Capítulo 1

Teoría de números

1.1. Principio de inducción

Una característica fundamental de los números naturales es que cualquiera de ellos puede ser obtenido a partir del 1 mediante una suma reiterada de unos. Esta propiedad es la base de un método de demostración extraordinariamente útil en Matemáticas.

El principio de inducción (también llamado Tercer Axioma de Peano) afirma que si el 1 tiene una propiedad P y, se cumple que la propiedad P se transmite de cualquier número natural n a su sucesor $(n+1)$, entonces todos los números naturales satisfacen esa propiedad.

Hay muchos tipos de imágenes gráficas que pueden ayudar a comprender el principio anterior. Por ejemplo, usando fichas de dominó. Si las colocamos unas junto a otras, de tal modo que al empujar una caiga la siguiente (paso inductivo) y empujamos la primera (base inductiva), está claro que esa propiedad se transmite de una ficha a su sucesora y, por lo tanto, todas caerán.

Si denotamos por $P(n)$ al predicado "n satisface la propiedad P", podemos enunciar el principio anterior de la siguiente manera:

Si se cumple

- **Base inductiva**: $P(1)$
- **Paso inductivo**: Para todo $k \in \mathbb{N}$, $P(k) \Longrightarrow P(k+1)$

Entonces, para todo $n \in \mathbb{N}$, $P(n)$.

Ejemplo 1.1.1. I) *Para todo natural n, se verifica que*

$$1+2+\cdots+n=\sum_{i=1}^{n} i=\frac{n(n+1)}{2}.$$

II) *Para todo natural n, se verifica que $1+2+\cdots+2^n=2^{n+1}-1$.*

III) *Para todo natural n, se tiene que*

$$\left(1+\frac{1}{3}\right)^n \geq \left(1+\frac{n}{3}\right)$$

Es evidente que la base inductiva se cumple. Además, si suponemos que

$$\left(1+\frac{1}{3}\right)^n \geq \left(1+\frac{n}{3}\right)$$

entonces

$$\begin{array}{rcl}
\left(1+\frac{1}{3}\right)^{n+1} & = & \left(1+\frac{1}{3}\right)^n\left(1+\frac{1}{3}\right) \\
& \geq & \left(1+\frac{n}{3}\right)\left(1+\frac{1}{3}\right) \\
& = & \left(1+\frac{n}{3}\right)+\frac{1}{3}\left(1+\frac{n}{3}\right) \\
& \geq & \left(1+\frac{n}{3}\right)+\frac{1}{3} \\
& = & \left(1+\frac{n+1}{3}\right).
\end{array}$$

Ejemplo 1.1.2. *En un entrenamiento de un equipo de fútbol, el entrenador coloca a los jugadores en el campo de tal manera que no hay dos que estén a la misma distancia, y cada uno de ellos tiene un balón. Cuando el entrenador hace sonar un silbato, los jugadores deben pasarle el balón al compañero que tengan más próximo. Demostraremos que si hay $2n+1$ jugadores, con $n \geq 1$, por lo menos uno de ellos no recibe ningún pase.*

Si $n=1$, hay $3=2\cdot 1+1$ jugadores, que estarán en los vértices de un triángulo escaleno. Así, los que ocupen los extremos del lado más corto se pasarán el balón entre ellos, y el tercer jugador no recibirá ningún pase. Tenemos así la base inductiva. Supongamos entonces que se cumple la propiedad para n, es decir, si hay $2n+1$ jugadores, por lo menos uno de ellos no recibe ningún pase. Comprobemos que si hay $2n+3$ jugadores, también habrá por lo menos uno que no reciba ningún pase. Sean A y B los dos jugadores más próximos entre sí. Estos se pasarán el balón entre ellos. Si hay otro que le pase el balón a A o a B, entonces uno de sus compañeros se queda sin recibir ningún balón. Si no hay ningún otro jugador que le pase el balón a A o a B, tendremos una disposición de $2n+1$ jugadores, que, por hipótesis de inducción, cumplen que uno de ellos no recibirá ningún pase.

En algunas ocasiones, el principio de inducción no se puede aplicar directamente. El siguiente ejemplo ilustra esta situación:

Ejemplo 1.1.3. *El juego del Nim procede de China, y tiene muchas variantes. Veamos aquí una de las más sencillas. En este juego participan dos jugadores que disponen de un montón de palillos. Alternativamente, retiran uno, dos o tres palillos del montón. El jugador que retire el último palillo, pierde el juego.*

Nuestro objetivo consiste en encontrar una estrategia ganadora, si existe, para el primer jugador. Esta estrategia dependerá del número inicial de palillos. Tras un breve análisis, podemos conjeturar que el primer jugador ganará siempre (si sabe jugar bien) cuando y sólo cuando la cantidad inicial de palillos no sea de la forma $4k+1$ para algún $k \in \mathbb{Z},\ k \geq 0$.[1]

Procedamos a aplicar el principio de inducción para demostrar esta afirmación: Supongamos que hay un solo palillo. En este caso tenemos que $1 = 4 \cdot 0 + 1$. Entonces debemos demostrar que el primer jugador pierde, pero esto es evidente ya que es él quien retira el último palillo. Se cumple entonces $P(1)$. Supongamos que es cierta $P(n)$, es decir, que si hay una cantidad inicial de n palillos, el primer jugador gana si y sólo si $n \neq 4k+1$, para algún $k \in \mathbb{Z}, k \geq 0$. Intentemos demostrar utilizando únicamente esta hipótesis que se cumple $P(n+1)$.

Supongamos entonces que hay $n+1$ palillos. Si el primer jugador retira un palillo, quedan n palillos en el montón, y podríamos utilizar la hipótesis de inducción $P(n)$. Pero el primer jugador tiene la opción de retirar 2 o incluso 3 palillos, lo que nos llevaría a tener que utilizar las hipótesis $P(n-1)$ o $P(n-2)$ respectivamente, que no son nuestra hipótesis de inducción, ya que en ésta sólo se contempla la veracidad de $P(n)$.

En el ejemplo anterior, así como en muchos otros, se necesita una hipótesis de inducción más fuerte que la que se da en el principio de inducción. En estos casos aplicaremos el llamado *principio de inducción fuerte o completa* que podemos enunciar como sigue:

Si se cumple

- **Base inductiva**: $P(1)$
- **Paso inductivo completo**: Si para todo natural k se cumple que $(P(i)\ \forall i, 1 \leq i \leq k) \Longrightarrow P(k+1)$,

[1] Basta analizar los casos en los que se parte de 1, 2, 3 y 4 palillos para comprobar que esta conjetura tiene sentido.

Entonces, para todo $n \in \mathbb{N}$, $P(n)$.

Así, volviendo al ejemplo 1.1.3 obtenemos el resultado anunciado:

Ejemplo 1.1.4. *El primer jugador del juego del Nim descrito en el Ejemplo 1.1.3 puede ganar siempre el juego si, y sólo si, el número inicial de palillos n no es igual a $4k+1$, para algún $k \in \mathbb{Z},\ k \geq 0$.*

En efecto, ya se ha visto en el Ejemplo anterior que si hay un palillo, entonces el primer jugador pierde, ya que debe tomarlo necesariamente. Supongamos entonces el resultado cierto para cualquier número i inicial de palillos, con $1 \leq i \leq n$, y comprobemos que se cumple para un número inicial $n+1$.

Observemos antes que en cada jugada, el papel de los jugadores se invierte. Supongamos que A es el primer jugador y B el segundo. En el momento en el que A realice la primera jugada, es el turno de B, que en ese momento actuará como si fuese el primer jugador de un nuevo juego en el que se parte de un montón de palillos menor, y A es el que está a la espera, con lo cual actúa de segundo jugador.

En el enunciado del resultado encontramos, implícitamente, que debemos observar 4 casos distintos, que son $n+1 = 4k+1$, $n+1 = 4k+2$, $n+1 = 4k+3$ y $n+1 = 4k$.

Supongamos que $n+1 = 4k+1$ para algún $k \in \mathbb{Z},\ k \geq 0$. A puede tomar 1, 2 o 3 palillos quedando así $n = 4k$, $n-1 = 4(k-1)+3$ o $n-2 = 4(k-1)+2$ respectivamente. Utilizando la hipótesis de inducción completa, tenemos que $P(n-1)$, $P(n-2)$ y $P(n-3)$ son ciertas. Así, cualquiera de los tres casos implica la existencia de una estrategia ganadora para B, que es el que ahora desempeña el papel de primer jugador, con lo cual A resultará perdedor.

Si $n+1 = 4k$, A debe tomar 3 palillos, ya que en ese caso quedan $n-2 = 4(k-1)+1$. Por lo dicho anteriormente, B ahora desempeña el papel de primer jugador en un juego que parte de $4(k-1)+1$ palillos, que pierde siempre, por la hipótesis de inducción.

Si $n+1 = 4k+2$, A debe tomar 1 palillo, de modo que a B le queden $n = 4k+1$, lo que por la hipótesis de inducción implica que B no puede ganar nunca.

Por último, si $n+1 = 4k+3$, claramente A debe tomar 2 palillos, para que B tenga $n-1 = 4k+1$, resultando de nuevo a causa de la hipótesis de inducción que B será perdedor.

Ejemplo 1.1.5. *Después de transcurrir n meses en un experimento de invernadero, el número p_n de plantas de un tipo particular satisface las ecuaciones $p_1 = 3$, $p_2 = 7$ y*

$$p_n = 3p_{n-1} - 2p_{n-2}$$

para todo $n \geq 3$. *Probar que* $p_n = 2^{n+1} - 1$.

En primer lugar, es claro que los casos $n = 1, 2$ se verifican. Además si $n \geq 3$ y, se supone que para todo $1 \leq k \leq n$ se verifica la hipótesis, entonces

$$p_{n+1} = 3p_n - 2p_{n-1} = 3(2^{n+1} - 1) - 2(2^n - 1) = 3 \cdot 2^{n+1} - 2^{n+1} - 1 = 2^{n+2} - 1.$$

con lo que queda probado.

En ocasiones conviene demostrar que una propiedad es cierta para todos los enteros mayores que un entero n_0. Los principios de inducción simple y fuerte son válidos también en este caso sin más que cambiar $\mathbb{N}$ por

$$\{n \in \mathbb{Z} \,;\, n \geq n_0\}.$$

Ejemplo 1.1.6. *Cualquier número natural* $n \geq 2$ *se puede expresar como producto de números primos.*

Utilicemos el principio de inducción completa. En este caso la base inductiva será $P(2)$, que es cierta, ya que 2 es primo. Supongamos entonces que $P(k)$ es verdadera $\forall k \in \mathbb{Z},\ 2 \leq k \leq n$, y veamos que es cierta para $P(n+1)$. Si $n+1$ es primo, ya habremos acabado la demostración. Si $n+1$ no es primo, entonces existe algún primo p tal que $n+1 = pk$, donde $2 \leq k < n+1$, con lo que $2 \leq k \leq n$. Así, k se puede expresar como producto de números primos. Si $k = q_1 \cdot \ldots \cdot q_s$ es la factorización en primos de k, tendremos que $n+1 = p \cdot q_1 \cdot \ldots \cdot q_s$, quedando así demostrada la afirmación.

Ejemplo 1.1.7. *El ministro de Economía de Heiden decidió imprimir únicamente billetes de* 5 *y* 6 *crugens al comprobar que todos los productos costaban al menos* 20 *crugens. Demostrar que su razonamiento era correcto.*

Vamos a probar que todo natural mayor o igual que 20 se puede escribir como suma de 5's y 6's. Desde luego $20 = 5 \cdot 4$ verifica la propiedad. Además, dado $n \in \mathbb{N}$, si $k = 5x + 6y$, para todo $20 \leq k \leq n$, entonces demostremos que $n+1$ verifica la propiedad. Si suponemos $n \geq 24$, entonces $n - 4 \geq 20$ y $n - 4 = 5x + 6y$, con lo que

$$n + 1 = n - 4 + 5 = 5(x + 1) + 6y$$

Finalmente basta comprobar los casos intermedios $k = 21, 22, 23, 24$.

$$21 = 5 \cdot 3 + 6 \cdot 1, 22 = 5 \cdot 2 + 6 \cdot 2, 23 = 5 \cdot 1 + 6 \cdot 3, 24 = 6 \cdot 4.$$

Es interesante destacar que tanto la base inductiva como el paso inductivo son necesarios ya que, en ausencia de alguno de ellos el principio de inducción no es cierto. Veamos dos ejemplos en los cuales se aplica incorrectamente el principio de inducción.

Ejemplo 1.1.8. *Para cada n, sea $P(n)$ la propiedad que afirma que*

$$\sum_{i=1}^{n} i = \frac{\left(n+\frac{1}{2}\right)^2}{2}$$

Es fácil comprobar que si $P(k)$ es cierta, entonces

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + k + 1 = \frac{\left(k+\frac{1}{2}\right)^2}{2} + k + 1 = \frac{\left(k+1+\frac{1}{2}\right)^2}{2}.$$

Así se concluye que la propiedad es cierta para todos los naturales. Sin embargo, no es cierta para ninguno ya que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \neq \frac{\left(n+\frac{1}{2}\right)^2}{2}$$

Ejemplo 1.1.9. *Probemos que todos los coruñeses tienen la misma edad, usando el principio de inducción en el número de coruñeses.*

Es evidente que un conjunto unitario verifica la propiedad.
Si tomamos ahora un conjunto de n coruñeses

$$C = \{p_1, \ldots, p_n\}$$

y lo dividimos en dos conjuntos de $n-1$ elementos

$$A = \{p_1, \ldots, p_{n-1}\} \text{ y } B = \{p_2, \ldots, p_n\}$$

aplicando el paso inductivo a cada uno de ellos concluimos que todos las personas de A tienen la misma edad (d) y todas las de B también (f). Como $p_2 \in A \cap B$, se tiene que $d = f$ y se concluye que todos las personas de C tienen la misma edad. El principio de inducción permite concluir que todos los coruñeses tienen la misma edad, siendo evidentemente falsa tal afirmación.

1.2. Divisibilidad en $\mathbb{Z}$

En el conjunto de los números enteros, $\mathbb{Z}$, hay definidas dos operaciones: $+$ y $\cdot$. Se cumple que, si x, y son enteros tales que $xy = 0$, entonces $x = 0$ ó $y = 0$. En consecuencia, si $ab = ac$, siendo a, b, c tres números enteros y $a \neq 0$, entonces $b = c$.

Definición 1.2.1. *Dados dos enteros a y b, se dice que a* divide a *b (o que a es un factor o divisor de b o que b es un múltiplo de a), si existe algún entero q tal que $b = aq$. Esta situación se denota $a \mid b$ o, a veces, como $b = \dot{a}$.*

Como consecuencia inmediata, si $0 \mid b$, entonces $b = 0$. Además $1 \mid b$ y $b \mid 0$, para todo entero b.

Lema 1.2.2. *Sean $a, b, c, d \in \mathbb{Z}$. Se verifican las siguientes propiedades:*

I) *$a \mid a$.*

II) *Si $a \mid b$, entonces $a \mid bn$, $\forall n \in \mathbb{Z}$.*

III) *Si $a \mid b$ y $b \mid c$ entonces $a \mid c$, es decir, $\mid$ es transitiva.*

IV) *Si $a \mid b$ y $a \mid c$ entonces $a \mid bx + cy$, para cualquier par de enteros x, y. En general, si $a \mid b_i$, para ciertos enteros b_i, con $i = 1, \ldots, n$, se verifica que*

$$a \mid \sum_{i=1}^{n} x_i b_i,$$

para cualquier familia de enteros x_i.

V) *Si $a, b > 0$ y $a \mid b$ entonces $a \leq b$.*

VI) *Si $a \mid b$ y $b \mid a$ entonces $a = b$ o $a = -b$.*

VII) *Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.*

VIII) *Si $c \neq 0$ y $ac \mid bc$, entonces $a \mid b$.*

En temas relativos a la divisibilidad nos centraremos en enteros positivos ya que si $a \mid b$ entonces $\pm a \mid \pm b$.

Teorema 1.2.3. (Algoritmo de la división) *Sean a, b dos enteros, siendo b estrictamente positivo. Existen enteros q (cociente) y r (resto), tales que $a = bq + r$ y $0 \leq r < b$. Además, q y r son los únicos enteros verificando esas condiciones.*

Demostración. Probemos, en primer lugar la existencia y luego la unicidad.

- **Existencia** Consideremos el conjunto:

$$M = \{tb \leq a\}$$

de los múltiplos de b menores o iguales que a. Podemos encontrar q en $\mathbb{Z}$ tal que qb es el máximo de M. Por lo tanto, se verifica 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: $a = bq_i + r_i$, con $0 \leq r_i < b$, para $i = 1, 2$. Es claro que:

$$b(q_1 - q_2) = r_2 - r_1$$

y, por lo tanto, $b|q_1 - q_2| = |r_1 - r_2| < b$. Así pues, $b(|q_1 - q_2| - 1) < 0$ y, como estamos suponiendo que $b > 0$, deducimos que $0 \leq |q_1 - q_2| < 1$ y que $|q_1 - q_2| = 0$, por ser q_1 y q_2 enteros. Las propiedades del valor absoluto permiten concluir que $q_1 = q_2$.

□

Corolario 1.2.4. *Sean a y $b \neq 0$ dos enteros. Existen dos únicos enteros q y r con $0 \leq r <\mid b \mid$ y $a = bq + r$*

Demostración. Podemos suponer que $b < 0$, entonces el teorema anterior garantiza la existencia de dos únicos enteros q y $0 \leq r < -b =\mid b \mid$ tales que $a = (-b)q + r = b(-q) + r$. □

Recordemos que $|\ |: \mathbb{Z} \to \mathbb{N}$ es la aplicación definida como $\mid a \mid = a$ si $a \geq 0$ y $\mid a \mid = -a$ si $a < 0$.

Ejemplo 1.2.5. *Supongamos que queremos dividir -13 entre 6. Resulta muy tentador escribir el siguiente resultado para la división:*

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

Esta divisón, sin embargo, no está bien resuelta, ya que el resto es $-1 < 0$, lo cual contradice el enunciado del Teorema. El resultado correcto será

$$-13 = 6 \cdot (-3) + 5,$$

donde el resto, 5, es mayor que cero. Nótese que, aunque el múltiplo de 6 más próximo a -13 es $6 \cdot (-2) = -12$, a nosotros nos interesa que el resto sea mayor que cero, así elegimos el múltiplo $6 \cdot (-3) = -18$.

El siguiente esquema se corresponde con un posible algoritmo de división para dividir números positivos:

`leer` a, b
`hacer` $q := 0$ `y` $r := a$
`mientras` $r \geq b$ `hacer` $q := q + 1$ `y` $r := r - b$
`fin mientras`
`escribir` q, r

Ejemplo 1.2.6. *Veamos como resulta el algoritmo anterior para* $a = 23$ *y* $b = 5$.

n	a	b	q	r
0	23	5	0	23
1	23	5	1	18
2	23	5	2	13
3	23	5	3	8
4	23	5	4	3

Sin embargo, si a es negativo, este algoritmo debe ser cambiado por
`leer` a, b
`hacer` $q := 0$ `y` $r := a$
`mientras` $r < 0$ `hacer` $q := q - 1$ `y` $r := r + b$
`fin mientras`
`escribir` q, r

Ejemplo 1.2.7. *Comprobemos el nuevo algoritmo para* $a = -23$ *y* $b = 5$*:*

n	a	b	q	r
0	-23	5	0	-23
1	-23	5	-1	-18
2	-23	5	-2	-13
3	-23	5	-3	-8
4	-23	5	-4	-3
4	-23	5	-5	2

Ejemplo 1.2.8. *Si* a *es cualquier número entero, entonces* a, $a + 1$ *o* $a + 2$ *es un múltiplo de* 3.

Al dividir a entre 3, obtenemos q y $0 \leq r < 3$ tales que $a = 3q + r$. Si $r = 0$, entonces $a = \dot{3}$, si $r = 1$, se sigue que $a + 2 = 3q + 3 = \dot{3}$ y, si $r = 2$, se sigue que $a + 1 = \dot{3}$.

1.3. Algoritmo de Euclides

Definición 1.3.1. *Sean* $a, b \in \mathbb{Z}$*. Un entero* d *es un divisor común de* a *y* b *si* $d \mid a$ *y* $d \mid b$.

Sean $a, b \in \mathbb{Z}$ *no nulos. El* máximo común divisor *de* a *y* b, $d = mcd(a, b)$, *es un divisor común de* a *y* b *tal que* $d > 0$ *y,* $\forall c \in \mathbb{Z}$ *tal que* $c \mid a$ *y* $c \mid b$, *se tiene que* $c \mid d$*. Por convenio,* $mcd(a, 0) = \mid a \mid$*, en particular* $mcd(0, 0) = 0$.

La definición de máximo común divisor se puede extender a un conjunto finito de enteros $a_1, a_2, \ldots, a_n$*. Así,* $d = mcd(a_1, \ldots, a_n)$ *si* $d > 0$, $d \mid a_i$ $(\forall i, 1 \leq i \leq n)$ *y si* $c \mid a_i$ $(\forall i, 1 \leq i \leq n)$ *entonces* $d \mid c$.

Nota 1.3.2. *Sean $a, b \in \mathbb{Z}$ no nulos. Entonces se verifica:*

I) $a \mid b \Leftrightarrow mcd(a, b) = |a|$.

II) $mcd(a, b) = mcd(|a|, |b|)$.

Lema 1.3.3. *Si a, b, q, t son números enteros tales que $a = bq + t$, entonces*

$$mcd(a, b) = mcd(b, t).$$

Demostración. Sólo hay que tener en cuenta que los divisores comunes de a y b son los mismos que los de b y t. □

La aplicación reiterada del resultado anterior conduce al cálculo del máximo común divisor y se conoce con el nombre de **Algoritmo de Euclides**. Para aplicarlo haremos lo siguiente:

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:

$$\begin{array}{lcll}
a_0 & = & a_1q_1 + a_2 & 0 \leq a_2 < a_1 \\
a_1 & = & a_2q_2 + a_3 & 0 \leq a_3 < a_2 \\
a_2 & = & a_3q_3 + a_4 & 0 \leq a_4 < a_3 \\
 & \vdots & & \vdots \\
a_{k-2} & = & a_{k-1}q_{k-1} + a_k & 0 \leq a_k < a_{k-1} \\
a_{k-1} & = & a_nq_k + 0. &
\end{array}$$

Como la cadena de restos es tal que $a_1 > a_2 > a_3 > \ldots$ y son números naturales, se llegará a un resto nulo. Dado que:

$$mcd(a_0, a_1) = mcd(a_1, a_2) = mcd(a_2, a_3) = \cdots = mcd(a_{k-1}, a_k) = a_k$$

se concluye que el máximo común divisor es el último resto no nulo. Este método resulta bastante sencillo en algunos casos:

Ejemplo 1.3.4. *Utilizaremos el algoritmo de Euclides para obtener $mcd(1496, 612)$:*

$$\begin{aligned}
1496 &= 612 \cdot 2 + 272 \\
612 &= 272 \cdot 2 + 68 \\
272 &= 68 \cdot 4 + 0,
\end{aligned}$$

con lo que $mcd(1496, 612) = 68$.

Ejemplo 1.3.5. *Utilicemos el algoritmo anterior para el cálculo de* $mcd(250, 111)$. *Se obtiene la siguiente cadena de divisiones:*

$$\begin{aligned} 250 &= 111 \cdot 2 + 28 \\ 111 &= 28 \cdot 3 + 27 \\ 28 &= 27 \cdot 1 + 1 \\ 27 &= 1 \cdot 27 + 0 \end{aligned}$$

es decir: $mcd(250, 111) = 1$.

Teorema 1.3.6. (Teorema de Bezout) *Sean* a *y* b *enteros no ambos nulos. Existen enteros* r *y* s *tales que* $d = ra + sb$, *donde* $d = mcd(a, b)$. *Además,* d *es el menor entero positivo que se puede expresar de esa manera.*

Esquema de la demostración. Para demostrar el teorema de Bezout se comprueba, apoyándose en el algoritmo de la división, que el mínimo del conjunto $S = \{ma + nb > 0 \ ; \ m, n \in \mathbb{Z}\}$ es $d = mcd(a, b)$. □

El algoritmo de Euclides nos proporciona un método para el cálculo del máximo común divisor de a y b ($d = mcd(a, b)$) y, al mismo tiempo, nos calcula r y s tales que $d = ra + sb$.

Suponiendo que $a_{k+1} = 0$ y $a_k = mcd(a, b)$, tomaremos $r_0 = 1$, $r_1 = 0$, $s_0 = 0$ y $s_1 = 1$. Hallamos r_i y s_i, para $i \geq 2$, del modo siguiente:

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

Es fácil comprobar que, para cada $i \geq 0$, se verifica que:

$$a_i = r_i \cdot a + s_i \cdot b.$$

En particular,

$$a_k = r_k \cdot a + s_k \cdot b.$$

Recogemos los resultados para $mcd(250, 111)$ en la siguiente tabla:

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

Así, se tiene que $1 = 4 \cdot 250 + (-9) \cdot 111$.

Si recopilamos los resultados para $mcd(1496, 612)$ obtenemos:

i	a_i	q_i	m_i	n_i
0	1496	-	1	0
1	612	2	0	1
2	272	2	1	-2
3	68	4	-2	5

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

Como consecuencia del Teorema de Bezout tenemos:

Corolario 1.3.7. *Sean a y b números enteros no ambos nulos. Las siguientes afirmaciones son ciertas:*

I) *Existen enteros r y s tales que $1 = ra + sb$ si, y sólo si, $mcd(a, b) = 1$.*

II) *Si $mcd(a, b) = mcd(a, c) = 1$, entonces $mcd(a, bc) = 1$.*

III) *Si $mcd(a, b) = 1$, entonces $mcd(a^2, b^2) = 1$.*

IV) *Si $d \in \mathbb{Z}, d > 0$, entonces $d = mcd(a, b) \Leftrightarrow d \mid a$, $d \mid b$ y $mcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

1.4. Números primos. Factorización

Definición 1.4.1. *Sea $n \in \mathbb{N}$ un número natural. Una factorización de n es una expresión de la forma $n = ab$ con $1 \leq a, b \leq n$. Si $a = 1$ o $b = 1$, se dice que la factorización es trivial.*

Un número natural $n \neq 1$ es primo *si sólo admite la factorización trivial o, lo que es lo mismo, sus únicos divisores (en $\mathbb{N}$) son 1 y n. Los números que no son primos se denominan compuestos.*

Ejemplo 1.4.2. I) *Los primeros números primos son* 2,3,5,7,11,13,...

II) *Si $p \neq 3$ es primo, entonces p^2+2 es compuesto. Es claro que $p = 3q+r$ para $q \in \mathbb{Z}$ y $r = 1$ o $r = 2$ ya que p es primo y no es 3. Entonces*

$$p^2 + 2 = 9q^2 + 6qr + r^2 + 2$$

Como $r = 1, 2$, tenemos que $p^2 + 2 = \dot{3}$.

Definición 1.4.3. *Los números enteros $a_1, a_2, \ldots, a_n$ son* primos entre sí *si $mcd(a_1, \ldots, a_n) = 1$.*

Lema 1.4.4. (Lema de Euclides) *Si $a \mid bc$ y $mcd(a, b) = 1$, entonces $a \mid c$.*

Demostración. Si $a \mid bc$ existe un entero q tal que $bc = aq$ y enteros r, s tales que $1 = ra + sb$, con lo que $c = cra + csb = rca + saq = a(rc + sq)$, es decir $a \mid c$. □

Corolario 1.4.5. *Sea $p > 1$ un entero. Las siguientes condiciones son equivalentes:*

I) *p es primo*

II) *Si $p \mid ab$ y $a, b \in \mathbb{Z}$, entonces $p \mid a$ o $p \mid b$.*

Ejemplo 1.4.6. *El resultado anterior puede utilizarse para demostrar que $\sqrt{2}$ es irracional. En caso contrario, sean a, b dos naturales primos entre sí, tales que $\sqrt{2} = a/b$. Puesto que $2 \cdot b^2 = a^2$, se tiene que $2 \mid a^2$ y, en consecuencia, $a = 2m$. De este modo, $b^2 = 2 \cdot m^2$ y, por ello, $2 \mid b$, con lo que 2 es un divisor común de a y b y, por lo tanto, $mcd(a, b) \neq 1$.*

Teorema 1.4.7. Teorema Fundamental de la Aritmética *Sea $n \in \mathbb{Z}$ un entero con $|n| > 1$. Existen números primos $p_1, p_2, \ldots, p_r$ tales que*

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

Además, esta factorización es única.

Demostración. Por lo visto en el Ejemplo 1.1.6, podemos afirmar que cualquier número se puede expresar como producto de primos. Además, la factorización es única ya que, si $n = \pm q_1 q_2 \cdots q_s$ con $q_1 \leq q_2 \leq \ldots \leq q_s$ primos, se tiene que $r = s$ y $p_i = q_i$, para todo i. Luego, cualquier entero n admite una única factorización

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

con $p_1 < p_2 < \ldots < p_r$, primos distintos y $\alpha_i \geq 1$. □

Ejemplo 1.4.8. $10800 = 2 \cdot 5400 = 2^2 \cdot 2700 = \cdots = 2^4 \cdot 675 = \cdots = 2^4 3^3 5^2$

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

Teorema 1.4.9. (Criba de Eratóstenes) *Sea a un número entero mayor que 1. Si, para todo primo $p \leq \sqrt{a}$, se tiene que p no divide al número a, entonces a es primo.*

Demostración. Supongamos que a no es primo, es decir, existen $1 < b \leq c < a$ tales que $a = bc$. 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, tomemos p primo que divida a b. Es claro que $p \leq b \leq \sqrt{a}$. Como $p \mid b$ y $b \mid a$, se tiene que $p \mid a$ y de nuevo una contradicción. □

Ejemplo 1.4.10. *Encontremos todos los primos menores que* 60*. Como* $\sqrt{60} < 8$*, si un primo* $p \leq \sqrt{60}$*, se tiene que* $p = 2, 3, 5$ *o* 7*. Si escribimos todos los números entre* 1 *y* 60 *y tachamos 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

Ejemplo 1.4.11. *Comprobemos que el número* 2011 *es primo. Para ello realizamos las divisiones entre los sucesivos primos* $2, 3, 5, \ldots$*, y comprobamos que no dividen a* 2011*. Cuando llegamos al primo* 47 *obtenemos* $2011 = 47 \cdot 42 + 37$*. Vemos aquí que el cociente* 42 *es menor que* 47*, con lo que* 2011 *es primo.*

Definición 1.4.12. *Sean* a, b *dos enteros no nulos. Un número entero* m *es* múltiplo común *de* a *y* b *si* $a \mid m$ *y* $b \mid m$*. El* mínimo común múltiplo *de* a *y* b*,* $m = mcm(a, b)$*, es un múltiplo común de* a *y* b *tal que* $m > 0$ *y,* $\forall$ c *tal que* $a \mid c$ *y* $b \mid c$*, entonces* $m \mid c$*.*

La definición de mínimo común múltiplo se puede extender a un conjunto finito de enteros $a_1, a_2, \ldots, a_n$*. Así,* $m = mcm(a_1, \ldots, a_n)$ *si* $m > 0$*,* $a_i \mid m$ $(\forall i, 1 \leq i \leq n)$ *y si* $a_i \mid c$ $(\forall i, 1 \leq i \leq n)$ *entonces* $m \mid c$*.*

Nótese que si a es cualquier entero, entenderemos que $mcm(a, 0) = 0$.

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

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

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

Teorema 1.4.13. *Dados* a, b *enteros con la descomposición anterior, se verifica que:*

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

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

III) *Dados* a, b *enteros no nulos se verifica que:* $mcd(a, b)mcm(a, b) = \mid ab \mid$.

1.5. 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, que se llaman así en honor al matemático griego Diofanto (200-284). Hay ecuaciones diofánticas de muchos tipos, siendo tal vez la más conocida la que dio lugar al *último Teorema de Fermat*:

$$x^n + y^n = z^n, n \in \mathbb{Z}\ n \geq 3.$$

A consecuencia de este teorema, se sabe que esta ecuación no tiene soluciones enteras no triviales sea cual sea el entero $n \geq 3$.

Nosotros solo veremos un tipo de ecuaciones diofánticas, que son las conocidas como ecuaciones diofánticas lineales y tienen la forma $ax + by = n$, donde a, b y n son números enteros. Nuestro objetivo es buscar las soluciones enteras de estas ecuaciones.

Teorema 1.5.1. *Sean a, b, n números enteros. La ecuación $ax+by = n$ tiene solución si, y sólo si, $d = mcd(a, b)$ divide a n.*

Demostración. Sean x_0, y_0 dos números enteros tales que $ax_0 + by_0 = n$ y sea $d = mcd(a, b)$. Puesto que $d \mid a$ y $d \mid b$, por el apartado 4 del Lema 1.2.2, se tiene que $d \mid n$.

Recíprocamente, si $n = n'd$, entonces, dado que el Teorema de Bezout garantiza la existencia de enteros r, s tales que $ar + bs = d$, tenemos que los enteros $n'r$ y $n's$ forman una posible solución de la ecuación diofántica. □

Veamos cómo se obtienen las demás soluciones.

Teorema 1.5.2. *Sean a, b y n tres números enteros no nulos y supongamos que $d = mcd(a, b)$ es un divisor de n. Si (x_0, y_0) es una solución cualquiera de $ax + by = n$, cualquier otra solución (x, y) es de la forma:*

$$x = x_0 + t\frac{b}{d}\ ,\ y = y_0 - t\frac{a}{d}$$

siendo $t \in \mathbb{Z}$.

Demostración. Sean (x, y) y (x_0, y_0) dos soluciones de $ax + by = n$. Es claro que:

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

con lo que $\frac{b}{d}$ divide a $\frac{a}{d}(x - x_0)$. Teniendo en cuenta el corolario 1.3.7 y el lema de Euclides, se concluye que $x - x_0$ es un múltiplo de $\frac{b}{d}$, es decir, existe t entero tal que $x = x_0 + t\frac{b}{d}$. □

Ejemplo 1.5.3. *Calcula las soluciones de* $20x + 50y = 430$.

Dado que $10 = mcd(20, 50)$ y que

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

si multiplicamos la expresión anterior por 43, obtenemos que $x_0 = -86$, $y_0 = 43$ es una solución particular, con lo que la solución general viene dada por:

$$x = -86 + 5t \ , \ y = 43 - 2t$$

siendo t cualquier número entero.

Ejemplo 1.5.4. *La dueña de un restaurante necesita comprar por lo menos* 3 *besugos y* 6 *merluzas, para lo que dispone de* 196 *euros, que quiere gastar íntegros. Cada besugo cuesta 16 euros, y cada merluza cuesta 12. ¿Cuántos besugos y cuántas merluzas debe comprar, teniendo en cuenta que quiere comprar la menor cantidad de merluzas posible?*

Para resolver este problema planteamos la ecuación diofántica correspondiente, donde x es el número de merluzas e y el número de besugos:

$$12x + 16y = 196.$$

Como $mcd(16, 12) = 4$ divide a 196, la ecuación tiene solución. Además $4 = 16 - 12$, y $196 = 4 \cdot 49$, con lo que $x_0 = -49$ y $y_0 = 49$. Así la solución general es de la forma:

$$\begin{aligned} x &= -49 + 4t \\ y &= 49 - 3t. \end{aligned}$$

Como se deben comprar por lo menos 6 merluzas, los valores de t para los que esto sucede:

$$-49 + 4t \geq 6 \Rightarrow t \geq 13,5.$$

Teniendo en cuenta que necesita 3 besugos, veamos que valores de t cumplen esta condición:

$$49 - 3t \geq 3 \Rightarrow t \leq 15,3.$$

Obtenemos así que bien $t = 14$, bien $t = 15$. Es fácil ver que el número de merluzas es menor si $t = 14$, así obtenemos que se compran $-49 + 4 \cdot 14 = 7$ merluzas y $49 - 3 \cdot 14 = 7$ besugos.

1.6. Congruencias

Definición 1.6.1. *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:*

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

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

Ejemplo 1.6.2. $7 \equiv_3 4$ *y* $18 \equiv_2 6$.

Teorema 1.6.3. *Sean $a, b \in \mathbb{Z}$ y m un entero positivo. Entonces $a \equiv_m b$ si, y sólo si, el resto obtenido al dividir a y b entre m es el mismo. Como consecuencia, cada entero a es congruente módulo m con uno de los enteros $\{0, 1, \ldots, m-1\}$. Así, el conjunto cociente $\mathbb{Z}_m$ tiene m elementos que son:*

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

Ejemplo 1.6.4. *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 este conjunto, $[4] = [0], [5] = [1], \ldots$. En general, $[4n + r] = [r]$, con $0 \leq r < 4$.

Propiedades 1.6.5. *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 $ac \equiv_m bd$. Como consecuencia, podemos definir una suma y un producto en $\mathbb{Z}_m$.*[2]

II) *Si $ah \equiv_m bh$ y $mcd(h, m) = 1$, entonces $a \equiv_m b$.*[3]

Demostración. I) Si $a - b = mt$ y $c - d = mt'$, entonces $a + c = b + d + mt + mt'$ y $ac = (b + mt)(d + mt') = bd + mtd + mt'b + m^2tt'$.

II) Puesto que $m|h(a-b)$ y $mcd(h, m) = 1$, el lema de Euclides permite concluir que $a \equiv_m b$.

□

[2]Para un análisis detallado ver el Apéndice.

[3]La condición $mcd(h, m) = 1$ es necesaria ya que, por ejemplo $24 \equiv_2 6$ pero 4 no es congruente con 1 módulo 2.

Ejemplo 1.6.6. *Hallar el resto de la división de* $81412 \cdot 917$ *entre* 5.

El resto de dividir 81412 entre 5 es 2, con lo que $81412 \equiv_5 2$, y el resto de dividir 917 entre 5 es 2, es decir, $917 \equiv_5 2$. Así, $81412 \cdot 917 \equiv_5 4$.

Corolario 1.6.7. *Sean* $\{a_i \ ; \ i = 1, \ldots, n\}$ *y* $\{b_i \ ; \ i = 1, \ldots, n\}$ *enteros tales que* $a_i \equiv_m b_i$*, para cada* $1 \leq i \leq n$*. Entonces:*

$$\sum_{i=1}^{n} a_i \equiv_m \sum_{i=1}^{n} b_i$$

$$\prod_{i=1}^{n} a_i \equiv_m \prod_{i=1}^{n} b_i$$

Ejemplo 1.6.8. *Hallar el resto de la división de* 37^{7541} *entre* 7.

Puesto que $37 \equiv_7 2$ y que $2^3 \equiv_7 1$, basta tener en cuenta que:

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

con lo que el resto de la división es 4.

Teorema 1.6.9. *La ecuación* $ax \equiv_m b$ *tiene solución entera si, y sólo si,* $d = mcd(a,m)$ *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 (x_0, y_0) enteros tales que $ax_0 + my_0 = b$. Eso quiere decir que nuestra ecuación tendrá solución cuando la tenga la ecuación diofántica $ax + my = b$, lo cual ocurre si, y sólo si, $d = mcd(a, m)$ divide a b.

Además, las soluciones son de la forma

$$(x_0 + t\frac{m}{d}, y_0 - t\frac{a}{d})$$

siendo t 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

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

y, por lo tanto:

$$m(t_1 - t_2) = kmd, (t_1 - t_2) = kd.$$

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

Si ahora $s \geq d$, entonces, al dividir s entre d, obtenemos un resto $0 \leq r < d$, tal que

$$s = dq + r.$$

De este modo,

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

es decir que

$$(x_0 + \frac{sm}{d}) \equiv_m (x_0 + \frac{rm}{d})$$

□

Ejemplo 1.6.10. *Encontrar todas las soluciones no congruentes de* $9x \equiv_{15} 6$.

Como $mcd(9, 15) = 3$ 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 $4 + 10 = 14$.

Definición 1.6.11. *Dado un número natural m, se designa por $\phi(m)$ al número de enteros positivos r menores o iguales que m y son primos con m. Su expresión es:*

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

La función $\phi(m)$ se denomina *función ϕ 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 1.6.12. *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 $mcd(n, p^r) = 1$, 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

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

Nota 1.6.13. *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 canónica 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:

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

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 1.6.14. *(* **Teorema de Euler***) Sean a y m dos números enteros con $m \geq 1$; si $mcd(a, m) = 1$, 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 $mcd(8, 1 \cdot 3 \cdot 5 \cdot 7) = 1$, entonces:

$$11^4 \equiv_8 1$$

Teorema 1.6.15. *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 $mcd(a, p) = 1$ y $\phi(p) = p - 1$. □

Ejemplo 1.6.16. *Encuéntrese el resto de la división de* 32^{98} *entre* 7.

Como 7 es un primo que no divide a 32, se tiene que

$$32^6 \equiv_7 1$$

Por otro lado, $98 = 16 \cdot 6 + 2$ y $32^{98} \equiv_7 32^2$. Finalmente, nótese que

$$32^2 \equiv_7 4^2 \equiv_7 2.$$

1.7. 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 1.7.1. *Escribamos* 45 *en base* 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 1.7.2. *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* $i = 0, \ldots, k$ *y* $a_k \neq 0$. *Denotaremos* $n = a_k a_{k-1} \ldots a_1 a_{0(b}$

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

Ejemplo 1.7.3. *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 tomar entonces $A = 10, B = 11, C = 12$, 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 0. Por ejemplo:

$$n = 1 \mid 001 \mid 101 \mid 001_{(2}$$

Completamos el primer bloque 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:

$$m = 011 \mid 000 \mid 111 \mid 000 \mid 110_{(2}.$$

1.8. Introducción a la Criptografía

La Criptografía y las Matemáticas son ciencias muy antiguas, pero hasta hace poco tiempo han estado separadas debido, en gran medida, a que la primera de ellas ha sido una actividad ligada principalmente a la diplomacia y la guerra, lo que ocasionaba que sus estudios se mantuvieran secretos.

Tradicionalmente, la criptografía tiene 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, incomprensible para un observador no autorizado.

Paralelo a la criptografía transcurre lo que se conoce como criptoanálisis, cuyo objetivo es el contrario al de la criptografía, esto es, diseñar métodos para permitir a usuarios no autorizados acceder a la información cifrada. La conjunción de la criptografía y el criptoanálisis se conoce como la criptología.

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.

Finalmente debemos señalar que, 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 1.8.1. *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*

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

- *Una familia de transformaciones de descifrado*

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

Cada transformación E_k está definida por un algoritmo de cifrado común a todas las transformaciones de la familia y una clave k particular de la transformación. Análogamente, para las transformaciones D_k. Además se debe cumplir que $(D_k \circ E_k)(m) = m, \forall m \in M$, esto es, que todos los mensajes cifrados utilizando la clave k se pueden descifrar correctamente.

Definición 1.8.2. *Llamaremos* texto llano *al mensaje que se quiere encriptar, previo a la encriptación. El mensaje encriptado se conoce también como* texto cifrado.

1.8.1. Criptografía simétrica o de clave privada

Estos sistemas se basan en el uso de una clave secreta, que deben conocer tanto el emisor del mensaje A, como el receptor del mismo, B. En este caso, la transformación de desencriptado $D_k : C \to M$ es inversa de la transformación de encriptado $E_k : M \to C$, es decir, $D_k^{-1} = E_k$.

Es claro que este sistema plantea el problema de poder distribuir de manera segura las claves que se van a utilizar, ya que si no se dispone de un canal seguro, la clave puede ser interceptada, y si se dispone de uno, no es necesaria la encriptación.

Los métodos de cifrado simétrico son esencialmente de dos tipos: trasposición y substitución.

• **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 1.8.3. *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 SUELTAS, TU ERES SU PRISIONERO.

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

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

Texto cifrado:
TSCEOSURSOEOIOULATEESPIINRUERTETPIINRSLSETSURSURSOEO

• **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 1.8.4. *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

Cifrados afines

Un sistema criptográfico afín sigue el siguiente esquema:

- En este caso M y C son $\mathbb{Z}_n$, para algún $n \in \mathbb{Z}$ positivo y suficientemente grande.
- **Elección de la clave:** Se escojen dos valores $a, b \in \mathbb{Z}_n$ tales que $mcd(a, n) = 1$, y que conocen el emisor A y el receptor B. Es decir, el conjunto K de claves es $K = \{(n, a, b),\ n \in \mathbb{Z},\ n > 0,\ a \in \mathbb{Z}_n,\ mcd(a, n) = 1,\ b \in \mathbb{Z}_n\}$.
- **Cifrado:** A le quiere enviar a B el mensaje m, que previamente ha transformado en un elemento de $\mathbb{Z}_n$. Entonces realiza la transformación:

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

siendo c el mensaje que le envía a B.

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

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

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

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.

Ejemplo 1.8.5. *Para poder utilizar un cifrado afín, a cada letra del alfabeto se le asigna un número, por ejemplo, el lugar que ocupa alfabéticamente.*

Así:

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	07	L	12	R	19	Y	26
F	06	M	13	S	20	Z	27
G	07	N	14	T	21		

Para cifrar un mensaje utilizando un método de trasposición, multiplicaremos el valor de cada letra por un elemento inversible de Z_{27}, por ejemplo, haremos $E(x) \equiv_{27} 10x$, donde x denota una letra. Así, el mensaje SOMOS CAMPEONES, que se escribe $(20, 16, 13, 16, 20, 03, 01, 13, 17, 07, 16, 14, 07, 20)$, se convierte en $(11, 25, 22, 25, 11, 03, 10, 22, 08, 23, 25, 05, 23, 11)$, es decir, KXUXK CJUHVXEVK.

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

Nótese que no todas las sustituciones son posibles con este método, ya que solo podemos escojer valores de a que tengan inverso en $\mathbb{Z}_{27}$.

Ejemplo 1.8.6. *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 la cifra de Julio César, lo que haremos será transformar cada letra en un elemento de $\mathbb{Z}_{27}$ según la tabla dada en el ejemplo anterior, 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 $b = 3$.

Las cifras del tipo de Julio César pueden ser rotas fácilmente, mediante un análisis de las frecuencias de las letras de un idioma. Para resolver este problema se utilizó el *sistema Vigenére*, que consiste en separar el mensaje en bloques de letras del mismo tamaño, y a cada letra del bloque aplicarle una cifra tipo Julio César, lo que dificulta mucho el descifrado de un mensaje, aunque actualmente se conocen métodos para hacerlo.

Ejemplo 1.8.7. *El siguiente mensaje ha sido encriptado mediante el método de Vigenére:*

BYEIECEULQQKUCFW

Para desencriptarlo, necesitamos conocer el tamaño de los bloques, y saber cuántos lugares se ha movido cada letra. Si el emisor nos dice que ha escogido bloques de cuatro letras, y que en cada bloque la primera letra se ha movido 3 lugares a la derecha, la segunda 2 lugares a la izquierda (o, lo que es lo mismo, 25 lugares a la derecha), la tercera 12 lugares a la derecha y la cuarta 18 lugares a la izquierda, simplemente tendremos que deshacer estos cambios obteniendo que el mensaje en texto llano es

YA SABES MI SECRETO

Ejemplo 1.8.8. *Un cifrado de clave privada utilizado de forma muy extendida hasta hace poco, es el conocido como* cifrado DES *(Data Encryption Standard). Es un cifrado por bloques, para el que se dispone de una clave de una longitud determinada (usualmente* 64 *bits), y que funciona como combinación de sustituciones y trasposiciones.*

Se han encontrado formas de romper el cifrado DES, con lo que, a pesar de que se utilizó mucho en el pasado, actualmente se prefieren algoritmos mejorados o incluso otros estándares de cifrado.

Hagamos notar, finalmente, que la seguridad de un criptosistema simétrico se basa en la clave que se utiliza (esencialmente, en la longitud de la misma, si ésta es un número) y en la garantía que podamos tener de que sólo el emisor y el receptor conocen esta clave. Así, aunque hay sistemas de clave

privada muy seguros, no se pueden garantizar al cien por cien los objetivos que se mencionaban anteriormente. Como contrapartida, con un criptosistema simétrico suele ser fácil (computacionalmente) encriptar y desencriptar un mensaje. Esta característica es la que hace que sigan siendo utilizados actualmente.

1.8.2. Criptografía asimétrica o de clave pública

La idea de la criptografía asimétrica es utilizar funciones de dirección única $f : M \to C$, 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.[4]

El proceso es el siguiente, cada usuario U dispone de una *clave pública* (que podrán conocer todos los demás) k_U^1 y una *clave privada* (que se reserva para él) k_U^2. 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 $m = D_{k_B^2}(s)$. Está claro que $D_{k_B^2} \circ E_{k_B^1}$ es la función identidad.

Hay un 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 sóla vía se ha basado, hasta el momento, en el uso de la Aritmética modular.

Ejemplo 1.8.9. *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 $s = D_{k_B^2}(c)$ que le resulta ininteligible. Finalmente, hace uso de la clave pública de A y obtiene $m = D_{k_A^1}(s)$.*[5] *Nótese que ahora necesitamos, además que $D_{k_A^1} \circ E_{k_A^2}$ sea igual a la identidad.*

Método de El-Gamal

El método de El-Gamal se basa en el problema computacional difícil de calcular logaritmos discretos. Es decir, dados dos elementos $a, b \in \mathbb{Z}_n$, ¿existe

[4] 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 $f^{-1}(y)$.

[5] El hecho de que sólo la clave pública de A invierte su clave privada garantiza que ha sido A el emisor del mensaje.

un entero positivo k tal que $a^k = b$? Aunque la respuesta es fácil de encontrar si n es un número pequeño, si es un número muy grande el tiempo de computación para encontrar una respuesta se dispara.

Los usuarios del método El-Gamal conocen el valor de un número primo p grande y el de un número entero positivo a tal que $a^{p-1} \equiv_p 1$. Además, el mensaje a enviar m será un entero en el conjunto $\{1, \ldots, p-1\}$. En este caso, el mensaje encriptado constará de dos elementos C_1 y C_2 de $\mathbb{Z}_p$. Una vez fijado ésto, veamos cómo son la clave pública, la clave privada y los algoritmos de encriptado y desencriptado:

- **Clave privada:** La clave privada de un usuario B es un entero $k_B \in \{2, \ldots, p-2\}$ escogido aleatoriamente.
- **Clave pública:** La clave pública de B es $y_B \equiv_p a^{k_B}$.
- **Algoritmo de encriptado:** Supongamos que un usuario A desea enviar un mensaje m a B. Entonces A deberá seguir los pasos indicados a continuación:

  I) Escoger un entero $k \in \{2, \ldots, p-1\}$.

  II) Hacer $K \equiv_p (y_B)^k$.

  III) Hacer $C_1 \equiv_p a^k$ y $C_2 \equiv_p K \cdot m$. Así obtiene el mensaje encriptado (C_1, C_2).

- **Algoritmo de desencriptado:** Cuando B recibe el mensaje cifrado (C_1, C_2) que le ha enviado A, procede a desencriptarlo de la siguiente manera:

  I) Recupera K como $K \equiv_p (C_1)^{k_B}$. En efecto:

  $$K = (y_B)^k = (a^{k_B})^k = (a^k)^{k_B} = C_1^{k_B}.$$

  II) Calcula K^{-1} en $\mathbb{Z}_p$ y recupera m como $m \equiv_p K^{-1} \cdot C_2$.

Si una persona, que no conociera la clave privada de B, quisiera decodificar el mensaje tendría que despejar m de $C_2 \equiv_p K \cdot m$. Para ello debe resolver un logaritmo discreto, lo que supone un tiempo de ejecución no polinomial.

Nota 1.8.10. *Si se quiere cifrar un mensaje deberemos transformarlo en un número m. Puede suceder que una vez transformado, el número con el que se corresponde el mensaje resulte demasiado grande. En este caso, demasiado grande quiere decir mayor que $p-1$. Si esto sucede, el mensaje se dividirá en bloques de tamaño $p-1$.*

Ejemplo 1.8.11. *Dos amigos, Benito y Alicia, convinieron en utilizar el primo* $p = 17$ *y* $a = 3$ *para encriptar sus mensajes con el método de El-Gamal. La clave privada de Alicia es* $k_B = 6$*. Así, su clave pública es* $y_B \equiv_{17} 3^6 \equiv_{17} 15$.

Benito quiere enviarle un mensaje m *con valor numérico 9 a Alicia para ello, genera un número aleatorio* $k = 5$*. Para ello calcula* $K = 15^5 \equiv_{17} 2$, $C_1 = 3^5 \equiv_{17} 5$ *y* $C_2 = K \cdot 9 \equiv_{17} 2 \cdot 9 \equiv_{17} 18 \equiv_{17} 1$ *y le envía a Alicia* $(5, 1)$.

Alicia para decodificar el mensaje sólo tiene que calcular $K^{-1} \equiv_{17} 9$*, con lo que obtiene* $m \equiv_{17} 9 \cdot 1 = 9$.

El método de El-Gamal tiene inconvenientes. En primer lugar, requiere mucho tiempo de computación. Además por cada trozo de mensaje que se codifique hay que enviar dos mensajes C_1 y C_2, con lo cual se está duplicando la información original.

Método de Merkle-Hellman

Este método se basa en el problema difícil conocido como *problema de la mochila*.

Problema de la mochila: Dado un conjunto de números enteros positivos $\Delta = \{a_1, \ldots, a_n\}$ y otro entero positivo t, ¿existe algún subconjunto $\{a_{k_1}, \ldots, a_{k_r}\}$ de Δ tal que $t = a_{k_1} + \cdots + a_{k_r}$? Es decir, ¿existe algúna secuencia binaria $(x_1, \ldots, x_n)$ tal que

$$t = \sum_{i=1}^{n} x_i a_i ?$$

Aunque el problema tiene un enunciado sencillo, y a priori puede parecer fácil de resolver, lo cierto es que si el conjunto Δ es muy grande, la solución se vuelve muy complicada, ya que analizar todas las posibles sumas de todos los subconjuntos de Δ puede llevar años en un computador potente.

Sin embargo, si el conjunto Δ es de un tipo especial, existe un algoritmo sencillo que dice si el problema tiene solución, y en caso afirmativo encontrarla.

Definición 1.8.12. *Un conjunto* $\Delta = \{a_1, \ldots, a_n\}$ *de enteros positivos es* supercreciente *si* $a_k > \sum_{i=1}^{k-1} a_i \ \forall k, 1 \leq k \leq n$.

Si Δ es supercreciente y t es un entero positivo, existe un algoritmo para resolver el problema en esta situación. Se busca una sucesión binaria $(x_1, \ldots, x_n)$ verificando que $t = \sum_{i=1}^{n} a_i \cdot x_i$. Dado que $a_n > \sum_{i=1}^{n-1} a_i$, $x_n = 1$ si, y solo si, $t \geq a_n$; y podemos repetir el razonamiento para $t - a_n \cdot x_n$ y el conjunto $\{a_1, \ldots, a_{n-1}\}$. El algoritmo en pseudocódigo se define como

para $i = 1$ hasta $i = n$ hacer
si $t \geq a_i$ entonces $x_i = 1$
en otro caso $x_i = 0$
$t = t - a_i \cdot x_i$
fin para
si $t = 0$ $x = (x_1, \ldots, x_n)$ es la solución
en otro caso no existe solución

Ejemplo 1.8.13.

- *Por ejemplo, si* $\Delta = \{2, 3, 37, 13, 28, 55, 110, 221\}$ *y* $t = 353$ *el algoritmo nos da* $t_8 = 353 - 221 = 132$, $t_7 = 22$, $t_6 = t_7$, $t_5 = t_6$, $t_4 = 22 - 13 = 9$, $t_3 = 9 - 7 = 2$, $t_2 = t_3$, $t_1 = 2 - 2 = 0$. *Tiene solución* $353 = 221 + 132 + 22 + 9 + 2$.

- *En el caso de tener una sucesión arbitraria que no sea supercreciente podemos tener todo tipo de resultados. Por ejemplo, si tenemos* $\Delta = \{20, 5, 7, 36, 13, 2\}$ *y* $t = 35$ *el algoritmo nos da* $t_6 = 35 - 2 = 33$, $t_5 = 20$, $t_4 = t_5$, $t_3 = 13$, $t_2 = 13 - 5 = 8$ *y* $t_1 = t_2$ *como ninguno es cero deduciríamos que no tiene solución. Pero no es cierto ya que* $35 = 20 + 13 + 2$.

Basándose en la existencia de este algoritmo, y en que el problema de la mochila es un problema de solución difícil, se puede pensar en transformar una sucesión supercreciente Δ en otra B que no lo sea, y encriptar un mensaje utilizando la condición del problema de la mochila para B. Así:

- El conjunto M está formado por cadenas de 0's y 1's de longitud n. Si un mensaje tiene una longitud mayor, se divide en varios bloques de longitud n, completando con 0's si alguno de los bloques tiene longitud menor que n.

  El conjunto C es un subconjunto de $\mathbb{Z}$.

- **Clave privada:** La clave privada de un usuario B consiste en tres componentes $k_B^2 = (\Delta, N, W)$:

  - Un conjunto supercreciente $\Delta = \{a_1, \ldots, a_n\}$, con n suficientemente grande.
  - Un entero $N > \sum_{i=1}^{n} a_i$.
  - Un entero $0 < W < N$ tal que $mcd(W, N) = 1$.

- **Clave pública:** La clave pública de B es la sucesión $k_B^1 = \{b_1, \ldots, b_n\}$, donde $b_i \equiv_N W a_i$, $\forall i = 1, \ldots, n$.

- **Algoritmo de encriptado:** Si el mensaje que desea enviar A a B es $m = x_1 \cdots x_n$, donde $x_i \in \{0, 1\}$, se obtiene

$$E_{k_B}(m) = \sum_{i=1}^{n} x_i b_i = c.$$

- **Algoritmo de desencriptado:** Para desencriptar c, B debe:

  I) Hacer $s \equiv_N cW^{-1}$, donde W^{-1} es el inverso de W en $\mathbb{Z}_N$. Nótese además que, como $\sum_{i=1}^{n} a_i < N$:

$$s = cW^{-1} = (\sum_{i=1}^{n} x_i b_i)W^{-1} = (\sum_{i=1}^{n} x_i a_i W)W^{-1} = \sum_{i=1}^{n} x_i a_i.$$

  II) Aplicar el algoritmo descrito más arriba para obtener los x_i no nulos dentro de la expresión de s.

Se debe resaltar que este método ha sido roto hace ya años, por lo que se han introducido modificaciones que lo hacen más seguro, por ejemplo, introduciendo una permutación en el orden de la sucesión supercreciente, que formará parte de la clave privada.

Método 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. Aunque obtener la factorización en números primos de un número pequeño es relativamente fácil, cuando es muy grande la tarea se convierte en algo realmente complicado. Para hacernos una idea, miembros de la Universidad de Bonn, de la compañía japonesa NTT y de la École Polytechnique Fédérale de Lausanne tardaron 11 meses en factorizar un número de 307 cifras, con la particularidad de que este era un número de una forma especial que facilitó la tarea. Un número escogido aleatoriamente de esta magnitud puede tardar años en factorizarse[6]. Por otro lado, también se basa en la dificultad que existe en la obtención de logaritmos discretos.

[6]Los RSA Laboratories, una empresa que se dedica a explotar el código RSA, propone retos que consisten en factorizar números enormes. Como curiosidad puede consultarse la página web `http://www.rsa.com/rsalabs/node.asp?id=2093`

Corolario 1.8.14. *Sean p, q dos primos distintos, sea $n = pq$ y sea e un número natural tal que $mcd(e, \phi(n)) = 1$. Entonces, para todo número natural a, se tiene que:*

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

donde $e \cdot d \equiv_{\phi(n)} 1$.

Demostración. Si $mcd(a, n) = 1$, entonces el Teorema de Euler garantiza que $a^{\phi(n)} \equiv_n 1$ y, en consecuencia:

$$a^{ed} = a^{\phi(n)k+1} \equiv_n a$$

Supongamos, pues que $mcd(a, n) \neq 1$. Si a y n sólo tienen un divisor en común, este puede ser p o q. Supongamos que es p. Como $mcd(a, q) = 1$, se tiene que $a^{q-1} \equiv_q 1$ y, ya que, $\phi(n) = (p-1)(q-1)$, se cumple que $a^{\phi(n)} \equiv_q 1$ y, en consecuencia

$$a^{ed} \equiv_q a.$$

La misma igualdad se verifica si sustituimos q por p, ya que a y a^{ed} son múltiplos de p . Dado que $n = pq = mcm(p, q)$, concluimos que:

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

Únicamente queda por analizar el caso en el que a es un múltiplo de n. Es claro que, con esa hipótesis, se verifica trivialmente la igualdad. □

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

- B escoje 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 cuyo inverso es difícil de calcular.

- **Algoritmo de desencriptado:** Para descifrar el mensaje, B utiliza la siguiente fórmula:
$$m \equiv_n c^d,$$
que sabemos que nos permite recuperar el mensaje original gracias al Corolario 1.8.14.

Nota 1.8.15. *Una vez escrito el mensaje en un código numérico (ASCII, o el que se haya elegido), el número resultante es mayor o igual que n, se procederá, como en los métodos anteriormente descritos, a dividir el mensaje en bloques menores que n.*

Ejemplo 1.8.16. *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	07	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 3012001.

Ejemplo 1.8.17. *Alicia quiere transmitir a Benito el mensaje CASA. La clave pública RSA de Benito es*
$$(n, e) = (328419349, 220037467).$$
La clave privada de Benito es $\phi(n) = 328366764$ y $d = 119923$.

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

Benito desencripta c haciendo:

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

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

Finalmente, hay que señalar que no todo son ventajas con los criptosistemas de clave pública. Por un lado, son muy lentos (es más rápido encriptar con claves simétricas), por otro lado, hemos de encriptar nuestro mensaje m tantas veces como destinatarios (usando en cada caso la clave pública de cada receptor). Es por ello que, actualmente, algunos programas como PGP, combinan clave simétrica y clave asimétrica. La idea es la siguiente.

Supongamos que A quiere enviar m a B y C simultáneamente. A comienza generando una clave simétrica K de manera aleatoria y encripta m con dicha clave (rápido, por ser una clave simétrica) con lo que resulta c. A continuación, encripta K con las claves públicas de B y C, obteniendo, respectivamente, s_B y s_C (rápido también porque, aunque se usa clave asimétrica el mensaje a encriptar es la clave K que es relativamente pequeña).

Lo que envía A es el "paquete"

$$(c, s_B, s_C).$$

Cuando B lo recibe, descifra s_B con su clave privada y recupera la clave K, con la cual descifrará el cuerpo del mensaje c para obtener finalmente m.

El peligro potencial para la criptografía de clave pública RSA es que en algún tiempo futuro, alguien logre encontrar una manera rápida de factorizar n ya que, se cree que en el 2014 se podrán factorizar números de $2^{11} = 2048$ bits. Todo ello, sabiendo además que los servicios de inteligencia militares y civiles (CIA, FBI, etc) no comparten sus resultados con el resto del mundo e invierten muchos recursos en investigación.

1.9. Apéndice

1.9.1. Operaciones en $\mathbb{Z}_m$

Hemos visto en Propiedades 1.6.5 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, $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$, y tendremos una suma y un producto:

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

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

Ejemplo 1.9.1. *Si $m = 9$ tenemos el conjunto*

$$\mathbb{Z}_9 = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\}.$$

Realicemos alguna suma en este conjunto: $[5]+[8] = [4]$, ya que $5+8 = 13$ y $13 = 9+4$, con lo que $13 \equiv_9 4$. Del mismo modo, tenemos que $[7] \cdot [8] = [2]$, porque $56 = 9 \cdot 6 + 2$ y por lo tanto $56 \equiv_9 2$.

Para tener una visión más amplia vamos a representar la suma y el producto en $\mathbb{Z}_9$ en una tabla del tipo

$*$	$[0]$	$\cdots$	$[i]$	$\cdots$	$[m-1]$
$[0]$	$[0 * 0]$	$\cdots$	$[0 * i]$	$\cdots$	$[0 * (m-1)]$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$[j]$	$[j * 0]$	$\cdots$	$[j * i]$	$\cdots$	$[j * (m-1)]$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$[m-1]$	$[(m-1) * 0]$	$\cdots$	$[(m-1) * i]$	$\cdots$	$[(m-1) * (m-1)]$

donde $*$ será $+$ o $\cdot$, según convenga.

Ejemplo 1.9.2. *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 1.9.3. *Sea $m \in \mathbb{Z}$, $m > 0$, y $[a], [b] \in \mathbb{Z}$.*

I) $[a] + [b] = [b] + [a]$ *(propiedad conmutativa)*

II) $[a] + [0] = [a]$ *(elemento neutro)*

III) $[a] + [m - a] = [0]$. *En general, $-k \equiv_m m - k \ \forall k \in \mathbb{Z}$ (elemento opuesto).*

Ejemplo 1.9.4. *Estudiemos ahora la tabla de la multiplicación en $\mathbb{Z}_9$:*

$\cdot$	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 1.9.5. *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* $[a] \cdot [1] = [a]$

En virtud del Teorema 1.6.9 podemos calcular todos los elementos inversibles en $\mathbb{Z}_m$:

Proposición 1.9.6. *$[a]$ tiene inverso en $\mathbb{Z}_m$ si, y sólo si, $mcd(a, m) = 1$.*

Demostración. $[a]$ tiene inverso en $\mathbb{Z}_m$ si, y sólo si, existe $x \in \mathbb{Z}$ tal que $ax \equiv_m 1$, y sabemos que esta ecuación tiene solución cuando, y sólo cuando, $mcd(a, m)|1$. □

Como corolario obtenemos:

Corolario 1.9.7. *Todos los elementos no nulos de $\mathbb{Z}_m$ tienen inverso si, y sólo si, m es primo.*

Una consecuencia de que el elemento $[a]$ tenga inverso en $\mathbb{Z}_m$ es que si $[a] \cdot [b] = [a] \cdot [c]$, entonces $[b] = [c]$. Si $[a]$ no tiene inverso, esta propiedad no se cumple. Por ejemplo, en $\mathbb{Z}_9$ se tiene que $[4] \cdot [6] = [7] \cdot [6]$, pero $[4] \neq [7]$.

1.9.2. Criterios de Divisibilidad

Dado un número natural $n = a_k \cdots a_1 a_{0(b}$ 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 $m = 2$. Para cualquier m, 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 $10 \equiv 1 \bmod 3$, 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 $10 \equiv 3\ mod(7)$, $10^2 \equiv 9 \equiv 2\ mod(7)$, $10^3 \equiv 6 \equiv -1\ mod(7)$, $10^4 \equiv 4 \equiv -3\ mod(7)$, $10^5 \equiv 5 \equiv -2\ mod(7)$, $10^6 \equiv 1\ mod(7)$ 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 $10 \equiv -1 \bmod 11$, tenemos que $r_{2k} = 1$ y $r_{2k+1} = -1$, para cualquier k. De este modo, n es múltiplo de 11 si lo es $a_0 - a_1 + a_2 - a_3 + \cdots$.