FORMAS CUADRÁTICAS BINARIAS

RICARDO MENARES

Índice

1. Introducción 1
2. Finitud 3
2.1. Demostración del Teorema 1.5 4
2.2. Ejemplos 4
3. Ley de composición 5
3.1. Existencia de B 6
3.2. Complementos sobre representaciones de enteros 7
3.3. Composición de Dirichlet en clases 8
3.4. Demostración del Teorema 3.1 8
3.5. Elementos de orden 2 en $C(D)$ 9
4. Número de clases 9
Referencias 10

1. Introducción

Esta charla está basada en partes del Capítulo 1, sección 2 de [Cox13]. Nos interesaremos en formas cuadráticas del tipo

$$f(x,y) = ax^2 + bxy + cy^2, \tag{1.1}$$

con a, b, c enteros. Diremos que

- f es *primitiva* si m.c.d.$(a,b,c) = 1$
- $m \in \mathbb{Z}$ es *representado* por f si existen $u, v \in \mathbb{Z}$ con $f(u,v) = m$
- $m \in \mathbb{Z}$ es *propiamente representado* por f si podemos tomar u, v como antes, cumpliendo además m.c.d.$(u,v) = 1$.

Observación 1.1. Si $m \in \mathbb{Z}$ es libre de cuadrados y es representado por f, entonces también es propiamente representado.

Diremos que dos formas cuadráticas $f(x,y), g(x,y) \in \mathbb{Z}[x,y]$ son *equivalentes* si existen $p, q, r, s \in \mathbb{Z}$ con $ps - qr = 1$ y

$$f(x,y) = g(px + qy, rx + sy).$$

Notar que en tal caso, la matriz $\gamma := \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ es un elemento del grupo $SL_2(\mathbb{Z})$. A menudo usaremos la notación

$$\gamma \cdot g(x,y) = g(px + qy, rx + sy). \tag{1.2}$$

Es sencillo ver que la relación definida es una relación de equivalencia. Denotaremos por $[f]$ a la clase de equivalencia de f. La fórmula (1.2) define una acción de $SL_2(\mathbb{Z})$ en el conjunto de las formas cuadráticas binarias. Las matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ y } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generan $SL_2(\mathbb{Z})$, por lo que introduciremos una notación especial para la acción de estas. Para f como en (1.1), definimos

$$\begin{aligned} f_T(x,y) &:= T \cdot f(x,y) = ax^2 + (2a+b)xy + (a+b+c)y^2, \\ f_S(x,y) &:= S \cdot f(x,y) = cx^2 - bxy + ay^2. \end{aligned} \tag{1.3}$$

La relación introducida es pertinente desde el punto de vista de la clasificación de los enteros representados por tales formas. Dada una forma cuadrática f y $m \in \mathbb{Z}$, definimos

$$R(f,m) = \{(u,v) \in \mathbb{Z}^2 : f(u,v) = m\}$$
$$R^*(f,m) = \{(u,v) \in \mathbb{Z}^2 : \text{m.c.d.}(u,v) = 1 \text{ y } f(u,v) = m\}.$$

Proposición 1.2. *Dos formas cuadráticas equivalentes representan los mismos enteros. Lo mismo vale para las representaciones propias. Más precisamente, si f, g son formas cuadráticas equivalentes y $\gamma \in SL_2(\mathbb{Z})$ es tal que $f = \gamma \cdot g$, entonces la regla*

$$(u,v) \mapsto (u,v) \cdot \gamma^t$$

induce una biyección entre $R(f,m)$ y $R(g,m)$, así como entre $R^*(f,m)$ y $R^*(g,m)$.

Demostración: De la definición de acción, vemos que $g\left((u,v) \cdot \gamma^t\right) = f(u,v)$, luego la aplicación descrita envía $R(f,m)$ en $R(g,m)$. La función inducida por $(a,b) \mapsto (a,b) \cdot \gamma^{-t}$ es una inversa, luego es una biyección.

Para ver que también es una biyección cuando se restringe a $R^*(f,m)$, basta verificar que si m.c.d. $(u,v) = 1$, entonces el m.c.d. entre los coeficientes de $(u,v) \cdot \gamma^t$ también es 1. Se trata de un ejercicio sencillo. □

El discriminante de $f(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ se define por $D = b^2 - 4ac$. Notar que $D \equiv 0$ o $1 \mod 4$.

Lema 1.3. *Dos formas equivalentes tienen el mismo discriminante.*

Demostración: Es un cálculo directo de las definiciones. □

La identidad ("completar el cuadrado")

$$4af(x,y) = (2ax + by)^2 - Dy^2$$

muestra que

i) Si $D > 0$, entonces f representa enteros tanto negativos como positivos. En particular, f es una forma indefinida

ii) Si $D < 0$ y $a > 0$, entonces f representa solo enteros positivos. En particular, f es una forma definida positiva

ii') Si $D < 0$ y $a < 0$, entonces f representa solo enteros negativos. En particular, f es una forma definida negativa.

El problema de representación de enteros por formas cuadráticas puede reducirse a estudiar formas primitivas. Esto motiva definir

$$C(D) = \{\text{clases de equivalencia de formas cuadráticas binarias primitivas y definidas positivas de discriminante } D\}.$$

Observación 1.4. Es sencillo ver que $C(D) \neq \emptyset$ si y solo si $D < 0$ y $D \equiv 0$ o $1 \mod 4$.

Lo que sigue tiene como objetivo demostrar los siguientes teoremas.

Teorema 1.5. *El conjunto $C(D)$ es finito*

Teorema 1.6. *Existe una operación binaria en $C(D)$ que lo dota de una ley de grupo conmutativo y con la propiedad siguiente: para todo $\alpha, \beta \in C(D)$, la clase de la composición de α y β representa a todos los enteros de la forma $n \cdot m$, donde n es representado por α y m es representado por β.*

El Teorema 1.6 está enunciado aquí de manera imprecisa, ver el Lema 3.6 y el Teorema 3.1 para una formulación precisa.

Observación 1.7. Para $D > 0$ hay un $C(D)$ análogo para el que se cumple el Teorema 1.5 y una variante del Teorema 1.6, pero las técnicas que establecen estos hechos son distintas de las que veremos a continuación.

1.1. Agradecimientos. Matías Alvarado y Patricio Pérez hicieron comentarios y correcciones valiosas a una primera versión de este texto.

2. Finitud

El objetivo de esta sección es demostrar el Teorema 1.5 (ver la sección 2.1). Para ello estableceremos una *teoría de la reducción*, cuyo fin es describir el elemento más "pequeño" en una clase de $C(D)$. La noción de 'elemento pequeño" está dada en la siguiente definición.

Definición 2.1. Una forma primitiva $f(x,y) = ax^2 + bxy + cy^2$ se dice *reducida* si se cumplen las dos condiciones siguientes:

i) $|b| \leq a \leq c$
ii) $(|b| = a \vee a = c) \Rightarrow b \geq 0$.

Proposición 2.2. *Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma reducida de discriminante $D < 0$. Entonces*

$$a \leq \sqrt{\frac{-D}{3}}. \tag{2.4}$$

Demostración: Como f es reducida y definida positiva, tenemos $b^2 \leq a^2$ y además $1 \leq a \leq c$. Así,

$$D = b^2 - 4ac \leq a^2 - 4a^2 = -3a^2.$$

De aquí se deduce (2.4). □

Lema 2.3. *Sea $f(x,y) = ax^2+bxy+cy^2$ una forma reducida y definida positiva. Si $u, v \in \mathbb{Z}$ cumplen $m.c.d.(u,v) = 1$ y $f(u,v) \leq c$, entonces $f(u,v) \in \{a, c\}$ y $(u,v) \in \{\pm(1,0), \pm(0,1), \pm(1,-1)\}$. Más aún, el número de representaciones propias de a es*

$$\begin{array}{ll} 2 & \text{si } a < c \\ 4 & \text{si } 0 \leq b < a = c \\ 6 & \text{si } a = b = c. \end{array}$$

Demostración: ver [NZM91], Lemma 3.24, p. 182. □

Proposición 2.4. *Toda forma primitiva y definida positiva es equivalente a una única forma reducida.*

Observación 2.5. La Proposición 2.4 falla para formas indefinidas, pues puede haber formas reducidas equivalentes y distintas.

Demostración: Fijemos un discriminante $D < 0$.

Existencia: Sea $\alpha \in C(D)$. Veamos que existe una forma reducida en la clase α.

Sea $f(x,y) = ax^2 + bxy + cy^2 \in \alpha$ tal que $|b|$ es mínimo entre las formas de la clase α.

Afirmación: $|b| \leq a$.

Razonaremos por absurdo. Suponemos $|b| > a$. Tomemos una matriz de la forma

$$\gamma = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}), \quad m \in \mathbb{Z}.$$

Sea $g := \gamma \cdot f$. Por definición, g es una forma equivalente a f. Además, vemos que g tiene la forma

$$g(x,y) = ax^2 + (2am + b)xy + \tilde{c}y^2, \quad \tilde{c} \in \mathbb{Z}.$$

Como $|b| > a$, tenemos que existe m tal que

$$|2am + b| < |b|,$$

lo que contradice la elección de f. Esto demuestra la afirmación.

La forma f_S definida en (1.3) es equivalente a f y cumple $f_S(x,y) = cx^2 - bxy + ay^2$. Deducimos que, reemplazando f por f_S de ser necesario, podemos suponer que $a \leq c$.

En resumen, gracias a la afirmación tenemos una forma $f \in \alpha$ tal que $|b| \leq a \leq c$. Si f es reducida, hemos terminado. Supongamos entonces que f no es reducida. Esto quiere decir que $b < 0$ y que $a = -b$ o $a = c$.

Si $a = -b$, entonces $f(x,y) = ax^2 - axy + cy^2$. En tal caso

$$f_T(x,y) = f(x+y, y) = ax^2 + axy + cy^2$$

es una forma equivalente a f y reducida.

Si $a = c$, entonces $f(x,y) = ax^2 + bxy + ay^2$. En tal caso

$$f_S(x,y) = f(-y, x) = ax^2 - bxy + ay^2$$

es una forma equivalente a f y reducida.

Unicidad: Sean f, g formas de discriminante D, reducidas y equivalentes. Escribimos

$$f(x,y) = ax^2 + bxy + ay^2, \quad g(x,y) = a'x^2 + b'xy + a'y^2.$$

Como f y g son equivalentes, de la Proposición 1.2 sabemos que representan propiamente a los mismos enteros. El Lema 2.3 caracteriza al coeficiente de x^2 como el menor entero positivo propiamente representado por una forma reducida. Luego, $a = a'$.

Caso 1: $a < c$.

Por el Lema 2.3, sabemos que hay exactamente 2 representaciones propias de a por f. También sabemos que c es el segundo menor entero positivo propiamente representado por f. La Proposición 1.2 asegura que lo mismo vale para g. Usando otra vez el Lema 2.3, concluimos que $a < c'$ y que c' es el segundo menor entero positivo propiamente representado por g. De nuevo por la Proposición 1.2, deducimos que $c = c'$.

Como $D = b^2 - 4ac = (b')^2 - 4ac$, deducimos $b = \pm b'$. Sea

$$\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z})$$

una matriz tal que $g = \gamma \cdot f$. Entonces

$$a = g(1,0) = f(p,q), \quad c = g(0,1) = f(q,s).$$

Como $ps - rq = 1$, estas representaciones son propias. Luego el Lema 2.3 asegura que

$$(p,r) \in \{\pm(1,0)\} \text{ y } (q,s) \in \{\pm(0,1), \pm(1,-1)\}.$$

Dado que $f(1,-1) = \underbrace{a-b}_{>0} + c > c$, concluimos que $(q,s) \in \{\pm(1,0)\}$. Deducimos que $\gamma = \pm I_{2\times 2}$ y que $f = g$.

Caso 2: $a = c$.

El Lema 2.3 asegura que f representa propiamente a al menos 4 veces. De la Proposición 1.2 deducimos que lo mismo vale para g. Usando el Lema 2.3 otra vez, concluimos que $a = c'$. Como $D = b^2 - 4a^2 = (b')^2 - 4a^2$, deducimos que $b = \pm b'$. Al tratarse de formas reducidas, tenemos $0 \leq b, b'$, de donde $b = b'$.

□

2.1. Demostración del Teorema 1.5. Por la Proposición 2.4, basta demostrar que hay a lo más un número finito de formas reducidas en $C(D)$. Si

$$f(x,y) = ax^2 + bxy + cy^2. \tag{2.5}$$

es una forma reducida de discriminante $D < 0$, la Proposición 2.2 asegura que hay a lo más un número finito de posibilidades para el coeficiente a. Como $|b| \leq a$, lo mismo puede decirse sobre el coeficiente b. Finalmente, dado que

$$D = b^2 - 4ac. \tag{2.6}$$

y que D está fijo, vemos que hay a lo más un número finito de posibilidades para c. Esto demuestra el Teorema 1.5.

2.2. Ejemplos. Es sencillo convertir la demostración del Teorema 1.5 en un algoritmo para determinar $C(D)$ con $D < 0$. Realizaremos tal determinación para algunos valores pequeños de $|D|$.

1. $C(-4) = \{[x^2 + y^2]\}$.

   Si $f(x,y)$ como en (2.5) es una forma primitiva, reducida y de discriminante -4, la Proposición 2.2 afirma que

   $$a \leq \sqrt{\frac{4}{3}} = 1{,}1547...$$

   Al ser a un entero positivo, tenemos $a = 1$. Como $|b| \leq a$, tenemos que $b \in \{-1, 0, 1\}$. La relación (2.6) dice $-4 = b^2 - 4c$, de donde deducimos que b es par. Por lo tanto, $b = 0$ y $-4 = -4c$ implica $c = 1$. Es decir, la única forma primitiva y reducida de discriminante -4 es $x^2 + y^2$, como se quería.

2. $C(-20) = \{[x^2 + 5y^2], [2x^2 + 2xy + 3y^2]\}$.

   Como antes, deducimos $a \leq \sqrt{\frac{20}{3}} = 2{,}581...$, luego $a \in \{1, 2\}$.

   Si $a = 1$, entonces $b = 0$ (pues $|b|$ es par y ≤ 1). La relación (2.6) se lee $-20 = -4c$, luego $c = 5$. Así, encontramos la forma $x^2 + 5y^2$.

   Si $a = 2$, igual que antes vemos que b es par. Como $|b| \leq 2$, tenemos que $b \in \{-2, 0, 2\}$. Notar que $b = -2$ no puede ocurrir pues en tal caso $|b| = a$, lo que obliga a $b \geq 0$. Si $b = 0$, la relación (2.6) se lee $-20 = -8c$, lo que es imposible en $\mathbb{Z}$. Por lo tanto, $b = 2$ y (2.6) implica $-20 = 4 - 8c$, de donde $c = 3$. Así, encontramos la forma $2x^2 + 2xy + 3y^2$, como se quería.

3. $C(-32) = \{[x^2 + 8y^2], [3x^2 + 2xy + 3y^2], [3x^2 - 2xy + 3y^2]\}$.

   Como antes, $a < \sqrt{\frac{32}{3}} = 3{,}265...$, luego $a \in \{1, 2, 3\}$. Además, b es par.

   Si $a = 1$, entonces $b = 0$. La relación (2.6) se lee $-32 = -4c$, luego $c = 8$. Así, encontramos la forma $x^2 + 8y^2$.

   Si $a = 2$, tenemos que $b \in \{-2, 0, 2\}$. Al igual que antes, $b = -2$ no puede ocurrir. Si $b = 0$, la relación (2.6) se lee $-32 = -8c$, lo que fuerza c a ser par, pero esto no es posible porque la forma es primitiva. Por lo tanto, $b = 2$ y (2.6) implica $-32 = 4 - 8c$, lo que es imposible en $\mathbb{Z}$.

   Si $a = 3$, tenemos que $b \in \{-2, 0, 2\}$. Si $b = 0$, entonces (2.6) dice $-32 = -12c$, lo que no es posible en $\mathbb{Z}$. Si $b = \pm 2$, entonces la relación (2.6) se lee $-32 = 4 - 12c$, de donde $c = 3$. Luego obtenemos las dos formas $3x^2 \pm 2xy + 3y^2$, como se quería.

4. $C(-4 \cdot 31) = \{[x^2 + 31y^2], [5x^2 + 4xy + 7y^2], [5x^2 - 4xy + 7y^2]\}$.

   Tenemos $a < \sqrt{\frac{4 \cdot 31}{3}} = 6{,}42...$, luego $a \in \{1, 2, 3, 4, 5, 6\}$. Además, b es par y $|b| \leq 6$.

   Si $b = 0$, la relación (2.6) implica $31 = ac$, lo que obliga $a = 1$ y $c = 31$ (pues 31 es primo y $a < c$). Luego, encontramos la forma $x^2 + 31y^2$.

   Si $b = \pm 2$, entonces $a \geq 2$ y (2.6) es $-4 \cdot 31 = 4 - 4ac$, de donde $32 = ac$. Como $2 \leq a \leq 6$, esto fuerza a que a y c sean ambos pares, lo que no es posible pues la forma debe ser primitiva.

   Si $b = \pm 4$, entonces $a \geq 4$ y (2.6) es $-4 \cdot 31 = 16 - 4ac$, de donde $35 = ac$. Luego $a = 5, c = 7$, encontrando las formas $5x^2 \pm 4xy + 7y^2$.

   Si $b = \pm 6$, entonces $a = b = 6$. Luego (2.6) da $-4 \cdot 31 = 36 - 24c$, lo que no es posible en $\mathbb{Z}$.

5. $C(-56) = \{[x^2 + 14y^2], [2x^2 + 7y^2], [3x^2 - 2xy + 5y^2], [3x^2 + 2xy + 5y^2]\}$.

   Como antes, b es par. La Proposición 2.2 asegura que $a < \sqrt{\frac{56}{3}} = 4{,}3204...$, luego $a \in \{1, 2, 3, 4\}$.

   $a = 1$: necesariamente $b = 0$, luego $c = \frac{56}{4} = 14$. Encontramos la forma $x^2 + 14y^2$.

   $a = 2$: se tiene $b \in \{0, 2\}$. Si $b = 0$, entonces $c = \frac{56}{8} = 7$, luego se trata de la forma $2x^2 + 7y^2$. Si $b = 2$, entonces (2.6) lleva a la relación $2c = 15$, lo que no es posible en $\mathbb{Z}$.

   $a = 3$: en este caso $b \in \{-2, 0, 2\}$. Si $b = \pm 2$, entonces de (2.6) se deduce $c = 5$. Luego aparecen las formas $3x^3 \pm 2xy + 5y^2$.

   $a = 4$: en este caso $b \in \{-2, 0, 2, 4\}$. Si $b = \pm 2$, entonces de (2.6) se deduce $4c = 15$, lo que es imposible. Si $b = 0$, la misma ecuación conduce a $7 = 2c$, también imposible. Si $b = 4$, llegamos a la relación $-7 = 2 - 2c$, de nuevo imposible.

3. Ley de composición

Desde el punto de vista del problema de representar enteros, es deseable contar con un procedimiento que, dadas dos formas f y g de igual discriminante, produzca una tercera forma $f * g$, con la propiedad: todo entero de la forma nm, donde n es representado por f y m es representado por g, es representado por $f * g$. La búsqueda de tal procedimiento - denominado *composición de formas cuadráticas* - llevó a descubrir una ley de grupo en $C(D)$. Gauss fue el primero en explotar esta ley de grupo. A continuación describiremos esta ley de composición, siguiendo el tratamiento posterior de Dirichlet.

Sean

$$f(x,y) = ax^2 + bxy + cy^2, \quad g(x,y) = a'x^2 + b'xy + c'y^2$$

formas primitivas de discriminante $D < 0$. Supondremos además que

$$\text{m.c.d.}\left(a, a', \frac{b+b'}{2}\right) = 1. \tag{3.7}$$

Notar que b y b' tienen la misma paridad, al ser f y g formas de igual discriminante. Definimos

$$f * g(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2, \tag{3.8}$$

donde B es un entero que satisface

$$\begin{aligned} B &\equiv b \mod 2a \\ B &\equiv b' \mod 2a' \\ B^2 &\equiv D \mod 4aa' \end{aligned} \tag{3.9}$$

Esta definición requiere varias aclaraciones:

1. no hay razón para que la hipótesis (3.7) se cumpla siempre, en particular si $f = g$. Sin embargo, veremos más adelante (Lema 3.6) que, dadas dos clases en $C(D)$, siempre es posible encontrar representantes que cumplan (3.7).
2. la existencia de un entero B con las propiedades indicadas requiere justificación. Esto se hará en la sección 3.1.
3. veremos que B no es único. Así, $f*g$ no depende solo de f y g, sino también de la elección de B. Sin embargo, veremos que al cambiar B por otro que cumpla las propiedades indicadas, la clase de equivalencia de $f * g$ no cambia. Esto será justificado en la charla de Claudio Bravo.

Teorema 3.1. *Sea $D < 0$ un entero, con $D \equiv 0$ o $1 \mod 4$. La operación * definida en (3.8) induce una ley de grupo abeliano en $C(D)$. El elemento identidad es la clase de*

$$\begin{array}{ll} x^2 - \frac{D}{4}y^2 & \text{si } D \equiv 0 \mod 4 \\ x^2 + xy + \frac{1-D}{4}y^2 & \text{si } D \equiv 1 \mod 4. \end{array}$$

Además, $[ax^2 + bxy + cy^2]^{-1} = [ax^2 - bxy + cy^2]$.

La demostración de que la operación * define una ley de grupo conmutativo está incluida en la charla de Claudio Bravo, quien también explicará la relación entre $C(D)$ y el grupo de clases de un orden de $\mathbb{Q}(\sqrt{D})$. En la sección 3.4 demostraremos el resto de las afirmaciones.

Para D arbitrario, determinar la estructura de grupo de $C(D)$ no es fácil. Aún así, podemos decir algo cuando $|D|$ pequeño. En los los primeros cuatro ejemplos de la sección 2.2 se cumple que $|C(D)|$ es 1 o es un número primo, por lo que $C(D)$ es cíclico en todos esos casos. En la sección 3.5 determinaremos la estructura del último ejemplo de esa sección.

3.1. Existencia de B.

Lema 3.2. *Sean $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_r, m \in \mathbb{Z}$ con m.c.d.$(p_1, \ldots, p_r, m) = 1$. Entonces las congruencias*

$$p_i x \equiv q_i \mod m, \quad i = 1, 2, \ldots, r,$$

tienen solución única $\mod m$ si y solo si

$$p_i q_j \equiv p_j q_i \mod m, \quad \text{para todo } i, j = 1, 2, \ldots, r.$$

Demostración: La implicancia directa es clara. Demostraremos la afirmación recíproca.

Para ver que existe solución, tomamos $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}$ tales que $\alpha m + \sum_{j=1}^r \alpha_j p_j = 1$. Luego, para todo $1 \le i \le r$, se cumple $\alpha m q_i + \sum_{j=1}^r \alpha_j p_j q_i = q_i$. Mirando esta relación módulo m obtenemos

$$p_i \cdot \left(\sum_{j=1}^r \alpha_j q_j\right) \equiv \sum_{j=1}^r \alpha_j p_i q_j \equiv \sum_{j=1}^r \alpha_j p_j q_i \equiv q_i \mod m.$$

Concluimos que $x := \sum_{j=1}^r \alpha_j q_j$ es una solución al sistema de congruencias.

Para demostrar la unicidad, tomemos dos soluciones x, x'. Entonces, para todo $1 \le i \le r$ se tiene $p_i x \equiv p_i x' \mod m$. En particular, para todo primo p y entero $e \ge 1$ tal que $p^e | m$ se cumple

$$p_i x \equiv p_i x' \mod p^e.$$

Como m.c.d.$(p_1, \ldots, p_r, m) = 1$, tenemos que existe i_0 tal que $p \nmid p_{i_0}$. Entonces de la congruencia anterior aplicada a $i = i_0$ deducimos

$$x \equiv x' \mod p^e.$$

Como p^e es arbitrario entre las potencias de primo que dividen m, concluimos que $x \equiv x'$ mód m. □

Lema 3.3. *Si a, a', b, b' cumplen (3.7), entonces existe un entero B satisfaciendo las congruencias (3.9). Más aún, B es único módulo $2aa'$.*

Demostración: Primero afirmamos que las congruencias (3.9) son equivalentes a

$$a'B \equiv a'b \mod 2aa'$$
$$aB \equiv ab' \mod 2aa'$$
$$\left(\frac{b+b'}{2}\right) B \equiv \left(\frac{bb'+D}{2}\right) \mod 2aa'$$

Suponiendo la afirmación cierta, se concluye aplicando el Lema 3.2 con $m = 2aa', p_1 = a', p_2 = a, p_3 = \frac{b+b'}{2}, q_1 = a'b, q_2 = ab', q_3 = \frac{bb'+D}{2}$ y usando la hipótesis (3.7).

Justifiquemos la afirmación. Si B satisface (3.9), entonces multiplicando la primera congruencia por a' y la segunda por a obtenemos las primeras dos congruencias en la afirmación. Para obtener la tercera, notar que

$$B^2 - (b+b')B + bb' = (B-b)(B-b') \equiv 0 \mod 4aa'.$$

Dividiendo por 2 obtenemos

$$\frac{b+b'}{2} B = \frac{B^2 + bb'}{2} \mod 2aa'.$$

Usando que $B^2 \equiv D \mod 2aa'$, concluimos que B satisface la tercera congruencia en la afirmación. Este razonamiento es claramente reversible. □

3.2. Complementos sobre representaciones de enteros.

Lema 3.4. *Una forma cuadrática $f(x, y) \in \mathbb{Z}[x, y]$ representa propiamente a $m \in \mathbb{Z}$ si y solo si existen $B, C \in \mathbb{Z}$ tales que f es equivalente a*

$$mx^2 + Bxy + Cy^2.$$

Demostración: La afirmación recíproca es clara, tomando $(x, y) = (1, 0)$. Para demostrar la afirmación que va en el sentido de la lectura, escribimos $m = f(u, v)$ con m.c.d.$(u, v) = 1$. Elegimos $\alpha, \beta \in \mathbb{Z}$ con $u\alpha - v\beta = 1$. Sea $\gamma = \begin{pmatrix} u & \beta \\ v & \alpha \end{pmatrix}$. Entonces

$$\gamma \cdot f(x, y) = f(ux + \beta y, vx + \alpha y) = f(u, v)x^2 + Bxy + Cy^2,$$

donde B, C son enteros apropiados. Como $m = f(u, v)$, esto demuestra el enunciado. □

Lema 3.5. *Sea $f(x, y) \in \mathbb{Z}[x, y]$ una forma primitiva. Para cualquier $k \in \mathbb{Z}$, con $k \neq 0$, existe $m \in \mathbb{Z}$, propiamente representado por f, tal que m.c.d.$(m, k) = 1$.*

Demostración: escribimos $f(x, y) = ax^2 + bxy + cy^2$.

Caso 1: $|k| = 1$. Tenemos que $m := f(1, 0)$ es propiamente representado y m.c.d.$(m, \pm 1) = 1$.

Caso 2: k es primo. Notar que los enteros $a, a+b+c, c$ son todos primitivamente representados por f, pues $a = f(1, 0), a + b + c = f(1, 1), c = f(0, 1)$. Para concluir la demostración, bastará mostrar que al menos uno ellos no es divisible por k.

Supongamos que son todos divisibles por k. Entonces

$$k | (a + b + c) - a - c = b,$$

lo que no es posible al ser f una forma primitiva. Contradicción.

Caso 3: $|k| \geq 2$. Sea $\{p_1, p_2, \ldots, p_r\}$ el conjunto de divisores primos de k. Por el caso anterior, tenemos que para todo $i = 1, 2, \ldots, r$, existen $u_i, v_i \in \mathbb{Z}$ con m.c.d.$(u_i, v_i) = 1$ y $p_i \nmid f(u_i, v_i)$. Por el teorema chino del resto, existen $u_0, v_0 \in \mathbb{Z}$ con

$$u_0 \equiv u_i \mod p_i, \quad v_0 \equiv v_i \mod p_i, \text{ para todo } i = 1, 2, \ldots, r.$$

Sea $m_0 := f(u_0, v_0)$. Como $m_0 \equiv f(u_i, v_i) \neq 0 \mod p_i$ para todo $i = 1, \ldots, r$, tenemos que m.c.d.$(m_0, k) = 1$. Sea $d :=$m.c.d.(u_0, v_0). Entonces $m := m_0/d^2$ es un entero coprimo con k y $m = f(u_0/d, v_0/d)$ es propiamente representado por f. □

3.3. Composición de Dirichlet en clases.

Lema 3.6. *Sean f, g formas cuadráticas primitivas de discriminante D.*

i) *Existen*

$$\alpha_1(x,y;z,w) = a_1xz + b_1xw + c_1yz + d_1yw \in \mathbb{Z}[x,y,z,w]$$
$$\alpha_2(x,y;z,w) = a_2xz + b_2xw + c_2yz + d_2yw \in \mathbb{Z}[x,y,z,w]$$

tales que

$$f(x,y)\cdot g(z,w) = f * g\left(\alpha_1(x,y;z,w), \alpha_2(x,y;z,w)\right).$$

ii) *Si escribimos $f = ax^2 + bxy + cy^2$, entonces existen a', b', c' tales que g es equivalente a $a'x^2 + b'xy + c'y^2$ y además a, a', b, b' cumplen (3.7)*

iii) *Asumiendo que f, g cumplen (3.7), se tiene que $f * g$ es una forma cuadrática primitiva de discriminante D*

Demostración: i). De la primera de las congruencias (3.9), tenemos que existe $m \in \mathbb{Z}$ con $B = b + 2am$. Definiendo $T_1 := \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, tenemos que

$$T_1 \cdot f(x,y) = ax^2 + Bxy + a'Cy^2, \quad C = \frac{B^2 - D}{4aa'}.$$

Similarmente, podemos establecer que existe $T_2 \in SL_2(\mathbb{Z})$ tal que

$$T_2 \cdot g(x,y) = a'x^2 + Bxy + aCy^2.$$

Por otro lado, tenemos la identidad

$$(ax^2 + Bxy + a'Cy^2)(a'z^2 + Bzw + aCw^2) = aa'X^2 + BXY + CY^2$$
$$X = xz - Cyw, \quad Y = axw + a'yz + Byw.$$

Sean $\beta_1(x,y;z,w) = xz - Cyw, \quad \beta_2(x,y;z,w) = axw + a'yz + Byw$. La identidad anterior se puede escribir

$$\big(T_1 \cdot f(x,y)\big)\big(T_2 \cdot g(w,z)\big) = f * g\left(\beta_1(x,y;z,w), \beta_2(x,y;z,w)\right).$$

Definiendo

$$\alpha_1(x,y;z,w) := \beta_1((x,y)\cdot T_1^{-t}; z, w), \quad \alpha_2(x,y;z,w) := \beta_2(x,y;(z,w)\cdot T_2^{-t}),$$

obtenemos la identidad pedida.

ii). Del Lema 3.5 vemos que existe $a' \in \mathbb{Z}$ con m.c.d.$(a,a') = 1$ tal que a' es propiamente representado por g. Usando el Lema 3.4, vemos que existen $b', c' \in \mathbb{Z}$ tales que g es equivalente a $a'x^2 + b'xy + c'y^2$. Como

$$\text{m.c.d.}\left(a, a', \frac{b+b'}{2}\right) | \text{m.c.d.}(a,a') = 1,$$

vemos que (3.7) se cumple.

iii). Es sencillo ver que $f * g$ tiene discriminante D (sin importar la elección de B). Verificaremos que es primitiva. Razonando por contradicción, suponemos que existe un primo p que divide a todos los coeficientes de $f * g$. Entonces, p divide a todos los enteros representados por $f * g$. De la parte i), deducimos que p divide a todos los productos de la forma $f(u,v)g(s,t)$ con $u, v, s, t \in \mathbb{Z}$. Sin embargo, esto contradice el Lema 3.5 aplicado sucesivamente a f y a g con $k = p$. □

3.4. Demostración del Teorema 3.1.

Sea

$$I(x,y) = \begin{cases} x^2 - \frac{D}{4}y^2 & \text{si } D \equiv 0 \mod 4 \\ x^2 + xy + \frac{1-D}{4}y^2 & \text{si } D \equiv 1 \mod 4. \end{cases}$$

Claramente $I(x,y)$ es primitiva y de discriminante D. Verifiquemos que su clase es el elemento neutro. Sea $f(x,y) = ax^2 + bxy + cy^2 \in C(D)$. Claramente la hipótesis (3.7) se cumple con respecto a los coeficientes de I y f. Afirmamos que puede tomarse $B = b$ para formar $f * I$. En efecto, aquí $a' = 1, b' \in \{0,1\}$ y las congruencias (3.9) toman la forma

$$b \equiv b' \mod 2 \tag{3.10}$$
$$b^2 \equiv D \mod 4a. \tag{3.11}$$

La congruencia (3.11) es obvia de la definición de discriminante. Si $D \equiv 0 \mod 4$, entonces b es par y $b' = 0$, luego se cumple (3.10). Si $D \equiv 1 \mod 4$, entonces b es impar y $b' = 1$, luego en este caso también se cumple (3.10).

Tomando $B = b$, la definición de la ley de composición implica

$$f * I(x,y) = ax^2 + bxy + \underbrace{\frac{b^2 - D}{4a}}_{c} y^2 = f(x,y),$$

como se quería.

Sea $\tilde{f}(x) = ax^2 - bxy + cy^2$. Debemos verificar que $[f] * [\tilde{f}] = [I]$. Notar que el par $f, \tilde{f}$ no necesariamente cumple la hipótesis (3.7). Por tal razón, reemplazamos $\tilde{f}$ por la forma equivalente

$$g(x,y) := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \tilde{f}(x,y) = cx^2 + bxy + ay^2.$$

El par f, g cumple con la hipótesis (3.7). Al igual que antes, es sencillo verificar que podemos tomar $B = b$ para calcular $f * g$. Encontramos que

$$f * g(x,y) = acx^2 + bxy + y^2.$$

Para justificar que esta forma es equivalente a I, tomamos un entero s arbitrario y consideramos $\gamma_s := \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix} \in SL_2(\mathbb{Z})$. Luego

$$\gamma_s \cdot f * g(x,y) = x^2 + (2s - b)xy + (ac - bs + s^2)y^2.$$

Si $D \equiv 0 \mod 4$, entonces b es par, luego podemos tomar $s := \frac{b}{2}$ y encontramos que $\gamma_{b/2} \cdot f * g(x,y) = I(x,y)$.

Si $D \equiv 1 \mod 4$, entonces b es impar, luego podemos tomar $s := \frac{b+1}{2}$ y encontramos que $\gamma_{(b+1)/2} \cdot f * g(x,y) = I(x,y)$, como se quería.

3.5. Elementos de orden 2 en $C(D)$.

Proposición 3.7. *La clase en $C(D)$ de una forma primitiva y reducida $f(x,y) = ax^2+bxy+cy^2$ tiene orden ≤ 2 si y solo si $b = 0$ o $a = b$ o $a = c$.*

Demostración: La clase de f tiene orden ≤ 2 si y solo si $[f] = [f]^{-1}$. Del Teorema 3.1 vemos que esto ocurre si y solo si f es equivalente a $g(x,y) = ax^2 - bxy + cy^2$.

Caso 1: $|b| < a < c$. En este caso, g es reducida, luego de la Proposición 2.4, vemos que $f = g$, con lo cual $b = 0$.

Caso 2: $a = b$ o $a = c$. Si $a = b$, vemos que $g_T(x,y) = f(x,y)$. Similarmente, si $a = c$, es sencillo ver que $g_S(x,y) = f(x,y)$. □

Ejemplo 3.8. Del ejemplo (5) de la Sección 2.2 tenemos que

$$C(-56) = \{[x^2 + 14y^2], [2x^2 + 7y^2], [3x^2 - 2xy + 5y^2], [3x^2 + 2xy + 5y^2]\}$$

es un grupo de 4 elementos, luego es $\mathbb{Z}/4\mathbb{Z}$ o $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Del Teorema 3.1 vemos que el elemento neutro es $[x^2 + 14y^2]$ y de la Proposición 3.7 vemos que el único elemento de orden 2 es $[2x^2 + 7y^2]$. Concluimos que $C(-56) \simeq \mathbb{Z}/4\mathbb{Z}$.

4. Número de clases

Denotaremos $h(D)$ al número de elementos de $C(D)$. Al entero $h(D)$ se le llama *número de clases*.

Un Teorema de Siegel asegura que para todo $\varepsilon > 0$, existe $C_\varepsilon > 0$ tal que $h(D) > C_\varepsilon |D|^{\frac{1}{2}-\varepsilon}$. En particular, $h(D)$ tiende a infinito cuando $|D|$ crece.

Se cree que la situación para $D > 0$ es radicalmente distinta. Se conjetura que existe $A \geq 1$ tal que el número de elementos del correspondiente $C(D)$ es $\leq A$ para infinitos valores de D.

Es posible clasificar todos los discriminantes $D < 0$ con $h(D) = 1$.

Teorema 4.1. *(Baker, Heegner, Stark) Suponemos $D < 0$ y $D \equiv 0$ o $1 \mod 4$. Entonces $h(D) = 1$ si y solo si*

$$D \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

La demostración de este Teorema requiere toda la teoría CM que desarrollaremos durante el seminario. Por ahora demostraremos este Teorema bajo la hipótesis extra $D \equiv 0 \mod 4$.

Teorema 4.2. *(Landau) Sea n un entero positivo. Entonces $h(-4n) = 1$ si y solo si $n \in \{1, 2, 3, 4, 7\}$.*

Demostración: La forma x^2+ny^2 tiene discriminante $-4n$ y es reducida. La implicancia recíproca se demuestra verificando que es la única, usando la Proposición 2.2. Demostremos la implicancia directa.

Caso 1: n no es una potencia de un primo.

En este caso escribimos $n = ac$, con $a, c \geq 2, a < c$ y m.c.d.$(a, c) = 1$. Entonces $ax^2 + cy^2$ tiene discriminante $-4n$ y es reducida, luego $h(-4n) \geq 2$.

Caso 2: $n = 8$. Del ejemplo (3) de la sección 2.2 vemos que $h(-32) = 2$

Caso 3: $n = 2^r$ con $r \geq 4$.

La forma $4x^2 + 4xy + (2^{r-2} + 1)y^2$ es primitiva, tiene discriminante $4^2 - 4 \cdot 4 \cdot (2^{r-2} + 1) = -4 \cdot 2^r = -4n$ y además es reducida, pues $4 < 2^{r-2}+1$. Al ser distinta de $x^2+2^r y^2$, esto muestra que $h(-4n) \geq 2$ en este caso.

Caso 4: $n = p^r$ con p un primo impar y $n + 1$ no es potencia de primo.

En este caso escribimos $n+1 = ac$ con $2 \leq a < c$ y m.c.d.$(a, c) = 1$. Entonces $ax^2+2xy+cy^2$ es reducida, primitiva y de discriminante $4 - 4ac = 4 - 4(n + 1) = -4n$. Al ser distinta de $x^2 + ny^2$, vemos que $h(-4n) \geq 2$ en este caso.

Caso 5: $n = p^r$ con p un primo impar y $n + 1 = 2^s$ con $s \geq 1$.

Si $s \geq 6$, entonces

$$8x^2 + 6xy + (2^{s-3} + 1)y^2$$

es primitiva, reducida (pues $8 < 2^{s-3} + 1$) y de discriminante

$$6^2 - 4 \cdot 8(2^{s-3} + 1) = 36 - 4(n + 1 + 8) = -4n,$$

luego $h(-4n) \geq 2$.

Si $s = 5$, vemos que $h(-4 \cdot 31) = 3$ por el ejemplo (4) de la sección 2.2.

Si $s = 4$, entonces $n = 15$ no es potencia de primo.

Si $s \in \{1, 2, 3\}$, entonces $n \in \{1, 3, 7\}$ es un caso ya cubierto. □

Referencias

[Cox13] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication. 1

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991. 2

E-mail address: rmenares@mat.uc.cl