MATEMÁTICA DISCRETA

Bloque 2

LOS ENTEROS

Transparencias

Lección 1. Los números enteros.
Lección 2. Congruencias. Aritmética modular.

ESTRUCTURAS ALGEBRAICAS

Grupo

Sea A un conjunto, + una ley de composición.
(A,+) será un Grupo si (IANS)

- + es una ley de composición **I**nterna
- + es una ley **A**sociativa
- existe un elemento **N**eutro para +
- cada elemento de A tiene un elemento **S**imétrico para la ley +. (opuesto)

(A,+) será un Grupo Conmutativo (o Abeliano 1802-1829) si + es Conmutativa.

Anillo

Sea A un conjunto, + y • dos leyes de composición.
(A,+,•) será un Anillo si

- (A;+) es un Grupo Conmutativo
- • es una ley de composición Interna
- • es una ley Asociativa
- • es distributiva sobre + en ambos lados.

(A,+,•) será un Anillo Conmutativo si • es Conmutativa
(A,+,•) será un Anillo Unitario si existe un elemento Neutro para •
(A,+,•) será un Anillo Íntegro (o Dominio de Integridad) si no existen divisores de cero.

Cuerpo

Sea A un conjunto y +,• dos leyes de composición.
(A,+,•) será un Cuerpo si

- (A,+,•) será un Anillo Conmutativo
- cada elemento de A tiene un elemento Simétrico para la ley •. (Inverso)

MATEMÁTICA DISCRETA

Bloque 2

LOS ENTEROS

Transparencias

Lección 1.

LOS NUMEROS ENTEROS

1. Los enteros. Principio de la buena ordenación.
2. Divisibilidad.
3. Máximo común divisor y mínimo común múltiplo.
4. Números primos. Factorización.

1. LOS ENTEROS. PRINCIPIO DE LA BUENA ORDENACION.

Definición El conjunto $\mathbb{Z}$ verifica los siguientes axiomas:

A1 Hay definidas dos operaciones binarias $+$ y $\cdot$

A2 Son conmutativas

A3 Son asociativas

A4 Existe elemento neutro para cada una de ellas

A5 $\cdot$ es distributiva respecto de $+$

A6 $\forall a \in \mathbb{Z}\ \exists! (-a) \in \mathbb{Z}\ /\ a + (-a) = 0$

A7 Si $a \neq 0$ y $a \cdot b = a \cdot c$, entonces $b = c$

Existe en $\mathbb{Z}$ una relación $\leq$ que verifica:

A8 Es reflexiva

A9 Es antisimétrica

A10 Es transitiva

A11 Si $a \leq b$, entonces $a + c \leq b + c$

A12 Si $a \leq b$ y $0 \leq c$, entonces $a \cdot c \leq b \cdot c$

A13 Si X es un subconjunto no vacío y acotado inferiormente, entonces X posee mínimo.

2. DIVISIBILIDAD

Teorema (Algoritmo de la división)
Sean a, b dos enteros. Si b no es nulo, existen dos únicos enteros q, r verificando

$$a = b \cdot q + r \text{ y } 0 \leq r < |b|.$$

Definición
El cálculo de q y r en el teorema anterior se llama **división euclídea** de a por b; el número q es el **cociente** de la división, y r es el **resto**.

APLICACIÓN: REPRESENTACIÓN EN BASE t DE UN ENTERO

Sea $t \geq 2$ un entero (**base para el cálculo**). Para cualquier $x \in \mathbb{Z}$, por aplicación reiterada del algoritmo de la división, tenemos:

$$\begin{aligned} x &= t \cdot q_0 + r_0 \\ q_0 &= t \cdot q_1 + r_1 \\ q_1 &= t \cdot q_2 + r_2 \\ &\cdots \\ &\cdots \\ q_{n-2} &= t \cdot q_{n-1} + r_{n-1} \\ q_{n-1} &= t \cdot q_n + r_n \end{aligned}$$

con $r_i \in \mathbb{Z}$ / $0 \leq r_i \leq t-1,\ i = 0, 1, 2, \ldots, n$.
Si paramos cuando $q_n = 0$, obtenemos, eliminando los cocientes q_i:

$$x = r_n \cdot t^n + r_{n-1} \cdot t^{n-1} + \cdots + r_1 \cdot t + r_0.$$

Hemos representado x en base t:

$$x = (r_n r_{n-1} \cdots r_1 r_0)_t.$$

Convencionalmente $t = 10$ es la base usual y generalmente omitimos de dicha representación el subíndice $t = 10$. Por ejemplo

$$1432 = 1 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0.$$

Veamos cuál es la representación en base 2 de $(109)_{10}$:

$$\begin{aligned} 109 &= 2 \cdot 54 + 1 \\ 54 &= 2 \cdot 27 + 0 \\ 27 &= 2 \cdot 13 + 1 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

Así

$109 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1.$

Y su representación en base 2 es:

$$(1101101)_2$$

Definición
Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Se dice que b **divide a** a, b es un **divisor de** a, o que a es un **múltiplo de** b y lo representamos por b/a, si existe un entero q tal que $a = b \cdot q$.

Proposición Sean $a, b, c \in \mathbb{Z}$.

1. $1/a,\ a/0,\ a/a$

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 $a/bx,\ \forall x \in \mathbb{Z}$

5. Si a/b y a/c, entonces $a/(bx + cy),\ \forall x, y \in \mathbb{Z}$

3. MÁXIMO COMÚN DIVISOR. MÌNIMO COMÚN MULTIPLO

Definición
Sean $a, b \in \mathbb{Z}$, donde al menos uno de ellos es no nulo. Entonces, $c \in \mathbb{Z}$ se denomina **máximo común divisor** (mcd) de a, b si

1. c/a y c/b

2. Si d/a y d/b entonces d/c

Teorema
Para cualesquiera $a, b \in \mathbb{Z}^+$, existe un $c \in \mathbb{Z}^+$ único, que es el máximo común divisor de a y b.

Observación
mcd(a, b)=mcd($-a, b$)=mcd($a, -b$)=mcd($-a, -b$)

Definición

Los enteros a, b se denominan **primos entre sí**, cuando mcd(a, b)=1.

Corolario

Sean $a, b \in \mathbb{Z}$ y $d =$mcd(a, b). Entonces

$$\exists s, t \in \mathbb{Z} \ / \ \mathrm{d} = \mathrm{as} + \mathrm{bt}.$$

Teorema (Algoritmo de Euclides)

Si $a, b \in \mathbb{Z}$ y se aplica el algoritmo de la división:

$$\begin{array}{rcl}
a & = & q_1 b + r_1 \quad 0 < r_1 < b \\
b & = & q_2 r_1 + r_2 \quad 0 < r_2 < r_1 \\
r_1 & = & q_3 r_2 + r_3 \quad 0 < r_3 < r_2 \\
 & \ldots & \\
r_i & = & q_{i+2} r_{i+1} + r_{i+2} \quad 0 < r_{i+2} < r_{i+1} \\
 & \ldots & \\
r_{k-2} & = & q_k r_{k-1} + r_k \quad 0 < r_k < r_{k-1} \\
r_{k-1} & = & q_{k+1} r_k
\end{array}$$

Entonces, r_k el último resto distinto de cero es igual al mcd(a, b).