

Capítulo 2

Fundamentos esenciales

En este apartado, se tiene como objetivo presentar las definiciones y conceptos importantes para presentar de manera comprensible el capítulo de teoría trascendental de números. Por lo cual, los siguientes temas serán tratados de manera breve y no pretenden presentar un material exhaustivo de cada área, únicamente los resultados indispensables para este trabajo. Para un estudio más elaborado de estas áreas, se recomienda ampliamente los libros de Teoría de números [4], [16], [11], Álgebra [14], Análisis [1] y Variable compleja [8].

2.1 Teoría de números

Principio de Dirichlet: Sean m, n dos números naturales distintos de 0. Si se desean colocar n palomas en m cajas con $n > m$, alguna caja debe contener al menos $n + 1$ palomas.

Principio del buen orden: En cualquier conjunto de números naturales $A \subset \mathbb{N}$ distinto del conjunto vacío, $A \neq \emptyset$, existe un mínimo, es decir, un número $n \in A$ tal que $n \leq a$ para todo $a \in A$.

2.1.1 Divisibilidad

Si bien los conceptos de divisibilidad son comúnmente conocidos en el conjunto de los números enteros, en realidad, las siguientes propiedades son válidas en otros conjuntos. Aunque no se demostrará explícitamente, los siguientes resultados son válidos para polinomios con coeficientes en algún campo. Como referencia, recomendamos [14, Cap. 3, Sec. 9].

Teorema 2.1.1 (Algoritmo de la división). Dados $a, b \in \mathbb{Z}$ tal que $b > 0$, existen enteros únicos q y r que satisfacen

$$a = qb + r \quad 0 \leq r < b$$

Demostración. Primero, definamos el conjunto

$$S = \{a - xb \mid x \in \mathbb{Z}, \quad a - xb \geq 0\}$$

Veamos que el conjunto es no vacío. Como el entero $b \geq 1$, entonces $|a|b > |a|$ y así,

$$u = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$$

Es decir, $u \in S$. Por el Principio del buen orden, existe el entero más pequeño en S , sea ése entero r . Por definición de S , existe un entero q que satisface

$$r = a - qb \quad 0 \leq r$$

Supongamos que $r \geq b$, entonces $r - b \geq 0$, así,

$$a - (q + 1)b = (a - qb) - b = r - b \geq 0$$

Entonces $a - (q + 1)b \in S$ y además, $a - (q + 1)b = r - b < r$, lo cual contradice que r sea el entero más pequeño contenido en S . Esto implica que $r < b$. Entonces, existen enteros q y r que satisfacen

$$a = qb + r \quad 0 \leq r < b$$

Veamos que q y r son únicos. Supongamos que existe otra representación de la misma forma, es decir,

$$a = qb + r = q'b + r' \quad 0 \leq r < b \quad 0 \leq r' < b$$

Entonces $r' - r = b(q - q')$ y como $b > 0$

$$|r' - r| = |b(q - q')| = |b||q - q'| = b|q - q'|$$

Sumando las desigualdades $-b < -r \leq 0$ y $0 \leq r' < b$ obtenemos que $-b < r' - r < b$, de manera equivalente, $|r' - r| < b$. Así, $b|q - q'| < b$. Por lo cual,

$$0 \leq |q - q'| < 1$$

Entonces $|q - q'|$ es un entero no negativo menor a 1, por lo cual, la única posibilidad es que $|q - q'| = 0$. Por lo tanto, $q = q' \Rightarrow r = r'$, lo cual concluye la demostración. ■

Definición 2.1.1. Un entero b se dice que es divisible por un entero $a \neq 0$, en símbolos se representa como $a|b$, si existe un entero $c \neq 0$ tal que $b = ac$. Escribimos $a \nmid b$ para indicar que b no es divisible por a .

Las siguientes proposiciones son en realidad propiedades de la división, en particular, la más utilizada y de mayor interés es la proposición 2.1.5.

Proposición 2.1.1. Sea a un entero, entonces $a|0$, $1|a$, $a|a$.

Demostración: Claramente $0 = a \cdot 0$, $a = 1 \cdot a$ y $a = a \cdot 1$, por definición $a|0$, $1|a$ y $a|a$ respectivamente. ■

Proposición 2.1.2. Sean a, b, c, d enteros. Si $a|b$ y $c|d$, entonces $ac|bd$.

Demostración: Como $b = am$ para alguna m y $d = cn$ para alguna n , entonces multiplicando ambas expresiones $bd = amcn = (ac)mn$, por lo tanto, $ac|bd$. ■

Proposición 2.1.3. Sean a, b, c enteros. Si $a|b$ y $b|c$, entonces $a|c$.

Demostración: Como $b = am$ para alguna m y $c = bn$ para alguna n , entonces $c = (am)n = (a)mn$, por lo tanto, $a|c$. ■

Proposición 2.1.4. Sean a, b enteros. Si $a|b$ con $b \neq 0$, entonces $|a| \leq |b|$.

Demostración. Como $a|b$, entonces existe un entero $c \neq 0$ tal que $b = ac$. Por la Definición 2.1.1, $a \neq 0$. Claramente $|\frac{b}{a}| = |c| \geq 1$, por lo tanto, $|\frac{b}{a}| \geq 1$, así $|\frac{b}{a}| = \frac{|b|}{|a|} \geq 1$ finalmente $|b| \geq |a|$. ■

Proposición 2.1.5. Sean a, b, c enteros. Si $a|b$ y $a|c$ entonces a divide a cualquier combinación lineal de b y c , es decir, $a|bx + cy$ para cualesquiera enteros x, y .

Demostración. Como $b = am$ para alguna m , entonces $bx = amx$, entonces $a|bx$, análogamente $cy = any$, por lo tanto, $bx + cy = amx + any = a(mx + ny)$, como $mx + ny$ es un entero, entonces $a|bx + cy$. ■

Ahora, veremos un concepto que tiene mucha relevancia no solamente para los números enteros, si no también para los polinomios, aunque de nuevo, no lo demostraremos explícitamente.

Definición 2.1.2. Definimos el máximo común divisor entre dos enteros a, b como el entero d que satisface:

- $d|a, d|b$
- Si $c|a$ y $c|b$, entonces $c \leq d$.

Se denota $d = (a, b)$

Teorema 2.1.2. Sean enteros a, b , con al menos uno no nulo, entonces existen enteros r, s tales que el máximo común divisor se puede escribir como combinación lineal de a y b , es decir:

$$d = (a, b) = ar + bs$$

Demostración. Consideremos el conjunto S de todas las posibles combinaciones lineales de a y b :

$$S = \{au + bv : au + bv > 0 \quad u, v \in \mathbb{Z}\}$$

Claramente este conjunto es no vacío, pues si $u, v = 1$ entonces $a + b \in S$. Por el principio del buen orden, S debe contener un elemento mínimo d . Por lo tanto, por definición de S , $d = ar + bs$. Afirmamos que $d = (a, b)$. Por el algoritmo de la división, $a = dq + r$ con $0 \leq r < d$, entonces

$$r = a - dq = a - (ar + bs)q = a - arq - bsq = a(1 - rq) + b(-sq)$$

Por lo tanto, si r es un entero positivo entonces $r \in S$ con $r < d$, lo cual contradice la elección de d , así, $r = 0$. Con ello concluimos que $a = dq$, es decir, $d|a$, análogamente $d|b$. Supongamos que existe $c|a$ y $c|b$. Por la Proposición 2.1.5 $c|ax + by$ para cualesquiera enteros x, y , en particular, $c|d$. Por la Proposición 2.1.4, $c \leq d$. Por definición, d es el máximo común divisor entre a y b . Lo cual concluye la demostración. ■

Definición 2.1.3. Decimos que a y b son primos relativos si $(a, b) = 1$.

Teorema 2.1.3. Si a y b son primos relativos, entonces existen enteros r, s tales que el número 1 se puede escribir como combinación lineal de a y b , es decir:

$$1 = ar + bs$$

La demostración es una consecuencia directa del Teorema 2.1.2.

Lema 2.1.1 (Lema de Euclides). Si $a|bc$ tal que $(a, b) = 1$, entonces $a|c$.

Demostración. Como $(a, b) = 1$, entonces existen enteros r, s tales que $1 = ar + bs$. Multiplicando por c , $c = arc + bcs$, como $a|bc$, entonces existe algún entero q tal que $bc = aq$, por lo tanto, $c = arc + aqs = a(rc + qs)$, por lo tanto, $a|c$. ■

2.1.2 Congruencias

Definición 2.1.4. Decimos que $a \equiv b \pmod{m}$ si y solo si $m|a - b$.

En palabras, se lee a es congruente con b módulo m si y solo si m divide a $a - b$. Utilizar esta notación tiene muchos beneficios, en primer lugar, se puede demostrar que $\equiv$ es una relación de equivalencia, lo que permite simplificar muchos resultados en teoría de números. Veremos solamente algunas de sus propiedades.

Proposición 2.1.6. Sea $m > 1$ y a un entero. Entonces $a \equiv a \pmod{m}$.

Demostración: Claramente $m|a - a$, ya que $m|0$, por lo tanto, $a \equiv a \pmod{m}$. ■

Proposición 2.1.7. Sea $m > 1$, a y b enteros. Si $a \equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$.

Demostración: Como $a \equiv b \pmod{m}$, entonces $a - b = m \cdot q$, por lo tanto, $b - a = m \cdot (-q)$, por lo tanto, $m|b - a$. ■

Proposición 2.1.8. Sea $m > 1$, a, b, c enteros. Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$.

Demostración: Como $a - b = mq_1$ y $b - c = mq_2$, entonces sumando ambas ecuaciones $a - c = mq_1 + mq_2 = m(q_1 + q_2)$, por lo tanto, $m|a - c$. ■

Por supuesto, estas últimas tres proposiciones son suficientes para concluir que $\equiv$ es una relación de equivalencia. Las siguientes proposiciones son resultados difíciles de obtener sin la estructura que proporcionan las congruencias, es decir, no son evidentes.

Proposición 2.1.9. Sean a, b, c, d enteros y $m > 1$. Si $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, entonces $a + c \equiv b + d \pmod{m}$ y $ac \equiv bd \pmod{m}$.

Demostración: Como $a - b = mq_1$ y $c - d = mq_2$, entonces sumando ambas expresiones $a + c - (b + d) = m(q_1 + q_2)$, por lo tanto, $m|(a + c) - (b + d)$. Por otro lado, $ac = (mq_1 + b)(mq_2 + d) = bd + mq_1mq_2 + bmq_2 + dmq_1$, entonces $ac - bd = m(q_1q_2m + b + d)$ con $q_1q_2m + b + d \in \mathbb{Z}$, por lo tanto, $m|ac - bd$. ■

Proposición 2.1.10. Sean a, b, c enteros y $m > 1$. Si $a \equiv b \pmod{m}$, entonces $a + c \equiv b + c \pmod{m}$ y $ac \equiv bc \pmod{m}$.

Demostración: Como $a - b = mq$, entonces $a + c - (b + c) = mq$, es decir, $m|(a + c) - (b + c)$. Además, $c(a - b) = mqc$, por lo tanto, $m|ac - bc$. ■

Proposición 2.1.11. Sean a, b enteros. Si $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$ para cualquier entero positivo k .

Demostración: Por la Proposición 2.1.9 y usando $c = a$, $d = b$, entonces $a^2 \equiv b^2 \pmod{m}$ y se puede probar por inducción que $a^k \equiv b^k \pmod{m}$ para $k \in \mathbb{Z}$. ■

2.1.3 Fracciones continuas

Definición 2.1.5. Una fracción continua, es una expresión de la forma:

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}$$

Y se denota como $[a_0, a_1, a_2, \dots]$. A los números a_j se les conoce como los cocientes parciales.

Definición 2.1.6. Definimos a $[a_0, a_1, \dots, a_n]$ como el enésimo **convergente** de $[a_0, a_1, a_2, \dots]$. Es decir, es el resultado de la siguiente fracción continua:

$$\frac{p_n}{q_n} = [a_0, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_{n-1} + \frac{1}{a_n}}}}}$$

Donde $(p_n, q_n) = 1$. Y a los números $x_n = [a_n, a_{n+1}, \dots]$ se les conoce como cocientes completos.

Teorema 2.1.4. Sea $[a_0, a_1, \dots]$ una fracción continua. Entonces, afirmamos que:

- $p_n = a_n p_{n-1} + p_{n-2}$
- $q_n = a_n q_{n-1} + q_{n-2}$

Donde $p_{-1} = 1$ y $q_{-1} = 0$.

Demostración. Procedemos por inducción. Para $n = 1$, donde claramente $p_0 = a_0$ y $q_0 = 1$.

$$\begin{aligned} [a_0, a_1] &= a_0 + \frac{1}{a_1} \\ &= \frac{a_0 a_1 + 1}{a_1} \end{aligned}$$

Como se requería. Supongamos que el teorema es válido para n . Por lo tanto, observemos lo siguiente para utilizar la hipótesis de inducción:

$$\begin{aligned} [a_0, \dots, a_{n+1}] &= [a_0, \dots, a_{n-1}, a_n + \frac{1}{a_{n+1}}] \\ &= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \\ &= \frac{a_{n+1} a_n p_{n-1} + p_{n-1} + a_{n+1} p_{n-2}}{a_{n+1} a_n q_{n-1} + q_{n-1} + a_{n+1} q_{n-2}} \\ &= \frac{a_{n+1} (a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1} (a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_{n-1} + q_{n-1}} \\ &= \frac{p_{n+1}}{q_{n+1}} \end{aligned}$$

Lo cual finaliza la inducción. ■

Lema 2.1.2. Las siguientes relaciones se cumplen:

1. $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$
2. $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$

Demostración. Veamos la primera parte, utilizando el Teorema 2.1.4:

$$\begin{aligned}
 p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1} (a_n q_{n-1} + q_{n-2}) \\
 &= p_{n-2} q_{n-1} + a_n p_{n-1} q_{n-1} - a_n p_{n-1} q_{n-1} - p_{n-1} q_{n-2} \\
 &= (-1)(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\
 &\vdots \\
 &= (-1)^n (p_0 q_{-1} - p_{-1} q_0) \\
 &= (-1)^n (-1) \\
 &= (-1)^{n-1}
 \end{aligned}$$

Análogamente, y utilizando lo anterior,

$$\begin{aligned}
 p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2} (a_n q_{n-1} + q_{n-2}) \\
 &= p_{n-2} q_{n-2} + a_n p_{n-1} q_{n-2} - a_n p_{n-2} q_{n-1} - p_{n-2} q_{n-2} \\
 &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\
 &= (-1)^n a_n
 \end{aligned}$$

■

Definición 2.1.7. Sea α un número real. Para $m = 0, 1, 2, \dots$ definimos el siguiente algoritmo recursivo como sigue:

- $\alpha_0 = \alpha$
- $a_m = \lfloor \alpha_m \rfloor$ donde $\lfloor x \rfloor$ representa la función piso.
- $\alpha_m = a_m + \frac{1}{\alpha_m + 1}$

Observemos que dada esta definición, para un entero positivo m , se cumple que $\alpha = [a_0, a_1, \dots, a_{m-1}, \alpha_m]$ (se sigue de expandir $\alpha = \alpha_0$). Por lo cual, se justifica que se pueda aproximar cualquier número real a partir de las fracciones continuas.

Teorema 2.1.5. Sea α un número irracional y $\frac{p_n}{q_n}$ sea un convergente de su fracción continua. Por lo tanto,

$$\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{q_n (\alpha_{n+1} q_n + q_{n-1})}$$

Demostración. Sea n un entero positivo. Entonces, $\alpha = [a_0, a_1, \dots, a_n, \alpha_{n+1}]$. Entonces, utilizando el Teorema 2.1.4 y el Lema 2.1.2,

$$\begin{aligned}
 \alpha - \frac{p_n}{q_n} &= \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \\
 &= \frac{p_{n-1}q_n + \alpha_{n+1}p_nq_n - \alpha_{n+1}p_nq_n - p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})} \\
 &= \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})} \\
 &= \frac{(-1)(p_nq_{n-1} - q_n p_{n-1})}{q_n(\alpha_{n+1}q_n + q_{n-1})} \\
 &= \frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}
 \end{aligned}$$

■

Corolario 2.1.1. Sea α un número real con $\frac{p_n}{q_n}$ convergente en su fracción continua. Entonces,

$$|q_n\alpha - p_n| < |q_{n-1}\alpha - p_{n-1}|$$

Demostración. Por el Teorema 2.1.5, tenemos que:

$$|q_n\alpha - p_n| = \frac{1}{q_n\alpha_{n+1} + q_{n-1}}$$

Análogamente,

$$|q_{n-1}\alpha - p_{n-1}| = \frac{1}{q_{n-1}\alpha_n + q_{n-2}}$$

Por lo cual, es suficiente probar la siguiente desigualdad,

$$\frac{1}{q_n\alpha_{n+1} + q_{n-1}} < \frac{1}{q_{n-1}\alpha_n + q_{n-2}} \quad (2.1)$$

Notemos que:

$$\begin{aligned}
 \frac{1}{q_{n-1}\alpha_n + q_{n-2}} &= \frac{1}{q_{n-1}(a_n + \frac{1}{\alpha_{n+1}}) + q_{n-2}} \\
 &= \frac{1}{q_{n-1}a_n + \frac{q_{n-1}}{\alpha_{n+1}} + q_{n-2}} \\
 &= \frac{\alpha_{n+1}}{q_{n-1}a_n\alpha_{n+1} + q_{n-1} + q_{n-2}\alpha_{n+1}}
 \end{aligned}$$

Por lo tanto, se cumple la ecuación (2.1) si y solo si,

$$\begin{aligned} q_{n-1}a_n\alpha_{n+1} + q_{n-1} + \alpha_{n+1}q_{n-2} &< q_n\alpha_{n+1}^2 + q_{n-1}\alpha_{n+1} \iff \\ \alpha_{n+1}(q_{n-1}a_n + q_{n-2}) + q_{n-1} &< q_n\alpha_{n+1}^2 + q_{n-1}\alpha_{n+1} \iff \\ q_n\alpha_{n+1} + q_{n-1} &< \alpha_{n+1}(q_n\alpha_{n+1} + q_{n-1}) \iff \\ 1 &< \alpha_{n+1} \end{aligned}$$

Notemos que $\frac{1}{\alpha_{n+1}} = \alpha_n - [\alpha_n]$, por lo cual, $\frac{1}{\alpha_{n+1}} < 1$, por lo tanto, $\alpha_{n+1} > 1$, lo cual concluye la demostración. ■

Corolario 2.1.2. Sea α un número real, $\frac{p_n}{q_n}$ un convergente en la fracción continua de α , entonces,

$$\frac{1}{(a_{n+1} + 2)q_n^2} < \left| \alpha - \frac{p_n}{q_n} \right|$$

Demostración. Argumentamos que

$$a_{n+1} + 2 - \alpha_{n+1} > \frac{q_{n-1}}{q_n}$$

Primero, notemos que $q_n > q_{n-1}$, pues de hecho, $q_n = a_n q_{n-1} + q_{n-2}$, donde todos son enteros positivos. Por lo cual, es suficiente ver que $a_{n+1} + 2 - \alpha_{n+1} > 1$, lo cual es obvio, ya que $\alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+1} + 1} < a_{n+1} + 1$. Por lo tanto,

$$\begin{aligned} q_n(a_{n+1} + 2 - \alpha_{n+1}) &> q_{n-1} \\ (a_{n+1} + 2)q_n - \alpha_{n+1}q_n &> q_{n-1} \\ (a_{n+1} + 2)q_n &> \alpha_{n+1}q_n + q_{n-1} \\ (a_{n+1} + 2)q_n^2 &> q_n(\alpha_{n+1}q_n + q_{n-1}) \\ \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})} &> \frac{1}{(a_{n+1} + 2)q_n^2} \end{aligned}$$

Utilizando el Teorema 2.1.5, concluimos que,

$$\left| \alpha - \frac{p_n}{q_n} \right| > \frac{1}{(a_{n+1} + 2)q_n^2}$$
■