Number Theory
and Proof Methods

Mustafa Jarrar

4.1 Introduction

4.2 Rational Numbers

4.3 Divisibility

4.4 Quotient-Remainder Theorem

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 4 in "Discrete Mathematics with Applications by Susanna S. Epp (3rd Edition)".

,

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:

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

$$11 = \underbrace{2\cdot 4}_{\text{2 groups of 4}} + \underbrace{3}_{\text{3 left over}}.$$

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,

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

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

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

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

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

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

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

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 $4m$ *mod* 11?

$$m = 11q + 6$$

So, $4m = 44q + 24$

$= 44q + 22 + 2$

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

Thus **$4m$ *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.

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:

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

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

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

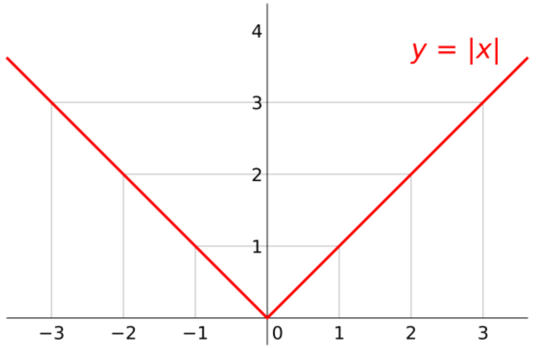
For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

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

Example:

$|2| = 2$

$|-2| = 2$



,

Absolute Value

Lemma 4.4.4

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

Proof:

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

Case 1 ($r \geq 0$): 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, $-|r| \leq r \leq |r|$

,

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

$$
\begin{aligned}
|-r| &= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ -(-r) & \text{if } -r < 0 \end{cases} && \text{by definition of absolute value} \\
&= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } -r < 0 \end{cases} && \text{because } -(-r) = r \text{ by Theorem T4 in Appendix A} \\
&= \begin{cases} -r & \text{if } r < 0 \\ 0 & \text{if } -r = 0 \\ r & \text{if } r > 0 \end{cases} && \text{because, by Theorem T24 in Appendix A, when } -r > 0, \text{ then } r < 0, \text{ when } -r < 0, \text{ then } r > 0, \text{ and when } -r = 0, \text{ then } r = 0 \\
&= \begin{cases} r & \text{if } r \geq 0 \\ -r & \text{if } r < 0 \end{cases} && \text{by reformatting the previous result} \\
&= |r| && \text{by definition of absolute value.}
\end{aligned}
$$

,

Absolute Value and Triangle Inequality

Theorem 4.4.6 The Triangle Inequality

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

Proof:

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

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

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

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

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

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

,