ÁLGEBRA Curso 2008/09

Tema III. ARITMÉTICA ENTERA Y MODULAR.

José Juan Carreño Carreño

Departamento de Matemática Aplicada
Escuela Universitaria de Informática
Universidad Politécnica de Madrid

ÍNDICE

Tema III. ARITMÉTICA ENTERA Y MODULAR.

1. Divisibilidad en $\mathbb{Z}$.
   - Definición y propiedades.
   - **Teorema fundamental de la aritmética.**
   - Máximo común divisor. **Algoritmo de Euclides.**
   - **Teorema de Bézout. Algoritmo de Euclides extendido.**
   - Ecuaciones diofánticas lineales.
2. Aritmética modular.
   - Suma y producto en $\mathbb{Z}_n$. Propiedades.
   - Ecuaciones modulares.

Definición y propiedades. 1

♣ **Definición:** *Dados* $a, b \in \mathbb{Z}$ *se dice que* a ***divide a*** b*, y lo notamos* $a \mid b$*, si existe* $c \in \mathbb{Z}$ *tal que* $b = a \cdot c$.

Si $a \mid b$ *se dice también que*

- a ***es divisor de*** b

o bien que

- b ***es múltiplo de*** a.

Si a ***no divide a*** b *se denota* $a \nmid b$.

⋆ **Ejemplo:**

Definición y propiedades. 2

♣ **Proposición:** *Para todo* $a, b, c \in \mathbb{Z}$ *se verifica:*

1. $1 \mid a, \quad -1 \mid a, \quad a \mid 0.$
2. $\pm a \mid a, \quad |a| \mid a.$
3. *Si* $a \mid b$ *y* $b \mid a \implies a = \pm b.$
4. *Si* $a \mid b \implies a \mid b \cdot x \quad \forall x \in \mathbb{Z}.$
5. *Si* $a \mid b,\ a \mid c \implies a \mid bx + cy \quad \forall x, y \in \mathbb{Z}.$
6. *Si* $x = y + z,\ a \mid x,\ a \mid y \implies a \mid z \quad \forall x, y, z \in \mathbb{Z}.$

DEM.

Teorema fundamental de la aritmética. 1

♣ **Definición:** *Sea $p \in \mathbb{N},\ p > 1$. Diremos que p es un* **número primo** *si sus únicos divisores en $\mathbb{N}$ son 1 y p, es decir:*

$$\forall\, n \in \mathbb{N}: \quad n \mid p \implies n = 1 \text{ ó } n = p.$$

Si $n \in \mathbb{N}, n > 1$ y n no es primo, se dice que n es ***compuesto***.

⋆ **Ejemplo:**

♣ **Teorema:** *Sea $n \in \mathbb{N},\ n > 1$, entonces n es divisible por, al menos, un número primo.*

Teorema fundamental de la aritmética. 2

♣ Teorema: Teorema Fundamental de la Aritmética

Todo número $n \in \mathbb{N},\ n > 1$, se descompone de manera única, salvo el orden de los factores, como producto de números primos, es decir,

existen únicos $p_1, \ldots, p_r \in \mathbb{N},$ números primos,

y existen únicos $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$:

$$n = {p_1}^{\alpha_1} \ldots {p_r}^{\alpha_r}$$

Esta expresión recibe el nombre de **descomposición en factores primos de** n.

⋆ Ejemplo:

Máximo común divisor. 1

♣ **Proposición:** $\forall a \in \mathbb{Z}$ *se tiene que*

$$\text{divisores}(a) = \text{divisores}(|a|).$$

Definiciones: *Sean* $a, b, d \in \mathbb{Z}$. *Se dice que:*

1. d *es un* ***divisor común*** *de* a *y* b *si* $d \mid a$ *y* $d \mid b$.
2. d *es el* ***máximo común divisor*** *de* a *y* b, *no simultáneamente nulos, si* d *es el mayor de los divisores comunes de* a *y* b.

   Lo denotaremos por $d = \text{mcd}(a, b)$.

Por convenio, $\text{mcd}(0, 0) = 0$.

⋆ **Ejemplo:**

Máximo común divisor. 2

♣ **Proposición:** $\forall a, b \in \mathbb{Z}$ *se verifica*

1. $\mathrm{mcd}(a, b) \geq 0$.
2. $\mathrm{mcd}(a, 0) = |a|$.
3. $\mathrm{mcd}(a, na) = |a|, \quad \forall n \in \mathbb{Z}$.
4. $\mathrm{mcd}(a, b) = \mathrm{mcd}(|a|, |b|)$.

♣ **Definición:** *Se dice que* $a, b \in \mathbb{Z}$ *son* **primos relativos** *si los únicos divisores comunes de* a *y* b *son* 1 *y* -1, *es decir, si* $\mathrm{mcd}(a, b) = 1$.

⋆ **Ejemplo:**

♣ **Proposición:** *Sean* $a, b \in \mathbb{Z}$ *tales que* $a, b > 1$. *El* $\mathrm{mcd}(a, b)$ *coincide con el producto de los primos comunes de las descomposiciones en factores primos de* a *y* b *elevados al menor exponente.*

⋆ **Ejemplo:**

Máximo común divisor. 3

♣ **Proposición:** *Sean $a, b \in \mathbb{Z}^*$, $b \neq 0$, y sea r el resto de la división euclídea de a por b, es decir: $a = b \cdot q + r$ con $0 \leq r < |b|$. Entonces, se verifica que:*

1. *Los divisores comunes de a y b son divisores de r.*
2. *Los divisores comunes de b y r son divisores de a.*

♣ **Proposición:** *Sean $a, b \in \mathbb{Z}^*$, $b \neq 0$, y sea r el resto de la división euclídea de a por b, es decir: $a = b \cdot q + r$ con $0 \leq r < |b|$. Entonces, se verifica que:*

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r).$$

Algoritmo de Euclides. 1

♣ Proposición: Algoritmo de Euclides

Sean $a, b \in \mathbb{N}$, tales que $a \geq b > 0$. Si aplicamos el teorema de división euclídea sucesivas veces, tomando $r_0 = a$ y $r_1 = b$, y las divisiones sucesivas son:

$$
\begin{array}{lll}
r_0 = r_1 \cdot q_1 + r_2 & \text{con} & 0 < r_2 < r_1 \\
r_1 = r_2 \cdot q_2 + r_3 & \text{con} & 0 < r_3 < r_2 \\
r_2 = r_3 \cdot q_3 + r_4 & \text{con} & 0 < r_4 < r_3 \\
\quad \vdots & & \quad \vdots \\
r_i = r_{i+1} \cdot q_{i+1} + r_{i+2} & \text{con} & 0 < r_{i+2} < r_{i+1} \\
\quad \vdots & & \quad \vdots \\
r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n & \text{con} & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n \cdot q_n + r_{n+1} & \text{con} & r_{n+1} = 0
\end{array}
$$

entonces, se verifica que $\mathrm{mcd}(a, b) = r_n$
*el **último resto no nulo** de las anteriores divisiones.*

Algoritmo de Euclides. 2

∗ **Observaciones:** La condición: $a \geq b > 0$, del algoritmo de Euclides no es ninguna restricción pues:

1. Como $\mathrm{mcd}(a, b) = \mathrm{mcd}(|a|, |b|)$ este algoritmo puede utilizarse para enteros cualesquiera.
2. Si en el algoritmo de Euclides se efectúa la primera división tomando como divisor el mayor de los dos números dados se realiza una división más que no aporta nada significativo.
3. Es habitual disponer los términos de las divisiones en una tabla como la siguiente:

$r_0 = a$	$r_1 = b$	r_2	$\cdots$	r_{n-1}	r_n	$r_{n+1} = 0$
	q_1	q_2	$\cdots$	q_{n-1}	q_n	

⋆ **Ejemplo:**

Algoritmo de Euclides. 3

♣ **Teorema:** **Teorema de Bézout.**

Sean $a, b \in \mathbb{N}^*$. *Entonces se verifica:*

$$\exists x, y \in \mathbb{Z} \quad \textit{tales que} \quad \mathrm{mcd}(a, b) = ax + by.$$

En particular, si $\mathrm{mcd}(a, b) = 1$ *entonces*

$$\exists x, y \in \mathbb{Z} \quad \textit{tales que} \quad 1 = ax + by.$$

Esta propiedad se llama ***identidad de Bezout.***

∗ **Observación:** El recíproco de la *identidad de Bézout* también se verifica:

$$\mathrm{mcd}(a, b) = 1 \iff \exists x, y \in \mathbb{Z} \,/\, \quad 1 = ax + by.$$

En este caso, para todo $m \in \mathbb{Z}$ se verifica que

$$\exists x, y \in \mathbb{Z} \quad \text{tales que} \quad m = ax + by.$$

⋆ **Ejemplo:**

Algoritmo de Euclides extendido. 1

El algoritmo de Euclides extendido permite hallar:

- dados dos números $a, b \in \mathbb{N}$, tales que $a \geq b > 0$, el $\mathrm{mcd}(a, b)$
- y a la vez calcular dos números $x, y \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, b) = ax + by$.

Algoritmo de Euclides extendido.

Para calcular el máximo común divisor de dos números $a, b \in \mathbb{N}$, tales que $a \geq b > 0$, se hace lo siguiente:

Algoritmo de Euclides extendido. 2

Algoritmo de Euclides extendido.

1. $r_0 := a, \quad x_0 := 1, \quad y_0 := 0.$
2. $r_1 := b, \quad x_1 := 0, \quad y_1 := 1.$
3. $i := 1.$
4. Si $r_i = 0$ devolver r_{i-1}.
5. Si $r_i > 0$, hacer
   - Dividir r_{i-1} entre r_i generando q_i y r_{i+1} que verifican:
     $$r_{i-1} = q_i \cdot r_i + r_{i+1} \quad \text{con} \quad 0 \leq r_{i+1} < r_i.$$
   - Definir $x_{i+1} := x_{i-1} - q_i x_i$ e $y_{i+1} := y_{i-1} - q_i y_i$.
   - Asignar $i := i + 1$ y volver a (4).

Además, si r_n es el último resto no nulo, se tiene que

$$\mathrm{mcd}(a, b) = r_n = ax_n + by_n.$$

De hecho $r_i = ax_i + by_i, \quad \forall i = 0, \ldots, n.$

Algoritmo de Euclides extendido.

- **Ejemplo:**

Propiedades de divisibilidad.

♣ Proposición:

$\forall a, b, d, p \in \mathbb{Z}$ *se verifica que:*

1. *Si* $d \mid a \cdot b$ *y* $\operatorname{mcd}(d, a) = 1 \implies d \mid b$.
2. *Si* $p \mid a \cdot b$, $p \nmid a$ *y* p *es primo* $\implies p \mid b$.
3. *Si* $p \mid a \cdot b$ *y* p *es primo* $\implies p \mid a$ *ó* $p \mid b$.
4. *Si* $d \mid a$ *y* $d \mid b \implies d \mid \operatorname{mcd}(a, b)$.

DEM. □

Ecuaciones diofánticas lineales. 1

♣ **Definición:** *Una ecuación se llama **diofántica** cuando sólo interesan sus soluciones enteras. Una ecuación diofántica del tipo* $ax + by = c$ *con* $a, b, c \in \mathbb{Z}$ *se llama **ecuación diofántica lineal** en dos variables.*

⋆ **Ejemplo:** Se considera el siguiente problema:

Una persona quiere gastarse exactamente 150 € en adquirir dos productos distintos, de los que cada unidad cuesta 48 € y 18 €, respectivamente.
¿Cuántas unidades puede comprar de cada producto?
Dar todas las posibles soluciones.

Ecuaciones diofánticas lineales. 2

♣ **Teorema:** *Se considera la ecuación diofántica*

$$ax + by = c \quad \text{con} \quad a, b, c \in \mathbb{Z} \quad y \quad d = \text{mcd}(a, b).$$

1. *Si* $d \nmid c$ *entonces la ecuación no tiene soluciones enteras.*
2. *Si* $d \mid c$ *entonces la ecuación tiene infinitas soluciones enteras.*
   En este caso, si (x_0, y_0) *es una solución particular de la ecuación, entonces todas las soluciones son:*

$$\left.\begin{array}{l} x = x_0 + \dfrac{b}{d}\,k \\ \\ y = y_0 - \dfrac{a}{d}\,k \end{array}\right\} \quad \forall k \in \mathbb{Z}.$$

DEM. □

Ecuaciones diofánticas lineales. 3

⋆ **Ejemplo:**

∗ **Nota:** Si la ecuación diofántica $ax + by = c$ tiene solución, para resolverla conviene **simplificarla dividiendo ambos miembros de la ecuación por** $\mathrm{mcd}(a, b)$, ya que se obtiene una nueva ecuación más sencilla de resolver y que es equivalente a la anterior, es decir, que tiene las mismas soluciones.

⋆ **Ejemplo:**

Suma y producto en $\mathbb{Z}_n$. Propiedades.

En el conjunto cociente de la relación de equivalencia de **congruencia módulo** n en $\mathbb{Z}$:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

se quiere definir una suma y un producto, que en algunos casos mejora las propiedades de $\mathbb{Z}$.

♣ **Teorema:** *En $\mathbb{Z}_n$ se puede definir una operación binaria, llamada* **suma de clases**, *de la siguiente manera:*

$$\begin{array}{rccc} \oplus : & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \oplus \overline{b} = \overline{a+b} \end{array}$$

que verifica:

Suma y producto en $\mathbb{Z}_n$. Propiedades. 2

1. $\oplus$ **está bien definida**, es decir, es una operación interna en $\mathbb{Z}_n$.
2. $\overline{a} \oplus (\overline{b} \oplus \overline{c}) = (\overline{a} \oplus \overline{b}) \oplus \overline{c}, \quad \forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ **(P. Asociativa)**.
3. $\exists\, \overline{0} \in \mathbb{Z}_n : \quad \overline{a} \oplus \overline{0} = \overline{0} \oplus \overline{a} = \overline{a}, \quad \forall\, \overline{a} \in \mathbb{Z}_n$ **(Existencia de elemento neutro)**.
4. $\forall\, \overline{a} \in \mathbb{Z}_n \ \exists\, \overline{a'} \in \mathbb{Z}_n : \quad \overline{a} \oplus \overline{a'} = \overline{a'} \oplus \overline{a} = \overline{0}$ **(Existencia de elemento opuesto)**.
   Al elemento $\overline{a'}$ lo llamaremos **opuesto** de $\overline{a}$ y lo notaremos $-\overline{a}$.
5. $\overline{a} \oplus \overline{b} = \overline{b} \oplus \overline{a}, \quad \forall\, \overline{a}, \overline{b} \in \mathbb{Z}_n$ **(P. Conmutativa)**.

DEM.

□

Suma y producto en $\mathbb{Z}_n$. Propiedades.

⋆ **Ejemplo:** Tablas de la suma en $\mathbb{Z}_2$ y $\mathbb{Z}_5$.

$\oplus$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Suma y producto en $\mathbb{Z}_n$. Propiedades.

⋆ **Notación:** Dados $a, k \in \mathbb{Z}$ notaremos por

$$k \cdot \overline{a} = \begin{cases} \overline{0} & k = 0 \\ \overline{a} \oplus \overset{k)}{\ldots} \oplus \overline{a} & k > 0 \\ (-\overline{a}) \oplus \overset{-k)}{\ldots} \oplus (-\overline{a}) & k < 0 \end{cases}$$

⋆ **Ejemplo:** En $\mathbb{Z}_3$, con la notación anterior:

- $4 \cdot \overline{2} = \overline{2} \oplus \overline{2} \oplus \overline{2} \oplus \overline{2} = \overline{2+2+2+2} = \overline{4 \cdot 2} = \overline{8} = \overline{2}.$
- $-4 \cdot \overline{2} = \overline{(-2)} \oplus \overline{(-2)} \oplus \overline{(-2)} \oplus \overline{(-2)} =$
  $= \overline{1} \oplus \overline{1} \oplus \overline{1} \oplus \overline{1} = \overline{4 \cdot 1} = \overline{4} = \overline{1}.$

Suma y producto en $\mathbb{Z}_n$. Propiedades.

♣ Teorema:

En $\mathbb{Z}_n$ se puede definir una operación binaria, llamada **producto de clases**,

$$\begin{array}{rccc} \odot : & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \odot \overline{b} = \overline{a \cdot b} \end{array}$$

que verifica las propiedades siguientes

Suma y producto en $\mathbb{Z}_n$. Propiedades. 6

1. $\odot$ **está bien definida**, es decir, es una operación interna en $\mathbb{Z}_n$.
2. $\overline{a} \odot (\overline{b} \odot \overline{c}) = (\overline{a} \odot \overline{b}) \odot \overline{c}, \quad \forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ **(P. Asociativa).**
3. $\exists\, \overline{1} \in \mathbb{Z}_n : \overline{a} \odot \overline{1} = \overline{1} \odot \overline{a} = \overline{a}, \quad \forall\, \overline{a} \in \mathbb{Z}_n$ **(Existencia de elemento neutro).**
4. $\forall\, \overline{a} \in \mathbb{Z}_n^*$ tal que $mcd(a, n) = 1, \quad \exists\, \overline{a'} \in \mathbb{Z}_n^* : \overline{a} \odot \overline{a'} = \overline{a'} \odot \overline{a} = \overline{1}$.
   (Existencia de elemento inverso)

   Al elemento $\overline{a'}$ lo llamaremos **inverso** de $\overline{a}$ y lo notaremos $\overline{a}^{-1}$. En particular, si p es primo:

   $$\forall\, \overline{a} \in \mathbb{Z}_p^* \ \exists\, \overline{a}^{-1} \in \mathbb{Z}_p^* : \quad \overline{a} \odot \overline{a}^{-1} = \overline{1}.$$

5. $\overline{a} \odot \overline{b} = \overline{b} \odot \overline{a}, \quad \forall\, \overline{a}, \overline{b} \in \mathbb{Z}_n$ **(P. Conmutativa).**

Suma y producto en $\mathbb{Z}_n$. Propiedades.

Además se verifica la **propiedad distributiva del producto respecto de la suma**:

$$\overline{a} \odot (\overline{b} \oplus \overline{c}) = (\overline{a} \odot \overline{b}) \oplus (\overline{a} \odot \overline{c}), \quad \forall\, \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n.$$

$\star$ **Notación:** Denotaremos la suma y el producto de clases con los símbolos de la suma y producto habituales, es decir, $\overline{a} \oplus \overline{b}$ lo notaremos $\overline{a} + \overline{b}$. Igual para el producto: $\overline{a} \cdot \overline{b}$.

$*$ **Observación:** $(\mathbb{Z}_n, +, \cdot)$ tiene **estructura de anillo** por verificar las propiedades de los teoremas anteriores. Además cuando p es primo, cada elemento de $\mathbb{Z}_p^*$ tiene inverso y, por tanto, $(\mathbb{Z}_p, +, \cdot)$ tiene **estructura de cuerpo**.

Suma y producto en $\mathbb{Z}_n$. Propiedades.

⋆ **Ejemplo:** Tablas del producto en $\mathbb{Z}_4$ y $\mathbb{Z}_5$.

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

⋆ **Observaciones:**

Suma y producto en $\mathbb{Z}_n$. Propiedades.

♣ **Proposición:** ***(Propiedad cancelativa en*** $(\mathbb{Z}_n, \cdot)$***)***

Sean $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ *entonces se verifica*

$$\overline{a} \cdot \overline{c} = \overline{b} \cdot \overline{c} \quad y \quad \operatorname{mcd}(n, c) = 1 \quad \Longrightarrow \quad \overline{a} = \overline{b}.$$

∗ **Nota:** Si $\operatorname{mcd}(n, c) \neq 1$ el resultado anterior es falso.

⋆ **Ejemplo:**

Suma y producto en $\mathbb{Z}_n$. Propiedades.

⋆ **Notación:** Dados $a, k \in \mathbb{Z}$ notaremos por

$$\overline{a}^k = \begin{cases} \overline{1} & k = 0 \\ \overline{a} \odot \overset{k)}{\ldots} \odot \overline{a} & k > 0 \\ \overline{a}^{-1} \odot \overset{-k)}{\ldots} \odot \overline{a}^{-1} & k < 0, \text{ si está definido } \overline{a}^{-1}. \end{cases}$$

⋆ **Ejemplo:**

Ecuaciones modulares. 1

Las **ecuaciones modulares** son ecuaciones de la forma

$$a\,x \equiv c\ (mod\ n) \qquad \text{o, equivalentemente}$$

$$\overline{a} \cdot \overline{x} = \overline{c} \quad \text{en} \quad \mathbb{Z}_n.$$

Estas ecuaciones tienen aplicaciones importantes. También en Informática, como es la aplicación en ***Criptología***, que *es la ciencia que se encarga de ocultar la información de forma que solo pueda entenderla su destinatario*.

Ecuaciones modulares. 2

Uno de los ***sistemas criptográficos*** más antiguos es el conocido con el nombre de **Julio Cesar**.

El ***proceso de cifrado*** consistía en:

- Traducir las letras a números (aplicación biyectiva).
- Aplicar una transformación a estos números (aplicación afín).
- La cadena de números resultante se vuelve a traducir a letras (inversa de la biyección).

Entonces se manda la *información cifrada*, que el receptor se encarga de *descifrar*.

Ecuaciones modulares. 3

La biyección f entre números y letras viene dada por la tabla:

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	Ñ	O	P	Q	R	S
10	11	12	13	14	15	16	17	18	19
T	U	V	W	X	Y	Z			
20	21	22	23	24	25	26			

La transformación utilizada por los romanos era:

$$C \equiv P + 3 (mod\ 27), \quad \text{con} \quad 0 \leq P \leq 26.$$

Ecuaciones modulares. 4

Por ejemplo: llamamos T a la transformación anterior

Si se quiere cifrar el mensaje PAZ

$$\text{PAZ} \xrightarrow{f} 16\ \ 0\ \ 26 \xrightarrow{T} 19\ \ 3\ \ 2 \xrightarrow{f^{-1}} \text{SDC}$$

el mensaje cifrado que se envía es SDC.

Ecuaciones modulares. 5

Para obtener el *mensaje en claro*, el receptor debe realizar el proceso inverso. Para ello emplea la función inversa de la función de cifrado:

$$P \equiv C + 24 (mod\ 27), \quad \text{con} \quad 0 \leq C \leq 26.$$

La transformación T es un caso particular de la familia de las transformaciones siguientes:

$$C \equiv aP + b (mod\ n), \quad \text{donde} \quad \mathrm{mcd}(a, n) = 1.$$

Estas transformaciones se llaman **transformaciones afines**.

Ecuaciones modulares. 6

En el proceso de codificación hay que resolver ecuaciones modulares.

Veamos cómo se resuelven las ecuaciones modulares del tipo:

$$\overline{a} \cdot \overline{x} = \overline{c} \quad \text{en} \quad \mathbb{Z}_n$$

que se corresponden con transformaciones afines en las que $b = 0$.

Ecuaciones modulares. 7

♣ **Proposición:** *Sean* $a, c \in \mathbb{Z}$, $n \in \mathbb{N}^*$, $mcd(n, a) = d$.

La siguiente ecuación de $\mathbb{Z}_n$, $\overline{a} \cdot \overline{x} = \overline{c}$:

1. *si* $d \nmid c$ *entonces no tiene soluciones.*
2. *si* $d \mid c$ *tiene exactamente* d *soluciones en* $\mathbb{Z}_n$.
   En este caso la ecuación diofántica tiene infinitas soluciones enteras de la forma:

$$x = x_0 + \frac{n}{d}k, \quad y = y_0 - \frac{a}{d}k, \quad con \quad k \in \mathbb{Z}.$$

Solo nos interesan los valores de x.
Se verifica que sólo hay d *soluciones distintas en* $\mathbb{Z}_n$:

$$\overline{x}_0, \quad \overline{x}_1 = \overline{x_0 + \frac{n}{d}},$$

$$\overline{x}_2 = \overline{x_0 + 2\frac{n}{d}}, \ \ldots \ , \overline{x}_{d-1} = \overline{x_0 + (d-1)\frac{n}{d}}.$$

Ecuaciones modulares. 8

∗ **Nota:** En particular, si $\mathrm{mcd}(n, a) = 1$, la ecuación $\overline{a} \cdot \overline{x} = \overline{c}$ tiene solución única:

$$\overline{x} = \overline{a}^{-1} \cdot \overline{c}$$

DEM.

□

∗ **Observación:** La ecuación modular $\overline{a} \cdot \overline{x} = \overline{c}$ tiene solución en $\mathbb{Z}_n$
$\iff$ la ecuación diofántica $ax + ny = c$ tiene soluciones enteras.

∗ **Nota:** La ecuación $ax + ny = c$ se llama ecuación diofántica asociada a la ecuación modular $\overline{a} \cdot \overline{x} = \overline{c}$.

⋆ **Ejemplo:**