Bloque 2. ARITMÉTICA ENTERA Y MODULAR

Bloque 2. ARITMÉTICA ENTERA Y MODULAR

MOTIVACIÓN

La aritmética entera y modular tiene multitud de aplicaciones a la informática y otras áreas.

Ejemplos de áreas de aplicación:

- **Representación de enteros en una cierta base**: Se justifica a partir del algoritmo de la división.
- **Sistemas de cifrado y descifrado**: Los números primos, la factorización y la aritmética modular se usan en sistemas criptográficos.
- **Números pseudoaleatorios**: La aritmética modular ayuda a crear funciones que "aparentan" generar números aleatorios.

Bloque 2. ARITMÉTICA ENTERA Y MODULAR

- **Computación con números grandes**: Es posible usar la aritmética entera para realizar operaciones con números grandes que sobrepasan cierta capacidad.
- **Dígitos de control**: Los dígitos de control de NIF, ISBN o cuentas corrientes se obtienen mediante aritmética modular.
- **Música y artes visuales**: Por ejemplo, el "Cuarteto para el fin de los tiempos", del compositor del siglo XX Olivier Messiaen. En esta pieza, Messiaen crea una sensación de tensión mediante el empleo de una secuencia de números primos.

Índice

Lección 1.
LOS NÚMEROS ENTEROS

1. LOS ENTEROS. PRINCIPIO DE LA BUENA ORDENACION.

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

- **A1.** Hay definidas dos operaciones binarias + y ·
- **A2.** Son conmutativas.
- **A3.** Son asociativas.
- **A4.** Existe elemento neutro para cada una de ellas.
- **A5.** · 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.

1. LOS ENTEROS. PRINCIPIO DE LA BUENA ORDENACION.

DEFINICIÓN: Sea ***X*** un subconjunto de un conjunto ***A***.

● Se dice que ***X*** está **acotado inferiormente** si

$$\exists a \in A \;\; / \;\; a \leq x \;\; \forall x \in X$$

Eneste caso, el elemento ***a*** se denomina una cota inferior de ***X***.

Ejemplo: En el conjunto de los números reales, ***R***:

- Cotas inferiores de [0,1]: 0,-1,-2,-2.5,... **ÍNFIMO: 0** **MÍNIMO: 0**
- Cotas inferiores de]0,1]: 0,-1,-2,-2.5,... **ÍNFIMO: 0** **NO HAY MÍNIMO**
- El subconjunto]-∞ ,0] no está acotado inferiormente.

● Sea ***X*** un conjunto acotado inferiormente. Llamaremos **ínfimo** a la mayor de todas las cotas inferiores.

● Sea ***X*** un conjunto acotado inferiormente. Diremos que ***X*** posee **mínimo** si el ínfimo pertenece al conjunt ***X***.

2. DIVISIBILIDAD

TEOREMA (Algoritmo de la división)

Sean a, b dos enteros. Si b no es nulo, existen dos únicos enteros q, r verificando $a = b \cdot q + r$, con $0 \leq r < |b|$.

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**.

EJEMPLO:

La división euclídea de a=27 por b=4, produce como cociente q=6 y como resto r=3.

$$27 = 4 \cdot 6 + 3$$

La división euclídea de a=27 por b=-4, produce como cociente q=-6 y como resto r=3.

$$27 = (-4) \cdot (-6) + 3$$

2. DIVISIBILIDAD

APLICACIÓN: REPRESENTACIÓN EN BASE t DE UN ENTERO

Sea t ≥ 2 un entero (base para el cálculo).

Para cualquier entero x, por aplicación reiterada del algoritmo de la división, tenemos:

$$\left\{\begin{array}{rcl} x & = & t\cdot q_0 + r_0 \\ q_0 & = & t\cdot q_1 + r_1 \\ q_1 & = & t\cdot q_2 + r_2 \\ & & \dots \\ & & \dots \\ q_{n-2} & = & t\cdot q_{n-1} + r_{n-1} \\ q_{n-1} & = & t\cdot q_n + r_n \end{array}\right.$$

Con:

$$r_i \in \mathbb{Z} \;/\; 0 \leq r_i \leq t-1,\; i = 0,1,2,\dots,n.$$

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:

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

2. DIVISIBILIDAD

EJEMPLO:

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

Y su representación en base 2 es: $(1101101)_2$

2. DIVISIBILIDAD

DEFINICIÓN:
Sean $a, b \in \mathbb{Z}$, con b no nulo. Se dice que:

- b **divide** al entero 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

$$a = b \cdot q.$$

EJEMPLO:
7 es un divisor de 63, ya que 63=7·9. Diremos también que 7 divide a 63, o que 63 es un múltiplo de 7.
Por el contrario, 8 no es divisor de 63 ya que:

$$\nexists q \in \mathbb{Z} \;/\; 63 = 8 \cdot q$$

2. DIVISIBILIDAD

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. MÍNIMO COMÚN MÚLTIPLO

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 existe un entero d, tal que d|a y d|b, entonces d|c.

EJEMPLO:

El máximo común divisor de a=60 y b=84 es d=12, ya que:

1. 12 es un divisor común de 60 y de 84 (60=12·5 y 84=12·7)
2. Los divisores comunes de 60 y 84 son los elementos del conjunto:

$$D=\{-12,-6,-4,-3,-2,-1,1,2,3,4,6,12\}$$

Cualquier elemento de este conjunto es un divisor de 12.

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

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

$$\text{mcd}(a,b) = \text{mcd}(-a,b) = \text{mcd}(a,-b) = \text{mcd}(-a,-b)$$

EJEMPLO:

$$\text{mcd}(8,24) = \text{mcd}(-8,24) = \text{mcd}(8,-24) = \text{mcd}(-8,-24)=4$$

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

DEFINICIÓN:

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

EJEMPLO:

15 y 8 son primos entre sí porque mcd(15,8)=1.

COROLARIO (Identidad de Bezout)

Sean a,b $\in \mathbb{Z}$ y d=mcd(a, b). Entonces $\exists$ s,t $\in \mathbb{Z}$ / d=as + bt.

EJEMPLO:

Sean a=21 y b=35. El mcd(21,35)=7.

Podemos tomar s=2 y t =-1 y tenemos que 7=21·2+35·(-1).

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

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

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

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

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

EJEMPLO:

Vamos a aplicar el algoritmo de Euclides para calcular el máximo común divisor de 791 y 336. Aplicaremos el algoritmo de la división a los enteros iniciales y después iremos dividiendo divisor entre resto hasta obtener un resto nulo.

$$
\begin{array}{ll}
791=2\cdot 336+119, & 0<119<336 \\
336=2\cdot 119+98, & 0<98<119 \\
119=1\cdot 98+21, & 0<21<98 \\
98=4\cdot 21+14, & 0<14<21, \\
21=1\cdot 14+7, & 0<7<14, \\
14=2\cdot 7 &
\end{array}
$$

Por lo tanto, el mcd (791,336)=7.

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

EJEMPLO: Además, podemos utilizar las ecuaciones anteriores para expresar 7 como combinación lineal de 791 y 336, es decir, para encontrar una solución de la identidad de Bezout

$$791s+336t=7.$$

$791=2\cdot336+119,$

$336=2\cdot119+98,$

$119=1\cdot98+21,$

$98=4\cdot21+14,$

$21=1\cdot14+7,$

$14=2\cdot7$

$$\begin{aligned} 7 &= 21 - 1\cdot14 \\ &= 21 - (98 - 4\cdot21) = 5\cdot21 - 98 \\ &= 5(119 - 1\cdot98) - 98 = 5\cdot119 - 6\cdot98 \\ &= 5\cdot119 - 6(336 - 2\cdot119) = 17\cdot119 - 6\cdot336 \\ &= 17(791-2\cdot336) - 6\cdot336 = 791\cdot17+336\cdot(-40) \end{aligned}$$

Así la solución de la identidad de Bezout es $s=17$ y $t=-40$.

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

DEFINICIÓN:

Sean $a,b \in \mathbb{Z}$ y $c \in \mathbb{Z}^+$. Se denomina ecuación diofántica a la ecuación $ax+by = c$, donde $x,y \in \mathbb{Z}$ son incógnitas.

TEOREMA

Sean $a,b \in \mathbb{Z}$, $c \in \mathbb{Z}^+$ y $d=mcd(a,b)$. La ecuación diofántica $ax+by = c$ tiene solución entera si, y sólo si, $d|c$, es decir, si $c = k \cdot d$, $k \in \mathbb{Z}$.

EJEMPLO:

El mcd(791,336)=7. Podemos asegurar que la ecuación diofántica $791x+336y=7$ tiene solución entera porque 7 es divisor de sí mismo (Sol.: $x=17$, $y=-40$).

Sin embargo $791x+336y=22$ no tiene solución entera porque 22 no es múltiplo de 7.

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

OBSERVACIÓN

Es obvio que obtenida una solución entera que verifique la identidad de Bezout,

$$ax+by=d,\ d=mcd(a,b)\ (x=x_0,\ y=y_0),$$

tendremos también una solución entera de la ecuación

$$ax+by=c,\ c=k\cdot d,$$

sin más que considerar $x=k\cdot x_0$, $y=k\cdot y_0$.

EJEMPLO:

Dado que se cumple

$$791x+336y=7 \quad \text{con} \quad x=17 \text{ e } y=-40$$

tendremos que la ecuación diofántica

$$791x+336y=28$$

tendrá como soluciones ($28=4\cdot7$):

$$x=4\cdot17=68 \text{ e } y=4\cdot(-40)=-160.$$

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

TEOREMA

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

Sean $\alpha,\beta \in \mathbb{Z}^+$ / a = α·d, b = β·d, y $x_0,y_0 \in \mathbb{Z}$ una solución de la ecuación diofántica:

$$ax+by = d\cdot n$$

Entonces, $x,y \in \mathbb{Z}$ es solución de la anterior ecuación si, y sólo si,

$$\left.\begin{array}{l} x = x_0 + k\beta \\ y = y_0 - k\alpha \end{array}\right\} \; k \in \mathbb{Z}.$$

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

EJEMPLO:

Estudiemos las soluciones de 791x+336y=28.

1. ¿Tiene solución?

Como mcd(791,336)=7, y 7|28, entonces existe solución.

2. Cálculo de una solución particular de 791x+336y=7:

Una solución es (17,-40).

3. Cálculo de una solución particular de 791x+336y=28:

Como 28=4·7, entonces x_0=4·17=68, y_0=4·(-40)=-160.

4. Cálculo de la solución general:

Como 791=113·7 y 336=48·7, entonces α=113 y β=48.

Por tanto, cualquier solución de esta ecuación es de la forma

$$\left.\begin{array}{l} x = 68 + 48\cdot k \\ y = -160 - 113\cdot k \end{array}\right\} \quad k \in \mathbb{Z}$$

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

DEFINICIÓN:
Sean a,b $\in \mathbb{Z}^+$. Diremos que c $\in \mathbb{Z}^+$. es el mínimo común múltiplo de a y b y escribiremos c=mcm(a, b), si c es el menor de los enteros positivos que son múltiplos comunes de a y b.

EJEMPLO: Sean a=550, b=84. Calculemos su mcm:

Múltiplos positivos de a=550: 550·x, x $\in \mathbb{Z}^+$.

Múltiplos positivos de b=84: 84·y, y $\in \mathbb{Z}^+$.

Para encontrar múltiplos comunes: 550x = 84y, x,y $\in \mathbb{Z}^+$.

Cuya solución es: x=42k, y=275k, k $\in \mathbb{Z}^+$.

Con lo que el conjunto de enteros positivos múltiplos comunes de 550 y 84 es:

$$S = \{550(42k)\ /\ k \in \mathbb{Z}^+\} = \{84(275k)\ /\ k \in \mathbb{Z}^+\}.$$

Su elemento mínimo será el mcm: éste se alcanza para k=1, y es

mcm(550,84)=550·42=84·75=23100.

Índice

3. MÁXIMO COMÚN DIVISOR. MÍNIMO COMÚN MÚLTIPLO

TEOREMA

Sean a,b $\in \mathbb{Z}^+$, y c=mcm(a,b).

Si $\exists$ d $\in \mathbb{Z}^+$. tal que a|d y b|d, entonces c|d.

EJEMPLO:

Sea a=550 y b=84. El mcm(550,84)=23100.

Tomemos cualquier entero positivo d que sea múltiplo de 550 y 84. Este conjunto es

$$S = \{550(42k)\ /\ k \in \mathbb{Z}^+\} = \{84(275k)\ /\ k \in \mathbb{Z}^+\}.$$

Y por tanto d será de la forma d=23100·k, es decir, d es también un múltiplo del mcm(550,84).

4. NUMEROS PRIMOS. FACTORIZACION

DEFINICIÓN:
Diremos que p $\in \mathbb{Z}^+$ es primo si tiene exactamente dos divisores positivos distintos.

EJEMPLO: Los divisores positivos de 13 son 1 y 13. Luego 13 es primo.

TEOREMA
Si a es un entero estrictamente mayor que 1, su menor divisor estrictamente mayor que 1 es un número primo.

EJEMPLO: Sea a=25. Su menor divisor estrictamente mayor que 1 es 5. 5 es un número primo.

4. NUMEROS PRIMOS. FACTORIZACION

TEOREMA

Todo elemento de $\mathbb{Z}^+$ mayor o igual que 2, es un número primo o es un producto de números primos. Esta descomposición es única salvo el orden.

DEFINICIÓN:

El cálculo de los números primos cuyo producto coincide con un número entero dado n, se llama descomposición en factores primos de n.

EJEMPLO: Sea n=2200. 2200 no es primo

Su descomposición en factores primos es $2200=2^3\cdot5^2\cdot11$.

Entero / cocientes	2200	1100	550	275	55	11	1
Menor divisor > 1	2	2	2	5	5	11	

4. NUMEROS PRIMOS. FACTORIZACION

TEOREMA

Sean a,b $\in \mathbb{Z}^+$ y

$$a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}, \ \ b = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t},$$

con cada p_i primo y e_i, $r_i \geq 0$, $1 \leq i \leq t$.

Entonces, si

$$a_i = \min\{e_i, r_i\}, \quad b_i = \max\{e_i, r_i\}, \quad 1 \leq i \leq t,$$

se obtiene que

$$\operatorname{mcd}(a, b) = \prod_{i=1}^{t} p_i^{a_i}, \quad \operatorname{mcm}(a, b) = \prod_{i=1}^{t} p_i^{b_i}$$

4. NUMEROS PRIMOS. FACTORIZACION

EJEMPLO:

Sean $a=2200$ y $b=3388$. Sus descomposiciones en factores primos son:

$$2200=2^3\cdot 5^2\cdot 11$$
$$3388=2^2\cdot 7\cdot 11^2$$

que reescritas quedan:

$$2200=2^3\cdot 5^2\cdot 7^0\cdot 11^1$$
$$3388=2^2\cdot 5^0\cdot 7^1\cdot 11^2$$

Por lo tanto:

$$mcd(2200,3388)=2^2\cdot 5^0\cdot 7^0\cdot 11^1=2^2\cdot 11=44,$$

$$mcm(2200,3388)=2^3\cdot 5^2\cdot 7^1\cdot 11^2=169400.$$

4. NUMEROS PRIMOS. FACTORIZACION

TEOREMA

Sean $a,b \in \mathbb{Z}^+$, entonces

$$a \cdot b = \text{mcd}(a,b) \cdot \text{mcm}(a,b).$$

EJEMPLO:

Sean $a=2200=2^3 \cdot 5^2 \cdot 11$ y $b=3388=2^2 \cdot 7 \cdot 11^2$.

$\text{mcd}(2200,3388)=2^2 \cdot 11=44$,

$\text{mcm}(2200,3388)=2^3 \cdot 5^2 \cdot 7 \cdot 11^2=169400$.

Podemos comprobar que:

$$\begin{aligned}2200 \cdot 3388 &= (2^3 \cdot 5^2 \cdot 11) \cdot (2^2 \cdot 7 \cdot 11^2)\\ &= (2^2 \cdot 11) \cdot (2^3 \cdot 5^2 \cdot 7^1 \cdot 11^2)\\ &= \text{mcd}(2200,3388) \cdot \text{mcm}(2200,3388)\end{aligned}$$