Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Héctor Pastén
Ayudante: José Cuevas Barrientos
Curso: Teoría de Números
Sigla: MAT2225
Fecha: 12 de octubre de 2023

Enteros gaussianos

Diofanto contraataca

1. Los enteros gaussianos

Lema 1.1: Sea $d \in \mathbb{Z}$ un entero cualquiera. Entonces

$$A := \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

es un anillo (i.e., cerrado bajo suma y producto).

Nótese que la proposición anterior permite construir anillos más grandes eligiendo d más pequeño. Por ejemplo, $\mathbb{Z}[\sqrt{n^2 m}] \subseteq \mathbb{Z}[\sqrt{m}]$.

Definición 1.2: Sobre el anillo $A := \mathbb{Z}[\sqrt{d}]$, donde d no es un cuadrado, se definen la función ***conjugado*** $\overline{()}\colon A \to A$ y la función ***norma*** $\mathrm{Nm}\colon A \to \mathbb{Z}$ dadas por

$$\overline{a + b\sqrt{d}} := a - b\sqrt{d}, \qquad \mathrm{Nm}(a + b\sqrt{d}) := (a + b\sqrt{d})\overline{(a + b\sqrt{d})} = a^2 - db^2.$$

Los elementos del anillo $\mathbb{Z}[\sqrt{-1}]$ se dicen ***enteros gaussianos***. Denotaremos $\mathrm{i} := \sqrt{-1}$.

Teorema 1.3: Los enteros gaussianos forman un dominio euclidiano con la norma y, por lo tanto, es un dominio de factorización única (DFU).

Recuérdese que un dominio íntegro A se dice euclidiano si existe una función $\phi\colon A_{\neq 0} \to \mathbb{N}$ para todo par $\alpha, \beta \in A$ con $\beta \neq 0$ existen γ, δ tales que $\alpha = \beta\gamma + \delta$, donde δ o bien es cero, o bien $\phi(\delta) < \phi(\beta)$.

Demostración: Sean $\alpha, \beta \in A := \mathbb{Z}[\mathrm{i}]$ con $\beta \neq 0$. Podemos identificar a $\alpha, \beta \in \mathbb{C}$ y así $\alpha/\beta =: \theta \in \mathbb{C}$ es un número complejo. Mirando el retículo $A = \mathbb{Z} + \mathrm{i}\mathbb{Z} \subseteq \mathbb{C}$ notamos que siempre existe $\gamma \in A$ tal que $|\theta - \gamma|$ es «pequeño», para ser más precisos, $|\theta - \gamma| \leq \sqrt{2}/2$ (ver fig. 1).

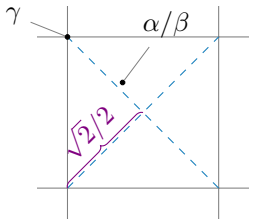

Figura 1

Así que definiendo $\delta := \beta(\theta - \gamma)$, tenemos la siguiente igualdad:

$$\alpha = \beta\theta = \beta\gamma + \delta,$$

donde $\delta = \alpha - \beta\gamma \in A$ puesto que A es un anillo, y donde $|\delta| < |\beta| \cdot \sqrt{2}/2 < |\beta|$. Finalmente, nótese que la norma realmente es $\mathrm{Nm}(a + b\mathrm{i}) = a^2 + b^2 = |a + b\mathrm{i}|^2$, de modo que $\mathrm{Nm}(\delta) < \mathrm{Nm}(\beta)$ como se quería probar. □

Cuando un anillo es un DFU tenemos la gran ventaja de que un elemento es irreducible syss es primo, de modo que se entiende la factorización conociendo las unidades y los primos.

Proposición 1.4: Sea d un entero que no es un cuadrado y sea $A := \mathbb{Z}[\sqrt{d}]$. Se cumplen:

1. La conjugación $\overline{()}\colon A \to A$ es un isomorfismo de anillos.
2. Para todo $\alpha, \beta \in A$ se cumple que $\mathrm{Nm}(\alpha\beta) = \mathrm{Nm}(\alpha)\ \mathrm{Nm}(\beta)$.
3. Un elemento $\alpha \in A$ es una unidad syss $\mathrm{Nm}(\alpha) \in \{\pm 1\}$.
4. Si $\alpha \in A$ es tal que $\mathrm{Nm}(\alpha)$ es primo, entonces α es irreducible en A.

Demostración:
1. Basta notar que $\overline{()}$ respeta sumas y productos, puesto que es claramente biyectivo.
2. $\mathrm{Nm}(\alpha\beta) = \alpha\,\overline{\alpha}\cdot\beta\,\overline{\beta} = \alpha\beta\cdot\overline{\alpha\beta} = \mathrm{Nm}(\alpha)\ \mathrm{Nm}(\beta)$.
3. $\Longrightarrow$. Si α tiene inversa $\gamma := \alpha^{-1}$, entonces
$$\mathrm{Nm}(\alpha)\,\mathrm{Nm}(\gamma) = \mathrm{Nm}(\alpha\gamma) = \mathrm{Nm}(1) = 1,$$
así que $\mathrm{Nm}(\alpha)$ es una unidad de $\mathbb{Z}$, es decir, es ± 1.
$\Longleftarrow$. Como $\alpha\overline{\alpha} = \mathrm{Nm}(\alpha) = \pm 1$, entonces $\pm\overline{\alpha} = \alpha^{-1}$.
4. Por contrarrecíproca, si $\alpha = \beta\gamma$, donde β, γ no son invertibles, entonces $\mathrm{Nm}(\alpha) = \mathrm{Nm}(\beta)\,\mathrm{Nm}(\gamma)$ y $\mathrm{Nm}(\beta), \mathrm{Nm}(\gamma)$ no son unidades de $\mathbb{Z}$, así que $\mathrm{Nm}(\alpha)$ es compuesto. □

El criterio del inciso 4 no es una equivalencia. Por ejemplo, es fácil probar que 2 es irreducible en $\mathbb{Z}[\sqrt{3}]$, pero $\mathrm{Nm}(2) = 4$.

De estudiar la ecuación $\mathrm{Nm}(a + b\mathrm{i}) = a^2 + b^2 = \pm 1$ se sigue que:

Corolario 1.5: $\mathbb{Z}[\mathrm{i}]^\times = \{\pm 1, \pm\mathrm{i}\}$.

Para tener control total sobre la factorización en un anillo es necesario conocer los primos, pero también las unidades. Nótese que esta es una ventaja de que el d sea negativo; cuando el d es positivo, la condición de la norma nos dice que las unidades vienen dadas por la solución a unas ecuaciones de Pell, por lo tanto tendrán infinitas unidades.

2. Dos ecuaciones diofantinas

Teorema 2.1: Las únicas soluciones enteras de la ecuación $y^2 = x^3 - 4$ son
$$(x, y) \in \{(2, \pm 2), (5, \pm 11)\}.$$

Demostración: Reescribamos $x^3 = 4 + y^2 = (2 - \mathrm{i}y)(2 + \mathrm{i}y)$.

- Si y es impar: Notamos que un divisor común α de $2 - \mathrm{i}y$ y $2 + \mathrm{i}y$ es divisor común de su suma 4 y por lo tanto $\mathrm{Nm}(\alpha) \mid 16$ y $\mathrm{Nm}(\alpha) \mid x^3$. Si y es impar, entonces x también y luego $\alpha = 1$, por lo que son coprimos. Luego ambos factores son cubos en $\mathbb{Z}[\mathrm{i}]$ y aplicando conjugados comprobamos:
$$2 + \mathrm{i}y = (a + \mathrm{i}b)^3, \qquad 2 - \mathrm{i}y = (a - \mathrm{i}b)^3,$$
restando ambas expresiones, e igualando partes imaginarias, se obtiene que
$$4 = 2b(b^2 - 3a^2) \iff 2 = b(b^2 - 3a^2).$$
Los divisores (racionales) de 2 permiten deducir que $b \in \{\pm 1, \pm 2\}$. Fijando el valor de b vemos que los únicos posibles valores son $(b, a) = (-1, \pm 1)$ y $(a, b) = (2, \pm 1)$. Nótese que
$$x^3 = \big((a - \mathrm{i}b)(a + \mathrm{i}b)\big)^3 = (a^2 + b^2)^3,$$
de modo que ésto induce los valores $x \in \{2, 5\}$ y de la ecuación $y^2 + 4 = 8, 125$ deducimos que las soluciones son las descritas.

- Si y es par: Entonces $y = 2Y$, y claramente $x = 2X$ lo que reduce la ecuación a $2X^3 = (1 - \mathrm{i}Y)(1 + \mathrm{i}Y)$. Nótese que Y debe ser impar, y que todo factor común a $1 \pm \mathrm{i}Y$ es un divisor de 2, los cuales son (salvo asociados) $1, 1 + \mathrm{i}, 2$. Definamos $\lambda := 1 + \mathrm{i}$ y recordemos que $2 = -\mathrm{i}\lambda^2$. Claramente $2 \nmid 1 \pm \mathrm{i}Y$, pero $\lambda \mid 1 \pm \mathrm{i}Y$ debido a que Y es impar. Dividiendo por λ^2 se obtiene que:
$$\frac{1 + \mathrm{i}Y}{\lambda}\frac{1 - \mathrm{i}Y}{\lambda} = -\mathrm{i}X^3 = (\mathrm{i}X)^3,$$
luego $\frac{1 \pm \mathrm{i}Y}{\lambda}$ son cubos en $\mathbb{Z}[\mathrm{i}]$ y $1 + \mathrm{i}Y = \lambda(a + \mathrm{i}b)^3$, y análogamente $1 - \mathrm{i}Y = \bar{\lambda}(a - \mathrm{i}b)^3$. Sumando y cancelando por 2 se obtiene la ecuación
$$1 = (a + b)(a^2 - 4ab + b^2),$$
cuyas soluciones son $(a, b) \in \{(1, 0), (0, 1)\}$ que inducen $y = \pm 2$. □

Teorema 2.2 (V.A. Lebesgue, 1850): La única solución entera de $y^2 + 1 = x^p$ con $p \geq 2$ es $(1, 0)$.

Demostración: Sea $p = qm$ con q primo y sea (x_0, y_0) solución no trivial de $x^{qm} = y^2 + 1$, entonces (x_0^m, y_0) es solución no trivial de $x^q = y^2 + 1$, así que podemos suponer que p es primo. El caso $p = 2$ es trivial, así que veremos $p \geq 3$.

Nótese que si x fuese par, entonces $y^2 \equiv -1 \pmod 8$ lo cual es imposible. Así que x es impar y por ende y es par. La ecuación se reescribe
$$x^p = (y + \mathrm{i})(y - \mathrm{i}).$$
Nótese que un factor común de ambos debe ser divisor de 2, pero como y es par y ± 1 impar se sigue que éste no es el caso. Los invertibles de Gauss son potencias p-ésimas, pues $(-\mathrm{i})^p = \mp\mathrm{i}$ si $p \equiv \pm 1 \pmod 4$, por lo que ambos factores son potencias p-ésimas conjugadas así que
$$y + \mathrm{i} = (m + \mathrm{i}n)^p = \sum_{j=0}^{p} \binom{p}{j} m^j (\mathrm{i}n)^{p-j},$$
igualando partes imaginarias se obtiene que
$$1 = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} m^{2j} n^{p-2j} (-1)^{\frac{p-1}{2}-j}.$$
Podemos notar que todos los términos poseen un n, de modo que $n \mid 1$ y $n = \pm 1$. Multiplicando por $(-1)^{\frac{p-1}{2}} n$ se obtiene que
$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j = (-1)^{\frac{p-1}{2}} n.$$
Volviendo a la ecuación original y recordando los conjugados se tiene que:
$$x^p = (y + \mathrm{i})(y - \mathrm{i}) = (m + \mathrm{i}n)^p (m - \mathrm{i}n)^p = (m^2 + 1)^p,$$
de modo que m es par, luego
$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j \equiv 1 \pmod 4,$$
por lo que debe ser 1 y $n = (-1)^{\frac{p-1}{2}}$. Como
$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j = 1,$$

notamos que si $p = 3$ entonces ésta ecuación induce $m = 0$. Si $p \geq 5$, entonces podemos despejar:

$$\sum_{j=2}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j = \binom{p}{2} m^2. \tag{1}$$

Ahora bien, nótese lo siguiente:

$$\begin{aligned}\binom{p}{2j} &= \frac{p!}{(p-2j)!(2j)!} = \frac{p(p-1)}{2j(2j-1)} \frac{(p-2)!}{(p-2j)!(2j-2)!} \\ &= \binom{p}{2} \cdot \frac{1}{j(2j-1)} \binom{p-2}{2j-2}.\end{aligned}$$

De ésto podemos notar que la valuación 2-ádica del lado izquierdo de (1) es:

$$\begin{aligned}\nu_2\left(m^{2j}\binom{p}{2j}\right) &\geq 2j\nu_2(m) - \nu_2(j) + \nu_2\left(\binom{p}{2}\right) \\ &\geq (2j - \nu_2(j))\nu_2(m) + \nu_2\left(\binom{p}{2}\right) \\ &> j\nu_2(m) + \nu_2\left(\binom{p}{2}\right),\end{aligned}$$

donde empleamos que $\nu_2(m) \geq 1$ (pues es par) y que $2j - \nu_2(j) > j$ cuando $j > 1$. Luego, el lado izquierdo posee mayor valuación 2-ádica que el derecho, lo cual es absurdo. □

3. Comentarios adicionales

El método empleado en el teorema 1.3 para ver que $\mathbb{Z}[\sqrt{-1}]$ es euclideo con la norma, puede generalizarse para estudiar con más detalle cuales $\mathbb{Z}[\sqrt{d}]$ son (norma-)euclideos; esto se hace en detalle en Eggleton *et al.* **[1]** y nos da la siguiente lista:

$$d \in \{-2,\ -1,\ 2,\ 3,\ 6,\ 7,\ 11,\ 19,\ 38\}.$$

(El artículo incluye otros valores con $d \equiv 1$ (mód 4), pero a estos les asociamos los anillos $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.) Además es un teorema de Motzkin **[3]** que un anillo de la forma $\mathbb{Z}[\sqrt{-d}]$ con $d > 0$ es euclidiano syss es euclidiano con la función norma.

El teorema de V.A. Lebesgue es un caso particular del problema de Catalan que no viene de la demostración general, es decir, que debe hacerse aparte.

Referencias y lecturas adicionales

1. Eggleton, R. B., Lacampagne, C. B. y Selfridge, J. L. Euclidean Quadratic Fields. *Amer. Math. Monthly.* doi:10.2307/2324118 (1992).
2. Mordell, L. J. *Diophantine Equations* (Academic Press, 1969).
3. Motzkin, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

Correo electrónico: josecuevasbtos@uc.cl