Capítulo 1

Congruencias

1.1. El algoritmo de Euclides

Notación básica. Los números primos. La identidad de Bezout. Fracciones continuas y $\mathrm{SL}_2(\mathbb{Z})$.

De forma vaga y rápida, la teoría de números podría describirse como la rama de las matemáticas que se ocupa de las propiedades de los *números enteros*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\},$$

los cuales constituyen una extensión sencilla de los *números naturales*

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \dots\}$$

que, salvo el cero que a veces se excluye, conforman una abstracción matemática presente desde los albores de la humanidad y que los niños interiorizan desde edades muy tempranas. Desde el punto de vista algebraico, la extensión de $\mathbb{N}$ a $\mathbb{Z}$ se hace para que no solo sea posible efectuar siempre sumas sino también restas, lo que en el plano económico permite representar deudas. La multiplicación en $\mathbb{N}$, que es una suma abreviada, pasa también a $\mathbb{Z}$ con una regla de signos que todos aprendimos en nuestra etapa escolar. La división, como inversa de la multiplicación, no es siempre posible en $\mathbb{Z}$ y negarse a superar este obstáculo con los *números racionales* $\mathbb{Q}$ da lugar a una infinidad de problemas sobre la divisibilidad de enteros de interés en teoría de números, algunos con literalmente siglos de antigüedad.

Si $m, n \in \mathbb{Z}$, la notación $m \mid n$ indica que n es divisible por m, en el sentido de que m multiplicado por un entero da n, es decir, que n es un *múltiplo* de m o, equivalentemente, que m es un *divisor* de n. En fórmulas:

$$m \mid n \quad \Longleftrightarrow \quad \exists k \in \mathbb{Z} \,:\, mk = n.$$

La ausencia de divisibilidad se indica con $m \nmid n$. Si nos acogemos a la letra de la definición, $0 \nmid m$ para $m \in \mathbb{Z} - \{0\}$, lo cual no llama demasiado la

atención porque siempre nos han prohibido dividir por cero, sin embargo se cumple $0 \mid 0$, que suena tan raro que rara vez se ve escrito.

Otra notación relacionada con la divisibilidad es la de las *congruencias*. Se dice que a y b son *congruentes* módulo m si $m \mid a-b$, donde hay que tener en cuenta que "|" tiene menor precedencia que las operaciones elementales, es decir, significa $m \mid (a-b)$. Prácticamente todos los autores limitan las congruencias a $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$ y emplean la notación $a \equiv b \pmod{m}$, sin el acento en el ámbito internacional, a veces abreviada como $a \equiv b\ (m)$, que preferiremos aquí. En resumen, para $a, b, m \in \mathbb{Z}$ con $m > 0$

$$a \equiv b\ (m) \quad \Longleftrightarrow \quad \exists k \in \mathbb{Z} : a = b + km.$$

Las congruencias están estrechamente ligadas a la división con resto. Dados $a \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$, a base de sumar o restar m a a repetidas veces, obtenemos $a - cm = r$ con $c \in \mathbb{Z}$ y $0 \leq r < m$. Al entero c se le llama *cociente* y a r *resto*. Es fácil ver que están únicamente determinados. Se tiene $a \equiv r\ (m)$ y por tanto decir que dos números son congruentes es lo mismo que decir que dejan el mismo resto al ser divididos por m. Por ejemplo, $2023 \equiv 0\ (7)$, $2023 \equiv 9\ (19)$ y $2023 \equiv 28\ (19)$.

Dentro de la teoría de números y en relación con la divisibilidad, los grandes protagonistas son los *números primos*. Estos son los enteros $p \in \mathbb{Z}_{>1}$ tales que $m \nmid p$ para $1 < m < p$. Los primeros números primos son:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, \ldots$$

En un contexto moderno más avanzado es conveniente considerar también que sus negativos son números primos, aunque no lo haremos aquí. Una curiosidad es que antiguamente se incluía el 1 entre los primos, en contra de lo que se hace hoy en día.

Hay muchas demostraciones de la infinitud de los números primos. La más conocida, con más de dos milenios de antigüedad, se atribuye a Euclides de Alejandría [15, IX, Pr.20], [11, §2.4] y seguro que el lector la conoce. No la recordaremos.

Uno de los pilares de la teoría de números es la descomposición única en primos. Tal es así, que a este resultado se le llama teorema fundamental de la aritmética. Seguramente, a muchos les parezca que es trivial. A fin de cuentas, por definición, los primos son los que no se pueden descomponer más entonces dado un número basta descomponerlo repetidamente hasta que ya no sea posible hacerlo. Este argumento no es suficiente en lo relativo a la unicidad. Parece evidente que si un primo está contenido, por decirlo de alguna manera, en un producto, entonces lo está en al menos uno de los factores. Sin embargo, ejemplos más avanzados muestran qué esto pudiera fallar en contextos más amplios y que estamos usando alguna propiedad no trivial de la divisibilidad. Hay un ejemplo elemental debido a D. Hilbert

que puede ofrecer algo de luz: Si cambiamos $\mathbb{N}$ por los elementos de una progresión aritmética $H = \{5, 9, 13, 17, 21, \dots\}$ y decretamos que los primos en H son los que admiten descomposición en H, entonces 33, 57, 77 y 133 son primos y 4389 tiene varias descomposiciones, como $57 \cdot 77$ y $33 \cdot 133$.

En el tratamiento moderno, y también en el original de Euclides [15, VII], es importante introducir un sencillo algoritmo iterativo llamado *algoritmo de Euclides* que consiste en aplicar sucesivamente

$$r_{n-1} = c_{n-1} r_n + r_{n+1} \qquad \text{para} \quad n \geq 1 \tag{1.1}$$

partiendo de $r_0 = a$, $r_1 = b \in \mathbb{Z}^+$ y donde c_{n-1} y r_{n-2} son, respectivamente, el cociente y el resto al dividir r_{n-1} entre r_n. El algoritmo termina cuando $r_{n+1} = 0$ (ya que no podríamos dividir por cero), lo cual se cumple a la larga porque $r_n > r_{n+1} \geq 0$.

Para relacionar varios temas del curso y abreviar algunas pruebas vamos a proceder de una manera no muy convencional, escribiendo la recurrencia (1.1) del algoritmo matricialmente como

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} c_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix}.$$

Al iterar se obtiene

$$\begin{pmatrix} a \\ b \end{pmatrix} = A_n \begin{pmatrix} r_{n+1} \\ r_{n+2} \end{pmatrix} \quad \text{con} \quad A_n = \begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix}. \tag{1.2}$$

Para conectar el algoritmo de Euclides con la divisibilidad, necesitamos una definición básica. Dados $a, b \in \mathbb{Z}$ no simultáneamente nulos, su *máximo común divisor* D es, como su nombre sugiere, el mayor $D \in \mathbb{Z}^+$ tal que $D \mid a$ y $D \mid b$. Las notaciones más comunes son $D = \gcd(a, b)$, por g*reatest* c*ommon* d*ivisor*, y $D = (a, b)$. Si $\gcd(a, b) = 1$ se dice que a y b son *coprimos* o *primos entre sí*.

Teorema 1.1.1. *Sean $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ y $D = \gcd(a, b)$. Si r_N es el último resto no nulo en el algoritmo de Euclides, entonces $r_N = D$. Además existen $x, y \in \mathbb{Z}$ tales que se verifica la* identidad de Bezout

$$ax + by = D \qquad \textit{con} \quad D = \gcd(a, b).$$

Cambiando a y x por $-a$ y $-x$ la identidad e Bezout queda invariante y tampoco tiene ningún efecto intercambiar a y b al mismo tiempo que x e y, por ello las precauciones con los signos son innecesarias.

▶ **Corolario 1.1.2.** *Si $a, b \in \mathbb{Z}$ no son simultáneamente nulos entonces existen $x, y \in \mathbb{Z}$ tales que $ax + by = \gcd(a, b)$.*

Corolario 1.1.3. *Para $a, b \in \mathbb{Z}$ no simultáneamente nulos, cualquier divisor común de a y b también divide a $\gcd(a, b)$.*

Este corolario es tan significativo en el desarrollo básico de la teoría que a menudo se incluye como hipótesis en la definición del máximo común divisor y se hace necesario un resultado de existencia.

Incidiendo sobre el tema de los signos, la restricción $b \in \mathbb{Z}$ impuesta en el algoritmo de Euclides no es una limitación seria para calcular el máximo común divisor porque $\gcd(a,0) = |a|$ y $\gcd(a,b) = \gcd(a,-b)$, de hecho $\gcd(\pm a, \pm b) = \gcd(|a|,|b|)$ para cualquier combinación de los signos.

Por ejemplo, el cálculo de $\gcd(-24,10)$ se reduce al de $\gcd(24,10)$, aunque nada impide aplicar directamente el algoritmo de Euclides con a negativo. Los cálculos en este caso serían:

$$\begin{array}{rcccl} n=1 & \to & -24 = (-3)\cdot 10 + 6 & \to & c_0 = -3,\ r_2 = 6 \\ n=2 & \to & 10 = 1\cdot 6 + 4 & \to & c_1 = 1,\ r_3 = 4 \\ n=3 & \to & 6 = 1\cdot 4 + 2 & \to & c_2 = 1,\ r_4 = 2 \\ N=n=4 & \to & 4 = 2\cdot 2 + 0 & \to & c_3 = 2,\ r_5 = 0 \end{array}$$

Aunque el ejemplo anterior sugiera que hallar $\gcd(a,b)$ con el algoritmo de Euclides es innecesariamente enrevesado, porque todos reconoceríamos a simple vista 2 como el mayor divisor común de -24 y 10 imaginando sus factorizaciones, esta es una falsa impresión cuando salimos del ámbito de los números pequeños. En realidad, el algoritmo de Euclides es muy eficiente desde el punto de vista computacional y constituye la base de muchos métodos en criptografía. Se puede probar que el número de pasos que requiere el algoritmo de Euclides dividido por el número de cifras de mín$(|a|,|b|)$ está acotado por una constante no muy grande. De esta forma, con el *software* adecuado, calcular el máximo común divisor de dos números de miles de cifras requiere un tiempo insignificante, a escala humana, usando un ordenador.

Demostración del Teorema 1.1.1. Aplicando (1.2) con $n = N-1$ se tiene $(a,b)^t = A(r_N,0)^t$ con $A = A_{N-1}$. Claramente, $\det A = \pm 1$, por tanto $B = A^{-1}$ es también un matriz entera. De $a = a_{11}r_N$, $b = a_{21}r_N$ se deduce que r_N es divisor común de a y b, entonces $r_N \le D$. Por otro lado, premultiplicando por B, $ax + by = r_N$ con $x = b_{11}$, $y = b_{12}$, de donde $D \mid r_N$ y se concluye $r_N = D$. □

Calcular A_n efectuando el producto de matrices de la forma habitual resulta un tedioso. Hay una forma rápida de proceder que llamaremos *algoritmo de la fracción continua*. Se parte de los vectores (columna) de la base canónica $\vec{e}_2$ y $\vec{e}_1$, se sitúa c_0 sobre $\vec{e}_1$ y se calcula $c_0\vec{e}_1 + \vec{e}_2$, que es $(c_0,1)^t$, para obtener una tercera columna a la derecha. Sobre ella se sitúa ahora c_1 y se repite el procedimiento hasta acabar los c_j. En un esquema:

	c_0	c_1	c_2	$\dots$	c_{N-1}	
0	1	c_0	c_0c_1+1	$\dots$	$\dots$	$\dots$
1	0	1	c_1	$\dots$	$\dots$	$\dots$

Lema 1.1.4. *Sea A_n como en (1.2). La primera columna de A_n coincide con la $n+3$ en el algoritmo de la fracción continua y la segunda con la $n+2$.*

Demostración. Basta aplicar inducción empleando que

$$A_n = A_{n-1}\begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \bar{a_{11}}c_n + \bar{a_{12}} & \bar{a_{11}} \\ \bar{a_{21}}c_n + \bar{a_{22}} & \bar{a_{21}} \end{pmatrix}$$

donde $\bar{a_{ij}}$ indican los elementos de A_{n-1}. □

Como ejemplo, tomemos el algoritmo de Euclides aplicado a $a = -24$, $b = 10$ que da $c_0 = -3$, $c_1 = c_2 = 1$, $c_3 = 2$. El algoritmo de la fracción continua sería

	-3	1	1	2	
0	1	-3	-2	-5	-12
1	0	1	1	2	5

Según el Lema 1.1.4, tenemos

$$A_0 = \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix},\ A_1 = \begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix},\ A_2 = \begin{pmatrix} -5 & -2 \\ 2 & 1 \end{pmatrix},\ A_3 = \begin{pmatrix} -12 & -5 \\ 5 & 2 \end{pmatrix}.$$

En la prueba del Teorema 1.1.1, x e y se obtenían a través de la matriz A_{N-1} por eso no debe extrañarnos que el algoritmo de la fracción continua constituya un método rápido para hallarlos.

Proposición 1.1.5. *Si c_1 y c_2 son los elementos de la penúltima columna del algoritmo de la fracción continua, entonces o bien $(x, y) = (c_2, -c_1)$ o bien $(x, y) = (-c_2, c_1)$ verifica $ax + by = \gcd(a, b)$.*

Demostración. Al tomar $n = N - 1$ en (1.2) con r_N es el último resto no nulo del algoritmo de Euclides, se sigue que la primera columna de A_{N-1} viene dada por a/D y b/D. Usando que $\det A_{N-1} = \pm 1$ y el Lema 1.1.4, se deduce el resultado. □

En el ejemplo anterior, tendríamos que decidir entre $(x, y) = (2, 5)$ y $(x, y) = (-2, -5)$. Claramente es el primero el que cumple $-24x + 10y = 2$.

Veamos otro ejemplo completo sin apelar a resultados anteriores. Supongamos que queremos hallar $x, y \in \mathbb{Z}$ con $34x + 25y = 1$. El algoritmo de Euclides para 34 y 25, que son coprimos, es

$$\begin{aligned} 34 &= 1 \cdot 25 + 9 \quad \to \quad c_0 = 1, \\ 25 &= 2 \cdot 9 + 7 \quad \to \quad c_1 = 2, \\ 9 &= 1 \cdot 7 + 2 \quad \to \quad c_2 = 1, \\ 7 &= 3 \cdot 2 + 1 \quad \to \quad c_3 = 3, \\ 2 &= 2 \cdot 1 + 0 \quad \to \quad c_4 = 2. \end{aligned}$$

El algoritmo de la fracción continua para estos cocientes c_j es

	1	2	1	3	2	
0	1	1	3	4	15	34
1	0	1	2	3	11	25

Por tanto una solución es $(11, -15)$ o su negativa. En este caso, es esta última, $(x, y) = (-11, 15)$.

Muchas veces se acompaña la definición del máximo común divisor con la del *mínimo común múltiplo* denotado con $\operatorname{lcm}(a, b)$, por l*east* c*ommon* m*ultiple*, o con $[a, b]$. La fórmula

$$\operatorname{lcm}(a, b) = \frac{|ab|}{\gcd(a, b)}$$

puede tomarse como definición y es un ejercicio comprobar que es coherente con su nombre siendo el menor entero positivo que es múltiplo de a y b simultáneamente. Además, en analogía con el Corolario 1.1.3, cualquier otro múltiplo común es múltiplo de $\operatorname{lcm}(a, b)$.

Por otro lado, de manera inductiva, las definiciones de máximo común divisor y mínimo común múltiplo se extienden a un número mayor de argumentos mediante

$$\gcd(a_1, a_2 \ldots, a_n) = \gcd\big(a_1, \gcd(a_2, \ldots, a_n)\big)$$

y

$$\operatorname{lcm}(a_1, a_2 \ldots, a_n) = \operatorname{lcm}\big(a_1, \operatorname{lcm}(a_2, \ldots, a_n)\big).$$

Estas fórmulas pueden colapsar si algunos a_j son nulos, porque no hemos definido $\gcd(0, 0)$. A pesar de que esto rara vez aparece en la práctica, el convenio natural para evitar problemas es que los argumentos nulos se pueden eliminar de gcd y que en lcm un solo argumento nulo provoca que el resultado sea cero.

Una consecuencia del Teorema 1.1.1 es la descomposición única en primos. Su participación en la prueba es a través del siguiente resultado auxiliar que tiene interés por sí mismo.

Lema 1.1.6. *Sean $a, b, c \in \mathbb{Z}$ con a y b coprimos. Si $a \mid bc$ entonces $a \mid c$.*

Demostración. Por el Teorema 1.1.1, $ax + by = 1$ para ciertos $a, b \in \mathbb{Z}$, por tanto $a\big(cx + \frac{bc}{a}y\big) = c$ y se concluye $a \mid c$. □

Teorema 1.1.7 (Teorema fundamental de la aritmética)**.** *Cada $n > 1$ entero se puede descomponer de forma única como*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad con \quad \alpha_j \in \mathbb{Z}^+$$

y $p_1 < \cdots < p_k$ primos.

A pesar de que el Lema 1.1.6 tiene su antecedente en los famosos *Elementos* de Euclides [15, VII.30] y están los ingredientes de la unicidad, allí no se encuentra un enunciado similar al Teorema 1.1.7. Por alguna razón, Euclides no consideró destacarlo.

Demostración. La existencia de la descomposición es sencilla por inducción. Si n es primo (en particular para $n = 2$), se tiene la descomposición trivial con $k = 1$ y si no lo es, $n = n_1 n_2$ con $1 < n_1 < n$, $1 < n_2 < n$ y se aplica la hipótesis de inducción a cada n_j.

Para la unicidad, supongamos $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$ con $q_1 < \cdots < q_\ell$ y $\beta_j \in \mathbb{Z}^+$. Si $p_1 \nmid q_j^{\beta_j}$ para todo $1 \leq j \leq \ell$ se tendría una contradicción con el Lema 1.1.6 porque un primo es coprimo con cualquier número al que no divide. Por tanto $p_1 \mid q_j^{\beta_j}$ para cierto j. De nuevo el Lema 1.1.6 lleva a una contradicción si $p_1 \nmid q_j$ y, como q_j es primo, $p_1 = q_j$. Repitiendo este argumento, $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_\ell\}$, en particular $k = \ell$, y la ordenación implica $p_j = q_j$. Si $\alpha_j \neq \beta_j$ dividiendo por $p_j^{\min(\alpha_j, \beta_j)}$ se obtiene una identidad incompatible con que los conjuntos de los primos son iguales. □

Una vez que tenemos el Teorema 1.1.7, es fácil ver que si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$ entonces $\gcd(n, m) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$ y $\operatorname{lcm}(n, m) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)}$ y que estas igualdades siguen siendo válidas incluso si admitimos que algunos α_j o β_j sean nulos. La conclusión es que es posible calcular $\gcd(n, m)$ y $\operatorname{lcm}(n, m)$ factorizando. Esto no suele ser lo más adecuado para números grandes. Por ejemplo, si $n = 2^{32} + 40$ y $m = 2^{32} + 1$ la factorización de estos números nos llevaría a un esfuerzo computacional considerable, sin embargo, un paso del algoritmo de Euclides nos dice $\gcd(n, m) = \gcd(n, 39)$ y un ejercicio con congruencias, que $n \equiv 39\ (23)$, así pues, n y m son coprimos.

Se llama *ecuación diofántica* a cualquiera en la que solo permitimos soluciones enteras (a veces, por extensión, también racionales). Una aplicación del Teorema 1.1.1 es una extensión del Corolario 1.1.3, la solución general de las ecuaciones diofánticas lineales. Cualquiera que haya oído hablar del *último teorema de Fermat* no se asombrará de que para grados superiores entramos en una teoría muy complicada [6].

Proposición 1.1.8. *Sean $a, b, c \in \mathbb{Z} - \{0\}$. La ecuación*

$$ax + by = c$$

tiene solución $x, y \in \mathbb{Z}$ si y solo si $D = \gcd(a, b)$ divide a c. En ese caso, hay infinitas soluciones parametrizadas por

$$x = \frac{cx_0 + bt}{D}, \quad y = \frac{cy_0 - at}{D} \qquad con \quad t \in \mathbb{Z}$$

donde x_0 e y_0 son enteros fijados cualesquiera que cumplen $ax_0 + by_0 = D$.

Demostración. Si $D \nmid c$, claramente $ax + by = c$ lleva a una contradicción y si $D \mid c$ la parametrización anterior produce enteros que, sustituyendo, satisfacen la ecuación. Basta probar que no hay más soluciones. Si $x', y' \in \mathbb{Z}$ cumplen $ax' + by' = c$ entonces, restando $ax + by = c$ y operando un poco,

$$\frac{b}{D}\Big(\frac{cy_0}{D} - y'\Big) = \frac{a}{D}\Big(x' - \frac{cx_0}{D}\Big).$$

Como a/D y b/D son coprimos, el Lema 1.1.6 implica $tb/D = x' - cx_0/D$ para $t \in \mathbb{Z}$ y de ahí, $cy_0/D - y' = ta/D$. □

En un ejemplo anterior habíamos visto que $(x_0, y_0) = (-11, 15)$ era solución de $34x + 25y = 1$, con ello podemos concluir que todas las soluciones de $34x + 25y = 3$ vienen dadas por

$$x = -33 + 25t, \qquad y = 45 - 34t.$$

Una cosa curiosa es que si $a, b \in \mathbb{Z}^+$ son coprimos, para cualquier $c > ab - a - b$ siempre existe alguna solución no negativa, $x, y \in \mathbb{Z}_{\geq 0}$. Por ejemplo, $34x + 25y = 2023$ lleva a la parametrización de las soluciones enteras

$$x = -22253 + 25t, \qquad y = 30345 - 34t.$$

La no negatividad obliga a que $t \geq 890{,}12$ y $t \leq 892{,}5$ y solo hay dos posibilidades, $t = 891$ y $t = 892$ que dan las soluciones $(22, 51)$ y $(47, 17)$.

Hay una relación estrecha entre el algoritmo de Euclides y otros dos temas que aparecerán en el curso. El primero son las *fracciones continuas* finitas. Estas son expresiones del tipo

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{}{a_{k-1} + \cfrac{1}{a_k}}}}} \qquad \text{con} \quad a_0 \in \mathbb{Z} \quad \text{y} \quad a_j \in \mathbb{Z}^+,\ j > 0.$$

Para abreviar, la notación moderna es $[a_0, a_1, \ldots, a_k]$, a veces sutituyendo la primera coma por un punto y coma para resaltar que a_0 se mueve en rango diferente al resto.

El siguiente resultado nos dice que cualquier fracción irreducible se expresa como una fracción continua finita. Seguimos el convenio habitual por el que se considera que las fracciones irreducibles siempre tienen denominador positivo.

Teorema 1.1.9. *Sea $a/b \in \mathbb{Q}$ una fracción irreducible. Se cumple*

$$\frac{a}{b} = [c_0, c_1, \ldots, c_{N-1}]$$

donde c_j y N son como en el algoritmo de Euclides (1.1) *aplicado a a y b.*

Demostración. La ecuación (1.1) que define el algoritmo de Euclides se reescribe como

$$\frac{r_{n-1}}{r_n} = c_{n-1} + \frac{1}{r_n/r_{n+1}}$$

y basta aplicarla repetidas veces partiendo de $n = 1$ hasta $n = N$. □

Comparando (1.2) y el Lema 1.1.4, sabremos por qué hemos llamado al algoritmo de la fracción continua de esa forma.

Corolario 1.1.10. *Con la notación del Teorema 1.1.9, al aplicar el algoritmo de la fracción continua a c_0, c_1,..., c_{N-1}, se obtienen como columnas, a partir de la tercera, el numerador y el denominador de $[c_0]$, $[c_0, c_1]$,..., $[c_0, \ldots, c_{N-1}] = a/b$.*

Por ejemplo, el algoritmo de Euclides aplicado a 18 y 7 es

$$18 = 2 \cdot 7 + 4, \qquad 7 = 1 \cdot 4 + 3, \qquad 4 = 1 \cdot 3 + 1, \qquad 3 = 3 \cdot 1 + 0.$$

Por tanto $c_0 = 2$, $c_1 = c_2 = 1$, $c_3 = 3$ y se cumple

$$\frac{18}{7} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}} = [2, 1, 1, 3].$$

Con el algoritmo de la fracción continua se tiene

		2	1	1	3	
0	1	2	3	5	18	
1	0	1	1	2	7	

$$\Rightarrow \quad \begin{array}{ll} [2] = 2/1, & [2,1] = 3/1, \\ [2,1,1] = 5/2, & [2,1,1,3] = 18/7. \end{array}$$

La otra aplicación del algoritmo de Euclides está relacionada con el grupo

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ M \in \mathcal{M}_{2\times 2}(\mathbb{Z}) \,:\, \det M = 1 \right\}$$

que es de gran relevancia en la teoría de números actual por su relación con las *formas modulares*. Dos elementos destacados de $\mathrm{SL}_2(\mathbb{Z})$ son la *traslación* T y la *inversión* S dadas por

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{y} \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

La razón de estos curiosos nombres aparecerá en otro capítulo.

Teorema 1.1.11. *Se tiene* $\mathrm{SL}_2(\mathbb{Z}) = \langle T, S \rangle$.

Recuérdese que, según la notación habitual de teoría de grupos, $\langle T, S\rangle$ es el grupo generado por T y S. La prueba será completamente constructiva, ofreciendo para cada $M \in \mathrm{SL}_2(\mathbb{Z})$ una expresión en términos de T y S basada en el algoritmo de Euclides que podríamos programar fácilmente en un ordenador.

No hay unicidad al expresar un elemento de $\mathrm{SL}_2(\mathbb{Z})$ como producto de potencias de T y S, incluso eliminando $S^4 = I$, porque existen relaciones entre T y S que derivan de $TSTST = S$ (véase [42, §1.2] para obtener unicidad en cierto sentido). Se puede probar que $\mathrm{SL}_2(\mathbb{Z})$ es isomorfo a $\langle x, y \,|\, x^4 = e,\, x^2 = y^3\rangle$ por medio de $S \mapsto x$ e $TS \mapsto y$.

Demostración. Sean

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \qquad \text{y} \qquad U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Tenemos que expresar M en términos de T y S, para ello nos valdremos de U en cálculos intermedios. En varias ocasiones utilizaremos que $S^2 = -I$, la opuesta de la matriz identidad, y que T^k es lo mismo que T cambiando t_{12} por k.

Si $c = 0$ las únicas posibilidades son $a = d = 1$ que corresponde a $M = T^b$ y $a = d = -1$ que corresponde a $M = T^{-b}S^2$.

Si $c \neq 0$, multiplicando por S^2 siempre podemos suponer $c \in \mathbb{Z}^+$. Claramente, $\det M = 1$ implica que a y c son coprimos. Unos cálculos muestran que se cumplen las relaciones matriciales:

$$\begin{pmatrix} c_j & 1 \\ 1 & 0 \end{pmatrix} = T^{c_j}U \qquad \text{y} \qquad UT^{c_j}U = -ST^{-c_j}S.$$

Si el algoritmo de Euclides aplicado a a y c acaba en $r_N = \gcd(a, c) = 1$, entonces por (1.2) y el Lema 1.1.4, teniendo en cuenta la primera relación matricial,

$$A_{N-1} = T^{c_0}UT^{c_1}UT^{c_2}UT^{c_3}U \cdots T^{c_{N-1}}U = \begin{pmatrix} a & b_- \\ c & d_- \end{pmatrix}$$

donde (b_-, d_-) es la penúltima columna del algoritmo de la fracción continua. Si N es par, la segunda relación matricial aplicada a j impar nos da

$$(-1)^{N/2}T^{c_0}ST^{-c_1}ST^{c_2}ST^{-c_3}S \cdots T^{(-1)^{N-1}c_{N-1}}S = A_{N-1}$$

y si N es impar, posmultiplicando además por $US = \mathrm{diag}(1, -1)$, se tiene lo mismo salvo que la segunda columna de A_{N-1} se cambia de signo y el factor inicial es $(-1)^{(N-1)/2}$. En definitiva,

$$S^{\lfloor N/2\rfloor}T^{c_0}ST^{-c_1}ST^{c_2}ST^{-c_3}S \cdots T^{(-1)^{N-1}c_{N-1}}S = \begin{pmatrix} a & b_0 \\ c & d_0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

donde $(b_0, d_0) = \pm(b_-, d_-)$, eligiendo el signo para que el determinante sea 1.

Por la Proposición 1.1.8, necesariamente $b = b_0 + at$ y $d = d_0 + ct$, de modo que posmultiplicando por T^t se obtiene M en términos de T y S. □

Siguiendo los pasos de la prueba, expresemos

$$M = \begin{pmatrix} 18 & -31 \\ 7 & -12 \end{pmatrix}$$

como producto de potencias de T y S. Sabíamos de un ejercicio anterior que al aplicar el algoritmo de Euclides a 18 y 7 se tenía $c_0 = 2$, $c_1 = c_2 = 1$, $c_3 = 3$, así que consideramos

$$T^2UTUTUT^3U = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix}$$

donde el último cálculo se ha hecho con el algoritmo de la fracción continua. Podemos reemplazar $UT^{c_j}U$ por $-ST^{c_j}S$, así pues

$$T^2ST^{-1}STST^{-3}S = \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix}.$$

Para ajustar la última columna, posmultiplicamos por T^{-2} y así se obtiene

$$M = T^2ST^{-1}STST^{-3}ST^{-2}.$$

Nótese que procediendo de esta forma el número de factores que resultan es aproximadamente el doble de los pasos que requiere el algoritmo de Euclides.

1.2. El anillo de clases de congruencias

La estructura de anillo. La función φ. El teorema chino del resto. Las congruencias de Euler-Fermat y de Wilson. Raíces primitivas.

En el marco de las estructuras algebraicas, $\mathbb{Z}$ tiene estructura de anillo conmutativo con unidad cuando se consideran la suma y el producto habituales. Dado un entero m, el conjunto de múltiplos de m, que indicaremos con $m\mathbb{Z}$, es un *ideal* de este anillo. Es decir, es un subgrupo respecto a la suma y es imposible salirse de él multiplicando por elementos del anillo. Según la teoría general [47, §3.5], el conjunto cociente $\mathbb{Z}/m\mathbb{Z}$ hereda la estructura de anillo. Notando que $m\mathbb{Z} = (-m)\mathbb{Z}$ y escapando de los ideales impropios $\{0\}$ y $\mathbb{Z}$, que dan cocientes triviales, es natural restringirse a $m > 1$.

Este cociente tiene una interpretación en términos de congruencias porque $a \equiv b\ (m)$ equivale a $a - b \in m\mathbb{Z}$. Entonces $\mathbb{Z}/m\mathbb{Z}$ es lo mismo que identificar cada entero con su *clase de congruencia*, el conjunto de los que son