

Discrete Mathematical Structures CS 3233 Lecture 23

Prof. William Winsborough
October 28, 2005

Business

- Assignment 8:
Section 2.4: 2, 4, 6, 14, 16, 28, 30, 40
- Any questions from the last homework?

28 October 2005

Winsborough CS 3233 Lecture 23

2

Division

- Let a and b be integers, $a \neq 0$
 - a *divides* b if there is an integer c such that $b=ac$
 - In this case, we write $a \mid b$ and say a is a *factor* of b and that b is a *multiple* of a
- Note that $a \mid b \equiv \exists c(ac=b)$

28 October 2005

Winsborough CS 3233 Lecture 23

3

Theorem

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 integers c
 3. If $a \mid b$ and $b \mid c$, then $a \mid c$
- Corollary:
If a , b , and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for all integers m and n

28 October 2005

Winsborough CS 3233 Lecture 23

4

Primes

- A positive integer $p > 1$ is called *prime* if the only positive factors of p are 1 and p
- A positive integer $p > 1$ is called *composite* if it is not prime

28 October 2005

Winsborough CS 3233 Lecture 23

5

The Fundamental Theorem of Arithmetic

- Every positive integer $p > 1$ can be written uniquely as a prime or as the product of two or more primes, in which the prime factors are written in non-decreasing order
 - $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$
 - $641 = 641$

28 October 2005

Winsborough CS 3233 Lecture 23

6

Size of Least Prime Factor

- Theorem:
If n is a composite integer, then n has a prime factor less than or equal to \sqrt{n}

Infinitude of Primes

- Theorem:
There are infinitely many primes

The Prime Number Theorem

- The ratio of the number of primes not exceeding x and $x/(\ln x)$ approaches 1 as x grows without bound
 - $\ln x$ is the natural log of x

The Division Algorithm

- The algorithm that isn't an algorithm:
- Theorem:
Let a and d be integers with $d > 1$
 - There are unique integers q and r with $0 \leq r < d$, such that $a = dq + r$
 - d is the *divisor*, a is the *dividend*, q is the *quotient*, and r is the *remainder*
 - $q = a \text{ div } d$
 - $r = a \text{ mod } d$

Greatest Common Divisor

- Let a and b be integers, not both zero
 - The largest d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor*
 - $d = \text{gcd}(a, b)$
- a and b are *relatively prime* if their greatest common divisor is 1