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.

$a \nmid b$

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

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

$2 \nmid 7$ $\qquad$ $2 \mid 10$

Integers Divisible by d

Example 2: Let n and d be positive integers. How many positive integers not exceeding n are divisible by $\cancel{n}$?

d

Integers Divisible by d

Example 2: Let n and d be positive integers. How many positive integers not exceeding n are divisible by $\cancel{n}$ d?

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.

$n = 11 \quad d = 3$

$3 \quad 6 \quad 9 \;|\; 12 \;|\; 15 \qquad \left\lfloor \frac{11}{3} \right\rfloor = \left\lfloor 3\,\frac{2}{3} \right\rfloor = 3$

Properties of the Divides Relation

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

$(a \mid b) + c$

$$a \mid b \quad \wedge \quad a \mid c \;\Rightarrow\; a \mid (b + c)$$

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

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

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

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

$a = 11$ $q = 3$ $r = 2$

$d = 3$

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 $a \not\equiv b \pmod{m}$

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

$a \bmod m =$
$b \bmod m$

Modular Arithmetic

Theorem 3

$a \equiv b \pmod{m}$ iff

$a \bmod m = b \bmod m$

Theorem 4

$a \equiv b \pmod{m}$ iff $\exists k : a + km = b$

Modular Arithmetic

Theorem 5

$a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$

$a + c \equiv b + d \pmod{m}$

$ac \equiv bd \pmod{m}$

Modular Arithmetic

Corollary 2

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$7 + 9 = 16 \qquad 16 \equiv 1 \pmod 3$$

$$7 \equiv \boxed{1} \pmod 3$$

$$9 \equiv \boxed{0} \pmod 3$$

$$+ \downarrow$$

$$1$$

Modular Arithmetic

$$4^{102} \pmod{3}$$

$$10! \equiv 0 \pmod{3}$$

$$1 \cdot 2 \cdot \underset{\equiv}{3} \cdot 4 \cdots 10$$

Primes

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

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

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

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11

~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17

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.

$$18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$$

Bound on Largest Prime Factor

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

n composite $\qquad n = a \cdot b$

we show that we must have

$a \leq \sqrt{n} \lor b \leq \sqrt{n}$

$a > \sqrt{n} \land b > \sqrt{n}$

$\Rightarrow \quad a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$

The Infinitude of Primes

Theorem 3: There are infinitely many primes.

Assume that there is only a finite number of primes, say, $p_1, p_2, \ldots, p_n$

Consider

$q = p_1 p_2 \cdots p_n + 1$ prime ↯

assume q is not prime $\Rightarrow$ q composite

$q = p_1 p_2 \cdots p_n + 1$ mod p_i

$q \equiv 1$ mod p_i

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 $\gcd(a, b)$.

$\gcd(24, 36) = 12$

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**~~ least **common multiple** of a and b.

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

$$\operatorname{lcm}(24, 36) = 72$$

$$24 = 2^3 \cdot 3$$
$$36 = 2^2 \cdot 3^2$$

$$\Rightarrow \gcd \; 2^2 \cdot 3 = 12$$
$$\operatorname{lcm} \; 2^3 \cdot 3^2 = 72$$

Prime Factorization/Gc~~m~~d/Lcm

Let a and b be two positive integers and

$$\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} = \prod_{j=1}^{n} p_j^{e_j} \\ b &= p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n} = \prod_{j=1}^{n} p_j^{f_j} \end{aligned}$$

their prime factorizations.

Prime Factorization/Gcm/Lcm

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

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

$$\mathrm{lcm}(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_n^{\max(e_n,f_n)} = \prod_{j=1}^{n} p_j^{\max(e_j,f_j)}$$

$\max(e_i,f_i) + \min(e_i,f_i)$

p_i

$= p^{e_i+f_i}$

We also have the identity

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

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