Prime Numbers?

- Euclid's proof for there being infinitely many prime numbers uses a particular fact:
  - If a prime number divides an integer, then it does not divide the next successive integer
- **Proposition 4.8.3:** For any prime number p, if $p \mid a$ then $p \nmid (a+1)$
  - Suppose not. That is, suppose that if there exists a prime number p such that $p \mid a$ and $p \mid (a+1)$
  - By definition of divisibility, there exist integers r and s such that $a = pr$ and $a + 1 = ps$

$$\begin{aligned}a + 1 - 1 &= a \\ ps - 1 &= pr && \text{(By substitution)}\\ ps - pr &= 1 && \text{(By subtraction)}\\ p(s - r) &= 1 && \text{(By distributive property)}\end{aligned}$$

  - $(s - r)$ is an integer because it is the difference between two integers
  - Thus, $p \mid 1$
  - A property of divisibility is that the only integer divisors of 1 are 1 and -1
  - However, p cannot equal 1 because it is prime and all prime numbers must be greater than 1
  - This a contradiction in the supposition, meaning that the proposition is true
- This proven preposition is used to prove the of **infinitude of primes** theorem which states "the set of prime numbers is infinite"
- **Theorem 4.8.4:** Infinitude of primes; the set of prime numbers is infinite
  - Suppose not. That is, suppose the set of prime numbers is finite

    - Therefore, some prime number p is the largest prime number

$$2, 3, 5, 7, 11, \ldots, p$$

    - Let N be the product of all prime numbers plus 1

$$N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$$

    - N must be greater than 1 and thus must be divisible by some prime number q according to theorem 4.4.4
    - If q is prime, then q must equal a prime number in the set $\{2, 3, 5, 7, 11, \ldots, p\}$
    - By proposition 4.8.3, q can't divide into $(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$
    - Thus, N is both divisible and not divisible by q, showing a contradiction in the supposition, proving the theorem true

When to Use Indirect Proof

- In general, indirect proofs are messier than direct proofs
- Thus, it is best to use them when unable to prove a statement by direct proof and by counterexample

▼ [4.10] Application: Algorithms

- Algorithms refer to a step-by-step method for performing actions

An Algorithmic Language

- Pseudocode used in this course is an instance of algorithmic language, with it being a synthesis of elements of Python, C, C++, Java, etc along with English
- Generally, it is implemented with computer language constructs like assignment or loops but with less technical details like delimiters or integer ranges
- In high-level computer languages, **variables** refer to specific store locations in a computer's memory
    - Given storage locations may only hold one value
- **Data types** denote the set from which a variable takes its values
- **Assignment statements** point a variable to a value and are denoted by:

$$x \coloneqq e$$

    - This helps avoid confusion, meant to be read as "let x be e" rather than "x equals e"

- **Conditional statements** use current values of variables to determine which algorithm statement will be executed next, overriding the general order of the program

```
if (condition)
    then s1
    else s2

if (condition) then s1
```

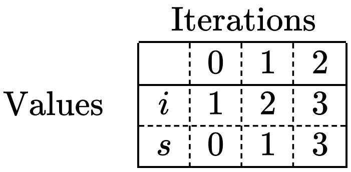
- The word **do** will be used as delimiters for grouped statements in a block

```
if x > 2
    then y := x + 1
    else do x := x - 1
        y := 3 * x end do
```

- **While** loops constantly evaluate a condition **(guard clause)** based on current values of all variables before executing all statements in its body breaking when the condition finally evaluates to false
    - The word **while** will also be used as the ending delimiter for the body

```
i := 1, s := 0
while (i <= 2)
    s := s + i
    i := i + 1
end while
```

- **Trace tables** show the current values of algorithm variables at various points during execution, making them useful for determining the output of loops



Iterations

		0	1	2
Values	i	1	2	3
	s	0	1	3

- **For-next** loops instantiate their own loop variable and check if they are less then or equal to the final expressions value before executing all the statements in its body and incrementing the loop variable

```
for i := 1 to 4
    x := i * i
next i
```

- These can be converted to while loops, as seen below

```
i := 1
while (i <= 4)
    x := i * i
    i := i + 1
end while
```

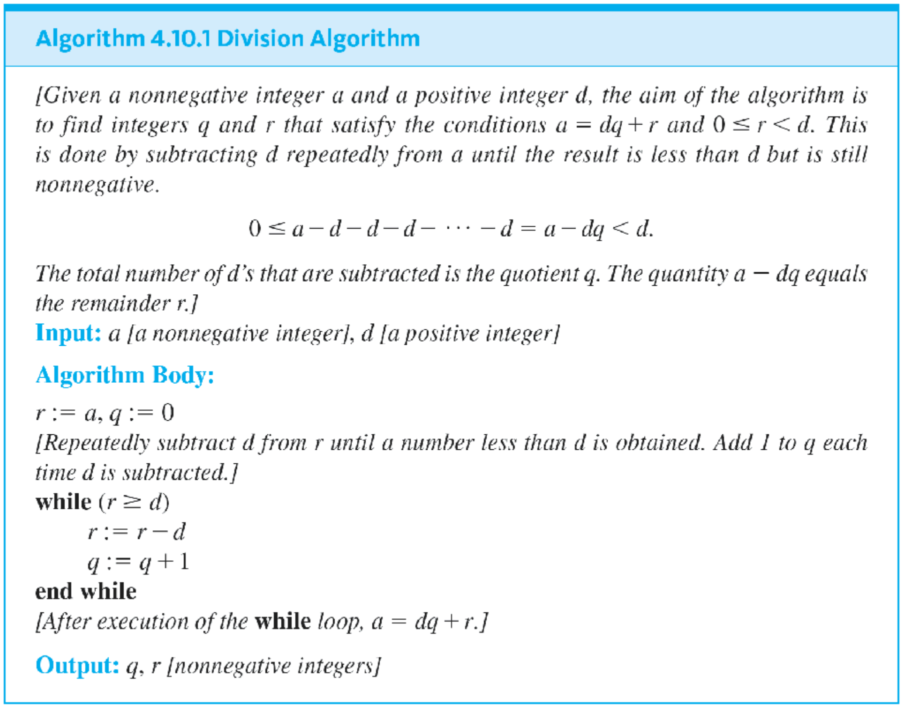
A Notation for Algorithms

- Algorithms will be expressed as **subroutines/methods/functions** that can be called upon by other algorithms when needed to transform inputs to outputs
- Output variables and their values will be assumed to be returned to the calling algorithm
- In formal descriptions of algorithm, it should include the name of the algorithm, a set of the input and output variables, and how it works

The Division Algorithm

- As denoted by the quotient-remainder theorem, there exists integers q and r such that

$$a = dq + r \text{ and } 0 \leq r < d$$



Algorithm 4.10.1 Division Algorithm

[Given a nonnegative integer a and a positive integer d, the aim of the algorithm is to find integers q and r that satisfy the conditions $a = dq + r$ and $0 \leq r < d$. This is done by subtracting d repeatedly from a until the result is less than d but is still nonnegative.

$$0 \leq a - d - d - d - \cdots - d = a - dq < d.$$

The total number of d's that are subtracted is the quotient q. The quantity $a - dq$ equals the remainder r.]

Input: a *[a nonnegative integer]*, d *[a positive integer]*

Algorithm Body:

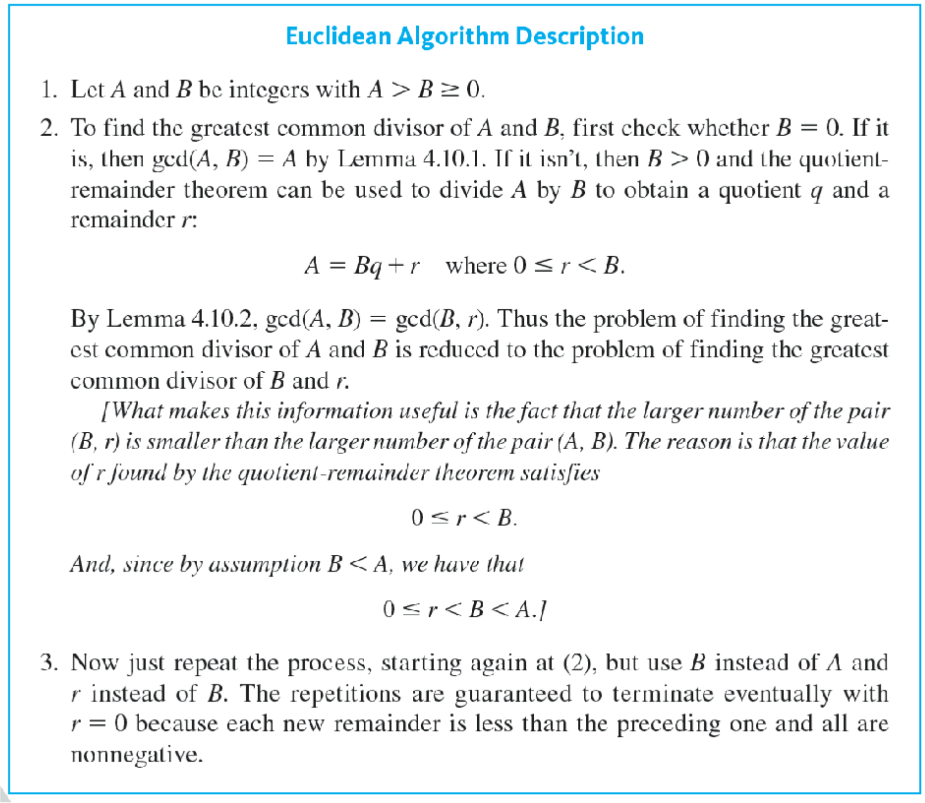
```
$r := a, q := 0$
[Repeatedly subtract $d$ from $r$ until a number less than $d$ is obtained. Add 1 to $q$ each time $d$ is subtracted.]
while ($r \geq d$)
    $r := r - d$
    $q := q + 1$
end while
[After execution of the while loop, $a = dq + r$.]
```

Output: q, r *[nonnegative integers]*

```
[The input is nonnegative integer a and positive integer d]
r := a, q := 0
[Repeatedly subtract d from r until a difference less than d is obtained.
Increment q each time d is subtracted]
while (r >= d)
    r := r - d
    q := q + 1
end while
[After execution, a = dq + r]
[Output is nonnegative integers q and r]
```

The Euclidean Algorithm

- The **Euclidean algorithm** is a very efficient way of computing the greatest common divisor of two integers



Euclidean Algorithm Description

1. Let A and B be integers with $A > B \geq 0$.
2. To find the greatest common divisor of A and B, first check whether $B = 0$. If it is, then $\gcd(A, B) = A$ by Lemma 4.10.1. If it isn't, then $B > 0$ and the quotient-remainder theorem can be used to divide A by B to obtain a quotient q and a remainder r:

$$A = Bq + r \quad \text{where } 0 \leq r < B.$$

By Lemma 4.10.2, $\gcd(A, B) = \gcd(B, r)$. Thus the problem of finding the greatest common divisor of A and B is reduced to the problem of finding the greatest common divisor of B and r.

[What makes this information useful is the fact that the larger number of the pair (B, r) is smaller than the larger number of the pair (A, B). The reason is that the value of r found by the quotient-remainder theorem satisfies

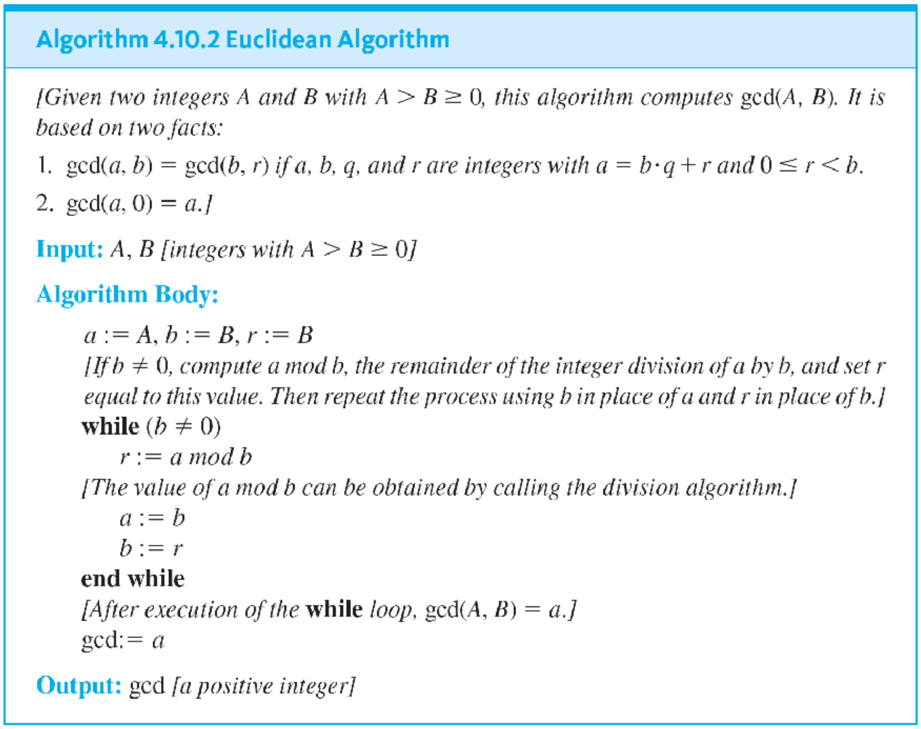
$$0 \leq r < B.$$

And, since by assumption $B < A$, we have that

$$0 \leq r < B < A.]$$

3. Now just repeat the process, starting again at (2), but use B instead of A and r instead of B. The repetitions are guaranteed to terminate eventually with $r = 0$ because each new remainder is less than the preceding one and all are nonnegative.

- This can also be expressed more formally



Algorithm 4.10.2 Euclidean Algorithm

[Given two integers A and B with $A > B \geq 0$, this algorithm computes $\gcd(A, B)$*. It is based on two facts:*

1. $\gcd(a, b) = \gcd(b, r)$ *if a, b, q, and r are integers with* $a = b \cdot q + r$ *and* $0 \leq r < b$.
2. $\gcd(a, 0) = a$.*]*

Input: A, B *[integers with* $A > B \geq 0$*]*

Algorithm Body:

```
$a := A, b := B, r := B$
[If $b \neq 0$, compute a mod b, the remainder of the integer division of a by b, and set r
equal to this value. Then repeat the process using b in place of a and r in place of b.]
while ($b \neq 0$)
    $r := a \bmod b$
[The value of a mod b can be obtained by calling the division algorithm.]
    $a := b$
    $b := r$
end while
[After execution of the while loop, $\gcd(A, B) = a$.]
gcd$:= a$
```

Output: gcd *[a positive integer]*

[5] Sequences, Mathematical Induction, Recursion

[5.1] Sequences

- A **sequence** is a function whose domain is either all the integers between two given integers or all the integers greater than or equal to a given integer
- Sequences are generally denoted as a set of elements written in a row

$$a_m, a_{m+1}, a_{m+2}, \ldots, a_n$$

  - Where each **term** is a_k (a sub k)
  - The **subscript** or **index** shows the corresponding term's place in the sequence
  - a_n is the **final term**
- **Infinite sequences** are concluded by dots to indicate there is no final value

$$a_m, a_{m+1}, a_{m+2}, \ldots$$

- **Explicit formulas** or **general formulas** show the dependency of a_k on k

$$a_k = \frac{k}{k+1} \text{ for every integer } k \geq 1$$
$$a_1 = \frac{1}{2}, a_2 = \frac{2}{3}, a_3 = \frac{3}{4}$$

- In mathematics, **sigma notation** is used to denote summation of terms
  - k denotes the index of each term
  - n denotes the upper bound of k
  - m denotes the starting value of k

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n$$

- Summation is expressed using **explicit formulas** in place of a_k

$$\sum_{k=1}^{5} k^2$$

- Summations can be written in expanded form using ellipsis to denote a continuation of a particular pattern

$$\sum_{i=0}^{n} \frac{(-1)^i}{i+1} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{(-1)^i}{i+1}$$

- The top index n is a **free variable** because it may be any integer greater than or equal to the bottom index
- The top index also acts as a **constant** because it does not change from iteration to iteration
- In some summations, each term is the difference between two quantities, allowing them to collapse toward a particular value
  - These sums converge to a finite value according to the telescoping series test

$$\begin{aligned}\sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{k+1} \\ &= \left(1 - \cancel{\frac{1}{2}}\right) + \left(\cancel{\frac{1}{2}} - \cancel{\frac{1}{3}}\right) + \cdots + \left(\cancel{\frac{1}{n-1}} - \cancel{\frac{1}{n}}\right) + \left(\cancel{\frac{1}{n-1}} - \frac{1}{n+1}\right) \\ &= \boxed{1 - \frac{1}{n-1}}\end{aligned}$$

Product Notation

- The notation for a product of a sequence of numbers is analogous to the summation of a sequence and is denoted by uppercase pi

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdots a_n$$

  - Similarly, this is the product from $k = m$ to n of "a sub k"

- Recursively, product notation is defined as

$$\prod_{k=m}^{m} a_k = a_m \qquad \text{and} \qquad \prod_{k=m}^{n} a_n = \left(\prod_{k=m}^{n-1} a_k \cdot a_n \right)$$

$$\text{for every integer } n > m$$

Properties of Summations and Productions

- There are a few properties concerning them

$$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$$

$$c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} (c \cdot a_k) \qquad \text{(Distributive property)}$$

$$\left(\prod_{k=m}^{n} a_k \right) \cdot \left(\prod_{k=m}^{n} b_k \right) = \left(\prod_{k=m}^{n} (a_k \cdot b_k) \right)$$

Change of Variable

- The symbol used to represent an index of summation is a local variable or **dummy variable** and can be replaced by other symbols as long as all instances are swapped out with the replacement

$$\sum_{k=m}^{n} k^3 = \sum_{j=m}^{n} j^3$$

- Changes of variables can also be accompanied by more complicated changes if the symbol means something completely different as long as the changes are consistent

$$\sum_{j=2}^{4}(j-1)^2 = \sum_{k=1}^{3}k^2$$

Factorial and “n Choose r” Notation

- Factorial is the product of consecutive integers up to a given integers denoted by factorial notation

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$$

- **Zero factorial** is a special case

$$0! = 1$$

- There is a recursive definition for factorial as well

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n \cdot (n-1)! & \text{if } n \geq 1 \end{cases}$$

  - This can be especially helpful for simplifying factorial expressions

$$\frac{8!}{7!} = \frac{8 \cdot 7!}{7!} = 8$$

- Another crucial use of factorial notation is calculating values of quantities known as n **choose** r and is denoted as follows
  - Let n and r be integers with $0 \leq r \leq n$

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

- n *choose* r represents the number of subsets of size r that can be chosen from a set with n elements
  - These quantities are known as **combinations** or **binomial coefficients**
- n *choose* r is always an integer, so the factors in the numerator and denominator always cancel out
- It may also be denoted in other ways, such as:

$$nCr$$
$$C(n,r)$$
$${}^{n}C_r$$
$$C_{n,r}$$

Sequences in Computer Programming

- In a programming context, finite sequences are known as **one-dimensional arrays**
- For instance, if you needed to storage a sequence of 50 related values, you would just use a single array to store all of them

$$\mathrm{W}[1], \mathrm{W}[2], \ldots, \mathrm{W}[50]$$

- The index variable of a **for-next** loop is a **local/dummy variable**

```
[All of these will have the same value]

for i := 1 to n
    print a[i]
next i

for j := 0 to n - 1
    print a[j + 1]
next j

for k := 2 to n + 1
    print a[k - 1]
next k
```

- Additionally, recursive sequence definitions lead naturally to computational algorithms

$$\sum_{k=1}^{n} a[k] = a[1], a[2], \ldots a[n]$$

```
[Normal definition]
s := 0
for k := 1
    s := s + a[k]
next k

[Recursive definition]
s := a[1]
for k := 2 to n
    s := s + a[k]
next k
```

Application: Algorithm to Convert from Base 10 to Base 2 Using Repeated Division by 2

- Suppose a is a nonnegative integer
- Divide a by 2 using the quotient remainder theorem, obtaining quotient $q[0]$ and remainder $r[0]$
- If the quotient is nonzero, divide $q[0]$ by 2 to obtain quotient $q[1]$ and $r[1]$
- Repeat the divisions until a zero quotient is obtained

$$\text{For } a = 38\text{:}$$

$$\begin{aligned} a &= 2 \cdot q[0] + r[0] \\ 38 &= 2 \cdot 19 + 0 \\ 19 &= 2 \cdot 9 + 1 \\ 9 &= 2 \cdot 4 + 1 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

- This sequence of equations may be substituted into the original quotient remainder theorem equation

$$\begin{aligned} 38 &= 2 \cdot 19 + 0 \\ &= 2 \cdot (2 \cdot 9 + 1) + 0 = 2^2 \cdot 9 + 2 \cdot 1 + 0 \\ &= 2^2 \cdot (2 \cdot 4 + 1) + 2 \cdot 1 = 2^3 \cdot 4 + 2^2 \cdot 1 + 2 \cdot 1 + 0 \\ &= 2^3 \cdot (2 \cdot 2 + 0) + 2^2 \cdot 1 + 2 \cdot 1 + 0 = 2^4 \cdot 2 + 2^2 \cdot 1 + 2 \cdot 1 + 0 \\ &= 2^4 \cdot (2 \cdot 1 + 0) + 2^2 \cdot 1 + 2 \cdot 1 + 0 = 2^5 \cdot 1 + 2^2 \cdot 1 + 2 \cdot 1 + 0 \\ &= 2^5 \cdot (2 \cdot 0 + 1) + 2^2 \cdot 1 + 2 \cdot 1 + 0 \\ &= 2^5 \cdot 1 + 2^2 \cdot 1 + 2 \cdot 1 \end{aligned}$$

$$\therefore 38_{10} = 0010\ 0110_{10}$$

- This works because it forms a sequence of terms which are powers of 2 with coefficients of only 1 or 0

```
while (i = 0 or q != 0)
    r[i] := q mod 2
    q := q div 2
    [r[i] and q can be obtained by calling the division algorithm]
    i := i + 1
end while
```

▼ [5.2] Mathematical induction I: Proving Formulas

- **Deduction** is inferring a conclusion from general principles using logical reasoning
- **Induction** is enunciating a **general principle** after observing it to hold in a large number of specific instances
- According to the **principles of mathematical induction**
  - Let $P(x)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:
    1. $P(a)$ is true
    2. For every integer $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true
  - Then the statement

$$\forall \text{ integer } n \geq a, P(a)$$

  - is true
- Thus, in a sequence the general case would be used to prove a related statement by mathematical induction
- **Proof by mathematical induction:**
  - **Basis step (1):** Show that $P(a)$ is true
  - **Inductive step (2):** Show that for every integer $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true. To do this:
    - **Inductive hypothesis:** Suppose that $P(k)$ is true, where k is any particular yet arbitrarily chosen integer with $k \geq a$
    - Then, show that $P(k+1)$ is true
- Sum of the first n integers:
  - Let $P(n)$ be the equation

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \qquad \text{for every integer } n \geq 1.$$

  - **Basis step:** *Show that* $P(1)$ *is true*

$$\begin{aligned}\frac{1(1+1)}{2} &= 1 \\ \frac{2}{2} &= 1 \\ 1 &= 1\end{aligned}$$

  - Thus, $P(1)$ is true
- **Inductive step:** *Show that for every integer* $k \geq 1$*, if* $P(k)$ *is true then* $P(k+1)$ *is also true*
  - Suppose k is any integer for $k \geq 1$ such that

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

  - We must show that

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

  - The left side of $P(k+1)$:

$$\begin{aligned}1 + 2 + \cdots + (k+1) &= 1 + 2 + \cdots + k + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) && \text{(By substitution)} \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} && \text{(By distributive property)}\end{aligned}$$

  - The right side of $P(k+1)$:

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

  - Since both sides of $P(k+1)$ are equal to the same quantity, they are equal to each other
  - Thus, $P(k+1)$ is true
- Since both the basis step and inductive step are proven to be true, the theorem is true
- The formula proven by this theorem is a sum written in **closed form** since it does not use an ellipsis or a summation symbol

Proving an Equality

- There are two ways of showing that an equation is true according to the inductive process
  1. Transforming the left and right side of the equation until they are visibly equal
  2. Transforming one side of the equation until it is the same as the other side
- However, it is also possible for to prove an equality in an invalid manner

$$\begin{aligned}\sum_{i=0}^{0} r^i &= \frac{r^{0+1}-1}{r-1} \\ r^0 &= \frac{r^1-1}{r-1} \\ 1 &= \frac{r-1}{r-1} \\ 1 &= 1\end{aligned}$$

  - Assuming that a form of an equality is true to prove it true is not a valid argument

Deducing Additional Formulas

- The sum of a geometric sequence formula can be thought of as a family of different formulas, one for each real number r except 1

$$\sum_{m=1}^{n} r^{n-1} = \frac{r^{n+1}-1}{r-1}$$

- The formula for the sum of the first n terms in a geometric sequence can be thought of in a simpler way, similar to proving the rationality of repeating decimals
- Given

$$S_n = 1 + r + r^2 + \cdots + r^n$$

- Then,

$$rS_n = r + r^2 + r^3 + \cdots + r^{n+1}$$

- Thus,

$$\begin{aligned}rS_n - S_n &= r + r^2 + r^3 + \cdots + r^{n+1} - (1 + r + r^2 + \cdots + r^n) \\ &= r^{n+1} - 1\end{aligned}$$

- Additionally,

$$rS_n - S_n = S_n(r-1)$$

- Both sides can now be set equal to each other

$$S_n(r-1) = r^{n+1} - 1$$
$$S_n = \frac{r^{n+1}-1}{r-1}$$

- While the derivation does work, it is not as airtight as mathematical induction because the terms denoted by … are unknown and uncheckable

[5.3] Mathematical Induction II: Applications

- If the United States abolished the penny and replaced it with a 3¢ coin, some prices may not be possible to obtain

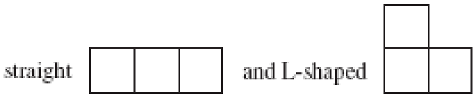
Number of cents	How to obtain
3¢	3¢
5¢	5¢
6¢	$3¢ + 3¢$
8¢	$5¢ + 3¢$
9¢	$3¢ + 3¢ + 3¢$
10¢	$5¢ + 5¢$
11¢	$5¢ + 3¢ + 3¢$
$\dots$	$\dots$

- Given this table, could it be possible to represent each successive price with those 2 coins?
- There are two cases: either k¢ contains a 5¢ coin or it doesn't
  - If it does, then $(k+1)$¢ can be represented by replaced the 5¢ coin with two 3¢ coins
  - Otherwise, $(k+1)$¢ can be represented by replacing three 3¢ coins with two 5¢ coins (given $k \geq 9$)
- Using those two cases, it can be proven that any price greater than or equal to 8¢ can be obtained using only 3¢ and 5¢ coins
- For every integer $n \geq 8$, n¢ can be obtained using 3¢ and 5¢ coins
  - Let $P(n)$ be the sentence "n¢ can be obtained using 3¢ and 5¢ coins"
  - **Basis step:** *Show $P(8)$ is true*

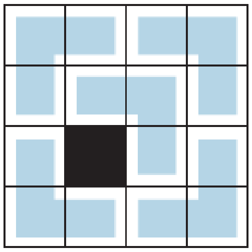
        - $P(8)$ is true because 8¢ can be obtained using one 3¢ coin and one 5¢ coin
    - **Inductive step:**
        - k¢ can be obtained using 3¢ and 5¢ coins
        - **Case 1:** *At least one 5¢ coin is used, thus* $(k+1)$¢ *can be obtained by replacing a 5¢ coin with two 3¢ coins*
        - **Case 2:** *No 5¢ coins are used, thus there are at least three 3¢ coins used and* $(k+1)$¢ *can be obtained by replacing them with two 5¢ coins*
    - In either case, $(k+1)$¢ can be obtained using 3¢ and 5¢ coins
    - Because the basis step and the inductive step have been proven true, the preposition is true

A Problem with Trominoes

- A **polyomino** is a block made up of numerous squares
- A **tromino** is a polyomino made up of three squares
    - Thus, there are two types, a **straight tromino** and an **L-shaped tromino**

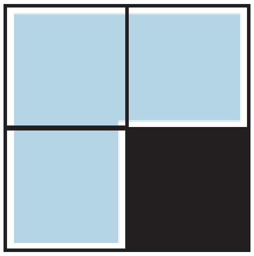


- In a 4×4 checkerboard, if one square is removed, then the remaining squares can all be filled by L-shaped trominoes

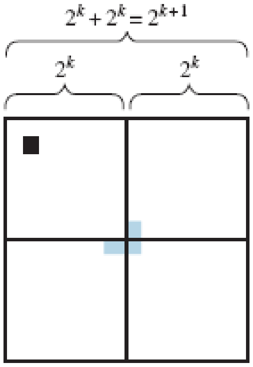


- For any integer $n \geq 1$, if one square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be completely covered by L-shaped trominoes
    - *The methodology by the proof is that for* k *and* $k+1$, *a quadrant of a* $2^{k+1} \times 2^{k+1}$ *board is a* $2^k \times 2^k$ *board*
    - Let $P(n)$ be the sentence: “If any square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be completely covered by L-shaped trominoes”
    - **Basis step:** *Show* $P(1)$ *is true*

    - A $2^1 \times 2^1$ checkerboard has four squares. If one square is removed, only an L-shape remains, which may be covered by one L-shaped tromino



- **Inductive step:** Show that for every integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is also true:
    - Let k be any integer such that $k \geq 1$, and suppose $P(k)$
    - We must show $P(k+1)$
        - A $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed can be split into 4 quadrants
        - Thus, each quadrant would be a $2^k \times 2^k$ checkerboard with one of the quadrants having a missing square
        - By inductive hypothesis, all the remaining squares in the quadrant with the missing square may be filled with L-shaped trominoes
        - The three remaining quadrants meet at the center of the $2^{k+1} \times 2^{k+1}$ checkerboard, meaning that the center is a corner piece for each of them
        - One L-shaped tromino can be placed across the three remaining quadrants such that it covers the corner piece for all three of them



        - By inductive hypothesis, all the remaining squares in the three quadrants may be filled with L-shaped trominoes
        - Thus, every square in the $2^{k+1} \times 2^{k+1}$ checkerboard sans the removed one may all be covered by L-shaped trominoes

    - The basis step and the inductive step have been proven true, thus the theorem is proven true

▼ [5.4] Strong Mathematical Induction and the Well-Ordering Principle for the Integers

- **Strong mathematical induction** is an "enhanced" version of ordinary mathematical induction
    - The basis step contains proofs for multiple initial values
    - The inductive step assumes the value of n in predicate $P(n)$ for all values through k rather than just one value
- Let $P(n)$ be a property that is defined for integers , and let a and b be fixed integers $a \leq b$. Suppose the following statements are true:
    1. **(Basis step)** $P(a)$, $P(a+1)$, $\ldots$, and $P(b)$ are all true
    2. **(Inductive step)** For every integer $k \geq b$, if $P(i)$ is true for each integer i from a through k then $P(k+1)$ is true
    - Then, the statement "for every integer $n \geq a$", $P(n)$ is true
    - Step 2 is also known as the inductive hypothesis

Applying Strong Mathematical Induction

- Ex: Any integer greater than 1 is divisible by a prime number
    - *Let $P(n)$ be the sentence: n is divisible by a prime number*
    - **(Basis step)** *Show $P(2)$*
        - 2 is divisible by 2, a prime number, so $P(2)$ is true
    - **(Inductive step)**
        - Let k be an integer for $k \geq 2$
        - Suppose that i is divisible by a prime number for each integer i from 2 through k
        - *Show that if $P(i)$ is true through $P(k)$, then $P(k+1)$ is true*
        - **Case 1:** $(k+1)$ is prime
            - By definition of prime, $(k+1)$ is divisible by a prime, *namely itself*
        - **Case 2:** $(k+1)$ is not prime
            - Thus, $k+1 = ab$ where a and b are integers for $1 < a < k+1$ and $1 < b < k+1$
            - In particular, $2 \leq a \leq k$

            - By inductive hypothesis, $k+1$ is divisible by a prime number
        - Regardless of whether $k+1$ is prime or not, it is divisible by a prime number
- A sequence $s_0, s_1, s_2, \ldots$ is defined as follows

$$\begin{aligned} s_0 &= 0 \\ s_1 &= 4 \\ s_k &= 6s_{k-1} - 5s_{k-1} \quad \text{for every integer } k \geq 2 \end{aligned}$$

    - Find the first four terms

$$s_0 = 0$$

$$s_1 = 4$$

$$\begin{aligned} s_2 &= 6s_1 - 5s_0 \\ &= 6(4) - 5(0) \\ &= 24 \end{aligned}$$

$$\begin{aligned} s_3 &= 6s_2 - 5s_1 \\ &= 6(24) - 5(4) \\ &= 144 - 20 \\ &= 124 \end{aligned}$$

$$0, 4, 24, 124, \ldots$$

    - Using mathematical induction, prove that for each integer $n \geq 0$

$$s_n = 5^n - 1$$

        - Let $P(n)$ be $s_n = 5^n - 1$
        - **(Basis step)**
            - *Show that $P(0)$ is true*

$$s_0 = 5^0 - 1$$

            - **Left**

$$s_0 = 0$$

- **Right**

$$\begin{aligned} 5^0 - 1 &= 1 - 1 \\ &= 0 \end{aligned}$$

- Both sides of the equation are equal to the same quantity, so they are equal, and $P(0)$ is true

- *Show that $P(1)$ is true*

$$s_1 = 5^1 - 1$$

- **Left**

$$s_1 = 4$$

- **Right**

$$\begin{aligned} 5^1 - 1 &= 5 - 1 \\ &= 4 \end{aligned}$$

- Both sides of the equation are equal to the same quantity, so they are equal, and $P(1)$ is true
- **(Inductive step)**
  - Suppose that $P(i)$ is true for each integer i from 0 through k where $k \geq 1$

$$s_i = 5^i - 1$$

  - *We must show $P(k+1)$ for $k \geq 1$*

$$s_{k+1} = 5^{k+1} - 1$$

  - *Simplifying one side to show they are equal to each other*

$$\begin{aligned} 5^k - 1 = s_{k+1} & \\ &= 6s_k - 5s_{k-1} && \text{(i)} \\ &= 6\left(5^k - 1\right) - 5\left(5^{k-1} - 1\right) && \text{(ii)} \\ &= 6\left(5^k - 1\right) - 5\left(5^k \cdot 5^{-1} - 1\right) && \text{(iii)} \\ &= 6\left(5^k - 1\right) - 5\left(5^k \cdot \frac{1}{5} - 1\right) \\ &= 6 \cdot 5^k - 6 - 5^k + 5 && \text{(iv)} \\ &= 5 \cdot 5^k - 1 \\ &= 5^{k+1} - 1 \end{aligned}$$

        - (i) → By substitution
        - (ii) → By inductive hypothesis
        - (iii) → By laws of exponents
        - (iv) → By distributive property
    - Both sides are equal to the same quantity, so they are equal, and $P(k+1)$ is true
  - Both the basis step and inductive hypothesis have been proven, so the statement is proven true
- As seen in the sequence example, strong mathematical induction is very useful for recursively defined sequences as it allows for numerous base cases and more than one value can be assumed

The Well-Ordering Principle for the Integers

- **Well-ordering principle for integers:** Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element
- This can be illustrated with numerous defined sets of integers

$$\mathbb{R}^+$$

  - There is no least positive number, but the principle is not violated because this is not a set of integers

$$\{\, n \in \mathbb{Z}^{\text{nonneg}} \mid n^2 < n \,\}$$

  - There is no least nonnegative integer n given this inequality because no nonnegative integer satisfies it.
  - The principle is not violated because it does not contain at least one element

$$\{\, n \in \mathbb{Z}^{\text{nonneg}} \mid \exists k \in \mathbb{Z}, n = 46 - 7k \,\}$$

- When noting the values of $46 - 7k$ for all values of k, it can be seen that all elements for $k \geq 7$ are negative and that $46 - 7k \geq 46$ for $k \leq 0$. Thus, there is a least nonnegative integer in the set at $k = 6$

- The well-ordering principle for integers also serves as the basis for the quotient-remainder theorem
- Additionally, the well-ordering principle guarantees that all strictly decreasing sequences of nonnegative integers are finite

$$\begin{gathered}\text{Given sequence of nonnegative integers} \\ r_1, r_2, r_3, \ldots \\ \text{satisfying } r_i > r_i + 1\text{, then the sequence is finite.}\end{gathered}$$

  - In computer science, this fact can prove that algorithms terminate after a finite number of steps

▼ [5.5] Application: Correctness of Algorithms

- A program is said to be **correct** if it produces a documentation-specified output for each documentation-specified input data set

Assertions

- The initial and final states of a program can be expressed as predicates based on an algorithm's inputs and outputs
- An algorithm's **pre-condition** is the predicate describing an initial state
- An algorithm's **post-condition** is the predicate describing a final state
- For instance, if an algorithm computes a product of nonnegative integers:
  - **Pre-condition:** The input variables m and n are nonnegative integers
  - **Post-condition:** The output variable p equals mn
- For an algorithm sorting a one-dimensional array of real numbers:
  - **Pre-condition:** The input variable $\mathrm{A}[1], \mathrm{A}[2], \ldots, \mathrm{A}[n]$ is a one-dimensional array of real numbers
  - **Post-condition:** The output variable $\mathrm{B}[1], \mathrm{B}[2], \ldots, \mathrm{B}[n]$ is a one-dimensional array of real numbers with the same elements as og but with the property $\mathrm{B}[i] \leq \mathrm{B}[j]$ whenever $i \leq j$

Loop Invariants

- The method of **loop invariants** proves loop correctness with respect to specific pre- and post-conditions based on mathematical induction
- Used when given an algorithm with a **while** loop and a restrictive condition G known as the **guard**

- The assertions before and after the loop are known as the **pre-condition** and **post-condition** respectively

```
[Pre-condition for the loop]
while (G)
    [Statements in the loop body
    None containing branch statements
    that lead outside the loop]
end while
[Post-condition for the loop]
```

- A **loop invariant** is a predicate with a domain as the set of integers satisfying the following condition:
    - For each iteration of the loop, if the predicate is true before the iteration, then it is true after
    - Additionally, if the loop invariant satisfies the two following conditions, the loop is correct with respect to its pre- and post-conditions
        1. The predicate is true before the loop’s first iteration
        2. If the loop terminates after a finite number of iterations, the loop invariant’s truth ensures the truth of the loop’s post-condition
- **Loop Invariant Theorem**
    - Let a while-loop with guard G be given with pre- and post-conditions that are predicates in the algorithm variables. Additionally, let $I(n)$ be the **loop invariant**. The following properties are true, if and only if, the loop is correct with respect to its pre- and post-conditions

    1. **Basis property:** The pre-condition for the loop implies that $I(0)$ is true before the loop’s first iteration
    2. **Inductive property:** For every integer $k \geq 0$, if the guard G and the loop invariant $I(k)$ are both true before an iteration, then $I(k+1)$ is true after an iteration
    3. **Eventual falsity of guard:** After a finite number of loop iterations, the guard G becomes false
    4. **Correctness of the post-condition:** If N is the least number of iterations after which G is false and $I(N)$ is true, then the algorithm variables’ values will be as specified in the post-condition
- For instance, here is a loop designed to calculate a product between a nonnegative integer m and a real number x without a built-in multiplication operator

```
[Pre-condition: m is a nonnegative integer,
x is a real number, i = 0, and product = 0]
while (i != m)
```

```
    1. product := product + x
    2. i := i + 1
end while
[Post-condition: product = mx]
```

  - **Loop invariant:** $I(n)$: $i = n$ and $\text{product} = nx$
  - **Guard clause:** G: $i \neq m$

Correctness of the Division Algorithm

```
[Pre-condition: a is a nonnegative integer
and d is a positive integer, r = a and q = 0]
while (r >= d)
    r := r - d
    q := q + 1
end while
[Post-condition: q and r are nonnegative integers
with the property that a = qd + r and 0 <= r < d]
```

- Let loop invariant be $I(n)$

$$I(n)\colon\ r = a - nd \geq 0 \quad \text{and} \quad n = q$$

- Let guard clause be G

$$G\colon\ r \geq d$$

- **Basis property**

$$I(0)\colon\ r = a \geq 0 \quad \text{and} \quad q = 0$$

  - This matches the precondition of $r = a$ for $a \geq 0$ and $q = 0$, thus $I(0)$ holds true

- **Inductive property**
  - *If $G \wedge I(k)$ before iteration, then $I(k+1)$ after iteration*
  - Suppose k is a nonnegative integer such that $G \wedge I(k)$
  - Given G

$$r_0 \geq d$$

  - Given $I(k)$

$$r_0 = a - kd \geq 0 \quad \text{and} \quad k = q_0$$

  - After the iteration

$$\begin{aligned} r_1 &= r_0 - d && \text{(Recursive def)} \\ &= (a - kd) - d && \text{(By substitution)} \\ &= a - (k+1)d && \text{(By factoring out } d\text{)} \\ \\ q_1 &= q_0 + 1 && \text{(Recursive def)} \\ &= k + 1 && \text{(By substitution)} \end{aligned}$$

  - Afterward, $I(k+1)$ can be evaluated in terms of $I(k)$

$$\begin{aligned} r_1 &= r_0 - d \geq d - d \\ &= r_0 - d \geq 0 \\ \\ q_1 &= q_0 + 1 \\ &= k + 1 \end{aligned}$$

  - Thus, $I(k+1)$ is now

$$r_1 \geq 0 \quad \text{and} \quad r_1 = a - (k+1)d \quad \text{and} \quad q_1 = k + 1$$

  - Therefore, $I(k+1)$ is true

- **Eventual falsity of the guard**
  - Given G: $r \geq d$ where r is decremented by 1 each iteration and r is nonnegative, r is a decreasing sequence of nonnegative integers
  - According to the well-ordering principle, there must be a minimum value, say r_{min} such that $r_{\text{min}} < d$
  - Thus, when $r = r_{\text{min}}$ guard G is false

- **Correctness of the post-condition**
  - *The post-condition can be thought of as a time where the loop invariant is true but the guard is false (the loop invariant's values matches the post-condition)*
  - Suppose that for some nonnegative integer N, G is false and $I(N)$ is true
  - Thus,

$$r < d \quad \text{and} \quad r = a - Nd \geq 0 \quad \text{and} \quad q = N$$

- - *To find a way for it to match the post-condition, the rightmost equality can be used to express* r *in terms of* q

$$\begin{aligned} r &= a - qd \geq 0 && \text{(By substitution)} \\ a &= r + qd \geq 0 && \text{(By adding } qd\text{)} \end{aligned}$$

- - Additionally, the inequality from this equation and the other given inequality form

$$0 \leq r < d$$

- - These are the values of q and r as specified in the post-condition
  - Profc oerkmtefpofekte t

Correctness of the Euclidean Theorem

▼ [5.6] Defining Sequences Recursively

- Sequences have many ways to be defined
- Sequences may be defined by writing the first few terms with an obvious general pattern implying the next few terms, although this may be ambiguous at times

$$3, 5, 7, \ldots$$

- Sequences maybe defined with their explicit formula

$$a_n = \frac{(-1)^n}{n+1} \qquad \text{for every integer } n \geq 0$$

- Sequences may also be defined **recursively**, requiring an equation known as a **recurrence relation** that defines later terms by referencing earlier terms
  - This can be practical if an explicit formula is difficult to determine
- The **recurrence relation** for a sequence $a_0, a_1, a_2, \ldots$ is a formula that relates each term a_k to its predecessors $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$ where i is an integer such that $k - i \geq 0$

- If i is a fixed integer, the relation's **initial conditions** specify the values of $a_0, a_1, a_2, \ldots, a_{i-1}$
- If i depends on k, they specify the values $a_0, a_1, \ldots, a_m$ where m is an integer such that $m \geq 0$

$$c_0, c_1, c_2, \ldots \qquad \text{for every integer } k \geq 2,$$

$$\begin{aligned} c_k &= c_{k-1} + kc_{k-2} + 1 \qquad &\text{(Recurrence relation)} \\ c_0 = 1 \quad \text{and} \quad c_1 &= 2 \qquad &\text{(Initial conditions)} \end{aligned}$$

$$\begin{aligned} c_2 &= c_1 + 2c_0 + 1 \\ &= 2 + 2 \cdot 1 + 1 \\ &= 5 \end{aligned}$$

$$\begin{aligned} c_3 &= c_2 + 3c_1 + 1 \\ &= 5 + 3 \cdot 2 + 1 \\ &= 12 \end{aligned}$$

$$\begin{aligned} c_4 &= c_3 + 4c_2 + 1 \\ &= 12 + 4 \cdot 5 + 1 \\ &= 33 \end{aligned}$$

- Recurrence relations can also be written in other ways
    - In the following relation, a variable is used to denote where a positive integer expression may be inserted

$$\text{For every integer } k \geq 1, \qquad s_k = s_{k-1} - 1$$

- In sequences with the same recurrence relation but different initial conditions, similarities can be found in their patterns

Examples of Recursively Defined Sequences

Recursive Definitions of Sums

- The summation from $i = 1$ to n of a_i

$$\sum_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i \right) + a_n \qquad \text{if } n > 1.$$

- The production from $i = 1$ to n of a_i

$$\prod_{i=1}^{1} a_i = a_1 \qquad \text{and} \qquad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) \cdot a_n \qquad \text{if } n > 1.$$

[6] Set Theory

▼ [6.1] Set Theory: Definitions and the Element Method of Proof

$$A = \{\, x \in S \mid P(x) \,\}$$

Subsets: Proof and Disproof

- The definition for a set being a subset of another can be rewritten as a universal conditional statement:

$$A \subseteq B \iff \forall x, \text{if } x \in A \text{ then } x \in B$$

- Thus, this the negation is existential:

$$A \not\subseteq B \iff \exists x, \text{if } x \in A \text{ and } x \notin B$$

- Proper subsets may also be defined:

$$\begin{aligned}&A \text{ is a proper subset of } B \iff \\ &(1)\ A \subseteq B, \text{ and} \\ &(2) \text{ there is at least one element in } B \text{ that is not in } A.\end{aligned}$$

- **Singleton sets** are sets with one element
- **Element Argument:** The basic method for proving that one set is a subset of another
  - Let sets X and Y be given. To prove that $X \subseteq Y$,
    1. Suppose that x is a particular but arbitrarily chosen element of X
    2. Show that x is an element of Y
- Applying the element argument:

$$\begin{aligned}A &= \{\, m \in \mathbb{Z} \mid m = 6r + 12 \qquad \text{for some } r \in \mathbb{Z} \,\} \\ B &= \{\, n \in \mathbb{Z} \mid n = 3s \qquad\qquad \text{for some } s \in \mathbb{Z} \,\}\end{aligned}$$

$$A \subseteq B?$$

  - Suppose x is *particular but arbitrarily chosen* element of A

- *Show that $x \in B$, or by definition, that $x = 3 \cdot (\text{integer})$*
- By definition of A, there is an integer, say r, such that

$$x = 6r + 12$$

- *Express x in the form of B*
- $(2r + 4)$ is an integer because it is the sum of an integer and a product of integers
- Let $s = 2r + 4$

$$\begin{aligned} 3s &= 3(2r+4) && \text{(By substitution)} \\ &= 6r + 12 && \text{(By distributive property)} \\ &= x && \text{(By hypothesis)} \end{aligned}$$

- By definition of B, $x \in B$
- By definition of subset, $A \subseteq B$

$$B \not\subseteq A?$$

- *Just one counterexample has to be found to disprove $B \subseteq A$. By using the definition of A and B, an answer can be very intuitive*
- Let $x = 3$

$$\begin{aligned} 6r + 12 &= 3 && \text{(By assumption)} \\ 2r + 4 &= 1 && \text{(Divide both sides)} \\ 2r &= -3 \\ r &= -\frac{3}{2} \end{aligned}$$

- $-\frac{3}{2}$ is not an integer
- Thus, $3 \in B$ but $3 \notin A$ so $B \not\subseteq A$

Set Equality

- Given sets A and B, A equals B, written $A = B$, if, and only if, every element of A is in B and every element of B is in A
  - Symbolically:

$$A = B \iff A \subseteq B \quad \text{and} \quad B \subseteq A$$

- Equality example

$$\begin{aligned} A &= \{\, m \in \mathbb{Z} \mid m = 2a \qquad \text{for some integer } a \,\} \\ B &= \{\, n \in \mathbb{Z} \mid n = 2b - 2 \quad \text{for some integer } b \,\} \end{aligned}$$

  - *This is a 2-part proof since they both sets must be subsets of each other*
  - **Part 1:**
    - Suppose x is a particular but arbitrarily chosen element of A
    - By definition of A, there is an integer a such that

$$x = 2a$$

    - *Express x in the form of B*
    - Let $b = a + 1$
    - b is an integer because it is the sum of integers

$$\begin{aligned} x &= 2(a+1) - 2 \\ &= 2a + 2 - 2 \\ &= 2a \end{aligned}$$

    - By definition of B, $x \in B$
    - By definition of subset, $A \subseteq B$ is true because $x \in A$ and $x \in B$
  - **Part 2:**
    - Suppose x is a particular but arbitrarily chosen element of B
    - By definition of B, there is an integer b such that

$$x = 2b - 2$$

    - *Express x in the form of A*
    - Let $a = b + 1$
    - a is an integer because it is the sum of integers

$$\begin{aligned} x &= 2a \\ &= 2(b+1)-2 \\ &= 2b+2-2 \\ &= 2b \end{aligned}$$

    - By definition of A, $x \in A$
    - By definition of subset, $B \subseteq A$
  - Because $A \subseteq B$ and $B \subseteq A$, $A = B$ by definition of set equality

Venn Diagrams

- The relationships between sets can be represented using **Venn diagrams**
- For instance, $A \subseteq B$ can be shown as a circle A within a circle B or one overlapping circle $A = B$
- On the other hand, $A \nsubseteq B$ can be sown as two circles A and B that are apart or somewhat overlapping, or as a circle B within a circle A
- One notable application is demonstrating the relations between the major number sets

$$\mathbb{Z} \subseteq \mathbb{Q}$$

- The set of all integers is a proper subset of the set of all rational numbers because all rational numbers must be able to be expressed as a quotient of integers, and all integers can be expressed as a quotient with a divisor of 1
- Meanwhile, not all rational numbers are integers due to the quotient remainder theorem

$$\mathbb{Q} \subseteq \mathbb{R}$$

- The set of all rational numbers is a proper subset of the set of all real numbers because all rational numbers exist
- Meanwhile, not all real numbers are rational because a number can exist without being expressible as the quotient of two integers

Operations on Sets

- Let A and B be subsets of a universal set U
  - The **union** of A and B is the set of all elements that are in at least one of them and denoted as

$$A \cup B$$

- The **intersection** of A and B is the set of all elements that are common to both and denoted as

$$A \cap B$$

- The **difference** of B and A—or **relative complement** of A in B)—is the set of all elements not in A but in B and denoted as

$$B - A$$

- The **complement** of A is the set of all elements in U not in A and denoted as

$$A^{\complement}$$

- Venn diagrams can be used to represent these operations
- Sets may also be represented as intervals
  - Given real numbers a and b with $a \leq b$:

$$\begin{gathered}(a, b) = \{\, x \in R \mid a < x < b \,\} \\ [a, b) = \{\, x \in R \mid a \leq x < b \,\} \\ (a, b] = \{\, x \in R \mid a < x \leq b \,\} \\ [a, b] = \{\, x \in R \mid a \leq x \leq b \,\} \\ \\ (-\infty, b) = \{\, x \in R \mid x < b \,\} \\ (-\infty, b] = \{\, x \in R \mid x \leq b \,\} \\ (a, \infty) = \{\, x \in R \mid a < x \,\} \\ [a, \infty) = \{\, x \in R \mid a \leq x \,\}\end{gathered}$$

- **Unions and intersections of an indexed collection of sets**
  - Given sets $A_0, A_1, \ldots$ that are subsets of universal set U and given nonnegative integer n

$$\bigcup_{i=0}^{n} A_i = \{\, x \in U \mid x \in A_i \ \text{ for at least one } i = 0, 1, 2, \ldots, n \,\}$$

$$A_0 \cup A_1 \cup A_2 \cup \cdots \cup A_n$$

$$\bigcup_{i=0}^{\infty} A_i = \{\, x \in U \mid x \in A_i \ \text{ for at least one nonnegative integer } i \ \}$$

$$A_0 \cup A_1 \cup A_2 \cdots$$

$$\bigcap_{i=0}^{n} A_i = \{\, x \in U \mid x \in A_i \ \text{ for every } i = 0, 1, 2, \ldots, n \,\}$$

$$A_0 \cap A_1 \cap A_2 \cap \cdots \cap A_n$$

$$\bigcap_{i=0}^{\infty} A_i = \{\, x \in U \mid x \in A_i \ \text{ for every nonegative integer } i \,\}$$

$$A_0 \cap A_1 \cap A_2 \cdots$$

- Interval notation for a union of an indexed collection of sets is the smallest interval of all the sets

$$\bigcup_{i=1}^{4} \left\{ x \in \mathbb{R} \mid -\frac{1}{i} \leq x \leq \frac{1}{i} \right\} = [-1, 1]$$

$$\bigcup_{i=1}^{\infty} \left\{ x \in \mathbb{R} \mid -\frac{1}{i} \leq x \leq \frac{1}{i} \right\} = [-1, 1]$$

- Interval notation for an intersection of an indexed collection of sets is the largest interval of all the sets

$$\bigcap_{i=1}^{4} \left\{ x \in \mathbb{R} \mid -\frac{1}{i} \leq x \leq \frac{1}{i} \right\} = \left[-\frac{1}{4}, \frac{1}{4} \right]$$

$$\bigcap_{i=1}^{\infty} \left\{ x \in \mathbb{R} \mid -\frac{1}{i} \leq x \leq \frac{1}{i} \right\} = (0, 0)$$

The Empty Set

- The only set with no elements is known as the **empty set** or **null set**, denoted by

$$\varnothing \quad \text{or} \quad \emptyset$$

- Thus,

$$\{\,1,3\,\} \cap \{\,2,4\,\} = \varnothing$$
$$\{\,x \in \mathbb{R} \mid x^2 = -1\,\} = \varnothing$$

Partitions of Sets

- Two sets are a **disjoint** if, and only if, they have no elements in common
    - Symbolically:

$$A \text{ and } B \text{ are disjoint } \iff A \not\cap B$$

- Sets $A_1, A_2, A_3, \ldots$ are **mutually disjoint**—or **pairwise disjoint** or **nonoverlapping**—if, and only if, no two sets with distinct subscripts have any elements in common
- A finite collection of nonempty sets $\{\,A_1, A_2, A_3, \ldots, A_n\,\}$ is a **partition** of a set A, if, and only if
    1. $\varnothing$ is not an element of the finite collection
    2. A is the union of all sets A_i for each integer i up to, and including, n in the finite collection

3. The sets $A_1, A_2, A_3, \ldots$ are mutually disjoint

- Partition examples given

$$A = \{\{\,1,2,3,4,5,7,8\,\}\}$$

$$\{\,\{\,5,4\,\},\{\,7,2\,\},\{\,1,3,4\,\},\{\,6,8\,\}\,\} \quad \text{a partition of } A?$$

- This set is a partition of A
    - The empty set is not an element
    - The union of all sets within the collection is equivalent to set A
    - None of the sets in the collection have any overlapping elements

$$\{\,\{\,3,7,8\,\},\{\,2\,\},\{\,1,4,5\,\}\,\} \quad \text{a partition of } A?$$

- This set is not a partition of A
    - The set does not have the empty set as an element nor are the sets of the collection mutually disjoint
    - However, the union of all sets within the collection results in the following set:

$$\{1, 2, 3, 4, 5, 7, 8\}$$

    - This set does not equal set A, thus this set is not a partition of A

Power Sets

- According to the **power set axiom**, given a set A, the **power set** of A is the set of all subsets of A, denoted as

$$\mathcal{P}(A)$$

  - The empty set is a subset of all sets

- For example, the power set of a set with two elements would include four elements

$$\mathcal{P}(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$$

▼ [6.2] Properties of Sets

- **Subset relations**
  1. **Inclusion of intersection:** For all sets A and B

$$A \cap B \subseteq A \quad \text{and} \quad A \cap B \subseteq B$$

  2. **Inclusion in union:** For all sets A and B

$$A \subseteq A \cup B \quad \text{and} \quad B \subseteq A \cup B$$

  3. **Transitive property:** For all sets A, B, and C

$$\text{if } A \subseteq B \quad \text{and} \quad B \subseteq C \quad \text{then} \quad A \subseteq C$$

- **Procedural versions of set definitions**
  - *These are derived in similar manners and can be important to some relations because they express how set operations impact the elements in the sets*
  - Let X and Y be subsets of universal set U and suppose x and y are elements of U

$$x \in X \cup Y \iff x \in X \text{ or } x \in Y \tag{1}$$
$$x \in X \cap Y \iff x \in X \text{ and } x \in Y \tag{2}$$
$$x \in X - Y \iff x \in X \text{ and } x \notin Y \tag{3}$$
$$x \in X^{\complement} \iff x \notin X \tag{4}$$
$$(x, y) \in X \times Y \iff x \in X \text{ and } y \in Y \tag{5}$$

Proving a Subset Relation

- Prove that for all sets A and B, $A \cap B \subseteq A$
    - Suppose A and B are any *particular but arbitrarily chosen* sets
    - *We are proving the inclusion of intersection property*
    - Suppose x is any element in $A \cap B$
        - *Show that x is in A*
    - Then, $x \in A$ and $x \in B$ by definition of intersection
    - In particular, x is in A since both components of an "and" statement must be true if it is true
    - Thus, every element in $A \cap B$ is in A
    - Therefore, $A \cap B \subseteq A$ by definition of subset

Set Identities

- An **identity** is an equation that is universally true for all elements in some set
- Here are some important laws

1. **Commutative Laws:** For all sets A and B

$$A \cup B = B \cup A \quad \text{and} \quad A \cap B = B \cap A$$

2. **Associative Laws:** For all sets A, B, and C

$$\begin{gathered}(A \cup B) \cup C = A \cup (B \cup C) \quad \text{and} \\ (A \cap B) \cap C = A \cap (B \cap C)\end{gathered}$$

3. **Distributive Laws:** For all sets A, B, and C

$$\begin{gathered}A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and} \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\end{gathered}$$

4. **Identity Laws:** For every set A

$$A \cup \varnothing = A \quad \text{and} \quad A \cap U = A$$

5. **Complement Laws:** For every set A

$$A \cup A^{\complement} = U \quad \text{and} \quad A \cap A^{\complement} = \varnothing$$

6. **Double Complement Law:** For every set A

$$(A^{\complement})^{\complement} = A$$

7. **Idempotent Laws:** For every set A

$$A \cup A = A \quad \text{and} \quad A \cap A = A$$

8. **Universal Bound Laws:** For every set A

$$A \cup U = U \quad \text{and} \quad A \cap \varnothing = \varnothing$$

9. **De Morgan's Laws:** For all sets A and B

$$(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement} \quad \text{and} \quad (A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$$

10. **Absorption Laws:** For all sets A and B

$$A \cup (A \cap B) = A \quad \text{and} \quad A \cap (A \cup B) = A$$

11. **Complements of U and $\varnothing$:**

$$U^{\complement} = \varnothing \quad \text{and} \quad \varnothing^{\complement} = U$$

12. **Set Difference Law:** For all sets A and B

$$A - B = A \cap B^{\complement}$$

The Empty Set (again)

- There are two main theorems associated with sets
- If E is a set with no elements and A is any set, then

$$E \subseteq A$$

- There is only one set with no elements
- Generalized distributive law proof
    - Prove that for all sets A and $B_1, B_2, B_3, \ldots, B_N$, where n is a positive integer

$$A \cup \left(\bigcap_{i=1}^{n} B_i \right) = \bigcap_{i=1}^{n} (A \cup B_i)$$

- Suppose A and $B_1, B_2, B_3, \ldots, B_N$ are any sets and n is a positive integer
- **Part 1:** Prove

$$A \cup \left(\bigcap_{i=1}^{n} B_i\right) \subseteq \bigcap_{i=1}^{n} (A \cup B_i)$$

  - Suppose x is any element in $A \cup (\bigcap_{i=1}^{n} B_i)$
  - *Following the element method of argument, we must show that x is an element of the first set*
  - By definition of union, $x \in A$ or $x \in (\bigcap_{i=1}^{n} B_i)$
  - **Case 1:**

$$x \in A$$

    - By definition of union, for every integer $i = 1, 2, \ldots, n$, $x \in A \cup B_i$
    - Thus, $x \in (\bigcap_{i=1}^{n} B_i)$
  - **Case 2:**

$$x \in \bigcap_{i=1}^{n} B_i$$

    - By definition of general intersection, for every integer $i = 1, 2, \ldots, n$, $x \in B_i$
    - By definition of union, for every integer $i = 1, 2, \ldots, n$, $x \in A \cup B_i$
    - Thus, $x \in (\bigcap_{i=1}^{n} B_i)$
  - In both cases, $x \in (\bigcap_{i=1}^{n} B_i)$ is shown to be true
- **Part 2:** Prove
  - Suppose x is any element in $\bigcap_{i=1}^{n} (A \cup B_i)$

$$\bigcap_{i=1}^{n} (A \cup B_i) \subseteq A \cup \left(\bigcap_{i=1}^{n} B_i\right)$$

  - **Case 1:**

$$x \in A$$

    - By definition of union, $x \in A \cup (\bigcap_{i=1}^{n} B_i)$

- **Case 2:**

$$x \notin A$$

  - By definition of intersection, $x \in A \cup B_i$ for every integer $i = 1, 2, \ldots, n$
  - Because $x \notin A$, x must be an element in B_i for every integer $i = 1, 2, \ldots, n$
  - Hence, by definition of general intersection, $x \in \bigcap_{i=1}^{n} B_i$
  - By definition of union, $x \in A \cup (\bigcap_{i=1}^{n} B_i)$

- Both containments are proven, so the proof is true

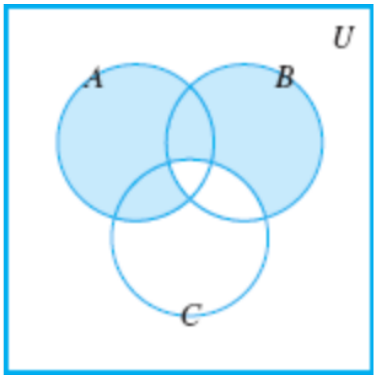
▼ [6.3] Disproofs and Algebraic Proofs

Disproving an Alleged Set Property

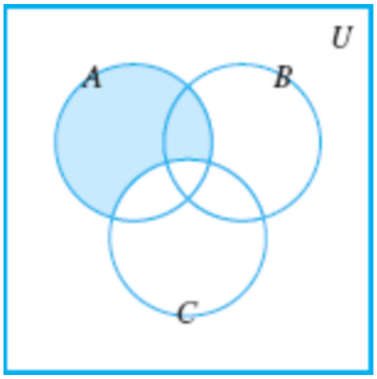
- Recall that universal statements only need one counterexample to show that they are false
- For all sets A, B, and C,

$$(A - B) \cup (B - C) = A - C$$

  - *We have to find sets A, B, and C for which the previous equality does not hold*
  - A Venn diagram can be used to determine a contradiction
    - The region corresponding to $(A - B) \cup (B - C)$ is



    - The region corresponding to $A - C$ is



- *The difference in shaded regions can be used to find a counterexample*

- Using the different subregions formed by the intersections of the Venn diagrams, different numbers may be assigned to them and be the elements of the sets
- Let $A = \{1, 2, 4, 5\}, B = \{2, 3, 5, 6\}, C = \{4, 5, 6, 7\}$
- Thus,

$$\begin{aligned} A - B &= \{1, 4\} \\ B - C &= \{2, 3\} \\ A - C &= \{1, 2\} \end{aligned}$$

- As a result,

$$\begin{aligned} (A - B) \cup (B - C) &= \{1, 4\} \cup \{2, 3\} \\ &= \{1, 2, 3, 4\} \end{aligned}$$

$$\{1, 2, 3, 4\} \neq \{1, 2\}$$

- Therefore,

$$(A - B) \cup (B - C) \neq A - C$$

- *You may also notice from the shaded regions that as long as an element is in B but not in A, then the proposed property is just false no matter what the other elements are;*

The Number of Subsets of a Set

- If set A has n elements, then $\mathcal{P}(A)$ has 2^n elements
- For every integer $n \geq 0$, if set X has n elements, then $\mathcal{P}(X)$ has 2^n elements
  - Let $P(n)$ be the sentence “Any set with n elements has 2^n subsets”

  - **(Basis step)** *Show* $P(0)$
    - Any set with 0 elements has 2^0 subsets
    - There is one distinct set with 0 elements, ∅, and itself only subset is itself
    - Thus, a 0 element set has one subset
    - $1 = 2^0$, thus $P(0)$
  - **(Inductive step)** *Show that for every integer* $k \geq 0$*, if* $P(k)$ *is true then* $P(k+1)$ *is also true*
    - Suppose that P(k) is true for *a particular but arbitrarily chosen* integer $k \geq 0$ such that
    - Any subset with k elements has 2^k subsets
    - *We must show that* $P(k+1)$ *is true*
    - Any set with $k+1$ elements has 2^{k+1} subsets
    - Let X be a set with $k+1$ elements
    - $k+1 \geq 1$
- By focusing on a particular element, the mathematical induction process becomes much easier

“Algebraic” Proofs of Set Identities

- After establishing a particular number of identities and properties, new properties can be derived algebraically
- Ex: Deriving a set difference property
  - *Construct an algebraic proof that for all sets* A*,* B*, and* C

$$(A \cup B) - C = (A - C) \cup (B - C)$$

  - Let A, B, and C be any sets
  - Thus,

$$\begin{aligned} (A \cup B) - C &= (A \cup B) \cap C^{\complement} && \text{(By set diff law)} \\ &= C^{\complement} \cap (A \cup B) && \text{(By commutative law)} \\ &= (A \cap C^{\complement}) \cup (B \cap C^{\complement}) && \text{(By distrib law)} \\ &= (A - C) \cup (B - C) && \text{(By set diff law)} \end{aligned}$$

- Ex: Deriving a set identity using properties of ∅
  - *Construct an algebraic proof that for all sets* A *and* B

$$A - (A \cap B) = A - B$$

- Suppose A and B are any sets
- Thus,

$$\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^{\mathsf{C}} && \text{(Set difference law)} \\
&= A \cap \left(A^{\mathsf{C}} \cup B^{\mathsf{C}}\right) && \text{(De Morgan's laws)} \\
&= (A \cap A^{\mathsf{C}}) \cup (A \cap B^{\mathsf{C}}) && \text{(Distributive laws)} \\
&= \varnothing \cup (A \cap B^{\mathsf{C}}) && \text{(Complement laws)} \\
&= A \cap B^{\mathsf{C}} && \text{(Identity laws)} \\
&= A - B && \text{(Set difference law)}
\end{aligned}$$

▼ [6.4] Boolean Algebras, Russell's Paradox, and the Halting Problem

- Logical equivalences and set properties have many similarities
  - For example

$$\begin{aligned}
p \vee q &\equiv q \vee p & A \cup B &= B \cup A \\
\\
p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r) & A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\
p \vee (q \wedge r) &\equiv (p \vee q) \wedge (p \vee r) & A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\
\\
p \vee \mathbf{c} &\equiv p & A \cup \varnothing &= A \\
p \wedge \mathbf{t} &\equiv p & A \cap U &= A
\end{aligned}$$

- This correspondence shows how logical equivalences and set properties are both cases of the same general structure called **Boolean algebra**
- A **Boolean algebra** is a set B together with two operations, generally denoted as $+$ (OR) and $\cdot$ (AND) such that for all a and b in B, both $a + b$ and $a \cdot b$ are in B and the following axioms hold

1. **Commutative laws:** For all a and b in B,

$$a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot 1$$

2. **Associative laws:** For all a, b, and c in B,

$$(a + b) + c = a + (b + c) \quad \text{and} \quad a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3. **Distributive laws:** For all a, b, and c in B,

$$a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

4. **Identity laws:** There are distinct elements 0 and 1 in B such that for each a in B,

$$a + 0 = a \quad \text{and} \quad a \cdot 1 = a$$

5. **Complement laws:** For each a in B, there exists an element in B, denoted $\overline{a}$, called the **complement** or **negation** of a, such that

$$a + \overline{a} = 1 \quad \text{and} \quad a \cdot \overline{a} = 0$$

- In any **Boolean algebra**, the complement of each element is unique, and the quantities 0 and 1 are unique
- Boolean algebras also share similar properties to sets

1. **Uniqueness of the complement laws:**

$$\begin{gathered}\text{For all } a \text{ an d } x \text{ in } B, \\ \text{If } a + x = 1 \text{ and } a \cdot x = 0 \text{ then } x = \overline{a}.\end{gathered}$$

2. **Uniqueness of 1 and 0:** If there exists x in B

$$\begin{gathered}\text{If there exists } x \text{ in } B \text{ such that} \\ a + x = a \\ \text{for every } a \text{ in } B, \text{ then} \\ x = 0 \\ \\ \text{and if there exists } y \text{ in } B \text{ such that} \\ a \cdot y = a \\ \text{for every } a \text{ in } B, \text{ then} \\ y = 1\end{gathered}$$

3. **Double complement law:**

$$\begin{gathered}\text{For every } a \in B \\ \overline{(\overline{a})} = a\end{gathered}$$

4. **Idempotent laws:**

$$\text{For every } a \in B$$
$$a + a = a \quad \text{and} \quad a \cdot a = a$$

5. **Universal bound laws:**

$$\text{For every } a \in B$$
$$a + 1 = 1 \quad \text{and} \quad a \cdot 0 = 0$$

6. **De Morgan's laws:**

$$\text{For all } a \text{ and } b \in B$$
$$\overline{a + b} = \overline{a} \cdot \overline{b} \quad \text{and} \quad \overline{a \cdot b} = \overline{a} + \overline{b}$$

7. **Absorption laws:**

$$\text{For all } a \text{ and } b \in B$$
$$(a + b) \cdot a = a \quad \text{and} \quad (a \cdot b) + a = a$$

8. **Complements of 0 and 1:**

$$\overline{0} = 1 \quad \text{and} \quad \overline{1} = 0$$

- Proving the first property
  - Suppose a and x are *particular but arbitrarily chosen* elements of B that satisfy the hypothesis

$$a + x = 1 \quad \text{and} \quad a \cdot x = 0$$

  - Then

$$\begin{aligned}
x &= x \cdot 1 && \text{(Identity laws)} \\
&= x \cdot (a + \overline{a}) && \text{(Complement laws)} \\
&= (x \cdot a) + (x \cdot \overline{a}) && \text{(Distributive laws)} \\
&= 0 + (x \cdot \overline{a}) && \text{(Hypothesis)} \\
&= (a \cdot \overline{a}) + (x \cdot \overline{a}) && \text{(Complement laws)} \\
&= \overline{a} \cdot (a + x) && \text{(Distributive laws)} \\
&= \overline{a} \cdot 1 && \text{(Hypothesis)} \\
&= \overline{a} && \text{(Identity laws)}
\end{aligned}$$

- Notice how this Boolean algebra property and the definitions all have **paired statements**

  - Interchanging $+$ and $\cdot$ signs and 1 and 0 may transform any Boolean identity into its **dual identity**
- According to the **duality principle**, the dual of any Boolean identity is also an identity
- Proving the idempotent law for $+$ *using dual identities*
  - Suppose B is a Boolean algebra and a is any element of B that satisfies the hypothesis

$$a + a = a$$

  - Then

$$\begin{aligned} a &= a + 0 && \text{(Identity laws)} \\ &= a + (a \cdot \overline{a}) && \text{(Complement laws)} \\ &= (a + a) \cdot (a + \overline{a}) && \text{(Distributive laws)} \\ &= (a + a) \cdot 1 && \text{(Complement laws)} \\ &= a + a && \text{(Identity laws)} \end{aligned}$$

Russell’s Paradox

- **Russell’s Paradox:**
  - Most elements are not sets of themselves
  - If we are allowed to use any description for set’s defining property, then we may let S be the set of all sets that are not elements of themselves

$$S = \{\, A \mid A \text{ is a set and } A \notin A \,\}$$

  - Given this definition, may S be an element of itself?
- Supposing $S \in S$, S satisfies the defining property for S, meaning that $S \notin S$
- Supposing $S \notin S$, S does not satisfy the defining property for S, meaning that $S \in S$
- In both cases, S is both an element of itself and not an element of itself
- The creator of the paradox, Bertrand Russell, devised the **barber puzzle** which follows the same logic
  - If a male barber only shaves men who do not shave themselves, does the barber shave himself?
- There are many methods of defining basic set theory concepts safely
  - Predicates may be used as the defining property for a set

The Halting Problem

- **The Halting Problem:**
    - Can an algorithm be implemented that checks whether a given data set results in an infinite loop?
    - Turing concluded that it was not possible
- Suppose there is an algorithm, $\mathrm{CheckHalt}$, such that if an algorithm X and a data set D are input, then
    - $\mathrm{CheckHalt}(X, D)$ prints "halts" if X terminates after a finite number of steps when run with data set D
    - $\mathrm{CheckHalt}(X, D)$ prints "loops forever" if X does not terminate after a finite number of steps when run with data set D
- Algorithm X is a sequence of characters, thus it is also a data set
- Let algorithm Test be defined as follows with an input algorithm X
    - Loops forever if $\mathrm{CheckHalt}(X, X)$ prints "halts"
    - Stops if $\mathrm{CheckHalt}(X, X)$ prints "loops forever"
- Run Test with itself as the input algorithm
    - If $\mathrm{Test}(\mathrm{Test})$ terminates after a finite number of iterations, then $\mathrm{CheckHalt}(\mathrm{Test}, \mathrm{Test})$ prints "halts" so $\mathrm{Test}(\mathrm{Test})$ loops forever
    - If $\mathrm{Test}(\mathrm{Test})$ loops forever, then $\mathrm{CheckHalt}(\mathrm{Test}, \mathrm{Test})$ prints "loops forever" so $\mathrm{Test}(\mathrm{Test})$ terminates
    - This shows that $\mathrm{Test}(\mathrm{Test})$ loops forever and terminates at the same time, which is a contradiction
    - The existence of the algorithm Test follows logically from the supposition that $\mathrm{CheckHalt}$ can check any algorithm and data set for termination
    - Therefore, the supposition must be false, and there is no such algorithm