Mixba'al
Revista Metropolitana de Matemáticas
No. 1, Vol. IV, junio de 2013, 29–38

SOLUCIÓN DE ECUACIONES DIOFANTINAS A TRAVÉS DE LA FACTORIZACIÓN ÚNICA

ALEJANDRO AGUILAR-ZAVOZNIK

Resumen. Estudiaremos algunas diferencias entre anillos de factorización única y anillos que no lo son. Veremos qué podemos hacer cuando no se tiene factorización única para recuperar algunas de las propiedades que perdemos cuando no se tiene esta propiedad. Usaremos estos resultados para decidir si algunas ecuaciones diofantinas no son solubles y, en el caso contrario, para encontrar todas sus soluciones.

1. Introducción

Un problema que frecuentemente encontramos en las matemáticas es expresar un elemento en términos de otros más sencillos, por ejemplo, si $a \in \mathbb{Z}$ podemos factorizar a como producto de números primos; si V es un espacio vectorial de dimensión finita, podemos expresar $v \in V$ en términos de los elementos de una base; si $A \subseteq \mathbb{R}$ es un conjunto abierto, es posible expresarlo como unión de intervalos abiertos, etc.

Usando la factorización en $\mathbb{Z}$ como modelo, han surgido muchas teorías similares en una gran variedad de anillos, por ejemplo, es común hablar de la factorización en conjuntos de polinomios o matrices. En la actualidad, los principales problemas de factorización se plantean en términos de los anillos de enteros de campos de números, campos de funciones o campos p-ádicos. Incluso hay casos en los que se ha prescindido de la suma, estudiando la factorización de los elementos de algunos monoides [2].

A continuación veremos algunos ejemplos de anillos o monoides donde tenemos factorización única y otros en los que no se tiene esta propiedad. Estudiaremos cómo los ideales se pueden usar para recuperar la factorización única y daremos una aplicación de esta idea para resolver algunas ecuaciones diofantinas.

2. Factorización única

Existen dos dominios de factorización única (DFU) ampliamente estudiados: los enteros y los anillos de polinomios con coeficientes de un campo $\mathbb{K}$. El Teorema Fundamental de la Aritmética afirma que todo número $a \in \mathbb{Z}\setminus\{0, \pm 1\}$ se puede escribir de forma única como producto de primos $a = p_1 \cdot p_2 \cdots p_t$. Es necesario aclarar lo que significa que dos factorizaciones sean iguales. En primer lugar, el orden de los factores no es relevante, por ejemplo, $6 = (2)(3) = (3)(2)$ son la misma factorización. Segundo, dos factorizaciones que difieren por asociados son la misma, por ejemplo $(2)(3)$ y $(-2)(-3)$ son la misma factorización. En esta sección vamos a aclarar lo que significan estos conceptos. A lo largo de este trabajo, la palabra anillo significa anillo conmutativo con unidad 1. Si $\mathbb{A} \subseteq \mathbb{B}$ son anillos y $b_1, \ldots, b_t \in \mathbb{B}$, entonces $\mathbb{A}[b_1, \ldots, b_t]$ es el subanillo más pequeño de $\mathbb{B}$ que contiene a $\mathbb{A}$ y a todos los elementos $b_1, \ldots, b_t$. Si $\mathbb{F} \subseteq \mathbb{K}$ son campos y $b_1, \ldots, b_t \in \mathbb{K}$, entonces $\mathbb{F}(b_1, \ldots, b_t)$ es el menor subcampo de $\mathbb{K}$ que contiene tanto a $\mathbb{F}$ como a los elementos $b_1, \ldots, b_t$. Denotaremos $U(\mathbb{A})$ al grupo de unidades de $\mathbb{A}$. Por ejemplo, $U(\mathbb{Z}) = \{1, -1\}$; si $\mathbb{F}$ es un campo entonces $U(\mathbb{F}[x]) = U(\mathbb{F}) = \mathbb{F} \setminus \{0\}$.

El Teorema Fundamental del Álgebra es el análogo al Teorema Fundamental de la Aritmética en el anillo $\mathbb{C}[x]$. Éste afirma que todo polinomio no constante en $\mathbb{C}[x]$ se

2010 *Mathematics Subject Classification.* 11A51, 11D45,11R04,11R11,11R29.
Palabras clave. Ecuaciones diofantinas, campos de números, factorización única.

factoriza de forma única como producto de polinomios irreducibles de la forma $ax+b$, salvo por el orden y los asociados.

En $\mathbb{Z}$ es común utilizar las palabras "primo" e "irreducible" como si fueran sinónimos. Aunque en este caso son conceptos equivalentes, veremos que no siempre es así.

Definición 1. Un elemento $a \in \mathbb{A}$ es irreducible si, siempre que $a = b_1\, b_2$, entonces $b_1 \in U(\mathbb{A})$ ó $b_2 \in U(\mathbb{A})$.

En un curso elemental de álgebra se demuestra la siguiente propiedad:

Proposición 2. *Si $p \in \mathbb{Z}$ es primo y $p \mid a_1\, a_2$, entones $p \mid a_1$ ó $p \mid a_2$.* □

A partir del resultado anterior surge la definición de primo:

Definición 3. Un elemento $p \in \mathbb{Z}$ es primo si $p \mid a_1\, a_2$ implica $p \mid a_1$ ó $p \mid a_2$.

En la siguiente tabla proporcionamos definiciones equivalentes de primo e irreducible para poder compararlas:

Primo	Irreducible
Para todo $d \in \mathbb{Z}$, $p\, d = a_1 a_2$ implica $p \mid a_1$ ó $p \mid a_2$.	$p = a_1 a_2$ implica $p \mid a_1$ ó $p \mid a_2$.

Podemos observar que, si un elemento es primo, también tiene que ser irreducible pues la definición de irreducible es la de primo con $d = 1$. Más adelante veremos ejemplos en los que estas definiciones no son equivalentes.

Ahora veamos un ejemplo de monoide de factorización única con una operación no conmutativa. Sea A un conjunto finito al que llamaremos alfabeto. Una sucesión finita de elementos de A la llamaremos una palabra de A y al conjunto de palabras de A lo denotaremos A^*. Este conjunto es un monoide con la operación concatenación, es decir,

$$(a_1, \ldots, a_t) * (b_1, \ldots, b_r) = (a_1, \ldots, a_t, b_1, \ldots, b_r).$$

Cuando no hay confusión, es común denotar la palabra $(a_1, a_2, \ldots, a_t)$ como $a_1\, a_2 \cdots a_t$. Claramente A^* es asociativo y el elemento neutro es la sucesión vacía, a la que llamaremos 1. Este monoide es de factorización única donde los elementos irreducibles son las letras del alfabeto A y $U(A^*) = \{1\}$. El conjunto de las palabras no vacías de A^* la denotaremos $A^+ = A^* - \{1\}$.

Si adicionalmente A es totalmente ordenado, podemos usar esta propiedad para ordenar A^+ por medio del orden lexicográfico, que es el que usa el diccionario. Formalmente esto se escribe como sigue: sean $p_1 = (a_1, a_2, \ldots, a_t)$, $p_2 = (b_1, b_2, \ldots, b_r) \in A^+$. Diremos que $p_1 > p_2$ si existe $i < min(t, r)$ tal que $a_j = b_j$ para $j < i$ y $a_i > b_i$ o bien si $t > r$ y $a_j = b_j$ para todo $j \leq r$. Si $A = \{a, b, c, \ldots, z\}$ es el alfabeto con veintisiete letras (incluyendo la ñ) donde $a < b < c < \cdots < z$, entonces: *campo* $>$ *anillo*, *campo* $>$ *cambio* y *cartagena* $>$ *carta*. En particular, una palabra $p \in A^+$ es de Lyndon si $p = p_1 * p_2$, con $p_1, p_2 \in A^+$ implica que $p < p_2 * p_1$. Si $A = \{a, b\}$, las primeras palabras de Lyndon son:

$$\{a, b, ab, aab, abb, aaab, aabb, abbb, aaaab, aaabb, aabab, \ldots\}.$$

Teorema 4. *Toda palabra en A^+ se puede escribir de forma única como producto de una cadena no creciente de palabras de Lyndon.*

Demostración. Ver [4], p.p. 64. □

Por ejemplo, la palabra *aababaaaabaab* se factoriza como producto no creciente de palabras de Lyndon como:

$$aababaaaabaab = aabab * aaaabaab.$$

Notemos que $aabab * aaaab * aab$ también es una factorización, pero $aaaab < aab$.

Los anillos de enteros son una de las familias de anillos donde más se ha estudiado la factorización. Trataremos el caso de los campos cuadráticos. Sugerimos al lector interesado consultar [1], [3], [8] y [10] para profundizar en el tema.

Sea d un entero libre de cuadrados. El campo cuadrático con radicando d es el campo $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Definimos el anillo de enteros de $\mathbb{F}$ como:

$$\mathbb{O}_d = \{a_1 + a_2\sqrt{d} : a_1, a_2 \in \mathbb{Z}\} \qquad \text{si } d \equiv 2, 3 \pmod 4,$$
$$\mathbb{O}_d = \{a_1 + a_2\frac{1+\sqrt{d}}{2} : a_1, a_2 \in \mathbb{Z}\} \quad \text{si } d \equiv 1 \pmod 4.$$

Para algunos valores de d, $\mathbb{O}_d$ es un DFU. Carl Friedrich Gauss conjeturó que solamente hay un número finito de valores negativos d para los que $\mathbb{O}_d$ es de factorización única. En 1967 Harlold Stark [9] probó que estos valores son $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. Una observación interesante es el hecho de que únicamente los primeros cinco anillos son dominios euclideanos, los últimos cuatro son ejemplos de anillos que son DFU pero no euclideanos. En el caso $d > 0$, también fue Gauss quien conjeturó que existe una infinidad de $\mathbb{O}_d$'s que son DFU. Esta célebre conjetura aún no ha sido probada.

Antes de continuar vamos a definir algunas herramientas que nos ayudarán a estudiar la factorización en los anillos de enteros. La función norma $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Z}$ se define como $N(a_1 + a_2\sqrt{d}) = a_1^2 - d\,a_2^2$. Algunas propiedades importantes de la norma son las siguientes:

(1) Un elemento $\alpha \in \mathbb{O}_d$ es unidad si y sólo si $|N(\alpha)| = 1$.
(2) Si $\alpha, \beta \in \mathbb{O}_d$ son asociados, entonces $|N(\alpha)| = |N(\beta)|$.
(3) Si $\gamma = \alpha\,\beta$, entonces $N(\gamma) = N(\alpha)N(\beta)$.

Usando la afirmación 1, es fácil verificar que:

(1) Si $d = -1$, $U(\mathbb{O}_{-1}) = \{\pm 1, \pm i\}$.
(2) Si $d = -3$, $U(\mathbb{O}_{-3}) = \left\{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\frac{1-\sqrt{-3}}{2}\right\}$.
(3) Si $d < 0, d \neq -1, -3$, entonces $U(\mathbb{O}_d) = \{\pm 1\}$.
(4) Si $d > 0$, existe una unidad μ tal que $U(\mathbb{O}_d) = \{\pm\mu^k : k \in \mathbb{Z}\}$.

Lo anterior nos indica que si $d < 0$, entonces $U(\mathbb{O}_d)$ es finito y en el caso $d > 0$ hay una infinidad de unidades en $\mathbb{O}_d$.

Al igual que en el caso de $\mathbb{Z}$, si $\mathbb{O}_d$ es DFU, entonces primo e irreducible son conceptos equivalentes. En la siguiente sección vamos a ver ejemplos de irreducibles que no son primos.

3. Anillos de enteros sin factorización única

Consideremos el anillo $\mathbb{O}_{10}$. El elemento $10 \in \mathbb{O}_{10}$ tiene dos factorizaciones distintas:

$$10 = (2)(5) = (\sqrt{10})^2.$$

Usando la propiedad 2 de la norma podemos ver que estas dos factorizaciones son esencialmente distintas, es decir, que no podemos ir de una factorización a la otra cambiando el orden de los factores o cambiando algunos de ellos por elementos asociados. Notemos que $N(2) = 2^2 - 10(0)^2 = 4$, $N(5) = 5^2 - 10(0)^2 = 25$ y $N(\sqrt{10}) = 0^2 - 10(1)^2 = -10$. Como $|N(2)| \neq |N(\sqrt{10})|$ y $|N(5)| \neq |N(\sqrt{10})|$, entonces 2 y 5 no son asociados de $\sqrt{10}$ en $\mathbb{O}_d$. Falta demostrar que 2, 5 y $\sqrt{10}$ son elementos irreducibles. Para esto utilizamos la propiedad 3 de la norma. Por ejemplo, si 2 no es irreducible, entonces $2 = \alpha_1\,\alpha_2$ para algunos $\alpha_1, \alpha_2 \in \mathbb{O}_{10}$ no unidades. Por la propiedad 3, $|N(\alpha_1)| = |N(\alpha_2)| = 2$, ya que la norma es un entero y es ± 1 si y sólo si el elemento es una unidad. Vamos a demostrar que no hay ningún elemento con norma ± 2 en $\mathbb{O}_{10}$. Con cálculos sencillos se puede observar que los cuadrados módulo 10 son $0, 1, 4, 5, 6, 9$. Como

$$N(a_1 + a_2\sqrt{10}) = a_1^2 - 10a_2^2 \equiv a_1^2 \pmod{10},$$

entonces la norma de cualquier elemento tiene que ser congruente con alguno de los valores $0, 1, 4, 5, 6, 9$, así que 2 y -2 no son norma de ningún elemento, por lo tanto, no pueden existir $\alpha_1, \alpha_2 \in \mathbb{O}_{10}$ no unidades tales que $2 = \alpha_1\,\alpha_2$. Por lo tanto 2 es irreducible. De forma análoga se puede demostrar que $\sqrt{10}$ es irreducible. Para probar que 5 es irreducible hay que usar un procedimiento similar módulo 40. Por tanto, $\mathbb{O}_{10}$ no es DFU.

Ya vimos que para algunos $d \in \mathbb{Z}$ se tiene que $\mathbb{O}_d$ no es un DFU, ¿esto es algo grave? La respuesta es sí, pues perdemos algunas propiedades. Por ejemplo, consideremos la siguiente proposición:

Proposición 5. *Sea $a, b, c \in \mathbb{Z}$ tales que $a^n = b\,c$ y $\text{m.c.d.}\,(b, c) = 1$. Entonces existen $b_1, c_1 \in \mathbb{Z}$ tales que $b = b_1^n$ y $c = c_1^n$.*

Si revisamos la demostración de la proposición anterior, se usa el hecho de que $\mathbb{Z}$ es un dominio de factorización única. Si esta propiedad no se tiene el resultado puede no ser cierto. Observemos que en $\mathbb{O}_{10}$, $(\sqrt{10})^2 = (2)(5)$, donde 2 y 5 son primos relativos, sin embargo, 2 y 5 no son cuadrados, pues de hecho son irreducibles. En este ejemplo no se cumple la proposición anterior.

¿Entonces qué hacemos para resolver el problema de no tener la factorización única? Kummer propuso el uso de los números ideales. Lo que debemos de hacer es agrandar el campo de tal forma que ahora sí se tenga la factorización única. Por ejemplo, si agregamos los elementos $\sqrt{2}$ y $\sqrt{5}$, entonces

$$(2)(5) = (\sqrt{2})^2(\sqrt{5})^2 = (\sqrt{2}\,\sqrt{5})^2 = (\sqrt{10})^2.$$

Podemos ver que en este caso las dos factorizaciones son la misma. Los números ideales tienen la desventaja de que hay varias opciones para recuperar la factorización única.

Basándose en esta idea, Dedekind propuso sustituir los números ideales por los ideales. En el caso de los anillos de enteros usaremos la notación

$$\langle \alpha_1, \ldots, \alpha_t \rangle = \{\alpha_1\beta_1 + \cdots + \alpha_t\beta_t : \beta_1, \ldots, \beta_t \in \mathbb{O}_d\}$$

para denotar al ideal generado por los elementos $\alpha_1, \ldots, \alpha_t$. En particular, todo ideal de $\mathbb{O}_d$ se puede describir con a lo más dos elementos ([10], Theorem 5.20). Por ejemplo, en $\mathbb{Z}$, $\langle a_1, a_2, \ldots, a_k \rangle = \langle \text{m.c.d.}\,(a_1, a_2, \ldots, a_k) \rangle$. En el anillo $\mathbb{O}_{10}$, $\left\langle 44 + 7\sqrt{10}, 17 + \sqrt{10}, 11 + 4\sqrt{10} \right\rangle = \left\langle 3, 2 + \sqrt{10} \right\rangle$ y los ideales $\left\langle 2, \sqrt{10} \right\rangle$ y $\left\langle 5, \sqrt{10} \right\rangle$ no se pueden expresar usando un solo elemento. Cuando un ideal I se puede escribir usando sólo un generador diremos que $I = \langle \alpha \rangle$ es el ideal principal generado por α. Si no es posible escribir al ideal usando solamente un elemento, diremos que I es un ideal no principal.

La idea de Dedekind era usar los ideales principales como los elementos del anillo y los ideales no principales como los números ideales de Kummer. De esta forma, el ejemplo $\sqrt{10}$ se puede escribir en términos de ideales como:

$$\left\langle \sqrt{10} \right\rangle = \left\langle 2, \sqrt{10} \right\rangle^2 \left\langle 5, \sqrt{10} \right\rangle^2,$$

donde el ideal $\left\langle 2, \sqrt{10} \right\rangle$ juega el papel de $\sqrt{2}$ en el ejemplo con números ideales y $\left\langle 5, \sqrt{10} \right\rangle$ juega el papel de $\sqrt{5}$. Sin importar si $\mathbb{O}_d$ es un DFU o no, el monoide de los ideales no cero de $\mathbb{O}_d$ siempre es de factorización única.

Como ya vimos, $(\sqrt{10})^2 = (2)(5)$ donde $2, 5$ no son cuadrados en $\mathbb{O}_{10}$. Si ahora consideramos la factorización en ideales tenemos:

$$\langle 2 \rangle = \left\langle 2, \sqrt{10} \right\rangle^2 \quad \text{y} \quad \langle 5 \rangle = \left\langle 5, \sqrt{10} \right\rangle^2,$$

por lo que ahora sí $\langle 2 \rangle$ es un cuadrado y $\langle 5 \rangle$ es un cuadrado. De esta forma, si usamos ideales, podemos dar un resultado análogo a la Proposición 5.

Proposición 6. *Sean $\alpha, \beta, \gamma \in \mathbb{O}_d$ tales que $\alpha^n = \beta\,\gamma$ y $\langle \alpha \rangle + \langle \beta \rangle = \mathbb{O}_d$. Entonces existen ideales $I, J \subseteq \mathbb{O}_d$ tales que $\langle \beta \rangle = I^n$ y $\langle \gamma \rangle = J^n$.*

Demostración. Es similar a la de la Proposición 5. □

Si $\mathbb{O}_d$ es de factorización única, entonces el análogo a la Proposición 5 sería:

COROLARIO 7. *Sean $\alpha, \beta, \gamma \in \mathbb{O}_d$ tales que $\alpha^n = \beta\,\gamma$ y $\langle\alpha\rangle + \langle\beta\rangle = \mathbb{O}_d$. Entonces existen $\beta_1, \gamma_1 \in \mathbb{O}_d$ y $\mu_1, \mu_2 \in U(\mathbb{O}_d)$ tales que $\beta = \beta_1^n\,\mu_1$ y $\gamma = \gamma_1^n\,\mu_2$.* □

Existen otros ejemplos de anillos o monoides sin factorización única, algunos ejemplos de esto se pueden consultar en [7].

En cualquier anillo donde sea posible la factorización en irreducibles (por ejemplo $\mathbb{O}_d$), cualquier elemento primo es irreducible pero no necesariamente irreducible implica primo. Así tenemos:

TEOREMA 8. *En un dominio entero en donde la factorización en irreducibles es posible, la factorización es única si y sólo si los elementos irreducibles son primos.*

Demostración. Ver Teorema 4.13 [10]. □

Más adelante estudiaremos esto con más detalle

4. Solución de ecuaciones diofantinas

4.1. **Ecuación de Catalan.** En 1844 el matemático belga Eugene Catalan, en una carta enviada al editor de la revista alemana *Journal für die reine und angewandte Mathematik*, se preguntaba sobre la posibilidad de que dos números consecutivos pudieran ser potencias perfectas. En otras palabras, el afirmaba que las únicas soluciones enteras de la ecuación:

$$x^u - y^w = \pm 1$$

son $x = 3, y = 2, u = 2, w = 3$. Este problema quedó sin resolver durante muchos años. Ahora sabemos que el matemático rumano Prida Mihăilescu ha resuelto esta importante conjetura ([5] y [6]). Si suponemos que los exponentes son $u = 2$ y $w = 3$, tenemos una versión débil de la ecuación de Catalan.

Usando argumentos de divisibilidad se puede mostrar que la ecuación $x^2 - y^3 = 1$ tiene una única solución en los enteros positivos: $x = 3,\ y = 2$. En efecto, pues si x es par, entonces m.c.d. $(x-1, x+1) = 1$ y podemos escribir $(x-1)(x+1) = y^3$. Por tanto

$$x - 1 = a^3 \quad \text{y} \quad x + 1 = b^3.$$

De lo anterior se sigue que $b^3 - a^3 = (b-a)(b^2 + ab + b^2) = 2$ y así $b^2 + ab + b^2 \mid 2$, lo cual es imposible. Por lo tanto, si existiera solución, $x = 2t + 1$ y $y = 2q$ con $t, q \geq 1$. Es claro que $t = 1$ implica $x = 3$ y $y = 2$. Si $t > 1$, tendríamos $t(t+1) = (2q)^3$, un número triangular que es un cubo, lo cual no es posible.

Ahora consideremos la ecuación $x^2 - y^3 = -1$, la cual afirmamos, tiene como única solución entera $y = 1$ y $x = 0$. En efecto, tenemos la factorización:

$$y^3 = (x + i)(x - i)$$

lo que nos sugiere trabajar en el anillo de los enteros gaussianos $\mathbb{Z}[i] = \mathbb{O}_{-1}$, el cual es de factorización única y como ya mencionamos, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Primero notemos que m.c.d. $(x + i, x - i) = 1$. Así que $x + i = (a + bi)^3$ y $x - i = (a - bi)^3$, salvo unidades. Se observa que $x + i = (a^3 - 3ab^2) + (3a^2b - b^3)i$ y por tanto $x - i = (a^3 - 3ab^2) - (3a^2b - b^3)i$. Igualando parte real e imaginaria tenemos $3a^2b - b^3 = b(3a^2 - b^2) = 1$, de donde $b \mid 1$ y así $b = \pm 1$. El caso $b = 1$ claramente no es posible. El caso $b = -1$ conduce a $y = 1$ y $x = 0$. En suma, la táctica consistió en ir a otro anillo en dónde la aritmética es más apropiada para encontrar la solución. ¿Cuál es la más apropiada? Es difícil saberlo, simplemente reconocer un anillo con factorización única es un problema que ocupa parte de las investigaciones en teoría de números.

4.2. **Ecuación de Bachet.** Antes de Catalan, el matemático francés Claude Gaspar Bachet (1581-1638) se preguntaba cuántas soluciones enteras tiene la ecuación $x^2 - y^3 = k$ con $k \in \mathbb{Z}$. Existen técnicas elementales para dar respuesta a la existencia de soluciones para ciertos valores de k. El caso que sirve para nuestro propósito es $x^2 - y^3 = -19$. Debido a la factorización $x^2 + 19 = (x + \sqrt{-19})(x - \sqrt{-19}) = y^3$, podríamos trabajar en el anillo $\mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} : a, b \in \mathbb{Z}\}$, el cuál es un subanillo de índice 2 en el anillo $\mathbb{O}_{-19}$. Es conocido que el anillo $\mathbb{O}_{-19}$ tiene la propiedad de la factorización única por la clasificación de H. Stark que ya comentamos. Tenemos las siguientes consideraciones:

1. $U(\mathbb{Z}[\sqrt{-19}]) = \{\pm 1\}$ pues $N(a + b\sqrt{-19}) = a^2 + 19b^2 = 1$ si y sólo si $b = 0$ y $a = \pm 1$. Notemos que cualquier unidad es un cubo.
2. Si $19 \mid y$, entonces $19 \mid y^3$ y $19 \mid x$. Así $x^2 - y^3 = 19^2 q = -19$. Por tanto $19 \nmid y$.
3. Si $2 \mid y$, entonces x es impar y $8 \mid y^3$. Por tanto $x^2 \equiv y^3 - 19 \equiv -1 \pmod 8$, lo cual es imposible.
4. Sea $\pi \in \mathbb{Z}[\sqrt{-19}]$ un divisor irreducible común de $x + \sqrt{-19}$ y $x - \sqrt{-19}$. Entonces $\pi \mid 2\sqrt{-19}$ y por tanto $\pi \mid 2\sqrt{-19}\sqrt{-19}$. Así, $\pi \mid (2)(19)$ y $\pi \mid y^3$. Como $1 = ry^3 + (2)(19)s$ en $\mathbb{Z}$, entonces $\pi \mid 1$ y por tanto m.c.d. $\left(x + \sqrt{-19}, x - \sqrt{-19}\right) = 1$ en $\mathbb{Z}[\sqrt{-19}]$.
5. De la factorización $y^3 = (x + \sqrt{-19})(x - \sqrt{-19})$ y usando el Corolario 7 podemos suponer que $x + \sqrt{-19}$ y $x - \sqrt{-19}$ son cubos, salvo por una unidad.

Supongamos que $x + \sqrt{-19} = (a + b\sqrt{-19})^3$ para ciertos $a, b \in \mathbb{Z}$. Igualando parte real e imaginaria tenemos el sistema

$$x = a^3 - 57\, a\, b^2$$
$$1 = 3\, a^2\, b - 19\, b^3$$

La primera ecuación no aporta mucho; sin embargo la segunda ecuación nos indica que $b \mid 1$ y así $b = \pm 1$. Cualquiera que sea el valor de b implica que $a \notin \mathbb{Z}$. Con todo lo anterior podemos concluir que la ecuación $x^2 - y^3 = -19$ no es soluble en $\mathbb{Z}$. Pero observemos que $18^2 - 7^3 = -19$. ¿ Qué hicimos mal? ¿cómo explicamos esto? Bueno, parte de la respuesta es que es falso que si el anillo $\mathbb{O}_d$ es de factorización única, entonces cualquier subanillo debe tener la misma propiedad. Así, el subanillo $\mathbb{Z}[\sqrt{-19}]$ no es de factorización única. Por ejemplo

$$35 = 5 \cdot 7 = (4 + \sqrt{-19})(4 - \sqrt{-19}).$$

Se puede probar sin mucha dificultad y con la ayuda de la función norma que los números $5, 7, 4 + \sqrt{-19}, 4 - \sqrt{-19}$ son irreducibles en $\mathbb{Z}[\sqrt{-19}]$ y no son primos ni asociados dos a dos. Por ejemplo, 5 es irreducible y no primo. Si $5 = \alpha\, \beta$, entonces

$$25 = N(\alpha)N(\beta)$$

y por tanto $N(\alpha) = N(\beta) = 5$ ó $N(\alpha) = 25$ y $N(\beta) = 1$. El primer caso no es posible pues obviamente la ecuación $a^2 + 19b^2 = 5$ no tiene solución en $\mathbb{Z}$. En el segundo caso tenemos que $\beta \in U(\mathbb{Z}[\sqrt{-19}])$ y 5 es irreducible. ¿Por qué 5 no es primo en $\mathbb{Z}[\sqrt{-19}]$? Claramente $5 \mid (4 + \sqrt{-19})(4 - \sqrt{-19})$. Si $5 \mid 4 + \sqrt{-19}$, entonces

$$4 + \sqrt{-19} = 5(a + b\sqrt{-19}) = 5a + 5b\sqrt{-19}.$$

Por tanto $5 \mid 4$ en $\mathbb{Z}$ lo cual es imposible. Similarmente $5 \nmid 4 - \sqrt{-19}$ y 5 no es primo. Este ejemplo es testimonio del Teorema 8.

Si escribimos $x + \sqrt{-19} = \left(\dfrac{a + b\sqrt{-19}}{2}\right)^3$ y seguimos las mismas ideas se puede concluir que las soluciones de $x^2 - y^3 = -19$ son $x = \pm 8, y = 7$. Notemos que ahora estamos trabajando en el anillo $\mathbb{O}_{-19}$ en lugar de $\mathbb{Z}[\sqrt{-19}]$.

Como dato histórico, Bachet es más conocido por su traducción al latín del texto griego de Diofanto en 1621. Esta versión es la que utilizó Fermat como libro de notas en donde escribió su famosa afirmación.

5. El grupo de clases de ideales y solución de ecuaciones diofantinas

Cuando no se tiene la factorización única se puede recurrir a la factorización única con respecto a ideales. Consideremos el anillo $\mathbb{O}_d$ y el monoide:

$$G = \{I \neq 0 : I \text{ es ideal de } \mathbb{O}_d\}.$$

Definimos la siguiente relación $\sim$ en G: Para $I, J \in G$, $I \sim J$ si existen $\alpha, \beta \in \mathbb{O}_d \setminus \{0\}$ tal que $(\alpha)I = (\beta)J$, donde (α) es el ideal principal generado por α. Se sabe que:

1.- $\sim$ es de equivalencia.
2.- El conjunto de clases de equivalencia es finito.
3.- El conjunto de clases de equivalencia tiene estructura de grupo abeliano, el cual denotamos por $\mathbb{G}$. La operación es la natural: $[I][J] = [IJ]$.
4.- El orden h_d del grupo $\mathbb{G}$ satisface: $h_d = 1$ si y sólo si $\mathbb{O}_d$ es de factorización única.

Obviamente cualquier ideal principal está relacionado con el ideal $\mathbb{O}_d = \langle 1 \rangle$ y en particular, el neutro del grupo $\mathbb{G}$ es la clase $[\langle 1 \rangle]$. Así por ejemplo, el grupo de clases de ideales de $\mathbb{O}_{-5}$ es:

$$\mathbb{G} = \{[\langle 1 \rangle], [\langle 3, 1 + \sqrt{-5} \rangle]\}.$$

El grupo de clases de ideales del anillo $\mathbb{O}_{-14}$ es:

$$\mathbb{G} = \{[\langle 1 \rangle], [\langle 2, -\sqrt{-14} \rangle], [\langle 3, 1 + \sqrt{-14} \rangle], [\langle 3, 1 - \sqrt{-14} \rangle]\},$$

y en los anillos $\mathbb{O}_{-5}$ y $\mathbb{O}_{-14}$ no hay factorización única. La pregunta que nos hacemos ahora es ¿cómo se calcula el orden de éstos grupos? La respuesta es que es muy difícil encontrar h_d y la razón es porque algunas fórmulas que se conocen involucran a la función ζ de Riemann y otras involucran el cálculo de unidades fundamentales (ϵ_d, $d > 0$), como en nuestro caso. Por ejemplo, para calcular la unidad fundamental se debe resolver la ecuación $x^2 - dy^2 = \pm 1$ y esto requiere de las fracciones continuas. Una vez encontrada la unidad fundamental, se puede recurrir por ejemplo, a la fórmula

$$h_d = \frac{\sqrt{d}}{2\epsilon_d} L(1, \chi_d),$$

donde L es una L-serie de Dirichlet.

También existen fórmulas explícitas para el caso cuadrático. Por ejemplo Dirichlet descubrió que si $p \equiv 3 \pmod 4$ es un primo y $\mathbb{F} = \mathbb{Q}(\sqrt{-p})$, entonces

$$h_{-p} = \frac{1}{p}\Big(\sum r_i - \sum s_i\Big),$$

donde $\sum r_i$ es la suma de los residuos cuadráticos y $\sum s_i$ es la suma de los residuos no cuadráticos en $\mathbb{F}_p$.

El producto de dos ideales principales es principal y si I satisface

$$\langle \alpha \rangle I = \langle \beta \rangle$$

para ciertos $\alpha, \beta \in \mathbb{O}_d \setminus \{0\}$, entonces I también es un ideal principal.

Para cualquier anillo cuadrático consideremos el monoide G de ideales $\neq 0$ de $\mathbb{O}_d$. Como sabemos, G tiene la propiedad de la factorización única en términos de ideales primos. Usaremos esta cualidad para decidir si cierta clase de ecuaciones diofantinas es soluble en $\mathbb{Z}$.

Teorema 9. *Sean $d > 1$ un entero que no es un cuadrado, $d \equiv 1, 2 \pmod 4$, $F = \mathbb{Q}(\sqrt{-d})$ con anillo de enteros $\mathbb{O}_{-d}$ y el orden de las clases de ideales de $\mathbb{O}_{-d}$ es igual a h_{-d}. Si $p^{2m} \nmid d$ para todo primo $p \mid d$ y $n \geq 2m$ con $n, m \in \mathbb{Z}$, de tal forma que* m.c.d. $(n, h_{-d}) = 1$ *y* m.c.d. $(d, n) \neq 1$, *entonces*

$$y^n = x^{2m} + d \tag{1}$$

no tiene solución en los enteros x, y.

Demostración. Supongamos que x, y es una solución de la ecuación (1). Si $d = d_1 d_2^2$ con d_1 libre de cuadrados, $\mathbb{O}_{-d} = \mathbb{Z}[\sqrt{-d_1}]$. En este anillo, la ecuación (1) se puede reescribir como

$$y^n = (x^m + \sqrt{-d})(x^m - \sqrt{-d}).$$

La factorización única no se cumple en $\mathbb{O}_{-d}$ a menos que $h_{-d} = 1$, así que la transformaremos en una ecuación de ideales:

$$\langle y \rangle^n = \langle x^m + \sqrt{-d} \rangle \langle x^m - \sqrt{-d} \rangle. \tag{2}$$

Primero demostremos que $\langle x^m + \sqrt{-d} \rangle$ y $\langle x^m - \sqrt{-d} \rangle$ son ideales primos relativos entre sí, esto es, no existe un ideal primo en $\mathbb{O}_{-d}$ que los divida a ambos.

El primer paso para probar la afirmación anterior es ver que x y d son primos relativos en $\mathbb{Z}$. Supongamos que existe un primo p tal que $p \mid x$ y $p \mid d$. Como $y^n = x^{2m} + d$, entonces $p \mid y^n$ y así $p \mid y$. De lo anterior, tenemos que $p^n \mid y^n = x^{2m} + d$. $p^{2m} \mid x^{2m}$ y $p^{2m} \mid x^{2m} + d$ implica que $p^{2m} \mid d$, lo que es una contradicción, pues $p^{2m} \nmid d$. Por lo tanto m.c.d. $(x, d) = 1$.

Ahora demostraremos que $x^{2m} + d$ y $x^{2m} - d$ son primos relativos en $\mathbb{Z}$. Si existiera un primo p tal que $p \mid$ m.c.d. $\left(x^{2m} + d, x^{2m} - d\right)$, entonces

$$p \mid 2x^{2m} = (x^{2m} + d) + (x^{2m} - d) \text{ y}$$

$$p \mid 2d = (x^{2m} + d) - (x^{2m} - d).$$

Como m.c.d. $(x, d) = 1$, entonces $p = 2$. Observemos que x y d deben ser impares, pues $2 \mid x^{2m} + d$ y m.c.d. $(x, d) = 1$, y como $d \equiv 1 \pmod 4$ tendremos que $x^{2m} + d \equiv 2 \pmod 4$. Pero entonces y es par, lo que implica que $y^n \equiv 0 \pmod 4$; y así no existe el primo p. Por lo tanto m.c.d. $\left(x^{2m} + d, x^{2m} - d\right) = 1$.

Finalmente, tenemos que ver que $\langle x^m + \sqrt{-d} \rangle + \langle x^m - \sqrt{-d} \rangle = \mathbb{O}_{-d}$, para concluir que efectivamente son primos relativos.

Sean $a, c \in \mathbb{Z}$ tales que $a(x^{2m} - d) + c(x^{2m} + d) = 1$. Si $b = ax^m + cx^m$, entonces

$$(a\sqrt{-d})(x^m + \sqrt{-d}) + (b + c\sqrt{-d})(x^m - \sqrt{-d}) =$$

$$(a\sqrt{-d})(x^m + \sqrt{-d}) + (ax^m + cx^m + c\sqrt{-d})(x^m - \sqrt{-d}) =$$

$$ax^m\sqrt{-d} - ad + ax^{2m} + cx^{2m} + cx^m\sqrt{-d} - ax^m\sqrt{-d} - cx^m\sqrt{-d} + cd =$$

$$a(x^{2m} - d) + c(x^{2m} + d) = 1.$$

Como

$$(a\sqrt{-d})(x^m + \sqrt{-d}) \in \langle x^m + \sqrt{-d} \rangle \text{ y}$$

$$(b + c\sqrt{-d})(x^m - \sqrt{-d}) \in \langle x^m - \sqrt{-d} \rangle,$$

entonces efectivamente los ideales son primos relativos. Con esto concluimos nuestra primera afirmación.

Como los ideales se factorizan de forma única, el hecho de que $\langle x^m + \sqrt{-d} \rangle$ y $\langle x^m - \sqrt{-d} \rangle$ son primos relativos junto con (2), implica que existen I y J, ideales de $\mathbb{O}_{-d}$, tales que

$$I^n = \langle x^m + \sqrt{-d} \rangle \text{ y}$$

$$J^n = \langle x^m - \sqrt{-d} \rangle.$$

Por hipótesis, m.c.d. $(n, h_{-d}) = 1$, por lo que existe $k \in \mathbb{Z}$ tal que $kn \equiv 1 \pmod{h_{-d}}$. Sea r tal que $kn = h_{-d}r + 1$. Entonces

$$I^{kn} = I^{h_{-d}r+1} = \langle \alpha \rangle I = \langle x^m + \sqrt{-d} \rangle^k = \langle (x^m + \sqrt{-d})^k \rangle.$$

Por esto, I debe de ser un ideal principal, digamos $I = \langle a + b\sqrt{-d} \rangle$. De lo anterior,

$$\langle x^m + \sqrt{-d} \rangle = I^n = \langle (a + b\sqrt{-d})^n \rangle,$$

y entonces $x^m + \sqrt{-d}$ debe de ser un asociado de $(a + b\sqrt{-d})^n$ en $\mathbb{O}_{-d}$. El grupo de unidades es $\{\pm 1\}$, pues $d_1 \neq 1, 3$, así que:

$$x^m + \sqrt{-d} = (a + b\sqrt{-d})^n = \pm \sum_{i=0}^{n} \binom{n}{i} a^{n-i} (b\sqrt{-d})^i = a' + b'\sqrt{d}.$$

Como $1 \neq \text{m.c.d.}\,(d, n) \mid \binom{n}{i}$ para $1 < i < n$ y d divide al último término de la suma (pues $n \geq 2$), entonces $\text{m.c.d.}\,(d, n) \mid b'$. Pero $b' = 1$; por lo que tenemos una contradicción, que significa que la suposición de que existen $x, y \in \mathbb{Z}$ es falsa, así que la ecuación (1) no tiene solución. □

Nota: Si n es par, el n-ésimo término de la suma corresponde a a', por lo que la condición de que $\text{m.c.d.}\,(d, n) \neq 1$ no es necesaria; en este caso, lo único que cambia es que en lugar de afirmar que $d \mid b'$ (en el último párrafo de la demostración) diremos que $n \mid b'$. Por lo tanto, también es cierto que:

TEOREMA 10. *Sean $d > 1$ un entero que no es un cuadrado, $d \equiv 1, 2 \pmod 4$ y $F = \mathbb{Q}(\sqrt{-d})$ con anillo de enteros $\mathbb{O}_{-d}$. Si $p^{2m} \nmid d$ para todo primo $p \mid d$ y $2n \geq 2m$ es un entero que cumple $\text{m.c.d.}\,(2n, h_{-d}) = 1$, con $n, m \in \mathbb{Z}$, entonces*

$$y^{2n} = x^{2m} + d$$

no tiene solución. □

Estas ideas también pueden usarse cuando hay soluciones, por ejemplo, resolvamos la siguiente ecuación:

$$y^3 = x^4 + 44 = (x^2 + \sqrt{-44})(x^2 - \sqrt{-44}) = (x^2 + 2\sqrt{-11})(x^2 - 2\sqrt{-11}).$$

Escribiendo la ecuación como ideales de $\mathbb{O}_{-11}$ tenemos:

$$\langle y \rangle^3 = \left\langle x^2 + 2\sqrt{-11} \right\rangle \left\langle x^2 - 2\sqrt{-11} \right\rangle.$$

Por la factorización única de ideales, existen $I, J \subseteq \mathbb{O}_{-11}$ tales que

$$\left\langle x^2 + 2\sqrt{-11} \right\rangle = I^3 \quad \text{y} \quad \left\langle x^2 - 2\sqrt{-11} \right\rangle = J^3.$$

Como $\mathbb{O}_{-11}$ es uno de los anillos de la lista de H. Stark, entonces I y J son principales. Supongamos $I = \left\langle \dfrac{a + b\sqrt{-11}}{2} \right\rangle$ con $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$, entonces

$$\left(\frac{a + b\sqrt{-11}}{2}\right)^3 = \frac{(a^3 - 33\,a\,b^2) + \sqrt{-11}(3\,a^2\,b - 11\,b^3)}{8} = \pm(x^2 + 2\sqrt{-11}).$$

Igualando términos, la ecuación anterior nos indica que tenemos que resolver el sistema

$$\begin{aligned} \pm 2 &= \frac{3\,a^2\,b - 11\,b^3}{8} = \frac{b(3\,a^2 - 11\,b^2)}{8}, \\ \pm x^2 &= \frac{a^3 - 33\,a\,b^2}{8}, \end{aligned} \tag{3}$$

de donde la primera ecuación se puede reescribir como $\pm 16 = b(3\,a^2 - 11\,b^2)$. Como en cualquier caso $b \mid 16$, entonces las posibilidades para b son ± 1, ± 2, ± 4, ± 8, ± 16. En cada uno de estos casos se obtiene:

$$\begin{array}{ll} b = 1 & \pm 16 = (1)(3\,a^2 - 11) \\ b = -1 & \pm 16 = (-1)(3\,a^2 - 11) \\ b = 2 & \pm 16 = (2)(3\,a^2 - 44) \\ b = -2 & \pm 16 = (-2)(3\,a^2 - 44) \\ b = 4 & \pm 16 = (4)(3\,a^2 - 176) \\ b = -4 & \pm 16 = (-4)(3\,a^2 - 176) \\ b = 8 & \pm 16 = (8)(3\,a^2 - 704) \\ b = -8 & \pm 16 = (-8)(3\,a^2 - 704) \\ b = 16 & \pm 16 = (16)(3\,a^2 - 2816) \\ b = -16 & \pm 16 = (-16)(3\,a^2 - 2816). \end{array}$$

De esta forma, resolver la ecuación diofantina se convierte en resolver veinte polinomios cuadráticos con una variable, lo que es mucho más sencillo. Además, observemos que los dos polinomios del primer renglón son los negativos de los dos polinomios del segundo renglón y así sucesivamente, de tal forma que únicamente hay que encontrar las soluciones de diez polinomios cuadráticos: $0 = 3\,a^2 - 27$ con soluciones ± 3 y $0 = 3\,a^2 + 5$, $0 = 3\,a^2 - 52$, $0 = 3\,a^2 - 36$, $0 = 3\,a^2 - 180$, $0 = 3\,a^2 - 172$, $0 = 3\,a^2 - 706$, $0 = 3\,a^2 - 702$, $0 = 3\,a^2 - 2817$, $0 = 3\,a^2 - 2815$, cuyas soluciones no son enteras. Como podemos ver, los únicos valores en $\mathbb{Z}$ que puede tomar a son ± 3, y esto solamente sucede si $b = \pm 1$. Regresando a la ecuación (3),

$$\pm x^2 = \pm \frac{27 - 99}{8} = \pm 9,$$

de donde x solamente puede ser ± 3. Sin importar el signo, $y^3 = x^4 + 44 = 81 + 44 = 125$. De esta forma, vemos que la ecuación tiene exactamente dos soluciones: $x = 3, y = 5$ y $x = -3, y = 5$.

Referencias

[1] Alaca, S., Williams, K. S., *Introductory Algebraic Number Theory*, Cambridge University Press, 2004.

[2] Halter-Koch, F., *Ideal systems. An introduction to multiplicative ideal theory*, Monographs and Textbooks in Pure and Applied Mathematics, **211**. Marcel Dekker, Inc., New York, 1998.

[3] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, GTM **84**, 2a edición, (1990).

[4] Lothaire, M., *Combinatorics on words*, Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1997.

[5] Mihăilesku, P., *Primary cyclotomic units and a proof of Catalan's conjeture*. J. Reine Angew. Math. **572** (2004), 167-195.

[6] Mihăilesku, P., *On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation*. J. Number Theory **118** (2006), no.1, 123-144.

[7] Pineda-Ruelas, M., Primo y/o irreducible, *Carta Informativa*, No. 54, México, Octubre, 2007.

[8] Ribenboim, P., *Clasical theory of algebraic numbers*, Springer-Velag, UTX, (2001).

[9] Stark, H., On complex quadratic fields with class number equal to one, *Trans. Amer. Math. Soc.*, **122**, 1966, 112-119.

[10] Stewart I., Tall D., *Algebraic Number Theory and Fermat's Last Theorem*, A K Peters, 3rd edition, (2001).

Dirección del autor:
Alejandro Aguilar-Zavoznik
Universidad Autónoma Metropolitana,
Unidad Azcapotzalco,
División de Ciencias Básicas e Ingeniería,
Departamento de Ciencias Básicas.
Av. San Pablo 180, Col. Reynosa Tamaulipas
Del. Azcapotzalco, C.P. 02200 México, D.F.
e-mail: `aaz@correo.azc.uam.mx`