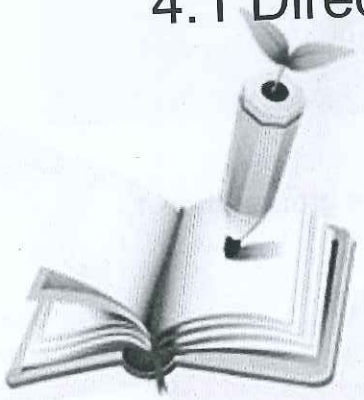
Chapter 4: Elementary Number Theory and Methods of Proof

4.1 Direct Proof and Counterexample I: Introduction



Even: $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}$ such that even$(n) \leftrightarrow n = 2 \cdot m$

Even and Odd Integers

iff $= (P \to Q) \wedge (Q \to P)$: $P \to Q$ describe Property $Q \to P$ How to Prove

Definition:

- An integer n is **even** if, and only if, n equals twice some integer.
- An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.

n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$.

Example: justify even and odd integers.

- Is 0 even? Yes. $0 = 2 \times 0$
- Is -301 odd? Yes. $-301 = 2 \times (-151) + 1$
- If a and b are integers, is $6a^2b$ even? Yes. $6a^2b = 2 \times 3a^2b$
- If a and b are integers, is $10a + 8b + 1$ odd?
  - Yes. $10a + 8b + 1 = 2 \times (5a + 4b) + 1$

Prime and Composite Numbers

Definition:

- An integer n is **prime** if, and only if, $\boldsymbol{n > 1}$ and for all positive integers r and s, if $n = rs$, then either r or s equals n.
- An integer n is **composite** if, and only if, $\mathbf{n > 1}$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

Symbolically, if n is an integer, then

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

n is composite $\Leftrightarrow$ $\exists$ positive numbers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$

Note:

- 1 is not a prime number, because a prime number must be greater than 1.
- Every integer greater than 1 either prime or composite.

Proving Existential Statements

A statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is true if, and only if,

$Q(x)$ is true for at least one x in D.

Proof methods:

- Constructive proof of existence
- Non-constructive proof of existence

Constructive Proofs of Existence

Constructive Proof of Existence:

1. Find an a in D that make $Q(a)$ true
2. Give a set of directions for finding such an a.

Example:

1. Show that there is a positive integer that can be written as a sum of cubes of positive integers in two different ways.
   Proof: $1729 = 10^3 + 9^3$ and $1729 = 12^3 + 1^3$.
2. Proof ∃ an even integer n that can be written in two ways as a sum of two prime numbers.
   Proof: let $n = 10$. then $10 = 5 + 5 = 3 + 7$ and 3,5, and 7 are all prime numbers.

Non-constructive Existence Proofs - Example

- Nonconstructive existence proof: show that $\exists x P(x)$ without explicitly giving a for which $P(a)$ is true.

Example: Show that there exist irrational numbers x and y such that x^y is rational.

Consider the number $\sqrt{2}^{\sqrt{2}}$. There are two possible cases:

i. $\sqrt{2}^{\sqrt{2}}$ Is rational: let $x = \sqrt{2}$, $y = \sqrt{2}$

ii. $\sqrt{2}^{\sqrt{2}}$ Is irrational: let $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$, then $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2$.

Disproof Universal Conditional Statements by Counterexample

Disproof by Counterexample

- To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false.
- Such an x is called a **counterexample**.

Example:

Statement: ∀ real numbers a and b, if $a^2 = b^2$ then $a = b$.

Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, so $a^2 = b^2$. But $a \neq b$.

Proving Universal Statement

- Universal statement form:

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

- Proof methods (not limited to):
  - The method of exhaustion. — not practical for big domains
  - Method of Generalizing from the Generic Particular
  - Direct proof

The Method of Exhaustion

- When there is a finite and small number of examples for which we need to prove a statement.

Use the method of exhaustion to prove the statement:
$\forall n \in Z$, if n is a positive integer with $n \leq 2$ then $(n + 1)^2 \geq 3^n$.

Examine the cases $n = 1, 2$.

For $n = 1, (n + 1)^2 = 2^2 = 4 \geq 3 = 3^n$.

For $n = 2, (n + 1)^2 = 3^2 = 9 \geq 3^2 = 3^n$.

Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property,

- suppose x is a particular but arbitrarily chosen element of the set
  - Particular: in its domain
  - Arbitrarily chosen: could be any one
- show that x satisfies the property.

Method of Direct Proof

Direct proof :

- A specific method of generalizing from the generic particular
- The proved property is in the form "if $P(x)$ then $Q(x)$"

Method of Direct Proof

1. Rewriting the Statement:
   Express the statement to be proved in the form $\forall x \in D$, if $P(x)$ then $Q(x)$
2. Chose an element:
   Start the proof by supposing x is a **particular but arbitrarily** chosen element of D for which the hypothesis P(x) is true.
3. Show that the conclusion Q(x) is true by using definitions, previously established results, and the rules for logical inference.

Direct Proof: Exercise

Theorem 4.1.1

The sum of any two even integers is even. → $\forall x, y \in \mathbb{Z}$, if x, y is even, then $x+y$ is even

Proof:

Suppose m and n are *[particular but arbitrarily chosen]* even integers. *[We must show that $m + n$ is even.]* By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then

$$m + n = 2r + 2s \quad \text{by substitution}$$
$$= 2(r + s) \quad \text{by factoring out a 2.}$$

Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence

$$m + n = 2t \quad \text{where } t \text{ is an integer.}$$

It follows by definition of even that $m + n$ is even. *[This is what we needed to show.]*

Start: $P(x,y)$ is true

x, y is even

$x = 2k \ (k \in \mathbb{Z})$

$y = 2L \ (L \in \mathbb{Z})$

$x + y = 2k + 2L = 2(k + L)$

$x + y = 2(\text{Some Integer})$

End: $x + y$ is even

$\forall a, b \in \mathbb{Z}$, if $\overbrace{a \text{ is odd and } b \text{ is even}}^{P(a,b)}$, then $\overbrace{2a + 3b \text{ even}}^{Q(a,b)}$

Start 2: $P(a,b) = \text{true}$

a is odd and b is even

$b = 2K \ (K \in \mathbb{Z})$

$a = 2L + 1 \ (L \in \mathbb{Z})$

$2a + 3b = 3(2K) + 2(2L + 1) = 4 \cdot L 3$

Exercise

If a is any odd integer and b is any even integer, then $2a + 3b$ is even.

Direct Proof

Hint:

a is any odd integer $\Rightarrow a = 2k + 1$ for some integer k.

b is any even integer $\Rightarrow b = 2l$ for some integer l.

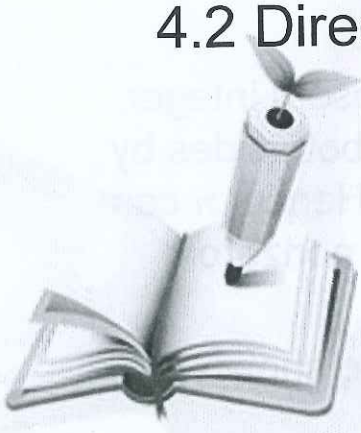
$$\begin{aligned} 2a + 3b &= 2(2k + 1) + 3(2l) \\ &= 2(2k + 1) + 2(3l) \\ &= 2(2k + 1 + 3l) \end{aligned}$$

Conclusion: ????? $\Rightarrow 2a + 3b$ is even.

$2a + 3b = 2r$ for some integer r $\Rightarrow 2a + 3b$ is even.

Chapter 4: Elementary Number Theory and Methods of Proof

4.2 Direct Proof and Counterexample II: Rational Numbers



Rational and Irrational Numbers

Definition

- A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator.
- A real number that is not rational is **irrational**.

More formally, if r is a real number, then

r is rational $\Leftrightarrow \exists$ integers a and b such that $r = \frac{a}{b}$ and $b \neq 0$.

- The word "**rational**" contains the word "**ratio**", which is another word for "**quotient**".
- A rational number can be written as a ratio of integers.

Exercise:

- Is 10/3 a rational number? Yes
- Is 2/0 is a rational number? No.
- Is 2/0 is an irrational number? No.

Proving Properties of Rational Numbers

Method of generalizing from the generic particular: prove the property is true for an arbitrarily chosen element in the domain.

Theorem 4.2.1

Every integer is a rational number.

Proof:

Suppose n is any [particular but arbitrarily chosen] integer. Then $n = n \cdot 1$, and so $n = n/1$ by dividing both sides by 1. Now n and 1 are both integers, and $1 \neq 0$. Hence, n can be written as a quotient of two integers with a nonzero denominator.

Therefore, n is rational. [This is what was to be shown.]

The Sum of Rational Numbers

Theorem 4.2.2: The sum of any two rational numbers is rational.

1. Rewriting the statement to be proved in the form:

   "∀_____, if _____ then_____."

   – Formal Restatement: ∀ real numbers r and s, if r and s are rational then $r + s$ is rational.

2. Find out the starting point and the conclusion.

   – Starting point:

   • Suppose r and s are particular but arbitrarily chosen real numbers such that r and s are rational. Or, more simply

   • Suppose r and s are particular but arbitrarily chosen rational numbers.

   – Conclusion: $r + s$ is rational.

3. How to get from the starting point to the conclusion?

The Sum of Rational Numbers

Proof:

Suppose r and s are rational numbers. [We must show that $r + s$ is rational.] Then, by the definition of rational, r and s can be expressed as:

$$r = \frac{a}{b} \text{ and } s = \frac{c}{d}$$

for some integers a, b, c, and d where $b \neq 0$ and $d \neq 0$.

• It follows by substitution that

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad}{bd} + \frac{bc}{bd} && \text{Rewriting the fraction with a common denominator.} \\ &= \frac{ad+bc}{bd} && \text{Adding fractions with a common denominator.} \end{aligned}$$

The Sum of Rational Numbers

$$r + s = \frac{ad + bc}{bd}$$

Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers and because a, b, c and d are all integers. Also $q \neq 0$ by the zero product property. Thus,

$r + s = \frac{p}{q}$ where p and q are integers and $q \neq 0$.

Therefore, $r + s$ is rational by definition of a rational number. [This is what was to be shown.]

Zero Product Property

If neither of two real numbers is zero, then their product is also not zero.

Corollary

- A corollary is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Theorem: The sum of any two rational numbers is rational.

Corollary: The double of a rational number is rational.

Proof:

Suppose r is any rational number. Then $2r = r + r$ is a sum of two rational numbers. So by the theorem 4.2.2, $2r$ is rational.

Hence the double of a rational number is rational.

Deriving Additional Results about Even and Odd Integers

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.

2. The sum and difference of any two odd integers are even.

3. The product of any two odd integers is odd.

4. The product of any even integer and any odd integer is even.

5. The sum of any odd integer and any even integer is odd.

6. The difference of any odd integer minus any even integer is odd.

7. The difference of any even integer minus any odd integer is odd.

Use the properties listed above to prove that if *a* is any even integer and *b* is any odd integer, then $\frac{a^2+b^2+1}{2}$ s an integer.

Example 3 – Solution

Proof:

Suppose a is any even integer and b is any odd integer. By property 3, b^2 is odd, and by property 1, a^2 is even.

Then by property 5, $a^2 + b^2$is odd, and because 1 is also odd, the sum $(a^2 + b^2) + 1 = a^2 + b^2 + 1$ is even by property 2.

Hence, by definition of even, there exists an integer k such that $a^2 + b^2 + 1 = 2k$.

Dividing both sides by 2 gives $\frac{a^2+b^2+1}{2} = k$, which is an integer.

Thus $\frac{a^2+b^2+1}{2}$ is an integer *[as was to be shown]*.

In-class Exercise 4

Prove the following statements by direct proof.

a) The product of any two odd integers is odd.

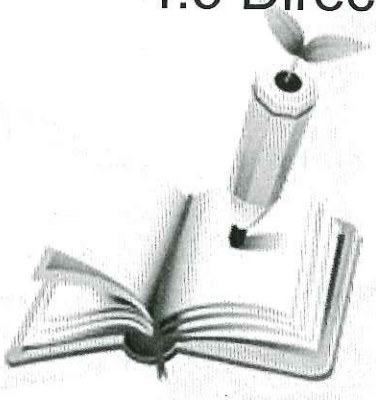
b) For all integers n and m, if $n - m$ is even, then $n^3 - m^3$ is even.

c) For all integers m, if $m > 2$, then $m^2 - 4$ is composite.

d) The square of any rational number is rational.

Chapter 4: Elementary Number Theory and Methods of Proof

4.3 Direct Proof and Counterexample III: Divisibility



Divisibility = gets integer quotient

Definition

- If n and d are integers and $d \neq 0$ then
  n is divisible by d if, and only if, n equals d times some integer.
- Instead of "n is divisible by d", we can say that
  n is a multiple of d, or
  d is a factor of n, or
  d is a divisor of n, or
  d divides n : $d|n$
- The notation $d|n$ is read "d divides n".
- Symbolically, if n and d are integers and $d \neq 0$:
  $d|n \quad \Leftrightarrow \quad \exists$ an integer k such that $n = d \cdot k$

Divisors of zero: if k is any nonzero integer, does k divide 0?
Solution: Yes, because $0 = k \cdot 0$

Property of Real Numbers

- T12: Rule for multiplication with negative signs:

$$(-a)b = a(-b) = -(ab),\ (-a)(-b) = ab$$

and

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$$

- T20: multiplying both sides of an inequality by a positive number preserves the inequality
- T25: if the product of any two real numbers is positive, then both real numbers are positive or both are negative

Properties of Divisibility - I

Theorem 4.3.1 A positive divisor of a positive Integer

For all integers a and b, if a and b are positive and a divides b, then $a \leq b$.

$a|b = b = ak$

Proof:

Suppose a and b are positive integers and a divides b. [we must show that $a \leq b$]. By the definition of divisibility, there exists an integer k such that $b = ak$. By property T25 k must be positive because both a and b are positive. It follows that

$$1 \leq k$$

Because every positive integer is greater than or equal to 1. Multiplying both sides by a gives

$$a \leq ka = b$$

Thus $a \leq b$ [as was to be shown]

Properties of Divisibility - II

Theorem 4.3.2 Divisors of 1

The only divisors of 1 are 1 and -1.

Proof:

Suppose m is any integer that divides 1. Then there exists an integer n such that $1 = m \cdot n$.

By property T25, either both m and n are positive or both m and n are negative.

1. If both m and n are positive, then m is a positive integer divisor of 1. By Theorem 4.3.1, $m \leq 1$. Since the only positive integer that is less than or equal 1 is 1 itself, it follows that $m = 1$.
2. If both m and n are negative, then, by property T12, $(-m)(-n) = mn = 1$. In this case $-m$ is a positive integer divisor of 1, and so, by the same reasoning, $-m = 1$ and thus $m = -1$.

Therefore there are only two possibilities: either $m = 1$ or $m = -1$. So the only divisors of 1 are 1 and −1 [as was to be shown].

Example 1 – Divisibility of Algebraic Expressions

a. If a and b are integers, is $3a + 3b$ divisible by 3? $\frac{3(a+b)}{3} = a+b$ ✓

b. If k and m are integers, is $10km$ divisible by 5?

Solution:

a. Yes. By the distributive law of algebra, $3a + 3b = 3(a + b)$ and $a + b$ is an integer because it is a sum of two integers.

b. Yes. By the associative law of algebra, $10km = 5 \cdot (2km)$ and $2km$ is an integer because it is a product of three integers.

Checking Nondivisibility

When the definition of divides is rewritten formally using the existential quantifier, the result is

$$d|n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = d \cdot k$$

Since the negation of an existential statement is universal, it follows that d does not divide n (denoted $d \nmid n$) if, and only if, $\forall$ integers k, $n \neq dk$, or, in other words, the quotient n/d is not an integer.

For all integers n and d, $\quad d \nmid n \quad \Leftrightarrow \quad \frac{n}{d}$ is not an integer.

Example 4 – Checking Nondivisibility

Does 4 | 15?

Solution:

No, $\frac{15}{4} = 3.75$, which is not an integer.

Properties of Divisibility - III

Theorem 4.3.3 Transitivity of Divisibility

For all integers a, b and c, if a divides b and b divides c, then a divides c.

Proof: $\forall a,b,c, \in \mathbb{Z},\ a|b \wedge b|c \rightarrow a|c$

Suppose $a, b,$ and c are *[particular but arbitrarily chosen]* integers such that a divides b and b divides c. *[We must show that a divides c.]*

By definition of divisibility, $b = ar$ and $c = bs$ for some integers r and s.

By substitution

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) \qquad \text{by basic algebra.} \end{aligned}$$

Let $k = rs$. Then k is an integer since it is a product of integers, and therefore $c = ak$ where k is an integer.

Thus a divides c by definition of divisibility. *[This is what was to be shown.]*

Exercise

- For all integers a, b, and c, if a|b and a|c, then a|$(b + c)$ $\forall a,b,c \in \mathbb{Z},\ a|b \wedge a|c \rightarrow a|(b+c)$, aw

  $b = aq_1$
  $c = aq_2$ $(q_1, q_2 \in \mathbb{Z})$
  $b+c = aq_1 + aq_2 = aq_3$ $(q_3 \in \mathbb{Z})$
  $(b+c) = ak$ $(k \in \mathbb{Z})$
  need $\rightarrow \exists k, b+c = ak$ $aq_3 = ak$ ✓

- For all integers a, b, and c, if a divides b then a divides bc.

Counterexamples and Divisibility

To show that a proposed divisibility property is not universally true, you need only find one pair of integers for which it is false.

Is the following statement true or false? For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Proposed Divisibility Property: For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Counterexample: Let $a = 2$ and $b = -2$. Then

$a \mid b$ since $2 \mid (-2)$ and $b \mid a$ since $(-2) \mid 2$, but $a \neq b$ since $2 \neq -2$.

Therefore, the statement is false.

Unique Factorization of Integers Theorem

Theorem 4.3.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \cdots, p_k$, and positive integers $e_1, e_2, \cdots, e_k$ such that

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

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

Because of the unique factorization theorem, any integer $n > 1$ can be put into a standard factored form in which the prime factors are written in ascending order from left to right.

Standard Factored Form

Definition: Standard factored form

Given any integer $n > 1$, the standard factored form of n is an expression of the form

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

where k is a positive integer; $p_1, p_2, \cdots, p_k$ are prime numbers; $e_1, e_2, \cdots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

Example: Write 3,300 integers in standard factored form

Solution: $3{,}300 = 100 \times 33 = 4 \times 25 \times 3 \times 11$

$= 2 \times 2 \times 5 \times 5 \times 3 \times 11$

$= 2^2 \times 3^1 \times 5^2 \times 11$

Test? No!

Exercise

- Write the standard factored form of 396

Exercise

- Find the least positive integer n such that $2^5 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot n$ is a perfect square

need 2^1 for 2^6 → need 3^1 for 3^2 → need 7^1 for 7^4

Example 9 – Using Unique Factorization to Solve a Problem

Suppose m is an integer such that

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

Does $17 \mid m$?

Solution:
Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization of integers theorem).

But 17 does not equal any prime factor of 8, 7, 6, 5, 4, 3, or 2 (because it is too large). Hence 17 must occur as one of the prime factors of m, and so $17 \mid m$.

Chapter 4: Elementary Number Theory and Methods of Proof

4.4 Direct Proof and Counterexample I: Division into Cases and the Quotient-Remainder Theorem

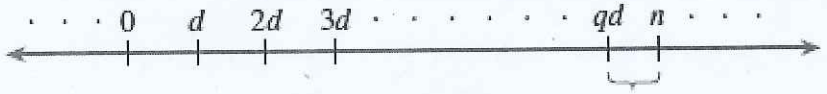
The Quotient-Remainder Theorem

Theorem 4.4.1 The Quotient-Remainder Theorem

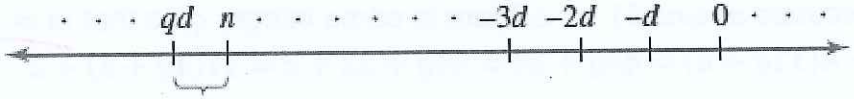
Given any integer n and positive integer d, there exist unique integers q and r such that

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

r = remainder
d = divisor
r is between 0 & d
$0 \leq r < d$



(a) n is positive



(b) n is negative

Example 1 – The Quotient-Remainder Theorem

For each of the following values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

a. $n = 54, d = 4$ **b.** $n = -54, d = 4$ **c.** $n = 54, d = 70$

Solution:

a. $54 = 4 \cdot 13 + 2$; hence $q = 13$ and $r = 2$.

b. $-54 = 4 \cdot (-14) + 2$; hence $q = -14$ and $r = 2$.

c. $54 = 70 \cdot 0 + 54$; hence $q = 0$ and $r = 54$.

Div and Mod

Definition

- Given any integer n and positive integer d,

  $n \; div \; d =$ the integer quotient obtained when n is divided by d,

  $n \; mod \; d =$ the nonnegative integer remainder obtained when n is divided by d.

  to get remainder

- Symbolically, if n and d are integers and $d > 0$, then

  $$n \; div \; d = q \text{ and } n \; mod \; d = r \quad \Leftrightarrow \quad n = dq + r$$

  where q and r are integers and $0 \leq r < d$.

Exercise: Suppose m is an integer. If $m \bmod 11 = 6$, what is $4m \; mod \; 11$?

Solution: Because $m \bmod 11 = 6$, there is some integer q so that $m = 11q + 6$.

Thus, $4m = 4(11q + 6) = 44q + 24 = 44q + 22 + 2 = 11(4q + 2) + 2$.

Since $4q + 2$ is an integer (because products and sums of integers are integers) and since 2<11, the remainder obtained when $4m$ is divided by 11 is 2.

Therefore, $4m \bmod 11 = 2$.

Exercise

$\forall n \in Z,\ n \bmod 5 = 3 \rightarrow n^2 \bmod 5 = 4$

- Prove that for all integers *n*, if *n mod* 5 = 3 then n^2 *mod* 5 = 4.

$n = d \cdot q + r$

$d = 5,\ r = 3$

need $n^2 = 5K + 4$

$n = 5q + 3 \quad (q \in Z)$

$n^2 = (5q+3)^2 = 25q^2 + 30q + 9 = 5(5q^2 + 6q + 1) + 4$

$n^2 = 5(K) + 4$ ✓✓

K ↓ r

- Prove that for all integers m and n, if m mod 5 = 2 and n mod 5 = 1 then mn mod 5 = 2.

Example 6 – Representations of Integers Modulo 4

Show that any integer can be written in one of the four forms

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q.

Solution:

Given any integer n, apply the quotient-remainder theorem to n with $d = 4$. This implies that there exist an integer quotient q and a remainder r such that

$$n = 4q + r \quad \text{and} \quad 0 \leq r < 4.$$

But the only nonnegative remainders r that are less than 4 are 0, 1, 2, and 3. Hence

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q.

Proof by Division into Cases

Method of Proof by Division into Cases

To prove a statement of the form "if A_1 or A_2 or $\cdots$ or A_n, then C," prove all of the following:

If A_1, then C,
If A_2, then C,
$\vdots$
If A_n, then C.

This process shows that C is true regardless of which of $A_1, A_2 \cdots, A_n$ happens to be the case.

The Parity Property

- Parity property: any integer is either even or odd.

Theorem 4.4.2 The Parity Property
Any two consecutive integers have opposite parity.

Proof:
Suppose that two *[particular but arbitrarily chosen]* consecutive integers are given; call them m and $m + 1$. *[We must show that one of m and m + 1 is even and that the other is odd.]* By the parity property, either m is even or m is odd. *[We break the proof into two cases depending on whether m is even or odd.]*

Case I: m is even, $m = 2k$ for some integer k.
It follows that $m + 1 = 2k + 1$.
Thus, $m + 1$ is odd. Therefore, m and $m + 1$ has opposite parity.

Case II: m is odd, so $m = 2k + 1$ for some integer k.
It follows that $m + 1 = 2k + 1 + 1 = 2(k + 1)$.
Thus, $m + 1$ is even. Therefore, m and $m + 1$ has opposite parity.

Hence, in either case, two consecutive integers m and $m + 1$ has opposite parity. *[This is what was to be shown.]*

1 = odd, 2 = even, 3 = odd ... consecutive #'s have opposite parity

Square of an Odd Integer

Theorem 4.4.3
The square of any odd integer has the form $8m + 1$ for some integer m.

Proof:

Suppose *n* is a *[particular but arbitrarily chosen]* odd integer. By the quotient-remainder theorem, *n* can be written in one of the forms

$$4q \quad \text{or} \quad 4q + 1 \quad \text{or} \quad 4q + 2 \quad \text{or} \quad 4q + 3$$

for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms $4q + 1$ or $4q + 3$.

Case 1 ($n = 4q + 1$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q + 1)^2 && \text{by substitution} \\ &= (4q + 1)(4q + 1) && \text{by definition of square} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + q$. Then m is an integer since 2 and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1$$

where m is an integer.

Square of an Odd Integer (cont')

Theorem 4.4.3
The square of any odd integer has the form $8m + 1$ for some integer m.

Proof (cont'):

Case 2 ($n = 4q + 3$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q + 3)^2 && \text{by substitution} \\ &= (4q + 3)(4q + 3) && \text{by definition of square} \\ &= 16q^2 + 24q + 9 \\ &= 8(2q^2 + 3q + 1) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + 3q + 1$. Then m is an integer since 1, 2, 3 and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1$$

where m is an integer.

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer m. *[This is what we needed to show.]*

Exercise

- Use the quotient-remainder theorem with d=3 to prove that the square of any integer has the form 3k or 3k+1 for some integer k.

3 groups
$0 \le r \le d-1$
$r = 0, 1, 2$

$n = dq + r$
$n = 3q + 0 \rightarrow n^2 = 3k$ or $3k+1$
$n = 3q + 1 \rightarrow n^2 = 3k$ or $3k+1$
$n = 3q + 2$

$n = 3q + 1$
$n^2 = 9q^2 + 6q + 1$
$n^2 = 3(3q^2 + 2q) + 1$
k

- The product of any four consecutive integers is divisible by 8.

Absolute Value

Definition:

For any real number x, the absolute value of x, denoted $|x|$, is defined as follows:

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

Lemma 4.4.4: For any real number r, $-|r| \leq r \leq |r|$.

Proof:

Suppose r is any real number.

Case 1 ***($r \geq 0$)***: by definition of absolute value, $|r| = r$. Also, since r is positive and $-|r|$ is negative, $-|r| < r$. Thus it is true that $-|r| \leq r \leq |r|$.

Case 2 ***($r < 0$)***: by definition of absolute value, $|r| = -r$. Multiplying both sides by −1 gives that $-|r| = r$. Also, since r is negative and $|r|$ is positive, $r < |r|$. Thus it is also true in this case that $-|r| \leq r \leq |r|$.

Hence, in either case, $-|r| \leq r \leq |r|$ *[as was to be shown]*.

Lemma 4.4.5

For any real number r, $|-r| = |r|$

Triangle Inequality

Theorem 4.4.6 The Triangle Inequality
For all real number x and y, $|x + y| \leq |x| + |y|$

Proof:

Suppose x and y are any real numbers.

Case 1 ***($x + y \geq 0$)***: in this case, $|x + y| = x + y$.

x and y are any real number, so by Lemma 4.4.4, $x \leq |x|$ and $y \leq |y|$.

Hence, by Theorem T26, $|x + y| = x + y \leq |x| + |y|$

Case 2 ***($x + y < 0$)***: in this case, $|x + y| = -(x + y) = (-x) + (-y)$.

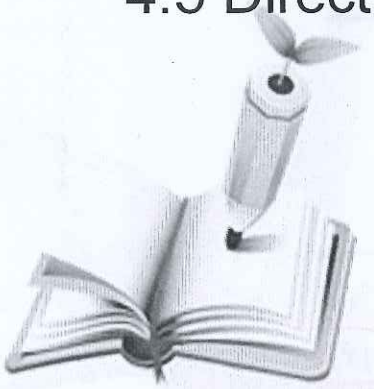
x and y are any real number, so by Lemma 4.4.4 and 4.4.5, $-x \leq |-x| = |x|$ and $-y \leq |-y| = |y|$.

It follows by Theorem T26, $|x + y| = (-x) + (-y) \leq |x| + |y|$

Hence, in either case, $|x + y| \leq |x| + |y|$ *[as was to be shown]*.

Chapter 4: Elementary Number Theory and Methods of Proof

4.5 Direct Proof and Counterexample IV: Floor and Ceiling



Computing Floors and Ceilings

Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the following values of x:

$X = -2.01$

a. 25/4 b. 0.999 c. -2.01 $= -3 \leq X < -2$

Solution: $-\infty$ ——— ∞

a. $25/4 = 6.25$ and $6 < 6.25 < 7$; hence $\lfloor 25/4 \rfloor = 6$ and $\lceil 25/4 \rceil = 7$.

b. $0 < 0.999 < 1$; hence $\lfloor 0.999 \rfloor = 0$ and $\lceil 0.999 \rceil = 1$.

c. $-3 < -2.01 < -2$; hence $\lfloor -2.01 \rfloor = -3$ and $\lceil -2.01 \rceil = -2$.

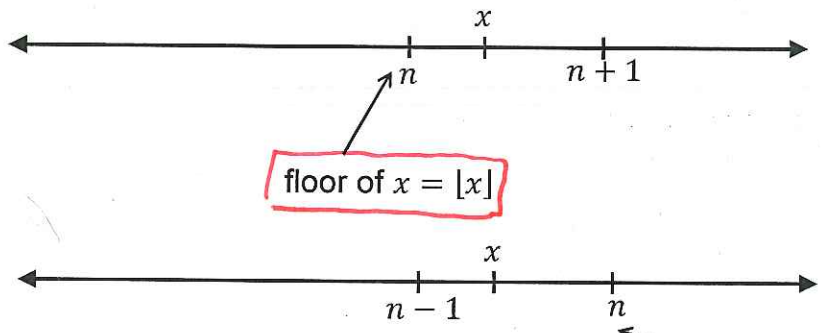
$\lfloor\ \rfloor$ = floor , $\lfloor x \rfloor$ = floor of x

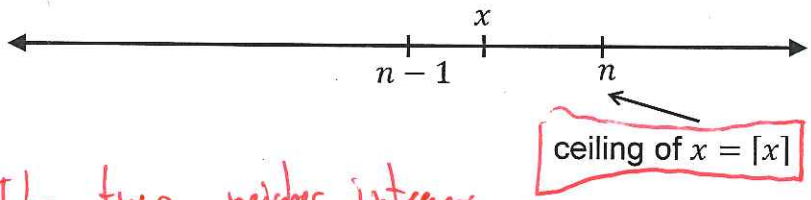
$\lceil\ \rceil$ = ceiling

Floor & Ceiling

Definition:

- Floor: If x is a real number and n is an integer, then
$$\lfloor x \rfloor = n \iff n \leq x < n+1$$
- Ceiling: if x is a real number and n is an integer, then
$$\lceil x \rceil = n \iff n-1 < x \leq n$$





The two neighbor integers of x

Exercise

If k is an integer, what are $\lfloor k \rfloor$ and $\lfloor k+1/2 \rfloor$?

Solution:

k is an integer and $k \leq k < k+1$, thus $\lfloor k \rfloor = k$.

k is an integer and $k \leq k + \frac{1}{2} < k+1$, thus $\left\lfloor k + \frac{1}{2} \right\rfloor = k$.

What are $\lceil k \rceil$ and $\lceil k + 1/2 \rceil$?

Solution:

k is an integer and $k - 1 < k \leq k$, thus $\lceil k \rceil = k$.

k is an integer and $k < k + \frac{1}{2} \leq k+1$, thus $\lceil k + 1/2 \rceil = k+1$.

Exercise

Is the following statement true or false?

"for all real numbers x and y, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$"

Ex: $\lfloor x \rfloor = m$

$\lfloor -x \rfloor = ?$ def: $\lfloor x \rfloor$ is $m \leq x < m+1$

$-1 \cdot [m \leq -x < m+1]$

$-m \geq x > -m-1$

$-m-1 < x \leq -m$

$\therefore \lfloor -x \rfloor = -m-1$

Floor Properties

Theorem 4.5.1

For all real numbers x and all integers m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$

Proof:

Suppose x is a [particular but arbitrarily chosen] real number and m is an [particular but arbitrarily chosen] integer.

[We must show that $\lfloor x + m \rfloor = x + m$.]

Let $n = \lfloor x \rfloor$. By definition of floor, n is an integer and

$$n \leq x < n + 1.$$

Add m to all three parts to obtain

$$n + m \leq x + m < n + m + 1$$

[since adding a number to both sides of an inequality does not change the direction of the inequality].

$n + m$ is an integer *[since n and m are integers and a sum of integers is an integer]*.

So, by definition of floor, the left-hand side of the equation to be shown is

$$\lfloor x + m \rfloor = n + m$$
$$= \lfloor x \rfloor + m \quad \text{by substitution of } n = \lfloor x \rfloor.$$

Thus $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ [as was to be shown.]

The Floor of $n/2$

Theorem 4.5.2 The Floor of n/2

For all integer n,

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

Proof:

Suppose n is a *[particular but arbitrarily chosen]* integer.

By the quotient-remainder theorem, either n is odd or n is even.

Case 1 (n is even):

In this case, $n = 2k$ for some integer k. *[We must show that* $\lfloor n/2 \rfloor = n/2$*.]*.

By dividing 2 to both sides, $n/2 = k$.

$\lfloor k \rfloor = k$ because k is an integer and $k \leq k < k + 1$.

Thus, by substituition $k = n/2$, $\lfloor n/2 \rfloor = k$ [as was to be shown.]

The Floor of $n/2$ (cont')

Proof (con't):

Case 2 (n is odd): In this case, $n = 2k + 1$ for some integer k. *[We must show that* $\lfloor n/2 \rfloor = (n-1)/2$*.]*.

By substitution $n = 2k + 1$ into the left-hand side of the equation to be shown is,

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

Because k is an integer and $\mathrm{k} \leq k + \frac{1}{2} < k + 1$.

By substitution $n = 2k + 1$ into the right-hand side of the equation to be shown is

$$\frac{n-1}{2} = \frac{2k+1-1}{2} = \frac{2k}{2} = k$$

Since both the left-hand and righ-hand sides equal k, they are equal to each other.

That is $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$ [as was to be shown.]

Exercise

- For all real numbers x, if $x - \lfloor x \rfloor < 1/2$ then $\lfloor 2x \rfloor = 2\lfloor x \rfloor$.
- For any odd integer *n*, $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$
- For any odd integer *n*, $\left\lceil \frac{n^2}{4} \right\rceil = \frac{n^2+3}{4}$

Floor Property

Theorem 4.5.3

If n is any integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d\lfloor n/d \rfloor$, then

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

Proof:

Suppose n is any integer, d is a positive integer, $q = \lfloor n/d \rfloor$ and $r = n - d\lfloor n/d \rfloor$. [*We must show that* $n = dq + r$ and $0 \leq r < d$]

By substitution,

$$dq + r = d\left\lfloor \frac{n}{d} \right\rfloor + n - d\left\lfloor \frac{n}{d} \right\rfloor = n$$

So it remains only to show that $0 \leq r < d$.

Since $q = \lfloor n/d \rfloor$, by the definition of floor, we have $q \leq \frac{n}{d} < q + 1$

Then,

$dq \leq n < dq + d$ by multiplying all parts by d

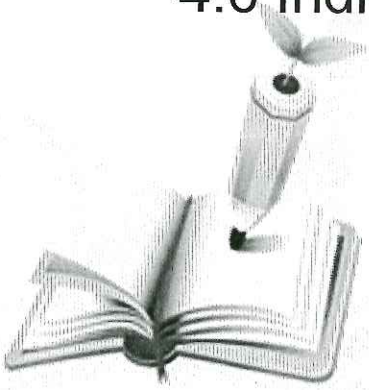
So, $0 \leq n - dq < d$ by subtracting dq from all parts

But $r = n - d\left\lfloor \frac{n}{d} \right\rfloor = n - dq$

Hence, by substitution we obtain $0 \leq r < d$ [*This is what was to be shown*].

Chapter 4: Elementary Number Theory and Methods of Proof

4.6 Indirect Argument: Contradiction and Contraposition



Direct vs. Indirect Proof

- Direct proofs:
  - begin with the premises,
  - continue with a sequence of deductions,
  - end with the conclusion.

- Indirect proof: proofs of theorems that do not start with the premises and end with the conclusion, are called indirect proofs.
  - Proof by contradiction
  - Proof by contraposition

Ex: $even(n^2) \rightarrow even(n)$

$\equiv$ $odd(n) \rightarrow odd(n^2)$

easy

Proof by Contradiction

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Proof by Contradiction - Exercise

Theorem 4.6.1

There is no greatest integer.

Proof:

[We take the negation of the theorem and suppose it to be true.]

Suppose there is a greatest integer N. Then $N \geq n$ for every integer n.

[We must deduce a contradiction.]

Let $M = N + 1$. Now M is an integer since it is a sum of integers. Also $M > N$ since $M = N + 1$. Thus M is an integer that is greater than N.

So N is the greatest integer and N is not the greatest integer, which is a contradiction. *[This contradiction shows that the supposition is false and, hence, that the theorem is true.]*

Proof by Contradiction - Exercise

Theorem 4.6.2

There is no integer that is both even and odd.

Proof:

[We take the negation of the theorem and suppose it to be true.]

Suppose there is at least one integer n that is both even and odd. *[We must deduce a contradiction.]*

By definition of even, $n = 2a$ for some integer a, and by definition of odd, $n = 2b + 1$ for some integer b.

Consequently,

$2a = 2b + 1$ by equating the two expressions for n

and so $a - b = 1/2$ by algebra.

Since a and b are integers, the difference $a - b$ must also be an integer. But $a - b = 1/2$, and 1/2 is not an integer.

Thus $a - b$ is an integer and $a - b$ is not an integer, which is a contradiction. *[This contradiction shows that the supposition is false and, hence, that the theorem is true.]*

Proof by Contradiction - Exercise

Theorem 4.6.3

The sum of any rational number and any irrational number is irrational.

r is rational and s is rational → r + s is irrational

Starting Point:

Suppose there is a rational number r and a irrational number s such that $r + s$ is rational.

To show:

this supposition leads to a contradiction.

Proof by Contradiction - Exercise

Theorem 4.6.3

The sum of any rational number and any irrational number is irrational.

Proof:

[We take the negation of the theorem and suppose it to be true.]

Suppose not. That is, there is a rational number r and an irrational number s such that $r + s$ is rational. *[We must deduce a contradiction.]*

By definition of rational, $r = a/b$ and $r + s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. By substitution,

$$\frac{a}{b} + s = \frac{c}{d}$$

And so,

$s = \frac{c}{d} - \frac{a}{b}$ by subtracting a/b from both sides

$= \frac{bc-ad}{bd}$ by the law of algebra $= \frac{\text{integ}}{\text{integ}} = \text{rational}$

Now $bc - ad$ and bd are both integers *[since a, b, c, and d are integers and since products and differences of integers are integers]*, and $bd \neq 0$ *[by the zero product property]*. Hence s is a quotient of the two integers $bc - ad$ and bd with $bd \neq 0$.

Thus, by definition of rational, s is rational, which contradicts the supposition that s is irrational. *[Hence the supposition is false and the theorem is true.]*

Exercise

- If a and b are rational numbers, $b = 0$, and r is an irrational number, then $a + br$ is irrational.

- For all integers a, if $a \bmod 6 = 3$, then $a \bmod 3 \neq 2$.

$\sim(a \bmod 6 = 3 \rightarrow a \bmod 3 \neq 2)$

$a \bmod 6 = 3 \wedge a \bmod 3 = 2$

$a = 6q + 3 \wedge a = 3k + 2 \quad (q, k \in \mathbb{Z})$

$6q + 3 = 3k + 2 \Rightarrow 6q - 3k = -1$

$3(2q - k) = -1 \Rightarrow 2q - k = -\frac{1}{3}$

not integer $\therefore$ contradiction

Proof by Contraposition

- Proof by Contraposition is based on the logical equivalence between a statement and its contraposition

$$(p \rightarrow q) \equiv (\sim q \rightarrow \sim p)$$

- To prove a statement $p \rightarrow q$ by contraposition
  - Start with the contrapositive of the statement (assume $\sim q$ is true),
  - Prove the contrapositive by a contraposition, $\sim q \rightarrow \sim p$
  - Conclude that the original statement is true
- Proof by Contraposition is a direct proof of the contrapositive statement !

Method of Proof by Contraposition

1. Express the statement to be proved in the form

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

2. Rewrite this statement in the contrapositive form

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

3. Prove the contrapositive by a 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.

Proof by Contraposition- Exercise

Theorem 4.6.4

For all integers n, if n^2 is even then n is even.

- Contraposition:

  For all integers n, if n is not even then n^2 is not even.

or

For all integers n, if n is odd then n^2 is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1$ by substitution

$n^2 = 2(2k^2 + 2k) + 1$ by algebra

$2k^2 + 2k$ = integer

$n^2 = 2(\text{integer}) + 1$

$\therefore n^2 = \text{odd}$

Proof by Contraposition- Exercise

Theorem 4.6.4

For all integers n, if n^2 is even then n is even.

Proof (by contraposition):

Suppose n is any odd integer. *[We must show that n^2 is odd.]*

By definition of odd, $n = 2k + 1$ for some integer k.

By substitution and algebra,

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

But $2k^2 + 2k$ is an integer because products and sums of integers are integers. Let $t = 2k^2 + 2k$, then $n^2 = 2t + 1$.

Thus, by definition of odd, n^2 is odd *[as was to be shown]*.

Exercise

- For all real numbers r, if r^2 is irrational then r is irrational.

- For all integers m and n, if mn is even then m is even or n is even.

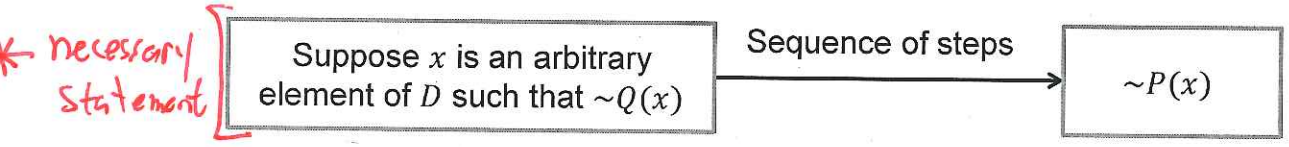
Relations between Proof by Contradiction and Proof by Contraposition

- To prove a statement

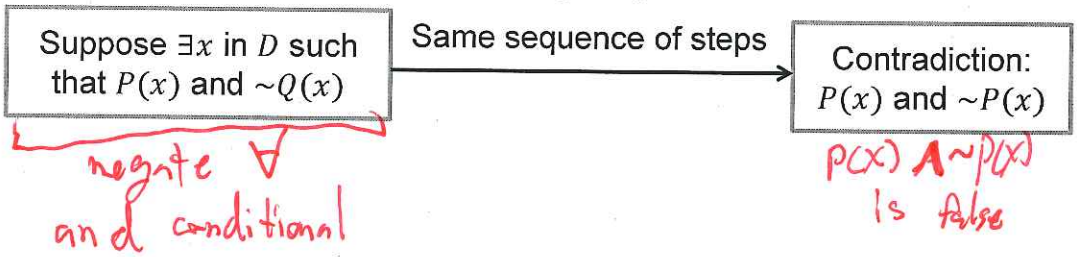
  $\forall x$ in D, if $P(x)$ then $Q(x)$ $\equiv$ $P(x) \to Q(x)$

- Proof by contraposition proves the statement by giving a direct proof of the equivalent statement

  $\forall x$ in D, if $Q(x)$ is false then $P(x)$ is false



- Proof by contradiction proves the statement by showing that the negation of the statement leads logically to a contradiction.



Direct Proof, Contradiction & Contraposition

- Universal statements:

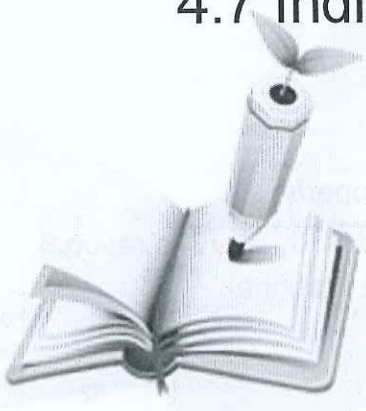
$$\forall x \in D, \text{if } P(x) \text{ then } Q(x)$$

use this for universal conditionals

Direct Proof	Contradiction	Contraposition
Suppose x is an arbitrary element of D such that $P(x)$	Suppose $\exists x \in D$, such that $P(x) \wedge \sim Q(x)$	Suppose x is an arbitrary element of D such that $\sim Q(x)$
Reasoning	Reasoning	Reasoning
$Q(x)$	Contradiction: $P(x)$ and $\sim P(x)$	$\sim P(x)$

Chapter 4: Elementary Number Theory and Methods of Proof

4.7 Indirect Argument: Two Classical Theorems



The Irrationality of $\sqrt{2}$

Proof by contradiction:

Starting point:

Negation: $\sqrt{2}$ is rational.

To show:

A contradiction.

$\sqrt{2} = \frac{m}{n}$, where m and n *are integers* with no common factors and $n \neq 0$, by definition of rational.

$m^2 = 2n^2$, by squaring and multiplying both sides with n^2

m^2 is even, then m is even. Let $m = 2k$ for some integer k.

$(2k)^2 = 4k^2 = 2n^2$, by substituting $m = 2k$ into $m^2 = 2n^2$.

n^2 is even, and so n is even.

Hence both m and n have a common factor of 2.

Irrationality of $1 + 3\sqrt{2}$

Proof by contradiction:

Suppose $1 + 3\sqrt{2}$ is rational. By definition of rational,

$$1 + 3\sqrt{2} = \frac{a}{b} \text{ for some integers } a \text{ and } b \text{ with } b \neq 0.$$

It follows that

$3\sqrt{2} = \frac{a}{b} - 1$ by subtracting 1 from both sides

$= \frac{a}{b} - \frac{b}{b}$ by substitution

$= \frac{a-b}{b}$ by the rule for subtracting fractions with a common denominator

Hence, $\sqrt{2} = \frac{a-b}{3b}$ by dividing both sides by 3.

$a - b$ and $3b$ are integers and $3b \neq 0$ by the zero product property.

Hence $\sqrt{2}$ is quotient of the two integers $a - b$ and $3b$ with $3b \neq 0$, so $\sqrt{2}$ is rational by the definition of rational. This contradicts the fact that $\sqrt{2}$ is irrational.

Exercise

Prove that for all integers n, if n^2 is divisible by 5, then n is divisible by 5.

Hint:

n^2 is divisible by 5 $\Rightarrow n^2 = 5k$ for some integer k.

Proof by contradiction:

n is not divisible by 5 $\Rightarrow n = 5q + r$ for some integers q and r with $0 < r < 5$ $(r = 1, 2, 3, 4)$.

$$n^2 = (5q + r)^2 = 25q^2 + 10qr + r^2$$

Case 1 (r=1): $n^2 = 5(5q^2 + 2q) + 1 \Rightarrow 5 \nmid n^2$

Case 2 (r=2): $n^2 = 5(5q^2 + 4q) + 4 \Rightarrow 5 \nmid n^2$

Case 3 (r=3): $n^2 = 5(5q^2 + 6q) + 9 = 5(5q^2 + 6q + 1) + 4 \Rightarrow 5 \nmid n^2$

Case 4 (r=4): $n^2 = 5(5q^2 + 8q) + 16 = 5(5q^2 + 6q + 3) + 1 \Rightarrow 5 \nmid n^2$

Conclusion: ????$\Rightarrow n$ is divisible by 5.

Contrapos: if $5 \nmid n \rightarrow 5 \nmid n^2$

$n \neq 5q + r$ $(1 < r < 4, q \in \mathbb{Z})$

$n^2 = 25q^2 + 10q + 1 =$ [illegible]

$5(5q^2 + 2q + 1) = 5(5q^2 + 2q) + 1 \therefore 5 \nmid n^2$

Exercise

Prove that $\sqrt{5}$ is irrational.

Hint: Proof by contradiction.

$\sqrt{5}$ is rational $\Rightarrow \sqrt{5} = \frac{a}{b}$ for some integers a and b with $b \neq 0$ and a and b have no common factor.

$\sqrt{5} = \frac{a}{b} \Rightarrow a^2 = 5b^2 \Rightarrow a^2$ is divisible by 5 $\Rightarrow$ a is divisible by 5 by last problem

$\Rightarrow a = 5k$ for some integer k.

$a^2 = 5b^2 \Rightarrow (5k)^2 = 5b^2 \Rightarrow 25k^2 = 5b^2 \Rightarrow b^2 = 5k^2 \Rightarrow b^2$ is divisible by 5$\Rightarrow b$ is divisible by 5.

Therefore, a and b have a common factor 5, which is contradict with a and b have no common factor.

Property of a Prime Divisor

Proposition 4.7.3

For any integer a and any prime number p, if $p|a$ then $p \nmid (a+1)$

If a prime number divides an integer, then it does not divide the next successive integer.

Starting point: there exists an integer a and a prime number p such that $p \mid a$ and $p \mid (a+1)$.

To show: a contradiction.

$a = pr$ and $a + 1 = ps$ for some integers r and s by definition of divisibility.

It follows that

$$1 = (a+1) - a = ps - pr = p(s-r),$$

$(s-r) = 1/p$, by dividing both sides with p.

$p > 1$ because p is prime, hence, $1/p$ is not an integer, thus $s-r$ is not an integer, which is a contradict $s-r$ is an integer since r and s are integers.

if n and d are integers and $d \neq 0$:

$d|n \quad \Leftrightarrow \quad \exists$ an integer k such that $n = d \cdot k$

4.8 Greatest Common Divisor (GCD)

- The greatest common divisor of two integers *a* and *b* is the largest integer that divides both a and b.

Definition

Let a and b be integers that are not both zero. The **greatest common divisor** of a and b, denoted **gcd(a, b)**, is that integer d with the following properties:

1. d is common divisor of both a and b, in other words,
   $d \mid a$, and $d \mid b$.
2. For all integers c, if c is a common divisor of both a and b, then c is less than or equal to d. In other words,
   for all integers c, if $c \mid a$, and $c \mid b$, then $c \leq d$.

Exercise:

- $\gcd(72,63) = 9$, since $72 = 9 \cdot 8$ and $63 = 9 \cdot 7$
- $\gcd(10^{20}, 6^{30}) = 2^{20}$, since $10^{20} = 2^{20} \cdot 5^{20}$ and $6^{30} = 2^{30} \cdot 3^{30}$

Greatest Common Divisor (GCD)

Lemma 4.8.1
If r is a positive integer, then $\gcd(r, 0) = r$.

Proof:

Suppose r is a positive integer. *[We must show that the greatest common divisor of both r and 0 is r.]*

1. r is a common divisor of both r and 0 because r divides itself and also r divides 0 (since every positive integer divides 0).
2. No integer larger than r can be a common divisor of r and 0 (since no integer larger than r can divide r).

Hence r is the greatest common divisor of r and 0.

Greatest Common Divisor (GCD)

Lemma 4.8.2
If a and b are any integers not both zero, and if q and r are any integers such that $a = bq + r$, then

$$\gcd(a, b) = \gcd(\boldsymbol{b}, r)$$

Proof:

[The proof is divided into two sections: (1) proof that $\gcd(a, b) \leq \gcd(b, r)$, and (2) proof that $\gcd(b, r) \leq \gcd(a, b)$. Since each gcd *is less than or equal to the other, the two must be equal.]*

1. $\gcd(\boldsymbol{a}, \boldsymbol{b}) \leq \gcd(\boldsymbol{b}, \boldsymbol{r})$:

a. *[We will first show that any common divisor of a and b is also a common divisor of b and r.]*

Let a and b be integers, not both zero, and let c be a common divisor of a and b. Then $c \mid a$ and $c \mid b$, and so, by definition of divisibility, $a = nc$ and $b = mc$, for some integers n and m. Now substitute into the equation

$$a = bq + r$$

to obtain

$$nc = (mc)q + r.$$

Greatest Common Divisor (GCD)

Lemma 4.8.2
If a and b are any integers not both zero, and if q and r are any integers such that $a = bq + r$, then

$$\gcd(a, b) = \gcd(\boldsymbol{b}, r)$$

Proof (cont'):

1. $\gcd(\boldsymbol{a}, \boldsymbol{b}) \leq \gcd(\boldsymbol{b}, \boldsymbol{r})$**:**

a. *[We will first show that any common divisor of a and b is also a common divisor of b and r.]*

$$nc = (mc)q + r.$$

Then solve for r :

$$r = nc - (mc)q = (n - mq)c.$$

But $n - mq$ is an integer, and so, by definition of divisibility, $c \mid r$. Because we already know that $c \mid b$, we can conclude that c is a common divisor of b and r *[as was to be shown]*.

Greatest Common Divisor (GCD)

Lemma 4.8.2
If a and b are any integers not both zero, and if q and r are any integers such that $a = bq + r$, then

$$\gcd(a, b) = \gcd(\boldsymbol{b}, r)$$

Proof (cont'):

1. $\gcd(\boldsymbol{a}, \boldsymbol{b}) \leq \gcd(\boldsymbol{b}, \boldsymbol{r})$**:**

b. *[Next we show that* $\gcd(a, b) \leq \gcd(b, r)$*.]*
By part (a), every common divisor of a and b is a common divisor of b and r . It follows that the greatest common divisor of a and b is defined because a and b are not both zero, and it is a common divisor of b and r . But then $\gcd(a, b)$ (being one of the common divisors of b and r) is less than or equal to the greatest common divisor of b and r :

$$\gcd(a, b) \leq \gcd(b, r).$$

2. $\gcd(\boldsymbol{b}, \boldsymbol{r}) \leq \gcd(\boldsymbol{a}, \boldsymbol{b})$**:**

The second part of the proof is very similar to the first part. It is left as an exercise.

The Euclidean Algorithm

- Problem:
  - Given two integer A and B with $A > B \geq 0$, find $\gcd(A, B)$
- Idea:
  - The Euclidean Algorithm uses the division algorithm repeatedly.
  - If B=0, by Lemma 4.8.1 we know $\gcd(A, B) = A$.
  - If B>0, division algorithm can be used to calculate a quotient q and a remainder r:

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

  - By Lemma 4.8.2, we have $\gcd(A, B) = \gcd(B, r)$, where B and r are smaller numbers than A and B.
- $\gcd(A, B) = \gcd(B, r) = \cdots = \gcd(x, 0) = x$

$r = A \bmod B$

* Test Qstion

The Euclidean Algorithm - Exercise

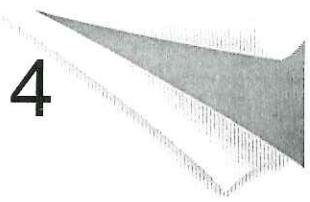
Use the Euclidean algorithm to find gcd(330, 156).

Solution:

gcd(330,156) = gcd(156, 18) 330 mod 156 = 18
= gcd(18, 12) 156 mod 18 = 12
= gcd(12, 6) 18 mod 12 = 6
= gcd(6, 0) 12 mod 6 = 0
= 6

Use the Euclidean algorithm to find gcd(1,001, 871).

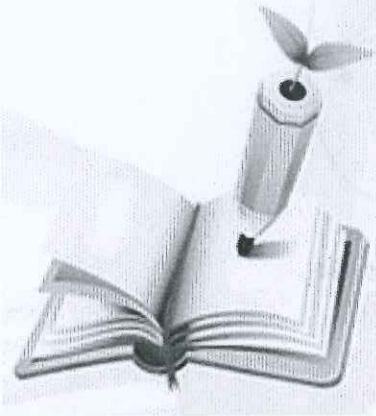
Summary of Chapter 4



- Number theories:
  - Even, odd, prime, and composite
  - Rational, divisibility, and quotient-remainder theorem
  - Floor and ceiling
  - The irrationality of $\sqrt{2}$ and gcd
- Proofs:
  - Direct proof and counterexample
  - Indirect proof by contradiction and contraposition

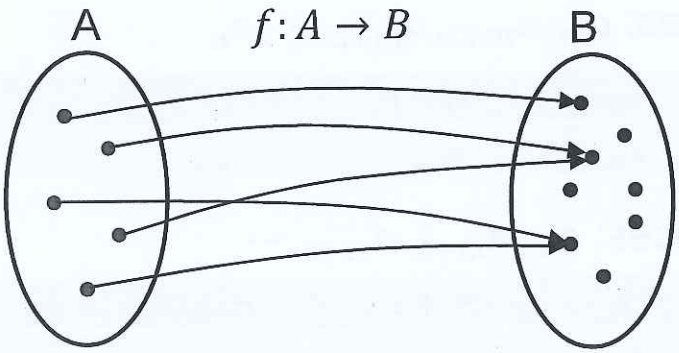
Chapter 5: Sequences, Mathematical Induction and Recursion

5.1 Sequences



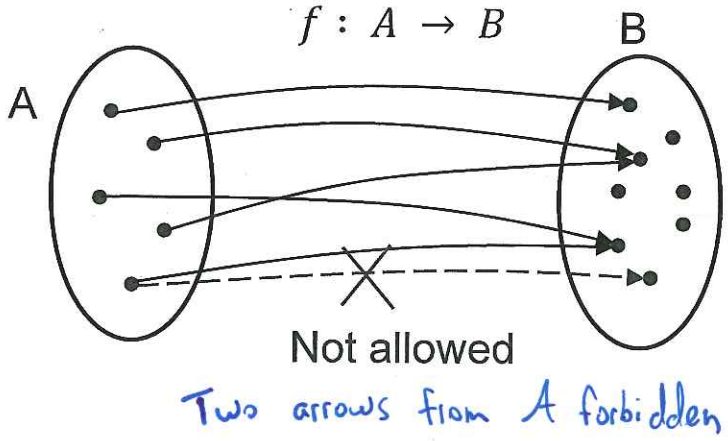
Functions

The Function $f : A \to B$ assigns exactly one element of B to each element of A.



Functions

The Function $f : A \to B$ assigns exactly one element of B to each element of A.



Sequences

Definition
- A sequence is a function.
- Domain is either all the integers between two given integers or all the integers greater than or equal to a given integer.

Finite sequences: $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$

Domain	m	$m+1$	$m+2$	$\cdots$	n
Codomain	a_m	a_{m+1}	a_{m+2}	$\cdots$	a_n

Infinite sequences: $a_m, a_{m+1}, a_{m+2}, \cdots$

Domain	m	$m+1$	$m+2$	$\cdots$	
Codomain	a_m	a_{m+1}	a_{m+2}	$\cdots$	

a_k (read "a sub k") is called a **term**.
k in a_k is called a **subscript** or **index.**

Initial term: a_m
Final term: a_n

Sequence Example 1

Finding Terms of Sequences Given by Explicit Formulas

Define sequences $a_1, a_2, a_3, \ldots$ and $b_2, b_3, b_4, \ldots$ by the following explicit formulas:

$$a_k = \frac{k}{k+1} \quad \text{for all integers } k \geq 1,$$

$$b_i = \frac{i-1}{i} \quad \text{for all integers } i \geq 2.$$

Compute the first five terms of both sequences.

Solution:

$a_1 = \frac{1}{1+1} = \frac{1}{2}$, $a_2 = \frac{2}{2+1} = \frac{2}{3}$, $a_3 = \frac{3}{3+1} = \frac{3}{4}$, $a_4 = \frac{4}{4+1} = \frac{4}{5}$, $a_5 = \frac{5}{5+1} = \frac{5}{6}$ ✓

$b_2 = \frac{2-1}{2} = \frac{1}{2}$, $b_3 = \frac{3-1}{3} = \frac{2}{3}$, $b_4 = \frac{4-1}{4} = \frac{3}{4}$, $b_5 = \frac{5-1}{5} = \frac{4}{5}$, $b_6 = \frac{6-1}{6} = \frac{5}{6}$ ✓ same

Note: all terms of both sequences are identical.

Sequence Example 2

Finding an Explicit Formulas to Fit Given Initial Terms

Find an explicit formula for a sequence that has the following initial terms:

$$1, -\frac{1}{4}, \frac{1}{9}, -\frac{1}{16}, \frac{1}{25}, -\frac{1}{36}, \ldots$$

Solution: index: 1 2 3 4 5 6

- Denote the general term of the sequence by a_k and suppose the first term is a_1.

$$a_1 = \frac{1}{1^2}, a_2 = (-1)\frac{1}{2^2}, a_3 = \frac{1}{3^2}, a_4 = (-1)\frac{1}{4^2}, a_5 = \frac{1}{5^2}, a_6 = (-1)\frac{1}{6^2}$$

- An explicit formulator that gives the correct first six terms is:

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

Summation Notation

Given a sequence $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$,

Domain	m	$m+1$	$m+2$	$\cdots$	n
Codomain	a_m	a_{m+1}	a_{m+2}	$\cdots$	a_n

The summation from k equals m to n of a-sub-k:

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

Summation notation — Expanded form

k: the index of the summation
m: the lower limit of the summation
n: the upper limit of the summation

$\sum_{k=m}^{n} a_k$

Summation Example

– Computing Summations

Let $a_1 = -2, a_2 = -1, a_3 = 0, a_4 = 1$, and $a_5 = 2$.
Compute the following:

a. $\sum_{k=1}^{5} a_k$

$$\sum_{k=1}^{5} a_k = a_1 + a_2 + a_3 + a_4 + a_5 = (-2) + (-1) + 0 + 1 + 2 = 0$$

b. $\sum_{k=2}^{2} a_k$

$$\sum_{k=2}^{2} a_k = a_2 = -1$$

c. $\sum_{k=1}^{2} a_{2k}$

$$\sum_{k=1}^{2} a_{2k} = a_2 + a_4 = (-1) + 1 = 0$$

Summation Example

– Changing from Summation Notation to Expanded Form

Write the following summation in expanded form:

$$\sum_{i=0}^{n} \frac{(-1)^i}{i+1}.$$

Solution:

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

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

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

Summation Example

– Changing from Expanded Form to Summation Notation

Express the following using summation notation:

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n}.$$

$\sum_{i=1}^{n+1} a_i = \frac{i}{n+i-1}$

Solution:

The general term of this summation can be expressed as $\frac{k+1}{n+k}$ for integers k from 0 to n.

Hence

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n} = \sum_{k=0}^{n} \frac{k+1}{n+k}.$$

Summation Notation - Recursive Definition

If m is any integer and $m < n$, then

$$\sum_{k=m}^{m} a_k = a_m$$

$$\sum_{k=m}^{m+1} a_k = \sum_{k=m}^{m} a_k + a_{m+1}$$

$$\sum_{k=m}^{m+2} a_k = \sum_{k=m}^{m+1} a_k + a_{m+2}$$

$$\cdots$$

$$\sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n$$

Recursive definition is useful to rewrite a summation,

- by separating off the final term of a summation
- by adding a final term to a summation.

Recursive Definition Example

– Separating Off a Final Term and Adding On a Final Term

a. Rewrite $\sum_{i=1}^{n+1} \frac{1}{i^2}$ by separating off the final term.

b. Write $\sum_{k=0}^{n} 2^k + 2^{n+1}$ as a single summation.

Solution:

a. $$\sum_{i=1}^{n+1} \frac{1}{i^2} = \sum_{i=1}^{n} \frac{1}{i^2} + \frac{1}{(n+1)^2}$$

b. $$\sum_{k=0}^{n} 2^k + 2^{n+1} = \sum_{k=0}^{n+1} 2^k$$

Summation Notation - A Telescoping Sum

- In certain sums each term is a difference of two quantities.

For example: $a_k = \frac{1}{k} - \frac{1}{k+1}, k = m, \cdots, n$

- When you write such sums in expanded form, you sometimes see that all the terms cancel except the first and the last.

$$a_k + a_{k+1} + a_{k+2} = \left(\frac{1}{k} - \frac{1}{k+1}\right) + \left(\frac{1}{k+1} - \frac{1}{k+2}\right) + \left(\frac{1}{k+2} - \frac{1}{k+3}\right)$$

- Successive cancellation of terms collapses the sum like a telescope.

A Telescoping Sum Example

Some sums can be transformed into telescoping sums, which then can be rewritten as a simple expression.

For instance, observe that

$$\frac{1}{k} - \frac{1}{k+1} = \frac{(k+1)-k}{k(k+1)} = \frac{1}{k(k+1)}.$$

Use this identity to find a simple expression for $\sum_{k=1}^{n} \frac{1}{k(k+1)}$.

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right)$$

$$= \left(\frac{1}{1} - \cancel{\frac{1}{2}}\right) + \left(\cancel{\frac{1}{2}} - \cancel{\frac{1}{3}}\right) + \left(\cancel{\frac{1}{3}} - \cancel{\frac{1}{4}}\right) + \cdots + \left(\cancel{\frac{1}{n-1}} - \cancel{\frac{1}{n}}\right) + \left(\cancel{\frac{1}{n}} - \frac{1}{n+1}\right)$$

$$= 1 - \frac{1}{n+1}.$$

Product Notation

Symbol = Π

Given a sequence $a_m, a_{m+1}, a_{m+2}, \cdots, a_n,$

Domain	m	$m+1$	$m+2$	$\cdots$	n
Codomain	a_m	a_{m+1}	a_{m+2}	$\cdots$	a_n

The product from k equals m to n of a-sub-k:

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

A recursive definition for the product notation is the following:
If m is any integer, then

$$\prod_{k=m}^{m} a_k = a_m \quad \text{and} \quad \prod_{k=m}^{n} a_k = \left(\prod_{k=m}^{n-1} a_k\right) \cdot a_n \quad \text{for all integers } n > m.$$

Product Notation Example – Computing Products

Compute the following products:

a. $\prod_{k=1}^{5} k$

b. $\prod_{k=1}^{1} \frac{k}{k+1}$

Solution:

a. $\prod_{k=1}^{5} k = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$

b. $\prod_{k=1}^{1} \frac{k}{k+1} = \frac{1}{1+1} = \frac{1}{2}$

Properties of Summations and Products

Theorem 5.1.1

If $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2}, \ldots$ are sequences of real numbers and c is any real number, then the following equations hold for any integer $n \geq m$:

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$ need same indexes

2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$ generalized distributive law

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

Properties of Summation & Product Exercise

Let $a_k = k + 1$ and $b_k = k - 1$ for all integers k. Write each of the following expressions as a single summation or product:

a. $\sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k$

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

Properties of Summation & Product Exercise

Solution:

a.

$$\sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (k+1) + 2 \cdot \sum_{k=m}^{n} (k-1) \qquad \text{by substitution}$$

$$= \sum_{k=m}^{n} (k+1) + \sum_{k=m}^{n} 2 \cdot (k-1) \qquad \text{by Theorem 5.1.1 (2)}$$

$$= \sum_{k=m}^{n} ((k+1) + 2 \cdot (k-1)) \qquad \text{by Theorem 5.1.1 (1)}$$

$$= \sum_{k=m}^{n} (3k-1) \qquad \text{by algebraic simplification}$$

Properties of Summation & Product Exercise

Solution:

b.

$$\left(\prod_{k=m}^{n} a_k \right) \cdot \left(\prod_{k=m}^{n} b_k \right) = \left(\prod_{k=m}^{n} (k+1) \right) \cdot \left(\prod_{k=m}^{n} (k-1) \right) \qquad \text{by substitution}$$

$$= \prod_{k=m}^{n} (k+1) \cdot (k-1) \qquad \text{by Theorem 5.1.1 (3)}$$

$$= \prod_{k=m}^{n} (k^2 - 1) \qquad \text{by algebraic simplification}$$

Change of Variable

- The index symbol in a summation or product is internal to summation or product.
- The index symbol can be replaced by any other symbol as long as the replacement is made in each location where the symbol occurs.

$$\sum_{i=m}^{n} a_i = \sum_{j=m}^{n} a_j \quad \text{and} \quad \prod_{i=m}^{n} a_i = \prod_{j=m}^{n} a_j$$

- As a consequence, the index of a summation or a product is called a dummy variable. a_k or a_i or a_j
- A **dummy variable** is a symbol that derives its entire meaning from its local context. Outside of that context, the symbol may have another meaning entirely.

Change of Variable Exercise 1

summation: $\sum_{k=0}^{6} \frac{1}{k+1}$ *change of variable:* $j = k + 1$

$j = 0+1$ $\quad j = 6+1$

$j = 1 \rightarrow j = 7$

$$\sum_{j=1}^{7} \frac{1}{j}$$

Change of Variable Exercise 1 - Solution

Solution:

- First calculate the lower and upper limits of the new summation:

  When $k = 0$, $\quad j = k + 1 = 0 + 1 = 1.$

  When $k = 6$, $\quad j = k + 1 = 6 + 1 = 7.$

  Thus the new sum goes from $j = 1$ to $j = 7$.

- Next calculate the general term of the new summation by replacing each occurrence of k by an expression in j:

  $$\text{Since } j = k + 1, \text{ then } k = j - 1.$$

  $$\text{Hence } \frac{1}{k+1} = \frac{1}{(j-1)+1} = \frac{1}{j}.$$

- Finally, put the steps together to obtain $\displaystyle\sum_{k=0}^{6} \frac{1}{k+1} = \sum_{j=1}^{7} \frac{1}{j}.$

Factorial Notation

• Definition

For each positive integer n, the quantity ***n* factorial** denoted ***n*!**, is defined to be the product of all the integers from 1 to n:

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

Zero factorial, denoted 0!, is defined to be 1:

$$0! = 1.$$

A recursive definition for factorial is the following: Given any nonnegative integer n,

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

used in permutation & combination

permutation → order matters

combination → order does not matter

Factorials Exercise

Simplify the following expressions:

a. $\dfrac{8!}{7!}$ **b.** $\dfrac{5!}{2!\cdot 3!}$ **c.** $\dfrac{1}{2!\cdot 4!}+\dfrac{1}{3!\cdot 3!}$

d. $\dfrac{(n+1)!}{n!}$ **e.** $\dfrac{n!}{(n-3)!}$

Solution:

a. $\dfrac{8!}{7!}=\dfrac{8\cdot 7!}{7!}=8$

b. $\dfrac{5!}{2!\cdot 3!}=\dfrac{5\cdot 4\cdot 3!}{2!\cdot 3!}=\dfrac{5\cdot 4}{2\cdot 1}=10$

d. $\dfrac{(n+1)!}{n!}=\dfrac{(n+1)\cdot n!}{n!}=n+1$

e. $\dfrac{n!}{(n-3)!}=\dfrac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)!}{(n-3)!}$

$=n\cdot(n-1)\cdot(n-2)$

$=n^3-3n^2+2n$

Factorials Exercise Solution

c. $\dfrac{1}{2!\cdot 4!}+\dfrac{1}{3!\cdot 3!}=\dfrac{1}{2!\cdot 4!}\cdot\dfrac{3}{3}+\dfrac{1}{3!\cdot 3!}\cdot\dfrac{4}{4}$ by multiplying each numerator and denominator by just what is necessary to obtain a common denominator

$=\dfrac{3}{3\cdot 2!\cdot 4!}+\dfrac{4}{3!\cdot 4\cdot 3!}$ by rearranging factors

$=\dfrac{3}{3!\cdot 4!}+\dfrac{4}{3!\cdot 4!}$ because $3\cdot 2!=3!$ and $4\cdot 3!=4!$

$=\dfrac{7}{3!\cdot 4!}$ by the rule for adding fractions with a common denominator

$=\dfrac{7}{144}$

"*n* Choose *r*" Notation

• Definition

Let n and r be integers with $0 \le r \le n$. The symbol

$$\binom{n}{r}$$

is read "***n* choose *r***" and represents the number of subsets of size r that can be chosen from a set with n elements. order does not matter

• Formula for Computing $\binom{n}{r}$

For all integers n and r with $0 \le r \le n$,

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

Chose 2 objects from {a,b,c,d}:

{a, b}, {a, c}, {a, d}, {b, c}, {b,d}, and {c, d}.

"*n* Choose *r*" Exercise

Use the formula for computing $\binom{n}{r}$ to evaluate the following expressions:

a. $\binom{8}{5}$ **b.** $\binom{4}{0}$ **c.** $\binom{n+1}{n}$

Solution:

a. $$\binom{8}{5} = \frac{8!}{5!(8-5)!}$$

$$= \frac{8 \cdot 7 \cdot \cancel{6} \cdot \cancel{5} \cdot \cancel{4} \cdot \cancel{3 \cdot 2 \cdot 1}}{(\cancel{5} \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot 1) \cdot (\cancel{3 \cdot 2 \cdot 1})}$$

$$= 56.$$

always cancel common factors before multiplying

"n Choose r" Exercise

b. $\binom{4}{4} = \frac{4!}{4!(4-4)!} = \frac{4!}{4!0!}$

$$= \frac{\cancel{4 \cdot 3 \cdot 2 \cdot 1}}{\cancel{(4 \cdot 3 \cdot 2 \cdot 1)}(1)}$$

$$= 1$$

c. $\binom{n+1}{n} = \frac{(n+1)!}{n!((n+1)-n)!} = \frac{(n+1)!}{n!1!} = \frac{(n+1) \cdot \cancel{n!}}{\cancel{n!}} = n+1$

n Choose r Properties

- $\binom{n}{k} = \binom{n}{n-k}$ for $0 \leq k \leq n$
- $\binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{k} = \binom{n}{k-1}\frac{n-k+1}{k}$ for $k > 0$
- $\binom{n}{k} = \binom{n-1}{k}\frac{n}{n-k}$ for $k < n$
- $\binom{n}{k} = \binom{n-1}{k-1}\frac{n}{k}$ for $n, k > 0$

Exercise

Prove that for all nonnegative integers n and r with $r + 1 \leq n$,
$\binom{n}{r+1} = \frac{n-r}{r+1}\binom{n}{r}$.

Hint:

$$\frac{n-r}{r+1}\binom{n}{r} = \frac{n-r}{r+1} \cdot \frac{n!}{r!\,(n-r)!}$$
$$= \frac{n-r}{r+1} \cdot \frac{n!}{r!(n-r)\cdot(n-r-1)!}$$
$$= \frac{n!}{(r+1)!(n-r-1)!}$$
$$= \binom{n}{r+1}$$

LHS : $\frac{n!}{(r+1)!\,(n-r-1)!}$

$= \frac{n!\,(n-r)}{(r+1)(r!)(n-r)!}$

$= \frac{(n-r)}{r+1} \cdot \frac{n!}{r!\,(n-r)!}$

$= \frac{n-r}{r+1}\left(\frac{n}{r}\right)$ = RHS

Permutations of Selected Elements

• Definition

An ***r*-permutation** of a set of n elements is an ordered selection of r elements taken from the set of n elements. The number of r-permutations of a set of n elements is denoted $P(n, r)$.

r permutation - order matters

Theorem 9.2.3

If n and r are integers and $1 \leq r \leq n$, then the number of r-permutations of a set of n elements is given by the formula

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) \qquad \text{first version}$$

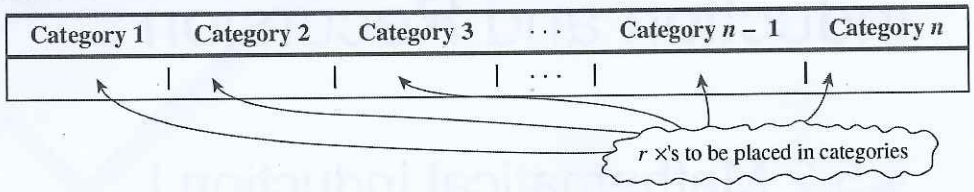
or, equivalently,

$$P(n, r) = \frac{n!}{(n-r)!} \qquad \text{second version.}$$

r-Combinations with Repetition Allowed

• Definition

An **r-combination with repetition allowed**, or **multiset of size r**, chosen from a set X of n elements is an unordered selection of elements taken from X with repetition allowed. If $X = \{x_1, x_2, \ldots, x_n\}$, we write an r-combination with repetition allowed, or multiset of size r, as $[x_{i_1}, x_{i_2}, \ldots, x_{i_r}]$ where each x_{i_j} is in X and some of the x_{i_j} may equal each other.



Theorem 9.6.1

The number of r-combinations with repetition allowed (multisets of size r) that can be selected from a set of n elements is

$$\binom{r+n-1}{r}.$$

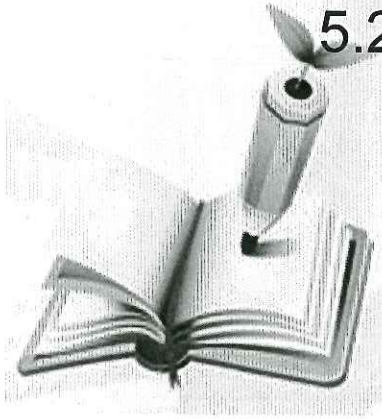
This equals the number of ways r objects can be selected from n categories of objects with repetition allowed.

Choosing k elements from n

	Order Matters	Order Does Not Matter
Repetition Is Allowed	n^k	$\binom{k+n-1}{k}$
Repetition Is Not Allowed	$P(n,k)$	$\binom{n}{k}$

Chapter 5: Sequences, Mathematical Induction and Recursion

5.2 Mathematical Induction I



Mathematical Induction

In general, mathematical induction

- Prove a property, defined for integers n, is true for all values of n that are greater than or equal to some initial integer.

Principle of Mathematical Induction

Let $P(n)$ 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 all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement

$$\text{for all integers } n \geq a,\ P(n)$$

is true.

Mathematical Induction

- Proving a statement by mathematical induction is a two-step process.
  - The first step is called the basis *step*
  - The second step is called the inductive *step*.

Method of Proof by Mathematical Induction

Consider a statement of the form, "For all integers $n \geq a$, a property $P(n)$ is true." To prove such a statement, perform the following two steps:

Step 1 (basis step): Show that $P(a)$ is true.

Step 2 (inductive step): Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true. To perform this step,

suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$.

[This supposition is called the **inductive hypothesis.***]*

Then

show that $P(k+1)$ is true.

Mathematical Induction Exercise

– Sum of the First n Integers

Use mathematical induction to prove that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for all integers } n \geq 1.$$

Solution:

Let the property *P(n)* be the equation

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

← the property $(P(n))$

Mathematical Induction Exercise Solution

– Sum of the First n Integers

Step 1 basic step: showing P(1) is true.

- The left-hand side of this equation is 1.
- The right-hand side is $\frac{1(1+1)}{2} = 1$

So, the left-hand side is equal to the right-hand side, thus P(1) is true.

Step 2 inductive step: Show that for all integers k ≥ 1, if $P(k)$ is true then $P(k + 1)$ is also true: (translation first)

Suppose that *k* is any integer with $k \geq 1$ such that

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

[We must show that P(k + 1) is true. That is:] We must show that

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

Mathematical Induction Exercise Solution

– Sum of the First n Integers

Step 2 inductive step: Show that for all integers k ≥ 1, if $P(k)$ is true then $P(k + 1)$ is also true:

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

$$1 + 2 + \cdots + k + (k+1)$$

$= 1 + 2 + \cdots + k + (k+1)$ by making the next-to-last term explicit

$= \frac{k(k+1)}{2} + (k+1)$ by substitution from the inductive hypothesis

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

So, the left-hand side is equal to the right-hand side, therefore P(k+1) is true.

[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

Sum of the First n Integers & Closed Form

Theorem 5.2.2 Sum of the First n Integers

For all integers $n \geq 1$,

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

• Definition Closed Form

If a sum with a variable number of terms is shown to be equal to a formula that does not contain either an ellipsis or a summation symbol, we say that it is written **in closed form.**

Applying the Formula for the Sum of the First n Integers

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

a. Evaluate 2 + 4 + 6 +· · ·+ 500.

b. Evaluate 5 + 6 + 7 + 8 +· · ·+ 50.

c. For an integer $h \geq 2$, write 1 + 2 + 3 +· · ·+ $(h - 1)$ in closed form.

~~Applying the Formula for the Sum of~~ the First n Integers - Solution

a. $2+4+6+\cdots+500 = 2\cdot(1+2+3+\cdots+250)$

$1+2+\cdots+n=\dfrac{n(n+1)}{2}.$

$= 2\cdot\left(\dfrac{250\cdot 251}{2}\right)$ by applying the formula for the sum of the first n integers with $n = 250$

$= 62{,}750.$

b. $5+6+7+8+\cdots+50 = (1+2+3+\cdots+50)-(1+2+3+4)$

$= \dfrac{50\cdot 51}{2} - 10$ by applying the formula for the sum of the first n integers with $n = 50$

$= 1{,}265$

c. $1+2+3+\cdots+(h-1) = \dfrac{(h-1)\cdot[(h-1)+1]}{2}$ by applying the formula for the sum of the first n integers with $n = h-1$

$= \dfrac{(h-1)\cdot h}{2}$ since $(h-1)+1 = h.$

Sum of a Geometric Sequence

Geometric sequence: each term is obtained from the preceding one by multiplying by a constant factor. $a_{k+1} = ra_k$ $(k \in Z, r \in R)$

Example: $1, r, r^2, r^3, \ldots, r^n$ where r is a constant factor.

Theorem 5.2.3 Sum of a Geometric Sequence

For any real number r except 1, and any integer $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}.$$

memorize

The expanded form of the formula is

$$r^0 + r^1 + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1},$$

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}.$$

Sum of a Geometric Sequence

Proof (by mathematical induction):

Let the property $P(n)$ be the equation

step 0: what is P(n)?

$$\sum_{i=0}^{n} r^i = \frac{r^{i+1} - 1}{r - 1} \qquad \leftarrow P(n)$$

We must show that $P(n)$ is true for all integers $n \geq 0$. → domain

Step 1 basic step: showing P(0) is true.

To establish $P(0)$, we must show that $\sum_{i=0}^{0} r^i = \frac{r^{0+1} - 1}{r - 1}$ $\leftarrow P(0)$

The left-hand side of this equation is $r^0 = 1$ and the right-hand side is $\frac{r^{0+1} - 1}{r - 1} = \frac{r - 1}{r - 1} = 1$ also because $r^1 = r$ and $r \neq 1$. Hence $P(0)$ is true.

LHS: $P(a) = P(0) = 1$ RHS: $\frac{r^{0+1} - 1}{r - 1} = \frac{r - 1}{r - 1} = 1$

Sum of a Geometric Sequence

Step 2 inductive step: Show that for all integers $k \geq 0$, 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 $k \geq 0$. That is:]

$n = k = P(n) = P(k)$

Let k be any integer with $k \geq 0$, and suppose that $P(k)$ is true

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1} \qquad \leftarrow P(k) \text{ inductive hypothesis}$$

Reasoning

[We must show P(k + 1) is true. That is:] We must show that

$$\sum_{i=0}^{k+1} r^i = \frac{r^{(k+1)+1} - 1}{r - 1}.$$

Or, equivalently,

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}. \qquad \leftarrow P(k+1)$$

$P(k + 1)$ is true

Sum of a Geometric Sequence

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

$$\sum_{i=0}^{k+1} r^i = \sum_{i=0}^{k} r^i + r^{k+1}$$ by writing the $(k+1)$st term separately from the first k terms

$$= \frac{r^{k+1}-1}{r-1} + r^{k+1}$$ by substitution from the inductive hypothesis

$$= \frac{r^{k+1}-1}{r-1} + \frac{r^{k+1}(r-1)}{r-1}$$ by multiplying the numerator and denominator of the second term by $(r-1)$ to obtain a common denominator

$$= \frac{(r^{k+1}-1) + r^{k+1}(r-1)}{r-1}$$ by adding fractions

$$= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r-1}$$ by multiplying out and using the fact that $r^{k+1} \cdot r = r^{k+1} \cdot r^1 = r^{k+2}$

$$= \frac{r^{k+2}-1}{r-1}$$ by canceling the r^{k+1}'s.

which is the right-hand side of $P(k+1)$ *[as was to be shown.]*

[Since we have proved the basis step and the inductive step, we conclude that the theorem is true.]

Applying the Formula for the Sum of a Geometric Sequence

In each of (**a**) and (**b**) below, assume that m is an integer that is greater than or equal to 3. Write each of the sums in closed form.

a. $1 + 3 + 3^2 + \cdots + 3^{m-2}$

b. $3^2 + 3^3 + 3^4 + \cdots + 3^m$

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}.$$

Solution:

a. $$1 + 3 + 3^2 + \cdots + 3^{m-2} = \frac{3^{(m-2)+1} - 1}{3-1}$$ by applying the formula for the sum of a geometric sequence with $r = 3$ and $n = m-2$

$$= \frac{3^{m-1}-1}{2}.$$

b. $$3^2 + 3^3 + 3^4 + \cdots + 3^m = 3^2 \cdot (1 + 3 + 3^2 + \cdots + 3^{m-2})$$ by factoring out 3^2

$$= 9 \cdot \left(\frac{3^{m-1}-1}{2}\right)$$ by part (a).