Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Composición de Formas Binarias Cuadráticas. Cubos de Bhargava

Trabajo de fin de grado

Grado en Matemáticas

Autor: Gonzalo González-Fierro López
Tutor: Enrique González Jiménez

Curso 2022-2023

Resumen

Las formas binarias cuadráticas son polinomios homogéneos de grado dos de dos variables con coeficientes enteros que llevan siendo objeto de estudio desde hace siglos. Muchos de los matemáticos con más renombre de la historia, como Legendre o Gauss, entre otros, han estudiado y desarrollado una amplía teoría sobre estas ecuaciones.

Una de las partes más interesantes e importantes de la teoría sobre formas binarias cuadráticas es que existe una relación de equivalencia y una compleja operación que otorgan a estos polinomios una estructura de grupo. El primero en conseguir demostrar esto fue Carl Friedrich Gauss.

Esta operación, que Gauss bautizó como composición directa de formas binarias cuadráticas, es trabajosa de operar. Por ello, han sido varios los matemáticos que han intentado obtener una manera de entender y realizar esta operación de forma más sencilla. Entre ellos, Dirichlet fue capaz de dar con una expresión más explícita del resultado de la composición..

En 2001, el matemático canadiense Manjul Bhargava publicó su tesis doctoral, titulada *Higher Composition Laws*. En su tesis, presentaba una forma mucho más visual de entender la composición directa de formas binarias cuadráticas a partir de unos cubos con coeficientes en cada vértice, llamados cubos de Bhargava. Además, este concepto es generalizable a dimensiones superiores, de ahí el título de su tesis.

Abstract

Binary quadratic forms are homogeneous polynomials of degree two of two variables with integer coefficients that have been a main subject of study for centuries. Many of the most renowned mathematicians in history, such as Legendre or Gauss, among others, have studied and developed an extensive theory about these equations.

One of the most interesting and important parts of this theory about binary quadratic forms is that there is an equivalence relation and a complex operation that give these polynomials a group structure. The first to succeed in proving this was Carl Friedrich Gauss.

This operation, which Gauss called direct composition of binary quadratic forms, is laborious to operate. Therefore, there have been several mathematicians who have tried to obtain a way to understand and solve this operation in a simpler way. Among them, Dirichlet was able to come up with an explicit expression of the result of the composition.

In 2001, Canadian mathematician Manjul Bhargava published his PhD thesis, entitled *Higher Composition Laws*. In his thesis, he presented a much more visual way of understanding the direct composition of binary quadratic forms from cubes with coefficients at each vertex, called Bhargava cubes. Moreover, this concept is generalizable to higher dimensions, hence the title of his thesis.

Índice general

Introducción

Las formas binarias cuadráticas son una de las áreas de la teoría de números más estudiadas a lo largo de la historia. Sus numerosas e importantes propiedades y aplicaciones le han dotado de un lugar especial dentro del campo de las matemáticas.

En el primer capítulo, nos centraremos en introducir algunas nociones básicas sobre formas binarias cuadráticas. Estas son polinomios homogéneos de grado dos con coeficientes enteros, de la forma

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

Cada forma binaria cuadrática tiene asociado un concepto fundamental, el discriminante,

$$D = b^2 - 4ac.$$

El grupo lineal especial de dimensión 2, $SL_2(\mathbb{Z})$, actúa sobre el conjunto de formas binarias cuadráticas de discriminante D mediante un cambio de variable. Además, esta acción de grupo induce una relación de equivalencia, y denotaremos por G_D a este conjunto bajo dicha relación.

De todas las formas binarias cuadráticas, nos centraremos en aquellas con discriminante negativo, primitivas y definidas positivas, es decir, con coeficientes coprimos y que representan solo números no negativos. De estas formas, existe un tipo especial de ellas, llamadas formas reducidas, que son aquellas que verifican:

$$|b| \leq a \leq c, \quad \text{y} \quad 0 \leq b \quad \text{siempre que} \quad a = |b| \quad \text{o} \quad a = c.$$

Lo que hace importante a las formas reducidas es que en cada clase de equivalencia de G_D existe una única de ellas, y que en G_D el número de formas reducidas es finito. Es decir, el número de clases de equivalencia de G_D es finito.

En el segundo capítulo nos centraremos en la composición de formas, primero desde una perspectiva histórica y finalmente demostrando que esta operación induce en G_D una estructura de grupo.

La existencia de una operación entre las clases de equivalencia de formas binarias cuadráticas, llamada composición directa, es uno de los resultados más interesantes sobre estas. Desde hace siglos, varios matemáticos como Diofanto o Brahmagupta han logrado dar con precedentes de esta identidad, algo menos generales. Legendre, estudiando el trabajo de Fermat y Lagrange, logró finalmente dar con una "composición" general, pero que no estaba del todo bien definida.

Fue Gauss quien, en *Disquisitiones Arithmeticae* [8], consiguió definir correctamente la composición. Además, en una época en la que el concepto de grupo ni siquiera existía aún, logró demostrar que esta operación otorgaba a G_D todas las propiedades de un grupo abeliano finito. La composición es trabajosa tanto de entender como de operar, y por ello, muchos matemáticos a lo largo de la historia han intentado simplificar este concepto.

Entre ellos, Dirichlet logró dar una expresión explícita de la composición de dos formas de un tipo especial, llamadas formas reunidas, y demostró que para cualquier par de clases de equivalencia existe una pareja de representantes reunidos. Aún así, esta expresión explícita aún dependía, no solo de encontrar una pareja de representantes reunidos, si no también de un coeficiente que resulta de resolver un sistema de tres congruencias.

En el tercer y último capítulo, estudiaremos los Cubos de Bhargava, uno de los últimos y más fructíferos progresos en el campo de las formas binarias cuadráticas. Dos siglos después de que Gauss definiese su composición, el matemático canadiense Manjul Bhargava dio con un concepto nuevo que revolucionó el área de la teoría de números. Él, en su tesis doctoral, introduce una nueva forma de visualizar esta operación a partir de cubos con coeficientes en cada uno de sus vértices, nombrados en su honor Cubos de Bhargava. Cada cubo C se puede cortar de tres formas distintas, con los llamados cortes fundamentales, dando lugar a tres formas binarias cuadráticas, Q_1^C, Q_2^C y Q_3^C. A aquellos cuyas formas asociadas sean primitivas, los llamaremos cubos proyectivos. Imponiendo sobre las clases de equivalencia de estas formas la Ley de Cubos,

$$[Q_1^C] \circ [Q_2^C] \circ [Q_3^C] = [Q_{id,D}],$$

donde $[Q_{id,D}]$ es la clase identidad de las formas binarias cuadráticas y $\circ$ denota la composición de formas, Bhargava logra probar que este axioma es equivalente a la composición de Dirichlet, y por tanto, a la de Gauss. Una consecuencia de esto es que las clases de equivalencia de cubos de enteros también forman un grupo. Pero, además de esto, el concepto de Cubos de Bhargava es generalizable a dimensiones superiores. Todo ello hizo del descubrimiento del canadiense un hito en el campo de la teoría de números.

CAPÍTULO 1
Formas binarias cuadráticas

Para poder entrar en materia sobre la composición directa de formas binarias cuadráticas, serán necesarias algunas nociones básicas.

Introduciremos los conceptos de discriminante y equivalencia de formas, que serán fundamentales para poder probar que las formas tienen estructura de grupo. Por último, definiremos la noción de formas reducidas y demostraremos la existencia y unicidad de estas en cada clase de equivalencia.

1.1. Nociones básicas

Definición 1.1. Una forma binaria cuadrática es un polinomio homogéneo de dos variables de grado dos de la forma

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

donde $a, b, c \in \mathbb{Z}$.

Una forma $ax^2 + bxy + cy^2$ se suele denotar generalmente como (a, b, c) ya que estos enteros determinan completamente la ecuación. Además, decimos que la forma binaria cuadrática es *primitiva* si a, b y c son coprimos, y que es *definida positiva* si $f(x, y) > 0$ para todo $x, y \neq 0$.

Definición 1.2. El discriminante de una forma binaria cuadrática (a, b, c) se define como $\text{Disc}((a, b, c)) = b^2 - 4ac$.

Se dice que un entero m está *propiamente representado* por una forma binaria cuadrática $f(x, y)$ si existen $p, q \in \mathbb{Z}$ coprimos tales que $f(p, q) = m$. Cuando p y q no son coprimos, decimos simplemente que m está representado por la forma $f(x, y)$.

Proposición 1.3. *La forma binaria cuadrática* (a, b, c) *es definida positiva si y solo si* $\text{Disc}((a, b, c)) < 0$ *y* $a > 0$.

Demostración. Si $f(x,y) = (a,b,c)$ y $D = \text{Disc}(f(x,y))$, entonces

$$4af(x,y) = (2ax+by)^2 - Dy^2,$$
$$f(x,y) = \frac{1}{4a}[(2ax+by)^2 - Dy^2].$$

Por lo tanto $f(x,y) > 0$ para todo $x, y \neq 0$ solamente si $a > 0$ y $D < 0$. □

De la proposición anterior, podemos concluir procediendo de la misma forma que si $a < 0$ y $D < 0$, entonces $f(x,y) < 0$ si $x, y \neq 0$ (es decir, la forma binaria cuadrática es *definida negativa*), y que si $D > 0$, no podemos asegurar nada sobre la positividad o negatividad de $f(x,y)$.

Nota 1. *En lo que resta, llamaremos simplemente formas a las formas binarias cuadráticas primitivas y definidas positivas, salvo que se indique algo distinto.*

Se puede definir la acción del grupo lineal especial

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}, ad - bc = 1 \right\}$$

sobre una forma como

$$(a,b,c) * \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2, \tag{1.1}$$

donde $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ cumplen $\alpha\delta - \beta\gamma = 1$.

Otra forma de ver está acción de grupo es como un cambio de variable. Si $f(x,y)$ es una forma y $M \in SL_2(\mathbb{Z})$, entonces $f(x,y) * M = f(x',y')$ con $(x',y')^t = M(x,y)^t$.

Esta operación es, efectivamente, una acción de grupo. Dadas $f(x,y)$ una forma, $M, N \in SL_2(\mathbb{Z})$ dos matrices y la matriz identidad $I \in SL_2(\mathbb{Z})$:

1. Se verifica inmediatamente que $f(x,y) * I = f(x,y)$ por (1.1).
2. $(f(x,y)*N)*M = f(x',y')$ con $(x',y')^t = MN(x,y)^t$, y $f(x,y)*MN = f(x',y')$.

Proposición 1.4. *Para cualquier matriz $M \in SL_2(\mathbb{Z})$ y cualquier forma (a,b,c), se tiene* $\text{Disc}((a,b,c) * M) = \text{Disc}((a,b,c))$.

Demostración. Si $(a,b,c) = ax^2 + bxy + cy^2$ tiene discriminante D y

$$N = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix},$$

se cumple $ax^2 + bxy + cy^2 = (x,y)N(x,y)^t$. Además, $\det(N) = ac - \frac{b^2}{4} = \frac{-D}{4}$, o, lo que es lo mismo, $D = -4\det(N)$. Puesto que $f(x,y) * M = f(x',y')$ por el cambio $(x',y')^t = M(x,y)^t$, $f(x,y) * M = (x,y)M^tNM(x,y)^t$, entonces su discriminante es $-4\det(M^tNM) = -4\det(N) = D$, pues M tiene determinante 1, y por tanto M^t también. □

De esta demostración se puede deducir de manera análoga que si $\det(M) = -1$, entonces el discriminante también es invariante por equivalencia. Es más, también se deduce que para cualquier matriz M de dimensión dos, no necesariamente en $SL_2(\mathbb{Z})$, $\mathrm{Disc}((a,b,c) * M) = \det(M)^2 \,\mathrm{Disc}((a,b,c))$ para cualquier forma (a,b,c).

Puesto que por esta proposición el discriminante es invariante por la acción de grupo, es natural definir la *relación de equivalencia*

$$f(x,y) \sim g(x,y) \quad \text{si y solo si} \quad f(x,y) * M = g(x,y) \quad \text{para algún} \quad M \in SL_2(\mathbb{Z}),$$

con $f(x,y)$ y $g(x,y)$ dos formas de igual discriminante D. Se denota por

$$G_D = \{(a,b,c) : a,b,c \in \mathbb{Z}, Disc((a,b,c)) = D\}/\sim$$

el conjunto de clases de equivalencia de las formas de discriminante D y por $[(a,b,c)]$ (o, equivalentemente, $[f(x,y)]$) el representante en G_D de la clase (a,b,c) (o $f(x,y)$).

Falta comprobar que esta relación es, efectivamente, de equivalencia. Sean tres formas $f(x,y), g(x,y), h(x,y)$ de discriminante D, dos matrices $M, N \in SL_2(\mathbb{Z})$ e I la matriz identidad de $SL_2(\mathbb{Z})$:

1. $f(x,y) * I = f(x,y)$, luego $f(x,y) \sim f(x,y)$ (reflexividad).
2. Si $f(x,y) \sim g(x,y)$, $f(x,y) * M = f(x',y') = g(x,y)$, con $(x',y')^t = M(x,y)^t$, se tiene $(x,y)^t = M^{-1}(x',y')$ y $g(x,y) * M^{-1} = f(x,y)$, luego si $f(x,y) \sim g(x,y)$, entonces $g(x,y) \sim f(x,y)$ (simetría).
3. Si $f(x,y) \sim g(x,y)$ y $g(x,y) \sim h(x,y)$, entonces por equivalencia se tienen los cambios $f(x,y) * M = f(x',y') = g(x,y)$ y $g(x,y) * N = f(x',y') * N = f(x'',y'') = h(x,y)$, luego $f(x,y) * NM = h(x,y)$, con $NM \in SL_2(\mathbb{Z})$, y entonces $f(x,y) \sim h(x,y)$ (transitividad).

Pese a que Legendre definió la relación de equivalencia de manera general para matrices $M \in GL_2(\mathbb{Z})$, Gauss introdujo el concepto de equivalencia propia, que restringía está acción únicamente a matrices de determinante $+1$. A la equivalencia de formas por una matriz de determinante -1 se le llama, análogamente, equivalencia impropia. Más adelante, al introducir la composición de formas, veremos la vital utilidad de esta distinción.

Una de las propiedades invariantes por equivalencia de formas más importantes es la representación de enteros:

Proposición 1.5. *Dos formas equivalentes representan los mismos enteros.*

Demostración. Sean $f(x,y)$ y $g(x,y)$ dos formas equivalentes de igual discriminante. Entonces, se tiene $f(x,y) = g(ax+by, cx+dy)$ para $a,b,c,d \in \mathbb{Z}$ tales que $ad-bc = 1$. Luego, para cualquier $m \in \mathbb{Z}$ tal que $f(r,s) = m$ para $r,s \in \mathbb{Z}$, entonces $g(ar+bs, cr+ds) = m$. Como además, $g(x,y) = f(a'x+b'y, c'x+d'y)$ por simetría de la relación de equivalencia para otros cuatro enteros a', b', c' y d', los números representados por $g(x,y)$ también son representados por $f(x,y)$ por el mismo razonamiento. □

Proposición 1.6. *Si una forma binaria cuadrática es equivalente a otra forma binaria cuadrática primitiva, la primera es también primitiva.*

Demostración. Sea una forma binaria cuadrática $f(x,y)$ equivalente a otra forma primitiva $g(x,y)$. Entonces, existe $M \in SL_2(\mathbb{Z})$ tal que

$$f(x,y) * M = g(x,y) = ax^2 + bxy + cy^2, \quad \text{con} \quad \text{mcd}(a,b,c) = 1.$$

Sea el conjunto $A = \{n : n = f(x,y), x, y \in \mathbb{Z}\}$ de los números representados por $f(x,y)$. Si $f(x,y)$ no fuese primitiva entonces existe $N \in \mathbb{Z}_{>1}$ tal que para todo $n \in A, n = kN, k \in \mathbb{Z}$. De hecho, se tiene que N es el máximo común divisor de los coeficientes de la forma $f(x,y)$. Sin embargo, como $g(x,y)$ es equivalente a $f(x,y)$, entonces representan a los mismos enteros, y como $g(x,y)$ es primitiva, $N = 1$. Es decir, si una forma binaria cuadrática es primitiva, también lo son todas las que sean equivalentes a ella, pues representan los mismos enteros. □

1.2. Formas reducidas

Definición 1.7. Decimos que una forma (a,b,c) es reducida si cumple

$$|b| \leq a \leq c, \quad \text{y} \quad 0 \leq b \quad \text{siempre que} \quad a = |b| \quad \text{o} \quad a = c. \tag{1.2}$$

Teorema 1.8. *En cada clase de equivalencia de G_D hay una única forma binaria cuadrática reducida.*

Demostración. Veremos primero que toda forma es equivalente a una forma reducida. Se toma un representante $f(x,y) = ax^2 + bxy + cy^2$ de una clase de equivalencia cualquiera de G_D. Consideremos las matrices

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

para algún $n \in \mathbb{Z}$. La matriz S lleva una forma (a_1, b_1, c_1) a $(c_1, -b_1, a_1)$, y T^n lleva (a_1, b_1, c_1) a $(a, 2an + b, an^2 + bn + c)$.

Si $a < |b|$, entonces existe $m \in \mathbb{Z}$ tal que

$$g(x,y) = f(x,y) * T^m = ax^2 + b'xy + c'y^2,$$

con $b' = 2am + b$ y $c' = am^2 + bm + c$. Así, se consigue $|b'| \leq a$ y $|b'| \leq c$. Si se tiene $c' \leq a$, con un último cambio

$$h(x,y) = g(x,y) * S = c'x^2 - b'x^2 + ay^2$$

concluimos que todas las formas son propiamente equivalentes a una con $|b| \leq a \leq c$. Esto es lo mismo que $-a \leq b \leq a \leq c$. Por lo tanto, la forma ya es reducida, salvo que $b < 0$ y $b = -a$ o $a = c$.

En el primer caso, vemos que $f(x,y) = ax^2 - axy + cy^2$ es propiamente equivalente a (a,a,c) a través del cambio dado por la matriz T, y en el segundo caso, se tiene que $h(x,y) = ax^2 + bxy + ay^2$ es propiamente equivalente a $(a,-b,a)$ a través del cambio dado por la matriz S. Como ambas formas son reducidas, hemos terminado.

Una vez probada la existencia, veamos la unicidad de las formas reducidas. Para ello, consideremos una forma reducida $f(x,y) = ax^2 + bxy + cy^2$. Es decir, se tiene que $|b| \leq a \leq c$. De esto, se puede deducir que $f(x,y) \geq (a - |b| + c)m$, donde $m = \text{mín}(x^2, y^2)$. Para ello, supongamos que $x \leq y$, entonces $x^2 \geq xy \geq -y^2$ y $x^2 \geq y^2$, y por tanto

$$f(x,y) = ax^2 + bxy + cy^2 \geq (a+c)y^2 + bxy \geq (a+c)y^2 - by^2 \geq (a - |b| + c)m,$$

donde en la última desigualdad hemos usado que $-b \geq -|b|$. Si $y \geq x$, se procede de la misma forma. Por tanto, siempre que $x, y \neq 0$, se tiene $f(x,y) \geq a - |b| + c$.

Por lo tanto, el menor valor que puede tomar una forma cuando $x, y \neq 0$ es $a - |b| + c$. Por supuesto, el menor valor representado por $f(x,y)$ es 0, en $x = y = 0$. Si suponemos que $x = k \geq 0$ e $y = 0$, entonces $f(k,0) = ak^2 \geq a$. Del mismo modo, $f(0,k) = ck^2 \geq c$, por lo que, si la forma es reducida, entonces $a < c$ y a es el menor valor distinto de 0 representado propiamente por $f(x,y)$ y c el segundo menor. Como $\text{mcd}(n,0) = n$ para $n \in \mathbb{Z}_{>1}$, aunque $f(k,0) \leq f(0,1)$, no estaríamos hablando de representación propia. Además, si $|b| < a < c$, entonces $a - |b| + c > a$ es por tanto el tercer menor valor distinto de 0 representado propiamente por $f(x,y)$. Estas observaciones fueron dadas por Legendre en [11].

Veamos además que, si se cumple estrictamente la desigualdad $|b| < a < c$, tenemos

$$\begin{aligned} a = f(x,y),\ \text{mcd}(x,y) &= 1 \iff (x,y) = (\pm 1, 0), \\ c = f(x,y),\ \text{mcd}(x,y) &= 1 \iff (x,y) = (0, \pm 1). \end{aligned} \tag{1.3}$$

Por simetría, probaremos solo el primer caso. La condición necesaria es inmediata.

Supongamos ahora que se cumple estrictamente la desigualdad $|b| < a < c$ y que existe una pareja de enteros coprimos $(x,y) \neq (\pm 1, 0)$ tal que $f(x,y) = a$. Si $y = 0$, entonces $f(x,0) = ax^2 = a$ si y solo si $x = \pm 1$. Ahora bien, si $x = 0$, entonces $f(0,y) = cy^2 = a$ si $c \leq a$, con lo cual tampoco es posible este caso, luego $xy \neq 0$. Por la observación anterior sobre los menores números representados propiamente por f, se tiene entonces que $a = f(x,y) \geq a - |b| + c > a$, lo cual es una contradicción, lo que concluye esta parte de la demostración.

De forma análoga, si se tuviese $a = c$, entonces $f(x,y) = a = c$ con $\text{mcd}(x,y) = 1$ si y solo si $(x,y) = (\pm 1, 0)$ o $(x,y) = (0, \pm 1)$.

Sea ahora otra forma reducida $g(x,y)$ equivalente a $f(x,y)$. Como representan los mismos enteros al ser equivalentes, deben tener el mismo primer coeficiente a, pues si es el menor número representado propiamente por $f(x,y)$, también lo es de $g(x,y)$. Si c' es el tercer coeficiente de $g(x,y)$, $a \leq c'$ por ser $g(x,y)$ reducida. Si se tuviese $a = c'$, entonces estos tendrían cuatro representaciones propias $(\pm 1, 0)$ y $(0, \pm 1)$, lo que sería una contradicción con (1.3) ya que $f(x,y)$ y $g(x,y)$ representan los mismos enteros. Por lo tanto, se tiene $a < c'$ y entonces el segundo menor número

representado por $g(x,y)$ es c' por la observación de Legendre, y por tanto $c = c'$, otra vez por representar $f(x,y)$ y $g(x,y)$ los mismos enteros. Por tener $g(x,y)$ el mismo discriminante que $f(x,y)$, se ha de tener que el segundo coeficiente de $g(x,y)$, $b' = \pm b$.

Terminamos probando que $b = b'$. Como $f(x,y)$ es propiamente equivalente a $g(x,y)$, supongamos que por el cambio de variable dado por la matriz

$$M = \begin{pmatrix} p & q \\ r & s \end{pmatrix},$$

entonces $g(x,y) = f(px+qy, rx+sy)$. Luego, se tiene que $a = g(1,0) = f(p,r)$ y $c = g(0,1) = f(q,s)$. Una vez más, a consecuencia de (1.3), $(p,r) = (\pm 1, 0)$ y $(q,s) = (0, \pm 1)$ y como la matriz M tiene determinante 1, $ps - qr = 1$, y obtenemos inmediatamente que $M = \pm I$, siendo I la matriz identidad. Como ninguna de las dos posibilidades produce ningún cambio en las formas, concluimos que $f(x,y) = g(x,y)$.

Si $a = c$, ese es el mínimo valor que toma f, y lo hace en $(x,y) = (\pm 1, 0)$ o $(x,y) = (0, \pm 1)$. Como $f(x,y)$ y $g(x,y)$ representan a los mismos enteros, $a = a' = c = c'$ por el mismo razonamiento hecho antes, y por tener igual discriminante, $b' = \pm b$.

En el caso $|b| = a$, por el mismo argumento usado previamente, si $f(x,y) = a$ con $\mathrm{mcd}(x,y) = 1$ y $(x,y) \neq (\pm 1, 0)$, entonces $xy \neq 0$. De esta forma, llegaríamos a la contradicción $a = f(x,y) \geq a - |b| + c = c$, ya que $a \leq c$. Luego, el valor a se alcanza tan solo en $(x,y) = (\pm 1, 0)$. Así, por representar $g(x,y)$ y $f(x,y)$ los mismos enteros, entonces $a = a' = |b| = |b'|$, y entonces $c = c'$ por tener el mismo discriminante.

En ambos casos ($a = c$ y $|b| = a$) hemos llegado a que $g(x,y) = ax^2 \pm b + cy^2$, pero por la Definición 1.7, ha de darse $b \geq 0$ y, lógicamente, también $b' \geq 0$, con lo que se concluye que $b = b'$, y hemos probado la unicidad de las formas reducidas. □

Este teorema nos sirve como preludio para probar que el número de clases de equivalencia de formas de discriminante D, número al que denotaremos $h(D)$, es finito.

Teorema 1.9. *Sea $D < 0$ un entero. Entonces, el número de formas reducidas en G_D es finito y coincide con $h(D)$, que es por tanto finito.*

Demostración. Como ya hemos demostrado en el anterior teorema la existencia y unicidad de una forma reducida en cada clase de equivalencia de G_D, probar que el número de formas reducidas que existen en G_D es finito implica inmediatamente que el número de clases de equivalencia también lo es, ya que ambos coinciden.

Esto se puede demostrar a partir de la Definición 1.7, que implica ciertas condiciones a los coeficientes de una forma . Sea $f(x) = ax^2 + bxy + cy^2$ una forma reducida de discriminante $D < 0$, luego $b^2 \leq a^2$ y $a \leq c$. De este forma, $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$. Por tanto, $a \leq \sqrt{\frac{-D}{3}}$ y como $|b| \leq a$ por ser reducida, hay un número finito de elecciones para a y, por lo tanto, también para b. Además, como $D = b^2 - 4ac$, también hay un número finito de elecciones para c, con lo que concluímos que $h(D)$ es finito.

□

CAPÍTULO 2
La ley de composición

Una de las propiedades más importantes de las formas binarias cuadráticas es que pueden operarse entre ellas. Esta operación, llamada composición, fue bien definida por primera vez por Gauss.

Muchos siglos antes, matemáticos como Brahmagupta o Fibonacci ya habían dado con identidades similares a la composición de formas, pero menos generales. Casi un milenio después, en su estudio sobre la representación de primos, Lagrange dio con una identidad que se correspondia con la composición de una forma consigo misma. Fue Legendre el que se dio cuenta de que esa igualdad podía generalizarse y en su estudio obtuvo una composición que, aunque casi igual a la que hallaría Gauss poco más tarde, no estaba del todo bien definida; el resultado no siempre era único.

2.1. Introducción histórica

Gauss introduce en el quinto capítulo de su obra *Disquisitiones Arithmeticae* [8] una compleja operación entre formas que bautiza como ley de composición. Aunque no existía en la época de Gauss el concepto de grupo, él matemático alemán es capaz de probar que esta operación, junto al conjunto de clases de equivalencia de formas, cumplen todas las propiedades de un grupo abeliano finito.

Antes de Gauss, otros matemáticos ya habían estudiado identidades menos generales a la que más tarde introduciremos como composición de formas. El matemático griego del siglo III, Diofanto de Alejandría, conocido como el padre del Álgebra, en su estudio sobre los números que pueden escribirse como suma de dos cuadrados, escribío en el Libro III (Problema 19) de [6]:

El número 65 *se puede escribir como suma de dos cuadrados:* $16 + 49$ *y* $64 + 1$. *Esto se debe a que* $65 = 5 \cdot 13$*, y ambos son la suma de dos cuadrados.*

Esta observación deriva en la siguiente identidad de Fibonacci, encontrada en el problema 6 de [13]:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \quad \text{donde} \quad a, b, c, d \in \mathbb{Z}.$$

En el siglo VII, el matemático indio Brahmagupta, dio con otra identidad aún más general estudiando las soluciones enteras de la Ecuación de Pell, que en notación moderna se expresaría como

$$(a^2 - Nb^2)(c^2 - Nd^2) = (ac \pm Nbd)^2 - N(ad \pm bc)^2, \tag{2.1}$$

o como

$$(a^2 + Nb^2)(c^2 + Nd^2) = (ac \pm Nbd)^2 + N(ad \mp bc)^2,$$

para cualesquiera $a, b, c, d, N \in \mathbb{Z}$.

La demostración en ambos casos es inmediata expandiendo ambos lados de la ecuación. Podríamos decir que, por esta identidad, las formas binarias cuadráticas de la forma $x^2 + Dy^2$ son cerradas bajo la multiplicación.

Lógicamente, la cuestión ahora se torna en conseguir una generalización de esta identidad que sea válida para todas las formas binarias cuadráticas.

2.2. Legendre

Euler, en [7], estudiando el trabajo de Fermat de la representación de números primos, quería probar su conjetura de que cualquier producto de primos p y q de la forma $20n+3$ o $20n+7$, con n un entero, sería representado por la ecuación x^2+5y^2, donde $x, y \in \mathbb{Z}$. Es decir, que

$$p, q \equiv 3, 7 \pmod{20} \quad \text{si y solo si} \quad pq = x^2 + 5y^2.$$

Para ello, supuso que $2p = x^2 + 5y^2$ para p un primo tal que $p \equiv 3, 7 \pmod{20}$. Entonces, multiplicando $2p = x^2 + 5y^2$ por $2q = z^2 + 5w^2$, con $x, y, z, w \in \mathbb{Z}$ impares, se obtendría

$$4pq = (x^2 + 5y^2)(z^2 + 5w^2) = (xz - 5yw)^2 + 5(xw + yz)^2,$$

lo cual implica, al cancelar el 4, la conjetura de Fermat.

Lagrange logró por fin demostrar esta conjetura, probando que esos primos están representados por la forma $f(x, y) = 2x^2 + 2xy + 3y^2$, y viendo que se verifica:

$$(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2zx + xw + yz + 3yw)^2 + 5(xw - yz)^2 \tag{2.2}$$

donde $x, y, z, w \in \mathbb{Z}$.

Lagrange dio una prueba en [9] de una identidad aún más general con respecto al producto de dos tipos particuales de formas:

$$(ax_1^2 + bx_1y_1 + a'cy_1^2)(a'x_2^2 + bx_2y_2 + acy_2^3) = aa'x^2 + bxy + cy^2, \tag{2.3}$$

donde $a, a', b, c \in \mathbb{Z}$, $x = x_1x_2 - cy_1y_2$ e $y = ax_1y_2 + a'x_2y_1 + bx_2y_2$.

El matemático francés Adrien-Marie Legendre fue quien se dio cuenta de que algo más profundo explicaba la existencia de esta identidad. Observó que, dadas dos formas

binarias cuadráticas de discriminante $D < 0$, $f(x, y)$ y $g(z, w)$, entonces existe otra forma $F(x, y)$ de igual discriminante tal que

$$f(x,y)g(z,w) = F(B_1(x,y;z,w), B_2(x,y;z,w)), \tag{2.4}$$

donde $B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw$, $a_i, b_i, c_i, d_i \in \mathbb{Z}$, $i = 1, 2$.

Ahora, observando la identidad (2.2), podemos ver que la forma $x^2 + 5y^2$ es la "composición" de $2x^2 + 2xy + 3y^2$ consigo misma.

Además, muestra que los números representados por la composición de dos formas serán el producto de los números que representan estas dos y que dos formas con el mismo discriminante siempre pueden componerse.

Para simplificar, veamos el caso en el que ambas formas tienen segundo coeficiente par, $f(x, y) = ax^2 + 2bxy + cy^2$ y $g(x, y) = a'x^2 + 2b'xy + c'y^2$, ambas de discriminante $D = 4n, n \in \mathbb{Z}_{<0}$, y tal que $\text{mcd}(a, a') = 1$. Esta última condición se puede obtener siempre con equivalencia de formas. Entonces, por el teorema chino del resto, la ecuación

$$\begin{cases} B \equiv \pm b \pmod{a}, \\ B \equiv \pm b' \pmod{a'}, \end{cases} \tag{2.5}$$

admite solución para B. De esto se sigue fácilmente que

$$B^2 - n \equiv B^2 - b^2 + ac \equiv 0 \pmod{a}.$$

Es decir, a divide a $B^2 - n$. Lo mismo se cumple en módulo a', por lo que se tiene que aa' divide a $B^2 - n$.

Entonces, Legendre prueba que la composición de $f(x, y)$ y $g(x, y)$ es

$$F(U,V) = aa'U^2 + 2BUV + \frac{B^2 - n}{aa'}V^2. \tag{2.6}$$

Para llegar a esto, Legendre toma el cambio

$$Z = ax + by, \quad Z' = a'z + b'w$$

que, como $n = b^2 - ac$, resulta en

$$\begin{aligned} af(x,y) &= Z^2 - ny^2, \\ a'g(z,w) &= Z'^2 - nw^2. \end{aligned}$$

Así, aplicando la identidad (2.1), se tiene

$$f(x,y)g(z,w) = \frac{1}{aa'}[(ZZ' \pm nyw)^2 - n(Zw \pm yZ')^2].$$

La parte derecha de esta ecuación se puede escribir como

$$F(U,V) = aa'U^2 + 2BUV + \frac{B^2 - n}{aa'}V^2$$

haciendo

$$V = Zw \pm yZ', \quad aa'U + BV = ZZ' \pm nyw,$$

donde B se toma como en (2.5) para que todos los coeficientes de $F(U, V)$ sean enteros por lo que habíamos visto antes. Despejando, obtenemos además que

$$U = xz + myz + m'xw + lyw,$$

con

$$m = \frac{b \mp B}{a}, m' = \frac{b' - B}{a'} \quad \text{y} \quad l = mm' \mp \frac{B^2 - n}{aa'}.$$

Además, vemos que el discriminante de $F(U, V)$ es

$$(2B)^2 - 4aa'\frac{B^2 - n}{aa'} = 4B^2 - 4B^2 + 4n = 4n = D.$$

El problema con la composición de Legendre es que esta composición no es única. Los signos $\pm$ de la ecuación (2.5) provocan que dos formas puedan componerse, en general, de cuatro maneras distintas. Las formas $(14, 10, 21)$ y $(9, 2, 30)$ admiten cuatro composiciones distinas:

$$(126, \pm 38, 5) \quad \text{y} \quad (126, \pm 74, 13),$$

y cada una de ellas cae en una clases de equivalencia distinta.

Sin embargo, como Legendre no diferenciaba entre equivalencia y equivalencia propia, para él la operación resultaba en general en tan solo dos soluciones, y no cuatro.

Mientras no se distinga entre la equivalencia y la equivalencia propia, el problema de signos en el segundo coeficiente no se puede solucionar, pero este no es el único problema. Se necesita probar que los signos de (2.5) se pueden elegir de forma que la composición esté bien definida.

2.3. Gauss

En la sección anterior ya habíamos visto una definición de la composición de Legendre en (2.4). Quedaba por solucionar la ambigüedad en el número de soluciones. La solución a este problema la dio Gauss en *Disquisitiones Arithmeticae* [8], y, aunque menciona los resultados de Legendre sobre la ley de reciprocidad cuadrática, no escribe nada sobre su estudio de formas binarias cuadráticas, por lo que parece que el matemático alemán no estaba al tanto de lo avances ya hechos por el francés. La clave final para definir la composición de formas reside en el siguiente resultado probado por Gauss:

Proposición 2.1. *Dadas dos formas $f(x, y)$ y $g(x, y)$ cuyo discriminante es $D < 0$ y su composición es $F(x, y)$, de forma que*

$$f(x, y) \cdot g(x, y) = F(a_1xz + b_1xw + c_1yz + d_1yw, a_2xz + b_2xw + c_2yz + d_2yw),$$

entonces

$$a_1b_2 - a_2b_1 = \pm f(1, 0) \quad y \quad a_1c_2 - a_2c_1 = \pm g(1, 0).$$

Demostración. Si $f(x,y)=(a,b,c)$, $g(z,w)=(a',b',c')$ y $F(x,y)=(A,B,C)$, usando la igualdad

$$f(x,y)g(z,w)=F(a_1xz+b_1xw+c_1yz+d_1yw, a_2xz+b_2xw+c_2yz+d_2yw)$$

podemos obtener estas tres igualdades:

$$\begin{cases} aa' = Aa_1^2+Ba_1a_2+Ca_2^2, \\ ac' = Ab_1^2+Bb_1b_2+Cb_2^2, \\ ab' = 2Aa_1b_1+B(a_1b_2+a_2b_1)+2Ca_2b_2. \end{cases} \tag{2.7}$$

La primera y la segunda igualdad se obtienen directamente haciendo $x=z=1$ e $y=w=0$, y $x=w=1$ e $y=z=0$, respectivamente. La tercera requiere un poco más de trabajo y resulta de hacer $x=z=w=1$ e $y=0$ y utilizar las otras dos igualdades anteriores para despejar la ecuación y llegar a la identidad deseada.

Ahora, si desarrollamos $a^2(b'^2-4a'c')=(ab')^2-4aa'ac'$, al usar las igualdades en (2.7), obtenemos que

$$a^2(b'^2-4a'c')=(a_1b_2-a_2b_1)^2(B^2-4AC).$$

Pero el discriminante de $F(x,y)$ y $g(x,y)$ es el mismo, D, por lo tanto

$$a^2D=(a_1b_2-a_2b_1)^2D.$$

Despejando D, lo cual es posible ya que $D\neq 0$, y utilizando que $f(1,0)=a$, llegamos a $f(1,0)=\pm(a_1b_2-a_2b_1)$.

Para obtener que $g(1,0)=a'=\pm(a_1c_2-a_2c_1)$, procedemos de forma análoga, obteniendo las identidades

$$\begin{cases} aa' = Aa_1^2+Ba_1a_2+Ca_2^2, \\ a'c = Ac_1^2+Bc_1c_2+Cc_2^2, \\ a'b = 2Aa_1c_1+B(a_1c_2+a_2c_1)+2Ca_2c_2, \end{cases}$$

y haciendo uso de estas para llegar a

$$a'^2(b^2-4ac)=(a_1c_2-a_2c_1)^2(B^2-4AC)$$

para obtener finalmente $g(1,0)=\pm(a_1c_2-a_2c_1)$. □

Ahora, Gauss hace buen uso de estas igualdades para dar con la clave final de la composición de formas, a la que el llama composición directa:

Teorema 2.2. *Dadas dos formas de igual discriminante $D<0$, $f(x,y)$ y $g(z,w)$, entonces existe otra forma $F(x,y)$, que llamaremos composición directa de $f(x,y)$ y $g(x,y)$,de igual discriminante D tal que*

$$f(x,y)g(z,w)=F(B_1(x,y;z,w),B_2(x,y;z,w)), \tag{2.8}$$

donde $B_i(x,y;z,w)=a_ixz+b_ixw+c_iyz+d_iyw$ con $a_i,b_i,c_i,d_i\in\mathbb{Z}, i=1,2$, y además se verifica que $f(1,0)=a_1b_2-a_2b_1$ y $g(1,0)=a_1c_2-a_2c_1$.

La composición directa de Gauss arregla el problema que tenía la composición de Legendre y le da a las clases de equivalencia de formas la estructura de grupo abeliano finito. Cabe destacar que en la época de Gauss todavía no existía el concepto de grupo; sin embargo, el matemático alemán fue capaz de demostrar igualmente todas las propiedades que hacen de este conjunto un grupo con esas características.

La demostración que da Gauss en *Disquisitiones Arithmeticae* [8] de la estructura del grupo es muy densa y trabajosa, así que trabajaremos con un concepto algo más sencillo: la composición de Dirichlet.

2.4. Dirichlet

Dirichlet fue un matemático prusiano del siglo XIX que dedicó gran parte su vida a estudiar la obra de Gauss. Entre sus numerosas aportaciones a la teoría de números, destaca su trabajo sobre la composición de formas. Dirichlet consiguió, para un tipo particular de formas que ahora veremos, dar una expresión explícita del resultado de la composición.

Para poder introducir el concepto de composición de Dirichlet, es necesario primero dar la siguiente definición:

Definición 2.3. Dos formas $f(x,y) = ax^2 + bxy + cy^2$ y $g(x,y) = a'x^2 + b'xy + c'y^2$ de igual discriminante D se dicen que están reunidas si $\mathrm{mcd}(a, a', \frac{b+b'}{2}) = 1$.

Además, necesitaremos un par de resultados para asegurar la existencia y unicidad de un entero B que será clave para la composición de Dirichlet:

Proposición 2.4. *Sean $p_1, q_1, \ldots, p_r, q_r, m$ enteros tales que $\mathrm{mcd}(p_1, \ldots, p_r, m) = 1$. Entonces, las congruencias*

$$p_i B \equiv q_i \pmod{m}, \quad i = 1, \ldots, r \tag{2.9}$$

tienen una única solución si y solo si para todo $i, j = 1, \ldots, r$ se tiene

$$p_i q_j \equiv p_j q_i \pmod{m}. \tag{2.10}$$

Demostración. Supongamos primero que se cumple (2.9). Entonces, existe un único $B \in \mathbb{Z}$ tal que para todo $i, j = 1, \ldots, r$, $p_i B \equiv q_i \pmod{m}$ y $p_j B \equiv q_j \pmod{m}$. Multiplicando p_j por q_i y usando las congruencias, obtenemos

$$p_j q_i \equiv p_j p_i B = p_i p_j B \equiv p_i q_j \pmod{m},$$

como buscábamos.

Supongamos ahora que (2.10) es cierto. Puesto que $\mathrm{mcd}(p_1, \ldots, p_r, m) = 1$, por Bézout, existen enteros

$$a, a_1, \ldots, a_r \quad \text{tales que} \quad am + \sum_{i=1}^{r} p_i a_i = 1, \tag{2.11}$$

que en términos de congruencias es $\sum_{i=1}^{r} p_i a_i \equiv 1 \pmod{m}$.

Si tomamos $B \equiv \sum_{i=1}^{r} q_i a_i \pmod{m}$. Entonces,

$$p_k B \equiv \sum_{i=1}^{r} a_i q_i p_k \equiv \sum_{i=1}^{r} a_i q_k p_i = q_k \sum_{i=1}^{r} a_i p_i \equiv q_k \pmod{m},$$

donde en la segunda congruencia hemos usado (2.10) y en la cuarta (2.11).

Veamos además que este entero B es único módulo m. Pare ello, suponemos que existe otra solución $C \in \mathbb{Z}$. Entonces, se verifica que $p_i(B - C) \equiv 0 \pmod{m}$ para $i = 1, \ldots, r$, con lo cual m divide a $p_i(B - C)$, y por tanto, a $B - C$, ya que p_i y m son coprimos. Luego, $B \equiv C \pmod{m}$, y la solución es única módulo m. □

Proposición 2.5. *Sean $f(x, y) = ax^2 + bxy + cy^2$ y $g(x, y) = a'x^2 + b'xy + c'y^2$ dos formas reunidas de discriminante $D < 0$. Entonces, existe un único entero $B = B(f, g)$ módulo $2aa'$ tal que*

$$\begin{aligned} B &\equiv b \pmod{2a}, \\ B &\equiv b' \pmod{2a'}, \\ B^2 &\equiv D \pmod{4aa'}. \end{aligned}$$

Demostración. El primer paso es sintetizar las tres congruencias. Si se cumplen las dos primeras, multiplicándolas obtenemos que

$$B^2 - (b + b')B + bb' = (B - b)(B - b') \equiv 0 \pmod{4aa'},$$

de forma que, como $(b + b')B \equiv B^2 + bb' \pmod{4aa'}$, la tercera de ellas se puede escribir como

$$(b + b')B \equiv bb' + D \pmod{4aa'},$$

que al dividir entre dos resulta en

$$\frac{(b + b')B}{2} \equiv \frac{bb' + D}{2} \pmod{2aa'}. \tag{2.12}$$

Multiplicando las dos primeras ecuaciones por a' y a respectivamente y combinándolas con (2.12), la hipótesis de la proposición es equivalente a:

$$a'B \equiv a'b \pmod{2aa'} \tag{2.13}$$

$$aB \equiv ab' \pmod{2aa'} \tag{2.14}$$

$$\frac{(b + b')}{2} B \equiv \frac{bb' + D}{2} \pmod{2aa'}. \tag{2.15}$$

Puesto que $f(x, y)$ y $g(x, y)$ son formas reunidas, se cumple $\operatorname{mcd}\left(a, a'\frac{b+b'}{2}\right) = 1$ y la condición sobre el máximo común divisor de la Proposición 2.4 se verifica. Por lo tanto, solo falta comprobar que las congruencias de (2.10) se cumplen para poder aplicarla. Sea entonces $p_1 = a'$, $p_2 = a$ y $p_3 = \frac{b+b'}{2}$ y $q_1 = a'b$, $q_2 = ab'$ y $q_3 = \frac{bb'+D}{2}$.

Entonces,

$$\begin{aligned}
p_1 \cdot q_2 &\equiv a' \cdot ab' \overset{(2.14)}{\equiv} a' \cdot aB \overset{(2.13)}{\equiv} a \cdot a'b' \equiv p_2 \cdot q_1 \pmod{2aa'},\\
p_1 \cdot q_3 &\equiv a' \cdot \frac{bb'+D}{2} \overset{(2.15)}{\equiv} a' \cdot B\frac{b+b'}{2} \overset{(2.13)}{\equiv} a' \cdot b\frac{b+b'}{2} \equiv p_3 \cdot q_1 \pmod{2aa'},\\
p_2 \cdot q_3 &\equiv a \cdot \frac{bb'+D}{2} \overset{(2.15)}{\equiv} a \cdot B\frac{b+b'}{2} \overset{(2.14)}{\equiv} a \cdot b'\frac{b+b'}{2} \equiv p_3 \cdot q_2 \pmod{2aa'}.
\end{aligned}$$

Luego, nos encontramos en las hipótesis de la Proposición 2.4 y la existencia y unicidad de B en módulo $2aa'$ se sigue de esta. □

Asegurada la existencia y unicidad de este entero B, tenemos ya todo lo necesario para poder definir la composición de Dirichlet:

Definición 2.6. Dadas dos formas reunidas, con el mismo discriminante $D < 0$, $f(x,y) = ax^2 + bxy + cy^2$ y $g(x,y) = a'x^2 + b'xy + c'y^2$, la composición de Dirichlet de estas dos formas es

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2, \tag{2.16}$$

donde $B = B(f,g)$ es como en la Proposición 2.5. Denotaremos $F = f \circ g$.

El siguiente paso es comprobar que, efectivamente, la composición de Dirichlet es la misma que la de Gauss, pero para formas reunidas:

Proposición 2.7. *Dadas dos formas reunidas $f(x,y)$ y $g(x,y)$ de mismo discriminante $D < 0$, su composición de Dirichlet $F(x,y)$ es la composición directa de Gauss de $f(x,y)$ y $g(x,y)$, y tiene discriminante D.*

Demostración. Sean $f(x,y) = ax^2+bxy+cy^2$ y $g(x,y) = a'x^2+b'xy+c'y^2$ dos formas reunidas de discriminante $D = b^2 - 4ac = b'^2 - 4a'c' < 0$ y

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}$$

su composición de Dirichlet, con $B = B(f,g)$ como en la Proposición 2.5. Es inmediato comprobar que el discriminante de $F(x,y)$ es $B^2 - 4aa'\frac{B^2-D}{4aa'} = B^2 - B^2 + D = D$.

Veamos que efectivamente es la composición directa de Gauss. Sea $C = \frac{B^2-D}{4aa'}$ de forma que $F(x,y) = aa'x^2 + Bxy + Cy^2$. Por tener que cumplir B la primera de las congruencias de la Proposición 2.5, existe un $n \in \mathbb{Z}$ tal que $B = b + 2an$. A través de la matriz T^n usada en la demostración del Teorema 1.8, $f(x,y)$ es equivalente a la forma

$$(a, b+2an, an^2 + bn + c) = (a, B, an^2 + bn + c).$$

Además,

$$a'C = \frac{B^2 - D}{4a} = \frac{b^2 + 4a^2n^2 + 4abn - b^2 + 4ac}{4a} = an^2 + bn + c.$$

Luego, $f(x,y)$ es propiamente equivalente a la forma $(a, B, a'C)$ y de manera análoga podemos ver que (a', b', c') es equivalente a (a', B, aC).

Ahora bien, si hacemos $X = xz - yw$ e $Y = axw + a'yz + Byw$ y consideramos la forma $F(X,Y) = aa'X^2 + BXY + CY^2$, obtenemos que

$$F(X,Y) = f(x.y) \cdot g(x,y).$$

Los cálculos para obtener esta igualdad se encuentran en el Apéndice A.

Falta por comprobar que $F(x,y)$ es primitiva (ver que es definida positiva es inmediato por ser el producto de dos formas que lo son). Para ello, supongamos por reducción a lo absurdo que existe cierto primo p que divide a aa', B y C. Entonces, también divide a todos los números representados por la forma $f(x,y)g(z,w)$, es decir, al producto de los números representados por $f(x,y)$ y por $g(z,w)$, entre ellos ac', $a'c$ $a(a'+b'+c'), cc'$ y $a'(a+b+c)$.

Supongamos que $p \nmid a$. Si este es el caso, se debe dar que $p \mid a'$. Entonces, como $p \mid ac'$, se tiene que $p \mid c'$ y como $p \mid a(a'+b'+c')$, $p \mid b'$, lo que contradice que $g(x,y)$ sea primitiva. Supongamos ahora que p divide tanto a a como a a', entonces, como $p \mid cc'$, al menos una de $f(x,y)$ o $g(x,y)$ no es primitiva. Por último, si $p \mid a$ y $p \nmid a'$, como $p \mid a'c$, $p \mid c$, y como $p \mid a'(a+b+c)$, $p \mid b$, por lo que $f(x,y)$ no es primitiva y concluimos que no existe tal primo p.

Por último, veamos que la composición de Dirichlet está bien definida. Para ello, veremos que la elección de B solo depende de su resto módulo $2aa'$. Sea (aa', B', C') otra composición de Dirichlet de las formas $f(x,y)$ y $g(z,w)$, donde $B' = B + 2aa'm$ para algún $m \in \mathbb{Z}$ y $C' = \frac{B'^2 - D}{4aa'}$. Entonces, la matriz T^{-m} lleva $F(x,y)$ a (aa', B', C'), con lo que ambas caen, como buscábamos, en la misma clase de equivalencia. □

Ahora, introduciremos un tipo de formas que jugarán un papel fundamental en esta sección, pues veremos más tarde que son el elemento identidad del grupo G_D:

Definición 2.8. Dado $D < 0$ tal que $D \equiv 0, 1 \pmod 4$, la clase de la forma principal de G_D es la que contiene a

$$\begin{aligned} x^2 - \frac{D}{4}y^2 \quad &\text{si} \quad D \equiv 0 \pmod 4, \\ x^2 + xy + \frac{1-D}{4}y^2 \quad &\text{si} \quad D \equiv 1 \pmod 4. \end{aligned}$$

En ambos casos, unos sencillos cálculos bastan para ver que el discriminante de las formas principales es D: en el primer caso, el discriminante es $-4(-\frac{D}{4}) = D$ y en el segundo, es $1 - 4\frac{1-D}{4} = D$. Además, son reducidas: en el primer caso

$$0 < 1 \leq -(-\frac{D}{4}) = \frac{4n_1}{4} = n_1$$

para algún $n_1 \in \mathbb{Z}$, y en el segundo,

$$1 = 1 \leq \frac{1-D}{4} = \frac{1 + 4n_2 - 1}{4} = n_2$$

para algún $n_2 \in \mathbb{Z}$.

Para la demostración de que la composición de Dirichlet induce en G_D una estructura de grupo abeliano finito necesitaremos demostrar previamente varios resultados sobre equivalencia de formas y representación propia:

Lema 2.9. *Si $f(x,y) = ax^2 + bxy + cy^2$ y $g(x,y) = a'x^2 + b'xy + c'y^2$ son dos formas de igual discriminante $D < 0$ tal que $a = a'$ y $b \equiv b'$ (mód $2a$), entonces son equivalentes.*

Demostración. Sea T^n una matriz como en la demostración del Teorema 1.8. Esta matriz lleva $f(x,y)$ a la forma equivalente $f'(x,y) = ax^2+(b+2an)xy+(an^2+bn+c)y^2$. Como $b + 2an \equiv b$ (mód $2a$), entonces se puede elegir al entero n de forma que $b+2an = b'$. Como además $a = a'$ y las dos formas tienen el mismo discriminante, el tercer coeficiente también debe coincidir y $f(x,y)$ y $g(x,y)$ han de ser equivalentes. □

Lema 2.10. *Sean (a,b,c) y (a',b',c') dos formas reunidas de igual discriminante $D < 0$. Entonces, existen dos enteros B y C tales que $\mathrm{mcd}(a,a',B) = 1$ y $(a,B,a'C)$ es propiamente equivalente a (a,b,c) y (a',B,aC) es propiamente equivalente a (a',b',c')*

Demostración. Para poder aplicar el Lema 2.9 bastaría con probar que existe un tal entero B que verifique

$$B \equiv b \pmod{2a} \quad \text{y} \quad B \equiv b' \pmod{2a'}.$$

y, en consecuencia, C estará determinado por el discriminante.

Si suponemos que se cumple la primera congruencia, entonces existe un entero k tal que $B = b + 2ak$, y la segunda congruencia equivaldría a $b + 2ak \equiv b'$ (mód $2a'$), o lo que es lo mismo, $\frac{b-b'}{2} \equiv -ak$ (mód a').

Como (a,b,c) y (a',b',c') tienen el mismo discriminante, entonces b y b' tienen la misma paridad, por lo que $\frac{b-b'}{2}$ es un entero y entonces la congruencia tiene solución si y solo si $m = \mathrm{mcd}(a,a')$ divide a $\frac{b-b'}{2}$.

Como $b^2 - 4ac = b'^2 - 4a'c'$, entonces

$$\frac{(b+b')}{2}\frac{(b-b')}{2} = \frac{b^2 - b'^2}{4} = \frac{4ac - 4a'c'}{4} = ac - a'c'. \tag{2.17}$$

Por ser las formas reunidas, $\mathrm{mcd}\left(a, a', \frac{b+b'}{2}\right) = 1$, y de (2.17) se deduce que entonces m debe dividir a $\frac{b-b'}{2}$, con lo cual $\frac{b-b'}{2} \equiv -ak$ (mód a') tiene solución.

Ahora, falta comprobar que C, que viene determinado por el discriminante, es un entero. Como B es único módulo $2n$, siendo $n = \mathrm{mcm}(a,a') = \frac{aa'}{\mathrm{mcd}(a,a')} = \frac{aa'}{m}$, entonces $B = B_0 + 2nt$ para B_0 un entero fijo y t otro entero arbitrario. Así,

$$B^2 = B_0^2 + 4ntB_0 + 4n^2t^2 = D + 4aa'C \Longrightarrow B^2 \equiv B_0^2 \equiv D \pmod{4n}, \tag{2.18}$$

ya que $n \mid aa'$ al ser su mínimo común múltiplo.

Ahora, si hallamos t tal que $B^2 \equiv D \pmod{4aa'}$, aseguraríamos entonces que C es un entero.

Despejando la segunda igualdad en (2.18) y usando que $n = \frac{aa'}{m}$, se tiene

$$\frac{D - B_0^2}{4n} = B_0 t + aa' \left(\frac{t^2}{m} + C \right) \Longrightarrow \frac{D - B_0^2}{4n} \equiv B_0 t \pmod{m}.$$

Es inmediato combrobar que la parte izquierda de la congruencia es un entero usando que $D = B_0^2 + 4ntB_0 + 4n^2t^2 - 4aC$. Además, B_0 es invertible en módulo m por como está definido, de forma que t queda totalmente determinado, en módulo m, de la siguiente forma:

$$t \equiv \frac{D - B^2}{4n} B_0^{-1} \pmod{m}.$$

Por último, vemos que $(a, B, a'C)$ y (a', B, aC) son formas reunidas, es decir, que $\mathrm{mcd}(a, a', B) = 1$, pues si no lo fuera, entonces existiría un entero d que dividiría a a, a' y B, y por lo tanto, a $\frac{b+b'}{2}$, y entonces (a, b, c) y (a', b', c') no serían reunidas.

□

Lema 2.11. *Dos formas $f(x, y) = (a, b, c)$ y $g(x, y) = (a', b', c')$ de igual discriminante son equivalentes si y solo si existen dos enteros α y γ que verifican:*

$$\begin{aligned} a\alpha^2 + b\alpha\gamma + c\gamma^2 &= a', \\ 2a\alpha + (b + b')\gamma &\equiv 0 \pmod{2a'}, \\ (b - b')\alpha + 2c\gamma &\equiv 0 \pmod{2a'}. \end{aligned}$$

Demostración. Supongamos que estas formas fueran equivalentes mediante el cambio dado por la matriz

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

donde $\beta, \delta \in \mathbb{Z}$.

Esto quiere decir que entonces

$$\begin{aligned} g(x, y) = f(\alpha x + \beta y, \gamma x + \delta y) = (a\alpha^2 + b\alpha\gamma + c\gamma^2)x^2 + \\ (2a\alpha\beta + 2c\gamma\delta + b(\alpha\delta + \beta\gamma))xy + (a\beta^2 + b\beta\delta + c\delta^2)y^2. \end{aligned}$$

Por lo tanto, se ha de satisfacer

$$\begin{aligned} a' &= f(\alpha, \gamma), \\ b' &= 2a\alpha\beta + 2c\gamma\delta + b(\alpha\delta + \beta\gamma), \\ c' &= f(\beta, \delta), \end{aligned} \tag{2.19}$$

con lo cual, se cumple la primera ecuación del enunciado. Además, por tratarse de equivalencia propia y por la ecuación (2.19), entonces β y δ deben verificar

$$\alpha\delta - \beta\gamma = 1. \tag{2.20}$$

$$\beta(2a\alpha + b\gamma) + \delta(2c\gamma + b\alpha) = b'. \tag{2.21}$$

Usando estas identidades, obtenemos que

$$\begin{aligned} 2a\alpha + (b+b')\gamma &= 2a'\delta, \\ (b-b')\alpha + 2c\gamma &= -2a'\beta, \end{aligned}$$

que es lo que buscamos. Los cálculos para llegar a estas identidades se encuentran en el Apéndice A.

Para la otra implicación, basta con recorrer el mismo camino en dirección opuesta, partiendo desde estas dos últimas identidades. □

Lema 2.12. *Sean $(a, B, a'C)$ y (a', B, aC) dos formas reunidas con discriminante $D < 0$ y $(m, N, m'L)$ y (m', N, mL), también reunidas y de igual discriminante D, y tal que $(a, B, a'C) \sim (m, N, m'L)$ y $(a', B, aC) \sim (m', N, mL)$ entonces*

$$(a, B, a'C) \circ (a', B, aC) \sim (m, N, m'L) \circ (m', N, mL).$$

Demostración. Para probar este resultado, aplicaremos el Lema 2.11, que, por la equivalencia entre $(a, B, a'C)$ y $(m, N, m'L)$ aseguran la existencia de dos enteros α_1 y γ_1 tales que

$$a\alpha_1^2 + B\alpha_1\gamma_1 + a'C\gamma_1^2 = m, \tag{1}$$
$$2a\alpha_1 + (B+N)\gamma_1 \equiv 0 \pmod{2m}, \tag{2}$$
$$(B-N)\alpha_1 + 2a'C\gamma_1 \equiv 0 \pmod{2m}, \tag{3}$$

y, por la equivalencia entre (a', B, aC) y (m', N, mL), otros dos enteros α_2 y β_2 tales que

$$a'\alpha_2^2 + B\alpha_2\gamma_2 + aC\gamma_2^2 = m', \tag{4}$$
$$2a'\alpha_2 + (B+N)\gamma_2 \equiv 0 \pmod{2m'}, \tag{5}$$
$$(B-N)\alpha_2 + 2aC\gamma_2 \equiv 0 \pmod{2m'}. \tag{6}$$

Ahora, con el objetivo de aplicar el lema a las composiciones $(a, B, a'C) \circ (a', B, aC)$ y $(m, N, m'L) \circ (m', N, mL)$, se combinan las ecuaciones anteriores y haciendo el cambio $X = \alpha_1\alpha_2 - C\gamma_1\gamma_2, Y = a\alpha_1\gamma_2 + a'\gamma_1\alpha_2 + B\gamma_1\gamma_2$, podemos llegar a:

$$aa'X^2 + BXY + CY^2 = mm', \tag{7}$$
$$2aa'X + (B+N)Y \equiv 0 \pmod{2mm'}, \tag{8}$$
$$(B-N)X + 2CY \equiv 0 \pmod{2mm'}. \tag{9}$$

Aplicando ahora el Lema 2.11, estas ecuaciones aseguran, como buscábamos, que $(a, B, a'C) \circ (a', B, aC) \sim (m, N, m'L) \circ (m', N, mL)$. Para obtener (7), simplemente se multiplican las ecuaciones (1) y (4). Para obtener (8), multiplicamos también (2) y (5), sustituimos $N^2 \equiv B^2 - 4aa'C \pmod{4mm'}$, lo cual se cumple por ser las formas de mismo discriminante D, y después se divide entre 2.

Para obtener (9) se necesita algo más de trabajo. Haciendo $U = \frac{B-\sqrt{D}}{2}X + CY$, obtenemos las siguientes cuatro ecuaciones:

$$\begin{aligned}
\left(\frac{B-\sqrt{D}}{2}\alpha_1 + a'C\gamma_1\right)\cdot\left(a'\alpha_2 + \frac{B+\sqrt{D}}{2}\gamma_2\right) &= a'U,\\
\left(a\alpha_1 + \frac{B+\sqrt{D}}{2}\gamma_1\right)\left(\frac{B-\sqrt{D}}{2}\alpha_2 + aC\gamma_2\right) &= aU,\\
\left(\frac{B-\sqrt{D}}{2}\alpha_1 + a'C\gamma_1\right)\left(\frac{B-\sqrt{D}}{2}\alpha_2 + aC\gamma_2\right) &= \frac{B-\sqrt{D}}{2}U,\\
C\left(a\alpha_1 + \frac{B+\sqrt{D}}{2}\gamma_1\right)\left(a'\alpha_2 + \frac{B+\sqrt{D}}{2}\gamma_2\right) &= \frac{B+\sqrt{D}}{2}U.
\end{aligned}$$

De nuevo, sustituyendo $N \equiv \sqrt{D} \pmod{4mm'}$, observamos que la parte izquierda de cada una de las cuatro igualdades es múltiplo de mm', de forma que también lo es la parte de la derecha. Por lo tango, $aU \equiv a'U \equiv BU \pmod{mm'}$, donde para obtener la tercera congruencia hemos sumado las dos últimas ecuaciones. Como por ser las formas reunidas se ha de tener $\mathrm{mcd}(a, a', B) = 1$, entonces $U \equiv 0 \pmod{mm'}$, de lo que obtenemos finalmente

$$U = \frac{B-\sqrt{D}}{2}X + CY \equiv \frac{B-N}{2}X + CY \equiv 0 \pmod{mm'},$$

y multiplicando esto por dos obtenemos (9). □

Lema 2.13. *Una forma $f(x, y) = (a, b, c)$ representa propiamente a $m \in \mathbb{Z}$ si y solo si es equivalente a (m, B, C) para $B, C \in \mathbb{Z}$.*

Demostración. Supongamos primero que $f(p, q) = m$, con $p, q \in \mathbb{Z}$ coprimos. Ahora, usamos la identidad de Bezout para asegurar la existencia de dos enteros r y s tales que $ps - qr = 1$. Entonces la matriz

$$M = \begin{pmatrix} p & r \\ q & s \end{pmatrix}$$

envía (a, b, c) a

$$f(px + ry, qx + sy) = (f(p, q), 2apr + bps + brq + 2cqs, f(r, s)) = (m, B, C),$$

con $B = (2apr + bps + brq + 2cqs)$ y $C = f(r, s)$.

Ahora supongamos que (a, b, c) es equivalente a $f(x, y) = (m, B, C)$. Entonces, $f(1, 0) = m$ y m está representado propiamente por (a, b, c). □

Lema 2.14. *Dada una forma $f(x, y)$ y un entero M, $f(x, y)$ representa propiamente al menos un entero coprimo con M.*

Demostración. Sea $f(x,y) = ax^2 + bxy + cy^2$ y M un entero. Primero, veamos que para cualquier p primo, alguno de $f(1,0), f(0,1)$ o $f(1,1)$ es coprimo con p. Si no fuese así, existirían tres enteros r, s y t tales que

$$\text{mcd}(p, f(1,0)) = r, \text{mcd}(p, f(0,1)) = s \quad \text{y} \quad \text{mcd}(p, f(1,1)) = t.$$

Como p es primo, entonces $r = s = t = p$. Pero como $f(1,0) = a$ y $f(0,1) = c$, se tendría $\text{mcd}(a,c) = p$, lo cual contradice que la forma sea primitiva.

La descomposición de M en factores primos es $|M| = \sum_{i=1}^{l} p_i^{n_i}$, con p_i primo y $n_i \in \mathbb{N}$ para todo $i = 1, \dots l$. Ahora bien, la observación anterior asegura que existe una pareja $(\alpha_i, \beta_i) \in \{(1,0),(1,1),(0,1)\}$ tal que $\text{mcd}(p_i, f(\alpha_i, \beta_i)) = 1$ para todo $i = 1, \dots, l$. Esto, en términos de congruencias, es $f(\alpha_i, \beta_i) \not\equiv 0 \pmod{p_i}$.

Por el teorema chino del resto, existen dos enteros $x_0, y_0 \in \mathbb{Z}$ que verifican

$$\begin{aligned} x_0 &\equiv \alpha_1 \pmod{p_1}, & y_0 &\equiv \beta_1 \pmod{p_1}, \\ x_0 &\equiv \alpha_2 \pmod{p_2}, & y_0 &\equiv \beta_2 \pmod{p_2}, \\ &\vdots & &\vdots \\ x_0 &\equiv \alpha_l \pmod{p_l}, & y_0 &\equiv \beta_l \pmod{p_l}. \end{aligned}$$

Por lo tanto,

$$f(x_0, y_0) = ax_0^2 + x_0y_0 + cy_0^2 \equiv a\alpha_i^2 + b\alpha_i\beta_i + c\beta_i^2 = f(\alpha_i, \beta_i) \not\equiv 0 \pmod{p_i}$$

para todo $i = 1, \dots s$, y entonces $\text{mcd}(M, f(x_0, y_0)) = 1$.

Solo falta por ver que $\text{mcd}(x_0, y_0) = 1$ para que se trate de equivalencia propia. Si $\alpha = \prod_{i=1}^{l} \alpha_i$ y $\beta = \prod_{i=1}^{l} \beta_i$, entonces $x_0 \equiv \alpha \pmod{M}$ e $y_0 \equiv \beta \pmod{M}$. El teorema de Dirichlet sobre la infitud de primos en progresiones aritméticas asegura que se puedan escoger x_0 e y_0 primos al existir infinitos primos representando cada clase en $\mathbb{Z}/M\mathbb{Z}$. □

Ahora ya tenemos todos los resultados necesarios para demostrar nuestro objetivo:

Teorema 2.15. *Sea $D \equiv 0, 1 \pmod 4$ un entero negativo. Entonces la composición de Dirichlet, que denotaremos por $\circ$, induce una operación binaria bien definida en G_D y convierte $(G_D, \circ)$ en un grupo abeliano finito, cuyo orden es el número de clases en G_D. Además, el inverso de la clase que contiene a $f(x,y) = ax^2 + bxy + cy^2$ es la clase que contiene a $f^{-1}(x,y) = ax^2 - bxy + cy^2$, y el elemento neutro es la clase que contiene a la forma principal de la Definición 2.8.*

Nota 2. *Sin que lleve a confusión, se utilizará el mismo símbolo, $\circ$, para denotar tanto la composición de clases de equivalencia de formas como la composición de formas.*

Demostración. Primero debemos probar que la composición de formas está bien definida para cualquier pareja de clases de formas de G_D. Dados dos representantes de dos clases distintas, (a_0, b_0, c_0) y $g(x,y)$ en G_D, el Lema 2.14 asegura la existencia de

$a_0' \in \mathbb{Z}$ representado propiamente por $g(x,y)$, con $\mathrm{mcd}(a_0, a_0') = 1$, y el Lema 2.13 que existen $b_0', c_0' \in \mathbb{Z}$ tales que $g(x,y)$ es equivalente a (a_0', b_0', c_0'). Entonces, como

$$\mathrm{mcd}\left(a_0, a_0', \frac{b_0 + b_0'}{2}\right) \leq \mathrm{mcd}(a_0, a_0') = 1,$$

aseguramos que para cualquier pareja de clases existen dos representantes reunidos.

El segundo paso es ver que está bien definida a nivel de clases. Sean $f_1(x,y)$ y $g_1(x,y)$ dos representantes de clases de G_D. El Lema 2.10 nos permite encontrar $f_2(x,y) \sim f_1(x,y)$ tal que $f_2(x,y) = (m, N, m'L)$ y $g_2(x,y) \sim g_1(x,y)$ tal que $g'(x,y) = (m', N, mL)$. Entonces, si denotamos también por $\circ$ la composición de representantes de clases de equivalencia de formas,

$$[f_1(x,y)] \circ [g_1(x,y)] = [f_2(x,y)] \circ [g_2(x,y)] = [(f_2 \circ g_2)(x,y)]$$

por el Lema 2.12.

El tercer paso es probar la asociatividad. Dados tres representantes de clases $h_i(x,y) = (a_i, b_i, c_i)$ para $i = 1,2,3$ en G_D, de nuevo, usamos los lemas 2.13 y 2.14 para hallar formas equivalentes a estas tres que cumplan $\mathrm{mcd}(a_1, a_2, a_3) = 1$ de modo que las tres formas estén reunidas. Entonces, usando (2.16)

$$([h_1] \circ [h_2]) \circ [h_3] = [(a_1 a_2, B, C)] \circ [h_3] = [(a_1 a_2 a_3, B', C')],$$

donde

$$C = \frac{B^2 - D}{4a_1 a_2} \quad \text{y} \quad C' = \frac{B'^2 - D}{4a_1 a_2 a_3}, \quad \text{y} \quad B = B(h_1, h_2) \quad \text{y} \quad B' = B(h_1 \circ h_2, h_3),$$

con B y B' como en (2.16). Pero además, por la definición de B en la Proposición 2.5 y por tener el mismo discriminante, para que B' cumpla la última igualdad basta con que satisfaga $B' \equiv b_i \pmod{2a_i}$ para $i = 1,2,3$. También se tiene

$$[h_1] \circ ([h_2] \circ [h_3]) = [h_1] \circ [(a_2 a_3, \beta, \gamma)] = [(a_1 a_2 a_3, \beta', \gamma')],$$

con β, β', γ y γ' como en (2.16), y además β' verifica las mismas congruencias que B', por lo que $B \equiv \beta' \pmod{2a_1 a_2 a_3}$ ya que $\mathrm{mcd}(a_1, a_2, a_3) = 1$. Como ambas formas tienen el mismo primer coeficiente $a_1 a_2 a_3$, son equivalentes por el Lema 2.9..

Vayamos ahora con la prueba de que la forma principal es el elemento identidad. Para ello, mostraremos primero que $(1, b, c)$ es equivalente a la clase de la forma principal de G_D. Si $D \equiv 0 \pmod 4$, entonces b es par y se puede escribir como $b = 2b', b' \in \mathbb{Z}$. La matriz $T^{-b'}$, definida como en la demostración del Teorema 1.8, lleva nuestra forma $(1, b, c)$ a

$$(1, b - 2b', b'^2 - bb' + c) = \left(1, 0, -\frac{b^2}{4} + c\right) = \left(1, 0, -\frac{D}{4}\right),$$

que es la forma principal, como búscabamos.

Si suponemos ahora que $D \equiv 1 \pmod 4$, b es impar por lo que $b = 2n+1, n \in \mathbb{Z}$ y la matriz T^{-n} lleva $(1,b,c)$ a

$$(1, b-2n, n^2-bn+c) = \left(1, 2n-2n+1, -\frac{b^2+1-2b}{4} - \frac{b-1}{2} + c\right) = \left(1, 1, \frac{1-D}{4}\right),$$

que es también la forma principal.

Ahora veremos que efectivamente $(1,b,c)$ es el elemento identidad. Sean (a_4,b_4,c_4) y (a_5,b_5,c_5) dos formas de discriminante D. Observamos que $(1,b_4,c_4) \sim (1,b_5,c_5)$ por el Lema 2.9, ya que por tener el mismo discriminante, su segundo coeficiente tiene la misma paridad, y por tanto $b_4 \equiv b_5 \pmod 2$. Entonces,

$$[(1,b_4,c_4)] \circ [(a_5,b_5,c_5)] \overset{(2.10)}{=} [(1,B_0,a_5C_0)] \circ [(a_5,B_0,C_0)] = \\ [(a_5,B_0,C_0)] \overset{(2.9)}{=} [(a_5,b_5,c_5)],$$

donde se ha usado el Lema 2.9 en la última igualdad ya que $B \equiv b_5 \pmod{2a_5}$.

Lo último que falta para probar la estructura del grupo es ver que la inversa de la clase $[(a_6,b_6,c_6)]$ es la clase que contiene a la forma $[(a_6,-b_6,c_6)]$. Puesto que $\operatorname{mcd}\left(a_6, a_6, \frac{b_6-b_6}{2}\right) = a_6$, no podemos aplicar directamente la composición de Dirichlet. La matriz S de la demostración del Teorema 1.8, lleva $(a_6,-b_6,c_6)$ a (c_6,b_6,a_6), de forma que $\operatorname{mcd}\left(c_6, a_6, \frac{b_6+b_6}{2}\right) = \operatorname{mcd}(a_6,c_6,b_6) = 1$ por tratarse de formas primitivas, pudiendo ya entonces aplicar la composición de Dirichlet

$$[(a_6,b_6,c_6)] \circ [(a_6,-b_6,c_6)] = [(a_6,b_6,c_6)] \circ [(c_6,b_6,a_6)] = [(a_6c_6,b_6,1)],$$

donde para la última identidad se ha usado que, $b_6 \equiv b_6 \pmod{2a_6}$ y $b_6 \equiv b_6 \pmod{2c_6}$, como es lógico, y que $b_6^2 \equiv D \pmod{4a_6^2c_6}$, pues $D = b_6^2 - 4a_6c_6$. Así,

$$C = \frac{b_6^2 - D}{4a_6c_6} = \frac{4a_6c_6}{4a_6c_6} = 1.$$

Ahora, si $D \equiv 0 \pmod 4$, entonces $b_6 = 2b_6', b_6' \in \mathbb{Z}$ y el cambio dado por la matriz

$$M_1 = \begin{pmatrix} 0 & -1 \\ 1 & b_6' \end{pmatrix}$$

lleva $(a_6c_6,b_6,1)$ a $(1,0,a_6c_6-b_6'^2)$, que es la forma principal ya que

$$-4(a_6c_6 - b_6'^2) = 4b_6'^2 - 4a_6c_6 = b_6^2 - 4a_6c_6 = D.$$

En cambio, si $D \equiv 1 \pmod 4$, entonces $b_6 = 2n_0+1$ para algún $n_0 \in \mathbb{Z}$, el cambio dado por la matriz

$$M_2 = \begin{pmatrix} 0 & -1 \\ 1 & n_0+1 \end{pmatrix}$$

lleva $(a_6c_6,b_6,1)$ a $(1,1,a_6c_6-n_0-n_0^2)$, que es la forma principal ya que

$$1 - 4(a_6c_6 - n_0 - n_0^2) = -4a_6c_6 + (2n_0+1)^2 = D.$$

La conmutatividad se sigue directamente de la definición de composición de Dirichlet en (2.16) y la finitud se sigue de que el cardinal de G_D coincide con el número de formas reducidas, que ya habíamos visto que es finito. □

CAPÍTULO 3
Cubos de Bhargava

Como ya hemos visto, la composición de Dirichlet nos permite entender y trabajar con la composición directa de formas de una forma más sencilla. Sin embargo, dos siglos más tarde, se siguen estudiando otras maneras de comprender la composición.

El matemático canadiense Manjul Bhargava publicó en 2001 su tesis doctoral, dirigida por Andrew Wiles, en la que desarrolla toda una teoría sobre la composición de formas, extendible a dimensiones superiores. Esta teoría, basada en cubos de enteros, es una forma mucho más visual de entender la composición de formas binarias cuadráticas.

El objetivo principal de este capítulo será entender las nociones básicas de los cubos de Bhargava para poder asociarlos a la composición de Dirichlet.

3.1. Cubos de enteros y cortes fundamentales

Bhargava introduce en su tesis el concepto de *cubo de enteros*, un cubo con un entero en cada uno de los vértices, como se muestra en la Figura 3.1. Puesto que los coeficientes de las aristas definen completamente el cubo, lo podremos denotar como (a, b, c, d, e, f, g, h).

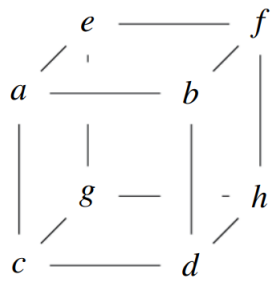

Figura 3.1: Cubo de enteros

Este cubo se puede cortar de tres formas distinas para obtener dos cuadrados distintos por cada corte, que definiremos como matrices 2×2:

1. Delante - Atrás:

$$M_1 := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{y} \qquad N_1 := \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

2. Izquierda - Derecha:

$$M_2 := \begin{pmatrix} a & c \\ e & g \end{pmatrix} \qquad \text{y} \qquad N_2 := \begin{pmatrix} b & d \\ f & h \end{pmatrix}.$$

3. Arriba - Abajo:

$$M_3 := \begin{pmatrix} a & e \\ b & f \end{pmatrix} \qquad \text{y} \qquad N_3 := \begin{pmatrix} c & g \\ d & h \end{pmatrix}.$$

A estos cortes los llamaremos *cortes fundamentales.*

Ahora, igual que hemos hecho con las formas, vamos a definir la acción del grupo $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ sobre $\mathcal{C}$, el conjunto de todos los cubos de enteros. Dado $\gamma = (L_1 \times L_2 \times L_3) \in \Gamma$, con

$$L_i = \begin{pmatrix} r_i & s_i \\ t_i & u_i \end{pmatrix},$$

entonces la acción de γ en el cubo de enteros, denotada $\Gamma * C$, reemplaza

$$(M_i, N_i) \quad \text{por} \quad (r_i M_i + s_i N_i, t_i M_i + u_i N_i),$$

siendo (M_i, N_i) los cortes fundamentales de C para $i = 1, 2, 3$. Es importante recalcar que en cada "paso" de la acción (cada vez que aplicamos la acción de L_i a (M_i, N_i)) afecta a las otras dos parejas de matrices, que deben estar en concordancia con el nuevo cubo generado. Sin embargo, el orden en el que apliquemos los pasos no afecta al resultado, ya que las transformaciones de filas y columnas conmutan por la asociatividad de la multiplicación de matrices.

Dados dos cubos de enteros, C y C', podemos definir entonces la relación de equivalencia

$$C \sim C' \iff \gamma * C = C', \gamma \in SL_2(\mathbb{Z}).$$

Que esta relación es de equivalencia es consecuencia inmediata de que $SL_2(\mathbb{Z})$ induce una relación de equivalencia en cada corte fundamental, a saber,

$$(M, N) \sim (M', N') \iff (M', N') = (aM + bN, cM + dN),$$

donde a, b, c y d son enteros que verifican $ad - bc = 1$, y $M, N, M', N' \in SL_2(\mathbb{Z})$. Veamos que esta es una relación de equivalencia:

1. $(M, N) \sim (M, N)$ ya que $(M, N) = (M + 0N, 0M + N)$ (reflexividad).

2. Si $(M, N) \sim (M', N')$, entonces $(M', N') = (aM + bN, cM + dN)$ y, por tanto, $(M, N) = (dM' - bN', -cM' + aN')$, donde $da - (-b)(-c) = 1$, con lo cual $(M', N') \sim (M, N)$ (simetría).

3. Si $(M,N) \sim (M',N')$ y $(M',N') \sim (M'',N'')$, donde $M'', N'' \in SL_2(\mathbb{Z})$, entonces $(M',N') = (aM+bN, cM+dN)$ y $(M'',N'') = (a'M'+b'N', c'M'+d'N')$, donde $a', b', c', d' \in \mathbb{Z}$ tal que $a'd' - b'c' = 1$. Entonces,

$$(M'',N'') = ((aa'+cb')N + (ba'+db')N, (ac'+cd')M + (bc'+dd')N),$$

y unos cálculos, que se encuentran en el apéndice A, nos convencen de que $(M,N) \sim (M'',N'')$.

Además, dado un cubo de enteros C, se pueden definir a partir de él tres formas binarias cuadráticas, que no tienen por qué ser primitivas, de la siguiente forma:

$$Q_i^C = -\det(M_i x - N_i y), \tag{3.1}$$

con (M_i, N_i) los cortes fundamentales para $i = 1, 2, 3$.

Por ejemplo, las formas binarias cuadráticas que define la Figura 3.1 son:

$$\begin{aligned}
Q_1^C &= -\det \begin{pmatrix} ax-ey & bx-fy \\ cx-gy & dx-hy \end{pmatrix} = (bc-ad, ah+de-bg-cf, fg-eh), \\
Q_2^C &= -\det \begin{pmatrix} ax-by & cx-dy \\ ex-fy & gx-hy \end{pmatrix} = (ce-ag, ah+bg-cf-de, df-bh), \\
Q_3^C &= -\det \begin{pmatrix} ax-cy & ex-gy \\ bx-dy & fx-hy \end{pmatrix} = (be-af, ah+cf-de-bg, dg-ch).
\end{aligned}$$

Definición 3.1. Decimos que un cubo entero C es proyectivo si las tres formas binarias cuadráticas que induce, Q_1^C, Q_2^C y Q_3^C, son primitivas.

Ejemplo

Sea C el cubo de entero correspondiente a las siguientes matrices:

$$\begin{aligned}
M_1 &= \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \quad \text{y} \quad N_1 = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}. \\
M_2 &= \begin{pmatrix} 1 & 0 \\ 3 & 2 \end{pmatrix} \quad \text{y} \quad N_2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}. \\
M_3 &= \begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix} \quad \text{y} \quad N_3 = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}.
\end{aligned}$$

Entonces, las formas asociadas a este cubo son:

$$\begin{aligned}
Q_1^C &= (-2, 5, -3), \\
Q_2^C &= (-2, -3, -1), \\
Q_3^C &= (3, -7, 4),
\end{aligned}$$

que son todas primitivas, y por lo tanto C es un cubo proyectivo.

La acción de

$$\gamma = L_1 \times L_2 \times L_3 = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in \Gamma$$

en C produce el primer cambio:

$$M_1' = \begin{pmatrix} -1 & 2 \\ -2 & 3 \end{pmatrix}, \quad N_1' = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix},$$

de forma que el cubo resultante es $(-1, 2, -2, 3, 1, 1, 0, 2)$, y por tanto

$$M_2' = \begin{pmatrix} -1 & -2 \\ 1 & 0 \end{pmatrix}, \quad N_2' = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}.$$

Como L_2 deja el cubo invariante, entonces

$$M_3' = \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix}, \quad N_3' = \begin{pmatrix} -2 & 0 \\ 3 & 2 \end{pmatrix},$$

y la acción de L_3 hace

$$M_3'' = \begin{pmatrix} -4 & 2 \\ 7 & 4 \end{pmatrix}, \quad N_3'' = \begin{pmatrix} -3 & 1 \\ 5 & 3 \end{pmatrix},$$

con lo que finalmente, la acción de γ lleva C a $(-4, 7, -3, 5, 2, 4, 1, 3)$.

Proposición 3.2. *Para cualquier cubo de enteros C, se verifica*

$$Disc(Q_1^C) = Disc(Q_2^C) = Disc(Q_3^C).$$

Demostración. Dado un cubo C como en la Figura 3.1, desarrollamos los discriminante de Q_1^C, Q_2^C y Q_3^C con las expresiones obtenidas anteriormente para estas formas usando la fórmula del discriminante $b^2 - 4ac$. Unos cálculos, que se encuentran en el Apéndice A, prueban que los tres coinciden y dan como resultado

$$a^2h^2 + d^2e^2 + b^2g^2 + c^2f^2 - 2(adeh + abgh + acfh + bdeg + cdef + bcfg) + 4(bceh + adfg).$$

□

Por lo tanto, tiene sentido hablar del discriminante de un cubo de enteros, y lo denotaremos Disc(C).

3.2. Ley de Cubos

Bhargava, para asociar los cubos de enteros a la composición de formas, logró probar que la composición de Dirichlet era equivalente a la siguiente proposición:

Ley de cubos. La composición de las formas inducidas por un cubo de enteros C cumplen $[Q_1^C] \circ [Q_2^C] \circ [Q_3^C] = [Q_{id,D}]$.

Aquí, $[Q_{id,D}]$ denota la clase de la forma principal de la Definición 2.8. Más tarde, en el Teorema 3.4 demostraremos que, efectivamente, esto equivale a la composición de Dirichlet.

Veamos una consecuencia de esta ley. Si tomamos $\gamma = M \times I \times I \in \Gamma$, entonces, $\gamma * C$ induce las formas $Q_1^{\gamma * C}, Q_2^C$ y Q_3^C, y se tiene

$$[Q_1^C] \circ [Q_2^C] \circ [Q_3^C] = [Q_{id,D}] = [Q_1^{\gamma * C}] \circ [Q_2^C] \circ [Q_3^C] \Longrightarrow [Q_1^C] = [Q_1^{\gamma * C}] = [Q_1^C * M].$$

Además, la acción $I \times N \times L \in \Gamma$ deja invariante la primera forma inducida, Q_1^C. Ambas afirmaciones se pueden extender análogamente a la segunda y tercera forma inducida, Q_2^C y Q_3^C. Por lo tanto, podemos concluir que el discriminante es invariante por la acción de Γ, pues ya vimos en el Capítulo 1 que el discriminante era invariante por la acción de $SL_2(\mathbb{Z})$.

De hecho, después de probar que la Ley de Cubos equivale a la Composición de Dirichlet, veremos que, como consecuencia, el espacio de equivalencia de cubos de enteros de discriminante D, que denotaremos $C((\mathbb{Z}^2)^{\otimes 3}; D)$, forma un grupo.

Antes de ello, veamos primero cuáles son los "cubos identidad":

Definición 3.3. Dado $D \equiv 0, 1 \pmod 4$, definimos los cubos principales $A_{id,D}$ como aquellos que inducen tres formas binarias cuadráticas iguales, que además serán las formas principales definidas en la Definición 2.8. Podemos ver estos cubos principales en la Figura 3.2.

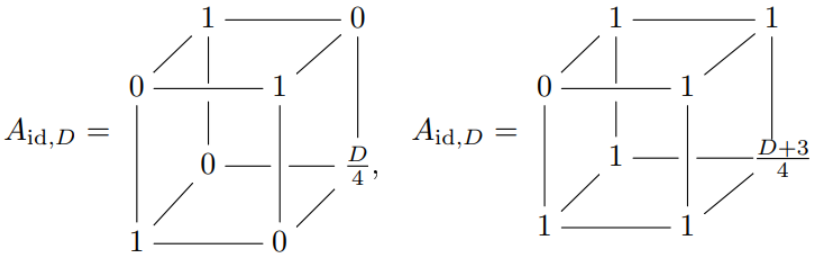

Figura 3.2: Cubos Principales

Teorema 3.4. *Sea $D \equiv 0, 1 \pmod 4$ un entero y sea $A_{id,D}$ el cubo principal, cuyas tres formas inducidas son todas $Q_{id,D}$. Entonces, existe una única ley de grupo en el conjunto de equivalencia de formas primitivas de discriminante D tal que:*

1. *$[Q_{id,D}]$ es la identidad.*
2. *Para cualquier cubo proyectivo C de discriminante D*

$$[Q_1^C] \circ [Q_2^C] \circ [Q_3^C] = [Q_{id,D}].$$

A la inversa, dadas tres formas primitivas de discriminante D, Q_1, Q_2 y Q_3 tales que $[Q_1] \circ [Q_2] \circ [Q_3] = [Q_{id,D}]$, existe un cubo C, único salvo $\Gamma-$equivalencia, tal que $Q_1 = Q_1^C, Q_2 = Q_2^C$ y $Q_3 = Q_3^C$. Si se escoge como identidad a la forma principal, esta ley de grupo es equivalente a la composición de Gauss.

Demostración. Para probar este resultado, vamos a mostrar primero que la Ley de Cubos es equivalente a la composición de Dirichlet (y por tanto a la de Gauss), y entonces el teorema es consecuencia inmediata de que G_D, como ya habíamos visto, es un grupo.

Tomamos un cubo proyectivo como en la Figura 3.1. Puesto que es primitivo, sus coeficientes son coprimos. Para ver esto, supongamos que $M = \text{mcd}(a, b, c, d, e, f, g, h)$, y por tanto M divide a $\text{mcd}(bc - ad, ed + ah - bg - fc, fg - eh) = 1$, pues son los coeficientes de Q_1^C, que es primitiva por ser C proyectivo. Esto implica entonces que $M = 1$.

Veremos ahora que existe $\gamma \in \Gamma$ que lleva nuestro cubo C a $(1, 0, 0, d, 0, f, g, h)$. Consideremos las matrices S y T^n de la demostración del Teorema 1.8.

Si $I \in SL_2(\mathbb{Z})$ es la matriz identidad, aplicando

$$S \times I \times I, \quad I \times S \times I \quad \text{o} \quad I \times I \times S$$

adecuadamente, pues estos cambian los coeficientes del cubo de orden y signo, podemos asumir que a es el menor coeficiente del cubo. Si a es coprimo con b, c o e, podemos usar el algoritmo de Euclides para encontrar una matriz en $SL_2(\mathbb{Z})$ que permita cambiar a por 1. Si no es el caso, entonces se aplica $T^n \times I \times I, I \times T^n \times I$ o $I \times I \times T^n$ para reducir b, c y e módulo a. Entonces, se puede reemplazar a por el menor coeficiente distinto de 0 y repetir el proceso.

Pararemos cuando $a = 1$, o, si esto no ocurre, cuando C sea de la forma

$$(a, 0, 0, d, 0, f, g, h).$$

En este caso, se debe dar $\text{mcd}(a, f) = 1$ para que el cubo sea proyectivo, y podemos aplicar entonces T a C para llegar a $(a, 0, d, d, f, f, g + h, g)$, y así, $\text{mcd}(a, e) = 1$. Entonces, podemos encontrar $\gamma \in \Gamma$ que reduzca a a 1, y usar entonces este 1 para reducir b, c y e a 0. De esta forma, ya tendríamos nuestro cubo equivalente $(1, 0, 0, d, 0, f, g, h)$, que induce las tres formas siguientes:

$$\begin{aligned} Q_1 &= (-d, h, fg), \\ Q_2 &= (-g, h, df), \\ Q_3 &= (-f, h, dg). \end{aligned}$$

Ahora, la Ley de Cubos implica $[Q_1] \circ [Q_2] = [Q_3]^{-1}$. Como $\text{mcd}(-d, h, fg) = 1$, entonces $\text{mcd}(d, g, h) = 1$, luego, en términos de la composición de Dirichlet,

$$[Q_1] \circ [Q_2] = [(-d, h, fg)] \circ [(-g, h, dg)] = [\left(dg, B, \frac{B^2 - (h^2 + 4dfg)}{4dg}\right)],$$

para algún $B \in \mathbb{Z}$ que verifica

$$\begin{aligned} B &\equiv h \pmod{2d}, \\ B &\equiv h \pmod{2g}, \\ B^2 &\equiv h^2 + 4dfg \pmod{4dg}. \end{aligned}$$

Claramente, $B = h$ cumple estas congruencias, por lo tanto $[Q_1] \circ [Q_2] = [(dg, h, -f)]$, pero la matriz S lleva esta forma a $[(-f, -h, dg)]$, que en términos de la composición de Dirichlet es la inversa de Q_3, y por tanto la Ley de Cubos corresponde a la composición de Dirichlet. □

Además. con este teorema podemos concluir que el conjunto de cubos de enteros forma también un grupo:

Teorema 3.5. *Sea $D \equiv 0, 1 \pmod 4$ un entero negativo y $A_{id,D}$ el cubo identidad. Entonces, existe una única operación binaria que transforma $C((\mathbb{Z}^2)^{\otimes 3}; D)$ en un grupo tal que:*

1. *$[A_{id,D}]$ es la identidad.*
2. *Para $i = 1, 2, 3$, la aplicación $[A] \longrightarrow [Q_i^A]$ es un homomorfismo de grupos del conjunto de clases de equivalencia de cubos de discriminante D a G_D.*

Demostración. Este resultado se deduce del teorema anterior, pues si A y B son dos cubos de discriminante D, como

$$([Q_1^A] \circ [Q_1^B]) \circ ([Q_2^A] \circ [Q_2^B]) \circ ([Q_3^A] \circ [Q_3^B]) = [Q_{id,D}],$$

entonces existe un cubo C de discriminante D, único salvo equivalencia, que induce las formas

$$[Q_1^A] \circ [Q_1^B], \quad [Q_2^A] \circ [Q_2^B], \quad \text{y} \quad [Q_3^A] \circ [Q_3^B].$$

Así, definimos la operación entre $[A]$ y $[B]$ como $[A] + [B] = [C]$.

Como además sabemos que $A_{id,D}$ da lugar a tres formas $Q_{id,D}$, que es la identidad de G_D, entonces $[A_{id,D}]$ es la identidad del grupo de cubos. □

Gracias a estos teoremas, podemos componer sin problema las formas inducidas por un cubo. Sin embargo, lo normal es no tener un cubo, sino tan solo dos formas que se quieren componer, así que la pregunta ahora es: dadas dos formas, ¿podemos encontrar un cubo que las induzca? La respuesta es sí:

Teorema 3.6. *Dado $D \equiv 0, 1 \pmod 4$, para cualquier pareja de formas (a, b, c) y (a', b', c') de discriminante D existe un cubo C tal que $Q_1^C = (a, b, c)$ y $Q_2^C = (a', b', c')$.*

Si además, $aa' \neq 0$ y $e = \operatorname{mcd}\left(a, a, \frac{b+b'}{2}\right)$, existen soluciones enteras para f y g de la ecuación

$$\frac{a'f - ag}{e} = \frac{b - b'}{2}$$

de forma que si se define

$$h = \frac{-f\frac{b+b'}{2} - ec'}{a},$$

h es entero. Además, para tales f, g, h, el cubo $(0, \frac{a}{e}, e, f, \frac{a'}{e}, \frac{b+b'}{-2e}, g, h)$ da lugar a las formas (a, b, c) y (a', b', c').

Demostración. Suponemos, sin perdida de generalidad, que $a' \neq 0$ (siempre se puede encontrar una forma equivalente que cumpla esta condición). Sea C el cubo

$$\left(0, \frac{a}{e}, e, f, \frac{a'}{e}, \frac{b+b'}{-2e}, g, h\right),$$

y $(M_i, N_i), i = 1, 2, 3$ las matrices de sus cortes fundamentales. C induce las formas

$$Q_1^C = \left(a, \frac{b+b'}{2} + \frac{a'f}{e} - \frac{ag}{e}, \frac{-a'h}{e} - g\frac{b+b'}{2e}\right),$$
$$Q_2^C = \left(a', \frac{b+b'}{2} - \frac{a'f}{e} + \frac{ag}{e}, \frac{-ah}{e} - f\frac{b+b'}{2e}\right).$$

El primer coeficiente en ambos casos ya es el que queremos. Igualando los segundos coeficientes a b y b', respectivamente, se obtiene en ambos casos la misma ecuación,

$$\frac{b-b'}{2} = \frac{a'}{e}f - \frac{a}{e}g. \tag{3.2}$$

Por la identidad (2.17) del Lema 2.10, $ac - a'c' = \frac{b+b'}{2}\frac{b-b'}{2}$, y como, por hipótesis, $\operatorname{mcd}\left(\frac{a}{e}, \frac{a'}{e}, \frac{b+b'}{2e}\right) = 1$, entonces $\operatorname{mcd}\left(\frac{a}{e}, \frac{a'}{e}\right)$ divide a $\frac{b-b'}{2}$, y el algoritmo de Euclides nos permite encontrar f y g que satisfagan (3.2).

Ahora, se necesita para el tercer coeficiente

$$\frac{-g\frac{b+b'}{2} - a'h}{e} = c \quad \text{y} \quad \frac{-f\frac{b+b'}{2} - ah}{e} = c'.$$

Usando que

$$\frac{b^2 - b'^2}{4} = ac - a'c' \quad \text{y} \quad f = \frac{ag}{a'} - \frac{e(b-b')}{2a'}.$$

se tiene

$$h = \frac{-f\frac{b+b'}{2} - ec'}{a} = \frac{-ag\frac{b+b'}{2}}{aa'} - \left(\frac{b^2-b'^2}{4}\right)\left(\frac{e}{aa'}\right) - \frac{ec}{a}$$
$$= \frac{-g\frac{b+b'}{2}}{a'} - \frac{e(ac-a'c') - aec}{aa'} = \frac{-g\frac{b+b'}{2} - ec'}{a'}.$$

Ahora, si h es un entero, hemos terminado. Si no, como

$$\frac{-ah}{e} = \frac{\frac{b+b'}{2}g}{e} - c \in \mathbb{Z},$$

y lo mismo se da para $\frac{-a'h}{e}$, luego el denominador de h divide a $\operatorname{mcd}\left(\frac{a'}{e}, \frac{a}{e}\right) = \alpha$ y podemos escribir $h = \frac{H}{\alpha}$, con $H \in \mathbb{Z}$. Como además, $\operatorname{mcd}\left(\alpha, \frac{b+b'}{2e}\right) = 1$, existe $r \in \mathbb{Z}$ tal que $r\frac{b+b'}{2e} \equiv H \pmod{\alpha}$. Sea

$$N_1' = \begin{pmatrix} e' & g' \\ f' & h' \end{pmatrix} = N_2 - \begin{pmatrix} r \\ \alpha \end{pmatrix} M_2 = \begin{pmatrix} e & f - \frac{ra}{\alpha e} \\ g - \frac{ra'}{\alpha e} & h - \frac{r(b+b')}{2e\alpha} \end{pmatrix},$$

y entonces, como $\frac{a}{e}$ y $\frac{a'}{e}$ son divisibles por α, $e' = e, f'$ y g' son todos enteros.

Además,

$$h' = h - \frac{r(b+b')}{2e\alpha} = \frac{H - r\frac{b+b'}{2e}}{\alpha} \in \mathbb{Z}$$

como se buscaba, y hemos construido un cubo equivalente que da lugar a nuestras dos formas binarias cuadráticas. □

Veamos un ejemplo práctico de este teorema. Si consideramos las dos formas reducidas de G_{-12}, que son $Q_1 = (1, 0, 3)$ y $Q_2 = (2, 2, 2)$, entonces tendríamos que encontrar dos enteros f y g tales que

$$2f - g = -1 \quad \text{y} \quad h = -f - 2.$$

Si tomamos $f = 1$ y $g = 3$, entonces $h = -3$. Por lo tanto, el cubo que define estas formas sería $C = (0, 1, 1, 1, 2, -1, 3, -3)$. Efectivamente, las formas generadas por este cubo verifican $Q_1^C = Q_1$ y $Q_2^C = Q_2$, y además, $Q_3^C = (2, -6, 6)$. Por lo tanto, la Ley de Cubos implica que

$$[(1, 0, 3)] \circ [(2, 2, 2)] = [(2, -6, 6)]^{-1} = [(2, 6, 6)].$$

Proposición 3.7. *El inverso de la clase de equivalencia del cubo*

$$A = (a, b, c, d, e, f, g, h)$$

es la clase que contiene a

$$-A = (a, -b, -c, d, -e, f, g, -h).$$

Demostración. En términos de la composición de Dirichlet, se tiene que $[Q_1^A] = [Q_1^{-A}]^{-1}$ y $[Q_2^A] = [Q_2^{-A}]^{-1}$, por lo que

$$[Q_1^A] \circ [Q_1^{-A}]^{-1} = [Q_2^A] \circ [Q_2^{-A}]^{-1} = [Q_{id,D}],$$

y el Teorema 3.5 junto al Teorema 3.6 implican $[A] + [-A] = [A_{id,D}]$. □

Uno de los aspectos más interesantes de este versión de la composición de formas es que es generalizable a otras dimensiones. Aunque en este trabajo nos hemos centrado en las formas binarias cuadráticas, Bhargava explica en su tesis cómo generalizar la Ley de Cubos a dimensiones más altas.

APÉNDICE A
Cálculos adicionales

En este apéndice se recogen algunos cálculos adicionales necesarios para completar algunas demostraciones.

Cálculos en la demostración de la Proposición 2.7

Desarrollamos $F(X,Y)$:

$$F(X,Y) = aa'x^2z^2 + aa'C^2y^2w^2 - 2aa'Cxyzw + aBx^2zw + \\ + a'Bxyz^2 + B^2xyzw - aBCxyw^2 - a'BCy^2zw - B^2Cy^2w^2 + \\ + Ca^2x^2w^2 + a'^2Cy^2z^2 + CB^2y^2w^2 + 2aa'Cxyzw + 2aBCxyw^2 + \\ + 2a'BCy^2zw = aa'(x^2z^2 + C^2Y^2W^2) + B(ax^2zw + a'xyz^2 + Bxyzw) + \\ + C(a^2x^2w^2 + a'^2y^2z^2) + aBCxyw^2 + a'BCy^2zw.$$

Ahora, veamos que coincide con $f(x,y)\cdot g(z,w)$:

$$f(x,y)\cdot g(z,w) = (ax^2 + Bxy + a'Cy^2)\cdot(a'z^2 + Bzw + aCw^2) = \\ = aa'\cdot x^2z^2 + aa'\cdot C^2y^2w^2 + B\cdot ax^2zw + B\cdot a'xyz^2 + B\cdot Bxyzw + \\ + C\cdot a^2x^2w^2 + C\cdot a'^2y^2z^2 + a'BCy^2zw + aBCxyw^2 = F(X,Y).$$

Cálculos en la demostración del Lema 2.12

Comprobamos la primera de las identidades:

$$2a\alpha + (b+b')\gamma - 2a'\delta \overset{(2.21)}{=} 2a\alpha + b\gamma + 2a\alpha\beta\gamma + b\beta\gamma^2 + 2c\delta\gamma^2 + b\alpha\gamma\delta - 2a'\delta = \\ 2a\alpha(1+b\gamma) + b\gamma(1+\beta\gamma+\alpha\delta) + 2c\delta\gamma^2 - 2a'\delta \overset{(2.20)}{=} \\ 2a\alpha^2\delta + 2b\alpha\gamma\delta + 2c\gamma^2\delta - 2a'\delta = 2\delta(f(\alpha,\gamma) - a') \overset{(2.19)}{=} 0.$$

Ahora, pasamos a comprobar la segunda de las identidades:

$$(b-b')\alpha+2c\gamma+2a'\beta \overset{(2.21)}{=} b\alpha-2a\alpha^2\beta-b\alpha\beta\gamma-2c\alpha\gamma\delta-b\alpha^2\delta+2c\gamma+2a'\beta=$$
$$b\alpha(1-\beta\gamma-\alpha\delta)+2c\gamma(1-\alpha\delta)-2a\alpha^2\beta+2a'\beta \overset{(2.20)}{=}$$
$$-2b\alpha\beta\gamma-2c\gamma^2\delta-2a\alpha^2\beta+2a'\beta \overset{(2.19)}{=} 2\beta(a'-f(\gamma,\delta))=0.$$

Cálculos en la demostración de la Proposición 3.2

Calculemos el discriminante de las tres formas que induce el cubo C para ver que son el mismo:

$$\begin{aligned}\mathrm{Disc}(Q_1^C)&=a^2h^2+d^2e^2+b^2g^2+c^2f^2-\\&\quad-2(-adeh+abgh+acfh+bdeg+cdef-bcfg)\\&\quad-4(bcfg+adeh-bceh-adfg)=a^2h^2+d^2e^2+b^2g^2+c^2f^2-\\&\quad-2(adeh+abgh+acfh+bdeg+cdef+bcfg)+4(bceh+adfg).\end{aligned}$$

$$\begin{aligned}\mathrm{Disc}(Q_2^C)&=a^2h^2+d^2e^2+b^2g^2+c^2f^2-\\&\quad-2(adeh-abgh+acfh+bdeg-cdef+bcfg)\\&\quad-4(cdef+abgh-bceh-adfg)=a^2h^2+d^2e^2+b^2g^2+c^2f^2-\\&\quad-2(adeh+abgh+acfh+bdeg+cdef+bcfg)+4(bceh+adfg).\end{aligned}$$

$$\begin{aligned}\mathrm{Disc}(Q_3^C)&=a^2h^2+d^2e^2+b^2g^2+c^2f^2-\\&\quad-2(adeh+abgh-acfh-bdeg+cdef+bcfg)\\&\quad-4(bdeg+acfh-bceh-adfg)=a^2h^2+d^2e^2+b^2g^2+c^2f^2-\\&\quad-2(adeh+abgh+acfh+bdeg+cdef+bcfg)+4(bceh+adfg).\end{aligned}$$

Cálculos en la demostración de la relación de equivalencia entre cubos de enteros

Lo único que faltaba por ver era que

$$U=\begin{pmatrix}aa'+cb' & ba'+db'\\ ac'+cd' & bc'+dd'\end{pmatrix}\in SL_2(\mathbb{Z}).$$

Para ello, tenemos que comprobar que el determinante de U es 1 :

$$\begin{aligned}(aa'+cb')(bc'+dd')-(ba'+db')(ac'+cd')=&\\ aba'c'+ada'd'+bcb'c'+cdb'd'-&\\ aba'c'-bca'd'-adb'c'-cdb'd'=&\\ ad(a'd'-b'c')+bc(b'c'-a'd')=ad-bc=1,&\end{aligned}$$

donde en las dos últimas igualdades se ha usado que $ad-bc=a'd'-b'c'=1$.

Bibliografía

[1] Bhargava, M. Higher Compositions Laws, PhD Thesis, *Princeton University*, (June, 2001).

[2] Bhargava, M. Higher Compositions Laws I: A New View on Gauss Composition and Quadratic Generalizations, *Annals of Mathematics*, Vol. 159, pp.217-250, (2004).

[3] Bouyer, F. Composition and Bhargava's Cubes (2012). https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/gauss_composition.pdf.

[4] Chamizo, F.: Ocho lecciones de teoría de números (2011). https://matematicas.uam.es/~fernando.chamizo/libreria/fich/lecc8.pdf.

[5] Cox, D. A.: Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication, *John Wiley*, (1989).

[6] Diofanto de Alejandría: La Aritmética y el Libro sobre los Números Poligonales, *Versión en castellano, introducción, notas y apéndices de Manuel Benito Muñoz, Emilio Fernández Moral y Mercedes Sánchez Benito. Nivola, Primera Edición* (2007).

[7] Euler, L.: Elements of Algebra, *Traducido por Rev. John Hewlett, B.D. F.A.S. Con introduccion de C. Truesdell. Springer* (1972).

[8] Gauss, C. F.: Disquisitiones Arithmeticae (Spanish), *Enrique Pérez Arbeláez Collection, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá; Traducido del latín por Hugo Barrantes Campos, Michael Josephy y Ángel Ruíz Zúñiga; con un prefacio por Ruíz Zúñiga,* **10** (1995).

[9] Lagrange, J. L.: Recherches d'Arithmétique, *Nouv. Mém. Acad. Sci.* (1773).

[10] Legendre A. M.: Essai sur la Théorie des Nombres, *Third edition retitled Théorie des Nombres,* Paris (1788).

[11] Legendre, A. M.: Recherches d'analyse indéterminée, *Histoire de l'Académie Royale des Sciences, 1785* pp. 465-559 (1788).

[12] Lemmermeyer, F.: Binary Quadratic Forms. An Elementary Approach to the Arithmetic of Elliptic and Hyperelliptic Curves (2010), http://www.rzuser.uni-heidelberg.de/~hb3/.

[13] Pisano, L. (Fibonacci): The Book of Squares, *An Annotation Translation into Modern English by L.E. Sigler* (1987).

[14] Séguin, F.: Composition of Binary Quadratic Forms. *Reson 24, 633–651* (2019). https://doi.org/10.1007/s12045-019-0822-4

[15] Weil, A.: Number Theory: An Approach Through History, *Birkhaüser, Boston, Basel and Stuttgart* (1984).