Capítulo 3

Teoría de números

3.1. Principio de inducción

Una característica fundamental de los números naturales es que cualquiera de ellos puede ser obtenido a partir del uno 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 uno tiene una propiedad P y, además 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. Si denotamos por $P(n)$ al predicado "n satisface la propiedad P", podemos enunciar el principio anterior como

`Para toda propiedad` P`:`

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

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

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 contigua (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.

Ejemplo 18. 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

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

En ocasiones el principio de inducción no puede aplicarse directamente. Aplicaremos entonces el llamado *principio de inducción fuerte o completa* que podemos enunciar como sigue:

`Para toda propiedad` P`:`

- **Base inductiva** $P(1)$
- **Paso inductivo completo** `Si para todo natural` n `se cumple que, si` $P(k)$ `para todos los naturales` $k \leq n$`, también se tiene` $P(n+1)$`.`

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

Ejemplo 19. *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

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

Veamos un ejemplo:

Ejemplo 20. *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* $20 = 5*4$ *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 $k = 21, 22, 23, 24$*.*

$$21 = 5 * 3 + 6 * 1, 22 = 5 * 2 + 6 * 2, 23 = 5 * 1 + 6 * 3, 24 = 6 * 4$$

Nota 2. *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.*

Ejemplo 21. *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 concluiría 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 22. *Probemos que todos los coruñeses tienen la misma edad. 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

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

aplicando el principio de inducción 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.

3.2. Divisibilidad en $\mathbb{Z}$

En el conjunto de los enteros $\mathbb{Z}$, hay definidas dos operaciones + y . verificando ciertas propiedades. Entre ellas que, si dados dos enteros x, y, se tiene que $xy = 0$, entonces $x = 0$ o $y = 0$. En consecuencia, si $ab = ac$, siendo a, b, c tres números enteros y $a \neq 0$, entonces $b = c$.

Definición 40. *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 $b = \dot{a}$.*[1]

Lema 1. *La relación anterior verifica las siguientes propiedades:*

I) *Si a es un entero, entonces $a \mid a$ (Reflexiva).*

II) *Si a y b son dos enteros y $a \mid b$, entonces $a \mid bc$, $\forall c \in \mathbb{Z}$.*

III) *Sean a, b y c tres números enteros. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$ (Transitiva).*

IV) *Sean a, b y c tres números enteros. 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*

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

para cualquier familia de enteros a_i.

[1] Si $a = 0$ y $a \mid b$, entonces $b = 0$. Además $1 \mid b$ y $b \mid 0$, para todo entero b.

v) *Sean $a > 0$ y $b > 0$ dos enteros. Si $a \mid b$, entonces $a \leq b$.*

Dado que $b = aq$ y q ha de ser mayor que cero, es claro que $q \geq 1$, y $a \leq b$.

vi) *Sean a y b dos enteros. Si $a \mid b$ y $b \mid a$, entonces $a = b$ o $a = -b$.*[2]

Puesto que existen enteros q, q' tales que $a = bq$ y $b = aq'$, se tiene que $a = aq'q$, y, por lo tanto $qq' = 1$. Concluimos pues que $q = q' = 1$ $(a = b)$ o $q = q' = -1$ $(a = -b)$.

vii) *Sean a, b, c y d cuatro números enteros. Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.*

viii) *Sean a, b y c tres números enteros tales que $c \neq 0$ y $ac \mid bc$, entonces $a \mid b$.*

Definición 41. *La aplicación:*

$$| \ |: \mathbb{Z} \to \mathbb{N} \cup \{0\}$$

definida, para cada entero a, como:

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

se denomina aplicación valor absoluto.

De la definición, se deduce que

- $| \ a \ | = max(a, -a) = | -a|$
- $| \ a \ | \geq 0$,
- $| \ a \ | = 0$ si, y sólo si, $a = 0$
- $| \ a + b \ | \leq | \ a \ | + | \ b \ |$, para todo par de enteros a y b.
- $| \ a \cdot b \ | = | \ a \ | \cdot | \ b \ |$, para todo par de enteros a y b.

Teorema 2. (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 en esas condiciones.*

[2]Esta propiedad junto con la I) y la III) garantizan que la relación "|"definida sobre cualquier subconjunto $X \subseteq \mathbb{Z}^+$ o $X \subseteq \mathbb{Z}^-$ es una relación de orden.

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 $b \mid (q_1 - q_2) \mid = \mid r_2 - r_1 \mid < b$ (ya que $0 \leq r_i < b$). Si $q_1 \neq q_2$, entonces $\mid q_1 - q_2 \mid \geq 1$, con lo que $\mid r_2 - r_1 \mid = b \mid (q_1 - q_2) \mid \geq b$. Se concluye, pues que $q_1 = q_2$ y $r_1 = r_2$.

□

Corolario 1. *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 $a = (-b)q + r = b(-q) + r$. □

El siguiente esquema se corresponde con un posible algoritmo de división:
`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 23. *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*

Ejemplo 24. *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 $a+1 = \dot{3}$.*

3.3. Algoritmo de Euclides

Definición 42. *Sean $a, b \in \mathbb{Z}$. Un entero d es un divisor común de a y b si $d \mid a$ y $d \mid b$.*

Un divisor común de a y b es el máximo común divisor *de a y b ($d = mcd(a,b)$) si, y sólo si, $d > 0$ y, $\forall c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$, se tiene que $c \mid d$. El máximo común divisor es, por lo tanto, el mayor de todos los divisores comunes de a y b.*[3]

Nota 3. *Fijémonos que el conjunto de divisores comunes de a y b:*

$$D = \{n \in \mathbb{Z} \,;\, n \mid a \text{ y } n \mid b\}$$

es no vacío ($1 \in D$) y está acotado superiormente por $\mid a \mid$ y $\mid b \mid$. Por lo tanto, admite máximo que es $mcd(a,b)$.

Nota 4. *Es claro que:*

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

Nota 5. *Para cualquier par de enteros a y b, se tiene que:*

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

Nota 6. *La definición de máximo común divisor se puede extender a un conjunto finito de enteros $a_1, a_2, \ldots, a_n$.*

El algoritmo de Euclides es un método para el cálculo del mcd de dos números que proviene del matemático de la Grecia clásica Euclides. Se basa en el siguiente lema. Además, podemos suponer que $a > b > 0$ (basta tener en cuenta la nota anterior y que $mcd(a,a) = a$).

Lema 2. *Si a, b, q, r son números enteros tales que $a = bq + r$, entonces $mcd(a,b) = mcd(b,r)$.*

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

[3]Cuando $a = b = 0$, el conjunto de los divisores comunes de a y b es no finito, por lo que diremos que $mcd(0,0) = 0$. Además, $mcd(a,0) = \mid a \mid$, para cualquier entero a.

La aplicación reiterada del lema anterior conduce al cálculo del máximo común divisor y se conoce con el nombre de *Algoritmo de Euclides*. 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 $a_{n+1} = 0$. La expresión del algoritmo es:

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

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:

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

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

Ejemplo 25. *Utilicemos el algoritmo anterior para el cálculo de* $mcd(250, 111)$. *Se obtiene la siguiente cadena de divisiones:*

$$\begin{array}{l} 250 = 111 * 2 + 28 \\ 111 = 28 * 3 + 27 \\ 28 = 27 * 1 + 1 \\ 27 = 27 * 1 + 0 \end{array}$$

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

Teorema 3. (Teorema de Bezout) *Sean a y b dos enteros. Existen $d = mcd(a, b)$ y enteros m y n tales que $d = ma + nb$. Además, d es el menor entero positivo que se puede expresar de esa manera (como "combinación lineal de" a y b)*

Demostración. Consideremos el conjunto:

$$S = \{ma + nb > 0 \ ; \ m, n \in \mathbb{Z}\}.$$

Es claro que[4] $S \neq \emptyset$. El principio del buen orden garantiza la existencia de $d = min(S)$. Al ser d un elemento de S, existen enteros m y n tales que $d = ma + nb$.

[4]Si a (o b) es estrictamente positivo, tomamos $a = a \cdot 1 + b \cdot 0$. Si a y b son enteros negativos, tomaremos $-a = a \cdot (-1) + b \cdot 0$

Por otro lado, si dividimos a entre d, obtenemos $a = dq+r$, con $0 \leq r < d$. Puesto que $r < d = min(S)$, es claro que $r \notin S$ y, dado que:

$$r = a - dq = a - (ma + nb)q = (1 - mq)a + (-nq)b,$$

concluimos que, necesariamente, $r = 0$, es decir $d \mid a$. Análogamente, se prueba que $d \mid b$.

Por último, si $c \mid a$ y $c \mid b$, y $a = cq$, $b = cs$, entonces

$$d = ma + nb = m(cq) + n(cs) = c(mq) + c(ns),$$

es decir, $c \mid d$ y d es, efectivamente, el máximo común divisor de a y b. □

Nota 7. *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 m y n tales que $d = ma + nb$. Suponiendo que $a_{k+1} = 0$ y $a_k = mcd(a, b)$, tomaremos $m_0 = 1$, $m_1 = 0$, $n_0 = 0$ y $n_1 = 1$. Hallamos m_i y n_i, para $i \geq 2$, del modo siguiente:*

$$m_i = m_{i-2} - m_{i-1}q_{i-1} \ , \ n_i = n_{i-2} - n_{i-1}q_{i-1}.$$

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

$$a_i = m_i \cdot a + n_i \cdot b.$$

En particular,

$$a_k = m_k \cdot a + n_k \cdot b.$$

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

i	a_i	q_i	m_i	n_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 $1 = 4 * 250 + (-9) * 111$.

Corolario 2. *$1 = ma + nb$ si, y sólo si, $mcd(a, b) = 1$.*

Corolario 3.

- *Si $mcd(a, b) = mcd(a, c) = 1$, entonces $mcd(a, bc) = 1$*
- *Si $mcd(a, b) = 1$, entonces $mcd(a^2, b^2) = 1$.*

Demostración. Es claro que $1 = ma + nb = ka + lc$, con lo que $1 = 1 * 1 = (ma + nb) * (ka + lc) = (mka + nkb + lmc) * a + (nl) * bc$ y se concluye que $1 = mcd(a, bc)$. El segundo apartado es consecuencia del primero. □

Corolario 4. *Para cualesquiera enteros a, b y $k \neq 0$, se tiene que:*

$$mcd(ka, kb) =\mid k \mid mcd(a, b)$$

y, si $d > 0$, entonces:

$$d = mcd(a, b) \Leftrightarrow d \mid a \ , \ d \mid b \ y \ mcd(\frac{a}{d}, \frac{b}{d}) = 1.$$

3.4. Números primos. Factorización

Definición 43. *Sea $n \in \mathbb{N}$ un número natural. Una factorización de n es cualquier descomposición $n = ab$ 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 26. I) *Los primeros 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 44. *Los números enteros $a_1, a_2, \ldots, a_n$ son* primos entre sí *si $mcd(a_1, \ldots, a_n) = 1$.*

Lema 3. (Lema de Euclides) *Si $a \mid bc$ y $mcd(a, b) = 1$, entonces $a \mid c$.*

Demostración. Se tiene que existe un entero k tal que $bc = ak$ y enteros m, n tales que $1 = ma+nb$, con lo que $c = mca+nbc = mca+nak = a(mc+nk)$, es decir $a \mid c$. □

Corolario 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 $p \mid b$*

Demostración. Veamos que 1) $\Rightarrow$ 2). Sea p un primo que divide a ab y sea $d = mcd(a, p)$. Como $d \mid p$, se tiene que $d = 1$ o $d = p$. Si $d = 1$, la conclusión se deduce del Lema de Euclides y, en el segundo caso, $p \mid a$.

Recíprocamente, si $p = ab$ (con a y b que podemos tomar naturales) y suponemos 2), tendremos que $p \mid a$ o $p \mid b$. Como $a \mid p$ y $b \mid p$, se sigue que $p = a$ y $b = 1$ o $p = b$ y $a = 1$. □

Ejemplo 27. *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,* $mcd(a, b) \neq 1$.

Corolario 6. *Si* p *es primo y* $p \mid \prod_{i=1}^{n} a_i$ *para* $a_1, \ldots, a_n \in \mathbb{Z}$, *se tiene que* $p \mid a_i$, *para algún* i.

Demostración. Basta aplicar el corolario anterior y el método de inducción. □

Corolario 7. *Si* p *es primo y* $p \mid \prod_{i=1}^{n} q_i$ *para* $q_1, \ldots, q_n \in \mathbb{Z}$ *números primos, se tiene que* $p = q_i$, *para algún* i.

Demostración. El corolario anterior permite deducir que $p \mid q_i$, para algún i y, dado que q_i es primo $p = q_i$. □

Teorema 4. 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* $n = \pm p_1 p_2 \cdots p_r$ *con* $p_1 \leq p_2 \leq \ldots \leq p_r$. *La descomposición 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.

Queda claro, pues, que cualquier entero n admite una única descomposición

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

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

Ejemplo 28. $10800 = 2 \times 5400 = 2^2 \times 2700 = \cdots = 2^4 \times 675 = \cdots = 2^4 3^3 5^2$

El siguiente resultado se debe a Euclides:

Teorema 5. *Existen infinitos primos distintos.*

Demostración. Supongamos que $p_1, \ldots, p_r$ fuesen todos los primos y consideremos $m = p_1 \cdots p_r + 1$. El teorema anterior garantiza que existen $q_1, \ldots, q_s$ primos tales que $m = q_1 \cdots q_s$. Cada q_i divide a m y, por lo tanto, no puede ser ningún p_i, con lo cual llegamos a una contradicción.[5] □

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

Teorema 6. (Criba de Eratóstenes) *Sea a un número entero mayor que 1. Si, para todo primo $p \leq \sqrt{a}$, se tiene que $p \nmid a$, entonces a es primo*[6].

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 29. *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

Definición 45. *Dados dos enteros a, b, se dice que m es el* mínimo común múltiplo *de a y b ($mcm(a, b)$) si m es el menor entero positivo que es múltiplo de ambos*[7]*. Si $m = mcm(a, b)$, se tiene que:*

- *$a \mid m$ y $b \mid m$*
- *Si $c > 0$ es tal que $a \mid c$ y $b \mid c$, entonces $m \mid c$.*

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

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

[5] Es claro que $m \equiv_{p_i} 1$ (para todo i) y $m \equiv_{q_j} 0$ (para todo j).

[6] Si existe primo q tal que el cociente de la división de x entre q es menor o igual que q y ningún primo p menor que q es divisor de x, entonces x es primo.

[7] Si a es cualquier entero, entenderemos que $mcm(a, 0) = 0$

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

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

Teorema 7. *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) $mcd(a,b)mcm(a,b) =\mid ab \mid$

Demostración. Se sigue de la definición y de que:

$$min(\alpha_i, \beta_i) + max(\alpha_i, \beta_i) = \alpha_i + \beta_i.$$

□

3.5. Ecuaciones diofánticas

Se puede decir que la ecuaciones diofánticas son una amplia clase de ecuaciones algebraicas (polinómicas) con más de una incógnita en el conjunto de los números enteros.

Comencemos con las ecuaciones diofánticas lineales $ax + by = n$.

Teorema 8. *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 $a = a'd$ y $b = b'd$, para ciertos enteros a', b', se tiene que

$$n = a'dx_0 + b'dy_0 = d(a'x_0 + b'y_0)$$

y, por lo tanto, $d \mid n$. Recíprocamente, si $n = n'd$, entonces, dado que el Teorema de Bezout garantiza la existencia de x_0, y_0 tales que $ax_0 + by_0 = d$, tenenemos que $n'x_0$ y $n'y_0$ son una posible solución de la ecuación diofántica. □

Veamos como se obtienen las demás soluciones.

Teorema 9. *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 4 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 30. *Hallense las soluciones de* $20x + 50y = 430$.

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

$$10 = 20 * (-2) + 50 * 1$$

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.*

Pasemos ahora a las ecuaciones del tipo $x^2 - y^2 = n$.

Teorema 10. *La ecuación* $x^2 - y^2 = n$ *admite solución si, y sólo si,* n *se puede factorizar como* $n = ab$ *siendo* a *y* b *de la misma paridad. En este caso, la solución viene dada por*

$$x_0 = \frac{a + b}{2} \ , \ y_0 = \frac{a - b}{2}.$$

Demostración. Si la ecuación admite solución, se tiene que $n = (x+y)(x-y)$. Si llamamos $a = x + y$ y $b = x - y$, es claro que $a + b = 2x$, es decir a y b son ambos pares o ambos impares. Inversamente, si a y b tienen la misma paridad, basta tomar como soluciones las indicadas en el enunciado del teorema. □

Nota 8. *Para encontrar la soluciones de la ecuación* $x^2 - y^2 = n$*, podemos tomar* n *positivo, ya que,* $-n = y^2 - x^2$*. Además, dado que, para cualquier entero* x*, se tiene que* $x^2 = (-x)^2$*, consideraremos, únicamente las soluciones positivas.*

Ejemplo 31. *Resolver la ecuación* $x^2 - y^2 = 435$.

Dado que $435 = 3*5*29$*, se tiene que las posibles factorizaciones* $435 = ab$ *con* a *y* b *de la misma paridad son:*

- $a = 435$ *y* $b = 1$*, con lo que* $x = 218$*,* $y = 217$

- $a = 145$ *y* $b = 3$*, con lo que* $x = 74$*,* $y = 71$
- $a = 87$ *y* $b = 5$*, con lo que* $x = 46$*,* $y = 41$
- $a = 29$ *y* $b = 15$*, con lo que* $x = 22$*,* $y = 7$*.*

El teorema anterior permite obtener un algoritmo para el reconocimiento de números primos. En efecto, sea n un número natural impar. Supongamos que no es primo, es decir, admite una factorización $n = ab$, con $1 < b \leq a$ y a y b ambos impares. Entonces, decidir si n es compuesto equivale a determinar si la ecuación $x^2 - y^2 = n$ admite solución. Puesto que

$$x^2 \geq x^2 - y^2 = n,$$

podemos suponer que el conjunto $H = \{x \ ; \ x^2 \geq n\}$ es no vacío. Sea entonces $q = min(H)$. Basta tomar $m \geq q$ y analizar si $m^2 - n$ es un cuadrado perfecto. Si existe algún m con esas condiciones, n no es primo y, en caso contrario, n sería primo. Además, este proceso es finito, ya que:

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2.$$

Basta tomar, entonces $q \leq m < \frac{n+1}{2}$. Este método se denomina **Algoritmo de factorización de Fermat** y lo podríamos esquematizar como:

- Calcula q tal que $q^2 \geq n$ y $(q-1)^2 < n$.
- Tomamos m tal que $q \leq m < (n+1)/2$. Entonces:
  - Si $m^2 - n = x^2$, para algún valor de m y algún entero x, n no es primo puesto que $n = (m+x)(m-x)$.
  - Si $m^2 - n \neq x^2$, para todo valor de m y todo entero x, n es primo.

Ejemplo 32. *Decidir si* 527 *es o no un número primo.*

Empecemos viendo quién es el menor entero positivo q *tal que* $q^2 \geq 527$*.* q *es* 23 *ya que* $22^2 = 484$ *y* $23^2 = 529$*. Puesto que* $23^2 - 527 = 2$*, probamos con* 24 *y vemos que* $24^2 - 527 = 576 - 527 = 49 = 7^2$*, con lo que:*

$$527 = (24+7) * (24-7) = 31 * 17$$

y 527 *no es primo.*

El último tipo de ecuaciones diofánticas a considerar son las ecuaciones pitagóricas $x^2 + y^2 = z^2$, siendo x, y, z números naturales. Son pues los catetos y la hipotenusa de un triángulo rectángulo.

Teorema 11. *La soluciones de la ecuación $x^2 + y^2 = z^2$ verificando que x, y, z son naturales, $mcd(x, y, z) = 1$ y x es par, vienen dadas por:*

$$\begin{cases} x = 2st \\ y = s^2 - t^2 \\ z = s^2 + t^2 \end{cases}$$

siendo s, t naturales de distinta paridad, $s > t$ y $mcd(s, t) = 1$. Estas soluciones se llaman ternas pitagóricas primitivas.

Las primeras ternas pitagóricas son:

s	t	x	y	z
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41

Fermat (1601-1665) abordó el problema más general de encontrar las soluciones enteras de $x^n + y^n = z^n$ con $n \geq 3$. Fermat concluyó que la ecuación anterior no tenía soluciones naturales y, en uno de sus escritos, afirma que posee una demostración maravillosa de ese hecho que, lamentablemente, el margen de tal escrito no podía contener, por lo que nunca se supo cuál era la demostración de Fermat.

La búsqueda de una demostración correcta de la llamada **Conjetura de Fermat** ha jugado un papel importantísimo en el desarrollo de las Matemáticas. Sólo, entre 1908 y 1912, aparecieron más de 1000 "demostraciones" todas incorrectas.

En el año 1993, Andrew Wiles (Universidad de Princeton) afirmó, durante un seminario celebrado en Oxford, que poseía una prueba de la citada conjetura. Tras algunos cambios en esa demostración y una cuidadosa revisión de la misma, fue publicada en el artículo "Modular elliptic curves and Fermat's Last Teorema" en la revista Annals of Mathematics, volumen 141, páginas 443-551 en el año 1995. Lo que sí probó Fermat fue su conjetura para $n = 4$.

3.6. Congruencias

Definición 46. *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:*

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

Ejemplo 33. $7 \equiv_3 4$ *y* $18 \equiv_2 6$.

Teorema 12. *Cada entero a es congruente módulo m con uno de los enteros* $\{0, 1, \ldots, m-1\}$.

Demostración Si dividimos a entre m, obtenemos:

$$a = m.q + r$$

con $0 \leq r < m$.□

Teorema 13. *Sean a y b dos números enteros. Se verifica que $a \equiv_m b$ si, y sólo si, el resto obtenido al dividir a y b entre m es el mismo.*

Demostración Es claro que si $a = m.q+r$ y $b = m.q'+r$ con $0 \leq r < m$, entonces

$$a - b = m(q - q')$$

y $a \equiv_m b$. Por otro lado, si $a - b = m.q$ y $b = m.q' + r$ con $0 \leq r < m$, entonces:

$$a = m(q + q') + r.\square$$

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

1) $a \equiv_m a$ (Reflexiva)

2) Si $a \equiv_m b$, entonces $b \equiv_m a$ (Simétrica)

3) Si $a \equiv_m b$ y $b \equiv_m c$, entonces $a \equiv_m c$ (Transitiva)

4) Si $a \equiv_m b$ y $c \equiv_m d$, entonces

$$a + c \equiv_m b + d$$

$$ac \equiv_m bd$$

5) Si $a \equiv_m b$, entonces $ha \equiv_m hb$

6) Si $ah \equiv_m bh$ y $m.c.d.(h, m) = 1$, entonces[8]

$$a \equiv_m b$$

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

Demostración

4) Si $a - b = mt$ y $c - d = mt'$, entonces

$$a + c = b + d + mt + mt'$$

$$ac = (b + mt)(d + mt') = bd + mtd + mt'b + m^2tt'$$

5) Sólo hay que tener en cuenta la propiedad anterior y que $h \equiv_m h$, para cualquier h.

6) Puesto que $a = ha'$ y $b = hb'$, se tiene que

$$h(a' - b') = mt$$

y como h y m son primos entre si, entonces $m|(a' - b')$, es decir

$$a' - b' = mt$$

Corolario 8. *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 34. *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:

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

El resto de la división es 4.

Teorema 14. *La ecuación* $ax \equiv_m b$ *tiene solución entera si, y sólo si, d = m.c.d.(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 cuando $d = m.c.d.(a, m)$ 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

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

Ejemplo 35. *Encontrar todas las soluciones no congruentes de* $9x \equiv_{15} 6$.

Como $m.c.d.(9, 15) = 3$ *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* $4 + 10 = 14$.

Teorema 15. (Teorema Chino del Resto.) *El sistema de congruencias*

$$x \equiv_{m_i} b_i, i = 1, 2, \ldots k$$

con $m.c.d.(m_i, m_j) = 1$ *para cada* $1 \leq i < j \leq k$*, tiene una única solución módulo* $m = m_1 m_2 \ldots m_k$ *y las demás soluciones son de la forma* $x = x_0 + \lambda m_1 m_2 \ldots m_k$*, donde* $\lambda \in \mathbb{Z}$.

Demostración. Para cada $i = 1, 2, \ldots, k$, sea $t_i = \frac{m}{m_i}$ y sea y_i la única solución módulo m_i que admite la ecuación:

$$t_i y \equiv_{m_i} 1$$

ya que $m.c.d.(t_i, m_i) = 1$. Sea entonces

$$x_0 = y_1 t_1 b_1 + \cdots + y_k t_k b_k$$

y veamos que x_0 es solución del sistema de congruencias. Sea $i = 1, 2, \ldots, k$; es claro que

$$x_0 = y_i t_i b_i + \sum_{j \neq i} y_j t_j b_j \equiv_{m_i} b_i$$

porque $t_i y_i \equiv_{m_i} 1$ y $t_j \equiv_{m_i} 0$ si $j \neq i$.

Supongamos que x_1 y x_2 son dos soluciones del sistema de congruencias, entonces:

$$x_1 \equiv_{m_i} x_2, i = 1, 2, \ldots, k$$

es decir que $m_i | (x_1 - x_2)$ para cada i. Así pues, $m.c.m(m_1, m_2, \ldots, m_k) = m_1 m_2 \ldots m_k | (x_1 - x_2)$.

Por último, observemos que, si $\lambda \in \mathbb{Z}$, entonces $x_0 + \lambda m$ es solución del sistema de congruencias.

Nota 9. *Si alguna de las ecuaciones de un sistema de congruencias es de la forma $a_j x \equiv_{m_j} c_j$, tendremos que resolverla para hallar los posibles valores $0 \leq b_j < m_j$ tales que $x \equiv_{m_j} b_j$. Para cada uno de ellos, habrá una única solución del sistema módulo m.*

Ejemplo 36. *Resolver el sistema de congruencias:*

$$\begin{aligned} 2x &\equiv_8 6 \\ 3x &\equiv_5 2 \\ x &\equiv_3 1 \end{aligned}$$

La primera ecuación tiene dos soluciones, por ello $x \equiv_8 3$ o $x \equiv_8 7$. Para la segunda, la única opción es $x \equiv_5 4$. Así pués tenemos dos posibilidades, aunque la mayoría de los cálculos sirven para ambas. Siguiendo la notación del Teorema Chino, tenemos que $m = 120$, $t_1 = 15$, $t_2 = 24$ y $t_3 = 40$. Las soluciones de $t_i y \equiv_{m_i} 1$ para $i = 1, 2, 3$, son $y_1 = 7$, $y_2 = 4$ y $y_3 = 1$. Las soluciones posibles son:

- **Opción 1:** $b_1 = 3$, $b_2 = 4$, $b_3 = 1$.

  En este caso,

  $$x_0 = 3 \cdot 15 \cdot 7 + 4 \cdot 24 \cdot 4 + 1 \cdot 40 \cdot 1 = 739.$$

  Las restantes soluciones son $x = 739 + \lambda \cdot 120 = 19 + \lambda \cdot 120$.

- **Opción 2:** $b_1 = 7$, $b_2 = 4$, $b_3 = 1$.

  En este caso,

  $$x_0 = 7 \cdot 15 \cdot 7 + 4 \cdot 24 \cdot 4 + 1 \cdot 40 \cdot 1 = 1159.$$

  Las restantes soluciones son $x = 1159 + \lambda \cdot 120 = 79 + \lambda \cdot 120$.

Definición 47. *Dado un número natural* m*, se designa por* $\phi(m)$ *al número de enteros positivos* r *que no exceden a* m *y son primos con* m*. Su expresión es:*

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

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 10. *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* $m.c.d.(n, p^r) = 1$*, 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 11. *Si* m *y* n *son dos naturales primos entre sí, se tiene que*

$$\phi(mn) = \phi(m)\phi(n).$$

Para demostrarlo, consideremos los conjuntos:

$$A = \{1 \leq a \leq m \ ; \ mcd(a, m) = 1\}$$
$$B = \{1 \leq b \leq n \ ; \ mcd(b, n) = 1\}$$
$$C = \{1 \leq c \leq mn \ ; \ mcd(c, mn) = 1\}$$

y utilicemos la aplicación:

$$f : C \to A \times B$$

definida por $f(c) = (a, b)$*, donde* $c \equiv_m a$ *y* $c \equiv_n b$*. Puesto que* f *es biyectiva, los conjuntos han de tener el mismo cardinal y se deduce el resultado. El carácter inyectivo de* f *es consecuencia de que es imposible encontrar dos elementos distintos en* C *que sean congruentes módulo* mn*. El carácter sobreyectivo también se deduce del Teorema Chino.*

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:

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

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 16. Teorema de Euler *Sean* a *y* m *dos números enteros con* $m \geq 1$*; entonces si* $m.c.d.(a, m) = 1$*, 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

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

se tiene que

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

y, como $m.c.d.(8, 1 \cdot 3 \cdot 5 \cdot 7) = 1$, entonces:

$$11^4 \equiv_8 1$$

Teorema 17. *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 $m.c.d.(a,p) = 1$ y $\phi(p) = p - 1$.□

Ejemplo 37. *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*

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

Teorema 18. Teorema de Wilson *Si p es un número primo, entonces*

$$(p-1)! \equiv_p -1$$

En realidad como $p - 1 \equiv_p -1$, basta probar que

$$(p-2)! \equiv_p 1.$$

Tomemos, por ejemplo, $p = 11$. Puesto que

$$2 \cdot 6 \equiv_{11} 1\ ,\ 3 \cdot 4 \equiv_{11} 1, 5 \cdot 9 \equiv_{11} 1 \text{ y } 7 \cdot 8 \equiv_{11} 1$$

se tiene que

$$9! \equiv_{11} 1$$

Ejemplo 38. *Encuentrese el resto de la división de* 15! *entre 17.*

Por el Teorema de Wilson, se tiene que

$$16! \equiv_{17} -1 \equiv_{17} 16$$

Como $16! = 16 \cdot 15!$ *y* $m.c.d.(16, 17) = 1$*, concluimos que*

$$15! \equiv_{17} 1$$

3.7. Introducción a la Criptografía

`Criptografía: Kryptos: escondido + graphein = escritura.`

El objetivo de la criptografía no es ocultar la existencia de un mensaje, sino la de ocultar su significado mediante un proceso conocido como encriptación.

La criptografía "clásica" puede dividirse en dos ramas: trasposición y substitución. En una trasposición, las letras del mensaje se colocan de otra manera. Por ejemplo: 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

Mientras en la trasposición cada letra mantiene su identidad pero cambia de posición, en la substitución cada letra cambia su identidad, pero mantiene su posición.

Por ejemplo, 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 O P Q R S T U V W X Y Z
D E F G H I J K L M N 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: YHQL, YLGL, YLFL

Podrá haber 25 cifras de este tipo, pero también podría haberse elegido cualquier ordenación de las letras del alfabeto, lo que daría más de 4×10^{26} cifras distintas.

Los árabes, además de utilizar cifras del tipo anterior, también fueron capaces de destruirlas. De hecho, fueron ellos los que inventaron el *criptoanálisis*, la ciencia que consiste en descifrar un mensaje sin conocer la clave. Durante la segunda guerra mundial, los descifradores inventaron un artefacto de descodificación, el Colossus, que determinaría el desarrollo de la criptografía

durante la segunda mitad del siglo XX. Después de la guerra, los criptoanalistas continuaron desarrollando y usando la tecnología de los ordenadores para descifrar todo tipo de cifras. La unión de criptografía y criptoanálisis constituye la *criptología*, que se ha desarrollado mediante una lucha continua entre criptógrafos y criptoanalistas, saldándose este duelo la mayor parte de las veces, con la victoria de los segundos.

Sin embargo, podemos decir que el cambio de perspectiva se produjo cuando Diffie y Hellman descubrieron en 1976 la criptografía de clave pública, sentando las bases de la criptografía moderna. Los objetivos más importantes de ésta 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 (Firma Digital).
- **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 afirmar que el mensaje no 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.

Hasta finales de los años 70, se utilizaron los llamados *criptosistemas de clave simétrica*, que se basaban en el uso de una clave secreta que A y B compartían (sobre la que debían ponerse de acuerdo antes de comenzar el proceso) y que se usaba tanto para cifrar como para descifrar. De este modo, si la clave que comparten A y B es k, cuando A quiere enviar a B un mensaje m utiliza una función f_k y B recibe $s = f_k(m)$. Entonces B utiliza la clave para descifrar el mensaje y recupera m, haciendo $f_k^{-1}(s) = (f_k^{-1} \circ f_k)(m) = m$. Es claro que este sistema plantea el problema de poder distribuir de manera segura las claves que se van a utilizar.

La idea de basar los criptosistemas en problemas matemáticos difíciles y, no sólo en el ingenio, iba a ser clave en el desarrollo de un nuevo tipo de criptografía, la llamada *criptografía asimétrica*, con la cual se alcanzan en un nivel mucho más satisfactorio los objetivos señalados anteriormente. Concretamente, lo que Diffie y Hellman proponen es utilizar funciones de dirección única $f : X \to Y$, 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.[9]

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 $s = f_{k_B^1}(m)$. Al recibir el mensaje, B utiliza su clave privada para descifrar s y recupera m haciendo $m = f_{k_B^2}(s)$. Está claro que debe verificarse que $f_{k_B^2} \circ f_{k_B^1}$ debe ser igual a la 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 (anillos de restos módulo n) y de las curvas elíticas sobre cuerpos (fundamentalmente finitos).

Esta idea es la misma que la que se usa en la la llamada *firma digital*. En este caso, si A quiere enviarle un mensaje m a B, entonces primero lo firma con su clave privada y construye $s = f_{k_A^2}(m)$, a continuación lo encripta con la clave pública de B, obteniendo $c = f_{k_B^1}(s)$ que es el mensaje que recibe B. B lo desencripta, primero con su clave privada y recupera $s = f_{k_B^2}(c)$ que le resulta ininteligible. Finalmente, hace uso de la clave pública de A y obtiene $m = f_{k_A^1}(s)$.[10] Nótese que ahora necesitamos, además que $f_{k_A^1} \circ f_{k_A^2}$ sea igual a la identidad

Rivest, Shamir y Adleman (RSA) encontraron en 1977 una función de una sola vía basada en funciones modulares:

i) Para elegir su clave personal, una persona A escoge dos números primos p y q suficientemente grandes [11], y que debe mantener en secreto. Calcula $n = pq$. Por simplicidad, supongamos que $p = 17$ y $q = 11$, en ese caso $n = 187$.

ii) Después, A elige otro número e, que debe ser primo con $\phi(n) = (p-1)(q-1)$, es decir:

$$mcd(e, \phi(n)) = 1$$

[9] Hay que añadir que, en realidad, lo que se van a utilizar son funciones de dirección única con trampa, es decir, el receptor dispondrá de una información adicional que le permite obtener $f^{-1}(y)$.

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

[11] Aproximadamente del mismo tamaño pero no demasiado próximos para que $p - q$ no proporcione información suficiente para el cálculo de $pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$

Supongamos que escoge $e = 7$. A hace públicos los números n y e en algo similar a una guía de teléfonos. (n, e) es la clave pública y son los datos necesarios para la encriptación.[12]

III) Para encriptar el mensaje, primero hay que convertirlo en un número, m. Por ejemplo, una palabra se cambia en dígitos binarios ASCII, y los dígitos binarios pueden ser considerados como un número decimal. Luego m se encripta para producir el texto cifrado, C, según la fórmula

$$C \equiv_n m^e.$$

IV) Las potencias en aritmética modular son funciones de una sola vía, por lo que es difícil invertir los cálculos partiendo de C y recuperar el mensaje original, m. Por ello, un tercer individuo no puede descifrar el mensaje.

V) Sin embargo, A descifra el mensaje porque tiene una información especial: conoce los valores de p y q. Calcula un número especial, d, que forma parte de su clave privada junto con $\phi(n)$. El número d se calcula utilizando el algoritmo de Euclides como:

$$e \times d \equiv_{\phi(n)} 1$$

que existe[13] puesto que $mcd(e, \phi(n)) = 1$.

VI) Para descifrar el mensaje, A utiliza la siguiente fórmula:

$$m \equiv_n C^d$$

En realidad, el siguiente resultado es el que prueba que las dos funciones anteriores son inversas.

Corolario 9. *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 $e \cdot d \equiv_{\phi(n)} 1$.

[12] El número e puede figurar en la clave pública de otra persona, pero n debe tener un valor distinto para cada individuo.

[13] El Teorema de Bezout garantiza la existencia de d y k tales que $d \cdot e + \phi(n) \cdot k = 1$

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. □

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.

Ejemplo 39. (Ejercicio 42.4 de Scheinerman) *Para traducir nuestro 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`*. La palabra* `CASA` *se traduce como* 30122001*.*

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*		

Supongamos que la clave pública RSA de Roberto es

$$(n, e) = (328419349, 220037467).$$

(Además, Roberto sabe que $\phi(n) = 328366764$ *y, en consecuencia, que* $d = 119923$*). Alicia encripta una palabra* M *para Roberto y este recibe* $N = 43853517$ *¿Quién es* M*?*

Roberto desencripta N haciendo:

$$N^d \equiv_n 43853517^{119923}$$
$$\equiv_n (43853517^{50000})^2 43853517^{19923} \equiv_n$$
$$(133807774)^2 \cdot 281712138 \equiv_n 300145477 \cdot 281712138$$
$$\equiv_n 126220401$$

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) y, además 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 tambien 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.

3.8. Sistemas de Numeración

En la vida ordinaria, el sistema de numeración que se utiliza 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:

$$12354 = 1 * 10^4 + 2 * 10^3 + 3 * 10^2 + 5 * 10 + 4$$

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). 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 cualquiera.

Ejemplo 40. *Escribamos* 45 *en base* 2, 3 *y* 4.

$$45 = 32 + 8 + 4 + 1 = 2^5 + 2^3 + 2^2 + 2^0$$
$$45 = 27 + 18 = 3^3 + 2 \times 3^2$$
$$45 = 2 \times 4^2 + 3 \times 4 + 4^0$$

Teorema 19. *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 algún* $a_i \neq 0$. *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 41. *Escribir* 277 *en base* 2.

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*

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

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

Cuando $b > 10$, habrá a_i mayores que 10. Se suele tomar entonces $A = 10, B = 11, C = 12$, etc. Por ejemplo, $B5C4_{(16} = B \times 16^3 + 5 \times 16^2 + C \times 16 + 4 = 46 \cdot 532$.

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 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 de tres 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:

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

3.8.1. 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 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 $a_0 - a_1 + a_2 - a_3 + \cdots$.