# Ciencias de la Computación I

## Tópicos de Teoría de Números

Eduardo Contrera Schneider

Universidad de la Frontera

12 de octubre de 2016

# Divisibilidad

## Divisibilidad

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimo que $b$ divide a $a$, y lo denotamos $b|a$, si existe un entero $n$ tal que $a = bn$. Cuando esto ocurre, decimos que $b$ es un divisor de $a$, o que $a$ es un múltiplo de $b$.

Esta definición nos permite hablar de división sin tener que extender el conjunto a los números racionales. Además, cuando $ab = 0$ para $a, b \in \mathbb{Z}$ entonces $a = 0$ o $b = 0$; decimos entonces que $\mathbb{Z}$ no tiene divisores propios de 0. Esta propiedad permite cancelar en $\mathbb{Z}$

# Propiedades de la División

## Propiedades

Para cualesquiera $a, b, c \in \mathbb{Z}$

1. $1|a$ y $a|0$.
2. Si $a|b$ y $b|a$ entonces $a = \pm b$.
3. Si $a|b$ y $b|c$ entonces $a|c$.
4. Si $a|b$ entonces $a|bx$ para todo $x \in \mathbb{Z}$.
5. Si $x = y + z$ para $x, y, z \in \mathbb{Z}$ y $a$ divide a dos de los enteros $x, y, z$, entonces $a$ divide al entero restante.
6. Si $a|b$ y $a|c$ entonces $a|(bx + cy)$, para todos $x, y \in \mathbb{Z}$.
7. Para $1 \leq i \leq n$, sea $c_i \in \mathbb{Z}$. Si $a|c_i$ para todo $i$, entonces $a|(c_1x_1 + c_2x_2 + \ldots + c_nx_n)$ donde $x_i \in \mathbb{Z}$ para todo $1 \leq i \leq n$.

## Ejemplos

- ¿Existen enteros $x, y, z$ (positivos, negativos o cero) tales que $6x + 9y + 15z = 107$?
- Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide $9a + 5b$.

# Números Primos

Cuando observamos detenidamente el conjunto $\mathbb{Z}^+$, nos damos cuenta que cualquier número mayor a 1 tiene al menos dos divisores.

## Números Primos

Sea $n \in \mathbb{Z}^+$ y $n > 1$. Decimos que $n$ es un número **primo** tiene exactamente dos divisores positivos. De lo contrario, el número se llama **compuesto**.

El siguiente lema relaciona los dos tipos de números.

## Lema

Si $n \in \mathbb{Z}^+$ y $n$ es compuesto, entonces existe un primo $p$ tal que $p|n$.

# Cardinalidad de los Números Primos

Euclides en los pergaminos con conforman su más célebre obra *Elementos*, demostró por primera vez el siguiente resultado.

**Teorema**

Existe una infinitud de números primos.

**División Euclidiana**

Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = qb + r$, con $0 \leq r < b$.

Además, llamamos al entero $b$ el divisor y a $a$ el dividendo.