

SFU MACM-101-D3 2004-2 week 12

Manuel Zahariev

E-mail: manuelz@cs.sfu.ca

November 25, 2004

Revision : 1.4

Division

Definition 1 (Division) For $a, b \in \mathbb{Z}$ and $b \neq 0$, b is said to **divide** a (written $b|a$) iff $\exists n \in \mathbb{Z}$ so that $a = bn$.

Lemma 1

$$\forall a, b, c \in \mathbb{Z} \forall x, y \in \mathbb{Z} (a|b \wedge a|c) \Rightarrow (a|bx + cy)$$

Prime numbers

Definition 2 (Prime, composite) *A number $p \in \mathbb{Z}^+$, $p \neq 1$ for which $\forall x \in \mathbb{Z} \ x|p \rightarrow x \in \{-p, -1, 1, p\}$ (called the set of *trivial divisors*) is called **prime number**.*

*An number in \mathbb{Z}^+ , not 1 which is not prime is said to be **composite**.*

Lemma 2

$\forall n \in \mathbb{Z}^+$ *composite* $\exists p$ *prime* so that $p|n$

(Every composite number has at least one prime divisor)

Proof: contradiction.

Theorem 1 *There are infinitely many primes.*

Proof: contradiction

The Division Theorem

Theorem 2 $\forall a, b \in \mathbb{Z}$ where $b \neq 0 \exists q, r \in \mathbb{Z}$ unique so that $a = qb + r$ and $0 \leq r < b$

Proof: by cases, using the well ordering principle (axiom) for \mathbb{Z}^+

Definition 3 :

- q is called **quotient**
- r is called **remainder**
- $r = a \bmod b$
- $q = a \div b$

Greatest Common Divisor

Definition 4 (gcd) *Considering $a, b \in \mathbb{Z}^+$, a number $d \in \mathbb{Z}^+$ is said to be the greatest common divisor of a and b (written $\gcd(a, b)$) iff:*

1. $d|a$ and $d|b$
2. $\forall e \ e|a \wedge e|b \Rightarrow e|d$

Lemma 3 (gcd existence, uniqueness) $\forall a, b \in \mathbb{Z}^+$, *there is exactly one d which is the $\gcd(a, b)$.*

Proof (2-part):

1. existence (using the principle of well-ordering)
2. uniqueness (by contradiction)

Least Common Multiple

Definition 5 (lcm) *Considering $a, b \in \mathbb{Z}^+$, a number $m \in \mathbb{Z}^+$ is said to be the least common multiple of a and b (written $\text{lcm}(a, b)$) iff:*

1. $a|m$ and $b|m$
2. $\forall n \in \mathbb{Z} \ a|n \wedge b|n \Rightarrow m|n$

Theorem 3

$$\forall a, b \in \mathbb{Z}^+ \ a \cdot b = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$$

Theorem 4 (Unique factorization) $\forall a \in \mathbb{Z}^+$ *composite*

$\exists \{(p_i)_{i \in 1..n}, (e_i)_{i \in 1..n}\}$ *unique,*

where $\forall i \in 1..n$ p_i *is prime,* $e_i \in \mathbb{N}^*$

and $\forall i \in 1..n - 1$ $p_i < p_{i+1}$ *so that:*

$$a = \prod_{i=1}^n p_i^{e_i}$$

(There is a unique way to write any positive integer as a product of prime numbers)

Proof (two-part):

1. existence
2. uniqueness