Notas para el curso de Teoría de números

Programa del curso

A lo largo del curso, estudiaremos el problema de representar un número primo de la forma $x^2 + ny^2$ con x e y números enteros. Buscando darle respuesta a esta pregunta, nos encontraremos con dos temas que nos serán de ayuda: leyes de reciprocidad y formas cuadráticas binarias.

Comenzaremos estudiando propiedades básicas de los números enteros, como divisibilidad y la relación de congruencia que se puede derivar de ella, e introduciremos algunas estructuras algebraicas, como anillos conmutativos y grupos finitos; no estudiaremos estas estructuras en profundidad, pero nos servirán para formular y enmarcar varios de los resultados que se presentarán. Específicamente, usaremos las definiciones como nombres, para poder hablar de los anillos de enteros modulares $\mathbb{Z}/m\mathbb{Z}$, los anillos $\mathbb{Z}\left[\sqrt{-1}\right]$ y $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ y sus grupos de unidades (elementos inversibles).

Usando los conceptos introducidos, relacionaremos la ecuación $p = x^2 + ny^2$ con la Ley de reciprocidad cuadrática, uno de los resultados fundamentales de Teoría de números. Daremos algunas aplicaciones y veremos las limitaciones de esta herramienta.

Luego de demostrar este resultado, volveremos sobre el problema inicial y lo pondremos en el contexto más general de formas cuadráticas binarias. Estudiaremos, específicamente, formas cuadráticas definidas positivas, introduciendo los conceptos de equivalencia propia, clase y género de una forma cuadrática, composición y grupo de clases. Esta teoría nos permitirá dar una respuesta satisfactoria al problema en algunos casos especiales, pero dejará de manifiesto sus limitaciones.

La última parte del curso estará dedicada a las leyes de reciprocidad cúbica y bicuadrática, las cuales nos permitirán dar un paso más en la dirección de la resolución del problema.

Una respuesta completa a la pregunta de bajo qué condiciones la ecuación $p = x^2 + ny^2$ tiene solución (en $\mathbb{Z}$) viene dada de la mano de la Teoría de cuerpos de clases. No es el objetivo del curso entrar en ese tema, sino presentar los conceptos básicos para poder encarar temas más avanzados dentro del área.

Estas notas están basadas, principalmente, en dos referencias: los libros *Primes of the form* $x^2 + ny^2$ de David A. Cox [Cox22] y *A Classical Introduction to Modern Number Theory* de Kenneth Ireland y Michael Rosen [IR90]. El material que presentamos se puede encontrar en el capítulo 1, secciones 1 a 4 de [Cox22] y los capítulos 1 a 9 de [IR90]. Hemos incluido una gran cantidad de ejercicios, tomados de estas y otras referencias,

que exploran en mayor profundidad algunos de los temas que veremos, como también otros temas que se pueden abordar usando los conceptos desarrollados durante el curso.

Salvo talvez algunos puntos de la presentación, no hay, esencialmente, nada novedoso en estas notas. Ojalá las fallas y omisiones de estas notas no constituyan un obstáculo.

Les agradezco a Mariano y a Matías por darle una leída a las notas y por sus comentarios. Agradezco también a Gonzalo y a Gustavo, cuyas versiones del curso me han servido de guía.

Introducción

A mediados del siglo XVII, Pierre de Fermat realizaba observaciones como las siguientes: si p es un primo impar que

- excede en 1 un múltiplo de 4, entonces existen enteros x e y tales que $p = x^2 + y^2$;
- excede en 1 o 3 un múltiplo de 8, entonces existen enteros x e y tales que $p = x^2 + 2y^2$;
- excede en 1 un múltiplo de 3, entonces existen enteros x e y tales que $p = x^2 + 3y^2$.

En un lenguaje un poco más moderno, Fermat afirmaba que,

- si p es congruente con 1 módulo 4, entonces p es de la forma $x^2 + y^2$;
- si p es congruente con 1 o 3 módulo 8, entonces p es de la forma $x^2 + 2y^2$;
- si p es congruente con 1 módulo 3, entonces p es de la forma $x^2 + 3y^2$.

En general, se preguntaba, dado un entero n ¿qué primos p se pueden expresar en la forma $x^2 + ny^2$, con x e y enteros?

La primera persona de la que queda registro que intentó dar demostraciones de las observaciones de Fermat fue Leonhard Euler. Trabajando para alcanzar dicho objetivo, Euler descubrió lo que conocemos por el nombre de Ley de reciprocidad cuadrática. Si bien no logró demostrar este resultado, consiguió demostrar algunas de las afirmaciones de Fermat, como también formular algunas conjeturas similares propias cuando $n > 3$. Euler afirmaba, por ejemplo, que, si p es un primo impar, entonces

- p es de la forma $x^2 + 5y^2$, si y sólo si p es congruente con 1 o 9 módulo 20;
- p es de la forma $x^2 + 27y^2$, si y sólo si p es congruente con 1 módulo 3 y 2 es congruente con un cubo módulo p.

El siguiente avance vino de la mano de Joseph-Louis Lagrange, quien llevó adelante el estudio de formas cuadráticas definidas positivas. Lagrange introdujo los conceptos de forma reducida, número de clases, género de una forma cuadrática. Estas ideas permiten dar respuesta a las conjeturas de Euler para $n = 5$ y otros casos similares. Pero la teoría de géneros tiene sus limitaciones.

Se le atribuye a Adrien-Marie Legendre la introducción de ideas rudimentarias acerca de la composición de formas cuadráticas. Pero es Carl Friedrich Gauss quien establece la relación entre la teoría de géneros y composición de formas cuadráticas. De esta manera, Gauss muestra que en el conjunto de formas cuadráticas existe una estructura algebraica subyacente. En relación con este trabajo, Gauss demuestra la Ley de reciprocidad cuadrática y formula las leyes de reciprocidad cúbica y bicuadrática. Esto último permite dar respuesta a dos de los casos del problema de Fermat que las ideas anteriores no lograban alcanzar: los casos $n = 27$ y $n = 64$. Si bien este avance puede parecer

insignificante, resultó ser de gran relevancia, pues abrió el camino al estudio de leyes de reciprocidad de orden superior.

Para dar una idea del intervalo de tiempo en que ocurrieron estos avances, las observaciones de Fermat se pueden fechar alrededor del año 1640. Las demostraciones por parte de Euler de algunas de dichas afirmaciones consisten en dos partes: por un lado, profundizar una idea de Fermat, *descenso* y, por otro lado, *reciprocidad*. El trabajo de Euler abarca, aproximadamente, el período que va del año 1730 al año 1772; pasaron ya más de 130 años desde que Fermat primero estudió el problema de representar un primo como suma de dos cuadrados. La primera publicación de *Disquisitiones arithmeticae* de Gauss data del año 1801. En el interim, ocurrió el desarrollo de la teoría de formas cuadráticas por Lagrange y Legendre. En este sentido, mencionamos los trabajos *Recherches d'arithmétique*, de Lagrange (publicado entre 1773 y 1775), y *Théorie des nombres*, de Legendre (publicado en 1798 y cuya última versión es de 1830). En este trabajo, Legendre introduce el nombre de "forma cuadrática" para referirse a expresiones del tipo $ax^2 + bxy + cy^2$ y para distingurlas de las "formas lineales", del tipo $mx + a$.

Las fechas anteriores dan una aproximación del marco temporal en el que ocurrieron estos avances. Para más detalles, referimos a la introducción y la § 1 del libro de Cox [Cox22].

Parte I

Divisibilidad y congruencia

1 Divisibilidad

En el fondo, Teoría de números es el estudio de los números naturales –los números 1, 2, 3, ...– y sus propiedades.

Definición 1.1. Un número natural a *divide* a un número natural b, si existe un número natural c tal que $ac = b$; en tal caso, escribimos $a \mid b$.

Teorema 1.2 (Propiedades básicas de la división)**.** *Sean a, b y c números naturales (en particular $a, b, c > 0$). Entonces,*

(i) $a \mid b$ *implica* $a \mid bc$*;*

(ii) $a \mid b$ *y* $b \mid c$ *implican* $a \mid c$*;*

(iii) $a \mid b$ *y* $a \mid c$ *implican* $a \mid bx + cy$*, para todo par de números naturales x e y;*

(iv) $a \mid b$ *y* $b \mid a$ *implican* $a = b$*;*

(v) $a \mid b$ *implica* $a \leq b$*;*

(vi) $a \mid b$ *es equivalente a* $ma \mid mb$*, para todo natural m.*

Corolario 1.3. *Si b es un número natural ($\neq 0$), existe otro natural x tal que $x \nmid b$; si a es un natural y $a \neq 1$, existe otro natural x tal que $a \nmid x$.*

Teorema 1.4 (Algoritmo de división)**.** *Dados números naturales a y b, si $b \geq a$, entonces*

(A) $a \mid b$ *y existe un único natural q tal que $b = qa$, o bien*

(B) existen únicos naturales q y r tales que $b = qa + r$ y $1 \leq r < a$.

Demostración. El conjunto $\{b - ta : t \text{ natural}, ta \leq b\}$ es finito. Si $a \nmid b$, este conjunto está contenido en los naturales y, por lo tanto, tiene un primer elemento, r ($\neq 0$). Se cumple $r < a$ y $r = b - qa$ para cierto natural q. Si $b = qa + r = q_1 a + r_1$ con $1 \leq r, r_1 < a$, asumiendo $r < r_1$, se ve que $1 \leq r_1 - r < a$ y que $r_1 - r = (q_1 - q)a$ es divisible por a, contradiciendo (v) del Teorema 1.2. □

Definición 1.5. Dados naturales a, b y c, decimos que a es un *divisor común* de b y de c, si $a \mid b$ y $a \mid c$. El *máximo común divisor* de b y c, es el supremo de los divisores comunes de b y de c; escribimos (b, c) para denotar el máximo común divisor de b y c.

Observación 1.6. El conjunto de divisores de un natural es un conjunto finito. En particular, es finito el conjunto de divisores comunes de dos naturales y, por lo tanto, debe existir un elemento de valor absoluto máximo dentro de este conjunto; dicho elemento es único y ≥ 1.

Teorema 1.7 (Identidad de Bézout)**.** *Si $g = (b, c)$, existen* enteros *x e y tales que*

$$g \;=\; bx + cy \;.$$

Demostración. Sea $\mathcal{C}$ el conjunto de números enteros de la forma $bx+cy$, donde $x, y \in \mathbb{Z}$. Se cumple que $0 \in \mathcal{C}$ y que existe $l \in \mathcal{C}$ *positivo* y mínimo entre los elementos positivos de $\mathcal{C}$ **(ejercicio)**. Este elemento es un número natural, se escribe como $l = bx + cy$ para ciertos $x, y \in \mathbb{Z}$ y es $l \leq b, c$.

Veamos que $l \mid b$ que $l \mid c$. Si $l \nmid b$, por Algoritmo de división (Teorema 1.4), existirían (únicos) naturales q y r tales que $b = lq + r$, $1 \leq r < l$. Pero, entonces

$$r \;=\; b - lq \;=\; b - (bx + cy)q \;=\; b(1 - qx) + c(-yq)$$

pertenecería a $\mathcal{C}$, sería positivo y estrictamente menor que l, lo que es absurdo. Por lo tanto, $l \mid b$. Análogamente, $l \mid c$.

Por otro lado, si d es un divisor común de b y de c, entonces $d \mid bx + cy = l$ y $d \leq l$. En consecuencia, el máximo común divisor de b y c debe ser $g = l$. □

Corolario 1.8. *Sean b y c números naturales. Las siguientes propiedades sobre un número natural g son equivalentes:*

(a) g es el menor natural de la forma $bx + cy$ con $x, y \in \mathbb{Z}$;

(b) g es un divisor común de b y de c y es divisible por cualquier otro divisor común;

(c) g es el máximo común divisor de b y c.

Teorema 1.9 (Propiedades del máximo común divior)**.** *Sean a, b, c y d números naturales. Entonces,*

(i) $(ma, mb) = m\,(a, b)$, para todo natural m;

(ii) si $d \mid a$ y $d \mid b$, entonces $(a/d, b/d) = (a, b)\,/d$;

(iii) $(a, b) = (a, b - ax)$, para todo entero x tal que $ax < b$;

(iv) $(a, b) = (b, a)$;

(v) si $c \mid ab$ y $(b, c) = 1$, entonces $c \mid a$.

Observación 1.10. La propiedad (v) del Teorema 1.9 es equivalente a: si $b \mid A$, $c \mid A$ y $(b, c) = 1$, entonces $bc \mid A$.

Ejercicios

Ejercicio 1.1. Extender la relación de divisibilidad a los enteros y demostrar propiedades análogas. En particular, mostrar que existe un algoritmo de división correspondiente; probar que $a \mid b$, si y sólo si $r = 0$.[1]

Ejercicio 1.2. Dados naturales a y b, sea $\mathsf{r}_a(b)$ el resto de la división de b por a, es decir, a divide a $b - \mathsf{r}_a(b)$ y $0 \leq \mathsf{r}_a(b) < a$. Probar las siguientes propiedades de $\mathsf{r} = \mathsf{r}_a$:

(i) para todo natural b, $\mathsf{r}(\mathsf{r}(b)) = \mathsf{r}(b)$;

(ii) para todo par de naturales b y c, $\mathsf{r}(b + c) = \mathsf{r}(\mathsf{r}(b) + \mathsf{r}(c))$;

(iii) para todo par de naturales b y c, $\mathsf{r}(bc) = \mathsf{r}(\mathsf{r}(b)\mathsf{r}(c))$.

Ejercicio 1.3. Extender la noción de máximo común divisor a los enteros ¿Es cierto que todo par de enteros admite un máximo divisor común? Probar propiedades análogas. En particular, demostrar

(i) que, si $b, c \in \mathbb{Z}$ y $g = (b, c)$ denota el máximo común divisor, existen $x, y \in \mathbb{Z}$ tales que $g = bx + cy$;

(ii) que las caracterizaciones del Corolario 1.8 siguen siendo válidas;

(iii) que, dados $b, c \in \mathbb{Z}$, siempre que exista, $(b, c) = (b, -c) = (b, c + bx)$, para todo $x \in \mathbb{Z}$.

Ejercicio 1.4. Hallar el máximo común divisor de los siguientes pares de enteros y expresarlo como combinación lineal entera de ellos:

- 7469 y 2464,
- 2689 y 4001,
- 2947 y 3997,
- 1109 y 4999,
- 1819 y 3587.

Ejercicio 1.5 (Algoritmo de Euclides para hallar el máximo común divisor)**.** Dados $b, c \in \mathbb{Z}$, $c > 0$, se definen las sucesiones siguientes:

$$r_{-1} = b\ , \quad r_0 = c\ , \quad r_i = r_{i-2} - q_i r_{i-1}\ ,$$

si $i \geq 1$, de manera que $r_{i-1} = 0$ o bien $0 \leq r_i < r_{i-1}$, y, luego,

$$\begin{aligned} x_{-1} &= 1\ , \quad x_0 = 0\ , \quad x_i = x_{i-2} - q_i x_{i-1} \quad (\ i \geq 1\ ), \\ y_{-1} &= 0\ , \quad y_0 = 1\ , \quad y_i = y_{i-2} - q_i y_{i-1} \quad (\ i \geq 1\ ). \end{aligned}$$

Entonces, si j es tal que $r_{j+1} = 0$ y $r_j \neq 0$ (útimo resto no nulo), se cumple que

$$(b, c) = r_j = bx_j + cy_j\ .$$

[1] Hint: Si $a, b \in \mathbb{Z}$ y $a \neq 0$, existe un único par $q, r \in \mathbb{Z}$ tal que $b = qa + r$ y $0 \leq r < |a|$.

Ejercicio 1.6. Hallar, si existen, $x, y \in \mathbb{Z}$ tales que

- $423x + 198y = 9$,
- $71x - 50y = 1$,
- $43x + 64y = 1$,
- $93x - 81y = 3$,
- $6x + 10y + 15z = 1$.

Ejercicio 1.7. Probar que, dados $b, c \in \mathbb{Z}$, no ambos nulos, la ecuación $bx + cy = k$ tiene solución, si y sólo si $(b, c) \mid k$. Describir el conjunto solución.[2]

Ejercicio 1.8. Con $a, b, c, d, u, v, m, n \in \mathbb{Z}$, probar las siguientes afirmaciones:

(i) si $ad - bc \in \{\pm 1\}$, $u = am + bn$ y $v = cm + dn$, entonces $(u, v) = (m, n)$;

(ii) si $(u, v) = 1$, entonces $(u + v, u - v) \in \{1, 2\}$;

(iii) si $u = am + bn$ y $v = cm + dn$, entonces (u, v) divide al producto $(m, n)\ (ad - bc)$.

2 Primos

Definición 2.1. Un número natural $n > 1$ se dice *primo*, si no posee *divisores propios*, es decir, no existe número natural d que cumpla simultáneamente que $d \mid n$ y que $1 < d < n$.

Teorema 2.2. *Todo número natural $n > 1$ es producto de números primos.*

Demostración. No existen naturales entre 1 y 2. En particular, 2 es primo. Si $n > 2$, o bien n es primo, o bien posee divisores propios. Si $d \mid n$ y $1 < d < n$ es un divisor propio, el natural $m = n/d$ satisface $1 < m < n$ y $md = n$. Inductivamente, m y d son productos de primos y, por lo tanto, también lo es n. □

Definición 2.3. Si $n > 1$ no es primo, se dice que es *compuesto* (pues es producto de más de un factor primo).

Observación 2.4. Si a y p son números naturales y p es primo, entonces, o bien $p \mid a$, o bien $(a, p) = 1$, pues $g = (a, p)$, siendo un divisor de p (que es primo), es, o bien $g = 1$, o bien $g = p$.

Lema 2.5. *Si a, b y p son números naturales, p es primo y $p \mid ab$, entonces $p \mid a$, o bien $p \mid b$. Más en general, si $p \mid a_1 \cdots a_k$, entonces $p \mid a_i$ para algún i.*

Demostración. **(ejercicio)**.[3] □

[2] Hint: si (x, y) y (x_1, y_1) son soluciones, entonces $b'(x - x_1) + c'(y - y_1) = 0$, donde $b' = b/(b, c)$ y $c' = c/(b, c)$; notar que b' y c' son coprimos.

[3] Hint: Si $p \nmid a$, entonces existen $x, y \in \mathbb{Z}$ tales que $ax + py = 1$.

Observación 2.6. Recíprocamente, si un número natural $p > 1$ posee la propiedad siguiente:

$$\text{para todo par de números naturales } a \text{ y } b,\ p \mid ab \text{ imlpica que } p \mid a \text{ o } p \mid b,$$

entonces p es primo, pues, si $d \mid p$ es un divisor, se cumple que $1 \leq d \leq p$, luego $p = dm$, con lo que, aplicando la propiedad, o bien $p \mid d$, o bien $p \mid m$ y, por lo tanto,

- $p \mid d$ y $p = d$, por (iv) del Teorema 1.2 (y, así, $m = 1$), o bien
- $p \mid m$ y $m = np$ y, así, $p = dnp$, con lo que, cancelando, $dn = 1$ y $d = n = 1$.

Definición 2.7. Dado un natural $n > 1$, llamamos *factorización de n como producto de primos* a toda escritura de n como producto de factores primos únicamente (o, por abuso, primos a potencias).

Teorema 2.8 (Teorema fundamental de la Aritmética)**.** *Si $n > 1$ es un número natural, existe un única factorización de n como producto de primos, salvo por el orden de los factores.*

Demostración. Que todo natural $n > 1$ se puede expresar como producto de primos es la conclusión del Teorema 2.2. Lo que resta probar es que dicha factorización es única, a menos de intercambiar el orden de los factores. Precisamente, si

$$n = p_1 \cdots p_r \quad \text{y} \quad n = q_1 \cdots q_s$$

son dos factorizaciones de n como producto de primos, entonces $r = s$ y los factores primos distintos que aparecen son los mismos y la cantidad de veces que cada uno de ellos aparece es igual en ambas factorizaciones.

Igualando $p_1 \cdots p_r = q_1 \cdots q_s$ y cancelando factores que aparecen a ambos lados de la igualdad, podemos suponer que ningún p_i está entre los q_j y viceversa. Pero, si t es un primo que divide a n, entonces $t \mid p_{i_0}$ para algún i_0, con lo que $t = p_{i_0}$. Análogamente, $t = q_{j_0}$ para algún j_0. Como consecuencia, $p_{i_0} = q_{j_0}$, contradiciendo la suposición. □

Ejercicios

Ejercicio 2.1. Consideremos el subconjunto $\mathcal{P} \subset \mathbb{N}$ conformado por los números naturales pares. Dados $a, b \in \mathcal{P}$, el producto ab también pertenece a $\mathcal{P}$. Podemos, entonces, definir una noción de divisibilidad en $\mathcal{P}$: decimos que *a divide a b en $\mathcal{P}$*, si existe $c \in \mathcal{P}$ talque $ac = b$. Podemos, por lo tanto, hablar de primos en $\mathcal{P}$: un elemento $p \in \mathcal{P}$ es *primo en $\mathcal{P}$*, si no posee *divisores propios en $\mathcal{P}$*, es decir, si no existe $d \in \mathcal{P}$ tal que d divide a p en $\mathcal{P}$ y $d < p$. Con estas definiciones, probar que

(i) los elementos 2, 6, 10, 14, ... y 30 son primos en $\mathcal{P}$, pero que 4, 8, 12, 16, ... y 28 no lo son, son *compuestos en $\mathcal{P}$*;

(ii) todo elemento de $\mathcal{P}$ se puede escribir como producto de primos en $\mathcal{P}$;

(iii) existe un elemento de $\mathcal{P}$ que admite más de una factorización en primos de $\mathcal{P}$ (exhibir un ejemplo).

Ejercicio 2.2. Sea $A \subset \mathbb{C}$ el siguiente subconjunto de los números complejos:

$$A = \left\{x + y\sqrt{-6} : x, y \in \mathbb{Z}\right\} .$$

Probar que

(i) $\mathbb{Z} \subset A$;

(ii) si $\alpha, \beta \in A$, entonces $\alpha + \beta \in A$ y $\alpha\beta \in A$;

(iii) si $\alpha \in A$, su conjugado, $\bar{\alpha}$, también pertenece a A.

Podemos, entonces, hablar de divisibilidad en A: α *divide a* β *en* A, si existe $\gamma \in A$ tal que $\alpha\gamma = \beta$.

Dado $\alpha = x + y\sqrt{-6} \in A$, definimos su *norma* como

$$N(\alpha) = x^2 + 6y^2 .$$

Probar que

(i) si $\alpha \in A$, entonces $N(\alpha) \in \mathbb{Z}$;

(ii) para todo $\alpha \in A$, $N(\alpha) \geq 0$, $N(\alpha) = 0$, si y sólo si $\alpha = 0$ y $N(\alpha) = 1$, si y sólo si $\alpha = \pm 1$;[4]

(iii) si $\alpha \in A$, entonces $N(\alpha) = \alpha\bar{\alpha}$;

(iv) si $\alpha, \beta \in A$, entonces $N(\alpha\beta) = N(\alpha)N(\beta)$.

Con esto podemos definir una noción de divisor propio A: decimos que α *divide propiamente a* β *en* A, si α divide a β en A y $N(\alpha) > 1$.

Un elemento $\gamma \in A$ es *primo en* A, si $N(\gamma) > 1$ y γ no posee divisores propios en A. Probar que

(i) 2 y 5 son primos en A;

(ii) todo elemento de A se puede escribir como producto de primos en A;

(iii) existe un elemento de A que admite más de una factorización en primos de A (exhibir un ejemplo);

(iv) $2 + \sqrt{-6}$ y $2 - \sqrt{-6}$ son primos en A.

Ejercicio 2.3. En este ejercicio veremos otra demostración del Teorema fundamental de la Aritmética (Teorema 2.8). Supongamos que el resultado es falso y sea n el menor natural para el cual existen dos factorizaciones distintas: $n = p_1 \cdots p_r = q_1 \cdots q_s$, donde los factores primos p_i no son los mismos que los q_j. Mostrar que

[4] En cualquier otro caso, $N(\alpha) > 1$.

(i) r y s son ambos > 1 y *ningún* p_i es igual a un q_j;[5]

(ii) si $p_1 < q_1$, entonces $N := (q_1 - p_1)q_2 \cdots q_r$ es $< n$;

(iii) el número natural N definido en (ii) satisface $N = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$;

(iv) N admite dos factorizaciones distintas, contradiciendo la minimalidad de n.

Ejercicio 2.4. La cantidad de números primos es infinita.[6]

Ejercicio 2.5. Fijado un entero positivo k, existen k números naturales compuestos consecutivos.[7]

Ejercicio 2.6. La sumatoria sobre los recíprocos de los primos diverge. Específicamente, dado $y \geq 2$, la sumatoria

$$\sum_{p \leq y} \frac{1}{p} > \log\log y - 1 \ . \tag{1}$$

En particular, hay infinitos primos. Separamos la demostración en distintos pasos:

(i) probar que, si $\mathcal{N}$ denota el conjunto de naturales n en cuya factorización sólo aparecen primos $p \leq y$, entonces[8]

$$\prod_{p \leq y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \sum_{n \in \mathcal{N}} \frac{1}{n} \ ;$$

(ii) probar que, si $n \leq y$, entonces $n \in \mathcal{N}$ y los sumandos de $\sum_{n \leq y} \frac{1}{n}$ son sumandos de $\sum_{n \in \mathcal{N}} \frac{1}{n}$;

(iii) probar que, si N es el mayor entero $\leq y$, entonces

$$\sum_{n=1}^{N} \frac{1}{n} \geq \int_1^{N+1} \frac{dx}{x} = \log(N+1) > \log y \ ;$$

(iv) deducir de (iii) que

$$\prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1} > \log y \ ;$$

(v) usando la desigualdad $e^{v+v^2} \geq (1-v)^{-1}$, probar que

$$\sum_{p \leq y} \frac{1}{p} + \sum_{p \leq y} \frac{1}{p^2} > \log\log y \ ;$$

[5] Hint: Para esto último, usar la minimalidad de n.

[6] Hint: Talvez la demostración más común de esto sea: asumir que la cantidad de primos es finita, $p_1, \ldots, p_k$ y considerar $n := 1 + p_1 \cdots p_k$.

[7] Hint: Si $2 \leq j \leq k+1$, entonces $j \mid (k+1)! + j$.

[8] La suma de las potencias de $1/p$, p primo converge absolutamente, con lo que no hay problema en la definición del producto (finito) sobre los primos $p \leq y$.

(vi) notar que $\sum_{p \leq y} \frac{1}{p^2} < 1$;[9]

(vii) deducir la desigualdad (1).

Ejercicio 2.7. Probar que

- todo entero de la forma $3k + 2$ tiene un factor primo del mismo tipo;
- todo entero de la forma $4k + 3$ tiene un factor primo del mismo tipo;
- todo entero de la forma $6k + 5$ tiene un factor primo del mismo tipo.

Ejercicio 2.8. Si $n > 4$ es compuesto, entonces $n \mid (n-1)!$.

Ejercicio 2.9. Sea $p > 1$ un primo. Dado $n \in \mathbb{Z}$, $n \neq 0$, el *orden de n en p* es el número entero no negativo $v_p(n) = j$ que cumple $p^j \mid n$ pero $p^{j+1} \nmid n$. Probar que, si $a, b \in \mathbb{Z}$,

- $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ y que, si $v_p(a) \neq v_p(b)$, entonces vale $=$;
- $v_p(ab) = v_p(a) + v_p(b)$ y la función v_p se extiende a $\mathbb{Q} \setminus \{0\}$ de una única manera posible de forma que esta igualdad valga para $a, b \in \mathbb{Q} \setminus \{0\}$.

Ejercicio 2.10. Sean $a, b, c, d \in \mathbb{Z}$ tales que $(a, b) = (c, d) = 1$. Si $\frac{a}{b} + \frac{c}{d} \in \mathbb{Z}$, entonces $b = \pm d$.

Ejercicio 2.11. Sean $a, b, m \in \mathbb{N}$, $(a, b) = 1$.

(i) Si $ab = m^2$, entonces a y b son cuadrados perfectos.

(ii) Si $ab = m^3$, entonces a y b son cubos perfectos.

Ejercicio 2.12. Sea $a \in \mathbb{Q} \setminus \{0\}$. Probar que a se puede escribir de una única manera como $a = m^2 n$, donde $m \in \mathbb{Q}$ y $n \in \mathbb{Z}$ es libre de cuadrados.

Ejercicio 2.13. La ecuación $x^2 + y^2 = 3$ no tiene soluciones con $x, y \in \mathbb{Q}$.

(i) Probar que la resolubilidad de $x^2 + y^2 = 3$ con $x, y \in \mathbb{Q}$ equivale a la resolubilidad de $a^2 + b^2 = 3c^2$, donde $a, b, c \in \mathbb{Z}$.

(ii) Probar que, si $a, b, c \in \mathbb{Z}$ forman una solución de $a^2 + b^2 = 3c^2$, entonces hay una solución con a, b y c sin divisores en común (común a los tres enteros). Decimos que una solución con a, b y c sin divisores es *primitiva*.

(iii) Probar que, si $a, b \in \mathbb{Z}$, entonces $3 \mid a^2 + b^2$ ocurre si y sólo si $3 \mid a$ y $3 \mid b$.

(iv) Probar que, si a, b, c es solución de $a^2 + b^2 + 3c^2$, entonces $3 \mid c$.

Concluir que $a^2 + b^2 = 3c^2$ no tiene soluciones con $a, b, c \in \mathbb{Z}$ y, por lo tanto, que $x^2 + y^2 = 3$ no tiene soluciones con $x, y \in \mathbb{Q}$.

[9] Hint: Usando el criterio de comparación ($\sum_{n \geq 2} \frac{1}{n}$) y el criterio integral ($\int_1^\infty \frac{dx}{x^2} = 1$), por ejemplo.

3 Congruencias

Ejemplo 3.1. La ecuación $x^2 - 117x + 31 = 0$ no tiene soluciones enteras. Deben haber varias maneras de probar esto. Una de ellas es notar que 31 es primo y que, en consecuencia, si x fuese solución, entonces $x \in \{1, 31\}$, pero ninguno de estos números es una solución ¿Qué hubiese pasado con $x^2 - 117x + 2^{136.279.841} - 1$? ¿Es $2^{136.279.841} - 1$ primo? Si lo es, parece razonable que la ecuación no tenga solución en $\mathbb{Z}$ ¿Si no lo fuese? Veamos una prueba alternativa de que no tiene solución. Calculando algunos valores del polinomio $f(x) = x^2 - 117x + 31$, se puede ver que todos los resultados que se obtienen son impares. Probemos, entonces, que $f(x)$ siempre es impar, si $x \in \mathbb{Z}$ (en particular, $f(x)$ nunca será cero, en ese caso). Para que $f(x)$ sea par, $x^2 - 117x = (x - 117)\, x$ debería ser impar, porque 31 es impar. En particular, x debería ser impar y $x - 117$ también. Pero, si x es impar, $x - 117$ es par. Absurdo.

Definición 3.2. Dados enteros a, b y m, $m \neq 0$, se dice que *a es congruente a b módulo m*, si m divide a $b - a$; expresamos esta condición por $a \equiv b \,(\mathsf{mod}\, m)$.

Ejemplo 3.3. -17 y 5 son congruentes módulo 11, pues $-17 - 5 = -22$, que es múltiplo de 11. Es decir, $-17 \equiv 5 \,(\mathsf{mod}\, 11)$.

Ejemplo 3.4. Se cumple que $-117 \equiv 1 \,(\mathsf{mod}\, 2)$, $31 \equiv 1 \,(\mathsf{mod}\, 2)$ y $-117 \equiv 31 \,(\mathsf{mod}\, 2)$. También es cierto que $-117 \not\equiv 0 \,(\mathsf{mod}\, 2)$, $31 \not\equiv 0 \,(\mathsf{mod}\, 2)$ y que $1 \not\equiv 0 \,(\mathsf{mod}\, 2)$. Por otro lado, $-117 + 31 \equiv 0 \,(\mathsf{mod}\, 2)$ y $(-117)\, 31 \equiv 1 \,(\mathsf{mod}\, 2)$.

Teorema 3.5. *La condición $a \equiv b \,(\mathsf{mod}\, m)$ determina, fijado m, una relación de equivalencia en $\mathbb{Z}$. Esta relación cumple, además, que*

$$a \equiv c \,(\mathsf{mod}\, m) \quad y \quad b \equiv d \,(\mathsf{mod}\, m)$$

implican

$$ab \equiv cd \,(\mathsf{mod}\, m) \quad y, \text{ también,} \quad a + b \equiv c + d \,(\mathsf{mod}\, m)\ .$$

Definición 3.6. Dado $m \in \mathbb{Z}$, $m \neq 0$, las clases de equivalencia en $\mathbb{Z}$ determinadas por $a \equiv b \,(\mathsf{mod}\, m)$ se denominan *clases de congruencia módulo m* y, a la relación, *relación de congruencia (módulo m).*

Ejemplo 3.7. Las clases de congruencia módulo 2 separan a los enteros entre pares, $a \equiv 0 \,(\mathsf{mod}\, 2)$, e impares, $a \equiv 1 \,(\mathsf{mod}\, 2)$. Los enteros 0 y 1 representan cada una de las clases de congruencia módulo 2; los enteros 2 y 3, también representan ambas clases de congruencia. Mientras que 0 y 3 representan clases distintas (y, por lo tanto, disjuntas), 0 y 2 representan la misma clase.

Ejemplo 3.8. Las clases de congruencia módulo 3 separan a los enteros entre aquellos cuyo resto de dividir por 3 es 0, 1 o bien 2: si $a \equiv b \,(\mathsf{mod}\, 3)$, entonces 3 divide a la diferencia $a - b$; si $a = 3k + r$ y $b = 3l + s$, entonces $a - b = 3\,(k - l) + (r - s)$, o sea, 3 divide a $a - b$, si y sólo si 3 divide a $r - s$. Entonces, las clases están representandas por los enteros 0, 1 y 2, que además representan clases distintas; también están representadas por -1, 0 y 1, es decir, todo entero es congruente módulo 3 a alguno de ellos (y, en este caso también, a exactamente uno de ellos).

Definición 3.9. Un *sistema de representantes módulo m* (o, también, *sistema completo de representantes*) es un subconjunto $R \subset \mathbb{Z}$ tal que todo entero sea congruente a un único elemento de R, es decir,

(i) si $x \in \mathbb{Z}$, existe $r \in R$ tal que $x \equiv r \,(\mathsf{mod}\, m)$ y

(ii) si $r, r' \in R$ y $r \neq r'$, entonces $r \not\equiv r' \,(\mathsf{mod}\, m)$.

Ejemplo 3.10. Con $m = 7$, un sistema completo de representantes es el de restos de la división por 7: $\{0, 1, 2, 3, 4, 5, 6\}$. Otro sistema completo de representantes es $\{0, 1, 2, 3, -3, -2, -1\}$. Incluso otro puede ser $\{-28, 50, 16, -4, 18, -30, -8\}$. Notemos que en este último ejemplo, todos los enteros del sistema de representantes son pares.[10]

Teorema 3.11. *Dado $m \in \mathbb{Z}$, $m \neq 0$, la relación de congruencia módulo m divide a $\mathbb{Z}$ en $|m|$ clases. Un sistema de representantes está dado por los $|m|$ restos de la división por m. En particular, todos los sistemas completos de representantes tienen el mismo cardinal, $|m|$.*

Demostración. $a \equiv b \,(\mathsf{mod}\, m)$, si y sólo si $\mathsf{r}_m(a) = \mathsf{r}_m(b)$. □

Ejemplo 3.12. Si $x \in \mathbb{Z}$,

$$x^2 - 117x + 31 \equiv x^2 + x + 1 \pmod 2 \,,$$

que es impar, es decir, congruente con 1 módulo 2, tanto si x es par ($x \equiv 0 \,(\mathsf{mod}\, 2)$), como si x es impar ($x \equiv 1 \,(\mathsf{mod}\, 2)$). Los polinomios $3x^2 + 3x + 1$ y $3x^3 + x^2 + 3x + 4$ tampoco tienen raíces enteras. En el primer caso, para todo x,

$$3x^2 + 3x + 1 \equiv 1 \pmod 3 \,.$$

En el segundo,

$$3x^3 + x^2 + 3x + 4 \equiv x^2 + 1 \pmod 3 \,.$$

Si $x \equiv 0 \,(\mathsf{mod}\, 3)$, entonces $x^2 + 1 \equiv 1 \,(\mathsf{mod}\, 3)$. Si, en cambio, $x \equiv 1 \,(\mathsf{mod}\, 3)$, entonces $x^2 + 1 \equiv 2 \,(\mathsf{mod}\, 3)$. Y, si $x \equiv 2 \,(\mathsf{mod}\, 3)$, entonces $x^2 + 1 \equiv 5 \equiv 2 \,(\mathsf{mod}\, 3)$. Con lo que el resultado siempre es congruente a 1 o a 2 módulo 3; nunca es congruente a 0.

Definición 3.13. La *cantidad de soluciones módulo m* a una ecuación es la cantidad de clases de congruencia módulo m que hacen que la ecuación se verifique módulo m.

Ejemplo 3.14. La ecuación $f(x) := x^2 - 117x + 31 = 0$ no tiene soluciones módulo 2; tampoco tiene soluciones módulo 3. Pero tiene una solución módulo 5: $f(1) = -115 \equiv 0 \,(\mathsf{mod}\, 5)$. De hecho,

$$x^2 - 117x + 31 \equiv x^2 - 2x + 1 \pmod 5 \,,$$

de donde se puede verificar que $x^2 - 2x + 1 \equiv 0 \,(\mathsf{mod}\, 5)$, sólo si $x \equiv 1 \,(\mathsf{mod}\, 5)$.[11] Esto quiere decir que hay una única solución módulo 5.

[10] Ver Ejercicio 3.8.

[11] $x^2 - 2x + 1 = (x - 1)^2$.

Definición 3.15. Un *sistema reducido de representantes módulo m* es un subconjunto $R \subset \mathbb{Z}$ cuyos elementos son coprimos con m y tal que todo entero *coprimo con* m sea congruente a un único elemento de R, es decir,

(i) si $r \in R$, entonces $(r, m) = 1$,

(ii) si $x \in \mathbb{Z}$ y $(x, m) = 1$, existe $r \in R$ tal que $x \equiv r \pmod{m}$ y

(iii) si $r, r' \in R$ y $r \neq r'$, entonces $r \not\equiv r' \pmod{m}$.

Ejemplo 3.16. En el Ejemplo 3.10 vimos que $\{0, 1, 2, 3, 4, 5, 6\}$, $\{0, 1, 2, 3, -3, -2, -1\}$ y $\{-28, 50, 16, -4, 18, -30, -8\}$ son sistemas completos de representantes de las clases módulo 7. A partir de ellos, podemos conseguir sistemas reducidos de representantes de las clases quitando aquellos elementos divisibles por 7: los conjuntos $\{1, 2, 3, 4, 5, 6\}$, $\{1, 2, 3, -3, -2, -1\}$ y $\{50, 16, -4, 18, -30, -8\}$ son sistemas reducidos de representantes módulo 7.

Ejemplo 3.17. Con $m = 21$, un sistema completo de representantes es el de los restos:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\} .$$

Un sistema reducido de representantes se obtiene quitando aquellos enteros que no son coprimos con 21, es decir, divisibles por 3 o por 7:

$$\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\} .$$

Otro sistema reducido de representantes es:

$$\{1, 2, 4, 5, 8, 10, -10, -8, -5, -4, -2, -1\} .$$

El siguiente conjunto también es un sistema reducido de representantes y cumple que todos sus elementos son pares:

$$\{22, 2, 4, 26, 8, 10, -10, -8, 16, -4, -2, 20\} .$$

También el conjunto

$$\{1, -19, 46, 26, -34, 31, 11, -29, 16, -4, 61, 41\}$$

es un sistema reducido de representantes de las clases módulo 21 y cumple que todos sus elementos son $\equiv 1 \pmod{5}$.[12]

Teorema 3.18. *Todos los sistemas reducidos de representantes tienen el mismo cardinal.*

Demostración. Este resultado es consecuencia de las dos propiedades siguientes **(ejercicio)**:

[12] Ver Ejercicio 3.8.

- si $b \equiv c \,(\mathsf{mod}\, m)$, entonces $(b, m) = (c, m)$ y
- todo sistema reducido se puede completar a un sistema completo de representantes.

□

Definición 3.19. El cardinal de un sistema reducido de representantes se denota por $\varphi(m)$; la función $m \in \mathbb{Z} \smallsetminus \{0\} \mapsto \varphi(m) \in \mathbb{N}$ se llama *función de Euler*.

Corolario 3.20. $\varphi(m) = \#\{1 \leq t \leq m \,:\, (t, m) = 1\}$.

Ejemplo 3.21. Según lo visto en el Ejemplo 3.16, $\varphi(7) = 6$.

Ejemplo 3.22. Según lo visto en el Ejemplo 3.17, $\varphi(21) = 12$.

Teorema 3.23. *Si* $(a, m) = 1$, *entonces* $a^{\varphi(m)} \equiv 1 \,(\mathsf{mod}\, m)$.

Demostración. Sea $R = \{r_1, \ldots, r_{\varphi(m)}\}$ un sistema reducido módulo m. Entonces, si $(a, m) = 1$, el conjunto $\{ar_1, \ldots, ar_{\varphi(m)}\}$ *también* es un sistema reducido (*). Así, para cada i, $1 \leq i \leq \varphi(m)$, existe un único $j = j(i)$, $1 \leq j \leq \varphi(m)$, tal que $r_i \equiv ar_j \,(\mathsf{mod}\, m)$. Además, si $i \neq i'$, entonces $j(i) \neq j(i')$ (*). En consecuencia,

$$\prod_{j=1}^{\varphi(m)} ar_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m} \,. \tag{2}$$

Pero

$$\prod_{j=1}^{\varphi(m)} ar_j = a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \,. \tag{3}$$

De (2) y de (3) se deduce que $a^{\varphi(m)} \equiv 1 \,(\mathsf{mod}\, m)$ (*). □

En la demostración del Teorema 3.23, las afirmaciones marcadas con (*) son consecuencias del siguiente resultado.

Lema 3.24. *Si* $(b, m) = 1$ *y* $bx \equiv by \,(\mathsf{mod}\, m)$, *entonces* $x \equiv y \,(\mathsf{mod}\, m)$.

Demostración. **(ejercicio)**. □

Ejercicios

Ejercicio 3.1. Si $f \in \mathbb{Z}[X]$ y $f(0) \equiv f(1) \equiv 1 \,(\mathsf{mod}\, 2)$, entonces f no tiene raíces enteras. Generalizar.

Ejercicio 3.2. Probar que la ecuación $3x^2 + 2 = y^2$ no tiene soluciones con $x, y \in \mathbb{Z}$.

Ejercicio 3.3. Probar que la ecuación $7x^3 + 2 = y^3$ no tiene soluciones con $x, y \in \mathbb{Z}$.

Ejercicio 3.4. Probar que la ecuación $x^2 - 117x + 31 = 0$ no tiene soluciones módulo 117. Investigar la ecuación módulo m para valores de m hasta ...; confeccionar una tabla. Mirar módulo $m \leq 30$, al menos, módulo 85, 115, 391 y 2713.

Ejercicio 3.5. ¿Existen $x \in \mathbb{Z}$ tales que $x^2 \equiv -1 \pmod{17}$? ¿$x^3 \equiv 2 \pmod{17}$? Hallar un sistema reducido módulo 17 cuyos elementos sean múltiplos de 3.

Ejercicio 3.6. Determinar $\varphi(26)$. Para cada x en el rango $0 \leq x \leq 25$ (un sistema completo), determinar el menor natural k ($k \geq 1$) tal que $x^k \equiv 1 \pmod{26}$. Repetir con 36 en lugar de 26 (y 35 en lugar de 25) ¿Qué relación hay entre estos exponentes y los valores de $\varphi(26)$ y de $\varphi(36)$, respectivamente?

Ejercicio 3.7. Probar que $19 \nmid 4n^2 + 4$ para ningún n natural.

Ejercicio 3.8. Hallar sistemas de representantes de las clases módulo 26 cuyos elementos sean:

(i) todos divisibles por 7;

(ii) congruentes con 1 módulo 3 y congruentes con 1 módulo 5

¿Es posible hallar un sistema de representantes que cumpla simultáneamente (i) y (ii)?

Ejercicio 3.9. Si $f \in \mathbb{Z}[X]$ y $a \equiv b \pmod{m}$, entonces $f(a) \equiv f(b) \pmod{m}$.

Ejercicio 3.10. Si $d \mid m$ y $a \equiv b \pmod{m}$, entonces $a \equiv b \pmod{d}$.

Ejercicio 3.11. Sea $g = (a, m)$. La congruencia $ax \equiv b \pmod{m}$ tiene solución $x \in \mathbb{Z}$, si y sólo si $g \mid b$. En tal caso, hay exactamente g soluciones (módulo m): si x e y son soluciones, entonces $x \equiv y \pmod{m/g}$.

Ejercicio 3.12. Dados $a, m \in \mathbb{Z}$, $m \neq 0$, se cumple $ax \equiv ay \pmod{m}$, si y sólo si $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Ejercicio 3.13. Si $d \mid m$ y si $a \equiv b \pmod{d}$, entonces $a \equiv b + kd \pmod{m}$, para un único k en el rango $1 \leq k \leq m/d$.

Ejercicio 3.14. Si p es primo, $(a, p) = 1$ equivale a $a \not\equiv 0 \pmod{p}$.

4 Ecuaciones lineales

5 El Teorema chino del resto

De la sección § 3, sabemos que una ecuación $ax \equiv b \pmod{m}$ tiene solución, si y sólo si $(a, m) \mid b$. Tales ecuaciones imponen una restricción a la clase de congruencia de x módulo m ¿Qué podemos decir si tenemos varias de tales restricciones en simultáneo?

Ejemplo 5.1. ¿Existe algún $x \in \mathbb{Z}$ tal que $x \equiv 5 \pmod{7}$ y $x \equiv 7 \pmod{11}$? El conjunto de enteros que son soluciones a ambas ecuaciones de manera simultánea el de enteros de resto 5 al dividir por 7 y de resto 7 al dividir por 11. Para encontrar una solución, podemos empezar por las soluciones a una de las dos ecuaciones, $x \equiv 5 \pmod{7}$, por

u	0	1	2	3	4	5	6	7	8	9	10	11
$x = 5 + 7u$	5	12	19	26	33	40	47	54	61	68	75	82
$\mathsf{r}_{11}(x)$	5	1	8	4	0	7	3	10	6	2	9	5

Tabla 1: Algunos enteros $5 + 7u$, $u \in \mathbb{Z}$, y sus restos de dividir por 11.

ejemplo, y buscar, dentro de este conjunto, un entero que también satisfaga la otra ecuación, $x \equiv 7 \,(\mathsf{mod}\, 11)$:

$$\left\{x \in \mathbb{Z} \,:\, x \equiv 5 \,(\mathsf{mod}\, 7)\right\} \supset \left\{x \in \mathbb{Z} \,:\, x \equiv 5 \,(\mathsf{mod}\, 7) \text{ y } x \equiv 7 \,(\mathsf{mod}\, 11)\right\} .$$

Las soluciones a la ecuación módulo 7 son exactamente los enteros que tienen resto 5 al dividir por 7: $x = 5 + 7u$, $u \in \mathbb{Z}$. Calculemos los primeros con $u \geq 0$ y su resto al dividir por 11. Podemos ver los resultados en la Tabla 1. A partir de $u = 11$, los restos se empezarán a repetir. El menor entero positivo que es solución es $x = 40$. Toda otra solución es congruente con 40 módulo 77.

Ejemplo 5.2. Veamos otra manera de llegar a la solución del Ejemplo 5.1. Sabemos que todo $x \in \mathbb{Z}$ que cumpla simultáneamente $x \equiv 5 \,(\mathsf{mod}\, 7)$ y $x \equiv 7 \,(\mathsf{mod}\, 11)$ debe ser, por la primera condición, de la forma $x = 5 + 7u$, $u \in \mathbb{Z}$. Reemplazando esta expresión en la segunda congruencia, obtenemos una condición para u:

$$5 + 7u \equiv 7 \pmod{11} .$$

Podemos intentar despejar u, o, mejor, su clase de congruencia. Por un lado, la congruencia anterior es equivalente a

$$7u \equiv 2 \pmod{11} .$$

Falta despejar el 7. Ahora,

$$7 \cdot 3 = 21 \equiv -1 \,(\mathsf{mod}\, 11) \quad \text{y} \quad 7\,(-3) \equiv 1 \,(\mathsf{mod}\, 11) .$$

Pero entonces,

$$u \equiv (-3)\,2 = -6 \pmod{11} .$$

En definitiva, las soluciones simultáneas a las congruencias módulo 7 y módulo 11 son $x = 5 + 7u$ con $u \equiv -6 \,(\mathsf{mod}\, 11)$, o sea, $u = -6 + 11k$, $k \in \mathbb{Z}$. Es decir, el conjunto solución es:

$$\left\{x = 5 + 77k \,:\, k \in \mathbb{Z}\right\} .$$

Notamos que $-6 \equiv 5 \,(\mathsf{mod}\, 11)$, con lo cual, esto coincide con lo que dedujimos de la Tabla 1.

Observación 5.3. Para poder resolver el sistema de congruencias con el método del Ejemplo 5.2, usamos el hecho de que $7\,(-3) \equiv 1 \,(\mathsf{mod}\, 11)$, es decir, que la ecuación $7b \equiv 1 \,(\mathsf{mod}\, 11)$ admite solución. Esto es coherente con que $(7, 11) = 1$. Por otro lado, podríamos preguntarnos qué nos garantizaba que, con el método del Ejemplo 5.1, íbamos a encontrar una solución (¿Y qué nos garantiza que los posibles restos que aparecieron en la tabla iban a ser una cantidad finita?)

Teorema 5.4 (Teorema chino del resto)**.** *Sean m_1, $m_2 \in \mathbb{Z}$ tales que $(m_1, m_2) = 1$. Entonces, para todo par a_1, $a_2 \in \mathbb{Z}$, existe una solución común x al sistema de ecuaciones de congruencia*

$$x \equiv a_1 \,(\mathsf{mod}\, m_1) \quad y \quad x \equiv a_2 \,(\mathsf{mod}\, m_2)\ .$$

Además, el conjunto de todas las soluciones comunes a ambas ecuaciones es igual a una clase de congruencia módulo el producto $m_1 m_2$.

En el Ejercicio 5.1 se puede encontrar una variante de este enunciado.

Observación 5.5. Dicho de otra manera, según el Teorema 5.4, si $(m_1, m_2) = 1$, entonces:

- existe $x \in \mathbb{Z}$ que cumple $x \equiv a_1 \,(\mathsf{mod}\, m_1)$ y $x \equiv a_2 \,(\mathsf{mod}\, m_2)$,
- toda la clase de congruencia de x módulo $m_1 m_2$ es solución: si $y \equiv x \,(\mathsf{mod}\, m_1 m_2)$, entonces y también es solución (satisface ambas condiciones) y
- dicho entero es único módulo $m_1 m_2$: si y es solución, entonces $y \equiv x \,(\mathsf{mod}\, m_1 m_2)$.

En una sola frase, existe una solución y dicha solución es única módulo $m = m_1 m_2$.

Demostración. Las soluciones a la congruencia $x \equiv a_1 \,(\mathsf{mod}\, m_1)$ son los enteros de la forma $x = a_1 + m_1 u$, $u \in \mathbb{Z}$. Reemplazando esta expresión en la congruencia $x \equiv a_2 \,(\mathsf{mod}\, m_2)$ obtenemos que x es una solución simultánea, si y sólo si

- x es de la forma $x = a_1 + m_1 u$, $u \in \mathbb{Z}$, y
- $a_1 + m_1 u \equiv a_2 \,(\mathsf{mod}\, m_2)$.

Ahora, la congruencia $a_1 + m_1 u \equiv a_2 \,(\mathsf{mod}\, m_2)$ admite solución u; las soluciones son exactamente los enteros u que cumplen

$$m_1 u \equiv a_2 - a_1 \quad (\mathsf{mod}\, m_2)\ .$$

Pero esta congruencia admite solución, dado que estamos asumiendo $(m_1, m_2) = 1$. Para describir las soluciones, notamos que, si $b \in \mathbb{Z}$ es tal que $b m_1 \equiv 1 \,(\mathsf{mod}\, m_2)$ –que tal entero exista está garantizado justamente por la condicón de coprimalidad–, entonces la condición sobre u es equivalente a:

$$u \equiv b\,(a_2 - a_1) \quad (\mathsf{mod}\, m_2)\ ,$$

o sea, $u = b\,(a_2 - a_1) + m_2 k$, $k \in \mathbb{Z}$. En definitiva, las soluciones simultáneas a ambas congruencias son los enteros de la forma

$$x = a_1 + m_1 b\,(a_2 - a_1) + m_1 m_2 k$$

con $k \in \mathbb{Z}$. En particular, $x = a_1 + m_1 b\,(a_2 - a_1)$ es solución simultánea.

Si $y \equiv x \,(\mathsf{mod}\, m)$, entonces $y \equiv x \,(\mathsf{mod}\, m_1)$ y también $y \equiv x \,(\mathsf{mod}\, m_2)$. Con lo cual, toda la clase de congruencia de x módulo $m = m_1 m_2$ es solución simultánea. Si, por otro lado, $y \in \mathbb{Z}$ es solución simultánea, entonces

$$y \;\equiv\; a_1 \;\equiv\; x \,(\mathsf{mod}\, m_1) \quad \text{e} \quad y \;\equiv\; a_2 \;\equiv\; x \,(\mathsf{mod}\, m_2)\;,$$

es decir, $m_1 \mid y - x$ y también $m_2 \mid y - x$. Como $(m_1, m_2) = 1$, se deduce que $m = m_1 m_2 \mid y - x$ y que $y \equiv x \,(\mathsf{mod}\, m)$. O sea que toda solución debe pertenecer a la clase de x módulo m. □

Si los módulos no son coprimos *podría no* existir solución.

Ejemplo 5.6. Las congruencias $x \equiv 29 \,(\mathsf{mod}\, 52)$ y $x \equiv 19 \,(\mathsf{mod}\, 72)$ no tienen soluciones en común. En este caso, $(52, 72) = 4$ y las toda solución común a estas congruencias debe satisfacer

$$x \;\equiv\; 29 \,(\mathsf{mod}\, 4) \quad \text{y} \quad x \;\equiv\; 19 \,(\mathsf{mod}\, 4)\;.$$

Pero $29 \equiv 1 \,(\mathsf{mod}\, 4)$, mientras que $19 \equiv 3 \,(\mathsf{mod}\, 4)$. En particular, las condiciones sobre x son inconsistentes.

Corolario 5.7. *Sean m y n enteros coprimos. Entonces, $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demostración. Sean R, S y T sistemas completos de representantes de las clases módulo m, n y mn, respectivamente. Podemos tomar, por ejemplo, los conjuntos $R = \{1,\, 2,\, \ldots,\, m\}$, etc. Por el Teorema 5.4, hay una biyección

$$T \;\simeq\; R \,\times\, S \tag{4}$$

dada por $t \mapsto (r, s)$, donde $r \in R$ y $s \in S$ son los representantes tales que $t \equiv r \,(\mathsf{mod}\, m)$ y $t \equiv s \,(\mathsf{mod}\, n)$: la sobreyectividad se deduce de que, como $(m, n) = 1$, las congruencias $x \equiv r \,(\mathsf{mod}\, m)$ y $x \equiv s \,(\mathsf{mod}\, n)$ admiten una solución común, mientras que la inyectividad se deduce de que toda solución simultánea pertenece a la misma clase módulo mn.

Ahora, sean R', S' y T' los sistemas reducidos de representantes obtenidos a partir de R, de S y de T, respectivamente. Vamos a ver que la biyección (4) determina una biyección

$$T' \;\simeq\; R' \,\times\, S'\;.$$

Como $(m, n) = 1$, se cumple que

$$(x, mn) \;=\; (x, m)\;(x, n) \tag{5}$$

para todo $x \in \mathbb{Z}$. En particular, $(x, mn) = 1$, si y sólo si $(x, m) = (x, n) = 1$. Sea, ahora, $t \in T$ y sea $(r, s) \in R \times S$ el par determinado por t según (4). Dado que $t \equiv r \,(\mathsf{mod}\, m)$, deducimos que $(t, m) = (r, m)$. Análogamente, $(t, n) = (s, n)$. Así, si $t \in T'$, entonces $(t, mn) = 1$ y concluimos que $r \in R'$ y que $s \in S'$. Recíprocamente, si $r \in R'$ y $s \in S'$, entonces $(r, m) = 1$ y $(s, n) = 1$, de lo que deducimos que $(t, mn) = 1$ y concluimos que $t \in T'$.

La igualdad $\varphi(mn) = \varphi(m)\varphi(n)$ es consecuencia de que el valor de φ es igual al cardinal de cualquier sistema reducido de representantes. □

En particular, si tuviésemos una fórmula para $\varphi(p^r)$, p primo, podríamos obtener una fórmula para $\varphi(m)$ en función de la factorización de m como producto de primos a potencias.[13]

Corolario 5.8. *Sea $f \in \mathbb{Z}[X]$ y, para cada $m \in \mathbb{Z}$, sea $N(m)$ la cantidad de soluciones a $f(x) \equiv 0 \pmod{m}$. Si $m = m_1 m_2$ es una factorización de m con $(m_1, m_2) = 1$, entonces $N(m) = N(m_1)N(m_2)$.*

Demostración. Cada solución $x \in \mathbb{Z}$ de $f(x) \equiv a \pmod{m}$ da lugar a una solución de $f(x) \equiv a \pmod{m_1}$ y a una solución de $f(x) \equiv a \pmod{m_2}$ (el mismo entero sirve). En la otra dirección, cada par de soluciones $x_1, x_2 \in \mathbb{Z}$ módulo m_1 y módulo m_2, respectivamente, es decir, enteros que satisfacen $f(x_1) \equiv a \pmod{m_1}$ y $f(x_2) \equiv a \pmod{m_2}$, dan lugar a un $x \in \mathbb{Z}$ que verifica $x \equiv x_1 \pmod{m_1}$ y $x \equiv x_2 \pmod{m_2}$. Dicho entero es único módulo m (Teorema 5.4) y verifica $f(x) \equiv a \pmod{m}$ (también por Teorema 5.4, aplicado al entero $f(x)$). □

Observación 5.9. Dado que, en un sistema de representantes, los representantes se corresponden con las clases que representan, podemos expresar el resultado del Corolario **??** diciendo que las soluciones módulo m están en biyección con el producto cartesiano de las soluciones módulo m_1 por las soluciones módulo m_2.

Ejemplo 5.10. La ecuación $x^2 + x + 7 \equiv 0 \pmod{15}$ no tiene solución. Por el Teorema chino del resto, la congruencia es equivalente al sistema

$$x^2 + x + 7 \equiv 0 \pmod{3} \quad \text{y} \quad x^2 + x + 7 \equiv 0 \pmod{5}\ .$$

Ahora, $7 \equiv 1 \pmod{3}$ y $7 \equiv 2 \pmod{5}$. Si bien $x^2 + x + 1 \equiv 0 \pmod{3}$ tiene como (única) solución módulo 3 a $x = 1$, la congruencia $x^2 + x + 2 \equiv 0 \pmod{5}$ no tiene solución con $x \in \mathbb{Z}$. En consecuencia, $N(15) = N(3)N(5) = 1 \cdot 0 = 0$.

Ejemplo 5.11. Vimos que $x^2 + x + 7 \equiv 0 \pmod{3}$ tiene una única solución módulo 3 ¿Cuántas soluciones módulo 189 hay? En primer lugar, factorizamos $63 = 9 \cdot 7$ y resolvemos las congruencias módulo 9 y módulo 7 por separado. Dado que hay soluciones módulo 3, *es posible que haya* soluciones módulo 9.

Sea $f(x) = x^2 + x + 7$. Sabemos que los $x \in \mathbb{Z}$ tales que $f(x) \equiv 0 \pmod{9}$ deben ser $x \equiv 1 \pmod{3}$. Mirando módulo 9, las distintas posibilidades son $x = 1$, $x = 4$ y $x = 7$. Efectivamente, $f(1) \equiv f(4) \equiv f(7) \equiv 0 \pmod{9}$. Con lo cual, $N(9) = 3$. Por otro lado, si $x \in \mathbb{Z}$, se cumple que $f(x) \equiv x^2 + x \pmod{7}$. Entonces, como 7 es primo, $f(x) \equiv 0 \pmod{7}$ tiene exactamente dos soluciones módulo 7: 0 y $6 \equiv -1$. O sea, $N(7) = 2$. Así, $N(63) = 3 \cdot 2 = 6$. Las seis soluciones módulo 63 vienen dadas por resolver los seis sistemas siguientes:

$$\begin{cases} x \equiv 1 \pmod{9} \\ x \equiv 0 \pmod{7}\ , \end{cases} \text{ y } \begin{cases} x \equiv 4 \pmod{9} \\ x \equiv 0 \pmod{7}\ , \end{cases} \text{ y } \begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 0 \pmod{7}\ , \end{cases} \text{ y}$$

$$\begin{cases} x \equiv 1 \pmod{9} \\ x \equiv 6 \pmod{7}\ , \end{cases} \text{ y } \begin{cases} x \equiv 4 \pmod{9} \\ x \equiv 6 \pmod{7}\ , \end{cases} \text{ y } \begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 6 \pmod{7}\ . \end{cases}$$

[13] Ver el Ejercicio 5.4.

Las soluciones son: 28, 49, 7, 55, 13 y 34.

Ejercicios

Ejercicio 5.1. El sistema de congruencias

$$x \equiv a_1 \,(\mathsf{mod}\, m_1) \quad \text{y} \quad x \equiv a_2 \,(\mathsf{mod}\, m_2)$$

admite una solución, si y sólo si $(m_1, m_2) \mid a_1 - a_2$. En ese caso, si $x \in \mathbb{Z}$ es una solución, entonces $y \in \mathbb{Z}$ es solución, si y sólo si $y \equiv x \,(\mathsf{mod}\, m)$, donde $m = [m_1, m_2]$ es el mínimo común múltiplo de m_1 y m_2.

Ejercicio 5.2. Si $m_1, \ldots, m_r \in \mathbb{Z}$ son coprimos de a pares y $a_1, \ldots, a_r \in \mathbb{Z}$, entonces existe una solución común a las congruencias

$$x \equiv a_i \quad (\mathsf{mod}\, m_i)$$

y, dada una solución $x \in \mathbb{Z}$, un $y \in \mathbb{Z}$ es solución, si y sólo si $y \equiv x \,(\mathsf{mod}\, m)$, donde $m = m_1 \cdots m_r$. Este resultado se puede demostrar aplicando inductivamente el Teorema 5.4. La siguiente es una demostración alternativa.

(i) Probar esta afirmación en los casos con $a_1 = 1, a_2 = 0, \ldots, a_r = 0$, etc. (considerar $x_1 = (m/m_1)\, b_1$, donde b_1 es solución de la ecuación $(m/m_1)\, b_1 \equiv 1 \,(\mathsf{mod}\, m_1)$).

(ii) Probar que, si x_j es solución del sistema con $a_j = 1$ como en (i), entonces, en el sistema con a_j arbitrarios, $x = \sum_j x_j a_j$ es solución.

(iii) Probar que, y es otra solución, entonces $y \equiv x \,(\mathsf{mod}\, m_i)$ para cada i (o sea, $m_i \mid y - x$) y concluir que $y \equiv x \,(\mathsf{mod}\, m)$.

Ejercicio 5.3. Si $f \in \mathbb{Z}[X]$, $m_1, \ldots, m_r \in \mathbb{Z}$ son coprimos de a pares y $m = m_1 \cdots m_r$, entonces la ecuación de congruencia

$$f(x) \equiv a \quad (\mathsf{mod}\, m)$$

es equivalente al sistema de ecuaciones

$$f(x) \equiv a \quad (\mathsf{mod}\, m_i)\ .$$

Además, las soluciones módulo m están en biyección con el producto cartesiano de las soluciones módulo m_i, para cada $1 \leq i \leq r$.

Ejercicio 5.4. Si p es un número primo, entonces $\varphi(p^r) = p^{r-1}\,(p-1) = p^r\,(1 - 1/p)$. Dar una fórmula para $\varphi(m)$, conociendo la factorización de m como potencia de primos.

Ejercicio 5.5. Hallar el menor entero positivo $\neq 1$ que es solución de

$$x \equiv 1 \,(\mathsf{mod}\, 3)\ , \quad x \equiv 1 \,(\mathsf{mod}\, 5) \quad \text{y} \quad x \equiv 1 \,(\mathsf{mod}\, 7)\ .$$

Ejercicio 5.6. Hallar todos los enteros que satisfacen los siguientes sistemas:

(i)
$$x \equiv 2 \,(\mathsf{mod}\, 3)\ , \quad x \equiv 3 \,(\mathsf{mod}\, 5) \quad \text{y} \quad x \equiv 5 \,(\mathsf{mod}\, 2)\ ;$$

(ii)
$$x \equiv 1 \,(\mathsf{mod}\, 4)\ , \quad x \equiv 0 \,(\mathsf{mod}\, 3) \quad \text{y} \quad x \equiv 5 \,(\mathsf{mod}\, 7)\ ;$$

(iii)
$$5x \equiv 1 \,(\mathsf{mod}\, 6)\ , \quad 4x \equiv 13 \,(\mathsf{mod}\, 15)\ .$$

Ejercicio 5.7. Resolver las siguientes ecuaciones de congruencia:

(i) $x^3 + 2x - 3 \equiv 0 \,(\mathsf{mod}\, 9)$;

(ii) $x^3 + 2x - 3 \equiv 0 \,(\mathsf{mod}\, 5)$;

(iii) $x^3 + 2x - 3 \equiv 0 \,(\mathsf{mod}\, 45)$;

(iv) $x^3 + 4x + 8 \equiv 0 \,(\mathsf{mod}\, 15)$;

(v) $x^3 - 9x^2 + 23x - 15 \equiv 0 \,(\mathsf{mod}\, 503)$;[14]

(vi) $x^3 - 9x^2 + 23x - 15 \equiv 0 \,(\mathsf{mod}\, 143)$.

Ejercicio 5.8. Si $N(m)$ es la cantidad de soluciones a $x^2 \equiv x \,(\mathsf{mod}\, m)$, hallar una fórmula para $N(p^r)$, con p primo.[15] Deducir una fórmula para $N(m)$, m arbitrario.

Ejercicio 5.9. Para $m \geq 1$, entero, sea $\psi(m) = \#\{1 \leq t \leq m \,:\, (t, m) = 1,\, (t+1, m) = 1\}$. Probar las siguientes afirmaciones:

(i) si p es primo, $\psi(p) = p - 2$;

(ii) si p es primo y $r \geq 1$, $\psi(p^r) = p^{r-1}\,(p-2) = p^r\,(1 - 2/p)$;

(iii) si $(m, n) = 1$, entonces $\psi(mn) = \psi(m)\psi(n)$.

Deducir una fórmula para $\psi(m)$.

Ejercicio 5.10. Sea $f \in \mathbb{Z}\,[X]$ y sean

- $N(m)$ la cantidad de soluciones de $f(x) \equiv 0 \,(\mathsf{mod}\, m)$ y
- $\phi_f(m) = \#\{1 \leq t \leq m \,:\, (f(t), m) = 1\}$.

Probar las siguientes afirmaciones:

(i) si p es primo, $\phi_f(p) = p - N(p)$;

[14] Hint: 503 es primo y $x^3 - 9x^2 + 23 - 15 = (x-1)\,(x-3)\,(x-5)$.
[15] Hint: Hacer el caso $r = 1$.

(ii) si p es primo y $r \geq 1$, $\phi_f(p^r) = p^{r-1}\phi_f(p) = p^r\,(1 - N(p)/p)$;

(iii) si $(m, n) = 1$, entonces $\phi_f(mn) = \phi_f(m)\phi_f(n)$.

Concluir que, si $m \in \mathbb{Z}$, vale

$$\phi_f(m) \;=\; m \prod_{p|m} \big(1 - N(p)/p\big)\ .$$

Comparar con la fórmula para φ y la fórmula para la función ψ del Ejercicio 5.8. Deducir nuevamente las fórmulas para estas funciones con el esquema de este ejercicio ¿Cuáles son los polinomios en cada caso?

6 El Lema de Hensel

Parte II

Herramientas

7 Estructuras algebraicas

Definición 7.1. Llamaremos *anillo* a un conjunto A dotado de:

- operaciones binarias $+, \cdot : A \times A \to A$, que llamamos *suma* y *producto*,
- elementos distinguidos $0, 1 \in A$, que llamamos *cero* y *uno*,
- una función $- : A \to A$ (operación unitaria), que escribimos $a \mapsto -a$ y cuya imagen llamamos "menos a"

que cumplen:

- con respecto a la suma,

$$(a+b)+c = a+(b+c)\ , \quad 0+a = a+0 = a\ ,$$
$$a+(-a) = (-a)+a = 0 \quad \text{y} \quad a+b = b+a\ ,$$

- con respecto al producto,

$$(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \text{y} \quad 1\cdot a = a\cdot 1 = a\ ,$$

- con respecto a ambas,

$$(a+b)\cdot c = a\cdot c + b\cdot c \quad \text{y} \quad c\cdot(a+b) = c\cdot a + c\cdot b\ .$$

Definición 7.2. Si $a \cdot b = b \cdot a$, se dice que a *y* b *conmutan*; si todo par de elementos conmuta, se dice que el anillo es *conmutativo*.

Observación 7.3. En general, esta estructura se denomina *anillo con unidad* (los anillos *sin* un 1 también son importantes).

Ejemplo 7.4. Los números enteros $\mathbb{Z}$ constituyen un anillo con la suma, el producto, el cero, el uno y el menos usuales. Los números racionales $\mathbb{Q}$, reales $\mathbb{R}$ y complejos $\mathbb{C}$, también. Todos éstos son anillos conmutativos. Los números naturales $\mathbb{N}$, en cambio, no forman un anillo con la suma y el producto usuales (dependiendo de la convención, no hay cero, pero, en general, $-n$ no es natural, si $n \geq 1$ es natural).

Ejemplo 7.5. El subconjunto $A \subset \mathbb{C}$ del Ejercicio 2.2,

$$A = \left\{x + y\sqrt{-6} \,:\, x, y \in \mathbb{Z}\right\}\ ,$$

es un anillo. La suma, el producto, el cero, el uno y el menos son los heredados de $\mathbb{C}$. En particular, A es un anillo conmutativo (porque $\mathbb{C}$ lo es). Este anillo se suele denotar por $\mathbb{Z}\left[\sqrt{-6}\right]$.

Ejemplo 7.6. Si A es un anillo, las matrices *cuadradas* con coeficientes en A constituyen un anillo. Por ejemplo, las matrices de tamaño 2×2 con coeficientes enteros, $\mathsf{Mat}(2 \times 2, \mathbb{Z})$, son un anillo con las operaciones usuales. Pero, en general, estos anillos no son conmutativos, aunque A lo sea.

Nos concentraremos en anillos conmutativos (con uno).

Definición 7.7. Un *dominio íntegro* es un anillo conmutativo (con uno) que tiene la siguiente propiedad:[16]

$$\text{para todo par de elementos } a \text{ y } b,\ ab = 0 \text{ implica } a = 0 \text{ o } b = 0.$$

Ejemplo 7.8. Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sus anillos de polinomios y $\mathbb{Z}\left[\sqrt{-6}\right]$ son dominios íntegros.

Definición 7.9. Un *dominio euclidiano* es un dominio íntegro D que admite una función $N : D \to \mathbb{Z}$ con las siguientes propiedades:

- $N(x) \geq 0$ para todo $x \in D$ y,
- dados $a, b \in D$, $a \neq 0$, existen $q, r \in D$ tales que $b = qa + r$ y $r = 0$ o bien $N(r) < N(a)$.

Ejemplo 7.10. Los enteros $\mathbb{Z}$ son un dominio euclidiano: la función valor absoluto $N(x) = |x|$ tiene la propiedad que los caracteriza. Los anillos de polinomios $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$ (o, más en general, polinomios en una indeterminada, sobre un cuerpo) son dominios euclidianos. Sin embargo, $\mathbb{Z}[X]$ no lo es. El dominio $\mathbb{Z}\left[\sqrt{-6}\right]$ tampoco es un dominio euclidiano.

Ejemplo 7.11. El anillo $\mathbb{Z}[i]$ es, como conjunto, el subconjunto de $\mathbb{C}$ de elementos de la forma $x + yi$, $x, y \in \mathbb{Z}$. Si $\alpha = a + bi$ y $\beta = c + di$ son elementos de $\mathbb{Z}[i]$ $(a, b, c, d \in \mathbb{Z})$, entonces

$$\begin{aligned} \alpha + \beta &= (a + bi) + (c + di) = (a + c) + (b + d)\, i \in \mathbb{Z}[i] \quad \text{y} \\ \alpha\beta &= (a + bi)\,(c + di) = (ac - bd) + (ad + bc)\, i \in \mathbb{Z}[i]\ . \end{aligned}$$

Además, $0, 1 \in \mathbb{Z}[i]$ (más aun, $\mathbb{Z} \subset \mathbb{Z}[i]$). También se cumple que $-\alpha \in \mathbb{Z}[i]$, si $\alpha \in \mathbb{Z}[i]$. De esto se deduce que $\mathbb{Z}[i]$ es un dominio íntegro **(ejercicio)**.[17]

Veamos que $\mathbb{Z}[i]$ es un dominio euclidiano.[18] Dados $x, y \in \mathbb{Q}$, definimos la *norma* de $x + yi$ como

$$N(x + yi) = x^2 + y^2\ .$$

Esta función cumple $N(\beta\beta') = N(\beta)N(\beta')$ y $N(x+yi) \in \mathbb{Z}$, si $x, y \in \mathbb{Z}$. Dados elementos $\alpha = a + bi$ y $\beta = c + di$ de $\mathbb{Z}[i]$, $\alpha \neq 0$,

(i) existen $u, v \in \mathbb{Q}$ tales que $(u + vi)\alpha = \beta$;

[16] C.f. la propiedad de la Observación 2.6.

[17] Hint: Todo ocurre dentro de $\mathbb{C}$.

[18] Esto sí depende de $\mathbb{Z}[i]$, no es algo "heredado".

(ii) dados $u, v \in \mathbb{Q}$, existen $m, n \in \mathbb{Z}$ tales que $|m - u| \leq 1/2$ y $|n - v| \leq 1/2$;

(iii) si $q := m + ni$ y $r := \beta - q\alpha$, entonces $N(r) < N(\alpha)$ (o $r = 0$).

Con respecto a (iii), $N(r) = N((u+vi)-q)N(\alpha)$, pero $N((u+vi)-q) \leq 1/2$. La función norma tiene la propiedad de la Definición 7.9

Definición 7.12. Dado $a \in A$, si existe $b \in A$ tal que $ab = ba = 1$, se dice que a es una *unidad* del anillo o que es *inversible* en el anillo.

Ejemplo 7.13. Las unidades de $\mathbb{Z}$ son ± 1.

Definición 7.14. Un anillo (conmutativo, con 1) con la propiedad de que todos sus elementos distintos de cero son inversibles se denomina *cuerpo*.

Ejemplo 7.15. Los anillos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos. El anillo $\mathbb{Z}$ no es un cuerpo.

Ejercicios

Ejercicio 7.1. Sea $\omega \in \mathbb{C}$ tal que $\omega^3 = 1$, pero $\omega \neq 1$.[19]

(i) Probar que $\omega^2 + \omega + 1 = 0$.

(ii) Probar que $\bar{\omega} \neq \omega$ y que $\bar{\omega}^2 + \bar{\omega} + 1 = 0$, también.

(iii) Concluir que $X^2 + X + 1 = (X - \omega)(X - \bar{\omega})$ y, en particular, que $\omega + \bar{\omega} = -1$ y que $\omega\bar{\omega} = 1$.

Dados $x, y \in \mathbb{Q}$, definimos

$$N(x + y\omega) := x^2 - xy + y^2 \ .$$

(i) Como $\{1, \omega\}$ es un conjunto l.i. sobre $\mathbb{Q}$, esta expresión no es ambigua.

(ii) Probar que $N(\beta\beta') = N(\beta)N(\beta')$ y que $N(x + y\omega) \in \mathbb{Z}$, si $x, y \in \mathbb{Z}$.

Sea $\mathbb{Z}[\omega] \subset \mathbb{C}$ el subconjunto

$$\mathbb{Z}[\omega] := \left\{a + b\omega \,:\, a, b \in \mathbb{Z}\right\} \ .$$

(i) Probar que, si $\alpha, \beta \in \mathbb{Z}[\omega]$, entonces $\alpha+\beta$, $\alpha\beta$, $-\alpha$ y $\bar{\alpha}$ pertenecen a $\mathbb{Z}[\omega]$, también.

(ii) Probar que, $\mathbb{Z} \subset \mathbb{Z}[\omega]$.

Emular el argumento del Ejemplo 7.11 para probar que $\mathbb{Z}[\omega]$ es un dominio euclidiano: dados $\alpha = a + b\omega$ y $\beta = c + d\omega$, $\alpha \neq 0$,

(i) existen $u, v \in \mathbb{Q}$ tales que $(u + v\omega)\alpha = \beta$;

[19] Por ejemplo, $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$.

(ii) dados $u, v \in \mathbb{Q}$, existen $m, n \in \mathbb{Z}$ tales que $|m - u| \leq 1/2$ y $|n - v| \leq 1/2$;

(iii) si $q := m + n\omega$ y $r := \beta - q\alpha$, entonces $N(r) < N(\alpha)$ (o $r = 0$).

¿En qué punto falla el argumento para el dominio $\mathbb{Z}\left[\sqrt{-6}\right]$?

Ejercicio 7.2 (Unidades de un anillo)**.** Dado $a \in A$, si existe $b \in A$ tal que $ab = ba = 1$, se dice que a es una *unidad* del anillo o que es *inversible* en el anillo. Por ejemplo, las unidades de $\mathbb{Z}$ son ± 1.

- En $\mathbb{Z}[i]$, probar que $N(\alpha) = \alpha\bar{\alpha}$ $(= \bar{\alpha}\alpha)$ y concluir que $\alpha \in \mathbb{Z}[i]$ es inversible, si y sólo si $N(\alpha) = \pm 1$ ¿Puede dar -1? Hallar todas las unidades, en este caso.
- En $\mathbb{Z}[\omega]$, probar que $N(\alpha) = \alpha\bar{\alpha}$ $(= \bar{\alpha}\alpha)$ y concluir que $\alpha \in \mathbb{Z}[\omega]$ es inversible, si y sólo si $N(\alpha) = \pm 1$ ¿Puede dar -1? Hallar todas las unidades, en este caso.
- Hacer lo mismo con $\mathbb{Z}\left[\sqrt{-6}\right]$ y con $\mathbb{Z}\left[\sqrt{-2}\right]$.[20]

Ejercicio 7.3. Repetir el argumento del Ejercicio 7.1 con $\mathbb{Z}[\delta] \subset \mathbb{C}$, el subconjunto de los complejos de la forma $a + b\delta$, donde $\delta \in \mathbb{C}$ es raíz de $X^2 + 2$.

Ejercicio 7.4. Probar que 2 es divisible por $(1 + i)^2$ en $\mathbb{Z}[i]$.

Ejercicio 7.5. Probar que 3 es divisible por $(1 - \omega)^2$ en $\mathbb{Z}[\omega]$.

8 Enteros modulares

Denotaremos el conjunto de clases de congruencia módulo m ($m \in \mathbb{Z}$, $m \neq 0$) por $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/m$ o por $\mathbb{Z}_m$ (talvez): un conjunto finito que podemos representar con los enteros a en el rango $0 \leq a \leq |m| - 1$, o bien $1 \leq a \leq |m|$, por ejemplo. Estudiando la resolubilidad de una ecuación módulo m, obtenemos información acerca de su esolubilidad en $\mathbb{Z}$; la ventaja que esto tiene es que la búsqueda de soluciones se lleva a cabo en un conjunto finito. En otras ocasiones, será relevante entender las soluciones a una ecuación de congruencia, sin que esto tenga por objetivo conocer las soluciones de la misma ecuación en $\mathbb{Z}$. Por esta razón es relevante entender qué estructura tiene el conjunto de clases $\mathbb{Z}/m\mathbb{Z}$.

Teorema 8.1. *El conjunto $\mathbb{Z}/m\mathbb{Z}$, junto con las clases $[0], [1] \in \mathbb{Z}/m\mathbb{Z}$ y las operaciones*

$$[a] + [c] := [a + c] \quad y \quad [a]\,[c] := [ac] \ ,$$

constituye un anillo conmutativo con unidad; el cero es $[0]$ y el uno es $[1]$.

Demostración. **(ejercicio)**. Que las operaciones están bien definidas, es decir, que no dependen de los representantes elegidos, es consecuencia del Teorema 3.5. □

[20] Ver Ejercicio 7.3.

Simplificaremos la notación y escribiremos "a", en lugar de "$[a]$" cuando creamos que no hay riesgo de confundir una expresión en $\mathbb{Z}/m\mathbb{Z}$ por una en $\mathbb{Z}$. En ocasiones, hablaremos de "buscar soluciones en $\mathbb{Z}/m\mathbb{Z}$". Con esto querremos decir buscar soluciones a una ecuación de congruencia, es decir, buscar soluciones módulo m.

Ejemplo 8.2. La ecuación $x^2 - 117x + 31 = 0$ no tiene soluciones en $\mathbb{Z}/2\mathbb{Z}$, es decir, no tiene soluciones módulo 2.

Ejemplo 8.3. Dados $a, m \in \mathbb{Z}$, $m \neq 0$, si $(a, m) = 1$, entonces la ecuación $ax = b$ tiene soluciones en $\mathbb{Z}/m\mathbb{Z}$. De hecho, existe una única solución módulo m. Si $b = 1$, podemos hacer lo siguiente: por la Identidad de Bézout (Teorema 1.7), existen $x, y \in \mathbb{Z}$ tales que $ax + my = 1$. Pero, entonces, $ax \equiv 1 \,(\mathsf{mod}\, m)$, o sea, $ax = 1$ en $\mathbb{Z}/m\mathbb{Z}$. Todo esto es lo mismo que decir que $m \mid ax - 1$.

Corolario 8.4. *Si $p \in \mathbb{Z}$ es primo, entonces $\mathbb{Z}/p\mathbb{Z}$ es un dominio íntegro. Recíprocamente, si $m \neq 0$ y $\mathbb{Z}/m\mathbb{Z}$ es un dominio íntegro, entonces m es primo. En particular, $\mathbb{Z}/m\mathbb{Z}$ es un cuerpo, si y sólo si m es primo.*

Demostración. Supongamos, primero, que p es primo. Sean $[a], [b] \in \mathbb{Z}/p\mathbb{Z}$ tales que $[a][b] = 0$. Como, por definición, $[a][b] = [ab]$, esta suposición implica que $ab \equiv 0 \,(\mathsf{mod}\, p)$, o sea, $p \mid ab$. Como p es primo, por el Lema 2.5, o bien $p \mid a$ o bien $p \mid b$. Pero esto implica que $a \equiv 0$ o $b \equiv 0 \,(\mathsf{mod}\, p)$. En términos de clases, esto se traduce en que, o bien $[a] = 0$, o bien $[b] = 0$ en $\mathbb{Z}/p\mathbb{Z}$. O sea, $\mathbb{Z}/p\mathbb{Z}$ es un dominio íntergro. Recíprocamente, si $m \neq 0$ es tal que $\mathbb{Z}/m\mathbb{Z}$ es dominio íntegro, entonces se verifica que m tiene la propiedad de la Observación 2.6 y, por lo tanto, que m es primo. □

Definición 8.5. Si A es un anillo conmutativo y $a \in A$, decimos que a es una *unidad de A* (o *en A*), si existe $x \in A$ tal que $ax = 1$ $(= xa)$.

Corolario 8.6. *Dados $a, m \in \mathbb{Z}$, $m \neq 0$, la clase $[a] \in \mathbb{Z}/m\mathbb{Z}$ es una unidad en $\mathbb{Z}/m\mathbb{Z}$, si y sólo si $(a, m) = 1$. En particular, las unidades de $\mathbb{Z}/m\mathbb{Z}$ están representadas por los elementos de un sistema reducido.*

Definición 8.7. Decimos que *a es una unidad módulo m*, si $[a] \in \mathbb{Z}/m\mathbb{Z}$ es una unidad de $\mathbb{Z}/m\mathbb{Z}$.

Observación 8.8. Si $a \in A$ es una unidad, existe un único $x \in A$ tal que $ax = xa = 1$, al que denotamos a^{-1}. Las unidades de un anillo forman un grupo, el *grupo de unidades* del anillo. Escribimos $A^\times$ o bien $U\big(A\big)$ para referirnos al grupo de unidades de A. En el caso de $A = \mathbb{Z}/m\mathbb{Z}$, a veces escribiremos $U\big(m\big)$.

Corolario 8.9. $\big|U\big(m\big)\big| = \varphi(m) = \#\{k \in \mathbb{Z} : 0 \leq k \leq |m| - 1,\, (k, m) = 1\}$. *En particular, si $(a, m) = 1$, entonces $a^{\varphi(m)} = 1$ en $\mathbb{Z}/m\mathbb{Z}$.*

Demostración. Con respecto a la última afirmación, $U\big(m\big)$ es un grupo de orden $\varphi(m)$. Por lo tanto, $a^{\varphi(m)} = 1$ en $U\big(m\big)$. Pero esto quiere decir que $a^{\varphi(m)} \equiv 1 \,(\mathsf{mod}\, m)$, o sea que $a^{\varphi(m)} = 1$ en $\mathbb{Z}/m\mathbb{Z}$. □

Ejercicios

Ejercicio 8.1. Probar que, si $(a, m) = 1$, entonces $ax = b$ tiene una única solución en $\mathbb{Z}/m\mathbb{Z}$, cualquiera sea $b \in \mathbb{Z}$. Describir las soluciones a la ecuación de congruencia $ax \equiv b \pmod{m}$, es decir, el conjunto de $x \in \mathbb{Z}$ tales que $ax \equiv b \pmod{m}$.

Ejercicio 8.2. Hacer una tabla de multiplicación y suma para los anillos $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ y $\mathbb{Z}/10\mathbb{Z}$.

Ejercicio 8.3. Sea p un primo impar y sea $k \in \{1, \ldots, p-1\}$. Entonces existe unúnico $b_k \in \{1, \ldots, p-1\}$ tal que $kb_k \equiv 1 \pmod{p}$. Además, $k \neq b_k$, excepto en los casos $k = 1$ y $k = p - 1$ ¿Son ciertas estas afirmaciones en el caso de un módulo m cualquiera, no necesariamente primo?

Ejercicio 8.4. Si p es primo $(p-1)! \equiv -1 \pmod{p}$. Si $n = 4$, entonces $(4-1)! = 3! = 6 \equiv 2 \pmod{4}$. Si $n > 4$ *no es* primo, entonces $(n-1)! \equiv 0 \pmod{n}$.

Ejercicio 8.5. Sea $R = \{r_1, \ldots, r_{\varphi(m)}\}$ un sistema reducido de representantes de las clases módulo m y sea $N \geq 0$ la cantidad de soluciones a la ecuación de congruencia $x^2 \equiv 1 \pmod{m}$. Probar que[21]

$$\prod_{i=1}^{\varphi(m)} r_i \equiv (-1)^{N/2} \pmod{m} .$$

Ejercicio 8.6. Sean p y q primos impares distintos y supongamos, además, que $p - 1 \mid q - 1$. Si $(n, pq) = 1$, entonces $n^{q-1} \equiv 1 \pmod{pq}$.[22]

Ejercicio 8.7. Probar que, si p es primo, entonces p divide al numerador de $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$.

Ejercicio 8.8. Probar que

(i) si p es un primo impar y $a \geq 1$, las únicas soluciones $x^2 = 1$ en $\mathbb{Z}/p^a\mathbb{Z}$ son ± 1;

(ii) $x^2 = 1$ tiene una única solución en $\mathbb{Z}/2\mathbb{Z}$, dos soluciones en $\mathbb{Z}/4\mathbb{Z}$ y cuatro soluciones en $\mathbb{Z}/2^b\mathbb{Z}$, si $b \geq 3$.

Determinar la cantidad de soluciones a $x^2 \equiv 1 \pmod{m}$ para $m \in \mathbb{Z}$, $m \neq 0$.[23]

Ejercicio 8.9. Si $R = \{r_1, \ldots, r_{p-1}\}$ es un sistema reducido módulo p, primo, entonces

$$\prod_{i=1}^{p-1} r_i \equiv -1 \pmod{p} .$$

Ejercicio 8.10. Si $R = \{r_1, \ldots, r_p\}$ y $R' = \{r'_1, \ldots, r'_p\}$ son dos sistemas completos de representantes módulo un primo $p > 2$, entonces $r_1r'_1, \ldots, r_pr'_p$ no pueden formar un sistema completo de representantes módulo p.

[21] Hint: Si $r \in R$, entonces, por un lado, existe $r' \in R$ tal que $rr' \equiv 1$. Por otro, $(-r, m) = 1$ y, si $m > 2$, entonces también $-r \not\equiv r$.

[22] Hint: Probar que $n^{q-1} \equiv 1 \pmod{p}$ y que $n^{q-1} \equiv 1 \pmod{q}$.

[23] Hint: Teorema chino del resto.

9 Polinomios

En esta sección, salvo aclaración, "anillo" querrá decir "anillo conmutativo con unidad".

Definición 9.1. Si A es un anillo y $B \subset A$ es un subconjunto con las propiedades: $0 \in B$, $B + B \subset B$, $B \cdot B \subset B$ y $1 \in B$, decimos que B *es un subanillo de* A.

Ejemplo 9.2. El subconjunto $\mathbb{Z} \subset \mathbb{Q}$ es un subanillo del anillo (cuerpo) de números racionales; como subconjuntos de los números complejos, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ son subanillos que satisfacen: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Los subconjuntos $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ y $\mathbb{Z}\left[\sqrt{-6}\right]$ también son subanillos de $\mathbb{C}$, pero ninguno de ellos está contenido en $\mathbb{R}$. El anillo $\mathbb{Z}\left[\sqrt{-6}\right]$ –definido de manera análoga a $\mathbb{Z}\left[\sqrt{-6}\right]$– es un subanillo de $\mathbb{R}$ (pero no de $\mathbb{Q}$).

Observación 9.3. Si $a \in A$ y $B \subset A$ es un subanillo, entonces a, a^2, ... son elementos de A y también lo son ba, ba^2, ..., si $b \in B$. Más en general, la expresión

$$b_0 + b_1 a + \cdots + b_m a^m \,, \tag{6}$$

donde m es natural o 0 y $b_0, \ldots, b_m \in B$, define un elemento de A. El elemento 0 es de este tipo (eligiendo $m = 0$ y $b_0 = 0$, por ejemplo), como también lo son 1 ($m = 0$ y $b_0 = 1$) y a ($m = 1$, $b_0 = 0$ y $b_1 = 1$). Más aun, dados dos elementos del tipo (6), p y q, su suma, $p + q$, y su producto, $p \cdot q$, son también del tipo (6) **(ejercicio)**. En particular, el subconjunto

$$B[a] = \left\{ b_0 + b_1 a + \cdots + b_m a^m \,:\, m \text{ natural o } 0 \text{ y } b_0, \ldots, b_m \in B \right\}$$

de A es un subanillo de A.

Definición 9.4. Sean A un anillo, $a \in A$ un elemento y $B \subset A$ un subanillo. Una *expresión polinomial en* a *con coeficientes en* B es un elemento de A del tipo (6). El *anillo de expresiones polinomiales en* a *con coeficientes en* B es el subanillo $B[a] \subset A$.

Ejemplo 9.5. Si $\sqrt{-6} \in \mathbb{C}$ es un número complejo que cumple que $\sqrt{-6}^2 = -6$, entonces el subanillo de expresiones polinomiales en $\sqrt{-6}$ con coeficientes en $\mathbb{Z}$ coincide con el anillo $\mathbb{Z}\left[\sqrt{-6}\right]$ **(ejercicio)**.

Observación 9.6. En general, no tiene por qué ser cierto *a priori* que $b_0 + b_1 a + \cdots + b_m a^m = c_0 + c_1 a + \cdots + c_n a^n$ implique $m = n$ y $b_i = c_i$ para cada i. Siguiendo con el Ejemplo 9.5, la igualdad $\sqrt{-6}^2 = -6$ muestra un ejemplo de esto. En particular, podría ocurrir que $b_0 + b_1 a + \cdots + b_m a^m = 0$, pero que $b_m \neq 0$.

Definición 9.7. Sean B un anillo, A un anillo del cual B es subanillo y $a \in A$ un elemento. Decimos que a *es trascendente sobre* B, si las únicas expresiones polinomiales en a con coeficientes en B iguales a cero son las *expresiones triviales*, es decir, aquellas cuyos coeficientes son todos iguales a cero. Expresado de otra manera, $a \in A$ es trascendente sobre B, si

$$b_0 + b_1 a + \cdots + b_m a^m = 0 \quad \text{implica} \quad b_0 = b_1 = \cdots = b_m = 0 \,.$$

Teorema 9.8. *Sean B un anillo, A, C anillos del cual B es subanillo y $x \in A$ y $c \in C$ elementos. Si x es trascendente sobre B, existe una única función $f : B[x] \to C$ tal que*

$$f(b) = b \text{ para todo } b \in B \quad y \quad f(x) = c$$

y tal que

$$f(u+v) = f(u) + f(v) \quad y \quad f(uv) = f(u)f(v) \ ,$$

siempre que $u, v \in B[x]$. La imagen de esta función es igual a $B[c]$.

Demostración. Veamos, primero, que puede existir a lo sumo una función con estas propiedades. Todo elemento de $B[x]$ se puede expresar como $b_0 + b_1x + \cdots + b_mx^m$, donde m es natural o 0 y $b_i \in B$ para cada i. Entonces, si $f : B[x] \to C$ tiene las propiedades del enunciado y $p = b_0 + b_1x + \cdots + b_mx^m$ es una expresión polinomial en x con coeficientes en B, $f(p)$ es igual a

$$\begin{aligned} f\left(b_0 + b_1x + \cdots + b_mx^m\right) &= f(b_0) + f(b_1)\, f(x) + \cdots + f(b_m)\, f(x)^m \\ &= b_0 + b_1c + \cdots + b_mc^m \ . \end{aligned} \tag{7}$$

En palabras, una función $f : B[x] \to C$ que respeta la suma y el producto y es la identidad en B está determinada por su valor en x. Aun no hemos usado que x es trascendente. El hecho de que $x \in A$ sea trascendente sobre B es equivalente a que cada elemento de $B[x]$ se puede expresar de a lo sumo una única manera como expresión polinomial en x con coeficientes en B. Con esto y la ecuación (7) en mente, definimos la siguiente función: si $p = b_0 + b_1x + \cdots + b_mx^m \in B[x]$,

$$f(p) := b_0 + b_1c + \cdots + b_mc^m \ .$$

La unicidad de la expresión para p garantiza que la identidad anterior *define una función.* Sólo resta verificar que esta función tiene las propiedades deseadas **(ejercicio)**. □

Observación 9.9. Sean B un anillo, A, C anillos del cual B es subanillo y $x \in A$ e $y \in C$ elementos trascendentes. Por el Teorema 9.8, existen únicas funciones $f : B[x] \to B[y]$ y $g : B[y] \to B[x]$ que respetan la suma y el producto y tales que $f(b) = g(b) = b$ para todo $b \in B$ y $f(x) = y$ y $g(y) = x$. En particular, $fg = \mathsf{id}_{B[y]}$ y $gf = \mathsf{id}_{B[x]}$. Es decir, desde un punto de vista algebraico, los anillos $B[x]$ y $B[y]$ son indistinguibles. Esta estructura común es la de polinomios en una indeterminada con coeficientes en B.

Definición 9.10. Sea B un anillo conmutativo con unidad $1 \neq 0$. Las expresiones polinomiales en un elemento trascendente, perteneciente a un anillo del cual B es subanillo serán *polinomios en una indetermianda con coeficientes en B.*

Observación 9.11. Por el Teorema 9.8, no importa cuál sea el anillo A del cual B es subanillo, ni tampoco el elemento trascendente $x \in A$ elegido para hacer las veces de variable, la estructura algebraica es esencialmente la misma.[24]

[24] ¿Es cierto que para cualquier anillo (conmutativo con unidad $1 \neq 0$) B existe un anillo $A \supset B$ del cual es subanillo y un elemento $x \in A$ trascendente sobre B? En el Ejercicio **??** mostramos una manera de responder la pregunta.

Definición 9.12. El *grado* de un polinomio $p \in B[x]$, $p \neq 0$, es el máximo $k \geq 0$ tal que $b_k \neq 0$ en la expresión polinomial $p = b_0 + b_1 x + \cdots + b_m x^m$. Al polinomio $0 \in B[x]$, lo llamamos el *polinomio nulo* y no le asignamos grado.

Si $p = b_0 + b_1 x + \cdots + b_m x^m$ y $q = c_0 + c_1 x + \cdots + c_n x^n$ son polinomios de grados m y n ($b_m \neq 0$, $c_n \neq 0$), respectivamente, entonces

$$p\,q \;=\; d_0 \;+\; d_1\,x \;+\; \cdots \;+\; d_{m+n}x^{m+n}\;, \quad \text{donde} \quad d_k = \sum_{i+j=k} b_i c_j\;.$$

En particular, $d_{m+n} = b_m c_n$ y, si $pq \neq 0$, entonces $\mathsf{gr}(pq) \leq \mathsf{gr}(p) + \mathsf{gr}(q)$; podría ocurrir que $d_{m+n} = 0$.

Ejemplo 9.13. Sean $p, q \in \mathbb{Z}/6\mathbb{Z}[x]$ los polinomios $p = 2x + 1$ y $q = 3x + 5$, entonces

$$pq \;=\; (2x+1)(3x+5) \;=\; (2\cdot 3)\,x^2 + (2\cdot 5 + 1\cdot 3)\,x + 1\cdot 5 \;=\; 6x^2 + 13x + 5 \;=\; x + 5\;.$$

En particular, si bien p y q son polinomios de grado 1 con coeficientes en $\mathbb{Z}/6\mathbb{Z}$, el producto pq tiene grado 1, menor estricto que la suma de los grados.

Definición 9.14. Si $p \in B[x]$ es un polinomio distinto del polinomio nulo de grado $\mathsf{gr}(p) = m \geq 0$, su *coeficiente principal* es el coeficiente b_m en la expresión $p = b_0 + b_1 x + \cdots + b_m x^m$; su *término independiente* es b_0. Decimos que un polinomio no nulo es *mónico*, si su coeficiente principal es igual a 1.

Observación 9.15. El coeficiente principal de un polinomio distinto del polinomio nulo es distinto de cero.

Definición 9.16. Un polinomio g *divide* a un polinomio f, si existe un polinomio h tal que $gh = f$; en tal caso, escribimos $g \mid f$.

Teorema 9.17. *Sea B un anillo (conmutativo con unidad $1 \neq 0$) y sean $f, g \in B[x]$ polinomios en una indeterminada. Si el coeficiente principal de g es una unidad en B, entonces*

(A) $g \mid f$ y existe un único polinomio $q \in B[x]$ tal que $f = qg$, o bien

(B) existen únicos polinomios $q, r \in B[x]$ tales que $f = qg + r$ y $\mathsf{gr}(r) < \mathsf{gr}(g)$.

Demostración. Como el coeficiente principal de g es inversible, el coeficiente principal de qg es igual al coeficiente principal de q (cero, si $q = 0$). En particular, si $f = 0$, se cumple $g \mid f$ y el único polinomio para el cual se verifica $f = qg$ es $q = 0$. Asumamos, entonces, que f no es el polinomio nulo. En ese caso, $\mathsf{gr}(f) = m \geq 0$ y, si $f = a_0 + a_1 x + \cdots + a_m x^m$, $a_m \neq 0$. Si $m < \mathsf{gr}(g)$, la única posibilidad es $q = 0$ y $r = f$. Supongamos que $m \geq \mathsf{gr}(g)$. Si $m = 0$, entonces $\mathsf{gr}(g) = 0$, con lo que $g = b_0 \in B$ es una unidad y $g \mid f$; el polinomio q, en este caso, es $q = a_0 b_0^{-1}$. Si $m > 0$ y $d = \mathsf{gr}(g) \leq m$, entonces el polinomio

$$f_1 \;=\; f \;-\; a_m b_d^{-1} x^{m-d}\, g$$

es, o bien el polinomio nulo, o bien $\mathsf{gr}(f_1) < \mathsf{gr}(f)$. Un argumento inductivo muestra que existen q y r tales que $f = qg + r$, donde $r = 0$ o bien $\mathsf{gr}(r) < \mathsf{gr}(g)$. Resta probar la unicidad **(ejercicio)**. □

Corolario 9.18. *Sea k un cuerpo. Entonces,*

(i) los polinomios en una indeterminada con coeficientes en k forman un dominio euclidiano;

(ii) si $f \in k[x]$ es un polinomio no nulo y $a \in k$, entonces a es una raíz de f, si y sólo si $x - a$ divide a f en $k[x]$;

(iii) en particular, si $\mathsf{gr}(f) = m \geq 0$, f tiene, a lo sumo, m raíces distintas en k;

(iv) si $U \subset k^\times$ es un subconjunto finito tal que $U \cdot U \subset U$, entonces existe $y \in U$ tal que todo $u \in U$ es de la forma $u = y^r$ para algún entero no negativo r.[25]

Ejercicios

Ejercicio 9.1. Probar que $\mathbb{Z}[i]$ y $\mathbb{Z}[\omega]$ son iguales a los subanillos $\mathbb{C}$ de expresiones polinomiales en i y, respectivamente, ω con coefcientes en $\mathbb{Z}$.

Ejercicio 9.2. Probar que el subanillo $\mathbb{Z}\left[\sqrt{2}\right] \subset \mathbb{R}$ de expresiones polinomiales en $\sqrt{2}$ con coeficientes en $\mathbb{Z}$ es, como conjunto, igual al subconjunto de elementos de la forma $a + b\sqrt{2}$ donde $a, b \in \mathbb{Z}$. Hacer lo análogo con $\mathbb{Z}\left[\sqrt{3}\right]$.

Ejercicio 9.3. Mostrar que no existe ninguna función $f : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{Z}\left[\sqrt{3}\right]$ tal que $f(1) = 1$ y que respete la suma y el producto.

Ejercicio 9.4. Describir los elementos del anillo de expresiones polinomiales $\mathbb{Z}\left[\frac{1}{2}\right]$ ¿Es $\frac{1}{2}$ trascendente sobre $\mathbb{Z}$? ¿Existe un polinomio mónico (coeficiente principal igual a 1) $p \in \mathbb{Z}[x]$ tal que $p\left(\frac{1}{2}\right) = 0$?

Ejercicio 9.5. Sean $p, q \in \mathbb{Z}[x]$ los polinomios $p = 3x^5 - 2x^3 + x^2 - 5x - 1$ y $q = 2x^4 - 3x^2 - x + 5$. Determinar:

(i) $\mathsf{gr}(p^2 - q^3)$;

(ii) el coeficiente de x^6 en pq;

(iii) $\mathsf{gr}(p + q^3)$;

(iv) el coeficiente de x^{10} en pq;

(v) si existe un polinomio $t \in \mathbb{Z}[x]$ tal que $p = tq$;

(vi) si existen enteros m, n tales que $p^n = q^m$.

Ejercicio 9.6. Sean $p, q \in \mathbb{Z}[x]$ los polinomios $p = x^3 - 2x + 3$ y $q = 2x^5 - 5x^4 + 3x^3 + 2x^2$. Hallar polinomios $t, r \in \mathbb{Z}[x]$ tales que $q = tp + r$ con $r = 0$ o $\mathsf{gr}(r) < 3$.

Ejercicio 9.7. Sea $\mathbb{Z}/4$ el anillo de enteros módulo 4.

[25] Se dice, entonces, que U es un subgrupo *cíclico* de $k^\times$

(i) Calcular los grados de p^2, pq y $q - h$, donde $p, q, h \in \mathbb{Z}/4\,[x]$ son los polinomios $p = 1 + 2x$, $q = 1 + 2x + 3x^2$ y $h = 2 - x + x^2$.

(ii) ¿Existen polinomios $t, s \in \mathbb{Z}/4\,[x]$, ambos no nulos, tales que $ts = 0$?

(iii) ¿Existen polinomios $t \in \mathbb{Z}/4\,[x]$ tales que $t^n = 0$ para algún $n \geq 0$, pero $t \neq 0$?

(iv) ¿Existen en $\mathbb{Z}/4\,[x]$ polinomios inversibles de grado mayor que 0?

Ejercicio 9.8. Si A es un dominio íntegro y $p, q \in A\,[x]$ son polinomios distintos del polinomio nulo, entonces $\mathsf{gr}(pq) = \mathsf{gr}(p) + \mathsf{gr}(q)$. Probar que A es un dominio íntegro, si y sólo si $A\,[x]$ lo es.

Ejercicio 9.9. Si A es un dominio íntegro, entonces los polinomios inversibles en $A\,[x]$ son exactamente los elementos inversibles en A, es decir, los polinomios de grado 0 que son unidades de A.

Ejercicio 9.10. Determinar los polinomios inversibles en $\mathbb{Z}/4\,[x]$ y en $\mathbb{Z}/5\,[x]$.

Ejercicio 9.11. Probar propiedades análogas a las de la relación de divisibilidad en $\mathbb{Z}$ para la relación de divisibilidad en polinomios.

Ejercicio 9.12. Si k es un cuerpo, dar una definición de primo (polinomios irreducibles) en $k\,[x]$ y enunciar y demostrar algunas de sus propiedades.

Ejercicio 9.13. El *máximo común divisor* entre dos polinomios no nulos $f, g \in k\,[x]$ con coeficientes en un cuerpo k se define como el polinomio *mónico* (coeficiente principal igual a 1) de grado máximo que divide a ambos.

(i) Probar la identidad de Bézout: que, si $h = (f, g)$ es el máximo común divisor de f y g, entonces existen polinomios p y q tales que $h = fp + gq$.

(ii) Probar que las siguientes afirmaciones sobre un polinomio $h \in k\,[x]$ son equivalentes:

   (a) h es *el* polinomio mónico de grado mínimo de la forma $h = fp + gq$ con $p, q \in k\,[x]$;

   (b) h es mónico, es divisor común de f y de g y es divisible por cualquier otro divisor común;

   (c) h es el máximo común divior de f y g.

Ejercicio 9.14. ¿Cómo se adapta la noción de primo (ver Ejercicio 9.12) al anillo de polinomios con coeficientes enteros $\mathbb{Z}\,[x]$? ¿Tiene sentido hablar de máximo común divisor en $\mathbb{Z}\,[x]$? ¿Se verifica la identidad de Bézout?

Parte III

Reciprocidad cuadrática

10 Reciprocidad y descenso

Usando el lenguaje desarrollado en la Parte I, podemos expresar algunas de las conjeturas de Fermat: si p es un primo impar,

$$\begin{aligned} p &= x^2 + y^2 \ , \quad x, y \in \mathbb{Z} \ , \quad \text{si y sólo si} \quad p \equiv 1 \,(\mathsf{mod}\, 4) \\ p &= x^2 + 2y^2 \ , \quad x, y \in \mathbb{Z} \ , \quad \text{si y sólo si} \quad p \equiv 1 \text{ o } 3 \,(\mathsf{mod}\, 8) \\ p &= x^2 + 3y^2 \ , \quad x, y \in \mathbb{Z} \ , \quad \text{si y sólo si} \quad p = 3 \text{ o } p \equiv 1 \,(\mathsf{mod}\, 3) \ . \end{aligned}$$

También tenemos la siguiente conjetura, un poco distinta de las tres anteriores: si p y q son primos impares distintos,

$$p \text{ y } q \equiv 3 \text{ o } 7 \,(\mathsf{mod}\, 20) \quad \text{implica} \quad pq = x^2 + 5y^2 \ , \quad x, y \in \mathbb{Z} \ .$$

Todas estas afirmaciones están relacionadas con el problema de representar un número en la forma $x^2 + ny^2$. La primera demostración de las primeras tres afirmaciones parece haber sido encontrada por Euler alrededor de cien años después de que Fermat las enunciara. La cuarta fue demostrada más tarde por Lagrange. Ver [Cox22, pp. 7–9].

Ejemplo 10.1. Si $p = x^2 + y^2$ con $x, y \in \mathbb{Z}$, entonces $p \equiv 1 \,(\mathsf{mod}\, 4)$, pues $x^2 \equiv 0$ o $x^2 \equiv 1$, dependiendo de si x es par o impar y, si p es un primo impar, x e y deben tener distinta paridad. Análogamente, si $p = x^2 + 2y^2$, entonces $p \equiv 1 \,(\mathsf{mod}\, 8)$ o bien $p \equiv 3 \,(\mathsf{mod}\, 8)$. Y, si $p = x^2 + 3y^2$, entonces $p = 3$ o bien $p \equiv 1 \,(\mathsf{mod}\, 3)$. **(ejercicio)**.

Teorema 10.2. *Un primo impar p se escribe como $x^2 + y^2$ con x e y enteros, si y sólo si $p \equiv 1 \,(\mathsf{mod}\, 4)$.*

Demostración. Vamos a probar que, si $p \equiv 1 \,(\mathsf{mod}\, 4)$, entonces existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$. La demostración estará dividida en dos pasos:

(Descenso) si p divide a una expresión del tipo $a^2 + b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$, entonces existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$;

(Reciprocidad) si $p \equiv 1 \,(\mathsf{mod}\, 4)$, entonces p divide a algún natural de la forma $a^2 + b^2$ con $a, b \in \mathbb{Z}$ y $(a, b) = 1$.

Probamos cada una de estas afirmaciones, a continuación. □

La idea de Fermat era, aparentemente, la siguiente: si p es primo, $p \equiv 1 \,(\mathsf{mod}\, 4)$ y p *no* se escribe como suma de dos cuadrados, debería existir un primo $p' < p$ que cumpla que es $p' \equiv 1 \,(\mathsf{mod}\, 4)$ y que tampoco es suma de dos cuadrados. Eventualmente, llegaríamos a 5 que sí es suma de dos cuadrados. De esta contradicción (de que 5 es y no debería ser suma de dos cuadrados) se deduciría el resultado.

Lema 10.3. *Sea N un natural que se puede expresar como suma de dos cuadrados* coprimos. *Si q es un divisor primo de N que se puede expresar como suma de dos cuadrados, entonces el cociente también se puede expresar como suma de dos cuadrados coprimos.*

Demostración. Por hipótesis, existen $a, b \in \mathbb{Z}$ tales que $N = a^2 + b^2$ y $(a, b) = 1$ y existen, además, $x, y \in \mathbb{Z}$ tales que $q = x^2 + y^2$ (x e y son, necesariamente, coprimos). Como $q \mid N$, se cumple que q divide a $(bx - ay)(bx + ay)$, pues

$$Nx^2 - a^2q \;=\; b^2x^2 + a^2x^2 - a^2x^2 - a^2y^2 \;=\; (bx)^2 - (ay)^2 \;=\; (bx - ay)\,(bx + ay)\;.$$

Como q es primo, $q \mid bx - ay$, o bien $q \mid bx + ay$. Cambiando el signo de a, podemos suponer que estamos en el primer caso. Esto quiere decir que existe $d \in \mathbb{Z}$ tal que $bx - ay = dq$. Ahora bien,

$$bx - dx^2 \;=\; bx - dq + dy^2 \;=\; ay + dy^2 \;=\; (a + dy)\,y\;.$$

Como $x \mid bx - dx^2$, se cumple que $x \mid (a + dy)y$. Pero $(x, y) = 1$, con lo que $x \mid a + dy$. Existe, entonces, $c \in \mathbb{Z}$ tal que $a + dy = cx$. O sea,

$$a \;=\; cx - dy \quad \text{y} \quad b \;=\; dx + cy\;.$$

Pero, entonces,

$$N \;=\; a^2 + b^2 \;=\; (cx - dy)^2 + (dx + cy)^2 \;=\; (c^2 + d^2)\,(x^2 + y^2) \;=\; (c^2 + d^2)\,q\;.$$

Así, $N/q = c^2 + d^2$, pero, además, $(a, b) = 1$ implica que $(c, d) = 1$ **(ejercicio)**. □

Observación 10.4. En la demostración del Lema 10.3 hicimos uso de la siguiente identidad **(ejercicio)**:

$$(cx - dy)^2 + (dx + cy)^2 \;=\; (c^2 + d^2)\,(x^2 + y^2)\;. \tag{8}$$

Ahora sí, probamos el paso de Descenso.

Lema 10.5 (Descenso)**.** *Sea p un primo impar que divide a una expresión del tipo a^2+b^2 donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$. Entonces, existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + y^2$.*

Demostración. La hipótesis es que $p \mid N = a^2+b^2$ y $(a, b) = 1$. Veamos, en primer lugar, que podemos asumir, además, que $|a| < p/2$ y que $|b| < p/2$. Cambiando a por $a-kp$ con algún k conveniente, conseguimos $|a-kp| < p/2$. Pero, $(a-kp)^2+b^2 = a^2+b^2-2kp+k^2p^2$. Como $p \mid a^2+b^2$, deducimos que p divide a $(a-kp)^2+b^2$. Cambiamos a por $a-kp$ y ahora p divide a una expresión $a_1^2 + b^2$, donde $|a_1| < p/2$. De la misma manera, conseguimos que p divida una expresión $N_1 := a_1^2 + b_1^2$ con $|b_1| < p/2$. Pero, al hacer estos cambios, podemos haber introducido divisores comunes entre a_1 y b_1. Es decir, puede pasar que $(a_1, b_1) > 1$. Sin embargo, dividiendo por (a_1, b_1), volvemos al caso coprimo. Veamos esto. Sea $d := (a_1, b_1)$. Por cómo fueron elegidos $a_1 = a - kp$ y $b_1 = b - lp$ con $k, l \in \mathbb{Z}$.

Como $(a,b)=1$, en particular, p no es un divisor común de a y de b. Pero, entonces, p tampoco es un divisor común de a_1 y de b_1. O sea, $(p,d)=1$. De esta manera, si $N_2 := N_1/d^2$, $a_2 := a_1/d$ y $b_2 := b_1/d$, entonces $a_2, b_2 \in \mathbb{Z}$, $|a_2| \leq |a_1| < p/2$ y $|b_2| \leq |b_1| < p/2$, $(a_2,b_2)=1$ y, finalmente, $p \mid N_2$ (aquí usamos que $(p,d)=1$).

Recapitulando, asumimos que $p \mid N$, donde $N = a^2+b^2$, $(a,b)=1$, $|a| < p/2$ y $|b| < p/2$. Bajo estas suposiciones adicionales, $N < p^2/2$. En particular, si $q \neq p$ es un divisor primo de N, debe ser $q < p$. Separamos dos casos: o bien todo tal q es suma de dos cuadrados, o bien existe un divisor primo q de N que no es suma de cuadrados. En el primer caso, por el Lema 10.3, se deduce, eliminando todos los factores primos distintos de p, que p también debe ser suma de cuadrados (notar que $p^2 \nmid N$). Supongamos, para llegar a una contradicción que p no es suma de cuadrados. Entonces, existiría un divisor primo de N, $q < p$, que tampoco es suma de cuadrados. Necesariamente, q debe ser impar ($2 = 1^2+1^2$) y, más aun, $q \equiv 1 \pmod 4$ (ver el Ejemplo 10.1). Pero, entonces, estaríamos en las mismas hipótesis del resultado que queremos probar: q es primo impar que divide a $N = a^2+b^2$, con la diferencia de que q es estrictamente más chico que p. Eventualmente, deberíamos llegar al menor primo con esta propiedad. Para terminar, notamos que el menor primo impar congruente con 1 módulo 4 es 5 que sí es suma de cuadrados ($5 = 2^2+1^2$). Llegamos a la siguiente contradicción 5 es suma de cuadrados, pero, por el proceso por el que *descendimos* hasta este primo, 5 no debería ser suma de cuadrados. Esta contradicción viene de suponer que el primo p del cual partimos no era suma de cuadrados. □

Lema 10.6 (Reciprocidad)**.** *Si p es un número primo impar y $p \equiv 1 \pmod 4$, entonces p divide a una expresión del tipo a^2+b^2 donde $a,b \in \mathbb{Z}$ y $(a,b)=1$.*

Demostración. Por hipótesis, $p-1 = 4k$, $k \in \mathbb{Z}$, y, entonces por el Teorema 3.23, como $\varphi(p) = p-1$, $x^{4k} \equiv 1 \pmod p$, para todo $x \in \mathbb{Z}$ coprimo con p (o sea, para todo $x \not\equiv 0 \pmod p$), o, lo que es lo mismo, $p \mid x^{4k}-1$. Pero $x^{4k}-1 = (x^{2k}-1)(x^{2k}+1)$. Como p es primo, $p \mid x^{2k}-1$ o bien $p \mid x^{2k}+1$. En términos de congruencias, para todo $x \in \mathbb{Z}$, $(x,p)=1$,

$$x^{2k}-1 \equiv 0 \pmod p \quad \text{o bien} \quad x^{2k}+1 \equiv 0 \pmod p\ .$$

Es decir, cada una de las $p-1$ clases de congruencia $\not\equiv 0$ módulo p es solución de alguna de estas dos ecuaciones de congruencia. Pero, como $2k < p$, existe $x \in \mathbb{Z}$ tal que $x^{2k}-1 \not\equiv 0 \pmod p$ **(ejercicio)**.[26] Entonces, debe ser $x^{2k}+1 \equiv 0 \pmod p$. Obtenemos el resultado eligiendo $a = x^k$ y $b = 1$. □

Ejercicios

Ejercicio 10.1. Verificar las siguientes identidades:

[26] Para dar una prueba de esto, se puede usar el resultado del Ejercicio 10.2. Usando los resultados de la § 9, se puede dar una demostración más algebraica. Más adelante, veremos otra demostración de que la cantidad de soluciones distintas a una ecuación de congruencia $f(x) \equiv 0 \pmod p$ está acotada por el grado del polinomio f (Lema **??**).

(i) $(x^2+y^2)\,(z^2+w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$;

(ii) $(x^2+ny^2)\,(z^2+nw^2) = (xz \pm nyw)^2 + n\,(xw \mp yz)^2$.

Generalizar y hallar una identidad del estilo

$$(ax^2+cy^2)\,(az^2+cw^2) \;=\; (¿?)^2 + ac\,(¿?)^2 \;.$$

Ejercicio 10.2. Sean p un número primo y

$$f \;=\; a_0 \,+\, a_1\,X \,+\, \cdots \,+\, a_{d-1}\,X^{d-1} \,+\, X^d$$

un polinomio mónico (coeficiente principal = 1) de grado $d < p$. Una de las conclusiones de este ejercicio será que $f(x) \not\equiv 0 \,(\mathsf{mod}\, p)$ tiene solución, es decir, existe $x \in \mathbb{Z}$ tal que $f(x) \not\equiv 0 \,(\mathsf{mod}\, p)$. Dicho de otra manera, $f(x) \equiv 0 \,(\mathsf{mod}\, p)$, con f de grado $d < p$, no puede tener p soluciones disitintas módulo p. Con este objetivo, definimos Δf como el polinomio

$$\Delta f \;=\; f(X+1) \;-\; f(X)\;;$$

podemos iterar y definir $\Delta^{k+1} f = \Delta(\Delta^k f)$. Probar las siguientes afirmaciones:

(i) si $k \geq 1$, entonces $\Delta^k f$ es una combinación lineal de $f(X)$, $f(X+1)$, $\ldots$, $f(X+k)$ con coeficientes enteros;

(ii) si $k = d$, el polinomio $\Delta^d f$ es constante: $\Delta^d f(X) = d!$;

(iii) existe $x \in \mathbb{Z}$ tal que $f(x) \not\equiv 0 \,(\mathsf{mod}\, p)$.[27]

Ejercicio 10.3. Probar la siguiente versión análoga del Lema 10.3:

> *Sea $n > 0$ un número entero positivo y sea N un natural que se puede expresar como $N = a^2 + nb^2$ con $a, b \in \mathbb{Z}$ y $(a, b) = 1$. Si q es un divisor primo de N que no divide a n y se puede expresar como $q = x^2 + ny^2$, entonces el cociente N/q también se puede expresar como $c^2 + nd^2$ con $c, d \in \mathbb{Z}$ y $(c, d) = 1$.*

Probar, además, que esto es cierto también si $n = 3$ y $q = 4$.

Ejercicio 10.4. Sea q un primo y sea $N = a^2 + mqb^2$ un natural ($n = mq$) donde $a, b, m \in \mathbb{Z}$. Probar que, si q divide a N, entonces $N/q = mc^2 + qd^2$ donde $c, d \in \mathbb{Z}$. Probar, además, que, si $(a, b) = 1$, entonces $(c, d) = 1$.

Ejercicio 10.5. Probar las siguientes versiones análogas del Lema 10.5 para $n = 2, 3$:

> *Sea p un primo que divide a una expresión del tipo $a^2 + 2b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$. Entonces, existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + 2y^2$.*
>
> *Sea p un primo impar que divide a una expresión del tipo $a^2 + 3b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$. Entonces, existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + 3y^2$.*

[27] Hint: si $f(x) \not\equiv 0 \,(\mathsf{mod}\, p)$ *no admitiera soluciones*, entonces por (i), $p \mid \Delta^d f$ y, por (ii) (y $d < p$) esto es imposible.

Ejercicio 10.6. Probar la siguiente versión análoga del Lema 10.6:

> *Si p es primo y $p \equiv 1 \pmod 3$, entonces p divide a una expresión del tipo $a^2 + 3b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$,*

usando, por ejemplo, la siguiente identidad:

$$4\,(x^{3k} - 1) \;=\; 4\,(x^{2k} + x^k + 1)\,(x^k - 1) \;=\; ((2x^k + 1)^2 + 3)\,(x^k - 1)\;.$$

Ejercicio 10.7. Probar que si $p \equiv 1 \pmod 8$ es primo, entonces p divide a una expresión del tipo $a^2 + 2b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$, usando la siguiente identidad:

$$x^{8k} - 1 \;=\; ((x^{2k} - 1)^2 + 2x^{2k})\,(x^{4k} - 1)\;.$$

Mostrar que existen primos $p \equiv 3 \pmod 8$ que dividen a números de la forma $a^2 + 2b^2$.

Ejercicio 10.8. Para cada primo $p \equiv 1 \pmod 3$, $p \leq 50$, buscar todos los valores $x, y \in \mathbb{Z}$ tales que $p = x^2 + 3y^2$.

Ejercicio 10.9. En este ejercicio investigaremos condiciones que sirvan para determinar si un primo divide a una expresión de la forma $a^2 + 5b^2$ donde $a, b \in \mathbb{Z}$ y $(a, b) = 1$.

(i) Calcular que, si p es un primo que divide a un natural de la forma $a^2 + 5b^2$ con $a, b \leq 40$ y $(a, b) = 1$, entonces p puede ser $\equiv 1, 3, 2, 4 \pmod 5$. O sea, en este caso, mirar congruencia módulo 5 no parece dar información acerca de si un primo divide o no a un natural de la forma $a^2 + 5b^2$.

(ii) Hallar primos $p \equiv 2, 4 \pmod 5$ que no dividen a ningún natural de la forma $a^2 + 5b^2$ con $a, b \leq 40$ y $(a, b) = 1$ (dicho de otra manera, que no aparecen entre los divisores de ninguno de estos números).

(iii) Calcular que, si p es un primo que divide a un natural de la forma $a^2 + 5b^2$ con $a, b \leq 40$ y $(a, b) = 1$, entonces $p \equiv 1, 3, 7, 9 \pmod{20}$.

Ejercicio 10.10. En este ejercicio investigamos otras formas de representar. En las siguientes afirmaciones, $a, b \in \mathbb{Z}$, $(a, b) = 1$ y $|a|, |b| \leq 40$.

(i) Determinar las posibles clases de congruencia módulo 28 de los primos p que dividen a los enteros $a^2 + 7b^2$.

(ii) Determinar las posibles clases de congruencia módulo 12 de los primos p que dividen a los enteros $a^2 - 3b^2$.

(iii) Determinar las posibles clases de congruencia módulo 20 de los primos p que dividen a los enteros $a^2 - 5b^2$.

(iv) Determinar las posibles clases de congruencia módulo 28 de los primos p que dividen a los enteros $a^2 - 7b^2$.

Notar que en los casos (ii), (iii) y (iv) las clases obtenidas se pueden representar como $\pm\beta^2$ donde β es un número impar.

11 La ecuación $p = x^2 + ny^2$ y Reciprocidad cuadrática

El Teorema 10.2 caracteriza los primos impares que se pueden expresar como suma de dos cuadrados enteros. Nuestro objetivo será entender en qué medida es posible adaptar el método que nos permitió demostrar este resultado para estudiar la ecuación $p = x^2+ny^2$.

El argumento de la demostración del Teorema 10.2 fue dividido en tres afirmaciones, agrupadas en dos partes: las dos primeras (Lema 10.3 y Lema 10.5) constituyen lo que llamamos "paso de descenso"; a la tercera (Lema 10.6) le dimos el nombre de "paso de reciprocidad". El Lema 10.3 depende de la identidad (8). Esta identidad se generaliza y, con ella, el resultado del Lema 10.3. Sin embargo, el argumento de la demostración del Lema 10.5 tiene sus limitaciones: depende de una cota que se adapta casi sin cambios a los casos $n = 2$ y $n = 3$, per que falla para $n \geq 4$. Más aun, la afirmación misma del Lema 10.5 puede ser falsa para $n \geq 4$, si se traduce literalmente. Por ejemplo,

- si $n = 5$, $3 \mid 21 = 1^2 + 5 \cdot 2^2$, pero $3 \neq x^2 + 5y^2$, pues $3 < 5$;
- si $n = 6$, $5 \mid 25 = 1^2 + 6 \cdot 2^2$, pero $5 \neq x^2 + 6y^2$, pues $5 < 6$.

¿Es cierto que si p divide a un natural de la forma $a^2 + nb^2$ con $(a, b) = 1$ entonces p se puede expresar en la forma $x^2 + ny^2$?

¿Qué pasa con $n = 4$ o $n = 7$? Si bien es cierto que, por ejemplo, $3 \neq x^2 + 4y^2$ y que $5 \neq x^2 + 7y^2$ ¿pueden 3 ser un divisor de un natural de la forma $a^2 + 4b^2$ o 5 un divisor de un natural de la forma $a^2 + 7b^2$ con $(a, b) = 1$? Deliberadamente estamos mirando $p < n$, pues, así, nos aseguraríamos de que $p \neq x^2 + ny^2$. Pero ¿si buscáramos $p \geq n$, encontraríamos un p tal que $p \mid a^2 + 4b^2$, pero $p \neq x^2 + 4y^2$, o tal que $p \mid a^2 + 7b^2$, pero $p \neq x^2 + 7y^2$? ¿Si $n \geq 8$? ¿Existen contraejemplos?

- para $n = 8$, se cumple $3 \mid 12 = 2^2 + 8 \cdot 1^2$, pero $3 \neq x^2 + 8y^2$ (ni 5 ni 7 funcionan);
- para $n = 9$, se cumple $5 \mid 10 = 1^2 + 9 \cdot 1^2$, pero $5 \neq x^2 + 9y^2$ (7 no funciona);
- para $n = 10$, se cumple $7 \mid 14 = 2^2 + 10 \cdot 1^2$, pero $7 \neq x^2 + 10y^2$ (3 no funciona);
- para $n = 11$, se cumple $3, 5 \mid 15 = 2^2+11 \cdot 1^2$, pero $3, 5 \neq x^2+11y^2$ (7 no funciona).

Vamos a poder decir algo más acerca de estas preguntas, una vez que hablemos de formas cuadráticas, reducción, sus clases de equivalencia y los números de clases.

Ya vemos que nos encontramos con algunas dificultades al querer estudiar el problema en general, en relación con el paso de descenso. Por otro lado, con respecto a reciprocidad, el Lema 10.6 nos muestra que una condición de congruencia garantiza que un primo impar divida una suma de cuadrados. Si bien la demostración de este resultado puede parecer *ad hoc*, veremos cómo rescatar la idea del enunciado. Precisamente, vamos a ver que existen condiciones de congruencia sobre un primo impar, $(p, n) = 1$, que garantizan que $p \mid a^2 + nb^2$, $(a, b) = 1$.

Definición 11.1. Dados un entero $a \in \mathbb{Z}$ y un primo impar p (> 0), decimos que a *es un residuo cuadrático módulo* p, si $p \nmid a$ y si la ecuación $x^2 \equiv a \pmod{p}$ tiene solución módulo p. El *símbolo de Legendre* (a/p) es:

$$\left(\frac{a}{p}\right) := \begin{cases} 0\ , & \text{si } p \mid a\ , \\ 1\ , & \text{si } p \nmid a \text{ y } a \text{ es residuo cuadrático,} \\ -1\ , & \text{si } p \nmid a \text{ y } a \text{ no es residuo cuadrático.} \end{cases}$$

Observación 11.2. Los enteros 0, 1 y todos los cuadrados perfectos son residuos cuadráticos módulo cualquier entero. En particular, $\left(n^2/p\right) = 1$ para todo primo impar p y todo entero n coprimo con p.

Lema 11.3. *Sea $n \in \mathbb{Z}$, $n \neq 0$, y sea p un primo impar que no divide a n. Entonces, existen $a, b \in \mathbb{Z}$ tales que $p \mid a^2 + nb^2$ y $(a, b) = 1$, si y sólo si $(-n/p) = 1$.*

Demostración. Supongamos que $a, b \in \mathbb{Z}$ son tales que $p \mid a^2 + nb^2$. Entonces, $x^2 \equiv -ny^2 \pmod{p}$. Si $p \nmid n$, debe ser $p \mid a$, si y sólo si $p \mid b$. Si, además, $(a, b) = 1$, entonces $p \nmid a$ y $p \nmid b$. En particular, $(b^{-1}a)^2 \equiv -n \pmod{p}$ y, así, $(-n/p) = 1$. Completar la demostración **(ejercicio)**. □

Pregunta 11.4. ¿Existen condiciones de congruencia sobre un primo impar p que garanticen que $(-n/p) = 1$?

Veamos con un poco más de cuidado qué podría querer decir "condiciones de congruencia". En el caso $n = 1$, suma de dos cuadrados, la condición es $p \equiv 1 \pmod{4}$. Sea $f(x, y) = x^2 + ny^2$. Podemos tratar de entender la situación calculando distintos valores que la función f toma, con $x, y \in \mathbb{Z}$ tales que $(x, y) = 1$, y luego factorizando cada uno de estos valores obtenidos, para buscar sus factores primos. La Tabla 2 y la Tabla 3 muestran los primos obtenidos de esta manera, para distintos valores de n, variando x e y en un cierto rango, agrupados de acuerdo a su clase de congruencia módulo $4|n|$. Dicho de otra manera, la tabla muestra las distintas *clases de congruencia módulo* $4|n|$ *representadas por primos que se obtienen como factores de enteros de la forma* $a^2 + nb^2$ *con* a *y* b *coprimos.*

Asumiendo que los valores de p que no aparecen son tales que $(-n/p) = -1$ (lo cual no hemos demostrado), se pueden conjeturar algunas propiedades del símbolo. Por ejemplo, de la Tabla 3, mirando las filas para $n = -2$, $n = -3$ y $n = -6$,

$$\left(\frac{6}{p}\right) = 1 \quad \text{si y sólo si} \quad p \equiv 1, 5, 19, 23 \pmod{24}\ ,$$

que equivale a

$$\begin{cases} p \equiv 1 \pmod{8} \text{ y} \\ p \equiv 1 \pmod{3}\ , \end{cases} \quad \begin{cases} p \equiv 5 \pmod{8} \text{ y} \\ p \equiv 2 \pmod{3}\ , \end{cases} \quad \begin{cases} p \equiv 3 \pmod{8} \text{ y} \\ p \equiv 1 \pmod{3}\ , \end{cases} \quad \text{o} \quad \begin{cases} p \equiv 7 \pmod{8} \text{ y} \\ p \equiv 2 \pmod{3}\ . \end{cases}$$

n	$(-n/p) = 1$
2	$p \equiv 1, 3 \pmod 8$
3	$p \equiv 1, 7 \pmod{12}$
5	$p \equiv 1, 3, 7, 9 \pmod{20}$
7	$p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$
11	$p \equiv 1, 3, 5, 9, 15, 23, 25, 27, 31, 37 \pmod{44}$
13	$p \equiv 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49 \pmod{52}$
17	$p \equiv 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63 \pmod{68}$
6	$p \equiv 1, 5, 7, 11 \pmod{24}$
10	$p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$
14	$p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}$
15	$p \equiv 1, 17, 19, 23, 31, 47, 49, 53 \pmod{60}$
21	$p \equiv 1, 5, 11, 17, 19, 23, 25, 31, 37, 41, 55, 71 \pmod{84}$
1	$p \equiv 1 \pmod 4$
4	$p \equiv 1, 5, 9, 13 \pmod{16}$

Tabla 2: Divisores primos de $a^2 + nb^2$ con $(a, b) = 1$ y $1 \leq a, b \leq 50$.

n	$(-n/p) = 1$
-2	$p \equiv 1, 7 \pmod 8$
-3	$p \equiv 1, 11 \pmod{12}$
-5	$p \equiv 1, 9, 11, 19 \pmod{20}$
-7	$p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}$
-11	$p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$
-13	$p \equiv 1, 3, 9, 17, 23, 25, 27, 29, 35, 43, 49, 51 \pmod{52}$
-17	$p \equiv 1, 9, 13, 15, 19, 21, 25, 33, 35, 43, 47, 49, 53, 55, 59, 67 \pmod{68}$
-6	$p \equiv 1, 5, 19, 23 \pmod{24}$
-10	$p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}$
-14	$p \equiv 1, 5, 9, 11, 13, 25, 31, 43, 45, 47, 51, 55 \pmod{56}$
-15	$p \equiv 1, 7, 11, 17, 43, 49, 53, 59 \pmod{60}$
-21	$p \equiv 1, 5, 17, 25, 37, 41, 43, 47, 59, 67, 79, 83 \pmod{84}$
-1	$p \equiv 1, 3 \pmod 4$
-4	$p \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16}$

Tabla 3: Divisores primos de $a^2 + nb^2$ con $(a, b) = 1$ y $1 \leq |a|, |b| \leq 50$.

Pero esto es lo mismo que

$$\begin{cases} p \equiv 1 \pmod 8 \text{ y} \\ p \equiv 1 \pmod{12} , \end{cases} \begin{cases} p \equiv 5 \pmod 8 \text{ y} \\ p \equiv 5 \pmod{12} , \end{cases} \begin{cases} p \equiv 3 \pmod 8 \text{ y} \\ p \equiv 7 \pmod{12} , \end{cases} \text{o} \begin{cases} p \equiv 7 \pmod 8 \text{ y} \\ p \equiv 11 \pmod{12} , \end{cases}$$

que equivale a

$$\begin{cases} (2/p) = 1 \quad \text{y} \\ (3/p) = 1 , \end{cases} \text{o} \begin{cases} (2/p) = -1 \quad \text{y} \\ (3/p) = -1 . \end{cases}$$

Expresado de otra manera,

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) .$$

Otra cosa que se puede observar es que, en la Tabla 3, en los casos en que $n = -q$ con q primo, las clases representadas son equivalentes a $\pm\beta^2$ con β impar, $\beta < q$. Sin embargo, esta observación deja de ser válida si n es compuesto. Por ejemplo, si $n = -6$, las clases módulo 24 representadas por factores primos p tales que $(6/p) = 1$ son, de acuerdo con la tabla, 1, 5, 19 y 23. Por otro lado, los cuadrados módulo 24 son 1, 4, 9, 12 y 16. En particular, sólo 1 y 23 son de la forma $\pm\beta^2$ con β impar (y coprimo con 24).

Teorema 11.5. *Si $p, q > 0$ son primos impares distintos, entonces*

$$\left(\frac{q}{p}\right) = 1 \text{ , si y sólo si } p \equiv \pm\beta^2 \pmod{4q} ,$$

para cierto $\beta \in \mathbb{Z}$ impar.

El Teorema 11.5 relaciona residuos cuadráticos módulo p con residuos módulo $4q$, si p y q son primos positivos, impares y distintos: q es cuadrado módulo p, si y sólo si $\pm p$ es cuadrado módulo $4q$ ¿Qué se puede decir si n es compuesto? ¿Qué pasa si $n > 0$? ¿Hay relación entre $(-n/p)$ y (n/p)? En la § 3, vimos que las ecuaciones de congruencia $ax \equiv b \pmod m$ tienen solución exactamente cuando $(a, m) \mid b$ ¿Hay alguna manera de saber si $x^2 \equiv D \pmod{4k}$ tiene soluciones? Antes de pasar a estudiar el símbolo de Legendre, veamos cómo podemos usarlo para dar respuesta a la Pregunta 11.4.

En primer lugar, con respecto al Teorema 11.5, ¿podemos precisar, en la congruencia $p \equiv \pm\beta^2$, en qué casos el signo debería ser $+$ y en qué casos debería ser $-$? De la Tabla 3, a partir de la cual formulamos el Teorema 11.5, vemos que $p \equiv +\beta^2 \pmod{4q}$, si $p \equiv 1 \pmod 4$, y que $p \equiv -\beta^2 \pmod{4q}$, si $p \equiv 3 \pmod 4$. Esto tiene sentido: los únicos cuadrados módulo 4 son los $\equiv 1 \pmod 4$. Pero, entonces, el signo debería ser

$$\pm = (-1)^{\frac{p-1}{2}} .$$

En definitiva, $p \equiv \pm\beta^2 \pmod{4q}$ quiere decir

$$p \equiv (-1)^{\frac{p-1}{2}} \beta^2 \pmod{4q} ;$$

no hay ambigüedad en el signo. Si escribimos $p^* := (-1)^{\frac{p-1}{2}} p$, entonces $p^* \equiv 1 \pmod 4$ y, en particular **(ejercicio)**, las siguientes afirmaciones son equivalentes:

- $p \equiv \pm\beta^2 \pmod{4q}$,
- $p^* \equiv \beta^2 \pmod{4q}$,
- $p^* \equiv \beta^2 \pmod{q}$,
- $(p^*/q) = 1$.

Lema 11.6. *El Teorema 11.5 es equivalente a la afirmación: para todo par de primos positivos, impares y distintos, p y q,*

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) .$$

Demostración. De lo anterior, $p \equiv \pm\beta^2 \pmod{4q}$, si y sólo si $(p^*/q) = 1$. Por lo tanto, el Teorema 11.5 es equivalente a $(q/p) = 1$, si y sólo si $(p^*/q) = 1$, para todo par de primos positivos, impares y distintos. Pero (q/p) y (p^*/q) son ± 1, con lo que la afirmación "$(q/p) = 1$, si y sólo si $(p^*/q) = 1$" equivale a $(q/p) = (p^*/q)$. □

El Teorema 11.7 resume algunas de las propiedades del símbolo de Legendre; su demostración la dejamos para la § 12.

Teorema 11.7. *Sea $p > 0$ un primo impar. Entonces, se cumple*

(i) $(n/p) = (n'/p)$, *si* $n \equiv n' \pmod{p}$;

(ii) $(ab/p) = (a/p)\,(b/p)$, *para todo par* $a, b \in \mathbb{Z}$;

(iii) $(-1/p) = (-1)^{\frac{p-1}{2}}$ *y, más en general,* $(n/p) \equiv n^{\frac{p-1}{2}} \pmod{p}$, *para todo* $n \in \mathbb{Z}$:

(iv) $(2/p) = (-1)^{\frac{p^2-1}{8}}$;

(v) $(q/p) = (p^*/q)$, *si q es un primo positivo, impar y distinto de p.*

Observación 11.8. El ítem (iii) es equivalente a

$$\left(\frac{-1}{p}\right) = \begin{cases} 1\ , & \text{si } p \equiv 1 \pmod{4} \quad \text{y} \\ -1\ , & \text{si } p \equiv 3 \pmod{4}\ . \end{cases}$$

El ítem (iv) equivale a

$$\left(\frac{2}{p}\right) = \begin{cases} 1\ , & \text{si } p \equiv 1, 7 \pmod{8} \quad \text{y} \\ -1\ , & \text{si } p \equiv 3, 5 \pmod{8}\ . \end{cases}$$

El ítem (v) lo podemos reescribir como

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) ,$$

o bien como

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} .$$

Este último es, de acuerdo con el Lema 11.6, equivalente al Teorema 11.5.

El Lema 11.6 nos permitió reinterpretar el problema de encontrar condiciones de congruencia que garanticen que un primo impar divida a una expresión de la forma a^2+nb^2 con $(a,b)=1$ en términos del símbolo de Legendre. El Lema 11.9 nos permitirá reinterpretar el problema en términos más algebraicos (Teorema 11.10).

Lema 11.9. *Si $D \equiv 0, 1 \pmod 4$, $D \neq 0$, existe una única función $\chi(m)$, $m \in \mathbb{Z}$, que cumple que:*

(1) $\chi(m) = \chi(m')$, si $m \equiv m' \pmod D$,

(2) $\chi(mn) = \chi(m)\chi(n)$, para todo par $m, n \in \mathbb{Z}$,

(3) $\chi(p) = (D/p)$, si p es un primo (positivo) impar que no divide a D y

(4) $\chi(m) = 0$, si $(m, D) > 1$.

Juntando el Lema 11.9 con el Lema 11.3 obtenemos la siguiente consecuencia.

Teorema 11.10. *Sean $n \in \mathbb{Z}$, $n \neq 0$, y χ la función del Lema 11.9 ($D = -4n$). Entonces, si p es un primo positivo impar que no divide a n, las siguientes afirmaciones son equivalentes:*

(a) existen $a, b \in \mathbb{Z}$ tales que $p \mid a^2 + nb^2$ y $(a, b) = 1$;

(b) $(-n/p) = 1$;

(c) $\chi(p) = 1$.

De esta manera, obtenemos lo que buscábamos (o, por lo menos, en teoría). Si p es un primo impar que no divide a n, existen $a, b \in \mathbb{Z}$ tales que $p \mid a^2 + nb^2$ y $(a, b) = 1$, si y sólo si p pertenece a determinadas clases de congruencia: aquellas clases módulo $4|n|$ en las que χ toma el valor 1.[28]

A continuación, demostramos el Lema 11.9 asumiendo las propiedades del símbolo de Legendre enunciadas en el Teorema 11.7.

Demostración del Lema 11.9. Esencialmente, tanto existencia, como unicidad de la función χ, dependen del hecho de que todo número entero coprimo con D es congruente, módulo D, a un entero positivo, impar y coprimo con D.[29]

Con respecto a la unicidad, supongamos que χ posee las propiedades deseadas. Entonces, cuando $m \in \mathbb{Z}$,

- si $(m, D) > 1$, $\chi(m) = 0$;
- si $(m, D) = 1$,

[28] Para hacer las cosas explícitas deberíamos poder calcular esta función χ.

[29] Más aun, el teorema de Dirichlet sobre primos en progresiones aritméticas garantiza que toda clase de congruencia módulo D coprima con D contiene algún número primo positivo impar.

– si $m < 0$, se cumple que $m + kD > 0$ para algún $k \in \mathbb{Z}$, $m + kD \equiv m \,(\mathsf{mod}\, D)$ y $\chi(m + kD) = \chi(m)$;
– si m es par, debía ser $D \equiv 1 \,(\mathsf{mod}\, 4)$ y, en consecuencia, $m + |D|$ es impar, $m + |D| \equiv m \,(\mathsf{mod}\, D)$ y $\chi(m + |D|) = \chi(m)$;
– si m es impar y positivo, se escribe como producto de primos positivos impares, $m = p_1 \cdots p_r$ (posiblemente, con repeticiones), con lo que

$$\chi(m) \;=\; \chi(p_1) \cdots \chi(p_r) \;=\; \left(\frac{D}{p_1}\right) \cdots \left(\frac{D}{p_r}\right) .$$

En cualquier caso, al ser $\chi(mn) = \chi(m)\chi(n)$, χ queda determinada por su valor en los primos impares que no dividen a D y por la condición $\chi(m) = 0$, si $(m, D) > 1$.

Para probar la existencia, introducimos el símbolo de Jacobi, que se puede interpretar como una extensión del símbolo de Legendre. Dados $M, m \in \mathbb{Z}$, $m > 0$, si $m = p_1 \cdots p_r$ es la factorización de m en producto de primos (posiblemente, con repeticiones), el *símbolo de Jacobi* $\left(\frac{M}{m}\right)$ es

$$\left(\frac{M}{m}\right) \;=\; \left(\frac{M}{p_1}\right) \cdots \left(\frac{M}{p_r}\right) ,$$

donde, del lado derecho, (M/p_i) denota el símbolo de Legendre. El símbolo de Jacobi tiene propiedades análogas a las del símbolo de Legendre **(ejercicio)**:

(I) $(N/m) = (N'/m)$, si $N \equiv N' \,(\mathsf{mod}\, m)$,

(II) $(AB/m) = (A/m)\,(B/m)$, para todo par $A, B \in \mathbb{Z}$,

(III) $(-1/m) = (-1)^{\frac{m-1}{2}}$,

(IV) $(2/m) = (-1)^{\frac{m^2-1}{8}}$,

(V) $(M/m) = (m^*/M)$, si M es positivo, impar y $(M, m) = 1$, donde $m^* = (-1)^{\frac{m-1}{2}} m$.

En particular, en (V), si $M \equiv 1 \,(\mathsf{mod}\, 4)$, entonces $(M/m) = (m/M)$.

El símbolo de Jacobi tiene también la propiedad multiplicativa:

$$\left(\frac{M}{mn}\right) \;=\; \left(\frac{M}{m}\right)\left(\frac{M}{n}\right) , \tag{9}$$

si $m, n > 0$. Pero, además, el símbolo de Jacobi tiene la siguiente propiedad adicional: si $D \in \mathbb{Z}$, $D \neq 0$ y $D \equiv 0, 1 \,(\mathsf{mod}\, 4)$, entonces

$$\left(\frac{D}{m}\right) \;=\; \left(\frac{D}{n}\right) , \tag{10}$$

si $m, n \in \mathbb{Z}$, $m, n > 0$, impares y $m \equiv n \,(\mathsf{mod}\, D)$. Aceptando las propiedades (9) y (10), definimos la siguiente función $\chi(m)$, dado $m \in \mathbb{Z}$:

- si $(m, D) > 1$, $\chi(m) := 0$;
- si $(m, D) = 1$,
  - si $m < 0$, se cumple que $m + kD > 0$ para algún $k \in \mathbb{Z}$, $m + kD \equiv m \,(\mathsf{mod}\, D)$ y $\chi(m + kD) := \chi(m)$;
  - si m es par, debía ser $D \equiv 1 \,(\mathsf{mod}\, 4)$ y, en consecuencia, $m + |D|$ es impar, $m + |D| \equiv m \,(\mathsf{mod}\, D)$ y $\chi(m + |D|) := \chi(m)$;
  - si m es impar y positivo, $\chi(m) := (D/m)$.

La propiedad (10) muestra que χ está bien definida y, junto con (9) y las propiedades del símbolo de Jacobi, se deducen las propiedades mencionadas en el enunciado. □

Lema 11.11. *El símbolo de Jacobi tiene las propiedades* (9) *y* (10).

Demostración. En cuanto a (9), si $m = p_1 \cdots p_r$ y $n = q_1 \cdots q_s$, entonces $mn = p_1 \cdots p_r q_1 \cdots q_s$ es la factorización de mn y

$$\left(\frac{M}{mn}\right) = \left(\frac{M}{p_1}\right) \cdots \left(\frac{M}{p_r}\right) \left(\frac{M}{q_1}\right) \cdots \left(\frac{M}{q_s}\right) = \left(\frac{M}{m}\right) \left(\frac{M}{n}\right).$$

En cuanto a (10), sean $D \equiv 0, 1 \,(\mathsf{mod}\, 4)$, $D \neq 0$ y sean $m, n > 0$ impares tales que $m \equiv n \,(\mathsf{mod}\, D)$. Queremos ver que $(D/m) = (D/n)$. Notemos que $(m, D) = (n, D)$, con lo cual $(D/m) = 0$, si y sólo si $(D/n) = 0$. En particular, si m y n no son coprimos con D, $(D/m) = (D/n)$ (ambos siendo iguales a 0). En lo que queda, asumiremos que $(m, D) = (n, D) = 1$.

Supongamos, en primer lugar, que $D \equiv 1 \,(\mathsf{mod}\, 4)$ y $D > 0$. Entonces, por (V),

$$\left(\frac{D}{m}\right) = \left(\frac{m^*}{D}\right) = \left(\frac{m}{D}\right) = \left(\frac{n}{D}\right) = \left(\frac{n^*}{D}\right) = \left(\frac{D}{n}\right).$$

Manteniendo la hipótesis $D \equiv 1 \,(\mathsf{mod}\, 4)$, supongamos, en segundo lugar, que $D < 0$. Entonces, $|D| \equiv 3 \,(\mathsf{mod}\, 4)$, con lo cual,

$$\left(\frac{D}{m}\right) = \left(\frac{|D|}{m}\right) \left(\frac{-1}{m}\right) = \left(\frac{m^*}{|D|}\right) \left(\frac{-1}{|D|}\right) = \left(\frac{m}{|D|}\right).$$

Como lo mismo es cierto para n, y $(n/|D|) = (m/|D|)$, se deduce que $(D/m) = \left(\frac{D}{n}\right)$, en este caso.

Supongamos, ahora, que $D \equiv 0 \,(\mathsf{mod}\, 4)$ y que $D = 2^{2k+\delta} D_0$, donde $k \geq 1$, $\delta \in \{0, 1\}$ y D_0 es impar. Entonces, vale que

$$\left(\frac{D}{m}\right) = \left(\frac{2}{m}\right)^{\delta} \left(\frac{D_0}{m}\right)$$

y lo mismo para n en lugar de m. Además, como $4 \mid D$, debe ser $m \equiv n \,(\mathsf{mod}\, 4)$ y, por lo tanto,

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = (-1)^{\frac{n-1}{2}} = \left(\frac{-1}{n}\right).$$

Para terminar, vamos a ver que $(2/m) = (2/n)$, si $\delta \neq 0$, y que $(D_0/m) = (D_0/n)$. Primero, si $\delta \neq 0$, en particular vale que $8 \mid D$ y, en consecuencia, $m \equiv n \,(\mathsf{mod}\, 8)$. Pero, entonces,

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = (-1)^{\frac{n^2-1}{8}} = \left(\frac{2}{n}\right).$$

Por último, $D_0 \equiv 1, 3 \,(\mathsf{mod}\, 4)$. En el caso en que $D_0 \equiv 1 \,(\mathsf{mod}\, 4)$ (sea positivo o negativo), por el caso anterior (el caso $D \equiv 1 \,(\mathsf{mod}\, 4)$), sabemos que $(D_0/m) = (D_0/n)$. Si, en el otro caso, $D_0 \equiv 3 \,(\mathsf{mod}\, 4)$, entonces, para $D_0 > 0$,

$$\left(\frac{D_0}{m}\right) = \left(\frac{m^*}{D_0}\right) = \left(\frac{m}{D_0}\right)\left(\frac{(-1)^{\frac{m-1}{2}}}{D_0}\right) = \left(\frac{n}{D_0}\right)\left(\frac{(-1)^{\frac{n-1}{2}}}{D_0}\right) = \left(\frac{n^*}{D_0}\right) = \left(\frac{D_0}{n}\right),$$

y, para $D_0 < 0$, $|D_0| \equiv 1 \,(\mathsf{mod}\, 4)$, con lo que,

$$\left(\frac{D_0}{m}\right) = \left(\frac{|D_0|}{m}\right)\left(\frac{-1}{m}\right) = \left(\frac{|D_0|}{n}\right)\left(\frac{-1}{n}\right) = \left(\frac{D_0}{n}\right).$$

□

Observación 11.12. Tanto en la demostración del Lema 11.9, como en la demostración del Lema 11.11, hicimos uso de las propiedades (I), (II), (III), (IV) y (V), que, a su vez, dependen de las propiedades análogas del símbolo de Legendre. Por otro lado, la función χ del Lema 11.9 *no es* el símbolo de Jacobi: el símbolo de Jacobi (M/m) sólo está definido para valores impares y positivos de m. Sin embargo, χ está definida en todo $\mathbb{Z}$.

Apéndice

El Lema 11.9 tiene una versión equivalente expresada en el lenguaje de grupos:

Lema 11.13. *Si $D \equiv 0, 1 \,(\mathsf{mod}\, 4)$, $D \neq 0$, existe un único morfismo de grupos $\chi : U\big(D\big) \to \{\pm 1\}$ tal que $\chi\,[p] = (D/p)$, si p es un primo (positivo) impar que no divide a D.*

De la misma manera, el ítem (c) del Teorema 11.10 se traduce en que la clase del primo pertenezca al núcleo del morfismo: $[p] \in \mathsf{ker}\, \chi \leq U\big(4|n|\big)$.

Observación 11.14. Se puede probar, conociendo la estructura de los grupos abelianos finitos $U\big(q\big)$ (q primo impar), $U\big(4\big)$ y $U\big(8\big)$, que el Lema 11.13 (o, equivalentemente, el Lema 11.9) y el Teorema 11.7 son equivalentes: asumiendo la existencia de los morfismos $\chi :\, U\big(D\big) \to \{\pm 1\}$, se pueden deducir las propiedades del símbolo de Legendre.

Ejercicios

Ejercicio 11.1. Sea $D \equiv 0, 1 \pmod 4$, $D \neq 0$, y sea $\chi : \mathbb{Z} \to \{\pm 1\}$ la función del Lema 11.9 (o, equivalentemente, el morfismo del Lema 11.13).

(i) Probar que

$$\chi(-1) = \begin{cases} 1\ , & \text{si } D > 0 \quad \text{y} \\ -1\ , & \text{si } D < 0\ . \end{cases}$$

(ii) Probar que, si $D \equiv 1 \pmod 4$, entonces

$$\chi(2) = \begin{cases} 1\ , & \text{si } D \equiv 1 \pmod 8 \quad \text{y} \\ -1\ , & \text{si } D \equiv 5 \pmod 8\ . \end{cases}$$

Ejercicio 11.2. Sea $a \in \mathbb{Z}$ no un cuadrado perfecto. Probar que existen infinitos primos para los cuales a no es un residuo cuadrático:

(i) reducir al caso en que a es libre de cuadrados, o sea $a = 2^e q_1 \cdots q_r$, donde q_i son primos impares distintos, $r \geq 0$ y $e \in \{0, 1\}$;

(ii) suponer que a es divisible por algún primo impar (es decir, $a \neq 2$ y $r \geq 1$) y probar que, dado un conjunto finito de primos $\{l_1, \ldots, l_k\}$ que excluye a 2 y los q_i, existe $b \in \mathbb{Z}$ que satisface:

$$\begin{aligned} b &\equiv 1 \pmod{l_j}\ , \\ b &\equiv 1 \pmod 8\ , \\ b &\equiv 1 \pmod{q_i} \quad \text{, si } i \neq r \text{ y} \\ b &\equiv s \pmod{q_r}\ , \end{aligned}$$

donde s es un no residuo cuadrático módulo q_r y mostrar que $(a/b) = -1$ y que, por lo tanto, existe un primo $p \notin \{2, q_1, \ldots, q_r, l_1, \ldots, l_k\}$ tal que $(a/p) = -1$;

(iii) suponer que $a = 2$ y, dado un conjunto finito de primos $\{l_1, \ldots, l_k\}$ que excluye a 3, definir $b := 8l_1 \cdots l_k + 3$ y probar que $(2/b) = -1$ y que, por lo tanto, existe un primo $p \notin \{2, 3, l_1, \ldots, l_k\}$ tal que $(2/p) = -1$.

Ejercicio 11.3. Calcular el símbolo de Jacobi en los siguientes casos:

- $(113/997)$
- $(215/761)$
- $(514/1093)$
- $(401/757)$

Ejercicio 11.4. Determinar las clases en $\mathbb{Z}/84\mathbb{Z}$ para las cuales $(-21/p) = 1$, usando reciprocidad cuadrática.

12 Residuos cuadráticos y una demostración del Teorema 11.7

En esta sección estudiaremos la resolubilidad de $x^2 \equiv n \,(\mathsf{mod}\, m)$ especialmente en el caso $m = p$ un primo impar. Recordemos que $n \in \mathbb{Z}$ es un *residuo (cuadrático) módulo* m, si la ecuación tiene solución y un *no residuo*, en caso contrario. Nuestro objetivo ahora será demostrar las propiedades del Teorema 11.7:

Teorema 11.7. *Sea $p > 0$ un primo impar. Entonces, se cumple*

(i) $(n/p) = (n'/p)$, *si* $n \equiv n' \,(\mathsf{mod}\, p)$;

(ii) $(ab/p) = (a/p)\,(b/p)$, *para todo par* $a, b \in \mathbb{Z}$;

(iii) $(-1/p) = (-1)^{\frac{p-1}{2}}$ *y, más en general,* $(n/p) \equiv n^{\frac{p-1}{2}} \,(\mathsf{mod}\, p)$, *para todo* $n \in \mathbb{Z}$:

(iv) $(2/p) = (-1)^{\frac{p^2-1}{8}}$;

(v) $(q/p) = (p^*/q)$, *si q es un primo positivo, impar y distinto de p.*

La propiedad (i) es casi inmediata: si $n \equiv n' \,(\mathsf{mod}\, p)$, entonces $(n, p) = (n', p)$, con lo que $(n/p) = 0$, si y sólo si $(n'/p) = 0$, si y sólo si p divide a n y a n'; en otro caso, si x es solución de $x^2 \equiv n$, entonces $x^2 \equiv n'$, y viceversa, con lo que $(n/p) = 1$, si y sólo si $(n'/p) = 1$. Como el símbolo de Legendre toma valores 0, 1 o -1 (como $x^2 \equiv n$ tiene solución o no la tiene), concluimos que $(n/p) = (n'/p)$, si $n \equiv n' \,(\mathsf{mod}\, p)$.

Empezamos por el siguiente resultado general acerca de la cantidad de soluciones a una ecuación polinomial módulo un primo.

Lema 12.1. *Sea p un primo y sea $f \in \mathbb{Z}\,[X]\,X$, $f = c_0 + c_1 X + \cdots + c_n X^n$, $n \geq 0$ y $p \nmid c_n$.*[30] *Entonces, la congruencia $f(x) \equiv 0 \,(\mathsf{mod}\, p)$ tiene, a lo sumo, n soluciones distintas.*

Demostración. Si $n = 0$, $c_0 \not\equiv 0$ y $f(x) \equiv 0$ no tiene soluciones. Si $n > 0$ y $x_0 \in \mathbb{Z}$ cumple $f(x_0) \equiv 0$, entonces

$$f(x) \;-\; f(x_0) \;\equiv\; (x - x_0)\, g(x)\ ,$$

para cierto polinomio $g \in \mathbb{Z}\,[X]\,X$, $g = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}$, donde $b_{n-1} = c_n \not\equiv 0$, es decir, no es divisible por p **(ejercicio)**.[31] Pero, inductivamente, g no posee más de $n - 1$ raíces distintas módulo p, con lo que f no puede poseer más de n raíces distintas módulo p. □

Lema 12.2. *Sea p un primo positivo impar. Entonces,*

[30] El Lema 12.1 se puede omitir, teniendo en cuenta los resultados de la § 9, específicamente, el Corolario 9.18, ítem (iii). Es, sin embargo, una versión elemental, en el sentido de que no hace uso de los conceptos desarrollados en la § 9. Esencialmente, la hipótesis sobre f es que el polinomio en $\mathbb{Z}/p\mathbb{Z}\,[X]\,X$ que se obtiene reduciendo sus coeficientes módulo p tiene grado $n \geq 0$.

[31] Hint: Usar que $x^t - x_0^t = (x - x_0)\,(x^{t-1} + x^{t-2} x_0 + \cdots + x_0^{t-1})$.

(i) excluyendo 0, *existen exactamente* $\frac{p-1}{2}$ *residuos cuadráticos módulo* p *y, por lo tanto,* $\frac{p-1}{2}$ *no residuos en cualquier sistema reducido de representantes de las clases módulo* p*;*

(ii) las clases módulo p *de los enteros* 1^2, 2^2, ..., $(\frac{p-1}{2})^2$ *son distintas;*

(iii) en particular, exceptuando 0*, los residuos módulo* p *están representados por las* $\frac{p-1}{2}$ *clases del ítem* (ii)*.*

Demostración. Busquemos soluciones a la ecuación de congruencia

$$x^2 \equiv n \pmod{p} \ . \tag{11}$$

Si $n \equiv 0$, entonces la única solución es $x \equiv 0$. Supongamos que $n \not\equiv 0$ y que (11) admite una solución. Tomando resto de división por p, existe al menos una solución en el rango $0 \leq x \leq p-1$; como n no es divisible por p, $x = 0$ no es una de ellas. Si $x > p/2$, cambiando x por $p - x$, existe al menos una solución en el rango $1 \leq x \leq \frac{p-1}{2}$. Por lo tanto, (11) admite solución, si y sólo si n es congruente a alguna de las clases

$$1^2 \ , 2^2 \ , \ldots , (\tfrac{p-1}{2})^2 \ . \tag{12}$$

En particular, exceptuando 0, hay a lo sumo $\frac{p-1}{2}$ residuos cuadráticos módulo p. Pero las clases (12) son todas distintas **(ejercicio)**[32] y, en consecuencia, hay $\frac{p-1}{2}$ residuos cuadráticos módulo p (exceptuando 0). □

Lema 12.3 (Criterio de Euler)**.** *Si* p *es un primo positivo impar, entonces*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p} \ .$$

Demostración. Si $n \equiv 0$, no hay nada que probar. Supongamos que $n \not\equiv 0$. El Teorema 3.23 implica que $n^{p-1} \equiv 1$. En particular,

$$\left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right) \equiv 0 \ ,$$

o sea que $n^{\frac{p-1}{2}} \equiv \pm 1$. La afirmación es que este signo coincide con (n/p). Notamos que no pueden darse simultáneamente ambas posibilidades.

Por un lado, si $(n/p) = 1$, existe $x \in \mathbb{Z}$ tal que $n \equiv x^2$ y, entonces

$$n^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \ .$$

Por otro lado, por el Lema 12.1, la congruencia $n^{\frac{p-1}{2}} \equiv 1$ tiene, a lo sumo, $\frac{p-1}{2}$ soluciones distintas módulo p. Pero, por el Lema 12.2, los enteros 1^2, 2^2, ..., $(\frac{p-1}{2})^2$ representan

[32] Hint: Si x e y son soluciones a (11), entonces $x \equiv y$, o bien $x \equiv -y$, y estas posibilidades se excluyen mutuamente, si $n \not\equiv 0$. Si $1 \leq x, y \leq \frac{p-1}{2}$ e $y \neq x$, entonces tendríamos cuatro soluciones distintas módulo p, contradiciendo el Lema 12.1.

$\frac{p-1}{2}$ clases distintas y son, por lo tanto, $\frac{p-1}{2}$ soluciones distintas (módulo p) a dicha ecuación. Así, si $(n/p) = -1$, $n \not\equiv x^2$ para ningún $1 \leq x \leq \frac{p-1}{2}$ y, en consecuencia, $n^{\frac{p-1}{2}} - 1 \not\equiv 0$. Como p es primo, debe cumplirse, en este caso,

$$n^{\frac{p-1}{2}} \equiv -1 \ .$$

□

Del Lema 12.3, deducimos, eligiendo $a = -1$ que $(-1/p) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Pero, dado que ambos lados de esta congruencia son iguales a ± 1 y que p es impar, concluimos que, en realidad, $(-1/p) = (-1)^{\frac{p-1}{2}}$. Esto prueba el ítem (iii).

De manera similar, usando el Lema 12.3, también podemos probar el ítem (ii):

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p} \ ,$$

o sea que $(ab/p) \equiv (a/p)\,(b/p) \pmod{p}$. Pero, al igual que antes, ambos lados de la congruencia son iguales a ± 1 y p es impar, con lo cual, $(ab/p) = (a/p)\,(b/p)$.

Antes de pasar a la demostración del Teorema 11.7, demostramos un último resultado preliminar.

Lema 12.4 (Lema de Gauss)**.** *Dado un primo positivo impar p y un número entero n coprimo con p, de los $\frac{p-1}{2}$ restos de división por p provenientes de los enteros n, $2n$, $\ldots$, $\frac{p-1}{2}n$, sea $m \geq 0$ la cantidad de los mismos que pertenecen al rango $p/2 < r < p$. Entonces,*

$$\left(\frac{n}{p}\right) = (-1)^m \ .$$

Ejemplo 12.5. Si $p = 7$, $n = 10 \equiv 3 \pmod{7}$, entonces $3 \equiv x^2 \pmod{7}$ no tiene solución –los cuadrados son 1, 4 y 2. Por otro lado, 10, 20 y 30 tienen restos 3, 6 y 2, respectivamente, al dividir por 7, con lo que $m = 1$ y se verifica que $(10/7) = (3/7) = -1 = (-1)^m$.

Ejemplo 12.6. Si $n = 1$, $m = 0$ y, entonces $(1/p) = 1 = (-1)^m$ también en este caso.

Demostración. En primer lugar, como $(n, p) = 1$, los enteros n, $2n$, $\ldots$, $\frac{p-1}{2}n$ pertenecen a clases distintas módulo p y, en particular, sus restos de dividir por p son distintos (y son $\frac{p-1}{2}$ en cantidad). Sea, ahora, $m \geq 0$ como en el enunciado y sea $l = \frac{p-1}{2} - m$. Sea $\mathsf{r}(k) = \mathsf{r}_p(k)$ el resto de dividir $k \in \mathbb{Z}$ por p; si $k \not\equiv 0$, entonces $0 < \mathsf{r}(k) < p$. Sea $\{a_1, \ldots, a_l\}$ el subconjunto de restos $\mathsf{r}(nx) < p/2$ y sea $\{b_1, \ldots, b_m\}$ el subconjunto de restos $\mathsf{r}(nx) > p/2$ con x variando en el rango $1 \leq x \leq \frac{p-1}{2}$. Multiplicando,

$$\prod_{i=1}^{l} a_i \prod_{j=1}^{m} b_j \equiv \prod_{x=1}^{(p-1)/2} nx = n^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \ .$$

Por otro lado, para cada j, $p - b_j$ pertenece al intervalo $0 < p - b_j < p/2$, pues $p/2 < b_j < p$; los a_i también pertenecen a dicho intervalo, pero deben ser distintos de los $p - b_j$ **(ejercicio)**[33] Así, porque $l + m = \frac{p-1}{2}$, vale que los conjuntos siguientes son iguales:

$$\{a_1, \ldots, a_l\} \cup \{p - b_1, \ldots, p - b_m\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} .$$

Multiplicando,

$$\left(\frac{p-1}{2}\right)! = \prod_{i=1}^{l} a_i \prod_{j=1}^{m} (p - b_j) \equiv (-1)^m \prod_{i=1}^{l} a_i \prod_{j=1}^{m} b_j .$$

En definitiva,

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^m \, n^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

y, $1 \equiv (-1)^m n^{\frac{p-1}{2}}$, o, lo que es lo mismo, $(-1)^m \equiv n^{\frac{p-1}{2}}$. Pero, por el Criterio de Euler (Lema 12.3), $n^{\frac{p-1}{2}} \equiv (n/p)$. □

Demostración del Teorema 11.7. Sólo resta demostrar las partes (iv) y (v). Sea q un primo positivo impar distinto de p, o bien $q = 2$. Primero, probamos una congruencia válida para ambos casos (ver (13)), que luego usamos para deducir los resultados.

Para cada $x \in \mathbb{Z}$ en el rango $1 \leq x \leq \frac{p-1}{2}$, como en la demostración del Lema 12.4, con $n = q$, sea $\mathsf{r}_p(xq)$ el resto de la división por p. En particular, se cumple que

$$xq = \left\lfloor \frac{xq}{p} \right\rfloor p + \mathsf{r}_p(xq) ,$$

donde $\lfloor \cdot \rfloor$ denota la parte entera.[34] Sabemos que estos restos son todos distintos y, como $q \neq p$, distintos de cero y que se separan en dos subconjuntos disjuntos $\{a_1, \ldots, a_l\}$ y $\{b_1, \ldots, b_m\}$, donde $a_i < p/2$, $b_j > p/2$ y $l + m = \frac{p-1}{2}$. Además, sabemos que

$$\{a_1, \ldots, a_l\} \cup \{p - b_1, \ldots, p - b_m\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} .$$

De esto, deducimos que

$$\sum_{x=1}^{(p-1)/2} x = \sum_{i=1}^{l} a_i + \sum_{j=1}^{m} (p - b_j) = a + mp - b ,$$

donde $a := \sum_{i=1}^{l} a_i$ y $b := \sum_{j=1}^{m} b_j$. Por otra parte,

$$\sum_{x=1}^{(p-1)/2} \mathsf{r}_p(xq) = a + b \quad \text{y también} \quad \sum_{x=1}^{(p-1)/2} x = \frac{\frac{p-1}{2}\frac{p+1}{2}}{2} = \frac{p^2 - 1}{8} .$$

[33] Hint: Una igualdad $a_i = p - b_j$ implicaría $nx = p - ny$ con $1 \leq x, y \leq \frac{p-1}{2}$, lo que es absurdo, pues sería $n(x + y) \equiv 0$ y, por lo tanto, $x + y \equiv 0$ pero $2 \leq x + y \leq p - 1$.

[34] $\lfloor z \rfloor \in \mathbb{Z}$ y $\lfloor z \rfloor \leq z < \lfloor z \rfloor + 1$.

Con esto,

$$\begin{aligned}\frac{p^2-1}{8}(q-1) &= \sum_x (xq) - \sum_x x = \sum_x \left\lfloor \frac{xq}{p} \right\rfloor p + \sum_x \mathsf{r}_p(xq) - \sum_x x \\ &= \Big(\sum_x \left\lfloor \frac{xq}{p} \right\rfloor\Big) p + a + b - \big(a + mp - b\big) \\ &= \Big(\sum_x \left\lfloor \frac{xq}{p} \right\rfloor - m\Big) p + 2b\end{aligned}$$

y, en particular,

$$\frac{p^2-1}{8}(q-1) \equiv \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{xq}{p} \right\rfloor + m \pmod 2 . \tag{13}$$

Ahora bien, si $q = 2$, del lado izquierdo de (13) queda $\frac{p^2-1}{8}$ y del lado derecho sólo m, pues $\left\lfloor \frac{x2}{p} \right\rfloor = 0$ para $1 \le x \le \frac{p-1}{2}$. Usando el Lema 12.4 y esta congruencia módulo 2, se deduce (iv):

$$\left(\frac{2}{p}\right) = (-1)^m = (-1)^{\frac{p^2-1}{8}} .$$

Si, en cambio, q es un primo positivo impar distinto de p, el lado izquierdo de (13) es par y, de nuevo, usando el Lema 12.4 y esta congruencia módulo 2,

$$\left(\frac{q}{p}\right) = (-1)^m = (-1)^{\sum_x \left\lfloor \frac{xq}{p} \right\rfloor} ,$$

donde $1 \le x \le \frac{p-1}{2}$. Análogamente (porque q es primo impar y $p \ne q$), se cumple que $(p/q) = (-1)^{\sum_y \left\lfloor \frac{yp}{q} \right\rfloor}$, donde $1 \le y \le \frac{q-1}{2}$. En particular,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_x + \sum_y} .$$

Afirmamos que (y esto es suficiente para probar (v))

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{xq}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{yp}{q} \right\rfloor \equiv \frac{p-1}{2}\frac{q-1}{2} \pmod 2 . \tag{14}$$

De hecho, mostraremos que vale una igualdad.

Para probar (14), recurrimos al siguiente artilugio. Sea f la función[35]

$$f : \left[\!\left[1, \tfrac{p-1}{2}\right]\!\right] \times \left[\!\left[1, \tfrac{q-1}{2}\right]\!\right] \to \mathbb{Z} \quad \text{dada por} \quad f(x,y) = -xq + yp ;$$

[35] Si $a, b \in \mathbb{Z}$, $[\![a, b]\!] = \{a, a+1, \ldots, b\}$.

como $q \neq p$ son primos, $f(x,y) \neq 0$. Ahora, el dominio de f tiene cardinal $\frac{p-1}{2}\frac{q-1}{2}$. Vamos a expresar el dominio de f como la unión disjunta $\{f<0\} \cup \{f>0\}$ y determinar el cardinal de cada parte. Notemos, primero, que $\frac{yp}{q} \notin \mathbb{Z}$, si $1 \leq y \leq \frac{q-1}{2}$. Por otro lado, $f(x,y) > 0$, si y sólo si $\frac{yp}{q} > x$, o sea, teniendo en cuenta la observación inmediata anterior, $f(x,y) > 0$ equivale a $1 \leq x \leq \left\lfloor \frac{yp}{q} \right\rfloor$. Pero, fijado y en el rango $q \leq y \leq \frac{q-1}{2}$, todo x en el rango $1 \leq x < \frac{yp}{q}$ cumple $1 \leq x \leq \frac{p-1}{2}$, con lo que (x,y) pertenece al dominio de f. Entonces, fijado y, hay $\left\lfloor \frac{yp}{q} \right\rfloor$ pares (x,y) tales que $f(x,y) > 0$. Así,

$$\#\{f>0\} \;=\; \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{yp}{q} \right\rfloor \;.$$

Análogamente, $\#\{f<0\} = \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{xq}{p} \right\rfloor$. En definitiva,

$$\frac{p-1}{2}\frac{q-1}{2} \;=\; \#\{f<0\} \,+\, \#\{f>0\} \;=\; \sum_{x=1}^{(p-1)/2} \left\lfloor \frac{xq}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{yp}{q} \right\rfloor \;.$$

□

Ejercicios

Ejercicio 12.1. Sean $N \in \mathbb{Z}$, p un primo que no divide a N y $l \geq 1$. La cantidad de soluciones a la ecuación de congruencia

$$x^2 \;\equiv\; N \pmod{p^l} \tag{15}$$

es igual a:

- 1, si $p = 2$ y $l = 1$,
- 0, si $p = 2$, $l = 2$ y $N \equiv 3 \pmod 4$,
- 2, si $p = 2$, $l = 2$ y $N \equiv 1 \pmod 4$,
- 0, si $p = 2$, $l \geq 3$ y $N \not\equiv 1 \pmod 8$,
- 4, si $p = 2$, $l \geq 3$ y $N \equiv 1 \pmod 8$ y
- $1 + (N/p)$, si p es impar (l arbitrario).

Ejercicio 12.2. Sean $k, d \in \mathbb{Z}$, $k \geq 1$ y $(d,k) = 1$. Entonces, la cantidad de soluciones a la ecuación de congruencia

$$x^2 \;\equiv\; d \pmod{4k} \tag{16}$$

es igual a

$$2 \sum_{f|k} \left(\frac{d}{f}\right) \,,$$

donde f recorre los divisores positivos libres de cuadrados ($f = 1$ inclusive) y (d/f) denota el símbolo de Jacobi. Concluir de $(x + 2k)^2 \equiv x^2 \pmod{4k}$ que la sumatoria $\sum_{f|k} (d/f)$ es igual a la cantidad de enteros x en el rango $0 \leq x < 2k$ que satisfacen (16).

Ejercicio 12.3. Un entero a se dice *residuo bicuadrático módulo* p, si existe $x \in \mathbb{Z}$ tal que $a \equiv x^4 \pmod{p}$. Probar que -4 es residuo bicuadrático módulo p, si y sólo si $p \equiv 1 \pmod{4}$.[36]

Ejercicio 12.4. Probar que, si m y n son enteros coprimos, entonces

$$\frac{m-1}{2}\frac{n-1}{2} = \sum_{x=1}^{(m-1)/2} \left\lfloor \frac{xn}{m} \right\rfloor + \sum_{y=1}^{(n-1)/2} \left\lfloor \frac{ym}{n} \right\rfloor .$$

13 Los límites de Reciprocidad cuadrática

Volvamos al problema de determinar si un primo impar p se puede, o no, expresar en la forma $p = x^2 + ny^2$. La condición $(-n/p) = 1$ garantiza que p *divide* un entero $N = a^2 + nb^2$, $(a, b) = 1$. Pero no es cierto en general que $(-n/p) = 1$ implique que p sea de esa forma. Por ejemplo, con $n = 5$, si $p \neq 5$ es un primo impar y existen $x, y \in \mathbb{Z}$ tales que $p = x^2 + 5y^2$, entonces $p \equiv 1 \pmod{4}$ y $p \equiv 1, 4 \pmod{5}$, o sea

$$p = x^2 + 5y^2 \quad \text{implica} \quad p \equiv 1, 9 \pmod{20} .$$

Pero,

$$(-5/p) = 1 \quad \text{si y sólo si} \quad p \equiv 1, 3, 7, 9 \pmod{20} .$$

Al respecto, Euler conjeturó lo siguiente:

$$\begin{aligned} p &= x^2 + 5y^2 , \quad \text{si y sólo si} \quad p \equiv 1, 9 \pmod{20} \quad \text{y} \\ 2p &= x^2 + 5y^2 , \quad \text{si y sólo si} \quad p \equiv 3, 7 \pmod{20} . \end{aligned}$$

Algo similar, pero, como veremos más adelante, con una dificultad adicional, ocurre en el caso $n = 14$. Si $p \neq 7$ es un primo impar, Euler conjeturó que:

$$\begin{aligned} p &= \begin{cases} x^2 + 14y^2 & \text{o} \\ 2x^2 + 7y^2 & , \end{cases} \quad \text{si y sólo si} \quad p \equiv 1, 9, 15, 23, 25, 39 \pmod{56} \quad \text{y} \\ 3p &= x^2 + 14y^2 , \quad \text{si y sólo si} \quad p \equiv 3, 5, 13, 19, 27, 45 \pmod{56} . \end{aligned}$$

Nuevamente, sabiendo únicamente que $(-14/p) = 1$, no podemos determinar si p cae en el primer grupo o en el segundo. E incluso si supiésemos que p pertenece al primero, ¿cómo podríamos distinguir entre los primos de la forma $x^2 + 14y^2$ y aquellos de la forma $2x^2 + 7y^2$? Saber su clase de congruencia módulo 56 no es suficiente. En definitiva, lo

[36] Hint: $x^4 + 4 = ((x + 1)^2 + 1)((x - 1)^2 + 1)$.

que se puede observar en el caso general es que las clases de congruencia para las cuales $(-n/p) = 1$ se agrupan en lo que llamaremos "géneros", cada uno de los cuales tendrá distintas propiedades de representabilidad. Para precisar y poder explicar este fenómeno, introduciremos las formas cuadráticas.

Por último, mencionamos otras dos conjeturas de Euler que motivaron a Gauss a estudiar leyes de reciprocidad similares a las del símbolo de Legendre, de las cuales hablaremos en la Parte VII. Sea p un primo impar. Entonces,

$$p = x^2 + 27y^2 \text{ , si y sólo si } \begin{cases} p \equiv 1 \pmod 3 \text{ y} \\ 2 \equiv x^3 \pmod p \text{ tiene solución, y} \end{cases}$$

$$p = x^2 + 64y^2 \text{ , si y sólo si } \begin{cases} p \equiv 1 \pmod 4 \text{ y} \\ 2 \equiv x^4 \pmod p \text{ tiene solución.} \end{cases}$$

Estas afirmaciones caracterizan los primos p que se pueden expresar en la forma $p = x^2 + 27y^2$ y aquellos que se pueden expresar en la forma $p = x^2 + 64y^2$. Sin embargo, además de una condición de congruencia ($p \equiv 1 \pmod 3$ y $p \equiv 1 \pmod 4$, respectivamente), estas caracterizaciones involucran los conceptos de residuos cúbicos y bicuadráticos.

Ejercicios

Ejercicio 13.1. Probar que, si $p \neq 5$ es un primo impar y existen $x, y \in \mathbb{Z}$ tales que $2p = x^2 + 5y^2$, entonces $p \equiv 3, 7 \pmod{20}$.[37]

[37] Hint: Si $2p = x^2 + 5y^2$, entonces x e y son impares. Luego, mirar módulo 8.

Parte IV

Formas cuadráticas

14 Definiciones y primeras propiedades

Empecemos con la definición de forma cuadrática.

Definición 14.1. Por *forma cuadrática binaria* entenderemos un polinomio en dos variables, homogéneo de grado 2:

$$ax^2 + bxy + cy^2 .$$

Los coeficientes del polinomio, a, b y c, son los *coeficientes* de la forma cuadrática binaria. Usaremos la notación

$$\{a, b, c\} := ax^2 + bxy + cy^2 .$$

Definición 14.2. Decimos que una forma cuadrática es *entera*, si sus coeficientes son números enteros. El *contenido* de una forma es el máximo común divisor de sus coeficientes. Una forma *primitiva* es una forma cuadrática entera cuyos coeficientes son coprimos, es decir, si su contenido es igual a 1.

Ejemplo 14.3. La forma $\{1, 0, 1\} = x^2 + y^2$ es primitiva. La forma $\{2, 2, 3\} = 2x^2 + 2xy + 3y^2$, también.

Definición 14.4. Dado $m \in \mathbb{Z}$ y una forma f, decimos que m *es representado por* f (o que f *representa* m), si existen $x, y \in \mathbb{Z}$ tales que

$$f(x, y) = m ;$$

el par (x, y) solución de esta ecuación, o bien la expresión $f(x, y) = m$ es una *representación de* m *por la forma* f. Dicha representación se dice *propia*, si x e y son coprimos. Decimos que f *representa propiamente a* m (o que m *es propiamente representado por* f), si existe una representación propia de m por f.

Ejemplo 14.5. La forma $f(x, y) = \{1, 0, 1\}$ representa $m = 1$, pues $f(1, 0) = 1$; esta representación de 1 es propia. La forma f también representa $m = 5$: $f(2, 1) = 5$; la representación es propia. También representa propiamente a $m = 10$, pues $f(1, 3) = 10$. Pero f no representa a $m = 7$. De hecho, si f representa m, entonces $m \equiv 0, 1, 2 \pmod 4$, y, si f representa propiamente a m, entonces $m \equiv 1, 2 \pmod 4$.

Definición 14.6. Dada una forma cuadrática $f(x, y) = \{a, b, c\} = ax^2 + bxy + cy^2$, llamaremos *discriminante* a

$$\mathsf{disc}(f) = b^2 - 4ac .$$

Observación 14.7. El discriminante de una forma cuadrática entera es un número entero y congruente con 0 o 1 módulo 4; además, $D \equiv 0 \pmod 4$, si y sólo si $b \equiv 0 \pmod 2$. Recíprocamente, si $D \equiv 0, 1 \pmod 4$ existe una forma cuadrática entera de discriminante D: si $D \equiv 0$, la forma $\left\{1, 0, \frac{-D}{4}\right\}$ tiene discriminante D, si $D \equiv 1$, la forma $\left\{1, 1, \frac{1-D}{4}\right\}$ tiene discriminante D.

Lema 14.8. *Sea $f = \{a, b, c\}$ una forma cuadrática entera y sea $D := \mathsf{disc}(f)$ su discriminante. Si $D \neq 0$ no es un cuadrado perfecto, entonces $a \neq 0$, $c \neq 0$ y la única solución de $f(x, y) = 0$ con $x, y \in \mathbb{Z}$ es $x = y = 0$.*

Demostración. Si $a = 0$ o $c = 0$, entonces $D = b^2$ es cuadrado, con lo que asumimos que ni a ni c son nulos. En ese caso, sean $x, y \in \mathbb{Z}$ tales que $f(x, y) = 0$. Si $x = 0$, entonces $cy^2 = 0$ e $y = 0$. Análogamente, si $y = 0$, entonces $ax^2 = 0$ y $x = 0$. Podemos suponer, entonces, que $x \neq 0$ e $y \neq 0$. Ahora, en general,

$$4af(x, y) \;=\; (2ax + by)^2 \;-\; Dy^2 \;, \tag{17}$$

con lo que, $f(x, y) = 0$ implica $(2ax + by)^2 = Dy^2$. Pero, como $y \neq 0$, por factorización única, D debe ser un cuadrado. □

Definición 14.9. Decimos que una forma es *indefinida*, si toma valores tanto positivos como negativos. Si una forma toma valores no negativos decimos que es *semidefinida positiva*; si no toma valores positivos, *semidefinida negativa*. Una forma semidefinida que sólo toma el valor 0 en el origen se dice *definida*.

Teorema 14.10. *Sea f una forma cuadrática y sea $D := \mathsf{disc}(f)$, su discriminante. Entonces,*

(A) si $D > 0$, f es indefinida;

(B) si $D = 0$, f es semidefinida, pero no definida;

(C) si $D < 0$, f es definida.

Además, si $f = \{a, b, c\}$ y $D < 0$, entonces a y c tienen igual signo y son distintos de cero y f es positiva, si $a > 0$, y negativa, si $a < 0$.

Demostración. Supongamos que $D < 0$ (entonces, a y c deben tener el mismo signo y ser no nulos). Por (17) y el Lema 14.8, $4af(x, y) > 0$ para todo par $x, y \in \mathbb{Z}$, excepto $x = y = 0$. En particular, f es definida (positiva o negativa). Dado que

$$a \;=\; f(1, 0) \quad \text{y} \quad c \;=\; f(0, 1) \;,$$

vemos que a y c tienen igual signo y que este signo concuerda con el "signo" de f. □

Definición 14.11. Dos formas f y g son *equivalentes*, si existen $p, q, r, s \in \mathbb{Z}$ tales que

$$f(x, y) \;=\; g(px + qy, rx + sy) \quad \text{y} \quad ps - qr \;=\; \pm 1 \;;$$

si $ps - qr = 1$, entonces decimos que son *estrictamente equivalentes*.

Ejemplo 14.12. Las formas $\{2, -1, 3\}$ y $\{2, 1, 3\}$ son equivalentes, pero, con los resultados de la § 16, podremos probar que no pueden ser estrictamente equivalentes. En particular, las clases de equivalencia estricta no coinciden, en general, con clases a secas.

Ejemplo 14.13. Sea $f = \{1, 2, 4\}$. Su discriminante es $2^2 - 4\dot{1}\dot{4} = -12$ ¿Qué formas son estrictamente equivalentes a f? Otra forma de discriminante -12 con la que ya nos hemos encontrado es $\{1, 0, 3\} = x^2 + 3y^2$. Ambas son equivalentes:

$$f(x-y, y) \;=\; (x-y)^2 + 2(x-y)y + 4y^2 \;=\; x^2 + (-2+2)xy + (1-2+4)y^2 \;=\; x^2 + 3y^2 \;.$$

Más aun, en este caso, $p = 1$, $q = -1$, $r = 0$, $s = 1$, con lo que $ps - qr = 1$ y las formas son estrictamente equivalentes.

Observación 14.14. **(ejercicio)**. Si $p, q, r, s \in \mathbb{Z}$ y f y f_1 son formas relacionadas por

$$f_1(x, y) \;=\; f(px + qy, rx + sy) \;, \tag{18}$$

entonces los enteros representados por f_1 también son representados por f. Por otro lado, los coeficientes de f y de f_1 están relacionados de la siguiente manera: si $f = \{a, b, c\}$ y $f_1 = \{a_1, b_1, c_1\}$,

$$\begin{aligned} a_1 \;&=\; ap^2 \;+\; bpr \;+\; cr^2 \;=\; f(p, r) \;, \\ b_1 \;&=\; 2apq \;+\; b\,(ps + qr) \;+\; 2crs \quad \text{y} \\ c_1 \;&=\; aq^2 \;+\; bqs \;+\; cs^2 \;=\; f(q, s) \;. \end{aligned} \tag{19}$$

En particular, sus discriminantes, $D = \mathsf{disc}(f)$ y $D_1 = \mathsf{disc}(f_1)$, están relacionados por:

$$D_1 \;=\; (ps - qr)^2\, D \;. \tag{20}$$

Teorema 14.15. *La relación de equivalencia de formas cuadráticas y la relación de equivalencia estricta son relaciones de equivalencia en el conjunto de formas cuadráticas. Sean f y g formas cuadráticas equivalentes. Entonces,*

(i) un entero es representado por g, si y sólo si es representado por f;

(ii) un entero es propiamente representado por g, si y sólo si es propiamente representado por f;

(iii) $\mathsf{disc}(g) = \mathsf{disc}(f)$;

(iv) el signo de g es igual al signo de f;

(v) el contenido de g es igual al contenido de f; en particular, g es primitiva, si y sólo si f es primitiva.

Demostración. Son consecuencias de la Observación 14.14 **(ejercicio)**. □

Ejercicios

Ejercicio 14.1. Si $f(x, y) = m$ es una representación de m por f y $g = (x, y)$, entonces $g^2 \mid m$ y f representa propiamente a m/g^2. En particular, si m es libre de cuadrados (por ejemplo, si m es primo o $m = \pm 1$), sólo tiene sentido hablar de representaciones propias de m.

Las partes (iii) y (v) del Teorema 14.15 se pueden expresar de la siguiente manera: el discriminante y el contenido de una forma cuadrática son invariantes de la clase de equivalencia de la forma cuadrática (todas las formas en la misma clase tienen igual discriminante e igual contenido). Sea $\mathsf{Clases}(D)$ el conjunto de clases de formas cuadráticas de discriminante D, positivas, si $D < 0$, y sea $\mathsf{Clases}_g(D)$ el subconjunto de clases de discriminante D y contenido g. En particular, con esta notación $\mathsf{Clases}_1(D)$ denota el conjunto de clases de formas cuadráticas primitivas de discriminante D (positivas, si $D < 0$).[38]

Ejercicio 14.2. Mostrar que, si f es una forma de contenido g y discriminante D, entonces $g^2 \mid D$. Concluir que

$$\mathsf{Clases}(D) \;=\; \bigsqcup_{\substack{g>0\\ g^2|D}} \mathsf{Clases}_g(D) \;=\; \bigsqcup_{\substack{g>0\\ g^2|D}} \mathsf{Clases}_1(D/g^2)\ .$$

Un *discriminante fundamental* es un entero $D \neq 0$ que cumple

- $D \equiv 1 \,(\mathsf{mod}\, 4)$ y es libre de cuadrados, o bien
- $D = 4m$, donde $m \equiv 2, 3 \,(\mathsf{mod}\, 4)$ y es libre de cuadrados.

Equivalentemente, un discriminante fundamental es un discriminante *minimal*, es decir, $D \equiv 0, 1 \,(\mathsf{mod}\, 4)$, $D \neq 0$, y no existen enteros $D_0 \equiv 0, 1 \,(\mathsf{mod}\, 4)$ y $f > 1$ tales que $D = D_0 f^2$.

Ejercicio 14.3. Probar que un entero $D \equiv 0, 1 \,(\mathsf{mod}\, 4)$, $D \neq 0$, es un discriminante fundamental, si y sólo si toda forma de discriminante D es primitiva.

El producto de formas lineales da lugar a formas cuadráticas:

$$(kx + ly)\,(mx + ny) \;=\; kmx^2 \;+\; (kn + lm)\,xy \;+\; lny^2 \tag{21}$$

es una forma cuadrática. Veremos que éstas son muy especiales dentro del conjunto de todas las formas cuadráticas. Desde el punto de vista del problema de representabilidad, determinar si una forma como en (21) representa un entero $z \in \mathbb{Z}$ se reduce a descomponerlo como producto de enteros de alguna manera, $z = mn$, $m, n \in \mathbb{Z}$, y determinar si es posible representar los factores m y n por cada uno de los factores lineales de la forma.

Ejercicio 14.4. Una forma cuadrática es un producto de formas lineales, si y sólo si su discriminante es un cuadrado perfecto.

(i) Probar que el discriminante de la forma (21) es igual a $(kn - lm)^2$, o sea, un cuadrado perfecto.

[38] Comparar con la Definición 15.5.

(ii) Probar que, si $f = \{a, b, c\}$ y $\mathsf{disc}(f) = h^2$ es un cuadrado, entonces

$$4af \;=\; \big(2ax + (b+h)\,y\big)\,\big(2ax + (b-h)\,y\big)\;;$$

en particular, sobre $\mathbb{Q}$, f se descompone como producto de factores lineales.

(iii) Si $f = \{a, b, c\}$ es una forma cuadrática con coeficientes enteros y existe una factorización

$$f \;=\; (\kappa x + \lambda y)\,(\mu x + \nu y)$$

con $\kappa, \lambda, \mu, \nu \in \mathbb{Q}$, entonces existe una factorización

$$f \;=\; (kx + ly)\,(mx + ny)$$

con $k, l, m, n \in \mathbb{Z}$.[39]

A toda forma cuadrática le podemos asociar una matriz, definida a partir de los coeficientes de la forma: si $f = \{a, b, c\}$, su *matriz asociada* es[40]

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\;. \tag{22}$$

La matriz asociada a una forma cuadrática es una matriz simétrica. Si f es entera, los coeficientes de su matriz asociada serán enteros en la diagonal y medio enteros fuera de la diagonal. Recíprocamente, toda matriz simétrica como (22), con $a, b, c \in \mathbb{Z}$ determina un forma cuadrática entera:

$$f(x,y) \;=\; {}^t\begin{bmatrix} x \\ y \end{bmatrix}\,\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\,\begin{bmatrix} x \\ y \end{bmatrix}\;, \tag{23}$$

donde ${}^t v$ denota la matriz v transpuesta. En definitiva, hay una correspondencia entre formas cuadráticas binarias con coeficientes enteros y matrices "medio enteras". El discriminante de una forma se expresa de manera sencilla en términos del determinante de su matriz asociada: dada una forma f con matriz asociada F,

$$\mathsf{disc}(f) \;=\; -4\mathsf{det}(F)\;.$$

Ejercicio 14.5. Sea $f = \{a, b, c\}$ una forma cuadrática. Probar que la matriz asociada a $f(px + qy, rx + sy)$ es igual a

$${}^t\begin{bmatrix} p & q \\ r & s \end{bmatrix}\,\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\,\begin{bmatrix} p & q \\ r & s \end{bmatrix}\;.$$

[39] Hint: Escribir $\tilde{n} f = (kx + ly)(mx + ny)$ con $k, l, m, n, \tilde{n} \in \mathbb{Z}$; dividir por el máximo común divisor entre k, l, y $\tilde{n}$; dividir por el máximo común divisor entre m, n y (el nuevo) $\tilde{n}$; comparar coeficientes: $\tilde{n}a = km$, $\tilde{n}b = kn + lm$ y $\tilde{n}c = ln$; concluir que $\tilde{n} = 1$.

[40] A veces se llama "matriz asociada" a la matriz $\left[\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right]$.

Ejercicio 14.6. Probar que el grupo $\mathsf{GL}(2,\mathbb{Z})$ de matrices de tamanño 2×2 inversibles con coeficientes enteros actúa en el conjunto de matrices medio enteras vía $X \mapsto {}^tAXA$ (la acción es a derecha). Concluir que dos formas cuadráticas, f y f_1, son equivalentes, si y sólo si sus matrices asociadas, F y F_1, cumplen que existe $A \in \mathsf{GL}(2,\mathbb{Z})$ tal que $F_1 = {}^tAFA$. Probar que f y f_1 son estrictamente equivalentes si existe $A \in \mathsf{SL}(2,\mathbb{Z})$ tal que $F_1 = {}^tAFA$. Demostrar que las relaciones de equivalencia y de equivalencia estricta entre formas cuadráticas son, efectivamente, relaciones de equivalencia.

Si f es una forma cuadrática y $\gamma = \left[\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right]$, $f\cdot\gamma$ denota la forma

$$(f\cdot\gamma)(x,y) \;=\; f(px+qy, rx+sy)\;.$$

Dos formas, f y f_1, son equivalentes, si y sólo si existe $A \in \mathsf{GL}(2,\mathbb{Z})$ tal que $f_1 = f\cdot A$; si $A \in \mathsf{SL}(2,\mathbb{Z})$, entonces son estictamente equivalentes.

Dada una forma f, su *grupo de isotropía* es

$$\mathsf{Stab}(f)^+ \;=\; \left\{\gamma \in \mathsf{SL}(2,\mathbb{Z}) \;:\; f\cdot\gamma = f\right\}\;.$$

Ejercicio 14.7. Probar que $\mathsf{Stab}(f)^+$ es un subgrupo de $\mathsf{SL}(2,\mathbb{Z})$ y que, si $\gamma \in \mathsf{SL}(2,\mathbb{Z})$, entonces

$$\mathsf{Stab}(f\cdot\gamma)^+ \;=\; \gamma^{-1}\mathsf{Stab}(f)^+\gamma\;.$$

Ejercicio 14.8. Dada una forma cuadrática $f = \{a,b,c\}$ de discriminante $D = b^2 - 4ac$, el grupo $\mathsf{Stab}(f)^+$ contiene todas las matrices de la forma

$$\begin{bmatrix} \frac{u-bv}{2} & -cv \\ av & \frac{u+bv}{2} \end{bmatrix}\;, \tag{24}$$

donde el par $u, v \in \mathbb{Z}$ satisface

$$u^2 \;-\; Dv^2 \;=\; 4\;. \tag{25}$$

Si f es primitiva, entonces éstas son todas las matrices $\gamma \in \mathsf{SL}(2,\mathbb{Z})$ tales que $f\cdot\gamma = f$.[41]

[41] Hint: Se puede corroborar que las matrices de la forma (24) preservan f, a partir de las fórmulas (18) para los coeficientes de $f\cdot\gamma$. Sea $\gamma = \left[\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right] \in \mathsf{Stab}(f)^+$. Entonces,

$$\begin{aligned} a \;&=\; ap^2 \,+\, bpr \,+\, cr^2 \quad \text{y} \\ b \;&=\; 2apq \,+\, b\,(ps+qr) \,+\, 2crs \;=\; 2apq \,+\, b\,(1+2qr) \,+\, 2crs\;. \end{aligned}$$

De estas ecuaciones,

$$0 \;=\; apq \,+\, bqr \,+\, crs\;, \quad aq \;=\; -cr \quad \text{y} \quad as \;=\; ap \,+\, br\;.$$

O sea, $aq = -cr$ y $a\,(s-p) = br$. En particular, $a \mid cr$ y $a \mid br$. *Ahora*, asumiendo $(a,b,c) = 1$, se deduce que $a \mid r$. Si escribimos $r = av$, entonces $q = -cv$ y $s - p = bv$. De esto y de $ps - qr = 1$, se puede ver que $(p+s)^2 = Dv^2 + 4$. Elegir, entonces, $u = p + s$.

15 Representaciones, equivalencia y residuos

Lema 15.1. *Una forma f representa propiamente un entero m, si y sólo si f es estrictamente equivalente a una forma del tipo $\{m, B, C\}$, $B, C \in \mathbb{Z}$.*

Demostración. Sean $p, r \in \mathbb{Z}$ tales que $f(p, r) = m$ y $(p, r) = 1$. Por la identidad de Bézout (Teorema 1.7), existen $q, s \in \mathbb{Z}$ tales que $ps - qr = 1$. Si f_1 es la forma $f_1(x, y) := f(px+qy, rx+sy)$, entonces sus coeficientes están dados por las fórmulas (18). En particular, $a_1 = f(p, r) = m$. Recíprocamente, notamos que cualquier forma del tipo $\{m, B, C\}$, $B, C \in \mathbb{Z}$, representa propiamente a m vía $(1, 0)$. □

Lema 15.2. *Sea $D \equiv 0, 1 \pmod 4$ y sea $m \in \mathbb{Z}$, $(m, 2D) = 1$. Entonces, m es representado propiamente por* alguna *forma primitiva de discriminante D, si y sólo si D es un residuo cuadrático módulo m.*

Demostración. Supongamos, primero, que D es residuo cuadrático módulo m, o sea, existe $b \in \mathbb{Z}$ tal que $D \equiv b^2 \pmod m$. Como m es impar, cambiando b por $b + m$ de ser necesario, podemos suponer que $D \equiv b \pmod 2$. En ese caso, $D \equiv b^2 \pmod 4$ (porque $D \equiv 0, 1 \pmod 4$) y, en particular, $D \equiv b^2 \pmod{4m}$ (porque m es impar; $(m, 4) = 1$). Esto quiere decir que existe $c \in \mathbb{Z}$ tal que $D = b^2 - 4mc$. Ahora, la forma $f = \{m, b, c\}$ representa propiamente a m (vía $(1, 0)$) y su discriminante es igual a D y, además, f es primitiva, porque $(m, D) = 1$. Recíprocamente, si m es representado propiamente por una forma f de discriminante D, por el Lema 15.1, f es (estrictamente) equivalente a una forma del tipo $f_1 = \{m, B, C\}$, $B, C \in \mathbb{Z}$. Pero, entonces, $D = \mathsf{disc}(f) = \mathsf{disc}(f_1) = B^2 - 4mC$, con lo que D es residuo cuadrático módulo m. □

Teorema 15.3. *Sea $D \equiv 0, 1 \pmod 4$ y sea p un primo positivo impar que no divide a D. Entonces, p es representado por* alguna *forma cuadrática primitiva de discriminante D, si y sólo si $\chi(p) = 1$, donde χ es la función del Lema 11.9.*

Demostración. $\chi(p) = 1$, si y sólo si $(D/p) = 1$, si y sólo si D es un residuo cuadrático módulo p, si y sólo si (Lema 15.2) p es representado por una forma de discriminante D. □

Corolario 15.4. *Sea $n \in \mathbb{Z}$, $n \neq 0$, y sea p un primo positivo impar que no divide a n. Entonces, p es representado por una forma primitiva de discriminante $-4n$, si y sólo si p es un divisor primo de $x^2 + ny^2$, $(x, y) = 1$.*

Las formas cuya existencia está garantizada por el Teorema 15.3 son, en el caso $D < 0$, definidas *positivas*. Además, en cualquier caso, podemos suponer que son primitivas. Por esta razón, introducimos la siguiente definición y, de ahora en adelante, nos concentraremos en formas con dichas características.

Definición 15.5. Llamaremos *forma gaussiana* a toda forma cuadrática binaria que es

(A) primitiva e indefinida, o bien

(B) primitiva y definida *positiva*.

Introducimos, además, la siguiente notación:[42]

- $C(D)$ denota el conjunto de clases de equivalencia estricta de formas gaussianas de discriminante D y
- $\mathsf{h}(D)$ denota el cardinal del conjunto $C(D)$.

En ocasiones, diremos, simplemente, "clases de formas de discriminante D" en lugar de "clases de formas gaussianas de discriminante D".

Observación 15.6. El número de clases $\mathsf{h}(D)$ es siempre positivo: si $D \equiv 0 \,(\mathsf{mod}\, 4)$, la forma $\{1, 0, -D/4\}$ es gaussiana de discriminante D; si $D \equiv 1 \,(\mathsf{mod}\, 4)$, la forma $\{1, 1, (1-D)/4\}$ es gaussiana de discriminante D.

16 Formas reducidas (definidas positivas)

En esta sección estudiaremos la relación de equivalencia entre formas definidas. Las formas definidas se pueden separar, en una primera instancia, en dos grandes partes: las definidas positivas y las definidas negativas; las que representan enteros positivos y las que representan enteros negativos. Estos dos subconjuntos son disjuntos y la subdivisión respeta la relación de equivalencia de formas cuadráticas binarias (los conjuntos de enteros representados por formas equivalentes son iguales). Por otro lado, la función

$$f = \{a, b, c\} \mapsto -f := \{-a, -b - c\}$$

determina una biyección entre el conjunto de formas definidas positivas y el conjunto de formas definidas negativas. Además, esta correspondencia también respeta la relación de equivalencia (estricta): si dos formas f y g son (estrictamente) equivalentes, entonces las formas $-f$ y $-g$ también lo son. De esta manera, podemos concentrarnos en una de las dos partes; elegimos concentrarnos en las formas definidas positivas.

El objetivo de esta sección, entonces, es describir una manera de determinar si dos formas cuadráticas *definidas positivas* son estrictamente equivalentes. La idea es, en primer lugar, definir una noción de representante "canónico" para cada clase de equivalencia estricta; éstos serán las "formas reducidas". Cada clase de equivalencia estricta contiene exactamente una forma reducida. Luego, necesitamos una manera de "conectar", de pasar de una forma cuadrática definida positiva al representante canónico de su clase; diremos que "reducimos" la forma cuadrática. Finalmente, para poder comparar dos formas, determinar si son equivalentes estrictamente, o no, bastará con reducirlas y compararlas: la clase será la misma, si y sólo si tienen la misma forma reducida.

La noción de forma reducida que daremos en esta sección no se aplica a formas indefinidas. Con lo cual, nos estará faltando un procedimiento para determinar si dos formas indefinidas son equivalentes. Hay, sin embargo, una teoría de reducción de formas indefinidas. Pero tiene otras características.

[42] En la notación del Ejercicio 14.2, $C(D) = \mathsf{Clases}_1(D)$.

Lema 16.1. *Cada clase de equivalencia estricta de formas cuadráticas de discriminante no cuadrado contiene, al menos, un representante* $\{a, b, c\}$ *que cumple* $|b| \leq |a| \leq |c|$.

Demostración. Sea $f_0 = \{a_0, b_0, c_0\}$ una forma cuadrática arbitraria y sea $a \in \mathbb{Z}$ tal que:

- $a \neq 0$,
- a es representado por f_0 y
- $|a|$ es mínimo entre los enteros representados por f_0

Por minimalidad, si $a = f_0(p, r)$, entonces $(p, r) = 1$ **(ejercicio)** y existen $q, s \in \mathbb{Z}$ tales que $ps - qr = 1$. Sea f' la forma

$$f'(x.y) \;=\; f_0(px + qy, rx + sy) \;.$$

Por las fórmulas (18), el primer coeficiente de f' es $a = f_0(p, r)$, es decir, $f' = \{a, b', c'\}$ para ciertos $b', c' \in \mathbb{Z}$. Si, ahora, dado $h \in \mathbb{Z}$, definimos

$$f(x, y) \;=\; f'(x + hy, y) \;,$$

entonces la forma f cumple:

- es estrictamente equivalente a f' y, por lo tanto, a f_0,
- su primer coeficiente sigue siendo a, es decir, $f = \{a, b, c\}$ para ciertos $b, c \in \mathbb{Z}$, y
- $b = 2ah + b'$.

Eligiendo h convenientemente, $|b| \leq |a|$. Finalmente, si $c \neq 0$, entonces debe cumplirse $|a| \leq |c|$, por minimalidad de a. Pero $c \neq 0$ pues, por (18), $c = f'(h, 1)$ y, como $\mathsf{disc}(f') = \mathsf{disc}(f_0)$ no es un cuadrado perfecto, por el Lema 14.8, $f'(x, y) = 0$ sólo si $x = y = 0$. □

Lema 16.2. *Cada clase de equivalencia estricta de formas cuadráticas definidas positivas contiene, al menos, un representante que cumple*

$$-a \;<\; b \;\leq\; a \;<\; c \quad \textit{o bien} \quad 0 \;\leq\; b \;\leq\; a \;=\; c \;.$$

Demostración. En primer lugar, como el discriminante de una forma definida positiva es negativo, estamos en la situación del Lema 16.1. Sea $\{a_0, b_0, c_0\}$ una forma cuadrática definida postiva. Entonces, $a_0, c_0 > 0$. Podemos suponer, por el Lema 16.1, que $|b_0| \leq a_0 \leq c_0$. Ahora, si $a_0 = c_0$ pero $b_0 < 0$, obtenemos una forma estrictamente equivalente con $a = a_0 = c = c_0$ y $b = |b_0| \geq 0$ definiendo:

$$f_0(y, -x) \;=\; a_0 y^2 \;+\; b_0 y(-x) \;+\; c_0(-x)^2 \;=\; c_0 x^2 \;+\; (-b_0)\, xy \;+\; a_0\, y^2 \;.$$

Si $b_0 = -a_0$, obtenemos una forma estrictamente equivalente con $a = b = a_0$ y $c = c_0$ definiendo:

$$\begin{aligned} f_0(x + y, y) \;&=\; a_0\,(x + y)^2 \;+\; b_0(x + y)y \;+\; c_0 y^2 \\ &=\; a_0 x^2 \;+\; (2a_0 + b_0)xy \;+\; (a_0 + b_0 + c_0)y^2 \\ &=\; a_0 x^2 \;+\; a_0 xy \;+\; c_0 y^2 \;. \end{aligned}$$

□

Definición 16.3. Una forma cuadrática definida positiva $f = \{a, b, c\}$ *está reducida* (o *es una forma reducida*), si sus coeficientes cumplen las condiciones del Lema 16.2

Observación 16.4. Equivalentemente, $f = \{a, b, c\}$ (definida positiva) está reducida, si sus coeficientes cumplen:

$$|b| \leq a \leq c \quad \text{y , si} \quad |b| = a \quad \text{o} \quad a = c \,, \quad \text{entonces} \quad b \geq 0 \,.$$

Teorema 16.5. *Toda forma cuadrática primitiva definida positiva es estrictamente equivalente a una única forma reducida.*

Demostración. Lo único que falta probar es que cada clase de equivalencia estricta contiene *a lo sumo* una forma reducida. Sean, entonces, $f = \{a, b, c\}$ y $f_1 = \{a_1, b_1, c_1\}$ dos formas cuadráticas de discriminante $D < 0$, ambas reducidas en el sentido de la Definición 16.3. Probaremos que, si f y f_1 son estrictamente equivalentes, entonces deben ser iguales. Sin pérdida de generalidad, podemos asumir que $a \geq a_1$.

Veamos, primero, que $a = a_1$. Supongamos que $p, q, r, s \in \mathbb{Z}$ cumplen que $f_1(x, y) = f(px + qy, rx + sy)$. De las fórmulas (18), como $a \leq c$ y $|b| \leq a$, vale que

$$a_1 \,=\, ap^2 \,+\, bpr \,+\, cr^2 \,\geq\, ap^2 \,-\, a|pr| \,+\, ar^2 \,\geq\, a|pr| \,.$$

La última desigualdad es consecuencia de que $x^2 + y^2 \geq 2|xy|$ para todo par x e y. En consecuencia, $|pr| \leq 1$. Asumiendo que $ps - qr = 1$, vemos que $p, r \in \{-1, 0, 1\}$ y no son ambos nulos. Entonces, $p^2 - |pr| + r^2 = 1$ y $a \geq a_1 \geq a$, es decir, $a = a_1$.

Para terminar, distinguimos dos casos: $c = a$ y $c_1 = a_1$, o bien se cumple alguna de $c > a$ o $c_1 > a_1$. En el primer caso, $c = c_1$ y $D = b^2 - 4ac = b_1^2 - 4a_1c_1$ muestra que $b = \pm b_1$. Pero, como f y f_1 están reducidas, en esta situación $b, b_1 \geq 0$. En particular, $b = b_1$, con lo que $f = f_1$. Supongamos, finalmente, que estamos en el segundo caso y que es $c > a$. Sean $p, q, r, s \in \mathbb{Z}$ tales que $f_1(x, y) = f(px+qy, rx+sy)$ y que $ps-qr = 1$. Como antes, deducimos que $p^2 - |pr| + r^2 = 1$. Si fuese $r \neq 0$, entonces sería $cr^2 > ar^2$ y

$$a \,=\, a_1\, ap^2 \,+\, bpr \,+\, cr^2 \,>\, a\,(p^2 - |pr| + r^2) \,=\, a \,,$$

lo que es absurdo. Así, debe ser $r = 0$. Pero, ahora, $ps - qr = 1$ implica $ps = 1$ y, por lo tanto, de (18),

$$b_1 \,=\, 2apq \,+\, b\,(ps + qr) \,+\, 2crs \,\equiv\, b \pmod{2a} \,.$$

Pero b y b_1 están ambos en el rango $-a = -a_1 < b, b_1 \leq a = a_1$, lo que implica, junto con $b_1 \equiv b \pmod{2a}$, que $b = b_1$. Por último, $D = b^2 - 4ac = b_1^2 - 4a_1c_1$ implica que $c = c_1$ también. □

Como consecuencia del Teorema 16.5, podemos deducir versiones un poco más refinadas de los resultados de la § 15.

Teorema 16.6. *Sea $D \equiv 0, 1 \pmod{4}$, $D < 0$ y sea p un primo positivo impar que no divide a D. Entonces, p es representado por una forma primitiva* reducida *de discriminante D, si y sólo si $\chi(p) = 1$, donde χ es la función del Lema 11.9.*

Demostración. La diferencia con el Teorema 15.3 está en que aquí agregamos que la forma que representa p debe ser reducida. Pero si p es representado por una forma definida positiva de discriminante D, entonces, cambiando dicha forma por una (la) forma reducida y (estrictamente) equivalente a ella, vemos que p es representado por una forma reducida. □

El siguiente resultado refina el Corolario 15.4.

Corolario 16.7. *Sea $n \in \mathbb{Z}$, $n > 0$, y sea p un primo positivo impar que no divide a n. Entonces, p es representado por una forma primitiva* reducida *de discriminante $-4n$, si y sólo si p es un divisor de $x^2 + ny^2$, $(x, y) = 1$.*

Observación 16.8. Si $D < 0$, el número de clases $\mathsf{h}(D)$ coincide con la cantidad de formas reducidas de discriminante D (Teorema 16.5). Las formas primitivas x^2+ny^2 con $n > 0$ son formas reducidas. Pero eso no quiere decir que cada una sea la única forma primitiva reducida de discriminante $-4n$. Si $\mathsf{h}(-4n) = 1$, entonces la condición $(-n/p) = 1$ caracteriza aquellos primos que pueden ser expresados en la forma $p = x^2 + ny^2$ (Corolario 16.7) y esta condición puede ser formulada como una serie de condiciones de congruencia sobre p, módulo $4n$.

Ejemplo 16.9. Veamos que $x^2 + 7y^2$ es la única forma cuadrática reducida de discriminante -28. Si $f = \{a, b, c\}$ tiene discriminante -28, entonces b es par. Si está reducida, entonces $|b| \leq a \leq c$. Como $-28 = b^2 - 4ac$, se deduce que $-28 \leq -3a^2$ y, por lo tanto, que $a \in \{1, 2, 3\}$. Por otro lado, debe ser $-a < b \leq a$. Si $a = 3$, entonces $b \in \{-2, 0, 2\}$. Pero $-28 \equiv 2 \pmod 3$, mientras que $b^2 \equiv 0, 1 \pmod 3$. Así que debe ser $a \in \{1, 2\}$. Si $a = 2$, la única posibilidad sería $b = 0$, pero $-28 \equiv 4 \pmod 8$, mientras que $b^2 \equiv 0 \pmod 8$. Finalmente, la única posibilidad restante es $a = 1$. Entonces, $b = 0$ y $c = 7$. Así, $\mathsf{h}(-28) = 1$.

En particular, como $x^2 + 7y^2$ es la única forma cuadrática reducida de discriminante -28, por el Corolario 16.7, $(-7/p) = 1$, si y sólo si $p = x^2 + 7y^2$. Si ahora logramos describir qué primos p satisfacen $(-7/p) = 1$, habremos encontrado condiciones que garantizan que p se pueda expresar en la forma $p = x^2 + 7y^2$. Ahora, $(-7/p) = 1$, si y sólo si $(-1/p)\,(7/p) = 1$. Equivalentemente, $(-1/p) = (7/p) = 1$, o bien $(-1/p) = (7/p) = -1$. Es decir,

$$\begin{aligned} p &\equiv 1 \pmod 4 \quad \text{y} \quad p \equiv 1, 2, 4 \pmod 7\ , \quad \text{o bien} \\ p &\equiv 3 \pmod 4 \quad \text{y} \quad p \equiv 1, 2, 4 \pmod 7\ . \end{aligned}$$

O sea, un primo impar p se expresa en la forma $p = x^2+7y^2$, si y sólo si $p \equiv 1, 2, 4 \pmod 7$.

Teorema 16.10 (Landau)**.** *Para $n \in \mathbb{Z}$, $n > 0$, se cumple $\mathsf{h}(-4n) = 1$, si y sólo si $n \in \{1, 2, 3, 4, 7\}$.*

Demostración. Si $n \in \{1, 2, 3, 4, 7\}$, entonces $x^2 + ny^2$ es la única forma primitiva reducida de discriminante $-4n$ **(ejercicio)**.[43] Recíprocamente, si $n \notin \{1, 2, 3, 4, 7\}$, encontraremos una segunda forma reducida, primitiva y de discriminante $-4n$.

[43] Hint: Argumentar como en el Ejemplo 16.9.

Supongamos, primero, que n no es una potencia de un número primo y que $n = ac$ con $1 < a < c$, $(a, c) = 1$. Entonces, la forma $ax^2 + cy^2$ es una forma primitiva, reducida y de discriminante $-4ac = -4n$.

Supongamos, ahora, que $n = 2^r$. Si $r \in \{0, 1, 2\}$, entonces $n \in \{1, 2, 4\}$. Si $r = 3$, entonces $n = 8$ y se verifica que $\mathsf{h}(-4 \cdot 8) = 2$ **(ejercicio)**. Si $r \geq 4$, la forma

$$4x^2 + 4xy + (2^{r-2} + 1)\, y^2$$

es primitiva, reducida y de discriminante $4^2 - 4 \cdot 4 \cdot (2^{r-2} + 1) = -4 \cdot 2^r = -4n$.

Supongamos, por último, que $n = p^r$, p primo impar. Si $n + 1$ no es potencia de primo, entonces $n + 1 = ac$, donde $1 < a < c$, $(a, c) = 1$ y la forma $ax^2 + 2xy + cy^2$ es primitiva, reducida y de discriminante $4 - 4ac = -4n$. Si $n + 1$ es potencia de primo, entonces, como es par, $n + 1 = 2^s$. Si $s \in \{1, 2, 3\}$, entonces $n \in \{1, 3, 7\}$. Si $s = 4$, $n = 15$ no es potencia de primo. Si $s = 5$, entonces $n = 31$ y se verifica que $\mathsf{h}(-4 \cdot 31) = 3$ **(ejercicio)**. Si $s \geq 6$, entonces a forma

$$8x^2 + 6xy + (2^{s-3} + 1)\, y^2$$

es primitiva, reducida y de discriminante $6^2 - 4 \cdot 8 \cdot (2^{s-3} + 1) = 4 - 2^{s+2} = -4 \cdot (2^s - 1) = -4n$. □

Ejercicios

Ejercicio 16.1. Sea $\{a, b, c\}$ una forma cuadrática que verifica $|b| \leq |a| \leq |c|$ y sea $D = b^2 - 4ac$ su discriminante. Probar que,[44]

(A) si $D > 0$, entonces $0 \leq |a| \leq \sqrt{D/4}$ y que,

(B) si $D < 0$, entonces $0 < a \leq \sqrt{|D|/3}$.

Concluir, como consecuencia del Lema 16.1, que el número de clases de formas cuadráticas de discriminante no cuadrado es finito.

Ejercicio 16.2. Probar que $\{a, b, c\}$ es estrictamente equivalente a las formas:

$$\{c, -b, a\} \quad \text{y} \quad \left\{a, 2ah + b, ah^2 + bh + c\right\} .$$

Mostrar que $\{a, b, c\}$ y $\{a, -b, c\}$ son equivalentes, pero no necesariamente estrictamente equivalentes (asumir que $D < 0$).

Ejercicio 16.3. Probar que $\{a, -a, c\}$ y $\{a, a, c\}$ son estrictamente equivalentes.

Ejercicio 16.4. Sea $f = \{a, b, c\}$ una forma cuadrática. Probar que

(i) si $|b| \leq a \leq c$, entonces

$$|f(x, y)| \geq (a - |b| + c) \min\{|x|^2, |y|^2\} \quad \text{y que}$$

[44] Hint: Ver el Ejemplo 16.9.

(ii) si $|b| < a < c$, las únicas representaciones propias $f(x,y) = a$ son $(x,y) = (\pm 1, 0)$ y las únicas representaciones propias $f(x,y) = c$ son $(x,y) = (0, \pm 1)$

(iii) ¿Qué se puede decir en los casos $|b| = a < c$ y $|b| < a = c$?

Ejercicio 16.5. Hallar condiciones sobre un primo impar p que garantizan que $p = x^2 + ny^2$, para $n \in \{1, 2, 3, 4, 7\}$ (el caso $n = 7$ lo hicimos en el Ejemplo 16.9).

Ejercicio 16.6. Hallar la forma reducida estrictamente equivalente a $\{126, 74, 13\}$.

Ejercicio 16.7. Determinar las formas primitivas reducidas de discriminantes -20, -56, -3, -15, -24, -31, -52.

Ejercicio 16.8. Sea p un número primo y sean f y f_1 formas cuadráticas de igual discriminante que representan, ambas, p. Probar que f y f_1 son equivalentes (pero no necesariamente estrictamente equivalentes).

Ejercicio 16.9. Probar que, si $f = ax^2 + cy^2$ y f_1 es una forma equivalente a f, entonces f_1 es estrictamente equivalente a f. Concluir que, si $f = x^2 + ny^2$ y f_1 es una forma reducida equivalente a f, entonces $f_1 = f$.

Ejercicio 16.10. Probar que, si f es una forma de discriminante D que representa 1, entonces f es estrictamente equivalente a $\{1, 0, -D/4\}$, si $D \equiv 0$, o a $\{1, 1, (1-D)/4\}$, si $D \equiv 1$.[45]

17 Formas reducidas (indefinidas)

[45] Hint: Mostrar que toda forma f es estrictamente equivalente a una forma $\{a, b, c\}$ donde a es el menor entero positivo propiamente representado por f y $|b| \leq a$.

Parte V

Género de formas cuadráticas

18 Agrupar formas por género

En esta sección, introduciremos la noción de *género* de una forma cuadrática, que nos permitirá subdividir las formas cuadráticas teniendo en cuenta sus propiedades de representación. Sabemos que formas equivalentes representan los mismos enteros (el conjunto de enteros representados es un invariante de la clase de equivalencia de una forma). Con lo cual, la subdivisión del conjunto de formas de acuerdo con su género terminará siendo una subdivisión más gruesa que la subdivisión por clases de equivalencia o clases de equivalencia estricta; cada género de formas cuadráticas estará conformado por (posiblemente) varias clases de equivalencia.

En el caso de discriminantes negativos, el Teorema 16.10 nos muestra que, salvo muy pocos casos, si queremos caracterizar los primos representados en la forma $p = x^2 + ny^2$, las ideas introducidas hasta esta parte no son suficientes. Dado un discriminante D, el Teorema 15.3 nos permite decidir si un primo p es representado por *alguna* forma de discriminante D. Más aun, como toda forma es equivalente a una forma reducida, podemos decidir si p es representado por alguna forma reducida de discriminante D. Si el número de clases $\mathsf{h}(D) = 1$, entonces la condición $\chi(p) = 1$ es suficiente para saber cuál es dicha forma, pues hay, en ese caso, una única forma reducida; si $D = -4n$, dicha forma es $\{1, 0, n\}$. Pero, cuando el número de clases $\mathsf{h}(D) > 1$, la condición $\chi(p) = 1$ no da información acerca de cuál de todas las formas reducidas (o cuáles) representan p.

La definición de género que daremos en esta sección se aplica tanto a formas definidas, como a formas indefinidas. Los ejemplos serán todos de formas definidas positivas, simplemente porque no hemos descripto una manera de hallar las clases de equivalencia en el caso indefinido.

Ejemplo 18.1. Hay dos clases de formas de discriminante -20. El argumento es similar al del Ejemplo 16.9. Si $f = \{a, b, c\}$ es una forma cuadrática primitiva, reducida y de discriminante -20, entonces $1 \leq a \leq \sqrt{20/3} < 7$, o sea $a \in \{1, 2\}$. Además, como $D \equiv 0 \,(\mathsf{mod}\, 4)$, debe ser $b \equiv 0 \,(\mathsf{mod}\, 2)$. Si $a = 1$, entonces $b = 0$ y $c = 5$ es la única posibilidad. Si $a = 2$, entonces $b \in \{0, 2\}$, pero $-20 = b^2 - 4ac$ con $c \in \mathbb{Z}$ fuerza que $b = 2$ y, así, $c = 3$. O sea, $\mathsf{h}(-20) = 2$ y las clases están representadas por las formas primitivas reducidas

$$x^2 + 5y^2 \quad \text{y} \quad 2x^2 + 2xy + 3y^2 \ .$$

Por el Corolario 16.7, un primo impar $p \neq 5$ está representado por una forma reducida de discriminante -20, si y sólo si $(-5/p) = 1$. Pero

$$(-5/p) = 1 \ , \quad \text{si y sólo si} \quad p \equiv 1, 9, 7, 3 \,(\mathsf{mod}\, 20) \ .$$

En definitiva, un primo impar $p \neq 5$ es representado por una forma reducida de discrim-

inante -20, si y sólo si

$$p \equiv 1, 9, 7, 3 \pmod{20} \quad \text{si y sólo si} \quad \begin{cases} p = x^2 + 5y^2 & \text{o} \\ p = 2x^2 + 2xy + 3y^2 \ . \end{cases}$$

Hasta este punto, la teoría general no nos permite decidir si $p = x^2 + 5y^2$ o no. Ahora, si $p = x^2 + 5y^2$, entonces $p \equiv 1, 4 \pmod{5}$ y, en particular,

$$p \equiv 1, 9 \pmod{20} \quad \text{si y sólo si} \quad p = x^2 + 5y^2 \ .$$

Análogamente, si $(x, y) = 1$, entonces $2x^2 + 2xy + 3y^2 \equiv 2, 3 \pmod{5}$, con lo que

$$p \equiv 7, 3 \pmod{20} \quad \text{si y sólo si} \quad p = 2x^2 + 2xy + 3y^2 \ .$$

Ejemplo 18.2. Hay cuatro clases de formas de discriminante -56. Las formas reducidas correspondientes son

$$\{1, 0, 14\} \ , \quad \{2, 0, 7\} \ , \quad \{3, -2, 5\} \quad \text{y} \quad \{3, 2, 5\} \ .$$

Por el Corolario 16.7, un primo impar $p \neq 7$ está representado por alguna de estas formas cuadráticas, si y sólo si $(-14/p) = 1$. Pero **(ejercicio)**,

- si $p = x^2 + 14y^2$ o $p = 2x^2 + 7y^2$, entonces $p \equiv 1, 7 \pmod{8}$ y $p \equiv 1, 2, 4 \pmod{7}$, y,
- si $p = 3x^2 \pm 2xy + 5y^2$, entonces debe ser $p \equiv 3, 5 \pmod{8}$ y $p \equiv 3, 5, 6 \pmod{7}$.

La condición módulo 7 la podemos deducir, por ejemplo, de la condición módulo 8 y de que, por Reciprocidad cuadrática,

$$(-14/p) = (-7/p)\,(2/p) = (p/7)\,(2/p) \ .$$

Notamos, además, que $\{1, 0, 14\}$ y $\{2, 0, 7\}$ ambas representan primos en todas las clases $p \equiv 1, 25, 9, 15, 39, 23 \pmod{56}$, y que $\{3, \pm 2, 5\}$ representan exactamente los mismos enteros.

Observación 18.3. Fijado un discriminante D, la clase de congruencia de un primo p módulo D nos permite decir, en primera instancia, si p es representable por alguna forma de discriminante D. Como se ve en el Ejemplo 18.1 y en el Ejemplo 18.2, por la clase de congruencia de p también podemos precisar mejor las formas que posiblemente lo representen; podemos eliminar formas que no lo pueden representar, de acuerdo con la clase de congruencia. En el Ejemplo 18.1, podemos ver que la clase de congruencia de un primo p módulo 20 determina la forma reducida que lo representa. En el Ejemplo 18.2, no es posible distinguir exactamente cuál es la clase que lo representa. En particular, no podemos decir, dado $p \equiv 1, 25, 9, 15, 39, 23 \pmod{56}$, si p es de la forma $x^2 + 14y^2$. Más aun, p podría estar representado por más de una forma reducida. En definitiva, hay un límite a lo que podemos deducir a partir de (estas) congruencias.

Definición 18.4. Dados $D \in \mathbb{Z}$, una clase de congruencia $c \in \mathbb{Z}/D\mathbb{Z}$ y una forma f, decimos que *la clase c es representada por f* (o que *f representa la clase c*), si existe $m \in c$, perteneciente a la clase, tal que m es representado por f.

Ejemplo 18.5. La forma $\{1, 0, 14\}$ representa las clases

$$[1] \ , \quad [25] \ , \quad [9] \ , \quad [15] \ , \quad [39] \quad \text{y} \quad [23]$$

módulo 56, porque, por ejemplo, representa *los enteros* 1, 25, 9, 15, 39 y 23. Sin embargo, la forma $\{2, 0, 7\}$ también representa estas clases: representa

$$9 = 2 \cdot 1^2 + 7 \ , \quad 15 = 2 \cdot 2^2 + 7 \ , \quad 25 = 2 \cdot 3^2 + 7 \quad \text{y} \quad 39 = 2 \cdot 4^2 + 7 \ ;$$

pero también representa

$$57 = 2 \cdot 5^2 + 7 \equiv 1 \pmod{56} \quad \text{y} \quad 79 = 2 \cdot 6^2 + 7 \equiv 23 \pmod{56} \ .$$

Definición 18.6. Dos formas cuadráticas de discriminante D *pertenecen al mismo género*, si representan las mismas clases en $U\big(D\big)$.

Ejemplo 18.7. Para $D = -20$, hay dos formas reducidas y, por lo tanto, dos clases de formas de discriminante -20. De acuerdo con el Ejemplo 18.1, las dos formas reducidas no pertenecen al mismo género. En particular, en este caso, el género de una forma coincide con su clase de equivalencia (estricta). Las clases de congruencia módulo 20 también se dividen en dos, aquellas representadas por $\{1, 0, 5\}$ y aquellas representadas por $\{2, 2, 3\}$:

$$\big\{1,\, 9\big\} \quad \text{y} \quad \big\{7, 3\big\} \ .$$

Para $D = -56$, sin embargo, encontramos cuatro clases de formas cuadráticas de discriminante -56; hay cuatro formas reducidas. De acuerdo con el Ejemplo 18.2, las formas se agrupan en dos géneros:

$$\big\{\, \{1, 0, 14\} \,,\, \{2, 0, 7\} \,\big\} \quad \text{y} \quad \big\{\, \{3, -2, 5\} \,,\, \{3, 2, 5\} \,\big\} \ .$$

Las clases de congruencia módulo 56 se dividen en dos, aquellas representadas por uno y otro género:

$$\big\{1,\, 25,\, 9,\, 15,\, 39,\, 23\big\} \quad \text{y} \quad \big\{3,\, 19,\, 27,\, 45,\, 5,\, 13\big\} \ .$$

Ejercicios

19 El Teorema de Dirichlet

Con la Definición 18.6, parece que estamos dejando de lado el problema de representar primos por formas cuadráticas, porque, en lugar de responder qué primos representa cada una de las formas reducidas, el género de una forma parece responder qué clases de congruencia módulo el discriminante representa dicha forma; en particular, pareciera que nos hemos olvidado del problema de clasificar primos de la forma $p = x^2 + ny^2$

¿Cómo podemos determinar si una clase de congruencia módulo D es representada por alguna forma de discriminante D?

En esta sección hacemos una disgresión por el Teorema de Dirichlet sobre primos en progresiones aritméticas y lo relacionaremos con el estudio de la representabilidad por formas cuadráticas.

Teorema 19.1 (Dirichlet)**.** *Dados números enteros coprimos m y D, la sucesión*

$$m\ ,\quad m+D\ ,\quad m+2D\ ,\quad \dots$$

contiene infinitos números primos.

Una consecuencia del Teorema 19.1 es que toda clase de congruencia módulo D contiene algún número primo. Veamos cómo se relaciona esto con el problema de representabilidad por formas cuadráticas.

Por el Lema 15.2, fijado un entero m (impar), podemos decidir fácilmente qué discriminantes (coprimos con m) lo representan: son aquellos que pertenecen al subgrupo de cuadrados,

$$\big\{x^2\,:\,x\in U\big(m\big)\big\}\ \leq\ U\big(m\big)\ .$$

Si $m=p$ es primo (impar), entonces

$$\big\{x^2\,:\,x\in U\big(p\big)\big\}\ =\ \big\{y\in U\big(p\big)\,:\,(y/p)=1\big\}\ .$$

Recíprocamente, fijado un discriminante D, ¿existen condiciones sobre las clases de congruencia módulo D para determinar qué enteros m se pueden representar por formas de discriminante D? El Teorema 15.3 nos da un criterio sencillo para determinar qué *primos* podemos representar por formas de discriminante D: son aquellos que pertenecen al núcleo de la función χ del Lema 11.9,

$$\mathsf{ker}(\chi)\ =\ \big\{c\in U\big(D\big)\,:\,\chi(c)=1\big\}\ \leq\ U\big(D\big)\ .$$

Si $D\equiv 0,1\,(\mathsf{mod}\,4)$ es un discriminante y $c\in U\big(D\big)$, existe, por el Teorema 19.1, al menos un primo $p\in c$ ($[p]=c$); podemos suponer $p>0$. Ahora, por el Teorema 15.3, si $c\in\mathsf{ker}(\chi)$, entonces $\chi(p)=1$ y p está representado por alguna forma de discriminante D. En particular, deducimos lo siguiente: si $c\in\mathsf{ker}(\chi)$, entonces algún elemento $m\in c$ de la clase es representado (propiamente) por alguna forma primitiva de discriminante D; si $D<0$, la forma debe ser definida *positiva*.

Corolario 19.2. *Sea $D\equiv 0,1\,(\mathsf{mod}\,4)$ y sea $c\in U\big(D\big)$. Entonces, la clase c es representada (propiamente) por alguna forma gaussiana de discriminante D, si $c\in\mathsf{ker}(\chi)$.*

Observación 19.3. Recíprocamente, el Lema 20.5 muestra, entre otras cosas, que, si c es representada por una forma de discriminante D, *entonces* $c\in\mathsf{ker}(\chi)$.

En definitiva, tenemos una condición necesaria (y suficiente) para determinar qué *clases de congruencia* son representadas por *alguna* forma de discriminante D. Como

vimos en la § 18, no es posible, en general, representar cualquier clase de congruencia (detro de las clases representables) por cualquier forma cuadrática. El género agrupa formas de acuerdo con las clases de congruencia que cada una puede representar y clases de congruencia de acuerdo con las formas que las representan.

Terminamos esta sección con algunos ejemplos que ilustran el uso del Teorema 19.1 en este contexto.

Ejemplo 19.4. El grupo $U\big(3\big)$ consta de dos clases de congruencia:

$$[1] \quad \text{y} \quad [2] \ .$$

La clase [1] contiene al primo 7 y la clase [2] contiene a 5. Para decidir qué clases se pueden representar por formas de discriminante -3, necesitamos conocer el valor de χ en ellas. Ahora,

$$\chi(1) \,=\, \chi(7) \,=\, \left(\frac{-3}{7}\right) \,=\, 1 \ ,$$

mientras que

$$\chi(2) \,=\, \chi(5) \,=\, \left(\frac{-3}{5}\right) \,=\, -1 \ .$$

De hecho, podríamos deducir, usando las propiedades del símbolo de Legendre, que $(-3/p) = 1$, si sólo si $p \equiv 1 \,(\mathsf{mod}\, 3)$. Hay, por otro lado, sólo una forma reducida de discriminante -3:

$$x^2 \,+\, xy \,+\, y^2 \ .$$

Por el Corolario 19.2, la clase de congruencia módulo 3 [1] es representable por esta forma cuadrática. Efectivamente,

$$7 \,=\, 1^2 + 1 \cdot (-3) + (-3)^2 \ .$$

Ahora bien, nuevamente por el Corolario 19.2, los primos pertenecientes a la clase [2] no pueden ser representados por la forma $\{1, 1, 1\}$ (y, por lo tanto, por ninguna forma de discriminante -3). Pero cabe, aun, la posibilidad de que la clase sí sea representable, es decir, que exista algún entero $m \equiv 2 \,(\mathsf{mod}\,)3$ (no primo) que sí sea representado en la forma $\{1, 1, 1\}$. La recíproca del Corolario 19.2 garantiza que esto no puede pasar en general. De hecho, si no nos olvidamos de que la forma es $x^2 + xy + y^2$, podemos ver que, si $(x, y) = 1$, entonces

$$x^2 + xy + y^2 \,\equiv\, 0, 1 \quad (\mathsf{mod}\, 3) \ ,$$

con lo cual, la clase [2] no es representable por formas de discriminante -3.

Ejemplo 19.5. Las clases de congruencia módulo 15 en $U\big(15\big)$ son:

$$[1] \ , \quad [2] \ , \quad [4] \ , \quad [7] \ , \quad [8] \ , \quad [11] \ , \quad [13] \quad \text{y} \quad [14] \ .$$

Queremos decidir cuáles de estas clases son representadas por alguna forma de discriminante -15 y, dentro de lo posible, determinar, dada una clase representable, cuál de las

c	1	2	4	7	8	11	13	14
$p \in c$	31	17	19	37	23	41	43	29
$\chi(p)$	1	1	1	-1	1	-1	-1	-1
$p = f(x,y)$	$\{1,1,4\}$	$\{2,1,2\}$	$\{1,1,4\}$		$\{2,1,2\}$			

Tabla 4: Valores de χ para $D = -15$ y la forma reducida f que representa cada clase.

dos formas la representa. Empezamos calculando la función χ. Para eso necesitamos evaluarla en cada una de las clases en $U\big(15\big)$ (en las clases módulo 15 que no pertenecen a $U\big(15\big)$, su valor es 0). Pero, según el Lema 11.9, los únicos enteros en los que conocemos (más o menos) explícitamente la función χ es en los primos (que, en este caso, no dividen a 15). Dada una clase $c \in U\big(15\big)$, si $p \in c$ es primo perteneciente a la clase, entonces,

$$\chi(c) \,=\, \chi(p) \,=\, \left(\frac{-15}{p}\right) .$$

Pero, por propiedades del símbolo de Legendre,

$$\left(\frac{-15}{p}\right) \,=\, \left(\frac{-3}{p}\right)\left(\frac{5}{p}\right) .$$

Entonces,

$$\left(\frac{-15}{p}\right) \,=\, 1 \quad \text{si y sólo si} \quad \begin{cases} p \,\equiv\, 1 \,(\mathsf{mod}\, 3) & \text{y} \quad p \,\equiv\, \pm 1 \,(\mathsf{mod}\, 5) \quad \text{o} \\ p \,\equiv\, 2 \,(\mathsf{mod}\, 3) & \text{y} \quad p \,\equiv\, \pm 3 \,(\mathsf{mod}\, 5) \,. \end{cases}$$

O sea, $\chi(p) = 1$, si y sólo si $p \equiv 1, 4, 2, 8 \,(\mathsf{mod}\, 15)$. La Tabla 4 muestra, para cada clase $c \in U\big(15\big)$, un primo p perteneciente a c y el valor de $\chi(p)$. Por otro lado, hay dos formas reducidas de discriminante $D = -15$; ellas son:

$$x^2 \,+\, xy \,+ 4y^2 \quad \text{y} \quad 2x^2 \,+\, xy \,+\, 2y^2 \,.$$

Notamos que, si $(x, y) = 1$, entonces

$$x^2 \,+\, xy \,+\, 4y^2 \,\equiv\, 1 \,(\mathsf{mod}\, 3) \quad \text{y} \quad 2x^2 \,+\, xy \,+\, 2y^2 \,\equiv\, 2 \,(\mathsf{mod}\, 3) \,.$$

En particular, no hay posibilidad de que ambas formas representen las mismas clases módulo 15. Complementando esta última observación, si $(x, y) = 1$,

$$x^2 \,+\, xy \,+\, 4y^2 \,\equiv\, 1, 4 \,(\mathsf{mod}\, 5) \quad \text{y} \quad 2x^2 \,+\, xy \,+\, 2y^2 \,\equiv\, 2, 3 \,(\mathsf{mod}\, 5) \,.$$

De hecho, para los primos de la Tabla 4,

$$\begin{aligned} 31 \,&=\, 3^2 + 3 \cdot 2 + 4 \cdot 2^2 \\ 17 \,&=\, 2 \cdot 1^2 + 1 \cdot (-3) + 2 \cdot (-3)^2 \\ 19 \,&=\, 1^2 + 1 \cdot 2 + 4 \cdot 2^2 \\ 23 \,&=\, 2 \cdot 1^2 + 1 \cdot 3 + 2 \cdot 3^2 \,. \end{aligned}$$

No demostraremos en el curso el Teorema 19.1. Una desarrollo de este tema y otros relacionados se puede encontrar en [Dav80]. No lo usaremos, tampoco, en ninguna de las demostraciones. De todas maneras, es una ventaja *saber* que este resultado es cierto. Convencerse aunque sea experimentalmente es suficiente. El desarrollo de la teoría de formas cuadráticas y los primeros intentos de Dirichlet de demostrar este resultado se solapan en el tiempo y las ideas de uno y otro lado se entrelazan.

Ejercicios

Ejercicio 19.1. Para $D \in \{-24, -31, -52\}$, describir los géneros de formas cuadráticas de discriminante D. Para cada valor de D, hallar

- el subconjunto $U\big(D\big) \subset \mathbb{Z}/D\mathbb{Z}$,
- el subgrupo $\ker(\chi) \leq U\big(D\big)$,
- las formas reducidas (Ejercicio 16.7),
- las clases de congruencia módulo D representadas por la *forma principal*, es decir, por $\{1, 0, -D/4\}$, si $D \equiv 0 \pmod 4$, y por $\{1, 1, (1-D)/4\}$, si $D \equiv 1 \pmod 4$

y agrupar

- las formas reducidas por género y
- las clases de congruencia módulo D de acuerdo con el género que las representa.

Verificar, en cada caso, que

$$H \;=\; \big\{c \in U\big(D\big) \;:\; c \text{ es representada por la forma principal}\big\}$$

es un subgrupo de $\ker(\chi)$ (de $U\big(D\big)$).

20 Propiedades del género

Observación 20.1. Sea $D \equiv 0, 1 \pmod 4$ y sean f, g formas de discriminante D pertenecientes al mismo género. Si $c \in U\big(D\big)$ es representada por f, entonces es representada por g. Dicho de otra manera, si $m \in c$ y $m = f(x, y)$ para ciertos $x, y \in \mathbb{Z}$, entonces existen $n \in c$ y $x', y' \in \mathbb{Z}$ tales que $n = g(x', y')$.

Definición 20.2. Sea $D \equiv 0, 1 \pmod 4$ y sea f una forma de discriminante D. Si $c \in U\big(D\big)$ es representada por f, decimos también que *la clase c es representada por el género de f.*

Definición 20.3. Sea $D \equiv 0, 1 \pmod 4$. Llamamos *forma principal (de discriminante D)* a la forma

- $\{1, 0, -D/4\}$, si $D \equiv 0$, y a la forma

- $\{1, 1, (1-D)/4\}$, si $D \equiv 1$.

El *género principal (de discriminante D)* es el género al que pertenece la forma principal.

Observación 20.4. Dado un discriminante, la forma principal de dicho discriminante es una forma primitiva.

Lema 20.5. *Sea $D \equiv 0, 1 \pmod 4$ y sea f una forma de discriminante D. Entonces,*

(i) los valores en $U\big(D\big)$ representados por el género principal constituyen un subgrupo $H \leq \ker(\chi)$;

(ii) los valores en $U\big(D\big)$ representados por el género de f constituyen una coclase de H en $\ker(\chi)$.

Teorema 20.6. *Sea $D \equiv 0, 1 \pmod 4$ y sea $H \leq \ker(\chi)$ como en el Lema 20.5. Si $H' \subset \ker(\chi)$ es una coclase de H en $\ker(\chi)$ y p es un primo impar que no divide a D, entonces su clase de congruencia $[p] \in H'$, si y sólo si p es representado por una forma de discriminante D perteneciente al género correspondiente a H'.*

Observación 20.7. Dada una coclase H' de H en $\ker(\chi)$, las clases de congruencia contenidas en H' son representadas por formas de discriminante D (pues $H' \subset \ker(\chi)$; ver el Corolario 19.2). Dada una forma (primitiva) de discriminante D, f, las clases en $U\big(D\big)$ representadas por f constituyen una coclase de H en $\ker(\chi)$ (Lema 20.5 (4)). Existe, entonces, una biyección

$$\big(\text{coclases de } H \text{ en } \ker(\chi)\big) \simeq \big(\text{géneros de formas primitivas de discriminante } D\big)$$

dada por asignar, a una forma (primitiva de discriminante D) f, el conjunto de enteros que ella representa y, a cada entero m coprimo con D, el conjunto de formas (primitivas de discriminante D) que lo representan.

Demostración del Lema 20.5. La demostración estará dividida en cuatro partes:

1 si $m \in \mathbb{Z}$, $(m, D) = 1$, es tal que $m = f(x, y)$ para alguna forma f de discriminante D, entonces $[m] \in \ker(\chi)$;

2 si $H \subset \ker(\chi)$ denota el subconjunto de clases de congruencia módulo D representadas en el género principal, entonces H es un subgrupo de $\ker(\chi)$;

3 si f es una forma *primitiva* de discriminante D y $M \in \mathbb{Z}$, entonces existe, al menos, un $k \in \mathbb{Z}$, $(k, M) = 1$, propiamente representado por f;

4 si f es una forma primitiva de discriminante D, entonces los valores en $U\big(D\big)$ representados por f constituyen una coclase de H en $\ker(\chi)$.

Demostración de 1. Si $m = f(x,y)$ y $g = (x,y)$, entonces $g^2 \mid m$ y

$$f(x/g, y/g) \;=\; m/g^2$$

es una representación propia de $m' = m/g^2$ por f. Dado que χ es *multiplicativo* y *cuadrático*,[46]

$$\chi(m') \;=\; \chi(m)\;,$$

así que podemos suponer que m es representado propiamente por f. Ahora, separamos en dos casos. Si m es impar, por el Lema 15.2, existe $\beta \in \mathbb{Z}$ tal que $D \equiv \beta^2 \,(\mathsf{mod}\, m)$. Entonces, en este caso,

$$\chi(m) \;=\; \left(\frac{D}{m}\right) \;=\; \left(\frac{\beta^2}{m}\right) \;=\; \left(\frac{\beta}{m}\right)^2 \;=\; 1\;.$$

Es decir, $[m] \in \mathsf{ker}(\chi)$. Si, en cambio, m es par, entonces afirmamos:

.1 el discriminante es $D \equiv 1 \,(\mathsf{mod}\, 8)$;

.2 la clase $[m] \in \mathsf{ker}(\chi)$.

En cuanto a .1, si una forma f de discriminante D representa un número par m, entonces f es equivalente a $mx^2+Bxy+Cy^2$ y $D = B^2-4mC \equiv B^2 \,(\mathsf{mod}\, 8)$. Como $D \equiv 1 \,(\mathsf{mod}\, 4)$, se deduce que $D \equiv 1 \,(\mathsf{mod}\, 8)$ (es impar). En cuanto a , como $D \equiv 1 \,(\mathsf{mod}\, 8)$, se cumple que

$$\chi(2) \;=\; 1\;.$$

Entonces, si $m = 2^r m'$ con m' impar, vale que

$$\chi(m) \;=\; \chi(m')\;.$$

Pero $D \equiv \beta^2 \,(\mathsf{mod}\, m)$ implica $D \equiv \beta^2 \,(\mathsf{mod}\, m')$. Como m' es impar,

$$\chi(m') \;=\; \left(\frac{D}{m'}\right) \;=\; \left(\frac{\beta}{m'}\right)^2 \;=\; 1\;.$$

□

Demostración de 2. Por la parte 1, sabemos que $H \subset \mathsf{ker}(\chi)$. Veamos que es subgrupo. Si $D = -4n$, la forma principal es $\{1, 0, n\}$ y, por el Ejercicio 10.1 (ii), el subconjunto H es cerrado por multiplicación: si $m, m' \in H$, entonces $mm' \in H$. Ahora, como $\mathsf{ker}(\chi)$ $\big(U\big(D\big)\big)$ es un grupo finito (de torsión), H es un subgrupo. Si $D \equiv 1 \,(\mathsf{mod}\, 4)$, la forma principal es $f_0 := \{1, 1, (1-D)/4\}$, entonces

$$4\, f_0(x,y) \;=\; (2x+y)^2 - Dy^2 \;\equiv\; (2x+y)^2 \,(\mathsf{mod}\, D)\;.$$

[46] "Multiplicativo" quiere decir $\chi(x\,y) = \chi(x)\,\chi(y)$, para todo par $x, y \in \mathbb{Z}$, "cuadrático" quiere decir que $\chi(x)^2 = 1$ para todo $x \in \mathbb{Z}$, o sea, $\chi(x) \in \{\pm 1\}$.

En consecuencia, en este caso, H está contenido en el *subgrupo* de cuadrados módulo D (pues D es impar y $2 \in U\big(D\big)$). Recíprocamente, si $\beta \in \mathbb{Z}$,

$$4\, f(\beta, 0) \;=\; 4\, f(0, 2\beta) \;\equiv\; 4\, \beta^2 \,(\mathsf{mod}\, D)\ .$$

Dado que $(4, D) = 1$, f_0 representa la clase de β en $U\big(D\big)$. Entonces, en este caso también, H es un subgrupo de $U\big(D\big)$ y, más precisamente, es el subgurpo de cuadrados en $U\big(D\big)$. □

Demostración de 3. Sea $f = \{a, b, c\}$ una forma *primitiva* y sea p un número primo. Podemos recuperar los coeficientes de la forma evaluando en ciertos puntos:

$$f(1, 0) \;=\; a\ , \quad f(0, 1) \;=\; c \quad \text{y} \quad f(1, 1) \;=\; a + b + c\ .$$

Como estamos asumiendo que f es primitiva, el primo escogido p no puede dividir estos tres valores simultáneamente. Obtenemos, de esta manera, *algún* entero no divisible por p y propiamente representado por f. Si, ahora, $M \in \mathbb{Z}$ (arbitrario), podemos elegir, para cada primo $p \mid M$, un $k_p \in \mathbb{Z}$ no divisible por p y propiamente representado por f, es decir, existen k_p, x_p, y_p tales que

$$k_p \;=\; f(x_p, y_p)\ , \quad p \nmid k_p \quad \text{y} \quad (x_p, y_p) \;=\; 1\ .$$

Por el Teorema chino del resto, existen $x, y \in \mathbb{Z}$ tales que

$$x \;\equiv\; x_p \,(\mathsf{mod}\, p) \quad \text{y} \quad y \;\equiv\; y_p \,(\mathsf{mod}\, p)$$

para cada primo $p \mid M$. Si $k := f(x, y)$, entonces $k \equiv k_p \,(\mathsf{mod}\, p)$ y, por lo tanto, p no divide a k y $(k, M) = 1$. Si $g := (x, y) \geq 1$, dividiendo por g^2 a x y a y, el entero k/g^2 es coprimo con M y propiamente representado por f. □

Demostración de 4. Supongamos, en primer lugar, que $D \equiv 0 \,(\mathsf{mod}\, 4)$, $D = -4n$. Elegimos $M = D$. Si f es una forma primitiva discriminante D, podemos, por la parte 3, encontrar $a \in \mathbb{Z}$, $(a, M) = 1$, propiamente representado por f. Por el Lema 15.1, la forma f es estrictamente equivalente a una forma $f_1 = \{a, b, c\}$ (con a como primer coeficiente). Dado que f y f_1 representan los mismos enteros, podemos asumir que la forma f es $f = \{a, b, c\}$, con $(a, 4n) = 1$. Asumiendo esto, vemos que

$$\begin{aligned} -4n \;&=\; b^2 - 4ac\ , \\ b \;&=\; 2b' \quad \text{es par y} \\ af(x, y) \;&=\; (ax + b'y)^2 + ny^2 \;\in\; H\ . \end{aligned}$$

En particular, los valores en $U\big(D\big)$ representados por f pertenecen a la coclase $[a]^{-1}\, H$. Recíprocamente, dada $[c] \in [a]^{-1}\, H$, para ciertos $z, w \in \mathbb{Z}$, se cumple

$$ac \;\equiv\; z^2 + nw^2 \quad (\mathsf{mod}\, 4n)$$

(ejercicio). Sean $x, y \in \mathbb{Z}$ tales que

$$ax + b'y \equiv z \,(\mathsf{mod}\, 4n) \quad \text{y} \quad y \equiv w \,(\mathsf{mod}\, 4n)$$

(ejercicio). Entonces, $af(x,y) \equiv z^2 + nw^2 \equiv ac$ y $f(x,y) \equiv c \,(\mathsf{mod}\, 4n)$.

Si $D \equiv 1 \,(\mathsf{mod}\, 4)$, al igual que antes, podemos encontrar a coprimo con $|D|$ propiamente representado por f y cambiar f por una forma estrictamente equivalente $\{a, b, c\}$. Asumiendo que $f = \{a, b, c\}$ con $(a, D) = 1$,

$$4af(x,y) \;=\; (2ax + by)^2 - Dy^2 \;\equiv\; (2ax + by)^2 \pmod{D} \;.$$

Dado que $(4, D) = 1$ y también $(a, D) = 1$,

$$f(x,y) \;\equiv\; [a]^{-1} \left([2]^{-1} (2ax + by) \right)^2 \;\in\; [a]^{-1} H \;.$$

Recíprocamente, dada $[c] \in [a]^{-1} H$,

$$4ac \;\equiv\; 4\beta^2 \;\equiv\; 4\left(z^2 + zw + \frac{1 - D}{4} w^2 \right) \;\equiv\; (2z + w)^2 \pmod{D}$$

(ejercicio). Eligiendo $x, y \in \mathbb{Z}$, tales que

$$2ax + by \;\equiv\; 2z + w \pmod{D}$$

(ejercicio), vemos que $4af(x,y) \;\equiv\; 4ac \,(\mathsf{mod}\, D)$ y $f(x,y) \equiv c \,(\mathsf{mod}\, D)$. □

□

Corolario 20.8. *Sea $n \in \mathbb{Z}$ y sea p un primo impar que no divide a n. Entonces, p es representado en una forma de discriminante $-4n$ perteneciente al género principal, si y sólo si existe $\beta \in \mathbb{Z}$ tal que*

$$p \;\equiv\; \beta^2 \quad o \quad \beta^2 + n \pmod{4n} \;.$$

Demostración. Si p es representada en una forma perteneciente al género principal, entonces

$$p \;\equiv\; x^2 + ny^2 \,(\mathsf{mod}\, 4n) \;,$$

para ciertos $x, y \in \mathbb{Z}$. Si $y \equiv 0 \,(\mathsf{mod}\, 2)$, entonces $p \equiv x^2 \,(\mathsf{mod}\, 4n)$; si $y \equiv 1 \,(\mathsf{mod}\, 2)$, entonces $p \equiv x^2 + n \,(\mathsf{mod}\, 4n)$. Recíprocamente, si p es de esta forma, entonces p, su clase de congruencia, pertenece al subconjunto (subgrupo) de $U\big(4n\big)$ de valores representados en la forma principal y, por lo tanto, en el género principal. □

El Corolario 20.8 tiene una versión para $D \equiv 1$.

Corolario 20.9. *Sea $D \equiv 1 \,(\mathsf{mod}\, 4)$ y sea p un primo impar que no divide a D. Entonces, p es representado en una forma de discriminante D perteneciente al género principal, si y sólo si p es un cuadrado módulo $|D|$.*

Demostración. Si p es representado en una forma del género principal, entonces

$$p \equiv x^2 + xy + \frac{1-D}{4}\, y^2 \equiv \left([2]^{-1} \ (2x+y) \right)^2 (\mathsf{mod}\, |D|) \ .$$

Recíprocamente, si $p \equiv \beta^2 \,(\mathsf{mod}\, |D|)$, entonces p, su clase de congruencia, pertenece al subconjunto (subgrupo) de $U\big(D\big)$ de valores representados por la forma principal ($x = \beta$, $y = 0$) y, por lo tanto, por el género principal. □

Ejercicios

Ejercicio 20.1. Para $D \in \{-40, -60, -84, -88, -92, -120\}$, describir los géneros de formas cuadráticas de discriminante D.[47]

Ejercicio 20.2. Dar condiciones sobre un primo p para que se cumpla $p = x^2 + ny^2$, para $n \in \{6, 10, 13, 15, 21, 22, 30\}$.

21 Resumen

Consideremos el problema de representar un primo p en la forma $\{1, 0, n\}$ $(n > 0)$. Cuando $n = 1, 2, 3$, la solución queda sintetizada en los siguientes pasos:

(descenso) si existen $x, y \in \mathbb{Z}$, $(x, y) = 1$, tales que p divide $x^2 + ny^2$, entonces p se puede expresar en la forma $x^2 + ny^2$ (posiblemente distintos x e y);

(reciprocidad) es posible hallar enteros α, β, ..., tales que, si

$$p \equiv \alpha,\, \beta,\, \ldots \quad (\mathsf{mod}\, 4n) \ ,$$

entonces p divide $x^2 + ny^2$ para ciertos $x, y \in \mathbb{Z}$, $(x, y) = 1$.

Los resultados de la § 11 demuestran el paso de reciprocidad:

Teorema 11.10. *Sean $n \in \mathbb{Z}$, $n \neq 0$, y χ la función del Lema 11.9 ($D = -4n$). Entonces, si p es un primo positivo impar que no divide a n, las siguientes afirmaciones son equivalentes:*

(a) existen $a, b \in \mathbb{Z}$ tales que $p \mid a^2 + nb^2$ y $(a, b) = 1$;

(b) $(-n/p) = 1$;

(c) $\chi(p) = 1$.

Entonces, para un número primo, dividir un entero de la forma $x^2 + ny^2$, $(x, y) = 1$, es equivalente a una serie de condiciones de congruencia ((c)). Esto último no es especial de $n \in \{1, 2, 3\}$.

El paso de descenso se puede describir con el lenguage introducido en la § 15.

[47] Hint: Recordar que dos coclases distintas son disjuntas, tiene todas el mismo cardinal y su unión es todo.

Corolario 15.4. *Sea $n \in \mathbb{Z}$, $n \neq 0$, y sea p un primo positivo impar que no divide a n. Entonces, p es representado por una forma primitiva de discriminante $-4n$, si y sólo si p es un divisor primo de $x^2 + ny^2$, $(x, y) = 1$.*

Equivalentemente, por la § 16, podemos relacionarlo con la idea de forma reducida y número de clases.

Corolario 16.7. *Sea $n \in \mathbb{Z}$, $n > 0$, y sea p un primo positivo impar que no divide a n. Entonces, p es representado por una forma primitiva* reducida *de discriminante $-4n$, si y sólo si p es un divisor de $x^2 + ny^2$, $(x, y) = 1$.*

Este resultado es especialmente útil en los casos $\mathsf{h}(-4n) = 1$, pues, entonces, la única forma reducida de discriminante $-4n$ es la forma principal $\{1, 0, n\}$. Sin embargo, $\mathsf{h}(-4n) = 1$, si y sólo si $n \in \{1, 2, 3, 4, 7\}$. Lo único que queda es describir $\ker(\chi)$ en estos cinco casos.

La teoría de géneros entra al tratar de estudiar los casos $\mathsf{h}(-4n) > 1$. Resulta que las formas cuadráticas se pueden agrupar de acuerdo a los valores $c \in U\big(4n\big)$ que ellas representan. Además, hay una estrutura algebraica subyacente en esta manera de agruparlas.

Lema 20.5. *Sea $D \equiv 0, 1 \pmod 4$ y sea f una forma de discriminante D. Entonces,*

(i) los valores en $U\big(D\big)$ representados por el género principal constituyen un subgrupo $H \leq \ker(\chi)$;

(ii) los valores en $U\big(D\big)$ representados por el género de f constituyen una coclase de H en $\ker(\chi)$.

En el caso $D \equiv 0 \pmod 4$, este resultado tiene la siguiente consecuencia.

Corolario 20.8. *Sea $n \in \mathbb{Z}$ y sea p un primo impar que no divide a n. Entonces, p es representado en una forma de discriminante $-4n$ perteneciente al género principal, si y sólo si existe $\beta \in \mathbb{Z}$ tal que*

$$p \equiv \beta^2 \quad o \quad \beta^2 + n \pmod{4n} \ .$$

Nuevamente, esto es particularmente útil si el género principal consiste únicamente en la forma principal, es decir, si hay exactamente una forma reducida por género.

Ejemplo 21.1. El género principal de formas de discriminante $-4n$ contiene solamente la forma principal, si

$$n \in \{6, 10, 13, 15, 21, 22, 30\} \ .$$

Lo que resta en estos (y posiblemente otros) casos es describir el subgrupo $H \leq \ker(\chi)$ correspondiente al género pricipal.

Ejercicios

Ejercicio 21.1. Sea $D \equiv 0, 1 \pmod 4$ un discriminante y sea $\tilde{H} \subset U\big(D\big)$ el subconjunto de clases x que verifican las siguientes condiciones:

- para todo primo impar $q \mid D$, $(x/q) = 1$, y
- la clase es

$$x \equiv \begin{cases} x \equiv 1 \pmod 4 \ , & \text{si } D \equiv 12 \pmod{16} \ , \\ x \equiv 1 \pmod 4 \ , & \text{si } D \equiv 16 \pmod{32} \ , \\ x \equiv 1 \pmod 8 \ , & \text{si } D \equiv 0 \pmod{32} \ , \\ x \equiv 1, 7 \pmod 8 \ , & \text{si } D \equiv 8 \pmod{32} \quad \text{y} \\ x \equiv 1, 3 \pmod 8 \ , & \text{si } D \equiv 24 \pmod{32} \ . \end{cases}$$

Notar que la última condición es vacía, si $D \equiv 1 \pmod 4$ o si $D = -4n$ con $n \equiv 3 \pmod 4$.

(i) Probar que $\tilde{H}$ es subgrupo de $U\big(D\big)$ y que $\tilde{H} \subset \ker(\chi)$.

(ii) Probar que $\tilde{H} = H$,[48] donde $H \subset U\big(D\big)$ es el subconjunto

$$H = \begin{cases} \big\{x \equiv \beta^2 \text{ o } \beta^2 + n \pmod{4n} \ : \ \beta \in \mathbb{Z}\big\} \ , & \text{si } D = -4n \ , \\ \big\{x \equiv \beta^2 \pmod D \ : \ \beta \in \mathbb{Z}\big\} \ , & \text{si } D \equiv 1 \pmod 4 \ . \end{cases}$$

.

[48] Hint: En el caso $D = -4n$, traducir la condición sobre D a n y mostrar que, si n' es la parte impar de n, entonces la condición $(x/q) = 1$ para todo primo impar $q \mid n$ equivale a que x sea cuadrado módulo n'.

Parte VI

Composición de formas cuadráticas

22 Estructura en el conjunto de clases

Hasta el momento, contamos con un criterio para determinar si un número primo se puede representar por una forma cuadrática de discriminante prescrito ¿Qué pasa con números compuestos? ¿Podemos representar pq por una forma de discriminante D, si podemos representar los enteros p y q por formas de discriminante D?

23 El grupo de clases

24 El grupo de géneros

25 Números convenientes

Parte VII

Reciprocidad cúbica y bicuadrática

Referencias

[Cox22] D. A. Cox. *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*. 3rd edition. Vol. 387. AMS Chelsea Publ. Providence, RI: American Mathematical Society (AMS), 2022.

[Dav80] H. Davenport. *Multiplicative Number Theory*. 2nd. ed. Vol. 74. Grad. Texts Math. Springer, Cham, 1980.

[Dav08] H. Davenport. *The Higher Arithmetic. An Introduction to the Theory of Numbers*. 8th revised ed. Cambridge: Cambridge University Press, 2008.

[Fla89] D. E. Flath. *Introduction to Number Theory*. New York etc.: Wiley, 1989.

[Gau86] C. F. Gauß. *Disquisitiones arithmeticae*. New York etc.: Springer-Verlag. xx, 472 p. DM 148.00 (1986). 1986.

[Gen84] E. R. Gentile. *Notas de Álgebra I*. 3rd corrected and augmented ed. Ediciones Previas. Buenos Aires: EUDEBA, 1984.

[HW08] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Ed. by D. R. Heath-Brown and J. H. Silverman. 6th ed. Oxford: Oxford University Press, 2008.

[IR90] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. 2nd ed. Vol. 84. Grad. Texts Math. New York etc.: Springer-Verlag, 1990.

[KKS00] K. Kato, N. Kurokawa, and T. Saito. *Number Theory 1. Fermat's Dream*. Vol. 186. Transl. Math. Monogr. Providence, RI: American Mathematical Society, 2000.

[Kob77] N. Koblitz. *p-adic Numbers, p-adic Analysis, and zeta-functions*. Vol. 58. Grad. Texts Math. Springer, Cham, 1977.

[Lan99] E. Landau. *Elementary Number Theory*. Reprint of the 1966 2nd edition. Providence, RI: American Mathematical Society (AMS), 1999.

[Lan02] S. Lang. *Algebra*. 3rd revised ed. Vol. 211. Grad. Texts Math. New York, NY: Springer, 2002.

[NZM91] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An Introduction to the Theory of Numbers*. 5th ed. New York etc.: John Wiley &— Sons, Inc., 1991.

[Rob00] A. M. Robert. *A Course in p-adic Analysis*. Vol. 198. Grad. Texts Math. New York, NY: Springer, 2000.

[Rod07] F. Rodríguez Villegas. *Experimental Number Theory*. Vol. 13. Oxf. Grad. Texts Math. Oxford: Oxford University Press, 2007.

Índice de contenidos