CAPÍTULO

VI

Números

En este capítulo tratamos dos cuestiones importantes de teoría de números, aunque sólo sea en su aspecto más elemental: las sumas de cuadrados de números enteros (teorema de Lagrange), y el teorema último de Fermat para exponentes $\leqslant 4$. Además de su interés en sí mismos, estos resultados son una buena ilustración de la importancia de las nociones de divisibilidad y factorialidad en anillos más generales que el de los números enteros.

§1. SUMAS DE CUADRADOS

Trataremos aquí un problema fácil de formular sobre un anillo de números como $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$; o un anillo de restos $\mathbb{Z}/(n)$: el de la representación de sus elementos como sumas de cuadrados.

(1.1) Es conocido que todo número complejo $x = a + bi \in \mathbb{C}$ tiene raíz cuadrada, digamos $y = c + di \in \mathbb{C}$, esto es: $x = y^2$. Así, en $\mathbb{C}$ todo elemento es un cuadrado.

(1.2) El cuadrado de un número real es siempre $\geqslant 0$, y, por tanto, así lo es cualquier suma de cuadrados. Además, todo número $\geqslant 0$ (en particular, toda suma de cuadrados) tiene raíz cuadrada real. En consecuencia, en $\mathbb{R}$ todo elemento $\geqslant 0$ es suma de cuadrados, de hecho, es un cuadrado, y recíprocamente.

(1.3) En $\mathbb{Z}[i]$ tenemos la siguiente identidad: sean $x_k = a_k + b_k \cdot i \in \mathbb{Z}[i]$, $k = 1, \ldots, s$:

$$\sum_{k=1}^{s} x_k^2 = \sum_{k=1}^{s} (a_k^2 - b_k^2) + 2i \sum_{k=1}^{s} a_k b_k.$$

Si $x = a + bi \in \mathbb{Z}[i]$ es suma de cuadrados, resulta que las ecuaciones

$$a = \sum_{k=1}^{s} (a_k^2 - b_k^2)$$

(*)

$$b = 2 \sum_{k=1}^{s} a_k b_k$$

tienen solución en $\mathbb{Z}$. En particular, $2|b$, y obtenemos una condición necesaria.

(1.3.1) Si $x = a + bi \in \mathbb{Z}[i]$ es suma de cuadrados, entonces $b \equiv 0 \bmod 2$.

Por ejemplo i, $1 + i$, $1 - 3i$ *no* son suma de cuadrados en $\mathbb{Z}[i]$. A continuación estudiaremos el recíproco, para lo cual fijamos $x = a + bi$ con $b \equiv 0 \bmod 2$.

(1.3.2) Si $a \equiv 1 \bmod 2$, x es suma de dos cuadrados.

En efecto, por la hipótesis $x - 1 = (a - 1) + bi$ es múltiplo de 2, luego

$$\frac{x-1}{2} \in \mathbb{Z}[i], \quad \frac{x+1}{2} = \frac{x-1}{2} + 1 \in \mathbb{Z}[i],$$

y tenemos

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

(1.3.3) Si $a \equiv 0 \bmod 2$, x es suma de tres cuadrados.

Puesto que en este caso, $a - 1 \equiv 1 \bmod 2$ y por 1.3.2 existen $y, z \in \mathbb{Z}[i]$ con

$$x - 1 = y^2 + z^2,$$

esto es

$$x = 1^2 + y^2 + z^2.$$

(1.3.4) Si $a \equiv 2 \bmod 4$, $b \equiv 0 \bmod 4$, entonces x es suma de dos cuadrados:

Tendremos $x' = x/2 = a' + b'i \in \mathbb{Z}[i]$, donde:

$$a' = a/2 \equiv 1 \bmod 2, \quad b' = b/2 \equiv 0 \bmod 2,$$

por la hipótesis mod 4. Por 1.3.2, $x' = y^2 + z^2$ para ciertos $y, z \in \mathbb{Z}[i]$, y resulta:

$$x = 2x' = 2y^2 + 2z^2 = (y + z)^2 + (y - z)^2.$$

(1.3.5) Si $a \equiv 0 \bmod 4$, $b \equiv 2 \bmod 4$, entonces x es suma de dos cuadrados.

En efecto, tenemos los enteros

$$c = \frac{b}{2} \equiv 1 \bmod 2, \quad d = -\frac{a}{2} \equiv 0 \bmod 2,$$

y el elemento $y = c + di \in \mathbb{Z}[i]$ es suma de dos cuadrados por 1.3.2. Pero se tiene la igualdad

$$(1 + i)^2 y = 2i(c + di) = -2d + 2ci = a + bi = x,$$

luego x es también suma de dos cuadrados.

(1.3.6) Si $a \equiv b \equiv 0 \bmod 4$, x es suma de dos cuadrados.

Puesto que en ese caso $4|x$, tenemos:

$$\left(1+\frac{x}{4}\right)^2+\left(i\left(1-\frac{x}{4}\right)\right)^2=x.$$

(1.3.7) Si $a \equiv b \equiv 2 \bmod 4$, x no es suma de dos cuadrados.

En efecto, si lo fuera, las ecuaciones (*) del inicio de este epígrafe proporcionarían enteros a_1, b_1, a_2, b_2 tales que

(i) $a_1^2-b_1^2+a_2^2-b_2^2=a\equiv 2 \bmod 4,\ 2(a_1b_1+a_2b_2)=b\equiv 2 \bmod 4.$

La segunda relación significa $a_1b_1 + a_2b_2 \equiv 1 \bmod 2$, luego $a_1b_1 \not\equiv a_2b_2 \bmod 2$.

Si, por ejemplo, $a_2b_2 \equiv 0 \bmod 2$ resulta:

$$a_1 \equiv b_1 \equiv 1 \bmod 2$$

y

(ii) $a_2 \equiv 0 \bmod 2$ o $b_2 \equiv 0 \bmod 2.$

De lo primero deducimos

$$a_1-b_1 \equiv a_1+b_1 \equiv 0 \bmod 2,$$

luego

$$a_1^2-b_1^2=(a_1-b_1)(a_1+b_1)\equiv 0 \bmod 4,$$

así que:

$$a_2^2-b_2^2 \equiv a_1^2-b_1^2+a_2^2-b_2^2 \bmod 4,$$

luego por (i) tenemos

$$a_2^2-b_2^2 \equiv 2 \bmod 4.$$

Por (ii) resulta

$$a_2^2 \equiv 0 \bmod 4 \quad \text{o} \quad b_2^2 \equiv 0 \bmod 4,$$

esto es:

$$b_2^2 \equiv 2 \bmod 4 \quad \text{o} \quad a_2^2 \equiv 2 \bmod 4.$$

Esto es imposible, pues si, por ejemplo, $a_2^2 \equiv 2 \bmod 4$ tendríamos

$$2 \mid a_2^2, \quad \text{luego} \quad 2 \mid a_2, \quad \text{luego} \quad 4 \mid a_2^2$$

y así $a_2^2 \equiv 0 \bmod 4$. Absurdo.

Esta contradición significa que x no puede ser suma de dos cuadrados.

Reuniendo todo lo anterior, podemos enunciar:

Proposición 1.3.8.—Sea $x = a + bi \in \mathbb{Z}[i]$. Son equivalentes:

(1) $b \equiv 0 \bmod 2$.

(2) x es suma de cuadrados en $\mathbb{Z}[i]$.

(3) x es suma de tres cuadrados en $\mathbb{Z}[i]$.

Proposición 1.3.9.—Sea $x = a + bi$ suma de cuadrados en $\mathbb{Z}[i]$. Son equivalentes:

(1) $a \equiv b \equiv 2 \bmod 4$.

(2) x no es suma de dos cuadrados en $\mathbb{Z}[i]$.

Consideremos ahora el caso de un anillo de restos $\mathbb{Z}/(n)$, $n > 1$. Más adelante volveremos sobre este mismo caso, pero aquí nos interesa la siguiente:

Proposición 1.4.—Sea n un entero > 1 libre de cuadrados, esto es, entre cuyos divisores no hay ningún cuadrado diferente de 1. Entonces todo elemento

$$[k] \in \mathbb{Z}/(n)$$

es suma de dos cuadrados.

Demostración.—Por la hipótesis, la factorización de n es:

$$n = p_1 \dots p_s$$

y todos los $p_1, \dots, p_s$ primos distintos. Por el teorema chino del resto (I.3.7), tenemos un isomorfismo

$$\mathbb{Z}/(n) \sim \mathbb{Z}/(p_1) \times \dots \times \mathbb{Z}/(p_s),$$

puesto que mcd $(p_i, p_j) = 1$ para cualesquiera $i \neq j$. Si suponemos el resultado probado en $\mathbb{Z}/(p)$ para $p > 1$ primo tendríamos:

$$[k] \sim ([k_1], \dots, [k_s]) = ([a_1]^2 + [b_1]^2, \dots, [a_s]^2 + [b_s]^2) =$$
$$= ([a_1], \dots, [a_s])^2 + ([b_1], \dots, [b_s])^2 \sim [a]^2 + [b]^2$$

para ciertos enteros *a, b*. Así pues, se trata de demostrar la proposición en el caso en que n es primo. Si $n = 2$, se tiene:

$$[0] = [0]^2 + [0]^2,$$
$$[1] = [1]^2 + [0]^2,$$

y es trivial. En consecuencia, sea $n > 2$, con lo que n es impar. Fijemos $[k] \in \mathbb{Z}/(n)$ y consideremos los conjuntos

$$S = \left\{ [\ell]^2 : 0 \leqslant \ell < \frac{n+1}{2} \right\},$$
$$T = \left\{ [k] - [\ell]^2 : 0 \leqslant \ell < \frac{n+1}{2} \right\}.$$

Afirmamos:

(1.4.1) $\quad \text{card } S = \dfrac{n+1}{2} = \text{card } T.$

En efecto, como $[\ell]^2 \mapsto [k] - [\ell]^2$ es biyección, basta verlo para *S*. Se trata de comprobar que si $0 \leqslant \ell < \ell' < \dfrac{n+1}{2}$, entonces $\ell^2 \not\equiv \ell'^2$, ya que el número de enteros $\geqslant 0$ y $< \dfrac{n+1}{2}$ es precisamente $\dfrac{n+1}{2}$. Ahora bien, si $\ell^2 \equiv \ell'^2$,

$$n \mid (\ell'^2 - \ell^2) = (\ell' - \ell)(\ell' + \ell)$$

y por tanto,

$$n \mid (\ell' - \ell) \quad \text{o} \quad n \mid (\ell' + \ell),$$

puesto que n es primo. Así

$$n \leqslant \ell' - \ell \quad \text{o} \quad n \leqslant \ell' + \ell,$$

y como $\ell' - \ell \leqslant \ell' + \ell$, en todo caso:

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

Esto es absurdo, luego queda probado lo que queríamos.

Ya visto 1.4.1, resulta

$$\text{card } S + \text{card } T = n + 1 > n = \text{card } \mathbb{Z}/(n),$$

luego necesariamente $S \cap T$ no es vacío. Elegimos $z \in S \cap T$ y será

$$z = [\ell]^2 = [k] - [\ell']^2$$

para ciertos ℓ, ℓ', esto es: $[k] = [\ell]^2 + [\ell']^2$.

La prueba de 1.4 ha terminado.

Estamos ya prácticamente en condiciones de establecer el resultado fundamental de esta sección, que es el teorema de Lagrange (1770; 1.6), que describe las sumas de cuadrados de los números enteros. Hasta aquí hemos visto algunos resultados sencillos que involucran diversas nociones de las introducidas en el capítulo I. Este es también el caso del teorema de Lagrange (aunque no debe considerarse un resultado sencillo), que vamos a demostrar utilizando una curiosa propiedad de factorialidad en el anillo de matrices $M_2(\mathbb{Z}[i])$. (Véase el ejemplo I.1.9.4).

(1.5) **Factorización de matrices de enteros de Gauss.**

Consideremos el anillo $M_2(\mathbb{Z}[i])$ de las matrices

$$a = \begin{pmatrix} x & y \\ z & t \end{pmatrix}, \quad x, y, z, t \in \mathbb{Z}[i].$$

Utilizando la conjugación $x = c + di \mapsto \bar{x} = c - di$ de $\mathbb{Z}[i]$, I.1.25.1, definimos la norma $\|x\| = x\bar{x} = c^2 + d^2$ y la matriz

$$a^* = \begin{pmatrix} \bar{x} & \bar{z} \\ \bar{y} & \bar{t} \end{pmatrix}.$$

Se comprueba fácilmente que

$$(ab)^* = b^* a^*, \quad \det(a^*) = \overline{\det a}.$$

Se cumple la siguiente:

Proposición 1.5.—Sea $a \in M_2(\mathbb{Z}[i])$ tal que $a = a^*$ y $\det(a) = 1$. Entonces existe otra matriz $b \in M_2(\mathbb{Z}[i])$ tal que

$$a = \pm bb^*.$$

Demostración.—La condición $a = a^*$ significa

$$x = \bar{x}, \qquad y = \bar{z}, \qquad z = \bar{y}, \qquad t = \bar{t},$$

esto es: $x, t \in \mathbb{Z}$, $z = \bar{y}$ (que ya implica $\bar{z} = \bar{\bar{y}} = y$). Así pues,

$$a = \begin{pmatrix} n & c + di \\ c - di & m \end{pmatrix},$$

con $n, m, c, d \in \mathbb{Z}$, y

$$\det(a) = nm - (c+di)(c-di) = nm - c^2 - d^2 \in \mathbb{Z}.$$

Por otra parte, podemos suponer $n \geqslant 0$. En efecto, si $n < 0$ ponemos

$$a' = -a = \begin{pmatrix} -n & * \\ * & * \end{pmatrix},$$

y se ve que $a'^* = a'$ y $\det(a') = \det a$. Entonces, si

$$a' = \pm bb^*.$$

deducimos

$$a = -a' = \mp bb^*.$$

En suma, podemos suponer a partir de ahora que $n \geqslant 0$, y demostraremos por inducción sobre $c^2 + d^2$ que existe b tal que

$$a = bb^*.$$

En primer lugar, si $c^2 + d^2 = 0$, resulta

$$nm = \det(a) + c^2 + d^2 = 1,$$

y necesariamente $a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Basta tomar $b = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Sea, pues, $c^2 + d^2 > 0$ y válido el resultado para valores $< c^2 + d^2$.

Puesto que $nm = 1 + c^2 + d^2 > 0$ y $n \geqslant 0$, también $m \geqslant 0$. De hecho, $n > 0$ y $m > 0$. Distinguiremos ahora dos posibilidades.

Caso 1: $0 < n \leqslant m$.

Pongamos $a' = \tau a \tau^*$, donde

$$\tau = \begin{pmatrix} 1 & 0 \\ \alpha + \beta i & 1 \end{pmatrix} \quad (\alpha, \beta \in \mathbb{Z} \text{ se elegirán después}).$$

Operando queda:

$$a' = \begin{pmatrix} n & c' + d'i \\ c' - d'i & * \end{pmatrix}$$

con

$$c' = c + n\alpha, \quad d' = d - n\beta$$

y

$$\det(a') = (\det\tau)(\det a)(\det(\tau^*)) = 1\cdot 1\cdot 1 = 1.$$

Si la matriz a' admitiese una factorización del tipo

(*) $$a' = b'b'^*$$

poniendo

$$b = \tau^{-1}b', \qquad \tau^{-1} = \begin{pmatrix} 1 & 0 \\ -\alpha - \beta i & 1 \end{pmatrix}$$

resultaría

$$a = \tau^{-1}\tau a\tau^*(\tau^*)^{-1} = \tau^{-1}a'(\tau^*)^{-1} =$$
$$= \tau^{-1}b'b'^*(\tau^*)^{-1} = (\tau^{-1}b')b'^*(\tau^{-1})^* =$$
$$= (\tau^{-1}b')(\tau^{-1}b')^* = bb^*,$$

que es lo que queremos. Así pues, debemos asegurarnos de que (*) existe. Para ello utilizaremos la hipótesis de inducción, pues en virtud de ésta, basta con que elijamos α y β tales que

$$c^2 + d^2 > c'^2 + d'^2 = (c + n\alpha)^2 + (d - n\beta)^2.$$

Ahora bien:

— Si $|c| \leqslant n/2$ y $|d| \leqslant n/2$, resultaría

$$n^2 \leqslant nm = 1 + c^2 + d^2 \leqslant 1 + n^2/4 + n^2/4 = 1 + n^2/2,$$

de donde $n^2/2 \leqslant 1$ y $n^2 \leqslant 2$. En consecuencia $n = 1$ y $c = d = 0$; como $c^2 + d^2 > 0$, este caso no se puede dar.

— Si $|c| > n/2$, entonces $c > n/2$ o $c < -n/2$. En el primer caso tomamos $\alpha = -1$, $\beta = 0$, con lo que

$$c'^2 + d'^2 = (c - n)^2 + d^2 = c^2 + d^2 - n(2c - n) < c^2 + d^2,$$

pues $c > n/2$ significa $2c - n > 0$. Si $c < -n/2$, sean $\alpha = 1$, $\beta = 0$, de modo que

$$c'^2 + d'^2 = (c + n)^2 + d^2 = c^2 + d^2 + n(2c + n) < c^2 + d^2,$$

pues $c < -n/2$ equivale a $2c + n < 0$.

— Análogamente, si $|d| > n/2$, es $d > n/2$ o $d < -n/2$. Tomamos, respectivamente, $\alpha = 0$, $\beta = +1$ o $\alpha = 0$, $\beta = -1$.

CASO 2: $0 < m \leqslant n$.

El argumento es similar, y por ello sólo lo indicamos. Póngase: $a' = \tau a \tau^*$ donde ahora

$$\tau = \begin{pmatrix} 1 & \alpha + \beta i \\ 0 & 1 \end{pmatrix}.$$

Operando:

$$a' = \begin{pmatrix} * & c' + d'i \\ c' - d'i & m \end{pmatrix}$$

donde

$$c' = c + m\alpha, \qquad d' = d + m\beta \cdot$$

De nuevo, se trata de buscar α, β de modo que $c'^2 + d'^2 < c^2 + d^2$. Una discusión de los casos posibles: $|c| > m/2$ o $|d| > m/2$ proporciona las soluciones $(\alpha, \beta) = (-1, 0), (1, 0), (0, -1), (0, 1)$ correspondientes.

Observación.—El signo $\pm$ en la factorización de la proporción anterior está completamente determinado por a. En efecto, se tiene:

$$\begin{pmatrix} n & * \\ * & * \end{pmatrix} = \pm \begin{pmatrix} x & y \\ z & t \end{pmatrix} \begin{pmatrix} \bar{x} & \bar{z} \\ \bar{y} & \bar{t} \end{pmatrix} = \pm \begin{pmatrix} x\bar{x} + y\bar{y} & * \\ * & * \end{pmatrix} =$$

$$= \begin{pmatrix} \pm 1 & 0 \\ * & * \end{pmatrix} \begin{pmatrix} x\bar{x} + y\bar{y} & * \\ * & * \end{pmatrix} = \begin{pmatrix} \pm(x\bar{x} + y\bar{y}) & * \\ * & * \end{pmatrix},$$

y puesto que $x\bar{x} + y\bar{y} = \|x\| + \|y\| > 0$ (I.2.7.2), el *signo en cuestión es el de n*.

Por fin, podemos probar el resultado anunciado:

Proposición 1.6 (teorema de Lagrange).—Sea $n \in \mathbb{Z}$. Son equivalentes

(1) $n \geqslant 0$.

(2) n es suma de cuadrados en $\mathbb{Z}$.

(3) n es suma de *cuatro* cuadrados en $\mathbb{Z}$.

En otras palabras, todo número entero positivo es suma de cuatro cuadrados de números enteros.

Demostración.—Claramente (3) $\Rightarrow$ (2) $\Rightarrow$ (1), luego sólo probaremos la implicación restante. Consideremos la factorización

$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s}.$$