Lecture Notes on **Discrete Mathematics**.
Birzeit University, Palestine, 2016

Number Theory
and Proof Methods

Mustafa Jarrar

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)".

Mustafa Jarrar: Lecture Notes in Discrete Mathematics.
Birzeit University, Palestine, 2016

Number Theory

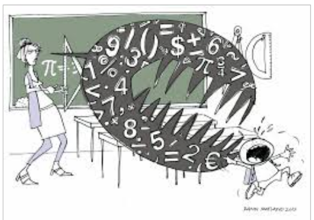
4.1 Introduction

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

3

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

Mustafa Jarrar: Lecture Notes in Discrete Mathematics.
Birzeit University, Palestine, 2016

Number Theory

4.1 Introduction

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

5

Odd and Even Numbers

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

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

Examples

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

6

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?

Mustafa Jarrar: Lecture Notes in Discrete Mathematics.
Birzeit University, Palestine, 2016

Number Theory

4.1 Introduction

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

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

9

Mustafa Jarrar: Lecture Notes in Discrete Mathematics.
Birzeit University, Palestine, 2016

Number Theory

4.1 Introduction

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

10

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 $1 \neq -1$.

Mustafa Jarrar: Lecture Notes in Discrete Mathematics.
Birzeit University, Palestine, 2016

Number Theory

4.1 Introduction

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**

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:

∀*n* ∈ Z, if *n* is even and 4 ≤ *n* ≤ 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.

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D, P(x) \rightarrow Q(x)$." (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: $\forall m,n \in \mathbf{Z}\ .\ \text{Even}(m) \wedge \text{Even}(n) \rightarrow \text{Even}(m+n)$

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 many examples