# Number Theory

Slides by Christopher M. Bourke
Instructor: Berthe Y. Choueiry

Spring 2006

Computer Science & Engineering 235
Introduction to Discrete Mathematics
Sections 2.4–2.6 of Rosen
cse235@cse.unl.edu

Notes

## Introduction I

When talking about division over the integers, we mean division with no remainder.

**Definition**

Let $a, b \in \mathbb{Z}, a \neq 0$, we say that $a$ *divides* $b$ if there exists $c \in \mathbb{Z}$ such that $b = ac$. We denote this, $a \mid b$ and $a \nmid b$ when $a$ does not divide $b$. When $a \mid b$, we say $a$ is a *factor* of $b$.

**Theorem**

Notes

## Introduction II

*Let $a, b, c \in \mathbb{Z}$ then*

1. *If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.*
2. *If $a \mid b$, then $a \mid bc$ for all $c \in \mathbb{Z}$.*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

**Corollary**

*If $a, b, c \in \mathbb{Z}$ such that $a \mid b$ and $a \mid c$ then $a \mid mb + nc$ for $n, m \in \mathbb{Z}$.*

Notes

## Division Algorithm I

Let $a$ be an integer and $d$ be a positive integer. Then there are unique integers $q$ and $r$, with:

- $0 \leq r \leq d$
- such that $a = dq + r$

Not really an algorithm (traditional name). Further:

- $a$ is called the dividend
- $d$ is called the divisor
- $q$ is called the quotient
- $r$ is called the remainder, and is positive.

Notes

## Primes I

**Definition**

A positive integer $p > 1$ is called *prime* if its only positive factors are 1 and $p$.

If a positive integer is not prime, it is called *composite*.

Notes

## Primes II

**Theorem (Fundamental Theorem of Arithmetic, FTA)**

*Every positive integer $n > 1$ can be written uniquely as a prime or as the product of the powers of two or more primes written in nondecreasing size.*

That is, for every $n \in \mathbb{Z}, n > 1$, can be written as

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$$

where each $p_i$ is a prime and each $k_i \geq 1$ is a positive integer.

Notes

## Sieve of Eratosthenes

### Preliminaries

Given a positive integer, $n > 1$, how can we determine if $n$ is prime or not?

For hundreds of years, people have developed various tests and algorithms for *primality testing*. We'll look at the oldest (and most inefficient) of these.

**Lemma**

*If $n$ is a composite integer, then $n$ has a prime divisor $x \leq \sqrt{n}$.*

Notes

## Sieve of Eratosthenes

### Preliminaries

**Proof.**

- Let $n$ be a composite integer.
- By definition, $n$ has a prime divisor $a$ with $1 < a < n$, thus $n = ab$.
- Its easy to see that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Otherwise, if on the contrary, $a > \sqrt{n}$ and $b > \sqrt{n}$, then

$$ab > \sqrt{n}\sqrt{n} = n$$

- Finally, either $a$ or $b$ is prime divisor or has a factor that is a prime divisor by the Fundamental Theorem of Arithmetic, thus $n$ has a prime divisor $x \leq \sqrt{n}$.

□

Notes

## Sieve of Eratosthenes

### Algorithm

This result gives us an obvious algorithm. To determine if a number $n$ is prime, we simple must test every prime number $p$ with $2 < p \leq \sqrt{n}$.

**Sieve**

```
Input  : A positive integer n > 4.
Output : true if n is prime.
1 foreach prime number p, 2 < p ≤ √n do
2     if p | n then
3         output false
4     end
5 end
6 output true
```

Can be improved by reducing the upper bound to $\sqrt{\frac{n}{p}}$ at each iteration.

Notes