Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Ricardo Menares
Ayudante: José Cuevas Barrientos
Curso: Teoría de Números
Sigla: MAT2814
Fecha: 11 de agosto de 2025

Aritmética modular y DFUs

Introducción

A lo largo de las ayudantías incluiré ciertos símbolos: los problemas/comentarios **recomendados** e importantes tendrán ojos interesados ◕◕, los problemas difíciles tendrán ojos asustados ◉◉, y los problemas/comentarios que son opcionales u omitibles tendrán ojos hastiados ◓◓.

1. Congruencias

1. Demuestre que la ecuación diofantina $x^2 + y^2 = 4z + 3$ no tiene soluciones enteras.
2. (Gersónides) Las únicas potencias consecutivas de 2 y 3 son $1, 2, 3, 4, 8$ y 9.
3. Demuestre que las únicas soluciones (en $\mathbb{Z}$) a la ecuación diofántica $y^2 + y = x^3$ son
$$(x, y) \in \{(0, 0), \quad (0, -1)\}.$$

◕◕ 4. («Elevando el exponente») Demuestre el siguiente clásico truco de olimpiadas: Dado un primo $p > 2$, un par de enteros $x, y \in \mathbb{Z}$ tales que $x \equiv y \not\equiv 0 \pmod{p}$ y un entero $n \geq 1$, entonces
$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n),$$

5. Recuerde que un entero $g \in \mathbb{Z}$ se dice una ***raíz primitiva módulo*** n si $(\mathbb{Z}/n\mathbb{Z})^\times$ está generado (como grupo) por $g \mod n$.
   a) Pruebe que para un primo p, si g es una raíz primitiva módulo p, entonces g ó $g + p$ es una raíz primitiva módulo p^2.
   b) Pruebe que si g es una raíz primitiva módulo p^2 para un primo $p > 2$, entonces g es raíz primitiva módulo p^n para todo $n \geq 1$.

2. El teorema fundamental de la aritmética

El adjetivo *fundamental* no es accidental, son varias las consecuencias de él y es, en muchas ocasiones, la principal herramienta para resolver ecuaciones diofánticas. Aquí veremos ejemplos de anillos que carecen de esta propiedad fundamental.

Definición 2.1: Un anillo A se dice un *dominio de factorización única* (abrev. ***DFU***) si es un dominio íntegro (i.e., no tiene divisores de cero no nulos) y todo elemento $a \in A$ admite una descomposición (*existencia*)
$$a = u\pi_1^{e_1} \cdots \pi_n^{e_n},$$
donde $u \in A^\times$ es una unidad, cada π_j es irreducible (i.e., si $\beta \mid \pi_j$ y $\beta \notin A^\times$, entonces $(\beta) = (\pi_j)$) y los ideales (π_j) son distintos dos a dos; además, de haber otra descomposición, entonces podemos reordenar los términos para que los ideales (π_j) y los exponentes e_j sean los mismos (*unicidad*).

Naturalmente, el «teorema fundamental de la aritmética» se reescribe ahora en términos de que $\mathbb{Z}$ es un DFU.

6. Considere el siguiente conjunto
$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$
   a) Pruebe que $\mathbb{Z}[\sqrt{-5}]$ es un subanillo de $\mathbb{C}$ y que es un dominio íntegro.

b) Definamos la «norma» de un elemento de $\mathbb{Z}[\sqrt{-5}]$ como

$$\mathrm{Nm}(x + y\sqrt{-5}) := x^2 + 5y^2 \in \mathbb{Z}.$$

Pruebe que para $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ se cumple que $\mathrm{Nm}(\alpha \cdot \beta) = \mathrm{Nm}(\alpha) \cdot \mathrm{Nm}(\beta)$.

c) Empleando la factorización

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

concluya que $\mathbb{Z}[\sqrt{-5}]$ no es un DFU.

◉◉ 7. Generalicemos el procedimiento anterior. Sea $\gamma \in \mathbb{C}$ un número algebraico cuyo polinomio minimal (respecto a $\mathbb{Q}$) tiene coeficientes en $\mathbb{Z}$.

a) Pruebe que $\mathbb{Z}[\gamma] = \{f(\gamma) : f(x) \in \mathbb{Z}[x]\}$ es un dominio íntegro.

b) Pruebe que $\gamma \in \mathbb{Z}[\gamma]$ es irreducible.
Pista: Si no lo fuese, ¿qué implicaría en el cociente $\mathbb{Z}[\gamma]/(\gamma)$? □

c) Muestre que hay un número primo (racional) $p \in \mathbb{Z}$ tal que $\gamma \nmid p$.
Pista: Para ello, pruebe que para todo $\alpha \notin \mathbb{Z}[\gamma]^\times$ hay *finitos* ideales primos $\mathfrak{p} \lhd \mathbb{Z}[\gamma]$ tales que $\alpha \in \mathfrak{p}$, y argumente por qué hay un primo racional que no pertenece a alguno de ellos. □

d) Finalmente, concluya que $\mathbb{Z}[n\gamma]$ no es un DFU para algún n.

Comentarios

En el mundo investigativo, para los teoristas de números las ecuaciones diofánticas en dos variables de grado cuadrático están «bien entendidas» (también conocidas como *cónicas planares*), de modo que el primer caso «interesante» sucede con cúbicas planares. En varios casos, hay cambios de variable mediante los cuales uno puede reducirse a estudiar ecuaciones del tipo $x^3 + ax + b = y^2 + cy + dxy$, que reflejan un objeto geométrico (más precisamente, una «curva algebraica») llamada una *curva elíptica*. Soluciones a coeficientes enteros de $y^2 = x^3 + a$ fueron arduamente estudiadas por el británico Louis Mordell.

Hay una razón del por qué $\mathbb{Z}[n\gamma]$ no es DFU en general; la estrategia que emplee para construir el contraejemplo tras bastidores está en una aplicación de álgebra conmutativa. Los elementos de $\mathbb{C}$ cuyo polinomio minimal tiene coeficientes en $\mathbb{Z}$ se dicen ***enteros algebraicos***; en general, para un anillo de enteros algebraicos, ser DFU equivale a ser DIP (esto no es trivial) y, por tanto, tal anillo debe ser íntegramente cerrado, y esta es la propiedad que los $\mathbb{Z}[n\gamma]$ carecen. (Está bien que, en una primera lectura, no entienda esta explicación; también está bien que el lector curioso la reciba de igual forma, aunque sea vaga y poco formal.) Para más detalles, vid. el primer capítulo de Janusz **[3]** o de Matsumura **[4].**

No obstante, el anillo $\mathbb{Z}[\sqrt{-5}]$ *sí* es íntegramente cerrado[1] y es por ello que es un ejemplo clásico en la teoría de números.

Quizá el estudiante note la relación entre álgebra abstracta y teoría de números que ya se hace notar. Esto no es coincidencia, varias de las nociones en álgebra (e.g., DIP y DFU) son abstracciones de fenómenos que ya se observan en $\mathbb{Z}$; por lo demás, los conceptos más avanzados que subyacen el contraejemplo del problema 7 (dígase, elemento entero y anillo íntegramente cerrado) fueron descubrimientos de teoristas de números alemanes (Dedekind, Kronecker, Gauss) que buscaban entender la aritmética en otros anillos. Cabe destacar que, del mismo modo que el análisis complejo facilita la teoría de integración real, la aritmética en anillos generales facilita la teoría de números sobre $\mathbb{Q}$ y $\mathbb{Z}$.

Referencias y lecturas adicionales

1. Andreescu, T. y Andrica, D. *Number Theory* (Birkhäuser, 2009).
2. Burton, D. M. *Elementary Number Theory* (McGraw-Hill, 1991).

[1] El lector puede pensar que no existe $\gamma \in \mathbb{C}$ con polinomio minimal a coeficientes enteros tal que $n\gamma = \sqrt{-5}$ con $|n| > 1$.

3. Janusz, G. J. *Algebraic Number Fields* 2.ª ed. *Graduate Studies in Mathematics* **7** (American Mathematical Society, 1973).
4. Matsumura, H. *Commutative Ring Theory* trad. por Reid, M. *Cambridge Studies in Advanced Mathematics* **8** (Cambridge University Press, 1986).

Correo electrónico: josecuevasbtos@uc.cl