**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

**Introduction I**

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

**Definition**

Let $a, b \in \mathbb{Z}$ 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 $n, m \in \mathbb{Z}$.

**Division Algorithm I**

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

- $a = dq + r$
- $0 \leq r < d$
- $q$ is called the quotient
- $r$ is called the remainder, and is positive.

**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 $n, m \in \mathbb{Z}$.

**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.

**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

$$n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$$

where each $p_i$ is a prime and each $k_i \geq 1$ is a positive integer.
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 $x \leq \sqrt{n}$.

**Proof.**

Let $n$ be a composite integer.

By definition, $n$ has a prime divisor $a$ with $1 < a < n$, thus $n = ab$.

It’s 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 $x \leq \sqrt{n}$.

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

**Algorithm**

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

Numerous algorithms for primality testing have been developed over the last 50 years.


Available at [http://projecteuclid.org/Dienst/UI/1.0/Summarize/euclid.annm/1111770735](http://projecteuclid.org/Dienst/UI/1.0/Summarize/euclid.annm/1111770735)
How Many Primes?

How many primes are there?

**Theorem**

*There are infinitely many prime numbers.*

The proof is a simple proof by contradiction.

**Proof**

- Assume to the contrary that there are a finite number of primes, \( p_1, p_2, \ldots, p_n \).
- Let \( Q = p_1 p_2 \cdots p_n + 1 \)
- By the FTA, \( Q \) is either prime (in which case we are done) or \( Q \) can be written as the product of two or more primes.
- Thus, one of the primes \( p_j \) \((1 \leq j \leq n)\) must divide \( Q \), but then if \( p_j \mid Q \), it must be the case that \( p_j \mid Q - p_1 p_2 \cdots p_n = 1 \)
- Since this is not possible, we've reached a contradiction—there are not finitely many primes.

Distribution of Prime Numbers

**Theorem**

*The ratio of the number of prime numbers not exceeding \( n \) and \( \frac{n}{\ln n} \) approaches 1 as \( n \to \infty \).*

In other words, for a fixed natural number, \( n \), the number of primes not greater than \( n \) is about \( \frac{n}{\ln n} \)

Mersenne Primes I

A Mersenne prime is a prime number of the form \( 2^k - 1 \) where \( k \) is a positive integer. They are related to *perfect numbers* (if \( M_k \) is a Mersenne prime, \( \frac{M_k(M_k + 1)}{2} \) is perfect).

Perfect numbers are numbers that are equal to the sum of their proper factors, for example \( 6 = 1 \cdot 2 \cdot 3 = 1 + 2 + 3 \) is perfect.

Mersenne Primes II

It is an open question as to whether or not there exist odd perfect numbers. It is also an open question whether or not there exist an infinite number of Mersenne primes.

Such primes are useful in testing suites (i.e., benchmarks) for large super computers.

To date, 42 Mersenne primes have been found. The last was found on February 18th, 2005 and contains 7,816,230 digits.

Division

**Theorem (The Division "Algorithm")**

*Let \( a \in \mathbb{Z} \) and \( d \in \mathbb{Z}^+ \) then there exists unique integers \( q, r \) with \( 0 \leq r < d \) such that \( a = dq + r \).*

Some terminology:

- \( d \) is called the *divisor*.
- \( a \) is called the *dividend*.
- \( q \) is called the *quotient*.
- \( r \) is called the *remainder*.

We use the following notation:

\[
q = a \div d \\
r = a \mod d
\]
Greatest Common Divisor I

Definition
Let $a$ and $b$ be integers not both zero. The largest integer $d$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of $a$ and $b$. It is denoted $\gcd(a, b)$.

The $\gcd$ is always guaranteed to exist since the set of common divisors is finite. Recall that 1 is a divisor of any integer. Also, $\gcd(a, a) = a$, thus $1 \leq \gcd(a, b) \leq \min\{a, b\}$.

Greatest Common Divisor

Computing
The $\gcd$ can “easily” be found by finding the prime factorization of two numbers.

Let
\[
\begin{align*}
a &= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \\
b &= p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}
\end{align*}
\]

Where each power is a nonnegative integer (if a prime is not a divisor, then the power is 0). Then the $\gcd$ is simply
\[
\gcd(a, b) = p_1^\min\{a_1, b_1\} p_2^\min\{a_2, b_2\} \cdots p_n^\min\{a_n, b_n\}
\]

\[\text{Easy conceptually, not computationally}\]

Least Common Multiple

Definition
The least common multiple of positive integers $a, b$ is the smallest positive integer that is divisible by both $a$ and $b$. It is denoted $\text{lcm}(a, b)$.

Again, the lcm has an “easy” method to compute. We still use the prime decomposition, but use the max rather than the min of powers.
\[
\text{lcm}(a, b) = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}
\]

Least Common Multiple

Example
What is the lcm(6600, 12740)?

Again, the prime decompositions are
\[
\begin{align*}
6600 &= 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^1 \cdot 13^0 \\
12740 &= 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 11^1 \cdot 13^1
\end{align*}
\]

So we have
\[
\text{lcm}(6600, 12740) = 2^{\max\{3, 2\}} 3^{\max\{1, 0\}} 5^{\max\{1, 1\}} 7^{\max\{2, 0\}} 11^{\max\{1, 1\}} 13^{\max\{0, 1\}} = 4 \cdot 204 = 204
\]
**Intimate Connection**

There is a very close connection between the gcd and lcm.

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let ( a, b \in \mathbb{Z}^+ ), then ( ab = \gcd(a, b) \cdot \text{lcm}(a, b) )</td>
</tr>
</tbody>
</table>

**Proof?**

---

**Congruences**

**Definition**

Often, rather than the quotient, we are only interested in the remainder of a division operation. We introduced the notation before, but we formally define it here.

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let ( a, b \in \mathbb{Z} ) and ( m \in \mathbb{Z}^+ ). Then ( a ) is congruent to ( b ) modulo ( m ) if ( m ) divides ( a - b ). We use the notation ( a \equiv b \pmod{m} )</td>
</tr>
</tbody>
</table>

If the congruence does not hold, we write \( a \not\equiv b \pmod{m} \)

---

**Inverses I**

**Definition**

An inverse of an element \( x \) modulo \( m \) is an integer \( x^{-1} \) such that \( xx^{-1} \equiv 1 \pmod{m} \)

Inverses do not always exist, take \( x = 5, m = 10 \) for example.

The following is a necessary and sufficient condition for an inverse to exist.

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let ( a ) and ( m ) be integers, ( m &gt; 1 ). A (unique) inverse of ( a ) modulo ( m ) exists if and only if ( a ) and ( m ) are relatively prime.</td>
</tr>
</tbody>
</table>