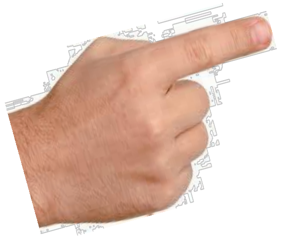
Number Theory
and Proof Methods

Mustafa Jarrar

&

Radi Jarrar



Watch this lecture and download the slides

http://jarrar-courses.blogspot.com/2014/03/discrete-mathematics-course.html

More Lectures Courses at: http://www.jarrar.info

Acknowledgement:
This lecture is based on, but not limited to, chapter 3 in "Discrete Mathematics with Applications by Susanna S. Epp (3rd Edition)".

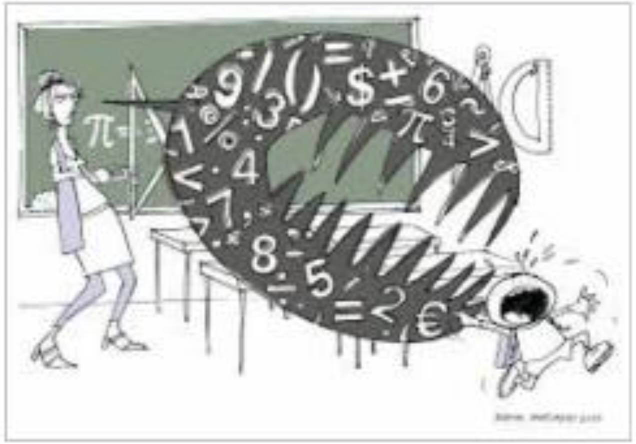
4.1 Introduction to Number Theory & Proofs Methods

In this lecture:

- Part 1: **Why Number theory for programmers**
- Part 2: Odd-Even & Prime-Composite Numbers
- Part 3: How to prove statements;
- Part 4: Disprove by counterexample;
- Part 5: Direct proofs

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, Odd, even, Prime, Composite

Why Number Theory for Programmers?



- How to learn to be precise in thinking and in programing?
- Mistakes and bugs in programs: e.g., medical applications, military applications, …
- We use numbers everywhere in programs especially in loops and conditions.
- Studying number theory (properties of numbers) is very helpful, especially **how to prove and disapprove**
- For example: (dis/)approve the following properties:
  - ❖ The product of any two even integers is even?
  - ❖ The sum/difference of any two odd integers is even?
  - ❖ The product of any two odd integers is odd?

4.1 Introduction to Number Theory & Proofs Methods

In this lecture:

- Part 1: Why Number theory for programmers
- Part 2: **Odd-Even & Prime-Composite Numbers**
- Part 3: How to prove statements;
- Part 4: Disprove by counterexample;
- Part 5: Direct proofs

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, Odd, even, Prime, Composite

Odd and Even Numbers

• Definitions

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

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

Examples

Is 0 even? ✓
Is −301 odd? ✓
If a and b are integers, is $6a^2b$ even? ✓
If a and b are integers, is $10a + 8b + 1$ odd? ✓
Is every integer either even or odd? ✓

Prime and Composite Numbers

- **Definition**

An integer n is **prime** if, and only if, $n > 1$ 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, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

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 integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

Example

Is 1 prime? ❌

Is it true that every integer greater than 1 is either prime or composite? ✓

4.1 Introduction to Number Theory & Proofs Methods

In this lecture:

- Part 1: Why Number theory for programmers
- Part 2: Odd-Even & Prime-Composite Numbers
- Part 3: **How to prove statements;**
- Part 4: Disprove by counterexample;
- Part 5: Direct proofs

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, Odd, even, Prime, Composite

How to (dis)approve statements

Before (dis)approving, write a math statements as a Universal or an Existential Statement:

	Proving	Disapproving
$\exists x \in D \;.\; Q(x)$	One example	Negate then direct proof
$\forall x \in D \;.\; Q(x)$	Direct proof	Counter example

This chapter: Direct proofs with numbers

4.1 Introduction to Number Theory & Proofs Methods

In this lecture:

- ❑ Part 1: Why Number theory for programmers
- ❑ Part 2: Odd-Even & Prime-Composite Numbers
- ❑ Part 3: How to prove statements
- ❑ Part 4: **Disprove by counterexample**
- ❑ Part 5: Direct proofs

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, Odd, even, Prime, Composite

Disproof by Counterexample

$\forall a,b \in \mathbf{R} \;.\; a^2 = b^2 \;\rightarrow\; a = b.$

Counterexample:

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

4.1 Introduction to Number Theory & Proofs Methods

In this lecture:

- ❑ Part 1: Why Number theory for programmers
- ❑ Part 2: Odd-Even & Prime-Composite Numbers
- ❑ Part 3: How to prove statements;
- ❑ Part 4: Disprove by counterexample;
- ❑ Part 5: **Direct proofs**

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, Odd, even, Prime, Composite

Proving Universal Statements

The Method of Exhaustion

The majority of mathematical statements to be proved are universal.

$$\forall x \in D \;.\; P(x) \rightarrow Q(x)$$

One way to prove such statements is called **The Method of Exhaustion**, by listing all cases.

Example

Use the method of exhaustion to prove the following:

$\forall n \in \mathbb{Z}$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two prime numbers.

$4 = 2 + 2$	$6 = 3 + 3$	$8 = 3 + 5$	$10 = 5 + 5$
$12=5+7$	$14=11+3$	$16=5+11$	$18=7+11$
$20=7+13$	$22=5+17$	$24=5+19$	$26=7+19$

➔ **This method** is obviously impractical, as we cannot check all possibilities.

Direct Proofs

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, and show that x satisfies the property.

عنصر محدد بس اختياره عشوائي

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "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.

Example

Prove that the sum of any two even integers is even.

Formal Restatement: $\forall m,n \in \mathbf{Z}$. Even(m) $\wedge$Even(n) $\rightarrow$ Even($m + n$)

Starting Point: Suppose m and n are even *[particular but arbitrarily chosen]*

We need to Show: $m+n$ is even

$m = 2k$
$n = 2j$
$m+n = 2k + 2j = 2(k+j)$
$(k+j)$ is integer
Thus: $2(k+j)$ is even

[This is what we needed to show.]

In the next sections

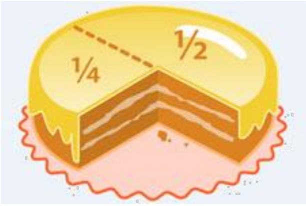
we will practice proving more examples

Number Theory
and Proof Methods

Mustafa Jarrar

Number Theory

4.2 Rational Numbers



In this lecture:

- ❑ Part 1: **Rational and irrational Numbers;**
- ❑ Part 2: Proving Properties of Rational Numbers;
- [redacted]

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, Odd, even, Prime, Composite

Relational and Irrational Numbers

الاعداد النسبية

• 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

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

Example

- ✓ Is 10/3 a rational number?
- ✓ Is -(5/39) a rational number?
- ✓ Is 0.281 a rational number?
- ✓ Is 7 a rational number?
- ✓ Is 0 a rational number?
- ✗ Is 2/0 a rational number?
- ✗ Is 2/0 an irrational number? Not number
- ✓ Is 0. 1212... a rational number (where 12 are assumed to repeat forever)? 12/99
- ✓ If m, n are integers and neither m nor n is zero, is $(m + n)/mn$ a rational number?
- ✗ Is (Sqr root of 2) an rational number?

Integers are rational numbers

Theorem 4.2.1

Every integer is a rational number.

$$n = \frac{n}{1}$$ which is a quotient of integers and hence rational.

$$7 = \frac{7}{1}$$ which is a quotient of integers and hence rational.

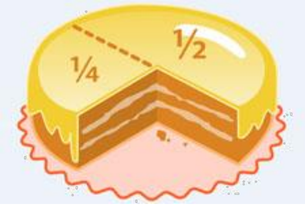
$$-12 = \frac{-12}{1}$$ which is a quotient of integers and hence rational.

$$0 = \frac{0}{1}$$ which is a quotient of integers and hence rational.

Mustafa Jarrar: Lecture Notes on **Number Theory and Proofs**.
Birzeit University, Palestine, 2021

Number Theory

4.2 Rational Numbers



In this lecture:

- ❑ Part 1: Rational and irrational Numbers;
- ❑ Part 2: **Proving Properties of Rational Numbers;**
- [redacted]

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, Odd, even, Prime, Composite

Proving Properties of Rational Numbers

Theorem 4.2.2

The sum of any two rational numbers is rational.

Proof:

$$r + s = \frac{a}{b} + \frac{c}{d} \quad \text{by substitution}$$

$$= \frac{ad + bc}{bd} \quad \text{by basic algebra.}$$

Let $p = ad + bc$ and $q = bd$.

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

نسطيع استخدام نظريات مثبتة لإثبات نظريات جديدة

Example

Derive the following as a corollary of Theorem 4.2.2.

Corollary 4.2.3

The double of a rational number is rational.

Solution:

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

Deriving Additional Results about Even and Odd Integers

Suppose you 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 $\frac{a^2+b^2+1}{2}$ is an integer.

a x a = even x even = even
b x b = odd x odd = odd
$a^2 + b^2$ = even + odd = odd
odd + 1 = even
$\frac{\text{even}}{2}$ = integer #

➔ Try it at home

Real Numbers in Real Life

Two mechanics were working on a car. One can complete a given job in 6 hours. But, the new guy takes 8 hours. They work together for first two hours. But then, the first guy left to help another mechanic on a different job. How long will it take for the new guy to finish the car work?

The first guy can do 1/6 part of job per hour and the second guy can do 1/8 part of job per hour and together they can do 1/6 + 1/8part of job per hour. Now, let 't' hours is the time to complete the car job. So, 1/t job will be completed per hour, Equating the two expressions, we get:

$1/6 + 1/8 = 1/t$

$7/24 = 1/t$

As they work for 2 hours, $2 \cdot 7/24 = 14/24$ part of job will be done.

The work remaining is $1 - 1/t = (1 - 14/24)$

$= 10/24$

∴ 10/24 job is left which has to be completed by the second guy, who will take $10/24 \div 1/8$

$= 40/12$

$= 10/3$

$= 3.33$ hours to complete the car job.

Number Theory
and Proof Methods

Mustafa Jarrar

4.1 Introduction

4.2 Rational Numbers

4.3 Divisibility

4.4 Quotient-Remainder Theorem

Number Theory

4.3 Divisibility

In this lecture:

- ❑ Part 1: **What is Divisibility;**
- ❑ Part 2: Proving Properties of Divisibility;
- ❑ Part 3: The Unique Factorization Theorem

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, divisibility, factorization

What is Divisibility?

• 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.

The notation **d | n** is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Examples

- ✓ Is 21 divisible by 3?
- ✓ Does 5 divide 40?
- ✓ Does $7 \mid 42$?
- ✓ Is 32 a multiple of -16?
- ✓ Is 6 a factor of 54?
- ✓ Is 7 a factor of -7?
- ✓ If k is any integer, does k divide **0?**

Number Theory

4.3 Divisibility

In this lecture:

- Part 1: What is Divisibility;
- Part 2: **Proving Properties of Divisibility;**
- Part 3: The Unique Factorization Theorem

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, divisibility, factorization

Positive Divisor of a Positive Integer

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 $a \leq b$.

Proof:

$$b = a.k$$

Thus $1 \leq k$

$a.1 \leq k . a$ multiply both sides with a.

Thus $a \leq k . a = b$

Thus $a \leq b$

Divisibility of Algebraic Expressions

If *a* and *b* are integers, is *3a* + *3b* divisible by 3?

$3a + 3b = 3(a + b)$ and $a + b$ is an integer because it is a sum of two integers.

If *k* and *m* are integers, is *10km* divisible by *5?*

$10km = 5 \cdot (2km)$ and $2km$ is an integer because it is a product of three integers.

Not divisible

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

Prime Numbers and Divisibility

An alternative way to define a prime number is to say that:

an integer $n > 1$ is prime if, and only if, its only positive integer divisors are 1 and itself.

Transitivity of Divisibility

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:

Starting Point: Suppose a, b, and c are particular but arbitrarily chosen integers such that $a \mid b$ and $b \mid c$.

We need to show: $a \mid c$.

since $a \mid b$, $b = ar$ for some integer r.
And since $b \mid c$, $c = bs$ for some integer s.
Hence, $c = bs = (ar)s$
But $(ar)s = a(rs)$ by the associative law
Hence $c = a(rs)$.
As rs is an integer, then $a \mid c$.

Divisibility by a Prime

Theorem 4.3.4 Divisibility by a Prime

Any integer $n > 1$ is divisible by a prime number.

Counterexamples and Divisibility

Checking a Proposed Divisibility Property

Is it true or false that 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 proposed divisibility property is false.

Number Theory

4.3 Divisibility

In this lecture:

- Part 1: What is Divisibility;
- Part 2: Proving Properties of Divisibility;
- Part 3: **The Unique Factorization Theorem**

Keywords: Number Theory, Prove, Disapprove, Direct Proofs, divisibility, factorization

Important
Theory

The Unique Factorization Theorem

By a German mathematician (Carl Friedrich Gauss) in 1801.

The Unique Factorization Theorem

أي رقم اكبر من واحد إما ان يكون عدد أولي او حاصل ضرب أعداد أولية

Any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique except,

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 3 \cdot 2$$

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 $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

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

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.

The Standard factored Form

• Definition

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; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

Example: Write 3,300 in standard factored form.

$$\begin{aligned} 3{,}300 &= 100 \,.\, 33 \\ &= 4 \,.\, 25 \,.\, 3 \,.\, 11 \\ &= 2 \,.\, 2 \,.\, 5 \,.\, 5 \,.\, 3 \,.\, 11 \\ &= 2^2 \,.\, 3^1 \,.\, 5^2 \,.\, 11^1. \end{aligned}$$

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 a prime in the left, it should be also in the right side.
Since we cannot produce 17 form (8,7,6,5,4,3 or 2) it should be a prime factor of m

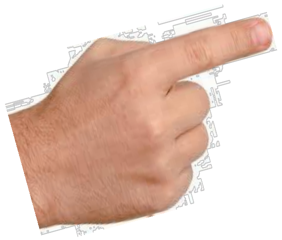
Number Theory
and Proof Methods

Mustafa Jarrar

4.1 Introduction

4.2 Rational Numbers

4.3 Divisibility



4.4 Quotient-Remainder Theorem

Number Theory

4.4 Quotient-Remainder Theorem

In this lecture:

- Part 1: **Quotient-Remainder Theorem**
- Part 2: *div* and *mod*, and applications in real-life
- Part 3: Representing Integers in Quotient-Remainder
- Part 4: Absolute Value

Keywords: Number Theory, Quotient-Remainder Theorem, div, mod, divide into cases" Proof Method, Parity, Integers Modulo, Absolute Value

Quotient-Remainder Theorem

Notice that:

$$\begin{array}{r|l} & \ \ 2 \leftarrow \text{quotient} \\ 4 & 11 \\ & \ \ \underline{8} \\ & \ \ 3 \leftarrow \text{remainder} \end{array}$$

$$11 = 2 \cdot 4 + 3.$$

↑ 2 groups of 4 ↑ 3 left over

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

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

Examples:

$54 = 4 \cdot 13 + 2$	$q = 13$	$r = 2$
$-54 = 4 \cdot (-14) + 2$	$q = -14$	$r = 2$
$54 = 70 \cdot 0 + 54$	$q = 0$	$r = 54$

Number Theory

4.4 Quotient-Remainder Theorem

In this lecture:

- ❑ Part 1: Quotient-Remainder Theorem
- ❑ Part 2: ***div* and *mod*, and applications in real-life**
- ❑ Part 3: Representing Integers in Quotient-Remainder
- ❑ Part 4: Absolute Value

Keywords: Number Theory, Quotient-Remainder Theorem, div, mod, divide into cases" Proof Method, Parity, Integers Modulo, Absolute Value

div and mod

• Definition

Given an integer n and a positive integer d,

$$\textbf{\textit{n div d}} = \text{the integer quotient obtained when } n \text{ is divided by } d \text{, and}$$

$$\textbf{\textit{n mod d}} = \text{the nonnegative integer remainder obtained when } n \text{ is divided by } d.$$

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

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

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

"/" in C++, JAVA, .net

"%" in C,JAVA
"\" in .net

Examples:

$$32 \text{ div } 9 = 3$$
$$32 \text{ mod } 9 = 5$$

Application of div and mod

Computing the Day of the Week

Suppose today is Tuesday, and neither this year nor next year is a leap year (سنة كبيسة). What day of the week will it be 1 year from today?

365 *div* 7 = 52 and 365 *mod* 7 = 1

So,
after 364 it will be Tuesday, and after 365 it will be Wednesday

Application of div and mod

Computing the Day of the Week

If today is Saturday and it is 16/10/2021, which day it will be on 20/2/2022?

The number of days from today to 20/2/2022 = 15 in October + 30 in November + 31 in December + 31 in January + 20 in February = **127 days**

127 div 7 = 18   127 mod 7 = 1

That is, after 18 weeks the day will be Saturday, and one day after, it will be **Sunday**

Application of div and mod

Solving a Problem about *mod*

Suppose *m* is an integer. If *m mod* 11 = 6, what is 4*m mod* 11?

$$m = 11q + 6$$

So, $4m = 44q + 24$

$= 44q + 22 + 2$

$= 11(\underline{4q + 2}) + 2$ $\quad$ (4*q* + 2) is integer

Thus $\quad$ **4*m* *mod* 11 = 2**

Number Theory

4.4 Quotient-Remainder Theorem

In this lecture:

- ❑ Part 1: Quotient-Remainder Theorem
- ❑ Part 2: *div* and *mod*, and applications in real-life
- ❑ Part 3: **Representing Integers in Quotient-Remainder**
- ❑ Part 4: Absolute Value

Keywords: Number Theory, Quotient-Remainder Theorem, div, mod, divide into cases" Proof Method, Parity, Integers Modulo, Absolute Value

Representing Integers using the quotient-remainder theorem

Parity Property

We represent any number as:

$$n = 2q + r \qquad \textbf{and} \quad 0 \le r < 2$$

Because we have only r = 0 and r =1, then:

$$n = 2q + 0 \qquad \textbf{or} \qquad n = 2q + 1$$

Even Odd

Therefore, n is either even or odd (parity)

Representing Integers using the quotient-remainder theorem

Proving Parity Property

Theorem 4.4.2 The Parity Property

Any two consecutive integers have opposite parity.

even or odd

Proof:

Given m and $m+1$ are consecutive integers

Then, one is odd and the other is even (by parity property)

Case1 (m is even): $m = 2k$, so $m + 1 = 2k + 1$, which is odd

Case2 (m is odd): $m = 2k + 1$ and so $m+1 = (2k+1) + 1 = 2k + 2 = 2(k+1)$.

thus $m + 1$ is even.

Proof by division into cases

The "divide into cases" Proof Method

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or ... or A_n, then C," prove all of the following:

$$\text{If } A_1, \text{ then } C,$$
$$\text{If } A_2, \text{ then } C,$$
$$\vdots$$
$$\text{If } A_n, \text{ then } C.$$

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

Representing Integers using the quotient-remainder theorem

Integers Modulo 4

We represent any integer as:

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

This implies that there exist an integer quotient q and a remainder r such that

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

Using the "divide into cases" Proof Method

Theorem 4.4.3

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

Proof: $\forall n \in Odd, \exists\, m \in Z\ .\ n^2 = 8m + 1.$

Hint: any odd integer can be (4q+1) or (4q+3).

Case 1 (n=4q+1):

$n^2 = 8m + 1 = (4q+1)^2 = 16q^2 + 8q + 1 = 8(\underline{2q^2 + q}) + 1$

$(2q^2 + q)$ can be is an integer m, thus $n^2 = 8m + 1$

Case 2 (4q+3):

$n^2 = 8m + 1 = (4q+3)^2 = 16q^2 + 24q + 8 + 1 = 8(\underline{2q^2 + 3q + 1}) + 1$

$(2q^2 + 3q + 1)$ can be is an integer m, thus $n^2 = 8m + 1$

Number Theory

4.4 Quotient-Remainder Theorem

In this lecture:

- ❑ Part 1: Quotient-Remainder Theorem
- ❑ Part 2: *div* and *mod*, and applications in real-life
- ❑ Part 3: Representing Integers in Quotient-Remainder
- ❑ Part 4: **Absolute Value**

Keywords: Number Theory, Quotient-Remainder Theorem, div, mod, divide into cases" Proof Method, Parity, Integers Modulo, Absolute Value

Absolute Value

القيمة المطلقة

Definition

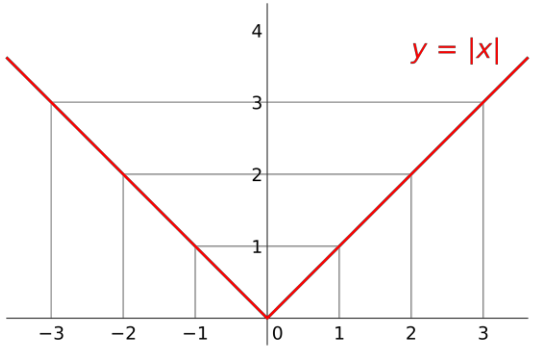
For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

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

Example:

$|2| = 2$

$|-2| = 2$



Absolute Value

Lemma 4.4.4

For all real numbers r, $-|r| \le r \le |r|$.

Proof:

Suppose r is any real number. We divide into cases according to whether $r \geq 0$ or $r < 0$.

Case 1 ($r \ge 0$): by definition $|r| = r$. Also, r is positive and $-|r|$ is negative, ➔ $-|r| < r$.

Case 2 ($r < 0$): by definition $|r| = -r$, thus, $-|r| = r$. Also r is negative and $|r|$ is positive. ➔ $r < |r|$.

Thus, in either case, $-|r| \le r \le |r|$

Absolute Value

Lemma 4.4.5

For all real numbers r, $|-r| = |r|$.

Proof: Suppose r is any real number. By Theorem T23 in Appendix A, if $r > 0$, then $-r < 0$, and if $r < 0$, then $-r > 0$. Thus

$$|-r| = \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ -(-r) & \text{if } -r < 0 \end{cases}$$ by definition of absolute value

$$= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } -r < 0 \end{cases}$$ because $-(-r) = r$ by Theorem T4 in Appendix A

$$= \begin{cases} -r & \text{if } r < 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } r > 0 \end{cases}$$ because, by Theorem T24 in Appendix A, when $-r > 0$, then $r < 0$, when $-r < 0$, then $r > 0$, and when $-r = 0$, then $r = 0$

$$= \begin{cases} r & \text{if } r \geq 0 \\ -r & \text{if } r < 0 \end{cases}$$ by reformatting the previous result

$$= |r|$$ by definition of absolute value.

Absolute Value and Triangle Inequality

Theorem 4.4.6 The Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.

Proof:

Case 1 $(x + y \geq 0)$: $|x + y| = x + y$ by Lemma 4.4.4,

and so, $x \leq |x|$ and $y \leq |y|$

hence, $|x + y| = x + y \leq |x| + |y|$

Case 2 $(x + y < 0)$: $|x + y| = -(x + y) = (-x) + (-y)$ by Lemmas 4.4.4 &4.4.5

and so, $-x \leq |-x| = |x|$ and $-y \leq |-y| = |y|$.

hence, $|x + y| = (-x) + (-y) \leq |x| + |y|$.