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

Course Page: http://www.jarrar.info/courses/DMath/
More Online Courses at: http://www.jarrar.info

Acknowledgement:
This lecture is based on (but not limited to) to chapter 4 in "Discrete Mathematics with Applications by Susanna S. Epp (3rd Edition)".
In this lecture:

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

### Quotient-Remainder Theorem

Notice that:

\[
\begin{align*}
4 & \longrightarrows 2 & \text{quotient} & 11 = 4 \cdot 2 + 3 & \uparrow & \uparrow & \text{2 groups of 4} & \text{3 left over} \\
8 & \longrightarrows 3 & \text{remainder} & \\
\end{align*}
\]

**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:**

- \( 54 = 4 \cdot 13 + 2 \quad q = 13 \quad r = 2 \)
- \( -54 = 4 \cdot (\text{odd number}) + 2 \quad q = -14 \quad r = 2 \)
- \( 54 = 70 \cdot 0 + 54 \quad q = 0 \quad r = 54 \)
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

div and mod

Definition
Given an integer \( n \) and a positive integer \( d \),

\[
\begin{align*}
 n \text{ div } d &= \text{ the integer quotient obtained when } n \text{ is divided by } d, \text{ and} \\
 n \text{ mod } d &= \text{ the nonnegative integer remainder obtained when } n \text{ is divided by } d.
\end{align*}
\]

Symbolically, if \( n \) and \( d \) are integers and \( d > 0 \), then
\[
 n \text{ div } d = q \text{ and } n \text{ mod } d = r \iff n = dq + r
\]

Where \( q \) and \( r \) are integers and \( 0 \leq r < d \)

Examples:

\[
\begin{align*}
32 \text{ div } 9 &= 3 \\
32 \text{ mod } 9 &= 5
\end{align*}
\]
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 (ليست سنة كبيسة). What day of the week will it be 1 year from today?

\[
365 \div 7 = 52 \quad \text{and} \quad 365 \mod 7 = 1
\]

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 Thursday and it is 16/10/2014, which day it will be the valentine's day in 2015?

Valentine's day = 14/2/2015

The number of days from today to 14/2/2015 = 15 in October + 30 in November + 31 in December + 31 in January + 14 in February = 121 days

\[
121 \div 7 = 17 \quad \text{and} \quad 121 \mod 7 = 2
\]

That is, after 17 weeks the day will be Thursday, and two days after, it will be Saturday
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,
\[
4m = 44q + 24
= 44q + 22 + 2
= 11(4q + 2) + 2
\]

(\( 4q + 2 \) 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
Representing Integers using the quotient-remainder theorem

Parity Property

We represent any number as:

\[ n = 2q + r \quad \text{and} \quad 0 \leq r < 2 \]

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

\[ n = 2q + 0 \quad \text{or} \quad n = 2q + 1 \]

Even \quad Odd

Therefore, \( n \) is either even or odd (parity)

---

Theorem 4.4.2 The Parity of 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)

Case 1 (\( m \) is even): \( m = 2k \), so \( m + 1 = 2k + 1 \), which is odd
Case 2 (\( m \) is odd): \( m = 2k + 1 \) and so \( m+1 = (2k+1) + 1 = 2k + 2 = 2(k+1) \).
thus \( m + 1 \) is even.
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:

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

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

Representing Integers using the quotient-remainder theorem

Integers Modulo 4

We represent any integer as:

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

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

\[ n = 4q + r \quad \text{and} \quad 0 \leq r < 4. \]
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:**
$\forall n \in \text{Odd}, \exists m \in \mathbb{Z}. \ n^2 = 8m + 1$

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

**Case 1 (n=4q+1):**
$n^2 = 8m + 1 = (4q+1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1$
$(2q^2 + q)$ can be is an integer $m$, thus $n^2 = 8m + 1$

**Case 2 (4q+3):**
$n^2 = 8m + 1 = (4q+3)^2 = 16q^2 + 24q + 8 + 1 = 8(2q^2 + 3q+1) + 1$
$(2q^2 + 3q+1)$ can be is an integer $m$, thus $n^2 = 8m + 1$
Absolute Value

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

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

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.

Case 1 ($r \geq 0$): $|r| = r$
- by definition,
- $-|r| < r$ as $r$ is positive and so $-|r|$ is negative

$\therefore -|r| \leq r \leq |r|$ 

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

$\therefore -|r| \leq r \leq |r|$ 

Thus, in either case, $-|r| \leq r \leq |r|$.
Absolute Value

Lemma 4.4.5
For all real numbers \( r \), \(|-r| = |r|\)

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

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

because \(-(-r) = r\) by Theorem T4 in Appendix A

when \(-r > 0\), then \( r < 0\), when \(-r < 0\), then \( r > 0\), and when \(-r = 0\), then \( r = 0\)

by reformatting the previous result

by definition of absolute value.

Absolute Value and Triangle Inequality

Theorem 4.4.6 The Triangle Inequality
For all real numbers \( x \) and \( y \), \(|x+y| \leq |x| + |y|\)

Case 1 \((x + y \geq 0)\):

\[|x + y| = x + y\]

by Lemma 4.4.4

so \( x \leq |x| \) & \( y \leq |y|\)

\[\therefore |x + y| = x + y \leq |x| + |y|\]

Case 2 \((x + y < 0)\):

\[|x + y| = -(x + y) = -x + -y\]

by Lemmas 4.4.4 & 4.4.5

so \(-x \leq |x| = |x|\) and \(-y \leq |y| = |y|\)

\[\therefore |x + y| = (-x) + (-y) \leq |x| + |y|\]