

## Tema 1

# Aritmética modular y aplicación a la Criptografía

Recuerda que estas notas son, únicamente, parte del material de trabajo de los profesores de esta asignatura. Los contenidos de este tema se pueden ver en los siguientes libros:

- García Merayo, F. y otros. Problemas Resueltos de Matemática Discreta. Ed. Thomson. (Capítulo 1).
- Rosen, K. H. Matemática Discreta y sus aplicaciones. Ed. McGraw-Hill Interamericana. (Tema 2).
- Biggs, N. L. Matemática Discreta. Ed. Vicens Vives (Parte I).
- Bujalance, E. y otros. Elementos de Matemática Discreta. Ed. Sanz y Torres (Tema 1).

### 1.1 Divisibilidad en $\mathbb{Z}$

Por  $\mathbb{Z}$  se denota el conjunto de los números enteros. La división entera de dos números enteros  $a$  y  $b$  es una operación aritmética que consiste en el cálculo de dos enteros, llamados cociente y resto de la división,

$$\begin{array}{ccc}
 & \text{dividendo} & \\
 & \swarrow \quad \searrow & \\
 a & | & b \\
 & \swarrow \quad \searrow & \\
 & r & q \\
 & \text{resto} & \text{cociente}
 \end{array}
 \qquad \text{de modo que } a = bq + r, \text{ con } 0 \leq r < |b|.$$

Si  $b = 0$  la división no está definida.

**Teorema 1.1. (Algoritmo de la división entera)** Sean  $a, b \in \mathbb{Z}$ . Si  $b \neq 0$  entonces existen dos únicos enteros  $q$  y  $r$  tales que  $a = bq + r$  y  $0 \leq r < |b|$ .

La condición  $0 \leq r < |b|$  es la que garantiza que el cociente y resto son únicos. Además, en particular, si  $b > 0$  entonces existen dos únicos enteros  $q$  y  $r$  tales que

$$a = bq + r \text{ con } 0 \leq r < b.$$

*Demostración.* En primer lugar, probamos la existencia y, en segundo lugar, la unicidad. Supongamos, además, que  $b > 0$ .

### Existencia:

Sea el conjunto  $M = \{tb \in \mathbb{Z} \mid tb \leq a\}$ . Es claro que  $M \neq \emptyset$ , ya que basta considerar  $t$  suficientemente pequeño. Además, por construcción, podemos decir que  $M$  está acotado superiormente por  $a$ . Así, como  $M$  es un subconjunto no vacío de números enteros acotado superiormente, admite máximo. Sea  $qb$  dicho máximo. Es evidente que:

$$qb \leq a < (q+1)b.$$

Si ahora llamamos  $r = a - bq$ , entonces  $0 \leq r < b$ .

### Unicidad:

Sean  $q_1, q_2, r_1$  y  $r_2$  enteros tales que

$$a = bq_1 + r_1, \quad a = bq_2 + r_2, \quad \text{con } 0 \leq r_1, r_2 < b;$$

restando ambas expresiones  $b(q_1 - q_2) = r_2 - r_1$  y, por tanto

$$b|q_1 - q_2| = |r_2 - r_1| < b$$

ya que  $0 \leq r_1, r_2 < b$ .

Si suponemos que  $q_1 \neq q_2$ , entonces  $|q_1 - q_2| \geq 1$ , por tanto

$$|r_2 - r_1| = b|q_1 - q_2| \geq b,$$

lo que no puede ser, así  $q_1 = q_2$  y  $r_1 = r_2$ .

Por último, si  $b < 0$ , lo que vimos hasta ahora nos garantiza la existencia de dos únicos enteros  $q$  y  $r$  tales que  $0 \leq r < -b = |b|$  y  $a = (-b)q + r = b(-q) + r$ ; por tanto tenemos el resultado para todo  $b \in \mathbb{Z}$  con  $b \neq 0$ . ■

### Ejemplo 1.2.

- i) Si  $a = -13$  y  $b = 6$  el cociente es  $q = -3$  y el resto  $r = 5$ .

En efecto, aunque la siguiente igualdad es cierta

$$-13 = 6 \cdot (-2) + (-1),$$

el resto no es  $-1 < 0$ . El resultado correcto es

$$\begin{array}{r} -13 \\ \hline 5 \quad | 6 \\ \quad \quad -3 \end{array} \quad \text{de modo que } -13 = 6 \cdot (-3) + 5, \text{ con } 0 \leq r = 5 < |b| = 6.$$

Nótese que, aunque el múltiplo de 6 más próximo a  $-13$  es  $6 \cdot (-2) = -12$ , nos interesa que el resto sea positivo, por tanto elegimos el múltiplo  $6 \cdot (-3) = -18$ .



ii) Análogamente

$$\begin{array}{c} 23 \quad | -5 \\ 3 \quad \underline{-4} \\ 23 = -5 \cdot (-4) + 3 \\ 0 \leq r = 3 < |-5| \end{array} \quad \begin{array}{c} -23 \quad | 5 \\ 2 \quad \underline{-5} \\ -23 = 5 \cdot (-5) + 2 \\ 0 \leq r = 2 < |5| \end{array} \quad \begin{array}{c} -23 \quad | -5 \\ 2 \quad \underline{5} \\ -23 = -5 \cdot 5 + 2 \\ 0 \leq r = 2 < |-5| \end{array}$$

**Observación.** Al dividir  $a$  entre  $b$  los posibles restos son  $0, 1, \dots, |b| - 1$ . Esto nos permite clasificar los infinitos números enteros teniendo en cuenta el resto que obtenemos al dividir entre  $b$ . Por ejemplo, si  $b = 2$  tenemos la clasificación de los enteros en pares o impares.

En esta parte del tema, estudiamos números que al dividirlos obtenemos resto igual a cero.

**Definición 1.3.** Sean  $a, b, d \in \mathbb{Z}$ . Decimos que

i)  $b$  es un **divisor** de  $a$  (o que  $b$  **divide a**) o que  $a$  es un **múltiplo** de  $b$ ) si existe algún número entero  $q$  tal que  $a = bq$ .

Lo denotamos por  $b|a$  o también por  $a = b$ .

ii)  $d$  es **divisor común** de  $a$  y  $b$  si  $d|a$  y  $d|b$ .

**Ejemplo 1.4.** Cualquier entero, distinto de 1 y  $-1$ , tiene al menos cuatro divisores, el mismo, su opuesto, 1 y  $-1$ . Algunos números no tienen más divisores que esos, como 2, 3, 5, 7, ... y otros números tienen varios divisores, por ejemplo 12 tiene divisores:  $1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12$ .

Los divisores comunes a 20 y 12 son:  $1, -1, 2, -2, 4, -4$ .

**Definición 1.5.** Un número natural  $n \geq 2$  es **primo** si sus únicos divisores positivos son 1 y  $n$ . Si un número no es primo se denomina **compuesto**.

**Ejemplo 1.6.** Los primeros números primos son 2, 3, 5, 7, 11, 13. Los números 4, 6, 8, 9, 10, 12, 14, 15 son compuestos.

El siguiente resultado es un método elemental para el reconocimiento de primos.

**Teorema 1.7. (Criba de Eratóstenes)** Sea  $a$  un número entero mayor que 1. Si, para todo primo  $p$  con  $p \leq \sqrt{a}$ , se tiene que  $p \nmid a$ , entonces  $a$  es primo.

**Demostración.** La comprobación del resultado anterior es muy sencilla. Si suponemos que  $a$  no es primo, es decir, que existen  $1 < b \leq c < a$  tales que  $a = bc$ , entonces es claro que  $b^2 \leq a$ , es decir  $b \leq \sqrt{a}$ . Si  $b$  es primo, llegaríamos a una contradicción y si no lo es, podemos elegir un  $p$  primo que divida a  $b$ . Así  $p \leq b \leq \sqrt{a}$ . Como  $p \mid b$  y  $b \mid a$ , se tiene que  $p \mid a$  y de nuevo una contradicción. ■

**Ejemplo 1.8.** Encontremos todos los primos menores que 60. Como  $7^2 = 49 < 60 < 8^2 = 64$ , si un primo  $p \leq \sqrt{60}$ , se tiene que  $p = 2, 3, 5$  o 7. Escribiendo todos los números enteros entre 1 y

60 y tachando los múltiplos de los primos anteriores, la criba de Eratóstenes garantiza que los números restantes son primos.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

**Definición 1.9.** Sean  $a, b, d \in \mathbb{Z}$ ,  $a, b$  no nulos. Decimos que

- i) El **máximo común divisor** de  $a$  y  $b$ , denotado por  $d = \text{mcd}(a, b)$ , es un divisor común de  $a$  y  $b$  tal que  $d > 0$  y, para cualquier  $c \in \mathbb{Z}$  tal que  $c|a$  y  $c|b$ , se tiene que  $c|d$ .  
Por convenio  $\text{mcd}(a, 0) = |a|$ . En particular  $\text{mcd}(0, 0) = 0$ .
- ii) En general,  $d = \text{mcd}(a_1, \dots, a_n)$  si  $d > 0$ ,  $d$  es un divisor común,  $d|a_i \forall i, 1 \leq i \leq n$  y, si existe  $c \in \mathbb{Z}$  tal que  $c|a_i \forall i, 1 \leq i \leq n$  entonces  $c|d$ .

**Observación.** Hay que señalar que, para cualesquiera  $a, b \in \mathbb{Z}$  el  $\text{mcd}(a, b)$  existe pues el conjunto  $D = \{n \in \mathbb{Z} \text{ tales que } n|a \wedge n|b\}$  es no vacío, ya que  $1 \in D$ , y está acotado superiormente por  $|a|$  y  $|b|$ .

**Ejemplo 1.10.** Los divisores positivos comunes a 20 y 12 son: 1, 2, 4. Entre los divisores comunes positivos escogemos el máximo y obtenemos que  $4 = \text{mcd}(20, 12)$ .

**Teorema 1.11. (Teorema de Bezout)** Sean  $a$  y  $b$  enteros no ambos nulos. Existen enteros  $r$  y  $s$  tales que

$$\text{mcd}(a, b) = ar + bs.$$

Además,  $d = \text{mcd}(a, b)$  es el menor entero positivo que se puede expresar de esa manera.

Es importante señalar que cuando  $\text{mcd}(a, b) = 1$  se verifica la equivalencia, es decir,

$$\text{mcd}(a, b) = 1 \text{ si, y solo si, } 1 = ar + bs.$$

A continuación, vemos un procedimiento que nos permite calcular el mcd de dos números enteros  $a$  y  $b$ . Para este procedimiento hay que tener en cuenta que los divisores comunes de  $a$  y  $b$  son los mismos que los de  $b$  y  $c$ , en el caso de que  $a = bq + c$ . El siguiente resultado recoge esta idea básica.

**Lema 1.12.** Si  $a, b, q, r$  son números enteros tales que  $a = bq + r$ , entonces

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

*Demostración.* Basta con definir los conjuntos

$$A = \{c \in \mathbb{Z} \mid c|a \wedge c|b\} \quad y \quad B = \{c \in \mathbb{Z} \mid c|b \wedge c|r\}$$

y demostrar que son iguales utilizando que  $a = bq + r$ . De ahí se obtiene la conclusión. ■

## 1.2 Algoritmo de Euclides

Veamos ahora cómo calcular  $\text{mcd}(a, b)$  usando el llamado **Algoritmo de Euclides**. Consideramos que  $a$  y  $b$  son enteros positivos ya que  $\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$ .

Se efectúa la división del entero mayor  $a_0 = a$  entre el menor  $a_1 = b$ , obteniéndose como cociente  $q_1$  y como resto  $a_2$ . A continuación se divide  $a_1$  entre  $a_2$ , obteniéndose como cociente  $q_2$  y resto  $a_3$ . Se continúa hasta obtener una división exacta, es decir un  $a_{k+1} = 0$ . La expresión del algoritmo es:

$$\begin{aligned} a_0 &= a_1 q_1 + a_2 & 0 < a_2 &< a_1 \\ a_1 &= a_2 q_2 + a_3 & 0 < a_3 &< a_2 \\ a_2 &= a_3 q_3 + a_4 & 0 < a_4 &< a_3 \\ &\vdots & &\vdots \\ a_{k-2} &= a_{k-1} q_{k-1} + a_k & 0 < a_k &< a_{k-1} \\ a_{k-1} &= a_k q_k + 0. \end{aligned}$$

Como la cadena de restos es tal que  $a_1 > a_2 > a_3 > \dots$  y son números enteros positivos, se llegará a un resto nulo. Dado que, por el Lema 1.12,

$$\text{mcd}(a_0, a_1) = \text{mcd}(a_1, a_2) = \text{mcd}(a_2, a_3) = \dots = \text{mcd}(a_{k-1}, a_k) = a_k \quad (1.1)$$

se concluye que el máximo común divisor es el último resto no nulo,

$$\text{mcd}(a, b) = \text{mcd}(a_0, a_1) = a_k.$$

**Ejemplo 1.13.** Utilizaremos el Algoritmo de Euclides para obtener  $\text{mcd}(1496, 612)$ :

$$\begin{array}{r} 1496 \longdiv{612} \\ 272 \quad 2 \\ \hline 1496 = 612 \cdot 2 + 272 \end{array} \quad \begin{array}{r} 612 \longdiv{272} \\ 68 \quad 2 \\ \hline 612 = 272 \cdot 2 + 68 \end{array} \quad \begin{array}{r} 272 \longdiv{68} \\ 0 \quad 4 \\ \hline 272 = 68 \cdot 4 + 0 \end{array}$$

con lo que  $\text{mcd}(1496, 612) = 68$ .

**Ejemplo 1.14.** Utilicemos el algoritmo anterior para el cálculo de  $\text{mcd}(250, 111)$ . Se obtiene la siguiente cadena de divisiones:

$$\begin{array}{r} 250 \longdiv{111} \\ 28 \quad 2 \\ \hline 250 = 111 \cdot 2 + 28 \end{array} \quad \begin{array}{r} 111 \longdiv{28} \\ 27 \quad 3 \\ \hline 111 = 28 \cdot 3 + 27 \end{array} \quad \begin{array}{r} 28 \longdiv{27} \\ 1 \quad 1 \\ \hline 28 = 27 \cdot 1 + 1 \end{array} \quad \begin{array}{r} 27 \longdiv{1} \\ 0 \quad 27 \\ \hline 27 = 1 \cdot 27 + 0 \end{array}$$

es decir:  $\text{mcd}(250, 111) = 1$ .

A continuación, **calculamos los números enteros  $r$  y  $s$  tales que  $\text{mcd}(a, b) = ar + bs$** .

Una **primera forma** de obtener los enteros  $r$  y  $s$  es sustituyendo los restos, de forma progresiva, tal y como que sugiere la expresión 1.1 de la página 5, empezando por  $a_k$ , el último resto no nulo. En el Ejemplo 1.13 el proceso es el siguiente:

$$68 = 612 - 272 \cdot 2 = 612 - (1496 - 612 \cdot 2) \cdot 2 = 612 - 1496 \cdot 2 + 612 \cdot 4 = 612 \cdot 5 - 1496 \cdot 2$$

con lo que  $\text{mcd}(1496, 612) = 68 = (-2) \cdot 1496 + 5 \cdot 612$ .

Análogamente, en el Ejemplo 1.14 el proceso es:

$$\begin{aligned} 1 &= 28 - 27 \cdot 1 = 28 - (111 - 28 \cdot 3) \cdot 1 = 28 - 111 + 28 \cdot 3 = 28 \cdot 4 - 111 \\ &= (250 - 111 \cdot 2) \cdot 4 - 111 = 250 \cdot 4 - 111 \cdot 8 - 111 = 250 \cdot 4 - 111 \cdot 9 \end{aligned}$$

de donde se obtiene que  $\text{mcd}(250, 111) = 1 = 4 \cdot 250 + (-9) \cdot 111$ .

Una **segunda forma** de obtener los enteros  $r$  y  $s$ , computacionalmente más efectiva, es la siguiente: supongamos que en el algoritmo obtuvimos  $a_{k+1} = 0$  y  $a_k = \text{mcd}(a, b)$ , entonces elegimos

$$r_0 = 1, \quad r_1 = 0, \quad s_0 = 0 \quad y \quad s_1 = 1.$$

y hallamos enteros  $r_i$  y  $s_i$ , para  $i \geq 2$ , del modo siguiente:

$$r_i = r_{i-2} - r_{i-1}q_{i-1}, \quad s_i = s_{i-2} - s_{i-1}q_{i-1}.$$

Se comprueba por inducción que, para cada  $i \geq 0$ , se verifica que:

$$a_i = ar_i + bs_i.$$

En particular,  $a_k = ar_k + bs_k$ .

Recogemos los resultados para  $\text{mcd}(1496, 612)$ , Ejemplo 1.13, en la siguiente tabla:

$i$	$a_i$	$q_i$	$r_i$	$s_i$
0	1496	-	1	0
1	612	2	0	1
2	272	2	1	-2
3	68	4	-2	5

$$1496 = 612 \cdot 2 + 272$$

$$612 = 272 \cdot 2 + 68$$

$$272 = 68 \cdot 4 + 0,$$

con lo que  $68 = (-2) \cdot 1496 + 5 \cdot 612$ .

Si recopilamos los resultados para  $\text{mcd}(250, 111)$ , Ejemplo 1.14, obtenemos:

$i$	$a_i$	$q_i$	$r_i$	$s_i$
0	250	-	1	0
1	111	2	0	1
2	28	3	1	-2
3	27	1	-3	7
4	1	27	4	-9

$$250 = 111 \cdot 2 + 28$$

$$111 = 28 \cdot 3 + 27$$

$$28 = 27 \cdot 1 + 1$$

$$27 = 1 \cdot 27 + 0$$

De donde se obtiene que  $1 = 4 \cdot 250 + (-9) \cdot 111$ .

Los anteriores algoritmos nos dan la pauta para resolver un importante tipo de ecuaciones que veremos a continuación.



### 1.2.1 Ecuaciones diofánticas lineales

Las ecuaciones diofánticas son una amplia clase de ecuaciones algebraicas (polinómicas) con más de una incógnita en el conjunto de los números enteros; se llaman así en honor al matemático griego Diofanto. Aquí nos centraremos en las ecuaciones diofánticas lineales que tienen la forma  $ax + by = n$ , donde  $a, b$  y  $n$  son números enteros.

**Observación.** Hay que señalar que, si conocemos los enteros  $r, s$  tales que  $ar + bs = \text{mcd}(a, b)$  entonces, en el caso de que  $n = z \cdot \text{mcd}(a, b)$ , obtenemos que  $arz + bsz = z \cdot \text{mcd}(a, b) = n$ .

El siguiente resultado nos da una condición que garantiza la existencia de solución.

**Teorema 1.15.** La ecuación  $ax + by = n$  tiene solución si, y solo si,  $\text{mcd}(a, b)$  divide a  $n$ . Si  $(x_0, y_0)$  es una solución de  $ax + by = n$ , cualquier otra solución  $(x, y)$  es de la forma:

$$x = x_0 + \frac{b}{\text{mcd}(a, b)}t, \quad y = y_0 - \frac{a}{\text{mcd}(a, b)}t, \quad \text{siendo } t \in \mathbb{Z}.$$

*Demostración.* Si la ecuación  $ax + by = n$  tiene solución entera, existen  $x_0, y_0 \in \mathbb{Z}$  de modo que  $ax_0 + by_0 = n$ . Como  $d = \text{mcd}(a, b)$ ,  $a = a_1d$  y  $b = b_1d$ , con  $a_1, b_1 \in \mathbb{Z}$ . Entonces

$$n = ax_0 + by_0 = a_1dx_0 + b_1dy_0 = d(a_1x_0 + b_1y_0)$$

esto es,  $d|n$ .

Recíprocamente, si  $d|n$ , existe  $k \in \mathbb{Z}$  tal que  $n = kd$ . Como  $d = \text{mcd}(a, b)$ , por el Teorema de Bezout, existen  $r, s \in \mathbb{Z}$  de modo que

$$d = r a + s b$$

Multiplicando la igualdad anterior por  $k$  se tiene que

$$n = kd = k(r a + s b) = (kr)a + (ks)b$$

esto es, una solución entera de la ecuación.

Acabamos de comprobar la existencia de solución. Veamos cómo son todas las soluciones enteras de la ecuación.

Es fácil comprobar que si  $(x_0, y_0)$  es una solución de  $ax + by = n$ , también lo es  $x = x_0 + t \frac{b}{d}$  e  $y = y_0 - t \frac{a}{d}$ , basta con sustituir.

Supongamos que  $(x_0, y_0)$  es una solución de  $ax + by = n$ , entonces  $ax_0 + by_0 = n$ . Si  $(x, y)$  es otra solución de la ecuación, tendremos que

$$ax_0 + by_0 = n \quad ax + by = n$$

y restando

$$a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = b(y_0 - y)$$

como  $d = \text{mcd}(a, b)$ , se tiene que  $d|a$  y  $d|b$ ; así

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

Pero,  $a/d$  y  $b/d$  son números enteros primos entre sí (ya que al dividirlos entre su máximo común divisor les hemos quitado los factores que tuvieran en común en un principio), y como  $a/d$  divide a  $\frac{b}{d}(y_0 - y)$  debe cumplirse que  $a/d$  divide a  $y_0 - y$ , por tanto, existe  $t \in \mathbb{Z}$  de modo que

$$y_0 - y = t \frac{a}{d}$$

De ahí,  $y = y_0 - t \frac{a}{d}$ . Y, sustituyendo el valor de  $y$  obtenemos que el valor de  $x$  es,  $x = x_0 + t \frac{b}{d}$ . ■

#### Estudio de las soluciones de la ecuación diofántica $ax + by = n$ .

- i) Estudiamos la existencia de alguna solución comprobando si  $\text{mcd}(a, b)$  divide a  $n$ . En caso afirmativo, existe un entero  $z$  tal que  $n = z \cdot \text{mcd}(a, b)$ .
- ii) Usando el Algoritmo de Euclides, calculamos los enteros  $r, s$  tales que  $ar + bs = \text{mcd}(a, b)$ .
- iii) Una solución particular de la ecuación es  $(x_0, y_0)$  donde  $x_0 = rz, y_0 = sz$ .
- iv) En general, las infinitas soluciones  $(x, y)$  se obtienen de la forma siguiente:

$$\text{para cada } t \in \mathbb{Z}, \quad x = x_0 + t \frac{b}{d}, \quad y = y_0 - t \frac{a}{d}, \quad \text{donde } d = \text{mcd}(a, b).$$

**Ejemplo 1.16.** Para calcular las soluciones de la ecuación diofántica lineal  $20x + 50y = 430$ , dado que  $10 = \text{mcd}(20, 50)$  y que

$$10 = 20 \cdot (-2) + 50 \cdot 1,$$

multiplicando la expresión anterior por 43 obtenemos que

$$430 = 43 \cdot 10 = 20 \cdot 43 \cdot (-2) + 50 \cdot 43 \cdot 1 = 20 \cdot (-86) + 50 \cdot 43,$$

así  $x_0 = -86, y_0 = 43$  es una solución particular, y la solución general viene dada por:

$$x = -86 + 5t, \quad y = 43 - 2t, \quad \text{siendo } t \text{ cualquier número entero.}$$

Curso 2021-2022

### 1.3 Factorización en números primos.

**Definición 1.17.** Sea  $n \geq 2$ . Una **factorización** de  $n$  es una expresión de la forma

$$n = a \cdot b \quad \text{con} \quad 1 \leq a, b \leq n.$$

Si  $a = 1$  o  $b = 1$ , se dice que la **factorización** es **trivial**.

Un número natural  $n \geq 2$  es primo si solo admite la factorización trivial.

Los números enteros  $a_1, a_2, \dots, a_n$  son **primos entre sí** si  $\text{mcd}(a_1, a_2, \dots, a_n) = 1$ .

**Teorema 1.18. (Teorema Fundamental de la Aritmética)** Sea  $n \in \mathbb{Z}$  con  $|n| > 1$ . Existen números primos  $p_1, p_2, \dots, p_r$  tales que

$$n = \pm p_1 p_2 \cdots p_r \quad \text{con} \quad p_1 \leq p_2 \leq \dots \leq p_r.$$

Además, esta factorización es única.

## 1.4. CONGRUENCIAS

**Ejemplo 1.19.**  $10800 = 2 \cdot 5400 = 2^2 \cdot 2700 = \dots = 2^4 \cdot 675 = \dots = 2^4 3^3 5^2$

**Definición 1.20.** Sean  $a, b$  dos enteros no nulos.

- Un número entero  $m$  es **múltiplo común** de  $a$  y  $b$  si  $a|m$  y  $b|m$ .
- El **mínimo común múltiplo** de  $a$  y  $b$ ,  $m = \text{mcm}(a, b)$ , es un múltiplo común de  $a$  y  $b$  tal que  $m > 0$  y,  $\forall c \in \mathbb{Z}$  tal que  $a|c$  y  $b|c$  se tiene que  $m|c$ .
- La definición de mínimo común múltiplo se puede extender a un conjunto finito de enteros de la forma siguiente:  $m = \text{mcm}(a_1, \dots, a_n)$  si  $m > 0$ ,  $a_i|m$  ( $\forall i, 1 \leq i \leq n$ ) y si existe  $c$  tal que  $a_i|c$  ( $\forall i, 1 \leq i \leq n$ ) entonces  $m|c$ .

Nótese que si  $a$  es cualquier entero,  $\text{mcm}(a, 0) = 0$ .

Como consecuencia del Teorema Fundamental de la Aritmética, podemos encontrar primos distintos  $p_1, p_2, \dots, p_r$  tales que:

$$\begin{aligned} a &= \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \\ b &= \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \end{aligned}$$

con  $\alpha_i, \beta_i \geq 0$ . Con esta descomposición se tiene que:

**Teorema 1.21.** Dados  $a, b$  enteros con la descomposición anterior, se verifica que:

$$\text{i) } \text{mcd}(a, b) = \prod_{i=1}^r p_i^{\min(\alpha_i, \beta_i)}$$

$$\text{ii) } \text{mcm}(a, b) = \prod_{i=1}^r p_i^{\max(\alpha_i, \beta_i)}$$

$$\text{iii) Dados } a, b \text{ enteros no nulos se tiene que: } \text{mcm}(a, b) = \frac{|ab|}{\text{mcd}(a, b)}$$

## 1.4 Congruencias

**Definición 1.22.** Sea  $m$  un número natural. Dados  $a, b \in \mathbb{Z}$ , se dice que  $a$  y  $b$  son **congruentes** módulo  $m$  cuando  $a - b$  es divisible por  $m$ . Simbólicamente:

$$a \equiv_m b \text{ si, y solo si, } m|(a - b).$$

La relación  $\equiv_m$  es una relación de equivalencia. El conjunto cociente lo denotaremos por  $\mathbb{Z}_m$ , y la clase de equivalencia de cada entero  $k$  se denominará por  $[k]$ .

**Ejemplo 1.23.**  $7 \equiv_3 4$  y  $18 \equiv_2 6$ .

**Teorema 1.24.** Sean  $a, b, m \in \mathbb{Z}$  y  $m > 0$ . Entonces  $a \equiv_m b$  si, y solo si, el resto obtenido al dividir  $a$  y  $b$  entre  $m$  es el mismo. Como consecuencia, cada número entero es congruente módulo  $m$  con uno de los elementos del conjunto  $\{0, 1, \dots, m - 1\}$ . Así, el conjunto cociente  $\mathbb{Z}_m$  tiene  $m$  elementos:

$$\mathbb{Z}_m = \{[0], [1], \dots, [m - 1]\}.$$

2022

**Ejemplo 1.25.** El conjunto cociente  $\mathbb{Z}_4$  de las clases de equivalencia de números congruentes módulo 4 es el conjunto de las clases de equivalencia de los restos de dividir entre 4:

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}.$$

En general,  $[4n + r] = [r]$ , con  $0 \leq r < 4$ . Por ejemplo:  $[4] = [0]$ ,  $[5] = [1]$ ,  $[18] = [2]$ ,  $[31] = [3]$ .

### 1.4.1 Operaciones en $\mathbb{Z}_m$

Usando la suma y producto en  $\mathbb{Z}$ , podemos definir una suma y un producto en  $\mathbb{Z}_m$  con propiedades similares (ver el Apéndice para un análisis detallado). La definición de estas operaciones se obtiene como consecuencia del siguiente resultado:

**Lema 1.26.** Sean  $a, b, c, d, h, m \in \mathbb{Z}$  con  $h \neq 0$  y  $m > 0$ , entonces:

- i) La suma y el producto son compatibles con la relación  $\equiv_m$ . Es decir,  
si  $a \equiv_m b$  y  $c \equiv_m d$ , entonces  $a + c \equiv_m b + d$  y  $ac \equiv_m bd$ .
- ii)  $[a]$  tiene inverso en  $\mathbb{Z}_m$  si, y solo si,  $\text{mcd}(a, m) = 1$ .
- iii) Si  $p$  es un número primo, para cualquier  $[a] \neq [0]$  se verifica que  $[a]$  tiene inverso en  $\mathbb{Z}_p$ .
- iv) Si  $ah \equiv_m bh$  y  $\text{mcd}(h, m) = 1$ , entonces  $a \equiv_m b$ .

*Demostración.*

- i) Si  $a - b = mt$  y  $c - d = mt'$ , entonces:  
sumando ambas expresiones  $a + c = b + d + mt + mt'$ ,  
y multiplicando  $ac = (b + mt)(d + mt') = bd + mtd + mt'b + m^2tt'$ .
- ii)  $[a]$  tiene inverso en  $\mathbb{Z}_m$  si, y solo si, existe  $x \in \mathbb{Z}$  tal que  $ax \equiv_m 1$ , es decir, si, y solo si, existe solución de la ecuación  $ax + my = 1$ . Y como sabemos, la ecuación  $ax + my = 1$  tiene solución si, y solo si,  $\text{mcd}(a, m) = 1$ .
- iii) Si  $p$  es un número primo entonces  $\text{mcd}(a, p) = 1$ , para cualquier  $a \in \{1, 2, \dots, p - 1\}$ .
- iv) Si  $[ah] = [bh]$  y existe el inverso de  $h$  en  $\mathbb{Z}_m$  entonces  $[a] = [ah][h^{-1}] = [bh][h^{-1}] = [b]$ , es decir,  $a \equiv_m b$ . ■

**Nota 1.** La condición  $\text{mcd}(h, m) = 1$  es necesaria ya que, por ejemplo  $24 \equiv_9 6$  pero 8 no es congruente con 2 módulo 9.

**Observación.** Las operaciones suma y producto en  $\mathbb{Z}_m$  heredan las propiedades de las operaciones en  $\mathbb{Z}$ . En particular, podemos tener

$$\sum_{i=1}^n a_i \equiv_m \sum_{i=1}^n b_i, \quad \text{y también} \quad \prod_{i=1}^n a_i \equiv_m \prod_{i=1}^n b_i,$$

siendo  $a_i$  y  $b_i$ , con  $i = 1, \dots, n$ , enteros tales que  $a_i \equiv_m b_i$ , para cada  $1 \leq i \leq n$ .

**Ejemplo 1.27.** Hallar el resto de la división de  $81623 \cdot 914$  entre 5.

El resto de dividir 81623 entre 5 es 3, con lo que  $81623 \equiv_5 3$ . El resto de dividir 914 entre 5 es 4, es decir,  $914 \equiv_5 4$ . Así,  $81623 \cdot 914 \equiv_5 3 \cdot 4 \equiv_5 2$ . Luego el resto pedido es 2.

**Ejemplo 1.28.** Hallar el resto de la división de  $37^{7541}$  entre 7.

Puesto que  $37 \equiv_7 2$ ,  $2^3 \equiv_7 1$  y que  $2513 \cdot 3 + 2 = 7541$ , se tiene que:

$$37^{7541} \equiv_7 2^{(2513 \cdot 3) + 2} \equiv_7 (2^3)^{2513} \cdot 2^2 \equiv_7 4$$

con lo que el resto de la división es 4.

**Ejemplo 1.29.** Dado que Hacienda detectaba que al consignar el número del DNI en documentos y facturas se producían muchos errores (principalmente transposición de dos dígitos contiguos), creó el NIF. El cálculo de este “código de verificación” emplea el número primo 23 y la siguiente secuencia de letras del alfabeto:

$$T, R, W, A, G, M, Y, F, P, D, X, B, N, J, Z, S, Q, V, H, L, C, K, E$$

que se corresponde con 0, 1, 2, ..., 22. Si  $z$  es el número del DNI, la letra del NIF es  $x$  siendo  $z \equiv_{23} x$ . Por ejemplo, el número de DNI 33203140  $\equiv_{23} 18$ , por tanto le corresponde la letra  $H$ .

**Ejemplo 1.30.** Para demostrar que el NIF detecta que se han intercambiado dos cifras consecutivas del DNI, supongamos que el DNI es

$$a_1 a_2 \dots x y \dots a_7 a_8$$

y consideremos el número

$$a_1 a_2 \dots y x \dots a_7 a_8.$$

Para que no se detecte la transposición, tendría que cumplirse:

$$10^i(10x + y) - 10^i(10y + x) \equiv_{23} 0$$

o equivalentemente,  $10^i 9(x - y) \equiv_{23} 0$  de donde se deduce que necesariamente  $x = y$ .

**Ejemplo 1.31.** Cada billete de euros está identificado con una cadena de longitud 12, puede ser una letra seguida de 11 números, o bien, dos letras seguidas de 10 números. La primera letra identifica al país emisor del billete (Z, Bélgica; Y, Grecia; X, Alemania; V, España; U, Francia; T, Irlanda; S, Italia; P, Países Bajos; N, Austria; M, Portugal, etc) mientras la segunda determina una serie.

Para verificar que un billete es válido, realizamos los siguientes pasos:

- Se cambian las letras por los dígitos que le corresponden en el orden alfabético usual más uno (A 2, B 3,..., V 23,...,Z 27).
- Los dígitos anteriores, se añaden a los restantes de la cadena de identificación obteniendo así un número  $x$ .
- Se reduce  $x$  módulo 9.

El billete es válido si el resultado es 0.

Para realizar este cálculo, tendremos en cuenta que el resto de dividir un número por nueve es el mismo que el de dividir, también por nueve, la suma de sus cifras. Podemos entonces realizar, reiteradamente, la suma de las cifras hasta que quede una sola y verificar que coincide con 0.

Por ejemplo, para un billete belga con código ZB0200851269:

- i) la  $Z$  se corresponde con 27, la  $B$  con 3;
- ii) se obtiene el número  $x = 2730200851269$ .

- iii) Para obtener la reducción de  $x$  módulo 9, basta con realizar la suma de las cifras de  $x$  ya que  $10^n \equiv_9 1$

$$2 + 7 + 3 + 0 + 2 + 0 + 0 + 8 + 5 + 1 + 2 + 6 + 9 \equiv_9 0$$

y vemos que el resultado obtenido es congruente con 0 módulo 9.

Concluimos, por tanto, que el billete es válido.

### 1.4.2 Criterios de Divisibilidad.

Dado un número natural  $n = a_k \cdots a_1 a_0$  escrito en base  $b$ , ¿cómo podemos averiguar si  $n$  es divisible por otro número  $m$ ? El primer paso consiste en calcular los valores  $r_i$  tales que

$$b^i \equiv_m r_i.$$

De este modo, se tiene que:

$$\sum_{i=0}^k a_i b^i \equiv_m \sum_{i=0}^k a_i r_i$$

Concluimos que  $n$  es divisible por  $m$  si  $\sum_{i=0}^k a_i r_i$  lo es. Veamos algunos casos particulares cuando  $b = 10$ :

- i) Tomemos  $m = 2$ . Se tiene que  $r_0 = 1$ . Además  $10^i$  es par, para todo  $i \geq 1$ , con lo que  $r_i = 0$ . Luego  $n$  es divisible por 2 si, y sólo si,  $a_0$  es un número par.
- ii)  $m = 3$ . Como  $10 \equiv_3 1$ , se tiene que  $r_i = 1$ , para todo  $i \geq 1$ . Concluimos que  $n$  es divisible por tres si, y sólo si,  $\sum_{i=0}^k a_i$  es un múltiplo de tres.
- iii)  $m = 7$ . En primer lugar  $10 \equiv_7 3$ ,  $10^2 \equiv_7 9 \equiv_7 2$ ,  $10^3 \equiv_7 6 \equiv_7 -1$ ,  $10^4 \equiv_7 4 \equiv_7 -3$ ,  $10^5 \equiv_7 5 \equiv_7 -2$ ,  $10^6 \equiv_7 1$  y, a partir de aquí, se repiten cíclicamente, con lo que  $n$  es múltiplo de 7 si

$$a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \cdots$$

es múltiplo de 7.

- iv)  $m = 11$ . Puesto que  $10 \equiv_{11} -1$ , tenemos que  $r_{2k} = 1$  y  $r_{2k+1} = -1$ , para cualquier  $k$ . De este modo,  $n$  es múltiplo de 11 si lo es  $a_0 - a_1 + a_2 - a_3 + \cdots$ .

## 1.5 Ecuaciones de congruencia

Ahora, vamos a estudiar la existencia de soluciones de la ecuación de congruencia  $ax \equiv_m b$ .

**Teorema 1.32.** La ecuación  $ax \equiv_m b$  tiene solución entera si, y solo si,  $d = \text{mcd}(a, m)$  divide a  $b$ . Además, el número de soluciones no congruentes módulo  $m$  es exactamente  $d$ .

*Demostración.* En primer lugar hay que tener en cuenta que encontrar una solución entera  $x_0$  de  $ax \equiv_m b$  implica encontrar un par de enteros  $(x_0, y_0)$  tales que  $ax_0 + my_0 = b$ . Es decir, la ecuación  $ax \equiv_m b$  tendrá solución cuando la tenga la ecuación diofántica  $ax + my = b$ , lo cual ocurre si, y solo si,  $d = \text{mcd}(a, m)$  divide a  $b$ . Además, como sabemos, las soluciones de  $ax + my = b$  son de la forma

$$\left( x_0 + t \frac{m}{d}, y_0 - t \frac{a}{d} \right) \text{ siendo } t \text{ un entero.}$$

Para cada  $0 \leq t < d$ , obtenemos una solución distinta, es decir, no hay dos soluciones congruentes módulo  $m$ , ya que si  $0 \leq t_2 < t_1 < d$  y suponemos que las soluciones para  $t_1$  y para  $t_2$  son congruentes módulo  $m$ , entonces tendríamos que

$$\left( x_0 + t_1 \frac{m}{d} \right) - \left( x_0 + t_2 \frac{m}{d} \right) = km$$

y, por lo tanto:

$$m(t_1 - t_2) = kmd, \text{ es decir } (t_1 - t_2) = kd.$$

De esta última igualdad, se deduce que  $d|(t_1 - t_2)$ , lo cual es imposible.

Si ahora elegimos un entero  $t_3$ , al dividir  $t_3$  entre  $d$  obtenemos un resto  $0 \leq r < d$  tal que  $t_3 = dq + r$ . De este modo,

$$\left( x_0 + t_3 \frac{m}{d} \right) - \left( x_0 + r \frac{m}{d} \right) = (t_3 - r) \frac{m}{d} = \frac{dqm}{d} = qm$$

es decir que  $\left( x_0 + \frac{t_3 m}{d} \right) \equiv_m \left( x_0 + \frac{r m}{d} \right)$ .

### Cálculo de las soluciones de la ecuación $ax \equiv_m b$ .

- i) Vemos si la ecuación tiene solución comprobando si existe algún entero  $z$  tal que  $b = z \cdot \text{mcd}(a, m)$ .
- ii) Usando el Algoritmo de Euclides, calculamos los enteros  $r, s$  tales que  $ar + ms = \text{mcd}(a, m)$ .
- iii) Una solución particular de la ecuación es  $x_0 \equiv_m rz$ .
- iv) En general, las soluciones se obtienen de la siguiente forma:

$$x \equiv_m x_0 + \frac{m}{d} t, \quad \text{para cada } t \in \{0, 1, \dots, d-1\}$$

donde  $d = \text{mcd}(a, m)$ .

**Ejemplo 1.33.** Encontrar todas las soluciones no congruentes de  $9x \equiv_{15} 6$ .

Como  $\text{mcd}(9, 15) = 3$  y 3 divide a 6, la ecuación tiene solución y, para resolverla, escribimos la ecuación diofántica:

$$9x + 15y = 6$$

Una solución es  $x_0 = 4$  y las otras dos no congruentes son  $4 + 5 = 9$  y  $4 + 10 = 14$ .

A continuación veremos unas ideas relevantes para la última parte del tema dedicada a los criptosistemas.

## 1.6 Función $\phi$ de Euler

**Definición 1.34. ( $\phi$  de Euler)** Dado un número natural  $m$ , se designa por  $\phi(m)$  al número de enteros positivos  $r$  menores o iguales que  $m$  y primos con  $m$ ,

$$\phi(m) = |\{0 < r \leq m ; \text{mcd}(r, m) = 1\}|.$$

Dicha función se denomina **función  $\phi$  de Euler**.

Claramente  $\phi(1) = 1$ ,  $\phi(2) = 1$  y, en general, si  $p$  es un primo, todos los enteros menores que  $p$  son primos con  $p$ , así que  $\phi(p) = p - 1$ . De hecho:

**Nota 2.** Si  $p$  es un primo y  $r$  un natural, entonces:

$$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p - 1).$$

Sea  $n$  uno de los  $p^r$  números que hay entre 1 y  $p^r$ . Si  $\text{mcd}(n, p^r) = 1$ , entonces  $p$  no divide a  $n$ . El resultado es consecuencia de que entre 1 y  $p^r$  hay exactamente  $p^{r-1}$  números divisibles por  $p$  que son

$$p, 2p, 3p, \dots, p^r = (p^{r-1})p$$

**Nota 3.** Si  $m$  y  $n$  son dos naturales primos entre sí, se tiene que  $\phi(mn) = \phi(m)\phi(n)$ .

Supongamos ahora que  $m$  es un natural cualquiera cuya factorización en producto de potencias de primos distintos es:

$$m = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}.$$

De lo dicho anteriormente, se deduce que:

$$\phi(m) = \prod_{i=1}^k \phi(p_i^{r_i}) = \prod_{i=1}^k (p_i^{r_i} - p_i^{r_i-1}) = \prod_{i=1}^k p_i^{r_i-1}(p_i - 1).$$

Así, por ejemplo, se tiene que

$$\phi(360) = \phi(2^3 3^2 5) = (2^3 - 2^2)(3^2 - 3)(5 - 1) = 4 \cdot 6 \cdot 4 = 96.$$

**Teorema 1.35. (Teorema de Euler)** Sean  $a, m \in \mathbb{Z}$  con  $m \geq 1$ . Si  $\text{mcd}(a, m) = 1$ , se tiene que

$$a^{\phi(m)} \equiv_m 1.$$

Veamos qué ocurre en un caso particular:  $a = 11$  y  $m = 8$ .

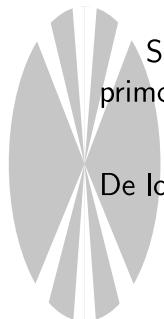
En primer lugar claramente  $\phi(8) = 4$  y los naturales menores que 8 y primos con él son 1, 3, 5, 7. Puesto que

$$\begin{aligned} 11 \cdot 1 &\equiv_8 3 \\ 11 \cdot 3 &\equiv_8 1 \\ 11 \cdot 5 &\equiv_8 7 \\ 11 \cdot 7 &\equiv_8 5 \end{aligned}$$

se tiene que

$$11^4(1 \cdot 3 \cdot 5 \cdot 7) \equiv_8 (3 \cdot 1 \cdot 7 \cdot 5)$$

y, como  $\text{mcd}(8, 1 \cdot 3 \cdot 5 \cdot 7) = 1$ , entonces:  $11^4 \equiv_8 1$ .



**Teorema 1.36.** Si  $p$  es un número primo que no divide al entero  $a$ , entonces

$$a^{p-1} \equiv_p 1.$$

*Demostración.* Basta aplicar el Teorema de Euler ya que si  $p$  es un primo que no divide a  $a$ , entonces  $\text{mcd}(a, p) = 1$  y  $\phi(p) = p - 1$ . ■

**Ejemplo 1.37.** Encuéntrese el resto de la división de  $32^{98}$  entre 7.

Como  $32 = 4 \cdot 7 + 4$  entonces  $32 \equiv_7 4$ . Se tiene que  $4^6 \equiv_7 1$  ya que 7 y 4 son primos entre sí. Finalmente,  $98 = 16 \cdot 6 + 2$  y  $4^{98} \equiv_7 4^2 \equiv_7 2$ .

## 1.7 Introducción a la Criptografía

Tradicionalmente, la Criptografía ha tenido como objetivo la transmisión o el almacenamiento de la información de manera confidencial entre los usuarios autorizados. Para ello se utiliza un sistema criptográfico que, mediante un algoritmo y una clave, transforma el mensaje original en un mensaje cifrado, incomprendible para un observador no autorizado.

En la actualidad, se han añadido otros objetivos a la criptografía, que son: Confidencialidad (A envía un mensaje a B que no puede ser interpretado por nadie más), Autenticidad (cuando B recibe un mensaje de A, puede estar convencido de que ha sido A quien lo ha enviado), Integridad (B puede detectar si el mensaje que le ha enviado A ha sido alterado por una tercera persona), No repudio (después de haber enviado un mensaje a B, A no puede negar que el mensaje es suyo).

La importancia de estos objetivos es fácil de entender si uno piensa que, por ejemplo, A desea intercambiar mensajes con B para comprarle un artículo a través de Internet, realizando el pago con una tarjeta de crédito.

Aunque la Criptografía es un campo muy importante de aplicación de la Teoría de Números, no toda la Criptografía se basa en ella. Nosotros nos centraremos en los aspectos que ambas tienen en común.

**Definición 1.38.** Un **sistema criptográfico** consta de 5 componentes:

- Un conjunto de mensajes a cifrar  $M$ .
- Un conjunto de mensajes cifrados  $C$ .
- Un conjunto de claves  $K$ .
- Una familia de transformaciones de cifrado

$$E = \{E_k : M \rightarrow C, k \in K\}.$$

- Una familia de transformaciones de descifrado

$$D = \{D_k : C \rightarrow M, k \in K\}.$$

tales que,  $D_k^{-1} = E_k$ , para cada  $k$ .

**Definición 1.39.** Llamaremos **texto llano** al mensaje previo a la encriptación. El mensaje encriptado se conoce también como **texto cifrado**.

**Nota 4.** En ocasiones, para poder utilizar un cifrado en el que intervengan funciones numéricas, a cada letra del alfabeto se le asigna un número. Por ejemplo, para traducir un mensaje del lenguaje ordinario a un número, usaremos 01 en vez de A, 02 en vez de B, etc y 27 en lugar de Z.

Letra	Cifra	Letra	Cifra	Letra	Cifra	Letra	Cifra
A	01	H	08	Ñ	15	U	22
B	02	I	09	O	16	V	23
C	03	J	10	P	17	W	24
D	04	K	11	Q	18	X	25
E	05	L	12	R	19	Y	26
F	06	M	13	S	20	Z	27
G	07	N	14	T	21		

La palabra CASA se traduce como 03012001.

### 1.7.1 Criptografía simétrica o de clave privada

Los métodos de cifrado simétrico se basan en el uso de una misma clave secreta para cifrar y descifrar. Son, esencialmente, de dos tipos: trasposición y sustitución.

**Trasposición:** En una trasposición, las letras del mensaje original se colocan de otra manera. Tanto el emisor como el receptor del mensaje deben estar de acuerdo en cómo se lleva a cabo esta nueva colocación. En este tipo de cifrado, cada letra cambia de posición, pero conserva su identidad.

**Ejemplo 1.40.** Una trasposición en riel, en la que el mensaje se escribe alternando las letras en dos líneas separadas. A continuación, la secuencia de letras de la línea inferior se añade al final de la secuencia de letras de la línea superior, creándose así el mensaje cifrado final.

Texto llano:

TU SECRETO ES TU PRISIONERO; SI LO SUELTA, TU ERES SU PRISIONERO.

Texto cifrado:

T S C E O S U R S O E O I O U L A T E E S P I I N R

U E R T E T P I I N R S L S E T S U R S U R S O E O

**Substitución:** Este método consiste en cambiar la identidad de cada letra mediante un método conocido por el emisor y el receptor. Sin embargo, no se cambia la posición de las letras.

**Ejemplo 1.41.** Una posible sustitución consiste en emparejar al azar las letras del alfabeto y luego sustituir cada letra por su pareja.

A	D	H	I	K	M	O	R	S	U	W	Y	Z
V	X	B	G	J	C	Q	L	N	E	F	P	T

Texto llano: ESTO ES UN SECRETO

Texto cifrado: UNZQ UN ES NUMLUZQ

### 1.7.2 Cifrado afín

Es un ejemplo de cifrado por substitución en el que:

- $M = C = \mathbb{Z}_n$ , para algún  $n \in \mathbb{Z}$ ,  $n > 0$  y suficientemente grande.
- **Elección de la clave:** Para la clave  $(a, b)$ , se escogen  $a, b \in \mathbb{Z}$  con  $\text{mcd}(a, n) = 1$ . Los valores de  $a$ ,  $b$  y  $n$  son conocidos por el emisor  $A$  y el receptor  $B$ . El conjunto  $K$  de claves, para un  $n \in \mathbb{Z}$ , es

$$K = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{mcd}(a, n) = 1\}.$$

- **Cifrado:**  $A$  le quiere enviar a  $B$  el mensaje  $m$ , que previamente ha trasformado en un elemento de  $\mathbb{Z}_n$ . Entonces realiza la transformación:

$$E_{(a,b)}(m) = c \equiv_n am + b,$$

siendo  $c$  el mensaje que le envía a  $B$ .

- **Descifrado:** Cuando  $B$  recibe el mensaje cifrado  $c$  efectúa:

$$D_{(a,b)}(c) = m \equiv_n a^{-1}(c - b),$$

donde  $a^{-1}$  es el inverso de  $a$  en  $\mathbb{Z}_n$ , que se puede calcular, porque hemos escogido  $a$  tal que  $\text{mcd}(a, n) = 1$ .

Debe hacerse notar que un cifrado afín, y en general cualquier tipo de cifrado, puede transformar el mensaje completo, por bloques o “letra a letra”. En los ejemplos que veremos a continuación, la transformación se realizará letra a letra.

Para usar un cifrado afín debemos seleccionar una clave  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$  escogiendo solo aquellos pares en los que  $a$  tenga inverso en  $\mathbb{Z}_{27}$ .

**Ejemplo 1.42.** Usemos el cifrado afín de clave  $(10, 0)$  para cifrar SOMOS CAMPEONES. Primero, usamos la tabla de la página 16 para transformar cada letra en un número y obtenemos

$$(20, 16, 13, 16, 20, 03, 01, 13, 17, 05, 16, 14, 05, 20).$$

A continuación lo ciframos usando

$$E(x) \equiv_{27} 10x,$$

donde  $x$  denota cada uno de los números correspondiente a una letra. El mensaje se convierte en

$$(11, 25, 22, 25, 11, 03, 10, 22, 08, 23, 25, 05, 23, 11).$$

De nuevo usamos la tabla para tener el texto: KXUXK CJUHVXEVK.

Para descifrar el mensaje se multiplica cada letra por  $a^{-1} = 19$  en  $\mathbb{Z}_{27}$ .

**Ejemplo 1.43.** En la guerra de las Galias, el emperador Julio César substituía cada letra del mensaje por la letra que estaba tres posiciones más adelante en el alfabeto.

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z  
D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C



Texto llano: V E N I, V I D I, V I C I

Texto cifrado: YHPL, YLGL, YLFL

Un cifrado del tipo del de Julio César puede ser visto como un criptosistema afín del siguiente modo:

Si queremos cifrar un mensaje utilizando el método de Julio César, lo que haremos será transformar cada letra en un elemento de  $\mathbb{Z}_{27}$  según la tabla de la página 16 y, a cada una de ellas, aplicarle la función

$$E(x) \equiv_{27} x + 3,$$

lo que nos da un cifrado afín con  $a = 1$  y  $b = 3$ .

### 1.7.3 Criptografía asimétrica o de clave pública.

Utiliza funciones de una sola vía  $f : M \rightarrow C$ , para las cuales es fácil de calcular  $f(x)$  y sin embargo, difícil de obtener  $f^{-1}(y)$ , en la mayor parte de los casos. Hay que tener en cuenta que aquí difícil es sinónimo de **computacionalmente no factible** con los mejores algoritmos y el mejor hardware.<sup>1</sup>

El proceso es el siguiente:

- Cada usuario U dispone de una **clave pública**  $k_U^1$  (que podrán conocer todos los demás) y una **clave privada**  $k_U^2$  (que se reserva para él).
- Cuando A quiere enviar a B un mensaje  $m$ , busca la clave pública de B y le envía  $s = E_{k_B^1}(m)$ .
- Al recibir el mensaje, B utiliza su clave privada para descifrar  $s$  y recupera  $m$  haciendo

$$m = D_{k_B^2}(s) = D_{k_B^2}\left(E_{k_B^1}(m)\right).$$

Es decir,  $D_{k_B^2} \circ E_{k_B^1}$  es la función identidad.

Hay una clara analogía con los buzones de correos: cualquiera puede enviar un mensaje a B utilizando su buzón (clave pública) pero sólo B, que dispone de la llave del buzón (clave privada), puede recuperarlo.

La obtención de funciones de dirección única, o funciones de una sola vía se ha basado, hasta el momento, en el uso de la Aritmética modular.

**Ejemplo 1.44.** Esta idea es la misma que está presente en la **firma digital**. En este caso, si A quiere enviarle un mensaje  $m$  a B, entonces primero lo firma con su clave privada y construye  $s = E_{k_A^2}(m)$ , a continuación, lo encripta con la clave pública de B, obteniendo  $c = E_{k_B^1}(s)$  que es el mensaje que recibe B.

B lo desencripta, primero con su clave privada y recupera  $s = D_{k_B^2}(c)$ . Finalmente, hace uso de la clave pública de A y obtiene  $m = D_{k_A^1}(s)$ .<sup>2</sup> Nótese que ahora necesitamos, además que  $D_{k_A^1} \circ E_{k_A^2}$  sea igual a la identidad.

<sup>1</sup>En realidad, se van a utilizar funciones de dirección única con trampa, es decir, el receptor dispondrá de una información adicional que le permite obtener  $f^{-1}(y)$ .

<sup>2</sup>El hecho de que sólo la clave pública de A invierte su clave privada garantiza que ha sido A el emisor del mensaje.

### 1.7.4 Cifrado RSA

Rivest, Shamir y Adleman (RSA) encontraron en 1977 una función de una sola vía basada en funciones modulares. En este caso, el problema difícil en el que se basa el método es la obtención de la factorización de un número grande en sus factores primos.

Si  $A$  quiere enviar un mensaje a  $B$  utilizando el método RSA deberán proceder del siguiente modo:

- $B$  escoge números primos  $p$  y  $q$  muy grandes, que procederá a multiplicar obteniendo un número  $n = pq$ . A continuación, buscará un entero  $e$  que sea primo con  $\phi(n) = (p - 1)(q - 1)$  y otro entero  $d$  tal que  $ed \equiv_{\phi(n)} 1$ , que obtiene mediante el algoritmo de Euclides.
- El conjunto  $M$  es un conjunto de números, lo mismo que el conjunto  $C$ .
- **Clave privada:** La clave privada de  $B$  consiste en los dos primos  $p$  y  $q$  y el número  $d$ , inverso de  $e$  en  $\mathbb{Z}_{\phi(n)}$ . Así, la clave privada es una terna  $(p, q, d)$ .
- **Clave pública:** La clave pública de  $B$  consiste en los números  $n$  y  $e$ , es decir, es el par  $(n, e)$ .
- **Algoritmo de encriptado:** El mensaje que  $A$  quiere enviar a  $B$  es  $m$ . Entonces  $A$  calcula

$$c \equiv_n m^e.$$

Como vemos, aquí aparece una potencia en  $\mathbb{Z}_n$ , que sabemos que es una función cuya inversa es difícil de calcular.

- **Algoritmo de desencriptado:** Para descifrar el mensaje,  $B$  utiliza la siguiente fórmula:

$$m \equiv_n c^d,$$

El siguiente resultado garantiza que las dos funciones anteriores son inversas.

**Teorema 1.45.** Sean  $n = pq$ , con  $p, q$  dos primos, y  $e$  un número natural tal que  $\text{mcd}(e, \phi(n)) = 1$ . Entonces, para todo número natural  $a$ , se tiene que:

$$a^{ed} \equiv_n a,$$

donde  $ed \equiv_{\phi(n)} 1$ .

**Ejemplo 1.46.** Alicia quiere transmitir a Benito un mensaje.

La clave pública RSA de Benito es  $(n, e) = (328419349, 220037467)$ .

La clave privada de Benito es  $(7243, 45343, 119923)$ .

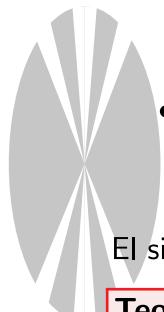
Tenemos que  $\phi(n) = 328366764$ .

Alicia encripta una palabra  $M$  para Benito y este recibe  $c = 43853517$  ¿Qué valor es  $M$ ?

Benito desencripta  $c$  haciendo:

$$\begin{aligned} c^d &\equiv_n 43853517^{119923} \equiv_n (43853517^{50000})^2 \cdot 43853517^{19923} \\ &\equiv_n (133807774)^2 \cdot 281712138 \equiv_n 300145477 \cdot 281712138 \\ &\equiv_n 126220401. \end{aligned}$$

Ahora convierte  $M$  al lenguaje ordinario (agrupando los dígitos de dos en dos de derecha a izquierda) y obtiene la palabra “AYUDA”.



## 1.8 Apéndice

### 1.8.1 Operaciones en $\mathbb{Z}_m$

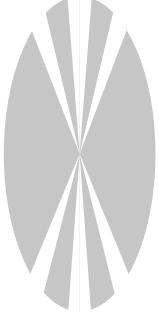
Hemos visto que si  $a \equiv_m b$  y  $c \equiv_m d$ , entonces  $a + c \equiv_m b + d$  y  $ac \equiv_m bd$ . Este hecho, como hemos comentado, se traduce en que podemos definir una suma y una multiplicación en el conjunto  $\mathbb{Z}_m$  de las clases de equivalencia de la relación  $\equiv_m$ . Recordemos que este conjunto se puede dar utilizando como representantes de clase los restos de dividir entre  $m$ . Así,  $\mathbb{Z}_m = \{[0], [1], \dots, [m-1]\}$ , y tendremos una suma y un producto:

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab].$$

Siempre que hagamos estas operaciones, daremos el resultado representado por su resto de dividir entre  $m$ .

**Ejemplo 1.47.** Si  $m = 9$  tenemos el conjunto  $\mathbb{Z}_9 = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\}$ . La suma  $[5] + [8] = [4]$ , ya que  $5 + 8 = 13$  y  $13 = 9 + 4$ , con lo que  $13 \equiv_9 4$ . De modo análogo, el producto  $[7] \cdot [8] = [2]$ , porque  $56 = 9 \cdot 6 + 2$  y por lo tanto  $56 \equiv_9 2$ .

**Ejemplo 1.48.** La tabla de la suma en  $\mathbb{Z}_9$  es la siguiente:



+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

En la tabla es fácil observar varias propiedades. Por ejemplo, que  $[i] + [j] = [j] + [i]$  para cualquier  $[i], [j]$ . Además  $[i] + [0] = [i]$  sea cual sea  $[i]$ . Finalmente notemos que  $[i] + [9 - i] = [0]$ .

Estas propiedades se cumplen para cualquier  $\mathbb{Z}_m$ . Así:

**Propiedades 1.49.** Sea  $m \in \mathbb{Z}$ ,  $m > 0$ , y  $[a], [b] \in \mathbb{Z}_m$ .

- i)  $[a] + [b] = [b] + [a]$  (propiedad conmutativa)
- ii)  $[a] + [0] = [a]$  (elemento neutro)
- iii)  $[a] + [m - a] = [0]$  ( $[m - a]$  es el opuesto de  $[a]$ ).

**Ejemplo 1.50.** Estudiemos ahora la tabla de la multiplicación en  $\mathbb{Z}_9$ :

.	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Igual que sucede para la suma, tenemos que  $[i] \cdot [j] = [j] \cdot [i]$  sean cuales sean  $[i]$  y  $[j]$ . Además encontramos dos elementos distinguidos. Por un lado,  $[0] \cdot [i] = [0]$  para cualquier  $[i]$ . Por otro lado,  $[1] \cdot [i] = [i]$  para cualquier  $[i]$ .

Nótese además que hay algunos elementos, como  $[4]$ , tales que existe otro elemento que al multiplicarlos el resultado es  $[1]$ . Por ejemplo,  $[4] \cdot [7] = [1]$ . Diremos que estos elementos tienen **inverso en  $\mathbb{Z}_9$** . Por el contrario, existen elementos distintos de cero que al multiplicarlos el resultado es cero. Así, por ejemplo,  $[3] \cdot [6] = [0]$ .

En general, tenemos:

**Propiedades 1.51.** Sea  $m$  un entero positivo, y  $[a], [b] \in \mathbb{Z}_m$ .

- i)  $[a] \cdot [b] = [b] \cdot [a]$
- ii)  $[a] \cdot [0] = [0]$  y  $[a] \cdot [1] = [a]$

## 1.8.2 Sistemas de Numeración

En la vida ordinaria, el sistema de numeración que utilizamos es el decimal. Las unidades se agrupan en bloques de 10 y forman las decenas, éstas se agrupan en grupos de 10 y forman las centenas, y así sucesivamente. Cuando escribimos cualquier número, por ejemplo 12354, entendemos que

$$12354 = 1 \cdot 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10 + 4.$$

El uso de este sistema de numeración y no otro, es convencional (quizás motivado por que aprendemos a contar con nuestros diez dedos de la mano). Los árabes y los chinos usan símbolos distintos a 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Otras civilizaciones utilizaban diferentes sistemas. Los babilonios utilizaban un sistema sexagesimal y posteriormente sistemas de base veinte fueron desarrollados en América Central por la civilización maya.

Con el desarrollo de la Informática ha crecido el uso de los sistemas de numeración que utilizan como base una potencia de 2. En realidad, podemos utilizar una base cualquiera.

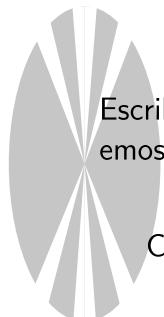
**Ejemplo 1.52.** Expresemos 45 como suma de potencias de 2, 3 y 4.

$$\begin{aligned} 45 &= 32 + 8 + 4 + 1 = 2^5 + 2^3 + 2^2 + 2^0 \\ 45 &= 27 + 18 = 3^3 + 2 \cdot 3^2 \\ 45 &= 2 \cdot 4^2 + 3 \cdot 4 + 4^0 \end{aligned}$$

**Teorema 1.53.** Sea  $b \geq 2$  un número natural que llamaremos **base**. Todo número natural  $n$  se puede escribir de manera única en base  $b$  de la forma

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

con  $0 \leq a_i < b$ , para todo  $0 \leq i \leq k$  y  $a_k \neq 0$ . Se denota  $n = a_k a_{k-1} \dots a_1 a_0$



Aunque no demostraremos este teorema, el siguiente ejemplo muestra el proceso a seguir.

**Ejemplo 1.54.** Para escribir 277 en base 2, éste se divide entre 2, así como los sucesivos cocientes, hasta obtener un cociente nulo.

$D$	$d$	$c$	$r$
277	2	138	1
138	2	69	0
69	2	34	1
34	2	17	0
17	2	8	1
8	2	4	0
4	2	2	0
2	2	1	0
1	2	0	1

Escribiendo ahora los sucesivos restos en sentido ascendente (desde el último hasta el primero), obtenemos:

$$277 = 100010101_{(2)}$$

Cuando  $b > 10$ , habrá valores de  $a_i$  mayores que 10. Se suele designar

$$A = 10, B = 11, C = 12, \text{ etc.}$$

Por ejemplo,  $B5C4_{(16)} = B \cdot 16^3 + 5 \cdot 16^2 + C \cdot 16 + 4 = 46.532$ .

Mención especial merecen el paso del sistema binario a cualquier sistema cuya base sea una potencia de 2 y el paso inverso. Veamos, por ejemplo cómo se pasa de base 2 a base 8. Agrupamos los dígitos binarios en bloques de tres dígitos de derecha a izquierda, completando, si fuera preciso, el último bloque con ceros. Por ejemplo si

$$n = 1|001|101|001_{(2)}$$

completamos el bloque  $1|$  a  $001|$ .

Nos quedan así bloques que se corresponden con números de 0 a 7 y serán los coeficientes en base 8. En el ejemplo anterior, tendríamos:

$$n = 1151_{(8)}$$

Recíprocamente, si consideramos  $m = 30706_{(8)}$ , escribimos cada coeficiente (comprendido entre 0 y 7) como un bloque binario de tres dígitos. De este modo, quedaría:

$$m = 011|000|111|000|110_{(2)}.$$