Intro to Discrete Structures
Lecture 12

Pawel M. Wocjan

School of Electrical Engineering and Computer Science

University of Central Florida

wocjan@eecs.ucf.edu

Division

Definition 1: If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say that a **divides** b if there exists $c \in \mathbb{Z}$ such that $b = ac$.

When a divides b we say that a is a **factor** of b and that b is a multiple of a.

The notation $a \mid b$ denotes that a divides b. We write $a \not| b$ if a does not divide b.

$$a \mid b \quad \text{if and only if} \quad \exists c\,(ac = b)$$

Integers Divisible by d

Example 2: Let n and d be positive integers. How many positive integers not exceeding n are divisible by n?

Integers Divisible by d

Example 2: Let n and d be positive integers. How many positive integers not exceeding n are divisible by n?

This equals the number of integers k with

$$0 < dk \leq n, \quad \text{or equivalently, with} \quad 0 < k \leq n/d\,.$$

Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

Properties of the Divides Relation

Theorem 1: Let a, b, and c be integers. Then

$$a \mid b \quad \wedge \quad a \mid c \quad \Rightarrow \quad a \mid b + c$$

$$a \mid b \quad \Rightarrow \quad \forall c\,(a \mid bc)$$

$$a \mid b \quad \wedge \quad b \mid c \quad \Rightarrow \quad a \mid c$$

Corollary 1:

$$a \mid b \quad \wedge \quad a \mid c \quad \Rightarrow \quad \forall m \forall n\,(a \mid mb + nc)$$

The Division Algorithm

Theorem 2: Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Quotient

$$q = a \operatorname{div} d = \lfloor a/d \rfloor$$

Remainder

$$r = a \bmod d = a - dq$$

Modular Arithmetic

Definition 3: If a and b are integers and m is a positive integer, then a is **congruent** b **modulo** m if m divides $a - b$.

We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m.

If there are not congruent, then we write $a \not\equiv b \pmod{m}$

$$a \equiv b \pmod{m} \quad \text{if and only if} \quad m \mid a - b$$

Modular Arithmetic

Modular Arithmetic

Modular Arithmetic

Modular Arithmetic

Primes

Definition 1: A positive integer p greater than 1 is called **prime** if the only positive integers of p are 1 and p.

A positive integer p greater than 1 and is not prime is called **coprime**.

`http://en.wikipedia.org/wiki/Prime_number`

The Fundamental Theorem of Arithmetic

Theorem 1: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Bound on Largest Prime Factor

Theorem 2: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

The Infinitude of Primes

Theorem 3: There are infinitely many primes.

Greatest Common Divisor

Definition 2: 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 by $\gcd(a, b)$.

Least Common Multiple

Definition 5: Let a and b be integers, not both zero. The smallest positive d such that $a \mid d$ and $b \mid d$ is called the **smallest common multiple** of a and b.

It is denoted by $\mathrm{lcm}(a, b)$.

Prime Factorization/Gcm/Lcm

Let a and b be two positive integers and

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} = \prod_{j=1}^{n} p_j^{e_j}$$

$$b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n} = \prod_{j=1}^{n} p_j^{f_j}$$

their prime factorizations.

Prime Factorization/Gcm/Lcm

Then, the greatest common divisor and the least common multiple are given by

$$\begin{aligned}
\gcd(a,b) &= p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_n^{\min(e_n,f_n)} = \prod_{j=1}^{n} p_j^{\min(e_j,f_j)} \\
\operatorname{lcm}(a,b) &= p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_n^{\max(e_n,f_n)} = \prod_{j=1}^{n} p_j^{\max(e_j,f_j)}
\end{aligned}$$

We also have the identity

$$ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)\,.$$

The Euclidean Algorithm

Lemma 1: Let

$$a = bq + r$$

where a, b, q, and r are integers. Then

$$\gcd(a, b) = \gcd(b, r)\,.$$

The Euclidean Algorithm

The Euclidean Algorithm

Example 12: Find $\gcd(414, 662)$ using the Euclidean Algorithm.

Some Useful Facts

Theorem 1:

$$\forall a \, \forall b \, \exists s \, \exists t \; \gcd(a, b) = sa + tb \, .$$

The pair (s, t) can be efficiently computed with the extended Euclidean algorithm.

Some Useful Facts

Lemma 2: If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Some Usful Facts

Lemma 1:

$$\gcd(a, b) = 1 \ \wedge \ a \mid bc \ \Rightarrow a \mid c$$

Proof of the uniqueness of the prime factorization of a positive integer:

Mathematical Induction