Number Theory

Slides by Christopher M. Bourke
Instructor: Berthe Y. Choueiry

Fall 2007

Computer Science & Engineering 235
Introduction to Discrete Mathematics
Sections 3.4–3.6 of Rosen

Introduction I

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

Definition

Let $a, b \in \mathbb{Z}, a \neq 0$, we say that a *divides* b if there exists $c \in \mathbb{Z}$ such that $b = ac$. We denote this, $a \mid b$ and $a \nmid b$ when a does not divide b. When $a \mid b$, we say a is a *factor* of b.

Theorem

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 $a \mid c$.*

Introduction II

Corollary

If $a, b, c \in \mathbb{Z}$ *such that* $a \mid b$ *and* $a \mid c$ *then* $a \mid mb + nc$ *for* $n, m \in \mathbb{Z}$.