Matemática Discreta

Mariam Cobalea

Universidad de Málaga
Dpto. de Matemática Aplicada

Tema 2: Teoría de números

- 2.1 Aritmética entera.
  - Introducción: Axiomática de $\mathbb{Z}$.
  - Algoritmo de la división de dos números enteros. Divisibilidad.
  - Máximo Común Divisor. Algoritmo de Euclides.
  - Algoritmo extendido de Euclides: Identidad de Bezout.
  - Primos. Teorema fundamental de la aritmética.
  - Ecuaciones Diofánticas.
- 2.2 Aritmética modular.

Para cualesquiera $a, b, c \in \mathbb{Z}$, se verifican las siguientes propiedades:

1. Clausura: $a + b \in \mathbb{Z}, \quad a \cdot b \in \mathbb{Z}$
2. Conmutativa: $a + b = b + a, \quad a \cdot b = b \cdot a$
3. Asociativa: $a + (b + c) = (a + b) + c, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
4. Elemento neutro: $\exists\, 0, 1 \in \mathbb{Z},\ a + 0 = a, \quad a \cdot 1 = a$
5. Elemento opuesto: $\forall a \in \mathbb{Z},\ \exists (-a) \in \mathbb{Z},\ a + (-a) = 0$
6. Cancelación: $a \neq 0,\ a \cdot b = a \cdot c \implies b = c$
7. Distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$

La ***diferencia*** de dos enteros se define como $a - b = a + (-b)$

Definición (Ordenación de los enteros)

Las relaciones $<$ *y* $\leq$ *en* $\mathbb{Z}$ *se definen:*

$$\begin{array}{lcl} a < b & \iff & \exists\, 0 \neq n \in \mathbb{N},\ b = a + n \\ a \leq b & \iff & a < b \ \text{ o bien } \ a = b \end{array}$$

Teorema (Propiedades de $\leq$)

Para cualesquiera $a, b, c \in \mathbb{Z}$ *se verifican:*

1. *Reflexiva:* $a \leq a$
2. *Antisimétrica:* si $a \leq b$ y $b \leq a$, entonces $a = b$
3. *Transitiva:* si $a \leq b$ y $b \leq c$, entonces $a \leq c$
4. Si $a \leq b$, entonces $a + c \leq b + c$
5. Si $a \leq b$ y $0 \leq c$, entonces $a \cdot c \leq b \cdot c$

2.1 Aritmética Entera

Definición (Valor absoluto)

El **valor absoluto** *de* $a \in \mathbb{Z}$, *denotado* $|a|$ *se define:*

$$|a| = \begin{cases} a & si\ a \geq 0 \\ -a & si\ a < 0 \end{cases}$$

Teorema (Propiedades)

Para cualesquiera $a, b, c \in \mathbb{Z}$, *se verifican:*

1. $|a| \geq 0$
2. $|a| = 0 \iff a = 0$
3. $|a \cdot b| = |a| \cdot |b|$
4. $|a + b| \leq |a| + |b|$

Teorema (Algoritmo de la división)

Sean $a, b \in \mathbb{N}$, con $b > 0$. Entonces existen únicos $q, r \in \mathbb{N}$ tales que

$$a = b \cdot q + r \quad y \quad 0 \leq r < b$$

- r es el **resto** y
- q es el **cociente** de **a** entre **b**.

Ejemplo $a = 17, \quad b = 3 \qquad\qquad 17 = 3 \cdot 5 + 2$

Demostración:

- Si $b > a$, entonces tomamos $q = 0$ y $r = a$. Por eso, podemos suponer que $b < a$.
- Consideramos el conjunto $S = \{s = a - b \cdot t \geq 0 \quad | \quad t \in \mathbb{N}\}$
  Este conjunto es no vacío, al menos $a \in S$, pues $a = a - b \cdot 0$.
- Así, del Principio de Buena Ordenación se sigue que S tiene un primer elemento. Sea r el primer elemento de S y sea $q \in \mathbb{N}$ tal que $a - b \cdot q = r$.
- Si r no fuese estrictamente menor que **b**, tendríamos $r - b \geq 0$
  y, por tanto, $r - b = a - bq - b = a - b(q + 1)$
- Pero $r - b$ sería un elemento de S estrictamente menor que r , contradiciendo la minimalidad de r.
- Por lo tanto, $0 \leq r < b$.

Teorema (Algoritmo de la división)

Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Entonces existen únicos $q, r \in \mathbb{Z}$ tales que

$$a = b \cdot q + r \quad y \quad 0 \leq r < |b|$$

Demostración: Análoga a la anterior.

- Obsérvese que, aunque los números divididos pueden ser negativos, el resto siempre es **no negativo**: $0 \leq r < |b|$.
- El cociente y el resto en el caso general se determinarán a partir de la división de los correspondientes valores absolutos, añadiendo los signos y corrigiendo el resto de forma adecuada.

Ejemplo $a = -17, \quad b = 3$

Dividiendo 17 entre 3 obtenemos: $\quad 17 = 3 \cdot 5 + 2$; por lo tanto:

$$\begin{aligned}\boxed{-17} &= -3 \cdot 5 - 2 \\ &= \boxed{3} \cdot (-5) - 2 \\ &= \boxed{3} \cdot (-5) + 1 - 3 \\ &= \boxed{3} \cdot (-5 - 1) + 1 \\ &= \boxed{3} \cdot (-6) + 1\end{aligned}$$

De forma análoga, podemos deducir las siguientes:

$$n = 17, \quad m = -3, \quad \Longrightarrow \quad 17 = (-3) \cdot (-5) + 2$$

$$n = -17, \quad m = -3, \quad \Longrightarrow \quad -17 = (-3) \cdot 6 + 1$$

Ejemplo

$$\begin{aligned} a &= 17, & b &= 3 & \qquad 17 &= 3\cdot 5 + 2 \\ a &= 17, & b &= -3 & \qquad 17 &= (-3)\cdot(-5) + 2 \\ a &= -17, & b &= 3 & \qquad -17 &= 3\cdot(-6) + 1 \\ a &= -17, & b &= -3 & \qquad -17 &= (-3)\cdot 6 + 1 \end{aligned}$$

Definición (Divisibilidad)

Sean $\mathbf{a}, \mathbf{b} \in \mathbb{Z}$, *con* $\mathbf{b} \neq 0$. *Se dice que el entero* $\mathbf{b}$ **divide** *al entero* $\mathbf{a}$ *si existe un* $q \in \mathbb{Z}$ *tal que* $\mathbf{a} = \mathbf{b} \cdot q$.

También se dice que:

- $\mathbf{b}$ *es un* **divisor** *de* $\mathbf{a}$ *y se denota* $\mathbf{b}|\mathbf{a}$.
- $\mathbf{a}$ *es un* **múltiplo** *de* $\mathbf{b}$ *y se denota* $\mathbf{a} = \dot{\mathbf{b}}$.

Ejemplos

- $6|192$, ya que $192 = 6 \cdot 32$
- $11|2310$, ya que $2310 = 11 \cdot 210$
- $8|-24$, ya que $24 = 8 \cdot (-3)$

Teorema (Propiedades de la divisibilidad (I))

Sean $a, b, c \in \mathbb{Z}$. *Entonces:*

1. $1|a$ y $-1|a$
2. $a|\text{-}a$, *para todo* $0 \neq a \in \mathbb{Z}$

Teorema (Propiedades de la divisibilidad (II))

Sean $a, b, c \in \mathbb{Z}$. *Entonces:*

3. $a|a$.
4. *Si* $a|b$ y $b|a$, *entonces* $a = b$ *ó bien* $a = \text{-}b$.
5. *Si* $a|b$ y $b|c$, *entonces* $a|c$.

- La relación de divisibilidad en $\mathbb{N}$ es una **relación de orden** y además, si $a|b$, entonces $a \leq b$.

Teorema (Propiedades de la divisibilidad (III))

Sean $a, b, c \in \mathbb{Z}$. *Entonces:*

6. *Si* $c|a$ *y* $c|b$, *entonces* $c|a+b$ *y* $c|a-b$.

Corolario (Propiedades de la divisibilidad)

Sean $a, b, c \in \mathbb{Z}$. *Entonces:*

7. *Si* $a|b$, *entonces* $a|m \cdot b$, $\forall m \in \mathbb{Z}$
8. *Si* $c|a$ *y* $c|b$, *entonces* $c|s \cdot a + t \cdot b$, $\forall s, t \in \mathbb{Z}$.
9. *Para* $1 \leq i \leq n$, *sea* $b_i \in \mathbb{Z}$. *Si* c *divide a cada* b_i, *entonces*

$$c|t_1 \cdot b_1 + t_2 \cdot b_2 + \cdots + t_n \cdot b_n, \ \forall t_1, \ldots, t_n \in \mathbb{Z}$$

Definición

Sean a y b *enteros no nulos. El* **máximo común divisor** *de* a y b *es un entero* $d \in \mathbb{Z}^+$ *tal que:*

- $d \mid a$ y $d \mid b$*; es decir,* d *es un* **divisor común** *de* a y b.
- *si* c *es cualquier divisor común de* a y b*, entonces* $c \mid d$.

El **máximo común divisor** *de* a y b *se denota* $mcd(a, b)$.

Ejemplos

- El conjunto de divisores comunes de 36 y 24 es $\{1, 2, 3, 4, 6, 12\}$.
  Así, $mcd(36, 24) = 12$.
- El conjunto de divisores comunes de 70 y 42 es $\{1, 2, 7, 14\}$.
  Así, $mcd(70, 42) = 14$.

2.1 Aritmética Entera

Máximo Común Divisor

Teorema

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

Demostración:

- Se considera el conjunto

$$S = \{as + bt \mid s, t \in \mathbb{Z},\ as + bt > 0\}$$

- Ya que $a = a \cdot 1 + b \cdot 0 \in S$, sabemos que S es un conjunto no vacío.
- Por el principio de buena ordenación, S tiene elemento mínimo. Sea d este elemento.
- Por ser d elemento de S, existirán enteros s y t tales que

$$d = as + bt$$

- Si c es divisor de a y es divisor de b, entonces c divide a d
- Así, c verifica la segunda condición.

Demostración:(cont.)

- A continuación demostramos que d es divisor de a y análogamente se demuestra que es divisor de b.
- Usando el algoritmo de la división, podemos escribir

$$a = d \cdot q + r, \text{ con } 0 \leq r < d$$

- Veamos que $r = 0$.
- Tenemos

$$r = a - d \cdot q = a - (as + bt) \cdot q = a(1 - sq) + b(-tq)$$

- Luego, si r fuera positivo, estaría en S. Sin embargo, d es el mínimo de S y r es estrictamente menor que d.
- Luego, r no está en S y, por eso, r no puede ser positivo.
- Por lo tanto, r es cero y d es un divisor de **a**.

Ahora sabemos que para cualesquiera $a, b \in \mathbb{Z}^+$, el $mcd(a, b)$ existe y es único.

Además se verifican:

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

Por la demostración del teorema anterior sabemos que el máximo común divisor de $\boldsymbol{a}$ y $\boldsymbol{b}$ es el menor entero positivo $\boldsymbol{d}$ que se puede expresar como combinación lineal de $\boldsymbol{a}$ y $\boldsymbol{b}$

$$\boldsymbol{d} = \boldsymbol{a} \cdot s + \boldsymbol{b} \cdot t, \quad s, t \in \mathbb{Z}$$

A continuación estudiaremos cómo se pueden encontrar el máximo común divisor $\boldsymbol{d}$ y estos enteros s, t.

Lema (1)

Sean a y b *enteros tales que* $b > 0$ y $b|a$. *Entonces el conjunto de los divisores comunes de* a y b *coincide con el conjunto de los divisores de* b.

Lema (2)

Sean a y b *enteros tales que* $a > b > 0$ y $a = b \cdot q + r$. *Entonces el conjunto de los divisores comunes de* a y b *coincide con el conjunto de los divisores comunes de* b y r; *en particular,* $mcd(a, b) = mcd(b, r)$.

Teorema (Algoritmo de Euclides)

Sean a y b enteros positivos. Aplicando repetidamente el algoritmo de la división, se tiene

$$
\begin{array}{rclcccccc}
a & = & b \cdot q_1 + r_1 & \qquad & 0 & < & r_1 & < & b \\
b & = & r_1 \cdot q_2 + r_2 & & 0 & < & r_2 & < & r_1 \\
r_1 & = & r_2 \cdot q_3 + r_3 & & 0 & < & r_3 & < & r_2 \\
r_2 & = & r_3 \cdot q_4 + r_4 & & 0 & < & r_4 & < & r_3 \\
 & \dots & & & & & \dots & & \\
r_{k-2} & = & r_{k-1} \cdot q_k + r_k & & 0 & < & r_k & < & r_{k-1} \\
r_{k-1} & = & r_k \cdot q_{k+1} + 0 & & & & r_{k+1} & = & 0
\end{array}
$$

Entonces r_k es el máximo común divisor de a y b.

Demostración:

- Aplicamos repetidamente el algoritmo de la división y obtenemos los restos $r_1, r_2, ..., r_k$.
- Por ser $b, r_1, r_2, ...$ una secuencia decreciente de números naturales, llegará a un resto nulo ($r_{k+1} = 0$).
- Como se indica en la última ecuación, el resto anterior r_k divide a r_{k-1} y, aplicando el lema 1, el conjunto de divisores comunes de r_k y r_{k-1} coincide con el conjunto de divisores de r_k y el máximo de todos ellos es el propio r_k; por lo que $mcd(r_k, r_{k-1}) = r_k$.
- Usando el lema 2 repetidamente, se obtiene

$$r_k = mcd(r_k, r_{k-1}) = mcd(r_{k-1}, r_{k-2}) = ... = mcd(a, b)$$

- Es decir, el máximo común divisor es el último resto distinto de cero.

Ejemplo Vamos a hallar el máximo común divisor de 70 y 42:

$$\begin{aligned} 70 &= 42 \cdot 1 + 28 \\ 42 &= 28 \cdot 1 + 14 \\ 28 &= 14 \cdot 2 + 0 \end{aligned}$$

Por lo tanto, $mcd(70, 42) = 14$.

2.1 Aritmética Entera

Algoritmo de Euclides

Ejemplo Halla el $mcd(36, 24)$

$$\left.\begin{array}{rcl@{\qquad}ccccc} 36 & = & 24 \cdot 1 + 12, & 0 & < & 12 & < & 24 \\ 24 & = & 12 \cdot 2 + 0, & & & r_2 & = & 0 \end{array}\right\}$$

Por tanto, $mcd(36, 24) = 2,$ ya que 2 es el último resto distinto de cero.

Ejemplo Halla el $mcd(136, 26)$

$$\left.\begin{array}{rcl@{\qquad}ccccc} 136 & = & 26 \cdot 5 + 6 & 0 & < & 6 & < & 26 \\ 26 & = & 6 \cdot 4 + 2 & 0 & < & 2 & < & 6 \\ 6 & = & 2 \cdot 3 + 0 & & & r_3 & = & 0 \end{array}\right\}$$

Por tanto, $mcd(136, 26) = 2,$ ya que 2 es el último resto distinto de cero

Ejemplo Halla el $mcd(21, 13)$

$$\left.\begin{array}{rcrcrcccccc}
21 & = & 13\cdot 1 & + & 8, & & 0 & < & 8 & < & 13 \\
13 & = & 8\cdot 1 & + & 5, & & 0 & < & 5 & < & 8 \\
8 & = & 5\cdot 1 & + & 3, & & 0 & < & 3 & < & 5 \\
5 & = & 3\cdot 1 & + & 2, & & 0 & < & 2 & < & 3 \\
3 & = & 2\cdot 1 & + & {\color{blue}1}, & & 0 & < & 1 & < & 2 \\
2 & = & 1\cdot 2 & + & 0, & & & & r_6 & = & 0
\end{array}\right\}$$

Por tanto, $mcd(21, 13) = 1$, ya que 1 es el último resto distinto de cero.

Lema (Bezout)

Sean a y b enteros tales que $b > 0$. Entonces existen enteros s y t tales que $mcd(a, b) = a \cdot s + b \cdot t$

Demostración Por el algoritmo de Euclides sabemos que

$$d = mcd(a, b) = r_k$$

Del mismo algoritmo obtenemos,

$$\begin{aligned} r_1 &= a - b \cdot q_1 \\ r_2 &= b - r_1 \cdot q_2 \\ r_3 &= r_1 - r_2 \cdot q_3 \\ &\dots \\ r_{k-1} &= r_{k-3} - r_{k-2} \cdot q_{k-1} \\ r_k &= r_{k-2} - r_{k-1} \cdot q_k \end{aligned}$$

Lema (Bezout)

Sean a y b enteros tales que $b > 0$. Entonces existen enteros s y t tales que $mcd(a, b) = a \cdot s + b \cdot t$

Demostración (cont.)

Recorriendo sucesivamente de forma **regresiva** las igualdades del algoritmo de Euclides, obtendremos valores de $r_{k-3}, r_{k-4}, \ldots.$ que, sustituidos en la anterior expresión de $\boldsymbol{d}$,

$$\boldsymbol{d} = r_n = r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = \ldots.$$

producirán la combinación lineal buscada

$$\boldsymbol{d} = a \cdot \boldsymbol{s} + b \cdot \boldsymbol{t}$$

Ejemplo Dados los enteros $a = 136$ y $b = 26$, aplicando el algoritmo de Euclides obtenemos

$$\left\{ \begin{array}{rcll} 136 & = & 26 \cdot 5 + 6 & \qquad (ii) \\ 26 & = & 6 \cdot 4 + 2 & \qquad (i) \\ 6 & = & 2 \cdot 3 + 0 & \end{array} \right.$$

Ahora sustituimos regresivamente cada uno de los restos hasta llegar a una combinación lineal de 136 y 26:

$$\left. \begin{array}{rcl} 2 & \overset{(i)}{=} & 26 - 6 \cdot 4 \\ & \overset{(ii)}{=} & 26 - (136 - 26 \cdot 5) \cdot 4 \\ & = & 136 \cdot (-4) + 26 \cdot 21 \end{array} \right\}$$

Así, tenemos $2 = 136 \cdot (\mathbf{-4}) + 26 \cdot \mathbf{21}$

Identidad de Bezout

Ejemplo Vamos a calcular el mcd de 250 y 111 y a obtener la combinación lineal establecida por la identidad de Bezout.

$$
\begin{aligned}
250 &= 111 \cdot 2 + 28 & \Longrightarrow && \boxed{28} &= \boxed{250} - \boxed{111} \cdot 2 && (1)\\
111 &= 28 \cdot 3 + 27 & \Longrightarrow && \boxed{27} &= \boxed{111} - \boxed{28} \cdot 3 && (2)\\
28 &= 27 \cdot 1 + 1 & \Longrightarrow && \boxed{1} &= \boxed{28} - \boxed{27} \cdot 1 && (3)\\
27 &= 27 \cdot 1 + 0
\end{aligned}
$$

Por lo tanto, $mcd(250, 111) = 1$ y:

$$
\begin{aligned}
\boxed{1} &= \boxed{28} - \boxed{27} && \text{Por (3)}\\
&= \boxed{28} - (\boxed{111} - \boxed{28} \cdot 3) = \boxed{111}(-1) + \boxed{28} \cdot 4 && \text{Por (2)}\\
&= \boxed{111}(-1) + (\boxed{250} - \boxed{111} \cdot 2) \cdot 4 && \text{Por (1)}\\
&= \boxed{250} \cdot 4 + \boxed{111} \cdot (-9)
\end{aligned}
$$

Definición

Se dice que los enteros a y b *son* **primos relativos** *o* **coprimos** *si*

$$mcd(a, b) = 1$$

Ejemplo 9 y 22 son coprimos, ya que $mcd(22, 9) = 1$.

Definición

Los enteros $a_1, a_2, \ldots, a_n$ *son* **primos relativos dos a dos** *si* $mcd(a_i, a_j) = 1$ *para* $1 \leq i < j \leq n$.

Ejemplo Los enteros 9, 22 y 35 son coprimos dos a dos, ya que

$$mcd(9, 22) = mcd(9, 35) = mcd(22, 35) = 1$$

Ejercicio Sean a y b enteros cualesquiera. Demuestra que:

1. Si $d = mcd(a, b)$, entonces $mcd(\frac{a}{d}, \frac{b}{d}) = 1$.

2. Existen enteros x e y tales que $ax + by = 1$

   si y sólo si $mcd(a, b) = 1$.

Teorema

Sean a, b *y* c *enteros, tales que* a *y* b *son coprimos.*

1. *Si* a *es un divisor de* bc, *entonces* a *es un divisor de* c.

$$\left\{ \begin{array}{rcl} mcd(a,b) & = & 1 \\ a & \mid & bc \end{array} \right\} \Longrightarrow a \mid c$$

2. *Si* a *es un divisor de* c *y* b *es un divisor de* c, *entonces* ab *es un divisor de* c.

$$\left\{ \begin{array}{rcl} mcd(a,b) & = & 1 \\ a & \mid & c \\ b & \mid & c \end{array} \right\} \Longrightarrow ab \mid c$$

Teorema

Sean a, b y c enteros, tales que a y b son coprimos.

1. *Si a es un divisor de bc, entonces a es un divisor de c.*

Demostración:

- Por ser a y b coprimos, existen enteros $s, t \in \mathbb{Z}$ tales que

$$1 = a \cdot s + b \cdot t$$

- Multiplicando por c ambos miembros de esta ecuación obtenemos

$$c = a \cdot c \cdot s + b \cdot c \cdot t \qquad (*)$$

- Aplicando la hipótesis y propiedades de la divisibilidad

$$\left.\begin{array}{ccccc} a \mid a & \Longrightarrow & a \mid a \cdot c & \Longrightarrow & a \mid a \cdot c \cdot s \\ & & a \mid b \cdot c & \Longrightarrow & a \mid b \cdot c \cdot t \end{array}\right\} \Longrightarrow a \mid c$$

Teorema

Sean a, b y c enteros tales que a y b son coprimos.

2. *Si a es un divisor de c y b es un divisor de c, entonces ab es un divisor de c.*

Demostración:

- Por ser a y b coprimos, existen enteros $s, t \in \mathbb{Z}$ tales que

$$1 = a \cdot s + b \cdot t$$

- Multiplicando por c ambos miembros de esta ecuación obtenemos

$$c = a \cdot c \cdot s + b \cdot c \cdot t \qquad (*)$$

- Aplicando la hipótesis y propiedades de la divisibilidad

$$\left.\begin{array}{lllll} b \mid c & \Longrightarrow & a \cdot b \mid a \cdot c & \Longrightarrow & a \cdot b \mid a \cdot c \cdot s \\ a \mid c & \Longrightarrow & a \cdot b \mid c \cdot b & \Longrightarrow & a \cdot b \mid c \cdot b \cdot t \end{array}\right\} \Longrightarrow a \cdot b \mid c$$

☛ Si los enteros a y b **no** son **coprimos**, puede que estos resultados **no** se verifiquen.

Ejemplos

1. Para $a = 6$, $b = 4$ y $c = 9$ se verifica que
   - $a \mid b \cdot c$: $6 \mid 36 = 4 \cdot 9$
   - pero $a \nmid c$: $6 \nmid 9$
   - ni tampoco $a \nmid b$: $6 \nmid 4$.
2. Para $a = 6$, $b = 4$ y $c = 12$ se verifica que
   - $a \mid c$ y $b \mid c$: $6 \mid 12$ y $4 \mid 12$
   - pero $a \cdot b \nmid c$: $6 \cdot 4 \nmid 12$

Definición

Un entero positivo p *mayor que* 1 *se llama* **primo** *si tiene exactamente dos divisores positivos:* 1 *y* p. *En caso contrario, se dice que es* **compuesto**.

☛ El entero n es compuesto si y sólo si existe un entero a tal que $a \mid n$ y $1 < a < n$.

Ejemplos

- 17 es primo, ya que sus únicos divisores positivos son 1 y 17.
- El entero 2310 es compuesto, ya que es divisible por 10: $10|2310$

2.1 Aritmética Entera

Números primos. Teorema fundamental de la aritmética.

- Mediante el procedimiento conocido como **criba de Eratóstenes** se obtienen los primos menor que un entero n.

➻ Los primos menores que 100 son:

	2,	3,	5,	7,	
11,		13,		17,	19,
		23,			29,
31,				37,	
41,		43,		47,	
		53,			59,
61,				67,	
71,		73,			79,
		83,			89,
				97	

Lema

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

- Es decir, todo número compuesto admite, al menos, un divisor primo.

Teorema (Euclides)

El conjunto de números primos es infinito.

Demostración Si suponemos que $p_1 < \cdots < p_n$ son **todos** los números primos, entonces $q = 1 + p_1 \cdot p_2 \cdot \cdots \cdot p_n$ es otro número primo estrictamente mayor que p_n. Luego el conjunto de números primos no es finito.

- En algunas aplicaciones es importante saber si un entero dado es primo o compuesto.
- Por ejemplo, en algunos métodos de criptografía se utilizan primos grandes para construir mensajes secretos.
- Un procedimiento para determinar si un entero es primo se basa en el siguiente resultado:

Lema

Sea $n \in \mathbb{Z}^+$. Si n es compuesto, entonces podemos encontrar un divisor primo p tal que $p \leq \sqrt{n}$.

Consecuencia:

Un entero es primo si no es divisible por ningún primo menor que su raíz cuadrada.

Ejemplo Demuestra que 101 es primo.

Solución

- Los únicos primos menores o iguales que $\sqrt{101}$ son $2, 3, 5$ y 7.
- Como 101 no es divisible por ninguno de ellos, se puede deducir que 101 es primo.

Teorema (Teorema Fundamental de la aritmética)

Todo entero positivo n *mayor que* 1 *se puede expresar de forma única como producto de potencias de primos.*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

donde $p_1 < p_2 < \cdots < p_k$ *son primos y* $e_j \in \mathbb{N}$ *para cada* $j = 1, \ldots, k$.

Ejemplo

$$\begin{aligned} 1024 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10} \\ 1001 &= 7 \cdot 11 \cdot 13 \\ 999 &= 3 \cdot 3 \cdot 3 \cdot 37 \\ 403 &= 13 \cdot 31 \end{aligned}$$

2.1 Aritmética Entera

¿Cómo se puede obtener la descomposición en factores primos de un entero n ?

1. Empezamos dividiendo $\boldsymbol{n}$ por primos sucesivos, iniciando por 2.
2. Si no hallamos un factor primo de $\boldsymbol{n}$ menor o igual que $\sqrt{\boldsymbol{n}}$, entonces $\boldsymbol{n}$ es primo.
3. Por el contrario, si encontramos para $\boldsymbol{n}$ un divisor primo $\boldsymbol{p}$, se continúa descomponiendo $\frac{\boldsymbol{n}}{\boldsymbol{p}}$. (Ahora no empezamos por 2, sino por $\boldsymbol{p}$.)
4. Si $\frac{\boldsymbol{n}}{\boldsymbol{p}}$ no tiene divisores primos mayores o iguales que $\boldsymbol{p}$ y que no sean mayores que su raíz cuadrada, entonces es primo.
5. En otro caso, si tiene un divisor primo $\boldsymbol{q}$, se sigue descomponiendo $\frac{\boldsymbol{n}}{\boldsymbol{pq}}$.
6. Este procedimiento continúa hasta que la descomposición se reduce a un número primo.

Ejemplos

1. Calcula la descomposición en factores primos de 7007.

- Para $n = 7007$ se comprueba que $2, 3, 5 \nmid 7007$ y que $7 | 7007$.
- Ahora empezamos de nuevo con 1001. Vemos que $7|1001$ ya que $1001 = 7 \cdot 143$
- Continuando con 143, se tiene que $7 \nmid 143$, pero $11|143$ ya que $143 = 11 \cdot 13$
- De esta manera, $7007 = 7^2 \cdot 11 \cdot 13$

2. Calcula la descomposición en factores primos de $n = 4675$

- $2 \nmid 4675,\ 3 \nmid 4675$ pero $5|4675$ ya que $4675 = 5 \cdot 935$
- $5|935$ ya que $935 = 5 \cdot 187$
- $5, 7 \nmid 187$, $11|187$
- De esta manera, $4675 = 5^2 \cdot 11 \cdot 17$

Teorema

Sean $a, b \in \mathbb{Z}$ *y sea* $p \in \mathbb{N}$ *primo. Si* $p|a \cdot b$*, entonces* $p|a$ *ó bien* $p|b$*.*

Demostración: ***Ejercicio***

Teorema

Sean $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ *y sea* $p \in \mathbb{N}$ *primo. Si* $p|b_1 \cdots b_k$*, entonces* $p|b_j$ *para algún* $j = 1, \ldots, k$*.*

Demostración: ***Ejercicio***

Cálculo del mcd a partir de la factorización

Supongamos que las factorizaciones de los enteros a y b no nulos son:

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

donde:

- cada exponente es no negativo y
- **todos** los factores primos, tanto de a como de b, aparecen en ambas factorizaciones, con exponente cero si es necesario.

  (Si un factor primo aparece en una sola descomposición, se muestra en la otra con exponente cero.)

Teorema

Sean $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ *y* $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$ *enteros. Entonces,*

$$mcd(a, b) = p_1^{min.\{a_1,b_1\}} \cdot p_2^{min.\{a_2,b_2\}} \cdots p_n^{min.\{a_n,b_n\}}$$

Demostración: Veamos que $p_1^{min.\{a_1,b_1\}} \cdot p_2^{min.\{a_2,b_2\}} \cdots p_n^{min.\{a_n,b_n\}}$ es divisor común de a y b y que no hay ningún entero mayor que lo sea.

En efecto, este entero divide a los enteros a y b, ya que la potencia de cada primo en su factorización no es mayor que la potencia de ese mismo primo en las factorizaciones de a y b.

Además, ningún entero mayor que él puede ser divisor común de a y b, porque los exponentes de los números primos en esta factorización no pueden incrementarse y no se pueden incluir otros enteros primos.

Ejemplos

Halla $mcd(3600, 3465)$, usando la descomposición en factores primos.

$$\left.\begin{array}{rcl} 3600 & = & 2^4 \cdot 3^2 \cdot 5^2 \\ 3465 & = & 3^2 \cdot 5 \cdot 7 \cdot 11 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} 3600 & = & 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^0 \cdot 11^0 \\ 3465 & = & 2^0 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \end{array}\right\}$$

Luego

$$\left.\begin{array}{rcl} mcd(3600, 3465) & = & 2^{min.(4,0)} \cdot 3^{min.(2,2)} \cdot 5^{min.(2,1)} \cdot 7^{min.(0,1)} \cdot 11^{min.(0,1)} \\ & = & 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^0 = 45 \end{array}\right\}$$

2.1 Aritmética Entera

Números primos. Teorema fundamental de la aritmética.

Ejemplo 2 Usa la descomposición en factores primos para hallar $mcd(2750, 1992)$

$$\left.\begin{array}{rcl} 2750 & = & 2^1 \cdot 5^3 \cdot 11^1 \\ 1992 & = & 2^3 \cdot 3 \cdot 83 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} 2750 & = & 2^1 \cdot 3^0 \cdot 5^3 \cdot 11^1 \cdot 83^0 \\ 3465 & = & 2^3 \cdot 3 \cdot 5^0 \cdot 11^0 \cdot 83 \end{array}\right\}$$

Por tanto,

$$\left.\begin{array}{rcl} mcd(2750, 1992) & = & 2^{min.(1,3)} \cdot 3^{min.(0,3)} \cdot 5^{min.(3,0)} \cdot 11^{min.(0,1)} \cdot 83^{min.(0,1)} \\ & = & 2^1 \cdot 3^0 \cdot 5^0 \cdot 11^0 \cdot 83^0 = 2 \end{array}\right\}$$

Definición

El **mínimo común múltiplo** *de dos enteros positivos* a y b *es un entero* $c \in \mathbb{Z}^+$ *tal que*

1. $a \mid c$ y $b \mid c$; *es decir,* c *es múltiplo común de* a y b.
2. *si* c' *es cualquier múltiplo común de* a y b, *entonces* $c \mid c'$.

El **mínimo común múltiplo** *de* a y b *se denota* $mcm(a, b)$.

- El mínimo común múltiplo de a y b es el menor entero que es divisible tanto por a como por b.
- El mínimo común múltiplo existe porque el conjunto de enteros divisibles por a y b es no vacío y, por el Principio de buena ordenación, todo conjunto no vacío tiene elemento mínimo.

Ejemplo Para $a = 10$ y $b = 25$, $mcm(a, b) = 50$.

Las factorizaciones de enteros se pueden utilizar también para obtener el ***mínimo común múltiplo*** de dos enteros.

Supongamos que las descomposiciones en producto de potencias de primos son las dadas anteriormente. Entonces el mínimo común múltiplo de $\boldsymbol{a}$ y $\boldsymbol{b}$ viene dado por

$$mcd(\boldsymbol{a}, \boldsymbol{b}) = p_1^{max\{a_1, b_1\}} \cdot p_2^{max\{a_2, b_2\}} \cdots p_n^{max\{a_n, b_n\}}$$

Esta fórmula es válida puesto que un múltiplo común de $\boldsymbol{a}$ y $\boldsymbol{b}$ contiene el factor primo p_i al menos $max\{a_i, b_i\}$ veces en su fatorización y el mínimo común múltiplo no contiene otros factores primos aparte de los contenidos en las factorizaciones de $\boldsymbol{a}$ y $\boldsymbol{b}$.

Ejemplo Usa las descomposiciones en factores primos para hallar el mínimo común múltiplo de 3600 y 3465.

$$\left.\begin{array}{rcl} 3600 & = & 2^4\cdot 3^2\cdot 5^2 \\ 3465 & = & 3^2\cdot 5\cdot 7\cdot 11 \end{array}\right\} \Longrightarrow \left\{\begin{array}{rcl} 3600 & = & 2^4\cdot 3^2\cdot 5^2\cdot 7^0\cdot 11^0 \\ 3465 & = & 2^0\cdot 3^2\cdot 5^1\cdot 7^1\cdot 11^1 \end{array}\right\}$$

Por tanto,

$$\begin{aligned} mcm(3600, 3465) &= 2^{\max\{4,0\}}\cdot 3^{max\{2,2\}}\cdot 5^{max\{2,1\}}\cdot 7^{max\{0,1\}}\cdot 11^{max\{0,1\}} \\ &= 2^4\cdot 3^2\cdot 5^2\cdot 7^1\cdot 11^1 \end{aligned}$$

Teorema

Sean a y b enteros positivos. Entonces, $a \cdot b = mcd(a, b) \cdot mcm(a, b)$.

Demostración: Evidente, usando la descomposición en factores primos de a y b para calcular el máximo común divisor y el mínimo común múltiplo.

Corolario

Si a y $b \in \mathbb{Z}^+$ son coprimos, entonces $mcm(a, b) = a \cdot b$.

Ejemplo Dados $a = 250$ y $b = 111$, tenemos que

$$\left.\begin{array}{rcl} 250 & = & 2 \cdot 5^3 \\ 111 & = & 3 \cdot 37 \end{array}\right\} \Longrightarrow mcm(250, 111) = 2 \cdot 5^3 \cdot 3 \cdot 37 = 250 \cdot 111$$

Ejemplo Vamos a calcular $mcm(210, 99)$ con los dos métodos:

1. Usando el algoritmo de Euclides:

$$\left.\begin{aligned} 210 &= 99 \cdot 2 + 12 \\ 99 &= 12 \cdot 8 + \boxed{3} \\ 12 &= 3 \cdot 4 \end{aligned}\right\} \Longrightarrow \qquad mcd(210, 99) = 3$$

Por lo tanto, $mcm(210, 99) = \dfrac{210 \cdot 99}{3} = 210 \cdot 33 = 6930$

2. Usando la factorización:

$$\left.\begin{aligned} 210 &= 2 \cdot 3 \cdot 5 \cdot 7 &&= 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0 \\ 99 &= 3^2 \cdot 11 &&= 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^1 \end{aligned}\right\}$$

Por lo tanto, $mcm(210, 99) = 2^1 3^2 5^1 7^1 11^1 = 6930$

Cuando se requiere que las **soluciones** de una determinada **ecuación** sean números **enteros**, tenemos una *ecuación diofántica*.

Las ecuaciones diofánticas deben su nombre al matemático griego Diophantus, quien escribió extensamente acerca de estas ecuaciones.

Definición

*Una **ecuación diofántica lineal de dos variables** es una ecuación*

$$ax + by = c$$

donde a, b, y c son enteros.

Teorema

Sean $a, b \in \mathbb{Z}^+$ *con* $d = mcd(a, b)$*. La ecuación*

$$ax + by = c$$

no tiene soluciones enteras si $d \not| c$*.*

Si $d|c$*, entonces hay infinitas soluciones enteras.*

Además, si $x = x_0, y = y_0$ *es una solución particular de la ecuación, entonces todas las soluciones vienen dadas por*

$$x = x_0 + (\frac{b}{d})k, \quad y = y_0 - (\frac{a}{d})k$$

donde $k \in \mathbb{Z}$

Demostración:

- Supongamos que x, y son enteros tales que $ax + by = c$.
- Entonces por ser $d = mcd(a, b)$, aplicando la propiedad (9) de la divisibilidad, sabemos que también $d|c$.
- Por lo tanto, si $d \not| c$, no hay soluciones enteras de la ecuación.
- Ahora supongamos que $d|c$. Por ser $d = mcd(a, b)$, sabemos que existen enteros s, t tales que

$$d = as + bt \tag{1}$$

Demostración:(cont.)

- Ahora supongamos que $d|c$. Por ser $d = mcd(a, b)$, sabemos que existen enteros s, t tales que
$$d = as + bt \tag{2}$$
- Ya que $d|c$, existe un entero d' tal que $c = dd'$. Multiplicando por d' ambos lados de la ecuación anterior, tenemos
$$c = dd' = (as + bt)d' = a(sd') + b(td')$$
- Por lo tanto, una solución particular de la ecuación es
$$x_0 = sd', \quad y_0 = td'.$$

Demostración:(cont.)

- Para mostrar que hay infinitas soluciones, consideramos
$$x = x_0 + (\frac{b}{d})k, \qquad y = y_0 - (\frac{a}{d})k, \text{ donde } k \in \mathbb{Z}.$$
- Este par (x, y) es una solución, ya que
$$ax + by = ax_0 + a(\frac{b}{d})k + by_0 - b(\frac{a}{d})k = ax_0 + by_0 = c$$
- Ahora mostramos que cada solución de la ecuación $ax + by = c$ debe ser de esta forma.

Demostración:(cont.)

- Supongamos que x e y son enteros tales que
$$ax + by = c$$
- Puesto que
$$ax_0 + by_0 = c$$
restando encontramos que
$$(ax + by) - (ax_0 + by_0) = 0$$
- lo que implica que
$$a(x - x_0) + b(y - y_0) = 0$$
- Por tanto,
$$a(x - x_0) = b(y_0 - y)$$
- Dividiendo ambos miembros de la ecuación por d, obtenemos
$$(\frac{a}{d})(x - x_0) = (\frac{b}{d})(y_0 - y)$$

Demostración:(cont.)

- Dividiendo ambos miembros de la ecuación por d, obtenemos
$$(\frac{a}{d})(x - x_0) = (\frac{b}{d})(y_0 - y)$$
- Teniendo en cuenta que $mcd((\frac{a}{d}), (\frac{b}{d})) = 1$, se deduce que
$$(\frac{a}{d}) \mid (y_0 - y)$$
- Por tanto, existe un entero k tal que $y_0 - y = (\frac{a}{d})k$.

  Esto significa que $y = y_0 - (\frac{a}{d})k$.
- Ahora sustituyendo este valor de y en la ecuación $a(x - x_0) = b(y_0 - y)$, encontramos que $a(x - x_0) = b(\frac{a}{d})k$, lo que implica que $x = x_0 + (\frac{b}{d})k$.

Dada una ecuación diofántica

$$ax + by = c$$

¿cómo encontramos todas las soluciones?

1. Estudiamos si tiene soluciones enteras, comprobando si $mcd(a, b) = d \mid c$
2. Hallamos una **solución particular**: $x_0, \ y_0$, a partir de la identidad de Bezout: $d = a \cdot s + b \cdot t$
3. Damos la solución general

$$x = x_0 + (\frac{b}{d})k, \quad y = y_0 - (\frac{a}{d})k, \quad k \in \mathbb{Z}$$

Ejemplo 1 Halla **todas** las soluciones enteras de la ecuación

$$14x + 21y = 70$$

Solución:

1. Estudiamos si tiene soluciones enteras:

$$\left.\begin{array}{rcl} mcd(14, 21) & = & 7 \\ 7 & \mid & 70 \end{array}\right\}$$

   Luego $14x + 21y = 70$ tiene soluciones enteras.

2. Expresamos el $mcd(14, 21)$ en función de los coeficientes 14 y 21 y hallamos una **solución particular**:

$$7 = 14(-1) + 21 \cdot 1 \implies 70 = 14(-10) + 21 \cdot 10$$

   Una solución particular es $x_0 = -10, \qquad y_0 = 10$

Ejemplo 1 Halla **todas** las soluciones enteras de la ecuación

$$14x + 21y = 70$$

Solución:

3. Damos la solución general a partir de la solución particular:

$$70 = 14(-10 + 3k) + 21(10 - 2k), \quad k \in \mathbb{Z}$$

$$x = -10 + 3k, \qquad y = 10 - 2k, \quad k \in \mathbb{Z}$$

Ejemplo 2 Halla **todas** las soluciones enteras no negativas de la ecuación

$$10x + 6y = 104$$

Solución:

1. Estudiamos si existen soluciones enteras:

$$\left.\begin{array}{rcl} mcd(10,6) & = & 2 \\ 2 & \mid & 104 \end{array}\right\}$$

   Luego $10x + 6y = 104$ tiene soluciones enteras.

2. Hallamos una **solución particular**, a partir de la identidad de Bezout.

$$2 = 10(-1) + 6 \cdot 2 \implies 104 = 2 \cdot 52 = 10(-52) + 6 \cdot 104$$

   Una solución particular es $x_0 = -52, \qquad y_0 = 104$

Ejemplo 2 Halla **todas** las soluciones enteras no negativas de la ecuación

$$10x + 6y = 104$$

Solución:

3. Damos la solución general a partir de la solución particular:

$$104 = 10(-52 + 3k) + 6(104 - 5k), \quad k \in \mathbb{Z}$$

$$x = -52 + 3k, \qquad y = 104 - 5k, \quad k \in \mathbb{Z}$$

4. Hallamos las soluciones enteras no negativas

Ejemplo 2 Halla **todas** las soluciones enteras no negativas de la ecuación

$$10x + 6y = 104$$

Solución:

4. Hallamos las soluciones enteras no negativas
   - ✍ $x = -52 + 3k \geq 0, \qquad y = 104 - 5k \geq 0, \quad k \in \mathbb{Z}$
   - ✍ $-52 + 3k \geq 0 \implies 3k \geq 52 \implies k \geq \dfrac{52}{3} \qquad (1)$
   - ✍ $104 - 5k \geq 0 \implies 5k \leq 104 \implies k \leq \dfrac{104}{5} \qquad (2)$
   - ✍ De (1) y (2) obtenemos que: $\dfrac{52}{3} \leq k \leq \dfrac{104}{5}, \quad k \in \mathbb{Z}$

Ejemplo 2 Halla **todas** las soluciones enteras no negativas de la ecuación

$$10x + 6y = 104$$

Solución:

4. Hallamos las soluciones enteras no negativas (cont.)
   - ✍ $\dfrac{52}{3} \leq k \leq \dfrac{104}{5}$, $\quad k \in \mathbb{Z} \implies 18 = \lceil \dfrac{52}{3} \rceil \leq k \leq \lfloor \dfrac{104}{5} \rfloor = 20$
   - ✍ Ahora, sustituimos estos valores de k en la solución general

$$x = -52 + 3k, \qquad y = 104 - 5k$$

y obtenemos las soluciones enteras no negativas:

$$\begin{array}{lrclrclrcl} (1) & k & = & 18, & x_1 & = & 14, & y_1 & = & 2 \\ (2) & k & = & 19, & x_2 & = & 9, & y_2 & = & 5 \\ (3) & k & = & 20, & x_3 & = & 4, & y_3 & = & 8 \end{array}$$

Ejemplo 3

1. Determina aquellos valores $c \in \mathbb{Z}, \quad 10 < c < 20$ tales que la ecuación

$$84x + 990y = c$$

   no tenga soluciones enteras.

2. Para los restantes valores de c halla las soluciones.

Ejemplo 3

1. Determina aquellos valores $c \in \mathbb{Z}$, $10 < c < 20$ tales que la ecuación

$$84x + 990y = c$$

no tenga soluciones enteras.

Solución

1. Usamos el algoritmo de Euclides para calcular $\mathrm{mcd}(84, 990)$

$$\begin{array}{rclcrcccc}
990 & = & 84 \cdot 11 + 66 & \quad & 0 & < & 66 & < & 84 \\
84 & = & 66 \cdot 1 + 18 & & 0 & < & 18 & < & 66 \\
66 & = & 18 \cdot 3 + 12 & & 0 & < & 12 & < & 18 \\
18 & = & 12 \cdot 1 + 6 & & 0 & < & 6 & < & 12 \\
12 & = & 6 \cdot 2 & & & & r_n & = & 0
\end{array}$$

Ejemplo 3

1. Determina aquellos valores $c \in \mathbb{Z}$, $10 < c < 20$ tales que la ecuación

$$84x + 990y = c$$

no tenga soluciones enteras.

Solución (cont.) Por ser $mcd(990, 84) = 6$, tendrán solución entera las ecuaciones

$$84x + 990y = c$$

cuyo término independiente sea:

$$c = 12, \qquad \text{o bien} \qquad c = 18$$

Por tanto, **NO** tiene solución entera la ecuación $84x + 990y = c$ para

$$c \in \{11, 13, 14, 15, 16, 17, 19\}$$

Ejemplo 3

2. Para los restantes valores de c halla las soluciones.

Solución (cont.)

2. Para resolver la ecuación en los dos casos posibles empezamos hallando la expresión de $mcd(990, 84)$ en función de 84 y 990:

$$\begin{aligned} 6 &= 18 - 12 \\ &= 18 - (66 - 18 \cdot 3) = (-1)66 + 4 \cdot 18 \\ &= (-1)66 + 4 \cdot (84 - 66) = 4 \cdot 84 + (-5) \cdot 66 \\ &= 4 \cdot 84 + (-5) \cdot (990 - 84 \cdot 11) = (-5) \cdot 990 + 59 \cdot 84 \end{aligned}$$

Ejemplo 3

2. Para los restantes valores de c halla las soluciones.

Solución (cont.)

- $c = 12, \qquad 84x + 990y = 12$

$$\begin{aligned} 84 \cdot 59 + 990 \cdot (-5) = 6 \quad &\Longrightarrow \quad 84 \cdot 59 \cdot 2 + 990 \cdot (-5) \cdot 2 = 6 \cdot 2 \\ &\Longrightarrow \quad 84 \cdot 118 + 990 \cdot (-10) = 12 \end{aligned}$$

- $c = 18, \qquad 84x + 990y = 18$

$$\begin{aligned} 84 \cdot 59 + 990 \cdot (-5) = 6 \quad &\Longrightarrow \quad 84 \cdot 59 \cdot 3 + 990 \cdot (-5) \cdot 3 = 6 \cdot 3 \\ &\Longrightarrow \quad 84 \cdot 177 + 990 \cdot (-15) = 18 \end{aligned}$$

Ejercicio: Se quieren retirar 510 euros de un cajero automático que sólo dispensa billetes de 20 y 50 euros. ¿Podremos hacer esto? Si es así, ¿cuántos billetes de cada tipo se pueden recibir?

Solución: Considerando las variables

x: el **número** de billetes de **20** euros
y: el **número** de billetes de **50** euros

que dispensa el cajero para dicha extracción, contestaremos a las preguntas resolviendo la ecuación

$$20x + 50y = 510, \quad \text{con} \quad x \geq 0,\ y \geq 0$$

Solución:

1. En primer lugar, estudiamos si existen soluciones enteras para la ecuación $20x + 50y = 510, \quad \text{con} \quad x \geq 0,\ y \geq 0$:

$$\left.\begin{array}{rcl} mcd(20,50) & = & 10 \\ 10 & \mid & 510 \end{array}\right\}$$

   Luego $20x + 50y = 510$ tiene soluciones enteras.

2. Hallamos una **solución particular**, a partir de la identidad de Bezout.

$$10 = 20(-2) + 50 \Longrightarrow 510 = 20(-102) + 50(51)$$

   Una solución particular es $x_0 = -102, \qquad y_0 = 51$.
   Pero no nos sirve por ser x_0 negativa.

3. Damos la solución general a partir de la solución particular:

$$510 = 20(-102 + 5k) + 50(51 - 2k), \quad k \in \mathbb{Z}$$

$$x = -102 + 5k, \qquad y = 51 - 2k, \quad k \in \mathbb{Z}$$

4. Hallamos las soluciones enteras no negativas.
   Al imponer $x \geq 0,\ y \geq 0$ se obtienen los valores que puede tomar k:

$$\left.\begin{array}{lcl} 0 \leq -102 + 5k & \Longrightarrow & 20{,}4 = \dfrac{102}{5} \leq k \\ 0 \leq 51 - 2k & \Longrightarrow & k \leq \dfrac{51}{2} = 25{,}5 \end{array}\right\} \Longrightarrow \quad 21 \leq k \leq 25$$

   Por lo tanto, las posibles soluciones (x, y) son:

$$(3, 9),\ (8, 7),\ (13, 5),\ (18, 3),\ (23, 1)$$