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

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)".

Mustafa Jarrar: Lecture Notes on **Number Theory and Proofs**.
Birzeit University, Palestine, 2015

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 | 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?**

Mustafa Jarrar: Lecture Notes on **Number Theory and Proofs**.
Birzeit University, Palestine, 2015

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.

7

Not divisible

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

8

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.

Proof:

Study at home
Maybe quiz next lecture?!

11

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.

12

Mustafa Jarrar: Lecture Notes on **Number Theory and Proofs**.
Birzeit University, Palestine, 2015

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

13

Important Theory

The Unique Factorization Theorem

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

14

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.

,

15

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.

3,300 = 100 . 33
= 4 . 25 . 3 . 11
= 2 . 2 . 5 . 5 . 3 . 11
= $2^2 . 3^1 \cdot 5^2 . 11^1$.

,

16

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 from (8,7,6,5,4,3 or 2) it should be a prime factor of *m*

17