Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Teoría de géneros de formas cuadráticas

Trabajo de fin de grado

Grado en Matemáticas

Autor: Laura Carralero Llano
Tutor: Enrique González Jiménez

Curso 2022-2023

Resumen

A mediados del Siglo XVII, Fermat conjetura cuando un primo puede escribirse como suma de dos cuadrados, a raíz de esto muchos grandes matemáticos como Euler, Lagrange y Legendre comenzaron a preguntarse qué primos eran representados como x^2+ny^2, donde n podía ser cualquier entero. Para dar respuesta a esto se dieron cuenta de que sería útil plantearse algo incluso más general, qué números son representados por una forma cuadrática $ax^2 + bxy + cy^2$ con discriminante $D = b^2 - 4ac$.

Este trabajo busca responder a la pregunta planteada a través de la Teoría de géneros, que fue introducida por Gauss en *Disquisitiones Arithmeticae* y consigue determinar qué unidades módulo D representarán las formas cuadráticas con este mismo discriminante. Para introducirnos en ella, antes debemos profundizar en las formas cuadráticas y desarrollar una teoría en base a sus propiedades. Una vez entendamos su funcionamiento nos introduciremos en la Teoría de géneros, primero desde un enfoque moderno y finalmente desde el ingenioso enfoque de Gauss.

Abstract

Since Fermat postulated whether a prime could be written as sum of two squares, many important Mathematicians like Euler, Lagrange and Legendre wondered which primes could be written as $x^2 + ny^2$ for n any integer. To answer this question, they realize it would be useful to generalize even more and investigate which numbers are represented by a quadratic form $ax^2 + bxy + cy^2$ with discriminant $D = b^2 - 4ac$.

The purpose of this thesis is to answer that question using Genus Theory. This theory was first introduced by Gauss in *Disquisitiones Arithmeticae* and its aim is to determine which units modulo D can be represented by a form with this discriminant. To begin with, we will study Binary Quadratic forms and develop some important results based on their properties. Once we acquire some knowledge about them, we will focus on studying Genus theory, first from a modern perspective and finally from the ingenious point of view of Gauss.

Índice general

Introducción

A mediados del Siglo XVII, el matemático Pierre de Fermat plantea, sin dar una demostración, las siguientes conjeturas siendo p un primo impar cualquiera:

$$\begin{array}{rcl} p = x^2 + y^2, \quad x, y \in \mathbb{Z} & \iff & p \equiv 1 \pmod 4, \\ p = x^2 + 2y^2, \ x, y \in \mathbb{Z} & \iff & p \equiv 1, 3 \pmod 8, \\ p = x^2 + 3y^2, \ x, y \in \mathbb{Z} & \iff & p = 3 \text{ o } p \equiv 1 \pmod 3. \end{array}$$

Podría decirse que este es el comienzo de la Teoría de géneros, pues a raíz de este planteamiento, varios matemáticos importantes como Euler, Lagrange y Legendre, buscaron no solo la demostración de estos teoremas sino también la generalización de este concepto. Es decir, buscaban saber qué primos podían representarse como $x^2 + ny^2$ donde n es cualquier entero positivo.

Con este objetivo, Lagrange introduce por primera vez en *Recherches d'Arithmétique* [6] las formas cuadráticas, que son polinomios de la forma $f(x, y) = ax^2+bxy+cy^2$, con a, b, c enteros, donde define su discriminante como $D = b^2 - 4ac$ y expone una relación de equivalencia entre ellas (nos fijamos en que x^2+ny^2 es una forma cuadrática de discriminante $D = -4n$). Por ello dedicaremos el primer capítulo a la Teoría de formas cuadráticas. Primero estudiaremos una relación de equivalencia entre formas de un mismo discriminante, y clasificaremos nuestras formas en las distintas clases de equivalencia. Una vez definida esta relación, introducimos la siguiente operación entre clases de formas cuadráticas: dadas dos formas cuadráticas f y g de discriminante D conseguimos otra forma F con el mismo discriminante definida como:

$$f(x, y) \cdot g(w, z) = F(B_1(x, y; z, w), B_2(x, y; z, w)),$$

con $B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw \ i = 1, 2$, formas bilineales.
Así, si conocemos qué primos representan f y g, esto nos permitirá conocer los enteros representados por F. Como es natural pensar, esta noción introducida por primera vez por Legendre y perfeccionada por Gauss dio un empujón a la Teoría de géneros consiguiendo resolver conjeturas más generales, como por ejemplo:

$$p, q \equiv 3, 7 \pmod{20} \to pq = x^2 + 5y^2 \qquad \text{(Fermat)},$$

$$p \equiv 3, 7 \pmod{20} \to 2p = x^2 + 5y^2 \qquad \text{(Euler)}.$$

En este primer capítulo desarrollaremos una composición equivalente: la composición de Dirichlet, la cual proporciona una fórmula general para $F = f \circ g$. Una vez definida,

dedicaremos una sección para ver que esta operación proporciona a las clases de formas cuadráticas de un discriminante $D < 0$ fijo una estructura de grupo abeliano finito. Además, le dedicaremos también otra sección a resultados de representación de enteros mediante formas cuadráticas, donde la Ley de reciprocidad cuadrática[1] irá ganando protagonismo.
Con la introducción de formas cuadráticas y la implicación de tantos matemáticos para resolver las conjeturas sobre primos de la forma $p = x^2 + ny^2$, se va creando una teoría que poco a poco va cogiendo forma. La pregunta que nos hacemos es la siguiente: cuándo surge la Teoría de géneros y qué es exactamente.
En 1801 se publica *Disquisitiones Arithmeticae* [5], donde Gauss no sólo reúne toda la Teoría de Números expuesta hasta entonces, sino que aporta nuevos conceptos y teoremas de gran profundidad y complejidad matemática[2]. En este libro, entre los artículos 229 y 287, aparece la Teoría de géneros: Gauss observa que dada una forma cualquiera de discriminante D, los números representados por ella guardan una relación estrecha si tomamos sus clases módulo los divisores primos de D. A raíz de este concepto define una serie de caracteres con los que clasifica a las formas de discriminante D en los llamados géneros. Es decir, la Teoría de géneros logra acotar qué posibles enteros representa una forma cuadrática, dando respuesta a muchas de las conjeturas anteriores.

En el segundo capítulo nos sumergimos en la Teoría de géneros desde un enfoque moderno. Primero definiremos un homomorfismo $\chi_D : U(\mathbb{Z}/D\mathbb{Z}) \to \{\pm 1\}$, cuyo núcleo contiene a todas las unidades módulo D representadas por formas con este discriminante. En especial, veremos que las unidades representadas por una forma concreta $f_0(x, y)$ forman un subgrupo del $\ker(\chi_D)$, y en función de ello asignamos a $f_0(x, y)$ un género u otro. Una vez asentada la definición, nos centraremos en los discriminantes fundamentales y buscaremos una fórmula para el número de géneros, a la vez que entendemos su estructura interna. A continuación, demostraremos uno de los teoremas más importantes de géneros, el Teorema de Duplicación de Gauss. En toda esta sección intentaremos aplicar los resultados a las formas con discriminante negativo, que son las que habremos estudiado en la primera sección.

La penúltima sección la dedicaremos a entender esta teoría desde su enfoque inicial, mediante la definición de caracteres que introdujo Gauss en *Disquisitiones Arithmeticae*. Esta se basa en clasificar las formas cuadráticas de discriminante D fijo en clases de equivalencia módulo p primo. En función a ello, podremos ver que una forma de discriminante D solo puede representar restos cuadráticos (o no restos cuadráticos) módulo $p \mid D$ primo impar, independientemente de si el discriminante es positivo o negativo. Finalmente para concluir demostraremos aquellas tres primeras conjeturas que dieron lugar a toda esta teoría.

[1] Esta ley era considerada por Gauss uno de los teoremas más importantes de *Disquisitiones Arithmeticae*, de hecho él mismo lo llamó *Aureum Theorema* (el Teorema de oro). Aunque Euler, y Legendre ya la habían mencionado anteriormente, fue Gauss quién consiguió dar una demostración completa, incluso de 8 maneras distintas.

[2] Hasta entonces toda la Teoría de Números se encontraba en distintos ensayos y publicaciones inconexas, por ello muchos consideran que con este libro se inicia realmente esta teoría, pues será la base de muchos matemáticos que deciden adentrarse en este área durante los siglos XIX y XX. Por ejemplo, se dice que Dirichlet tenía siempre una copia de *Disquisitiones Arithmeticae* en su escritorio.

CAPÍTULO 1
Formas cuadráticas

Comenzamos introduciendo qué son las formas cuadráticas y nos sumergiremos en varios resultados relativos de dicha teoría. En este capítulo, podemos encontrar los resultados expuestos en los libros [3], [1] y [4].

Definición 1.1. *Una forma cuadrática es un polinomio de la forma* $ax^2 + bxy + cy^2$*, donde* a, b, c *son enteros. Definimos su discriminante como* $D = b^2 - 4ac$*. Diremos que una forma es primitiva si* $mcd(a, b, c) = 1$ *y denotaremos esta forma como* (a, b, c) *cuando sea conveniente.*

Toda forma cuadrática $f(x, y) = ax^2 + bxy + cy^2$ admite una expresión matricial:

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Observación 1.2. *Sea* D *el discriminante de una forma cuadrática* (a, b, c)*. Como* $D \equiv b^2 \pmod 4$*, entonces* $D \equiv 0, 1 \pmod 4$*.*

Definición 1.3. *Dado un entero* m*, decimos que* m *es representado por una forma* $f(x, y)$ *si existen* $p, r \in \mathbb{Z}$ *tales que* $f(p, r) = m$*. En el caso en el que* $mcd(p, r) = 1$*, entonces diremos que* m *es propiamente representado por* $f(x, y)$*.*

Dada una forma cuadrática $f(x, y) = (a, b, c)$ con discriminante D se tiene que:

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

En consecuencia, si D es positivo $f(x, y)$ podrá tomar valores positivos y negativos. Mientras que si el discriminante es negativo, $f(x, y)$ representa enteros positivos si $a > 0$ y enteros negativos si $a < 0$. A raíz de este resultado podemos definir lo siguiente:

Definición 1.4. *Sea* $f(x, y) = (a, b, c)$ *una forma de discriminante* D*. Si* $D > 0$ *diremos que* $f(x, y)$ *es indefinida. Si* $D < 0$ *entonces diremos que* $f(x, y)$ *es definida positiva si* $a > 0$ *y definida negativa si* $a < 0$*.*

1.1. Equivalencias de formas cuadráticas

Ahora ya conociendo las definiciones básicas, definimos una relación de equivalencia entre las formas cuadráticas de discriminante D:

Definición 1.5. *Decimos que dos formas $f(x,y)$ y $g(x,y)$ son equivalentes si existen enteros p,q,r,s tales que:*

$$f(x,y) = g(px+qy, rx+sy), \qquad ps - qr = \pm 1.$$

Serán propiamente equivalentes si $ps - qr = 1$; en este caso usaremos la siguiente notación: $f(x,y) \sim g(x,y)$. Si F y G son las respectivas matrices asociadas a las formas $f(x,y)$ y $g(x,y)$, entonces:

$$(x \quad y)\, F \begin{pmatrix} x \\ y \end{pmatrix} = (x \quad y)\, M^t G M \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{con } M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}. \tag{1.1}$$

Proposición 1.6. *La relación definida entre formas cuadráticas es una relación de equivalencia.*

Demostración. Dada una forma cuadrática $f(x,y)$ es (propiamente) equivalente a ella misma por la matriz identidad. Para probar la transitividad consideramos tres formas $f(x,y) = (a_1, b_1, c_1)$, $g(x,y) = (a_2, b_2, c_2)$, $h(x,y) = (a_3, b_3, c_3)$, tales que $f(M(x,y)) = g(x,y)$ con $det(M) = \pm 1$ y $g(M'(x,y)) = h(x,y)$ con $det(M') = \pm 1$. Si las matrices son de la forma:

$$M = \begin{pmatrix} p_1 & q_1 \\ r_1 & s_1 \end{pmatrix}, \quad M' = \begin{pmatrix} p_2 & q_2 \\ r_2 & s_2 \end{pmatrix},$$

entonces:

$$\begin{aligned} g(x,y) &= a_1(p_1x + q_1y)^2 + b_1(p_1x + q_1y)(r_1x + s_1y) + c_1(r_1x + s_1y)^2, \\ h(x,y) &= a_1(p_1(p_2x + q_2y) + q_1(r_2x + s_2y))^2 + b_1(p_1(p_2x + q_2y) + q_1(r_2x + s_2y)) \\ &\quad (r_1(p_2x + q_2y) + s_1(r_2x + s_2y)) + c_1(r_1(p_2x + q_2y) + s_1(r_2x + s_2y))^2 \\ &= a_1((p_1p_2 + q_1r_2)x + (p_1q_2 + q_1s_2)y)^2 + b_1((p_1p_2 + q_1r_2)x + (p_1q_2 + q_1s_2)y) \\ &\quad ((r_1p_2 + s_1r_2)x + (r_1q_2 + s_1s_2)y) + c_1((r_1p_2 + s_1r_2)x + (r_1q_2 + s_1s_2)y)^2. \end{aligned}$$

Por tanto, podemos escribir $h(x,y) = f(M''(x,y))$ siendo

$$M'' = \begin{pmatrix} p_3 & q_3 \\ r_3 & s_3 \end{pmatrix} = \begin{pmatrix} p_1 & q_1 \\ r_1 & s_1 \end{pmatrix} \begin{pmatrix} p_2 & q_2 \\ r_2 & s_2 \end{pmatrix},$$

con $det(M'') = p_3s_3 - q_3r_3 = \pm 1$ (si ambos fuesen 1 entonces $g \sim f$ y $h \sim g$ implicaría $h \sim f$). Finalmente para ver que es una relación simétrica, se puede comprobar que si:

$$f(x,y) = g\left(M \begin{pmatrix} x \\ y \end{pmatrix}\right), \qquad det(M) = \pm 1,$$

entonces M es invertible y por tanto,

$$g(x,y) = f\left(M^{-1} \begin{pmatrix} x \\ y \end{pmatrix}\right), \qquad \text{con } det(M) = det(M^{-1}).$$

□

Proposición 1.7. *Sean $f(x,y)$ y $g(x,y)$ dos formas cuadráticas propiamente equivalentes. Se cumplen las siguientes propiedades:*

I. *Tienen el mismo discriminante.*

II. *Representan los mismos enteros.*

III. *Si una de ellas es primitiva entonces ambas son primitivas.*

Demostración. Sean F y G las matrices asociadas a las formas $f(x,y) = (a,b,c)$ y $g(x,y) = (a',b',c')$ del enunciado, y sean p,q,r,s los enteros tales que $ps - qr = 1$ y $g(x,y) = f(px+qy, rx+sy)$. Nos fijamos en que el discriminante de $f(x,y)$ es $-4det(F)$. Apoyándonos en la igualdad (1.1), vemos que $det(F) = (ps-qr)^2 det(G)$; por tanto los discriminantes de $f(x,y)$ y $g(x,y)$ han de ser iguales.

La segunda parte es directa, pues si $f(x,y)$ representa a un entero m, existen enteros k,l tales que $f(k,l) = m$, y entonces $g(pk+ql, rk+sl) = m$. Finalmente, se puede comprobar que se tiene la siguiente igualdad:

$$g(x,y) = f(p,r)x^2 + (2apq + bps + bqr + 2crs)xy + f(q,s)y^2, \tag{1.2}$$

y por tanto:

$$\begin{cases} a' = & f(p,r) = ap^2 + bpr + cr^2, \\ b' = & 2apq + bps + bqr + 2crs, \\ c' = & f(q,s) = aq^2 + bqs + cs^2. \end{cases}$$

Por lo que si $f(x,y)$ no es primitiva, existe $l \neq 1$ que divide a a,b y c. En este caso l divide a a',b' y c' también, por lo que $g(x,y)$ no sería primitiva. Utilizando la simetría de la relación conseguiríamos la otra dirección. □

1.1.1. Formas definidas positivas

Una vez definida la relación de equivalencia, fijamos un discriminante $D < 0$. Vamos a clasificar las formas cuadráticas de discriminante D en clases, y veremos que solo hay un número finito de estas. Primero daremos una definición que nos permitirá llegar a este resultado:

Definición 1.8. *Sea $f(x,y) = ax^2 + bxy + cy^2$ una forma primitiva, definida positiva de discriminante D. Diremos que $f(x,y)$ es una forma reducida si cumple $|b| \leq a \leq c$ y si $|b| = a$ o $a = c$ entonces $b \geq 0$.*

Proposición 1.9. *Toda forma primitiva, definida positiva es propiamente equivalente a una forma reducida.*

Demostración. Sea $f(x,y) = (a,b,c)$ y sea F la matriz asociada a esta forma. Consideramos las siguientes matrices:

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad V^+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad V^- = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},$$

con determinante 1. Aplicaremos las matrices U, V^+ y V^- a $f(x,y)$ hasta llegar a una forma reducida propiamente equivalente. Aplicando la matriz U obtenemos

$$U^tFU = \begin{pmatrix} c & -\frac{b}{2} \\ -\frac{b}{2} & a \end{pmatrix},$$

que intercambia los coeficientes a y c, por tanto si $a > c$ podemos obtener una forma equivalente $g(x,y) = f(U(x,y))$ con $a < c$. Por otro lado, si $|b| \geq a$, podemos disminuir el valor de b. Observamos que

$$(V^+)^tFV^+ = \begin{pmatrix} a & a+\frac{b}{2} \\ a+\frac{b}{2} & a+b+c \end{pmatrix} \qquad \text{y} \qquad (V^-)^tFV^- = \begin{pmatrix} a & -a+\frac{b}{2} \\ -a+\frac{b}{2} & a-b+c \end{pmatrix}$$

es decir, aplicando V^+ o V^- llevamos $b/2$ en $b/2+a$ o $b/2-a$ respectivamente y a se mantiene constante en ambas. Así en un número finito de pasos podemos ir reduciendo el valor de b hasta llegar a que $f(x,y)$ es equivalente a una forma con $|b| \leq a$. Si tenemos el caso en el que $|b| = a$ y $b \leq 0$, aplicando V^+ llegamos a que $b = a \geq 0$, y por tanto, a una forma reducida. Si $a = c$ y $b \leq 0$ entonces aplicamos la matriz U llegando a una forma reducida. □

Proposición 1.10. *Dos formas reducidas de discriminante D no pueden ser propiamente equivalentes.*

Demostración. Sean $f = (a,b,c)$ y $g = (d,e,h)$ dos formas reducidas equivalentes. Sin pérdida de generalidad, suponemos $a \geq d$. Como $g(1,0) = d$, existen u,t enteros tales que $d = f(t,u) \geq a(t^2+u^2) + btu \geq a(t^2+u^2) - a|tu| \geq a|tu|$. Por tanto solo se pueden dar dos casos: $|tu| = 0$ o 1. Antes de comenzar los cálculos recordamos que $g(x,y) = f(px+qy, rx+sy)$ con p,q,r,s enteros tales que $ps - qr = 1$, y esto nos da la siguiente igualdad :

$$g(x,y) = f(p,r)x^2 + (2apq + bps + bqr + 2crs)xy + f(q,s)y^2. \tag{1.3}$$

Empezamos el análisis: si $u = 0$ se tiene que $d = f(t,0) = at^2$ y por tanto $t = \pm 1$ y $a = d$. Gracias a (1.3) vemos que $f(p,r) = d = a$ y como $f(\pm 1, 0) = a$ entonces $p = \pm 1$ y $r = 0$, por lo que $ps = 1$. Igualamos los coeficientes que multiplican a xy en (1.3) y obtenemos:

$$e = 2apq + bps + bqr + 2crs = b \pm 2aq.$$

Como $g(x,y)$ es reducida teníamos que $|e| \leq d = a$ y como $|b| \leq a$ solo se pueden dar los casos $q = 0$, que implicaría $b = e$ y por tanto, al conservarse el discriminante, $f(x,y) = g(x,y)$. La otra posibilidad sería $q = \pm 1$ y $b = a$, en este caso llegamos a una contradicción pues tendríamos que $e = -a = -d < 0$ y $g(x,y)$ es reducida.
Para $u = 0$, $f(x,y)$ es única. Si $t = 0$, la prueba es análoga. En el caso en que $|tu| = 1$, se tiene que $a = d$ y repetimos el mismo proceso hasta llegar a que $f = g$. □

De ambas proposiciones obtenemos de forma directa el siguiente resultado:

Corolario 1.11. *Toda forma de discriminante D primitiva definida positiva es equivalente a una única forma reducida.*

A partir de aquí es fácil ver que dado un discriminante D negativo, el número de clases de formas es finito. Sabemos que en cada clase hay una forma reducida, si $f(x,y) = (a,b,c)$ es reducida, entonces $b^2 \leq a^2$ y $a \leq c$ y se tiene:

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

Por tanto $0 < a < \sqrt{-D/3}$. Por lo que va a existir un número finito de posibilidades para a, también para b, pues $|b| \leq a$, y para c, que queda completamente determinado por a, b y D. Es decir, el número de formas reducidas es finito y por la Proposición 1.9 también lo es el número de clases de discriminante $D < 0$. Veamos un par de ejemplos:

Ejemplo 1.12. *Para $D = -20$ buscamos las posibles formas reducidas. Tenemos $D = b^2 - 4ac \leq a^2 - 3a^2$. Por lo que $a^2 \leq 6$ y además b es par. Para $a = 1$, la única forma reducida posible es si $b = 0$, es decir, $x^2 + 5y^2$. Si $a = 2$, las posibilidades de b son 0 y 2. Llegamos a que solo puede haber otra forma con la siguiente expresión: $2x^2 + 2xy + 3y^2$.*

Ejemplo 1.13. *Para $D = -56$, con el mismo procedimiento nos quedaría $a^2 \leq 18$ y b par. Si $a = 1$, la única forma reducida sería con $b = 0$, es decir, $x^2 + 14y^2$. Para $a = 2$, se tiene $2x^2 + 7y^2$, para $a = 3$ hay dos posibilidades: $3x^2 \pm 2xy + 5y^2$ y para $a = 4$ comprobaríamos que no existe ninguna forma reducida.*

Definición 1.14. *Fijado $D \equiv 0, 1 \pmod 4$ negativo, diremos que dos formas pertenecen a la misma clase si son propiamente equivalentes y denotamos al número de clases de formas primitivas definidas positivas de discriminante D como $h(D)$.*

Hemos demostrado lo siguiente:

Lema 1.15. *Fijado $D < 0$. Entonces $h(D)$ es finito y es igual al número de formas reducidas de discriminante D.*

1.2. Representaciones dada una forma

Vamos a ver una serie de resultados que nos serán de gran utilidad para futuras demostraciones y en especial para la Teoría de géneros.

Lema 1.16. *Una forma $f(x,y)$ representa propiamente a un entero m si y solo si $f(x,y)$ es propiamente equivalente a la forma $mx^2 + Bxy + Cy^2$ para ciertos B, C enteros.*

Demostración. Si $f(x,y)$ representa propiamente a m, entonces existen $p, r \in \mathbb{Z}$ coprimos tales que $f(p,r) = m$. Queremos hallar $q, s \in \mathbb{Z}$ tales que: $ps - qr = 1$ y $mx^2 + Bxy + Cy^2 = f(px + qy, rx + sy)$. Como $mcd(p,r) = 1$, sabemos que existen q, s tales que $ps - qr = 1$. Por otro lado, teníamos que:

$$f(px + qy, rx + sy) = f(p,r)x^2 + (2apq + bps + bqr + 2rs)xy + f(q,s)y^2.$$

Por lo que bastaría tomar $B = (2apq + bps + bqr + 2rs)$ y $C = f(q, s)$.

La otra dirección es directa, pues $mx^2 + Bxy + Cy^2 = f(px + qy, rx + sy)$, para $p, s, q, r \in \mathbb{Z}$ tales que $ps - qr = 1$. Tomando $x = 1$ e $y = 0$ obtenemos $f(p, r) = m$ con $mcd(p, r) = 1$. □

Lema 1.17. *Sea $D \equiv 0, 1 \pmod 4$ y sea m un entero impar coprimo con D. Entonces m es representado propiamente por una forma primitiva de discriminante D si y solo si D es un residuo cuadrático módulo m.*

Demostración. Sea $f(x, y)$ forma de discriminante D que representa propiamente a m. El Lema 1.16 nos dice que $f(x, y) \sim mx^2 + Bxy + Cy^2$. Y por tanto, $D = B^2 - 4mC$ y $D \equiv B^2 \pmod m$.

Ahora, partimos de que $D \equiv b^2 \pmod m$ para algún b. Como m es impar, en la clase de b habrá enteros pares e impares, por lo que puedo tomar b de la misma paridad que D. Además, si $D \equiv 0 \pmod 4$, $b^2 \equiv 0 \pmod 4$. Para $D \equiv 1 \pmod 4$, $b^2 \equiv 1 \pmod 4$. Por lo que $D \equiv b^2 \pmod 4$; y como $mcd(4, m) = 1$, entonces $D \equiv b^2 \pmod{4m}$. Por lo que podemos escribir $D = b^2 - 4mc$, para algún $c \in \mathbb{Z}$. La forma $mx^2 + bxy + cy^2$ tiene discriminante D y representa propiamente a m. □

Lema 1.18. *Sea $f(x, y)$ una forma primitiva de discriminante D y m un entero. Entonces $f(x, y)$ representa infinitos números coprimos con m.*

Demostración. Primero vamos a demostrar el resultado para $m = p$ primo. Como $f(x, y)$ es primitiva se cumple que p no puede dividir a a, b y c simultáneamente. Hay 3 casos:

1) Si $p \nmid a$ entonces tomo (x_0, y_0) tales que:

$$\begin{cases} x_0 \not\equiv 0 \pmod p, \\ y_0 \equiv 0 \pmod p. \end{cases}$$

Reescribiendo $f(x_0, y_0) = ax_0^2 + y_0(bx_0 + cy_0)$ vemos que $p \nmid f(x_0, y_0)$.

2) Análogamente si $p \nmid c$ bastará tomar (x_0, y_0) tales que:

$$\begin{cases} x_0 \equiv 0 \pmod p, \\ y_0 \not\equiv 0 \pmod p. \end{cases}$$

3) El último caso sería cuando $p \nmid b$. Si $p \nmid a$ ó $p \nmid c$, estamos en los casos anteriores. Estudio cuando $p \mid a$ y $p \mid c$. Tomo (x_0, y_0):

$$\begin{cases} x_0 \not\equiv 0 \pmod p, \\ y_0 \not\equiv 0 \pmod p. \end{cases}$$

Entonces $f(x_0, y_0) = ax_0^2 + cy_0^2 + bx_0y_0$ y se tiene que $p \nmid f(x_0, y_0)$.

Para un m general, sea $m = p_1^{\alpha_1} ... p_s^{\alpha_s}$ su descomposición en factores primos. Entonces si queremos que $f(x_0, y_0)$ sea coprimo con m, basta ver que $p_i \nmid f(x_0, y_0)$ para $i \in \{1, \dots s\}$. Es decir, vamos a tener para cada i un par de ecuaciones módulo p_i según estemos en el caso 1), 2) o 3). Lo que queda en un sistema con s ecuaciones para

x y s ecuaciones para y, cada una módulo p_i para $i \in \{1, \ldots, s\}$. Por el Teorema chino del resto existen infinitas soluciones que cumplan estos sistemas; equivalentemente infinitos (x, y) tales que $f(x, y)$ es coprimo con m.

□

1.3. Composición de Dirichlet

Ya hemos definido una relación de equivalencia entre las formas definidas positivas de un discriminante D negativo dado. Nuestro objetivo ahora es definir una operación entre las clases a partir de la cual consigamos una estructura de grupo abeliano finito.

Gauss fue el primero en dar una composición de formas cuadráticas bien definida, pues hasta entonces se había intentado definir la operación entre clases equivalentes y no propiamente equivalentes, por lo que no se conseguía un resultado único al componer dos formas. El trabajo de Gauss sigue un proceso extenso y complicado, por lo que, de forma equivalente, estudiaremos la composición definida por Dirichlet, que además nos permite tener una fórmula explícita para la composición. Para definir esta operación nos harán falta un par de resultados previos:

Lema 1.19. *Sean $p_1, q_1, \ldots, p_r, q_r, m$ enteros tales que $mcd(p_1, \ldots, p_r, m) = 1$. Entonces las congruencias*

$$p_i x \equiv q_i \pmod{m}, \qquad i = 1, \ldots, r$$

tienen una única solución módulo m si y solo si para todo $j, k = 1, \ldots, r$ tenemos:

$$p_k q_j \equiv q_k p_j \pmod{m}.$$

Demostración. Si existe una única solución x_0 que cumple $p_i x_0 \equiv q_i \pmod{m}$ para $i = 1, \ldots, r$, entonces podemos comprobar que se cumplen las ecuaciones de abajo multiplicando por esta x_0 a ambos lados de la ecuación. Para la otra dirección basta ver que si $mcd(p_1, \ldots, p_r, m) = 1$, existen $a, a_1, \ldots, a_r \in \mathbb{Z}$ tales que: $am + \sum_{i=1}^{r} a_i p_i = 1$. Por tanto $\sum_{i=1}^{r} a_i p_i \equiv 1 \pmod{m}$ implica que $q_k \sum_{i=1}^{r} a_i p_i \equiv q_k \pmod{m}$ para $k = 1, \ldots, r$. Y utilizando la hipótesis se tiene que: $p_k \sum_{i=1}^{r} a_i q_i \equiv q_k \pmod{m}$. □

Lema 1.20. *Sean $f(x, y) = (a, b, c)$ y $g(x, y) = (a', b', c')$ dos formas de discriminante D tales que $mcd(a, a', \frac{b+b'}{2}) = 1$. Entonces existe un único entero $B \pmod{2aa'}$ que satisface las siguientes ecuaciones:*

$$\begin{aligned} B &\equiv b \pmod{2a}, \\ B &\equiv b' \pmod{2a'}, \\ B^2 &\equiv D \pmod{4aa'}. \end{aligned} \tag{1.4}$$

Demostración. Si B es un entero que satisface las dos primeras ecuaciones se tiene que $(B - b)(B - b') \equiv 0 \pmod{4aa'}$ y junto con la tercera ecuación tendríamos que

$(b+b')B \equiv bb' + D \pmod{4aa'}$. Reescribimos las congruencias de la siguiente forma:

$$\begin{aligned} a'B &\equiv a'b \pmod{2a}, \\ aB &\equiv ab' \pmod{2a'}, \\ (b+b')B/2 &\equiv (bb'+D)/2 \pmod{2aa'}. \end{aligned} \tag{1.5}$$

Como $mcd(a, a', \frac{b+b'}{2}) = 1$, podemos ver que existe una única solución $x_0 = B$ aplicando el lema anterior con $m = 2aa'$, $q_1 = a'b, q_2 = ab'$ y $q_3 = (bb' + D)/2$. □

Ahora ya tenemos los ingredientes para poder definir nuestra operación:

Definición 1.21. *Sean $f(x,y) = ax^2 + bxy + cy^2$ y $g(x,y) = a'x^2 + b'xy + c'y^2$ dos formas primitivas, definidas positivas de discriminante $D < 0$ con $mcd(a, a', \frac{b+b'}{2}) = 1$. Diremos que estas formas se pueden componer y definimos su Composición de Dirichlet de la siguiente forma:*

$$F(x,y) = f(x,y) \circ g(x,y) = aa'x^2 + Bxy + Cy^2,$$

donde B es la solución del Lema anterior y $C = \frac{B^2 - D}{4aa'}$.

Observación 1.22. *Independientemente del B que tomemos (pues solo tenemos unicidad módulo $2aa'$) siempre vamos a llegar a formas en la misma clase de equivalencia. Si tomo B' otra posible elección, de tal forma que la composición queda $F'(x,y) = (aa', B', \frac{(B')^2 - D}{4aa'})$, entonces asumiendo que $B' = B + 2aa'l$ para l algún entero se tiene que:*

$$F(M(x,y)) = F'(x,y) \quad \textit{con } M = \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix}.$$

Lema 1.23. *Si $F(x,y)$ es la composición de Dirichlet de $f(x,y)$ y $g(x,y)$, entonces $F(x,y)$ representa enteros de la forma $m_1 \cdot m_2$ donde $f(x,y)$ representa m_1 y $g(x,y)$ a m_2.*

Demostración. Sea $f = (a,b,c)$ y $g = (a',b',c')$. Veamos que $f \sim (a, B, a'C)$. Como $B \equiv b \pmod{2a}$, $B = b + 2ak$ con k algún entero. En este caso

$$f(M(x,y)) = (a, B, a'C) \quad \text{con } M = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},$$

y $det(M) = 1$. Análogamente veríamos que $g \sim (a', B, aC)$ usando la equivalencia $B \equiv b' \pmod{2a'}$. Por tanto, $f(x,y)$ y $g(x,y)$ representan los mismos valores que $(a, B, a'C)$ y (a', B, aC) respectivamente y se tiene que:

$$(ax^2 + Bxy + a'Cy^2)(a'z^2 + Bzw + aCw^2) = aa'X^2 + BXY + CY^2, \tag{1.6}$$

con $X = xz - Cwy$ e $Y = axw + a'yz + Byw$. □

Gracias al lema anterior nos será suficiente estudiar qué primos representa la forma reducida de cada clase, pues al componer con otras formas podemos ver qué enteros se representan.

Lema 1.24. *$F(x,y) = f(x,y) \circ g(x,y)$ es una forma primitiva, definida positiva de discriminante D.*

Demostración. El discriminante de F es $B^2 - 4aa'(\frac{B^2-D}{4aa'}) = D$. Como $f(x,y)$ y $g(x,y)$ son definidas positivas, $aa' > 0$ y en consecuencia F también lo es. Finalmente, si existe $p > 1$ que divide a aa', B y C. Podemos asumir que divide a a y por tanto la forma $(a, B, a'C)$ no sería primitiva. Esto lleva a una contradicción pues $f(x,y) \sim (a, B, a'C)$, lo que implica que la segunda forma ha de ser primitiva por la Proposición 1.7. □

1.3.1. Estructura de grupo

Una vez definida la composición de Dirichlet, vamos a poder obtener una estructura de grupo entre las clases de formas primitivas, definidas positivas, de discriminante D negativo. Por tanto vamos a ver que nuestra operación está bien definida para todas las clases.

Proposición 1.25. *Sean $f(x,y)$ y $g(x,y)$ dos formas primitivas con el mismo discriminante D. Entonces existe una tercera forma $h(x,y)$ propiamente equivalente a $g(x,y)$ tal que $f(x,y)$ y $h(x,y)$ se pueden componer.*

Demostración. Si $f(x,y) = (a,b,c)$, por las Proposiciones 1.18 y 1.16, se tiene que $g(x,y) \sim h(x,y) = (d,e,h)$ donde d es un entero coprimo con a representado por $g(x,y)$. En consecuencia, f y h se pueden componer ya que $mcd(a, d, \frac{b+e}{2}) = 1$. □

Lema 1.26. *Sean $f(x,y) = (a_1,b_1,c_1)$ y $g(x,y) = (a_2,b_2,c_2)$ dos formas primitivas con el mismo discriminante D. $f(x,y)$ y $g(x,y)$ son propiamente equivalentes si y solo si existen $p, r \in \mathbb{Z}$ tales que:*

$$\begin{cases} f(p,r) = a_2, \\ 2a_1p + (b_1+b_2)r \equiv 0 \pmod{2a_2}, \\ (b_1-b_2)p + 2c_1r \equiv 0 \pmod{2a_2}. \end{cases}$$

Demostración. Si $f(x,y) \sim g(x,y)$ existen enteros p, q, r, s tales que $f(p,r) = a_2$,

$$\begin{cases} ps - qr = 1, \\ b_2 = (b_1p + 2c_1r)s + (2a_1p + b_1r)q. \end{cases}$$

Si escribimos el sistema matricialmente:

$$\begin{pmatrix} p & -r \\ b_1p + 2c_1r & b_1r + 2a_1p \end{pmatrix} \begin{pmatrix} s \\ q \end{pmatrix} = \begin{pmatrix} 1 \\ b_2 \end{pmatrix},$$

donde el determinante de la matriz es $2f(p,r) = 2a_2 > 0$. Invirtiendo obtenemos:

$$2a_2 \begin{pmatrix} s \\ q \end{pmatrix} = \begin{pmatrix} b_1r + 2a_1p & r \\ -b_1p - 2c_1r & p \end{pmatrix} \begin{pmatrix} 1 \\ b_2 \end{pmatrix},$$

de donde conseguimos las dos siguientes ecuaciones:

$$\begin{cases} 2a_2s = b_1r + 2a_1p + b_2r = (b_1 + b_2)r + 2a_1p, \\ 2a_2q = -b_1p - 2c_1r + b_2p = p(b_2 - b_1) - 2c_1r. \end{cases}$$

Haciendo el proceso a la inversa llegaríamos a que son equivalentes usando que dos formas son iguales si tienen el mismo discriminante y los dos primeros coeficientes. □

Proposición 1.27. *Sean las formas $f(x,y) = (a_1, b_1, c_1) \sim f'(x,y) = (a_3, b_3, c_3)$ y $g(x,y) = (a_2, b_2, c_2) \sim g'(x,y) = (a_4, b_4, c_4)$ de discriminante D negativo. Si las formas $f(x,y)$, $g(x,y)$ y $f'(x,y)$, $g'(x,y)$ se pueden componer respectivamente, entonces $f(x,y) \circ g(x,y)$ y $f'(x,y) \circ g'(x,y)$ son propiamente equivalentes.*

Demostración. Llamemos $F(x,y) = f(x,y) \circ g(x,y) = a_1a_2x^2 + Bxy + Cy^2$ y $F'(x,y) = f'(x,y) \circ g'(x,y) = a_3a_4x^2 + B'xy + C'y^2$. Sabemos que:

$$\begin{aligned} f(x,y) &\sim (a_1, B, a_2C), \\ g(x,y) &\sim (a_2, B, a_1C), \\ f'(x,y) &\sim (a_3, B', a_4C'), \\ g'(x,y) &\sim (a_4, B', a_3C'). \end{aligned}$$

Como $(a_1, B, a_2C) \sim (a_3, B', a_4C')$, puedo aplicar el lema anterior y existen p, r enteros tales que:

$$\begin{cases} a_1p^2 + Bpr + a_2Cr^2 = a_3, \\ 2a_1p + (B + B')r \equiv 0 \pmod{2a_3}, \\ (B - B')p + 2a_2Cr \equiv 0 \pmod{2a_3}. \end{cases} \tag{1.7}$$

Análogamente, como $(a_2, B, a_1C) \sim (a_4, B', a_3C')$ existen p', r' enteros tales que::

$$\begin{cases} a_2(p')^2 + Bp'r' + a_1C(r')^2 = a_3, \\ 2a_2p' + (B + B')r' \equiv 0 \pmod{2a_4}, \\ (B - B')p' + 2a_1Cr' \equiv 0 \pmod{2a_4}. \end{cases} \tag{1.8}$$

Queremos ver que $(a_1a_2, B, C) \sim (a_3a_4, B', C')$, equivalentemente por el lema anterior, buscamos P, R enteros tales que:

$$\begin{cases} a_1a_2P^2 + BPR + CR^2 = a_3a_4, \\ 2a_1a_2P + (B + B')R \equiv 0 \pmod{2a_3a_4}, \\ (B - B')P + 2CR \equiv 0 \pmod{2a_3a_4}. \end{cases} \tag{1.9}$$

Por las primeras ecuaciones de los sistemas (1.7) y (1.8), sabemos que al evaluar (a_1, B, a_2C) en (p, r) representa a_3 y (a_2, B, a_1C) representa a_4 al evaluarlo en (p', r'). Usando la igualdad (1.6) podemos tomar:

$$\begin{cases} P = pp' - Crr', \\ R = a_1pr' + a_2rp' + Brr', \end{cases}$$

que cumplirán la primera ecuación de (1.9). Vemos que cumplen la segunda condición: tomando las ecuaciones centrales de los sistemas (1.7) y (1.8) tenemos:

$$\begin{cases} a_1p + \frac{(B+B')}{2}r \equiv 0 \pmod{a_3}, \\ a_2p' + \frac{(B+B')}{2}r' \equiv 0 \pmod{a_4}. \end{cases}$$

Por tanto,

$$2\left(a_1p + \frac{(B+B')}{2}r\right)\left(a_2p' + \frac{(B+B')}{2}r'\right) \equiv 0 \pmod{2a_3a_4}.$$

Como ambas $F(x,y)$ y $F'(x,y)$ tienen discriminante D, igualando discriminantes podemos escribir $(B')^2 = B^2 - 4a_1a_2C + 4a_3a_4C'$ en la ecuación anterior y nos queda:

$$2a_1a_2P + (B+B')R \equiv 2\left(a_1p + \frac{(B+B')}{2}r\right)\left(a_2p' + \frac{(B+B')}{2}r'\right) \equiv 0 \pmod{2a_3a_4},$$

que es la segunda condición en (1.9). Para ver que se cumple la tercera condición definimos:

$$U = \frac{B-\sqrt{D}}{2}P + CR,$$

es directo comprobar que se cumplen las siguientes igualdades:

$$\begin{aligned} \left(\tfrac{B-\sqrt{D}}{2}p + a_2Cr\right)\left(a_2p' + \tfrac{B+\sqrt{D}}{2}r'\right) &= a_2U, \\ \left(a_1p + \tfrac{B+\sqrt{D}}{2}r\right)\left(\tfrac{B-\sqrt{D}}{2}p' + a_1Cr'\right) &= a_1U, \\ \left(\tfrac{B-\sqrt{D}}{2}p + a_2C\right)\left(\tfrac{B-\sqrt{D}}{2}p' + a_1Cr'\right) &= \tfrac{B-\sqrt{D}}{2}U, \\ C\left(a_1p + \tfrac{B+\sqrt{D}}{2}r\right)\left(a_2p' + \tfrac{B+\sqrt{D}}{2}ra_2p'\right) &= \tfrac{B+\sqrt{D}}{2}U. \end{aligned}$$

Tomamos módulo $2a_3a_4$ en las igualdades y como $B' \equiv \sqrt{D} \pmod{a_3a_4}$, nos fijamos en que los términos de la izquierda son múltiplos de a_3a_4 por las igualdades anteriores, y por tanto los del lado derecho también lo serán. Es decir,

$$a_2U \equiv a_1U \equiv BU \equiv 0 \pmod{a_3a_4}.$$

Como (a_1, B, a_2C) es primitiva, se tiene que $mcd(a_1, B, a_2) = 1$ y esto implica que $U \equiv 0 \pmod{a_3a_4}$. Reescribiendo,

$$U = \frac{B-\sqrt{D}}{2}P + CR \equiv \frac{B-B'}{2}P + CR \equiv 0 \pmod{a_3a_4}.$$

Y así comprobamos que P y R cumplen la tercera ecuación. □

Parece que nuestra operación satisface todo lo que buscábamos. Ahora procedemos a dar una definición que nos es útil y ya a continuación enunciaremos el teorema que da nombre a la sección.

Definición 1.28. *Sea $D < 0$, $D \equiv 0, 1 (mod\ 4)$, entonces la forma principal de discriminante D es la siguiente:*

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

En ambos casos, la forma principal es reducida.

Teorema 1.29. *Sea $D \equiv 0, 1\ (\text{mod } 4)$ un entero negativo. Definimos $C(D)$ como el conjunto formado por las clases de formas cuadráticas primitivas, definidas positivas de discriminante D. Llamaremos clase principal a aquella que contiene a la forma principal, y dada $f(x, y) = (a, b, c)$ definiremos su forma opuesta como $(a, -b, c)$. Entonces se tiene lo siguiente:*

- *La composición de Dirichlet induce una operación bien definida en $C(D)$ que aporta a $C(D)$ una estructura de grupo abeliano finito de orden $h(D)$.*
- *La identidad de este grupo es la clase principal.*
- *La clase inversa de $[f(x, y)]$ es la que contiene a su opuesta.*

Demostración. Ya hemos visto que es una operación cerrada en $C(D)$ y gracias a los lemas anteriores sabemos que siempre vamos a poder componer dos clases cualesquiera y que está bien definida independientemente del representante que tomes de cada clase. La conmutatividad es directa, pues cuando elegimos B para definir la composición, no influye el orden en el que tomamos las clases. La asociatividad no la demostraremos pues no es un punto clave en la Teoría de géneros. La demostración se puede ver en [7, Cap. 1, p. 21].

Elemento identidad: primero notemos que siempre vamos a poder componer cualquier forma (a, b, c) con la forma principal pues el primer coeficiente es un 1. Además vamos a podemos tomar $B = b$ y la composición resulta en $(a, b, \frac{b^2-D}{4a} = c)$.

Elemento inverso: sean $f(x, y) = (a, b, c)$ y $f'(x, y) = (a, -b, c)$ su opuesta, ambas en clases distintas. Sea $g(x, y) = f'(-y, x) = cx^2 + bxy + ay^2$, entonces $g \sim f'$ y además se puede componer con $f(x, y)$ pues $mcd(a, c, \frac{b+b}{2}) = 1$. En este caso también podemos tomar $B = b$ y nos queda $F(x, y) = f(x, y) \circ g(x, y) = (ac, b, 1)$. Veamos que F es propiamente equivalente a la forma principal: si $D \equiv 0\ (\text{mod } 4)$ se puede ver que $F(y, -x - by/2)$ coincide con la forma principal y para $D \equiv 1\ (\text{mod } 4)$, el cambio sería $F(y, -x - (1 + b)y/2)$. Así, concluimos que $f'(x, y)$ es inversa de $f(x, y)$.

□

Ahora daremos un par de resultados que tendrán cierta relevancia más tarde:

Lema 1.30. *La clase cuya forma reducida sea $ax^2 + bxy + cy^2$ tiene orden ≤ 2 si y solo si $b = 0$, $a = b$ o $a = c$.*

Demostración. Sea $f'(x, y)$ la opuesta de $f(x, y)$. La clase $[f(x, y)]$ tiene orden 2 si y solo si contiene su opuesta, por lo tanto queremos ver que $f(x, y) \sim f'(x, y)$ si y solo

si se cumplen las condiciones del enunciado. Como $f(x,y)$ es reducida, si $|b| < a < c$ entonces $f'(x,y)$ es reducida, por el Lema 1.10 han de ser la misma y por tanto $b = 0$. Si $|a| = b$ entonces $f'(x+y,y) = f(x,y)$ y serán propiamente equivalentes. De forma análoga si $a = c$, f y f' son propiamente equivalentes pues $f(-y,x) = f'(x,y)$. □

Definición 1.31. *Sea $D \equiv 0,1 \pmod 4$ negativo, y sea r el número de primos impares que dividen a D. Definimos $\mu(D)$ como r si $D \equiv 1 \pmod 4$ y si $D = -4n$*

$$\mu(D) = \begin{cases} r & n \equiv 3 \pmod 4 \\ r+1 & n \equiv 1,2 \pmod 4 \text{ o } n \equiv 4 \pmod 8 \\ r+2 & n \equiv 0 \pmod 8 \end{cases}$$

Lema 1.32. *Sea $D \equiv 0,1 \pmod 4$ negativo. El grupo $C(D)$ tiene $2^{\mu(D)-1}$ elementos de orden ≤ 2.*

Demostración. Haremos nuestra demostración para $D = -4n$ con $n \equiv 1 \pmod 4$, donde r es el número de divisores primos de n. El resto de casos los podemos encontrar en el libro [3, §16, p. 327].

Gracias al Lema 1.30, para buscar las clases de orden ≤ 2 nos basta con encontrar las formas reducidas que cumplen $b = 0$, $a = c$ o $a = b$. Como $D \equiv 0 \pmod 4$, entonces b es par y podemos escribir cualquier forma de discriminante D como $(a, 2b, c)$. Veamos los posibles casos.

Si queremos encontrar f forma reducida de discriminante D con $2b = 0$, entonces $f = (a,0,c)$ y $D = -4ac$. Luego $n = ac$ y como $mcd(a,c) = 1$ existen 2^r posibles combinaciones para elegir a y c. Como f es reducida nos quedamos con las que cumplan $a < c$, en total, 2^{r-1} opciones posibles.

Vemos cuales son las posibles formas reducidas con $a = 2b$ o $a = c$. Sea $n = b \cdot k$ con $0 < b < k$ coprimos. Como antes, hay 2^{r-1} posibles elecciones de b y k. Elegidas k y b fijamos $c = b + k/2$ y definimos $f = (2b, 2b, c)$. La forma f tiene discriminante $D = -4n$ y es primitiva, pues:

$$\begin{cases} k = 2c - b \\ mcd(k,b) = 1 \end{cases} \rightarrow mcd(b, 2c) = 1 \rightarrow mcd(b,c) = 1.$$

Además c es impar, pues $n \equiv 1 \pmod 4$ implica que $b \equiv k \pmod 4$ y por tanto, $c = (b+k)/2$ ha de ser impar.

Con este método vamos a obtener 2^{r-1} formas reducidas o equivalentes a una reducida distintas que cumplen $a = 2b$ o $a = c$, pues si $2b < c$, entonces f es reducida y si $2b > c$, $f(y, x+y) = (c, 2(c-b), c)$, y será equivalente a una forma reducida con $a = c$, pues $2(c-b) < c$. Además vemos que estas son todas las posibles formas reducidas $f = (a, 2b, c)$ con $2b = 0$, $a = c$, $a = 2b$: si $a = 2b$, tomando $k = 2c - b$ llegaríamos al primer caso y si $a = c$, entonces $f(x,y) \sim f(x+y, -x)$ que nos lleva a una forma reducida con $a = 2b$. Por lo que en total tenemos $2^{r-1} + 2^{r-1} = 2^r$ formas reducidas que cumplen las hipótesis. Equivalentemente, hay 2^r clases de formas cuadráticas de orden menor o igual que 2. □

CAPÍTULO 2
Teoría de géneros

Fijado un entero $D \equiv 0, 1 \pmod 4$, la Teoría de géneros consiste en clasificar las formas cuadráticas con este discriminante en función de qué unidades representan módulo D. Nosotros aplicaremos esta teoría sobre las formas de discriminante negativo, que es donde hemos definido la composición y conocemos su estructura interna.

En este apartado se utilizarán el Símbolo de Legendre y Jacobi, así como sus propiedades, que se pueden ver en el Apéndice A. Comenzaremos exponiendo un homomorfismo cuyo núcleo contiene a las clases módulo D de los elementos que van a ser representados por formas de discriminante D y a partir de ahí intentaremos dar una estructura interna a estas clases representadas. A partir de ahora usaremos la notación U_D para referirnos a las unidades módulo D.

Teorema 2.1. *Dado $D \equiv 0, 1 \pmod 4$ discriminante podemos definir el siguiente homomorfismo*[1] *definido sobre las unidades módulo D:*

$$\chi_D : U_D \to \{\pm 1\},$$

tal que para todo m impar cumple: $\chi_D(\overline{m}) = \left(\dfrac{D}{m}\right)$. Si $D \equiv 1 \pmod 4$, entonces:

$$\chi_D(\overline{2}) = \begin{cases} 1 & si\ D \equiv 1 \pmod 8, \\ -1 & si\ D \equiv 5 \pmod 8. \end{cases}.$$

Demostración. Separamos en los dos casos. Para $D \equiv 1 \pmod 4$ vamos a demostrar que $\chi_D(\overline{m}) = \left(\dfrac{m}{|D|}\right)$. Al tratarse del símbolo de Jacobi sobre $|D|$, esto ya nos garantiza que sea un homomorfismo bien definido. Si $D > 0$, para m impar tenemos:

$$\chi_D(\overline{m}) = \left(\frac{D}{m}\right) = \left(\frac{m}{D}\right)(-1)^{\frac{(D-1)(m-1)}{4}} = \left(\frac{m}{D}\right).$$

[1] El homomorfismo χ_D coincide con el Símbolo de Kronecker, que es una generalización del Símbolo de Jacobi para números enteros, la diferencia entre ambos es que nuestro homomorfismo está definido sobre las unidades módulo D. Podemos encontrar más detalles de la construcción del símbolo de Kronecker en [8, §14].

Cuando el homomorfismo actúa sobre 2, se tienen las siguientes igualdades:

$$\chi_D(\overline{2}) = \left\{ \begin{array}{cc} 1 & si\ D \equiv 1 \pmod 8 \\ -1 & si\ D \equiv 5 \pmod 8 \end{array} \right\} = (-1)^{\frac{D^2-1}{8}} = \left(\frac{2}{D}\right).$$

Para $D < 0$, si m impar (nos fijamos en que $|D| \equiv 3 \pmod 4$):

$$\chi_D(\overline{m}) = \left(\frac{-1}{m}\right)\left(\frac{|D|}{m}\right) = (-1)^{\frac{m-1}{2}}\left(\frac{m}{|D|}\right)(-1)^{\frac{(|D|-1)(m-1)}{4}} =$$

$$= \left(\frac{m}{|D|}\right)(-1)^{\frac{(|D|+1)(m-1)}{4}} = \left(\frac{m}{|D|}\right).$$

Cuando actuamos sobre 2 basta observar que:

$$\chi_D(\overline{2}) = \left\{ \begin{array}{cc} 1 & si\ D \equiv 1 \pmod 8 \\ -1 & si\ D \equiv 5 \pmod 8 \end{array} \right\} = (-1)^{\frac{D^2-1}{8}} = (-1)^{\frac{|D|^2-1}{8}} = \left(\frac{2}{|D|}\right).$$

Para $D \equiv 0 \pmod 4$, observamos que si $m \in U_D$ entonces m es impar. Por otro lado, vamos a poder escribir $D = 2^\mu r$ con r impar y $\mu \geq 2$. Si $D > 0$ tenemos que:

$$\chi_D(\overline{m}) = \left(\frac{D}{m}\right) = \left(\frac{2}{m}\right)^\mu\left(\frac{r}{m}\right) = \left(\frac{2}{m}\right)^\mu\left(\frac{m}{r}\right)(-1)^{\frac{(r-1)(m-1)}{4}}.$$

Veamos que está bien definido. Sean enteros m, n tales que $m \equiv n \pmod D$, queremos ver que $\chi_D(\overline{m}) = \chi_D(\overline{n})$. Al ser $D = 2^\mu r$ entonces $m \equiv n \pmod r$ y por tanto $\left(\frac{m}{r}\right) = \left(\frac{n}{r}\right)$. Por otro lado, al ser $D \equiv 0 \pmod 4$, $m \equiv n \pmod 4$ y en consecuencia $\frac{m-1}{2}$ y $\frac{n-1}{2}$ tienen la misma paridad. Solo quedaría comprobar que $\left(\frac{2}{m}\right)^\mu = \left(\frac{2}{n}\right)^\mu$. Si μ es par, ya estaría. Si μ es impar, $\mu \geq 3$ y nos gustaría llegar a que:

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

Como en este caso $D \equiv 0 \pmod 8$, $m \equiv n \pmod 8$ y se da la igualdad. Ahora comprobaremos que es un homomorfismo. Sean a, b enteros impares, queremos ver que $\chi_D(\overline{ab}) = \chi_D(\overline{a})\chi_D(\overline{b})$, equivalentemente:

$$\left(\frac{2}{ab}\right)^\mu\left(\frac{ab}{r}\right)(-1)^{\frac{(r-1)(ab-1)}{4}} = \left(\frac{2}{a}\right)^\mu\left(\frac{2}{b}\right)^\mu\left(\frac{a}{r}\right)\left(\frac{b}{r}\right)(-1)^{\frac{(r-1)(a-1)}{4}}(-1)^{\frac{(r-1)(b-1)}{4}}.$$

Como el símbolo de Jacobi es multiplicativo solo habría que comprobar que $\frac{a-1}{2} + \frac{b-1}{2}$ y $\frac{ab-1}{2}$ tienen la misma paridad. Como a y b son impares, esto es cierto gracias al Lema A.1 del Apéndice A. Finalmente si $D < 0$ se puede comprobar que:

$$\chi_D(\overline{m}) = \left(\frac{2}{m}\right)^\mu\left(\frac{m}{|r|}\right)(-1)^{\frac{(r-1)(m-1)}{4}}.$$

□

El homomorfismo actúa de la siguiente forma:

- $D \equiv 1 \pmod 4$: $\chi_D(\overline{m}) = \left(\dfrac{m}{|D|}\right)$ (si m es impar es directamente $\left(\dfrac{|D|}{m}\right)$).
- $D \equiv 0 \pmod 4$: $\chi_D(\overline{m}) = \left(\dfrac{D}{m}\right) = \left(\dfrac{2}{m}\right)^c \left(\dfrac{u}{m}\right)$ siendo $D = 2^c u$.

Observación 2.2. *Como el homomorfismo está bien definido, generalmente si a es un entero coprimo con D escribiremos $\chi_D(a)$ para referirnos a $\chi_D(\overline{a})$.*

La siguiente proposición nos permite identificar qué clases módulo D van a ser representadas por las formas con este discriminante.

Proposición 2.3. *Sea $D \equiv 0, 1 \pmod 4$ y n entero positivo coprimo con D. Si n es representado por alguna forma de discriminante D, entonces $n \in \ker(\chi_D)$.*

Demostración. Sea $f(x, y) = ax^2 + bxy + cy^2$ forma de discriminante D tal que $f(s, r) = n$ con r, s enteros. Si llamamos $d = mcd(r, s)$ tenemos que $r = dp$ y $s = dq$ con p y q enteros coprimos. Entonces podríamos escribir $n = d^2 f(p, q) = d^2 m$ con m propiamente representado por $f(x, y)$ y $mcd(m, D) = 1$ (pues $mcd(n, D) = 1$). Se tiene que $\chi_D(n) = \chi_D(d^2 m) = \chi_D(m)(\chi_D(d))^2 = \chi_D(m)$. Por tanto para ver que $n \in \ker(\chi_D)$, nos basta ver que $m \in \ker(\chi_D)$ con m propiamente representado.

Si D es par y m impar, el Lema 1.17 nos dice que D es residuo cuadrático módulo m, por lo que $\chi_D(m) = 1$. También podemos aplicar el mismo Lema en el caso D impar y m impar, solo nos queda ver que ocurre cuando D es impar y m par. El Lema 1.16 nos dice que $f \sim mx^2 + Bxy + Cy^2$ y $D = B^2 - 4mC$. Como $D \equiv B^2 \pmod 4$, B ha de ser impar y al ser m es par, $D \equiv B^2 \equiv 1 \pmod 8$. Por tanto, $\chi_D(2) = 1$. Denotamos $m = 2^c m'$, con m' impar. Si $m' = 1$, entonces $\chi_D(m) = (\chi_D(2))^c = 1$. Si $m' \geq 3$, como $D = B^2 - 4 \cdot 2^c m' C$, D es residuo cuadrático módulo m'. Así, tendremos que $\chi_D(m) = (\chi_D(2))^c \chi_D(m') = 1$. □

En particular, para los primos tenemos también la otra dirección:

Teorema 2.4. *Sea $D \equiv 0, 1 \pmod 4$ entero y sea $\chi_D : U_D \to \{\pm 1\}$ definido anteriormente. Entonces para cualquier p primo impar que no divide a D, $[p] \in \ker(\chi_D)$ si y solo si p es representado por una forma de discriminante D.*

Demostración. Es una aplicación directa del Lema 1.17, que nos dice p es presentado por una forma de discriminante D si y solo si D es residuo cuadrático módulo p, equivalentemente $\chi_D(p) = \left(\frac{D}{p}\right) = 1$. □

Hemos conseguido demostrar que todas las unidades módulo D que pueden ser representadas por formas de discriminante D están en $\ker(\chi_D)$. Veremos ahora que se forma una estructura de grupo cociente en $\ker(\chi_D)$ un tanto sorprendente.

Lema 2.5. *Sea $D \equiv 0, 1 \pmod 4$ negativo. Los elementos en U_D representados por formas de la clase principal forman un subgrupo en $\ker(\chi_D)$ que denotaremos por H.*

Demostración. Si $D \equiv 0 \pmod 4$ nos fijamos en que:

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

Por lo que H es cerrado bajo multiplicación, y por tanto es un subgrupo. En el caso $D \equiv 1 \pmod 4$, se puede ver que:

$$4\left(x^2 + xy + \frac{1-D}{4}y^2\right) \equiv (2x+y)^2 \pmod D.$$

Sea $G = \{x^2 : x \in U_D\}$, si vemos que $H = G$ ya tendríamos el resultado que buscamos, pues G es cerrado bajo multiplicación. Si $m = k^2, \in G$ entonces $m = f(k, 0)$ siendo $f(x, y)$ la forma principal. Por otro lado, si $h \in H$, entonces $4h \in G$ y en consecuencia, $4h \equiv k^2 \pmod D$. Esto implica que $h \in G$ pues 4 tiene inverso módulo D.

□

Lema 2.6. *Sean $D \equiv 0, 1 \pmod 4$ negativo, H y $\ker(\chi_D)$ definidos previamente y sea $f(x, y)$ una forma primitiva, definida positiva de discriminante D. Entonces los elementos que representa $f(x, y)$ forman una clase lateral de H en $\ker(\chi_D)$.*

Demostración. Si $D \equiv 0 \pmod 4$, entonces $D = -4n$. Gracias a los Lemas 1.18 y 1.16 sabemos que $f(x, y)$ representa a un entero a coprimo con $4n$, y por tanto $f \sim ax^2 + bxy + cy^2$. Como $D \equiv 0 \pmod 4$, b ha de ser par: $b = 2b'$. Se puede comprobar que

$$af(x, y) = (ax + b'y)^2 + ny^2.$$

Como a y $4n$ son coprimos, se tiene que $f(x, y) \in [a^{-1}]H$. Por otro lado si $[c] \in [a^{-1}]H$, entonces $ac \equiv z^2 + nw^2 \pmod{4n}$. Lo que significa que $[a^{-1}]H$ es un subconjunto de los elementos representados por f módulo D, consiguiendo así la igualdad entre conjuntos.

Si $D \equiv 1 \pmod 4$, entonces b ha de ser impar. Podemos escribir $b = 2m + 1$ y seguir el mismo razonamiento de antes pero con la siguiente igualdad:

$$af(x, y) = (ax + my)^2 + (ax + my)y + \frac{1-D}{4}y^2.$$

□

Con estos resultados podemos definir los géneros:

Definición 2.7. *Sean D negativo, H y $\ker(\chi_D)$ definidos anteriormente y sea H' una clase lateral de H en $\ker(\chi_D)$. El género de H' consiste en las formas de discriminante D que representan exactamente las clases de H'. En otras palabras, dado un entero m, $\overline{m} \in H'$ si y solo si existe una forma f en el género de H' que represente a m.*

Es decir, dada una forma de discriminante D, esta representará elementos de un determinado subgrupo del $\ker(\chi_D)$ dependiendo del género en el que esté. Veamos un par de ejemplos que nos ayudarán a entender esta idea mejor.

Ejemplo 2.8. *Para $D = -20$, ya estudiamos en el Ejemplo 1.12 las dos posibles clases. Computacionalmente, podemos ver qué unidades módulo 20 representan:*

$$x^2 + 5y^2 \text{ representa } 1, 9 \text{ en } U_{20},$$

$$2x^2 + 2xy + 3y^2 \text{ representa } 3, 7 \text{ en } U_{20}.$$

Además el Teorema 2.4 nos da las siguientes equivalencias:

$$x^2 + 5y^2 = p \text{ primo} \iff p \equiv 1, 9 \pmod{20}$$

$$2x^2 + 2xy + 3y^2 = p \text{ primo} \iff p \equiv 3, 7 \pmod{20}$$

Ejemplo 2.9. *Para $D = -56$, en el Ejemplo 1.13 vimos las cuatro posibles clases. Se puede obtener computacionalmente qué unidades módulo 56 representan y aplicando el Teorema 2.4 se tiene:*

$$x^2 + 14y^2 \text{ o } 2x^2 + 7y^2 = p \text{ primo} \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$

$$3x^2 \pm 2xy + 5y^2 = p \text{ primo} \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$$

Al ver estos ejemplos, nos damos cuenta de que en ambos casos dada una forma, podemos saber qué enteros módulo su discriminante representa. En el caso de formas con discriminante $D = -20$ esta correspondencia es unívoca: dada una forma sé qué enteros coprimos con D representa y dado un entero coprimo con D sé si puedo representarlo a través de una forma cuadrática. Mientras que en el caso de discriminante $D = -56$, vamos a tener dos posibles formas donde ambas representan a las mismas unidades módulo 56.

Esto es debido a que en el primer caso tenemos una clase en cada género y en el segundo caso hay dos clases por género. Por lo tanto nos interesará saber cuando estamos en el mejor de los casos, es decir, para qué discriminantes se tiene una clase por género.

2.1. Número de géneros

El objetivo de este apartado es conseguir una fórmula para el número de géneros dado un discriminante D. Nos enfocaremos en las formas cuadráticas con discriminantes fundamentales, pues este tipo de discriminantes nos permiten un manejo mucha más cómodo del homomorfismo χ_D. En el Apéndice B están expuestos varios resultados de discriminantes fundamentales que necesitamos en varias demostraciones.

En esta sección nombraremos varias propiedades interesantes de χ_D siendo D discriminante fundamental; y más tarde las relacionaremos con la teoría expuesta antes. Para ello hemos seguido [8].

Definición 2.10. *Sea $D \in \mathbb{Z}\backslash\{0, 1\}$ con $D \equiv 0, 1 \pmod 4$. Decimos que D es un discriminante fundamental si no es divisible por ningún cuadrado de un primo impar y es impar o $D \equiv 8$ o $D \equiv 12 \pmod{16}$. Decimos que d es un discriminante primo si es un discriminante fundamental divisible solo por un único primo.*

Observación 2.11. *Nos fijamos en que los discriminantes primos si son impares, son de la forma* $d = (-1)^{\frac{p-1}{2}}p$*, y para el caso par solo pueden ser* -4*,* 8 *o* -8*.*

Teorema 2.12. *Sea* D *un discriminante fundamental. Entonces* D *puede escribirse como producto de discriminantes primos de forma única.*

Demostración. La demostración de este resultado la encontramos en el Apéndice B. □

Teorema 2.13. *Sea* D *discriminante fundamental,* $D = d_1 \dots d_t$ *su descomposición en discriminantes primos y* χ_D *el homomorfismo definido anteriormente. Entonces:*

$$\chi_D = \chi_{d_1} \cdots \chi_{d_t}.$$

Demostración. La demostración de este resultado la encontramos en el Apéndice B. □

Teorema 2.14. *El grupo cociente* $U_D/\ker(\chi_D)$ *es isomorfo a* $\mathbb{Z}/2\mathbb{Z}$*.*

Demostración. Es un resultado inmediato del Primer Teorema de Isomorfía y la sobreyectividad de χ_D. □

Usando la notación anterior definiremos:

$$B_D := \bigcap_{j=1}^{t} \ker(\chi_{d_j})\,.$$

Obsérvese que B_D es un subgrupo normal de U_D. Nuestro objetivo en un futuro cercano es ver que B_D coincide con lo que habíamos llamado H. Por tanto, si conocemos el cardinal de $\ker(\chi_D)/B_D$, tendremos una fórmula para el número de géneros. No solo eso, sino que además sabremos que las clases módulo D representadas por la forma principal son aquellas que pertenecen al $\ker(\chi_{d_j})$ para todo $d_j \mid D$.

Veamos primero que estructura tiene $\ker(\chi_D)/B_D$.

Teorema 2.15. *Sea* D *discriminante fundamental,* $D = d_1 \dots d_t$ *su descomposición en discriminantes primos. Entonces* U_D/B_D *es isomorfo a* $\mathbb{Z}/2\mathbb{Z}\times \overset{t}{\dots} \times\mathbb{Z}/2\mathbb{Z}$*, por lo que tiene cardinal* 2^t*.*

Demostración. Denotamos $A = \mathbb{Z}/2\mathbb{Z}\times \overset{t}{\dots} \times\mathbb{Z}/2\mathbb{Z}$. Definimos la siguiente aplicación, $\psi : U_D \to A$ con $\psi(m) = (\chi_{d_1}(m), \dots, \chi_{d_t}(m))$ para m entero coprimo con D. Vemos que ψ es un homomorfismo pues dados a, b coprimos con D:

$$\psi(ab) = (\chi_{d_1}(ab), \dots, \chi_{d_t}(ab)) = (\chi_{d_1}(a)\chi_{d_1}(b), \dots, \chi_{d_t}(a)\chi_{d_t}(b)) = \psi(a)\psi(b).$$

Además ψ es sobreyectivo, pues dado $(c_1, \dots, c_t) \in A$, tenemos que para cada $j \in \{1, \dots, t\}$ existe un y_j tal que $mcd(y_j, d_j) = 1$ y $\chi_{d_j}(y_j) = c_j$. Como los d_j son coprimos entre ellos, aplicando el Teorema chino del resto, existe a entero tal que $a \equiv y_j \pmod{|d_j|}$ para todo $j \in \{1, \dots, t\}$. Por tanto $\psi(a) = (\chi_{d_1}(a), \dots, \chi_{d_t}(a)) =$

$(\chi_{d_1}(y_1), \ldots, \chi_{d_t}(y_t)) = (c_1, \ldots, c_t)$. En consecuencia, ψ es un homomorfismo sobreyectivo donde $\ker(\psi) = B_D$; aplicando el Primer Teorema de Isomorfía nos queda:

$$U_D/B_D \cong \mathbb{Z}/2\mathbb{Z} \times \overset{t}{\ldots} \times \mathbb{Z}/2\mathbb{Z}.$$

Así, conseguimos la igualdad $|U_D/B_D| = 2^t$. □

Para terminar, el teorema que nos interesa:

Teorema 2.16. *Sea t el número de divisores primos de un discriminante fundamental D, entonces el grupo cociente $\ker(\chi_D)/B_D$ es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \overset{t-1}{\ldots} \times \mathbb{Z}/2\mathbb{Z}$, y por tanto $|\ker(\chi_D)/B_D| = 2^{t-1}$.*

Demostración. Gracias al Teorema 2.13 sabemos que $B_D \subset \ker(\chi_D)$ y además es un subgrupo normal. Además, a partir de las siguientes igualdades

$$|U_D/B_D| = |U_D/\ker(\chi_D)||\ker(\chi_D)/B_D|,$$

tenemos que $|\ker(\chi_D)/B_D| = 2^{t-1}$. Como los elementos de U_D/B_D tienen orden 1 o 2 y $\ker(\chi_D)/B_D \subset U_D/B_D$, entonces sus elementos tienen también orden 1 o 2 y obtenemos el siguiente isomorfismo:

$$\ker(\chi_D)/B_D \cong \mathbb{Z}/2\mathbb{Z} \times \overset{t-1}{\ldots} \times \mathbb{Z}/2\mathbb{Z}.$$

□

Nuestro objetivo ahora es demostrar que $B_D = H$, En este caso tendremos que el número de géneros de discriminante fundamental D es 2^{t-1} y además conseguimos una caracterización de H.

Proposición 2.17. *Sea $D < 0$ un discriminante fundamental y f_0 la forma principal de discriminante D. Podemos obtener cada una de las clases en $B_D \subset U_D$ tomando módulos a los enteros positivos representados por f_0. Equivalentemente, $B_D \subset H$.*

Demostración. Sea m un entero positivo coprimo con D con $m \in B_D$. Queremos ver que existe un entero n representado por f_0 con $n \equiv m \pmod{D}$. Separo por casos:

Si D es impar, $D = d_1 \ldots d_t$ con $d_j = (1)^{\frac{p_j-1}{2}} p_j$, p_j primos impares, $j = 1, \cdots, t$. Como m cumple que $\left(\frac{m}{p_j}\right) = 1$ para $j = 1, \ldots, t$ existen $x_1, \ldots, x_j$ enteros tales que $m \equiv x_j^2 \pmod{p_j}$. Por el Teorema chino del resto existirá x tal que $x \equiv x_j \pmod{p_j}$ y bastaría tomar $n = x^2 = f_0(x, 0)$.

Si D es par, denotaremos al discriminante primo par que lo divide como d_1. Si $d_1 = -4$, como m es impar y residuo cuadrático módulo 4, seguimos el procedimiento anterior pero cambiando la congruencia $m \equiv x_1^2 \pmod{p_1}$ por $m \equiv 1^2 \pmod 4$, y por tanto en vez de $x \equiv x_1 \pmod 4$ tendríamos $x \equiv 1 \pmod 4$ y completamos como el caso anterior.

Si D es par con $d_1 = -8$, como $\chi_{-8}(m) = 1$ entonces $m \equiv 1$ o $3 \pmod 8$. Si $m \equiv 1 \pmod 8$ completaríamos la prueba igual. Si $m \equiv 3 \pmod 8$, cambiamos otra

vez x_1 por 1 y al resolver el Teorema chino del resto elegimos x tal que $x^2 - \frac{D}{4} > 0$. Finalmente tomamos $n = f_0(x, 1) = x^2 - \frac{D}{4}$. Concluimos gracias al Lema B.4, que nos dice que $\frac{D}{4} \equiv 6 \pmod 8$ y por tanto $n \equiv 3 \equiv m \pmod 8$.

Si D es par con $d_1 = 8$. En este caso $\chi_8(m) = 1$ implica que $m \equiv 1$ o $7 \pmod 8$. Si $m \equiv 1 \pmod 8$, resolvemos como siempre y si $m \equiv -1 \pmod 8$ tomamos $n = f_0(x, 1)$. Análogamente usando el Lema B.4 sabemos que $\frac{D}{4} \equiv 2 \pmod 8$, por lo que se tiene que $n \equiv 7 \equiv m \pmod 8$. □

Ya tenemos una inclusión, para demostrar la igualdad de los subgrupos H y B_D necesitaremos el siguiente teorema:

Teorema 2.18. *Sea $D < 0$ un discriminante fundamental y sea $\boldsymbol{C}$ una clase en $C(D)$. Si m, n son enteros positivos coprimos con D representados por una forma $f \in \boldsymbol{C}$, entonces $\overline{m}$ y $\overline{n}$ pertenecen a la misma clase lateral de* $\ker(\chi_D)/B_D$.

Demostración. Sea $D = d_1, \ldots, d_t$ la factorización en discriminantes primos. Si D es par, asumimos que d_1 es el discriminante par que lo divide. Por la Proposición 2.3 sabemos que $\overline{n}$ y $\overline{m}$ pertenecen a $\ker(\chi_D)$. Consideremos $\overline{x} = \overline{m} \cdot \overline{n}^{-1} \in \ker(\chi_D)$ y nuestro objetivo será ver que $\overline{x} \in B_D$. Equivalentemente, como $\overline{m} \cdot \overline{n} = \overline{x} \cdot \overline{n}^2$ y $\overline{n}^2 \in B_D$, pues $\chi_{d_j}(\overline{n}^2) = \left[\chi_{d_j}(\overline{n})\right]^2 = 1$, tenemos que ver que $\overline{m} \cdot \overline{n} \in B_D$.

Sea $f = (a, b, c)$ una forma en $\mathbf{C}$ y sean p, q, r, s enteros tales que $f(p, r) = m$ y $f(q, s) = n$. Consideramos la matriz

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

Aplicando la igualdad 1.2, se tiene que $f(A(x, y)) = (m, l, n)$ para l algún entero. Usando la notación matricial tenemos lo siguiente:

$$A^t \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} A = \begin{pmatrix} m & l/2 \\ l/2 & n \end{pmatrix}.$$

Si igualamos discriminantes y multiplicamos por -4 obtenemos que $Dv^2 = l^2 - 4mn$, donde $v = det(A)$. Entonces para cada d_j impar, $l^2 \equiv 4mn \pmod{|d_j|}$ y equivalentemente $(l \cdot 2^{-1})^2 \equiv mn \pmod{|d_j|}$. Por tanto, $\chi_{d_j}(\overline{mn}) = 1$.

Por lo que si $D \equiv 1 \pmod 4$ ya hemos concluido lo que queríamos, pues todos los discriminantes primos que dividen a D son impares. Queda ver que si $D \equiv 0 \pmod 4$, entonces $\chi_{d_1}(\overline{m} \cdot \overline{n}) = 1$ para $d_1 = \{-4, 8, -8\}$. Antes de ver este caso nos fijamos en que como D es par, l será par, es decir, $l = 2k$ para k algún entero. En este caso, $k^2 = \frac{Dv^2}{4} + mn$, con $D/4 \in \mathbb{Z}$. Como m y n son unidades módulo D, entonces $m \cdot n$ es impar y positivo. Consideramos los 3 casos por separados:

1. Si $d_1 = -4$, entonces el Lema B.2 nos dice que $D/4 \equiv 3 \pmod 4$. En este caso, $mn \equiv k^2 + v^2 \pmod 4$. Al ser impar mn impar, entonces k o v es impar y solo uno de los dos. En ambos casos, se tendría que $mn \equiv 1 \pmod 4$ y por tanto $\chi_{-4}(\overline{nm}) = 1$.

2. Si $d_1 = -8$, el Lema B.4 nos dice que $D/4 \equiv 6 \pmod 8$. En este caso $mn \equiv k^2 + 2v^2 \pmod 8$. Como mn es impar, k tiene que ser impar y por tanto $mn \equiv 1 + 2v^2 \pmod 8$. Si v es par, $mn \equiv 1 \pmod 8$ y se tiene que $\chi_{-8}(\overline{n} \cdot \overline{m}) = 1$. Si v es impar, entonces $mn \equiv 3 \pmod 8$ y $\chi_{-8}(\overline{nm}) = \left(\frac{-8}{3}\right) = 1$.

3. Si $d_1 = 8$, entonces por el Lema B.4 sabemos que $D/4 \equiv 2 \pmod 8$ y por tanto, $mn \equiv k^2 - 2v^2 \pmod 8$. Al ser mn impar, k es impar y $mn \equiv 1 - 2v^2 \pmod 8$. Si v es par, entonces $mn \equiv 1 \pmod 8$ y $\chi_8(\overline{n} \cdot \overline{m}) = 1$. Si v es impar, entonces $mn \equiv 7 \pmod 8$ y $\chi_8(\overline{nm}) = \left(\frac{8}{7}\right) = 1$.

□

Corolario 2.19. *Sea $D < 0$ discriminante fundamental y f_0 la forma principal con discriminante D. Entonces elementos coprimos con D representados por f_0 módulo D son exactamente las clases de B_D. Es decir, $H = B_D$.*

Demostración. Por el Teorema 2.17 sabemos que cualquier elemento de B_D es representado por f_0. Sabemos que el $1 \in B_D$ por definición y además está representado por la forma principal pues $f_0(1,0) = 1$. En consecuencia, aplicando la proposición anterior, si m es representado por f_0, entonces $\overline{m}B_D = \overline{1}B_D$ y por tanto $\overline{m} \in B_D$. □

Con este resultado conseguimos de forma directa el siguiente teorema:

Teorema 2.20. *Sea $D < 0$ discriminante fundamental y sea t el número de discriminantes primos que lo dividen. Entonces hay 2^{t-1} posibles géneros.*

Veamos varios ejemplos de discriminantes fundamentales y sus géneros:

Ejemplo 2.21. *$D = -39 = -3 \cdot 13$, entonces $t = 2$ y hay dos géneros, el primero formado por $[(1,1,10)]$ y $[(3,3,4)]$, que representan $B_{-39} = \{\overline{1}, \overline{4}, \overline{10}, \overline{16}, \overline{22}, \overline{25}\}$ y por otro lado, $[(2,1,5)]$ y $[(2,-1,5)]$, que representan $\{\overline{2}, \overline{5}, \overline{8}, \overline{11}, \overline{20}, \overline{32}\}$.*

Ejemplo 2.22. *$D = -260 = -4 \cdot 5 \cdot 13$, entonces $t = 3$ y hay 4 géneros:*

Clases en cada género	*Clases laterales de B_D representadas*
$[(1,0,65)]$, $[(9,8,9)]$	$B_{-260} = \{\overline{1}, \overline{9}, \overline{29}, \overline{49}, \overline{61}, \overline{69}, \overline{81}, \overline{101}, \overline{121}, \overline{129}, \overline{181}, \overline{209}\}$
$[(3,2,22)]$, $[(3,-2,22)]$	$\overline{3} \cdot B_{-260} = \{\overline{3}, \overline{23}, \overline{27}, \overline{43}, \overline{87}, \overline{103}, \overline{107}, \overline{127}, \overline{147}, \overline{183}, \overline{207}, \overline{243}\}$
$[(6,2,11)]$, $[(6,-2,11)]$	$\overline{11} \cdot B_{-260} = \{\overline{11}, \overline{19}, \overline{31}, \overline{59}, \overline{71}, \overline{99}, \overline{111}, \overline{119}, \overline{151}, \overline{171}, \overline{219}, \overline{239}\}$
$[(5,0,13)]$, $[(2,2,33)]$	$\overline{33} \cdot B_{-260} = \{\overline{33}, \overline{37}, \overline{57}, \overline{73}, \overline{93}, \overline{97}, \overline{137}, \overline{177}, \overline{193}, \overline{197}, \overline{213}, \overline{253}\}$

Se conocen solo 65 discriminantes fundamentales tales que hay una única clase por género. Los mostramos ordenándolos según el valor de t:

$t = 1 : D = -3, -4, -7, -8, -11, -19, -43, -67, -163.$
$t = 2 : D = -15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148,$
$-187, -232, -235, -267, -403, -427.$
$t = 3 : D = -84, -120, -132, -168, -195, -228, -280, -312, -340, -372, -408,$
$-435, -483, -520, -532, -555, -595, -627, -708, -715, -760, -795, -1012, -1435.$
$t = 4 : D = -420, -660, -840, -1092, -1155, -1320, -1380, -1428, -1540,$

$-1848, -1995, -3003, -3315$.
$t = 5 : D = -5460$.

De forma más general, en [3, §3, p. 44] encontramos siguiente teorema:

Teorema 2.23. *Sea $D \equiv 0, 1 \pmod 4$ negativo, y sea r el número de primos impares que dividen a D. Definimos $\mu(D)$ como r si $D \equiv 1 \pmod 4$ y si $D = -4n$*

$$\mu(D) = \begin{cases} r & n \equiv 3 \pmod 4, \\ r+1 & n \equiv 1, 2 \pmod 4 \text{ o } n \equiv 4 \pmod 8, \\ r+2 & n \equiv 0 \pmod 8. \end{cases}$$

Entonces existen $2^{\mu(D)-1}$ géneros de formas de discriminante D.

Observación 2.24. *Se puede comprobar que para los discriminantes fundamentales $\mu(D)$ coincide con el número de discriminantes primos que lo dividen, lo que hemos denotado como t durante toda la sección.*

Si recordamos el Lema 1.32 del primer capítulo, observamos que el número de géneros coincide con el cardinal de clases de orden menor o igual que 2. Y esto no es una coincidencia, de hecho, dado un discriminante $D = -4n$, todo género de formas de discriminante D consiste de una sola clase si y solo si todas las clases tienen orden menor o igual que 2. Esto nos da una forma de buscar discriminantes que solo tengan una clase por género. Gauss da una lista de 65 discriminantes que cumplen esta propiedad cerca del final de la quinta sección de *Disquisitiones Arithmeticae*[1]:

$h(-4n)$	valores de n
1	$1, 2, 3, 4, 7$
2	$5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58$
4	$21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102,$ $112, 130, 133, 177, 190, 232, 253$
8	$105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385,$ $408, 462, 520, 760$
16	$840, 1320, 1365, 1848$

2.2. Teorema de Duplicación de Gauss

El Teorema de Duplicación de Gauss nos permite caracterizar el género principal dado un discriminante. El Teorema dice lo siguiente:

Teorema 2.25. *[Teorema de Duplicación de Gauss] El género principal coincide con $C(D)^2$. Es decir, está formado por el cuadrado de las clases en $C(D)$.*

[1] Gauss tenía especial interés en estos números pues ya habían aparecido anteriormente en otro contexto. Son los denominados números idóneos, Euler bautizó así a los enteros que cumplían la siguiente condición: " Sea m un entero impar coprimo con n, representado propiamente por $x^2 + ny^2$. Si la ecuación $m = x^2 + ny^2$ tiene una solución única con x e y positivos, entonces m es un número primo ".

Siguiendo la teoría anterior, daremos nuestra demostración para discriminantes fundamentales. Antes debemos definir el siguiente homomorfismo:

Teorema 2.26. *Sea $D < 0$ un discriminante fundamental, entonces existe el siguiente homomorfismo sobreyectivo, $\omega_D : C(D) \to \ker(\chi_D)/B_D$ donde $\omega_D(\boldsymbol{C}) = \overline{m}B_D$, siendo m un entero positivo coprimo con D representado por una forma en la clase $\boldsymbol{C}$.*

Demostración. El Teorema 2.18 nos garantiza que esté bien definido, ya que si una forma representa a m y n enteros positivos coprimos con D, entonces $\overline{m}B_D = \overline{n}B_D$. Es un homomorfismo pues si $F(x,y) = f(x,y) \circ g(x,y)$, gracias a la Proposición 1.23, obtenemos que si $\omega_D(f) = \overline{m_1}B_D$ y $\omega_D(g) = \overline{m_2}B_D$, entonces $\omega_D(F) = \overline{m_1 m_2}B_D$. Finalmente para ver la sobreyectividad apelamos al Teorema de Dirichlet, que nos asegura la existencia de infinitos primos en cada clase de equivalencia módulo D. Por tanto, si $\overline{m} \in \ker(\chi_D)$, existe un primo p tal que $\overline{p} = \overline{m}$ y el Teorema 2.4 nos dice que existe una forma $f(x,y)$ de discriminante D que lo representa, por lo que, $\omega_D([f(x,y)]) = \overline{p}B_D = \overline{m}B_D$. □

Observación 2.27. *Dadas f_1 y f_2 formas de discriminante $D < 0$ fundamental que pertenecen a las clases $\boldsymbol{C}_1$ y $\boldsymbol{C}_2$ respectivamente. Si $\omega_D(\boldsymbol{C}_1) = \omega_D(\boldsymbol{C}_2)$, entonces f_1 y f_2 están en el mismo género.*

Ahora ya podemos demostrar el Teorema de Duplicación de Gauss:

Demostración. (*Teorema 2.25*) Sea $\omega_D : C(D) \to \ker(\chi_D)/B_D \cong \{\pm 1\}^{\mu(D)-1}$ el homomorfismo definido anteriormente, queremos ver que $C(D)^2 = \ker(\omega_D)$.
Por un lado, $C(D)^2 \subset \ker(\omega_D)$, ya que los elementos en $C(D)^2$ son de la forma $[F = f(x,y) \circ f(x,y)]$, y por el Lema 1.23 $[F]$ representa a m^2 para algún entero m coprimo con D representado por $f(x,y)$. Por tanto, para todo n representado por una clase en $C(D)^2$ se tiene que $\overline{n}B_D = \overline{m}^2 B_D$ y $\overline{m}^2 \in B_D$, pues $\chi_{d_j}(m^2) = 1$ para todo d_j discriminante primo que divide a D. Como consecuencia podemos definir el siguiente homomorfismo sobreyectivo: $C(D)/C(D)^2 \to \{\pm 1\}^{\mu(D)-1}$.

Por otro lado, definimos $C'(D) = \{\mathbf{C}_i \in C(D) : \text{orden de } \mathbf{C}_i \leq 2\}$, que tiene orden $2^{\mu(D)-1}$ por el Lema 1.32. Si aplicamos el Primer Teorema de Isomorfía al homomorfismo $C(D) \to C(D)^2 \subset C(D)$ que compone a cada clase con ella misma, tenemos que: $C(D)/C'(D) \cong C(D)^2$, por tanto $C(D)/C(D)^2$ tiene orden $2^{\mu(D)-1}$. Por lo que el homomorfismo $C(D)/C(D)^2 \to \{\pm 1\}^{\mu(D)-1}$ será un isomorfismo y esto nos dice que $C(D)^2 = \ker(\omega_D)$. □

2.3. Equivalencia modular. Enfoque inicial de Gauss

Como comentamos en la introducción, Gauss expone en *Disquisitiones Arithmeticae* [5] toda la Teoría de Números conocida hasta la época junto con importantes aportaciones suyas. En especial, es el primero en tratar la Teoría de géneros, que aparece desde el artículo 229 hasta el 287. Mientras que nuestro enfoque de la Teoría de géneros es un enfoque moderno, donde hacemos uso de los avances de la Teoría de Números, Gauss presentó esta nueva teoría desde una perspectiva distinta. Él se dio

cuenta de lo siguiente: dada f una forma de discriminante D cualquiera, los números representados por f guardan una relación estrecha si tomamos sus clases módulo los primos divisores de D. La idea es que dado un primo impar que divide a D, entonces f representará sólo restos cuadráticos o no restos cuadráticos módulo p. Además, si D es par, entonces los enteros impares que representa una forma f solo pueden tomar unas determinadas clases módulo 8. Según estas nuevas premisas, Gauss define los caracteres de formas cuadráticas, y a partir de ahí crea una nueva clasificación de las formas en géneros. Esto además nos permite conocer los distintos géneros sin necesidad de programarlo computacionalmente. Estudiemos en profundidad estos resultados.

Definición 2.28. *Sean $f(x,y)$ y $g(x,y)$ dos formas cuadráticas, decimos que son equivalentes módulo n, con $n>1$ natural, si existen enteros a,b,c,d tales que:*

$$f(x,y) \equiv g(ax+by, cx+dy) \pmod{n}, \qquad mcd(ad-bc,n)=1.$$

En este caso, $f(x,y)$ y $g(x,y)$ representarán los mismos enteros módulo n y usaremos la notación $f \sim_n g$ para facilitar la lectura de algunas demostraciones.

Nos fijamos en que la última condición nos permite que la matriz que nos lleva una forma a otra sea invertible módulo n. Veamos un ejemplo:

Ejemplo 2.29. *Sea $g(x,y)=5x^2+9xy-7y^2$. Estudiaremos su equivalencia módulo 7 al aplicarle el siguiente cambio de variables*

$$g(x-2y,3y), \text{ o, equivalentemente, } g\left(\begin{pmatrix}1 & -2\\ 0 & 3\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}\right).$$

Como el determinante de la matriz es 3, esta será invertible módulo 7 y podemos decir que $f(x,y)=g(x-2y,3y)=5x^2-14xy+8y^2\equiv 5x^2+y^2 \pmod 7$ es equivalente a $g(x,y)$. Se puede comprobar que invirtiendo la matriz módulo 7:

$$f\left(M^{-1}\begin{pmatrix}x\\ y\end{pmatrix}\right)=f\left(\begin{pmatrix}15 & 10\\ 0 & 5\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}\right)\equiv g(x,y) \pmod 7.$$

Por tanto, las formas cuadráticas

$$g(x,y)=5x^2+9xy-7y^2 \quad y \quad f(x,y)=5x^2-14xy+8y^2$$

son equivalentes módulo 7, es decir, podemos pasar de una a otra mediante un cambio de variables invertible en $\mathbb{Z}/7\mathbb{Z}$ y representarán los mismos enteros módulo 7.

Gracias al siguiente teorema, nos vamos a poder centrar en las congruencias entre formas módulo un primo.

Teorema 2.30. *Sean $m,n\in\mathbb{Z}^+$ coprimos. Dos formas cuadráticas son equivalentes módulo mn si y solo si son equivalentes módulo m y módulo n.*

Demostración. Vamos a suponer que $f(x,y)\equiv g(a_1x+a_2y,a_3x+a_4y) \pmod m$ y $f(x,y)\equiv g(b_1x+b_2y,b_3x+b_4y) \pmod n$. Aplicando el Teorema chino del resto encontramos enteros c_i tales que $c_i\equiv a_i \pmod m$ y $c_i\equiv b_i \pmod n$. Por tanto, $f(x,y)\equiv g(c_1x+c_2y,c_3x+c_4y) \pmod{mn}$ y se puede comprobar que el determinante de la matriz es coprimo con mn. El recíproco es directo. □

Por lo que fijado $D \equiv 0, 1 \pmod 4$ vamos a estudiar las equivalencias módulo p^n, con p primo impar, entre formas de discriminante D. Sea $f(x, y)$ forma de discriminante D, los Lemas 1.18 y 1.16 nos dicen que $f \sim ax^2 + bxy + cy^2$ con a representado por f y $mcd(a, p) = 1$. Aplicando la matriz

$$M = \begin{pmatrix} 1 & -b \\ 0 & 2a \end{pmatrix} \quad \text{con } det(M) = 2a,$$

obtenemos que $(a, b, c) \sim_{p^n} a(x^2 - Dy^2)$. Ahora, fijaremos un resto no cuadrático r módulo p (recordemos que la mitad de las unidades módulo p^n son cuadrados). Entonces $\overline{r}$ y $\overline{rx}^2$ no serán residuos cuadráticos módulo p^n. De hecho, $\overline{rx}^2$ recorre los no residuos cuadráticos si $\overline{x}^2$ recorre los cuadrados; es decir,

$$U(\mathbb{Z}/p^n\mathbb{Z}) = U^2(\mathbb{Z}/p^n\mathbb{Z}) \cup rU^2(\mathbb{Z}/p^n\mathbb{Z}).$$

Por lo que existen dos posibles opciones: $\overline{a} = \overline{u}^2$ o $\overline{a} = \overline{ru}^2$ para alguna unidad $\overline{u}$. Por tanto, al evaluar $a(x^2 - Dy^2)$ en $(\overline{u}^{-1}x, \overline{u}^{-1}y)$, obtenemos que:

$$\begin{array}{rcl} \overline{a} = \overline{u}^2 & \rightarrow & a(x^2 - Dy^2) \text{ equivalente a } x^2 - Dy^2 \pmod{p^n}, \\ \overline{a} = \overline{ru}^2 & \rightarrow & a(x^2 - Dy^2) \text{ equivalente a } r(x^2 - Dy^2) \pmod{p^n}. \end{array}$$

Así concluimos que si p es un primo impar, hay como máximo dos clases de equivalencia módulo p^n.

Estudiamos el caso donde $p \nmid D$. Sabemos que x^2 y $r + Dy^2$ toman cada uno $(p+1)/2$ valores módulo p (que es el número de los posibles restos cuadráticos módulo p). Luego existen $u, v \in \mathbb{Z}$ tales que $u^2 \equiv r + Dv^2 \pmod p$, equivalentemente, $r \equiv u^2 - Dv^2 \pmod p$. Por consiguiente $u^2 - Dv^2$ no es un resto cuadrático módulo p y puedo tomar $r = u^2 - Dv^2$. De esta forma, si evalúo $x^2 - Dy^2$ en $(ux + Dvy, vx + uy)$ llegamos a la forma $r(x^2 - Dy^2)$ y por tanto, $x^2 - Dy^2 \sim_{p^n} r(x^2 - Dy^2)$. Es decir, si $p \mid D$ solo habrá una clase de equivalencia módulo p^n.

Si $p \mid D$, dada una forma $f(x, y)$ de discriminante D esta puede ser equivalente a $x^2 - Dy^2 \equiv x^2 \pmod p$, y en este caso $f(x, y)$ representa residuos cuadráticos módulo p o $f(x, y)$ es equivalente a $r(x^2 - Dy^2)$, y en este caso representará restos no cuadráticos módulo p. Lo resumimos en el siguiente teorema:

Teorema 2.31. *Sea p un primo impar.*

1. *Si $p \mid D$, toda forma cuadrática de discriminante D es equivalente módulo p^n a solo una de las siguientes formas cuadráticas:*

$$x^2 - Dy^2 \qquad o \qquad r(x^2 - Dy^2).$$

   Si es equivalente a la primera, entonces representa restos cuadráticos módulo p y si es equivalente a la segunda, representará restos no cuadráticos módulo p.

2. *Si $p \nmid D$, todas las formas de discriminante D son equivalentes módulo p^n.*

A raíz de esto, Gauss definió lo siguiente:

Definición 2.32. *Sea f forma cuadrática de discriminante D y p un primo impar.*

1. *Si $p \mid D$, decimos que f tiene carácter positivo módulo p si representa restos cuadráticos módulo p. En caso contrario diremos que tiene carácter negativo. Gracias a la teoría anterior podemos definir el carácter de f así:*

$$\chi_p(f) = \left(\frac{a}{p}\right),$$

   donde a es cualquier entero representado por $f(x, y)$.

2. *Si $p \nmid D$, entonces definimos $\chi_p(f) = 1$.*

El carácter módulo p está bien definido por el teorema anterior y además, dado que formas de una misma clase representan los mismos enteros, podríamos definir $\chi_p(\mathbf{C})$, el carácter de una clase $\mathbf{C}$.

Nos quedaría estudiar el caso $p = 2$. Antes de comenzar nos fijamos en que se tiene la equivalencia: $D \equiv 1 \pmod 8$ si y solo si ac es par.

Teorema 2.33. *Sea $D \equiv 1 \pmod 4$. Si $D \equiv 1 \pmod 8$ toda forma cuadrática de discriminante D es equivalente a xy módulo 2^n. Si $D \not\equiv 1 \pmod 8$, entonces toda forma es equivalente a $x^2 + xy + y^2$ módulo 2^n.*

Antes de comenzar la demostración daremos el siguiente lema:

Lema 2.34. *Un número impar a es residuo cuadrático módulo 2^k, con $k \geq 3$ si y solo si $a \equiv 1 \pmod 8$.*

Demostración. Es fácil comprobar que un número impar es residuo cuadrático módulo 8 si y solo si es equivalente a 1 módulo 8. Veamos que si a es resto cuadrático módulo 2^k entonces lo es módulo 2^{k+1}. En efecto, si $a = r^2 + m2^k$, entonces

$$(r + m2^{k-1})^2 = r^2 + m2^k + m^2 2^{2k-2} \equiv a \pmod{2^{k+1}}$$

si $k \geq 3$ (pues entonces $2k - 2 \geq k + 1$). Por tanto, si $a \equiv 1 \pmod 8$ entonces será residuo cuadrático módulo 2^{k+1} para $k \geq 3$. □

Demostración. (*Teorema* 2.33). Sea $f(x,y)$ forma cuadrática de discriminante D, por los Lemas 1.18 y 1.16, $f(x,y) \sim ax^2+bxy+cy^2$ con a impar representado por f. Como b es impar, entonces evaluando en (x, yb^{-1}) llegamos a que $f \sim_{2^n} (a,1,c')$. Si $D \equiv 1 \pmod 8$, entonces c será par y por tanto $f \sim_{2^n} (a,1,2c'')$.

Si evaluamos la forma xy en $(x+2uy, ax+vy)$ con $u,v \in \mathbb{Z}$ y v impar, entonces $xy \sim_{2^n} (a, 2au+v, 2uv)$. Teniendo en cuenta esta última congruencia, podremos concluir que $f(x,y)$ es equivalente a xy módulo 2^n si vemos que

$$\begin{cases} v+2au \equiv & 1 \pmod{2^n}, \\ uv \equiv & c'' \pmod{2^n}. \end{cases}$$

Multiplicando por v la primera congruencia y usando la segunda queda

$$v^2 - v \equiv -2ac'' \pmod{2^n}.$$

Por tanto, solo tenemos que ver que existe v impar solución de esta congruencia. Multiplicando por 4 a ambos lados y reordenando la congruencia queda:

$$(2v-1)^2 \equiv 1 - 8ac'' \pmod{2^{n+2}},$$

la cual tiene solución gracias al Lema 2.34.

Nos queda ver el caso $D \not\equiv 1 \pmod 8$. Existen [2] p,q enteros con p impar tales que: $ap^2+bpq+cq^2 \equiv 1 \pmod{2^n}$. Entonces si evaluamos la forma (a,b,c) en $(px, qx+y)$, nos queda que $(a,b,c) \sim_{2^n} (1,b',c)$ con b' impar. Si evaluamos esta última forma en (x, yb^{-1}), obtenemos que $(1,b',c) \sim_{2^n} (1,1,c')$ con c' impar, es decir, $c' = 2k+1$ para algún k entero. Concluimos que $(a,b,c) \sim_{2^n} (1,1,2k+1)$.

Por otro lado, evaluando x^2+xy+y^2 en $(x+ry, sy)$ con s impar vemos que $(1,1,1) \sim_{2^n} (1, 2r+s, r^2+rs+s^2)$. Por lo tanto, para ver que $(1,1,1)$ y $(1,1,2k+1)$ son equivalentes módulo 2^n, tenemos que encontrar r,s enteros, con s impar tales que:

$$\begin{cases} 2r+s \equiv & 1 \pmod{2^n}, \\ r^2+rs+s^2 \equiv & 2k+1 \pmod{2^n}. \end{cases}$$

Al despejar r llegaríamos a que $r^2 - r \equiv \text{par} \pmod{2^n}$, que es la ecuación que hemos resuelto en el caso anterior y sabemos que existe la solución que buscábamos. □

Por último, nos quedaría ver las congruencias módulo 2^n entre formas con discriminante D par. Sea $f=(a,b,c)$ forma de discriminante D, en este caso b es par y al igual que en la demostración anterior, podemos suponer a impar. Evaluando f en $(x-(b/2)y, ay)$, llegamos a que $f \sim_{2^n} a(x^2 - D'y^2)$ con $D' = D/4$.

Definimos $r = \pm 1, \pm 5$ de tal forma que $a \equiv r \pmod 8$, y sea $u \equiv r^{-1} \pmod 8$. Entonces $ua \equiv 1 \pmod 8$ y por el Lema 2.34 existe un k impar tal que $k^2 \equiv au \pmod{2^n}$. Por tanto $a \equiv rk^2 \pmod{2^n}$ y evaluando la forma $a(x^2 - D'y^2)$ en $(k^{-1}x, k^{-1}y)$ nos queda que esta es equivalente módulo 2^n a

$$r(x^2 - D'y^2), \qquad r = \pm 1, \pm 5. \tag{2.1}$$

[2] La demostración de la existencia se puede ver en [2, §14.1, p. 499].

Luego parece que las clases van a depender de qué impares módulo 8 representa f. Ahora vamos a ver que si $x^2-D'y^2$ representa a r módulo 8, entonces será equivalente a la forma (2.1) módulo 2^n. En efecto, si existen enteros u y v tales que $A = u^2-D'v^2 \equiv r \pmod 8$, entonces al evaluar $x^2-D'y^2$ en $(ux+D'vy, vx+uy)$ queda $A(x^2-D'y^2)$. Con un proceso análogo al anterior llegamos a que $x^2-D'y^2$ es equivalente a $r(x^2-D'y^2)$ módulo 2^n para el r considerado.

En vista de lo anterior estudiamos qué impares módulo 8 representa $x^2-D'y^2$ en función del valor de D' módulo 8:

D'	0	1	2	3	4	5	6	7
r	1	±1	±1	1	1	±1	1	1
		±5		5	5	±5	-5	5

Veamos varios ejemplos de como interpretar la tabla:
Si $D' = D/4 \equiv 3,4,7 \pmod 8$, entonces $x^2-D'y^2$ representa impares congruentes con $1,5$ módulo 8, por tanto, $x^2-D'y^2 \sim_{2^n} 5(x^2-D'y^2)$, de donde se sigue que $-(x^2-D'y^2) \sim_{2^n} -5(x^2-D'y^2)$. Por ello habrá dos clases de equivalencia módulo 2^n, la primera representa impares congruentes con $1,5$ módulo 8 y la segunda impares congruentes con $-1,-5$ módulo 8.
Si $D/4 \equiv 1,5 \pmod 8$, la forma $x^2-D'y^2$ es equivalente módulo 2^n a $r(x^2-D'y^2)$ para $r = \pm1, \pm5$, es decir, todas las formas son congruentes módulo 2^n. Luego no podemos acotar qué impares representa una forma cuadrática módulo 8.

En conclusión, dada una forma de discriminante D par, para determinar qué clase es módulo 2^n tenemos que fijarnos en qué impares representa módulo 8. Por lo que, ya no basta con ver el Símbolo de Legendre de un elemento representado por $f(x,y)$, ahora vamos a tener que considerar los siguientes caracteres:

$$\delta(k) = \left(\frac{-1}{k}\right) = \begin{cases} 1 & \text{si} \quad k \equiv 1,5 \pmod 8, \\ -1 & \text{si} \quad k \equiv -1,-5 \pmod 8, \end{cases}$$

$$\epsilon(k) = \left(\frac{2}{k}\right) = \begin{cases} 1 & \text{si} \quad k \equiv 1,-1 \pmod 8, \\ -1 & \text{si} \quad k \equiv 5,-5 \pmod 8, \end{cases}$$

$$\delta\epsilon(k) = \left(\frac{-2}{k}\right) = \begin{cases} 1 & \text{si} \quad k \equiv 1,-5 \pmod 8, \\ -1 & \text{si} \quad k \equiv -1,5 \pmod 8. \end{cases}$$

Donde vemos que módulo 8 el carácter δ distingue a las clases $\{1,5\}$ de $\{-1,-5\}$, ϵ distingue las clases $\{1,-1\}$ de $\{-5,5\}$ y $\delta\epsilon$ distingue las clases $\{1,-5\}$ de $\{-1,5\}$. Por lo que definiremos el carácter módulo 2 de una forma f de la siguiente forma:

$$\chi_2(f) = \begin{cases} 1 & \text{si} \quad D/4 \equiv 1,5 \pmod 8, \\ \epsilon(a) & \text{si} \quad D/4 \equiv 2 \pmod 8, \\ \delta(a) & \text{si} \quad D/4 \equiv 3,4,7 \pmod 8, \\ \delta\epsilon(a) & \text{si} \quad D/4 \equiv 6 \pmod 8. \end{cases}$$

donde a es un entero representado por f. Con esta nueva definición y con la tabla, podemos dar el siguiente teorema:

Teorema 2.35. *Si p es primo y $p \mid D$, dos formas cuadráticas de discriminante D son equivalentes módulo p^n si y solo si tienen el mismo carácter módulo p.*

La conclusión de este apartado es que vamos a poder clasificar las formas de discriminante D en función de si representan restos cuadráticos o no módulo p para todo $p \mid D$. En caso de ser D par, también las clasificaremos según si representan los mismos impares o no módulo 8. Es decir, hemos conseguido llegar a la noción de géneros desde otro camino distinto. En este caso, diremos que dos formas pertenecen al mismo género si tienen los mismos caracteres. Veamos varios ejemplos:

Ejemplo 2.36. *Volvemos a nuestro discriminante $D = -20$ para cerciorarnos de que estamos hablando de lo mismo. Como $D/4 = -5 \equiv 3 \pmod 8$, la tabla nos dice que una forma cuadrática de discriminante -20 puede representar impares congruentes con $\{1, 5\}$ o $\{-1, -5\} \pmod 8$. Para estudiarlo necesitamos el carácter $\chi_2 = \delta$. Tenemos la siguiente tabla:*

$D = -20$	δ	χ_5
$x^2 + 5y^2$	$+$	$+$
$2x^2 + 2xy + 3y^2$	$-$	$-$

La primera fila nos dice que x^2+5y^2 representa enteros congruentes con $1, 4 \pmod 5$ y $1, 5 \pmod 8$. Por el Teorema chino del resto, son congruentes con $1, 9, 29, 21 \pmod{40}$. Por consiguiente, si $x^2 + 5y^2$ representa un entero m, entonces $m \equiv 1, 9 \pmod{20}$. Análogamente, la segunda fila dice que $2x^2 + 2xy + 3y^2$ representa enteros de la forma $m \equiv 2, 3 \pmod 5$ y $m \equiv -1, -5 \pmod 8$; equivalentemente, $m \equiv 3, 7, 23, 27 \pmod{40}$ y por tanto, $m \equiv 3, 7 \pmod{20}$, que son los resultados que conocíamos.

Ejemplo 2.37. *Si $D = 60 = 3 \cdot 4 \cdot 5$, entonces $D/4 = 15 \equiv 7 \pmod 8$. El carácter χ_2 será δ, y una forma de discriminante 60 puede representar impares congruentes con $\{1, 5\}$ o $\{-1, -5\}$ módulo 8. En la siguiente tabla se muestran varias formas cuadráticas de discriminante $D = 60$ y sus correspondientes caracteres.*

$D = 60$	δ	χ_3	χ_5
$x^2 - 15y^2$	$+$	$+$	$+$
$15x^2 - y^2$	$-$	$-$	$+$
$3x^2 - 5y^2$	$-$	$+$	$-$
$5x^2 - 3y^2$	$+$	$-$	$-$

Ejemplo 2.38. *Si $D = -28$, entonces $D/4 \equiv 1 \pmod 8$. Dada f forma de discriminante D, $\chi_2(f) = 1$, por lo que representará cualquier impar módulo 8. En particular, solo hay una clase de formas cuadráticas y su tabla de caracteres es la siguiente:*

$D = -28$	χ_2	χ_7
$x^2 + 7y^2$	$+$	$+$

Lo que quiere decir que $x^2 + 7y^2$ representa cualquier impar módulo 8 y enteros que sean restos cuadráticos módulo 7.

Ejemplo 2.39. *Para $D = -504 = -8 \cdot 3^2 \cdot 7$, como $D/4 \equiv 2 \pmod 8$, una forma f de discriminante -504 representa impares congruentes con $\{1, -1\}$ módulo 8 si $\epsilon(f)$*

es positivo y congruentes con $\{5,-5\}$ *módulo* 8 *si* $\epsilon(f)$ *es negativo. También se puede ver si representan restos cuadráticos o no módulo* 3 *(*$\chi_3(f)$ *es positivo o negativo) y restos cuadráticos o no módulo* 7 *(*$\chi_7(f)$ *es positivo o negativo).*
Si $D=-480=-2^5\cdot 3\cdot 5$*, en este caso como* $D/4\equiv 0 \pmod 8$*, una forma de discriminante* -480 *representa impares congruentes a una única clase módulo* 8 *y por tanto tenemos que estudiar los* 3 *posibles caracteres módulo* 2 *de cada forma cuadrática. Representamos los caracteres en una tabla:*

$D=-504$	ϵ	χ_3	χ_7
x^2+126y^2	$+$	$+$	$+$
$9x^2+14y^2$	$+$	$-$	$+$
$2x^2+63y^2$	$+$	$-$	$+$
$7x^2+18y^2$	$+$	$+$	$+$
$5x^2+4xy+26y^2$	$-$	$-$	$-$
$10x^2-4xy+13y^2$	$-$	$+$	$-$
$5x^2-4xy+26y^2$	$-$	$-$	$-$
$10x^2+4xy+13y^2$	$-$	$+$	$-$

$D=-480$	ϵ	δ	$\delta\epsilon$	χ_3	χ_5
x^2+120y^2	$+$	$+$	$+$	$+$	$+$
$4x^2+4xy+31y^2$	$-$	$+$	$-$	$+$	$+$
$8x^2+15y^2$	$-$	$+$	$-$	$-$	$-$
$8x^2+8xy+17y^2$	$+$	$+$	$+$	$-$	$-$
$3x^2+40y^2$	$-$	$-$	$+$	$+$	$-$
$12x^2+12xy+13y^2$	$+$	$-$	$-$	$+$	$-$
$5x^2+24y^2$	$+$	$-$	$-$	$-$	$+$
$11x^2+2xy+11y^2$	$-$	$-$	$+$	$-$	$+$

Estos últimos ejemplos son muy útiles pues permiten apreciar toda la teoría expuesta en las páginas anteriores. Por un lado, nos permiten distinguir los distintos géneros que hay de forma visual, e incluso podemos ver qué clases pertenecen a un mismo género (que serán aquellas que tengan los mismos caracteres). Además como hemos hecho en los primeros ejemplos, sabremos qué unidades módulo D representan cada clase de formas cuadráticas, pues conocemos qué unidades módulo p representan para cada p primo divisor de D.

Además, nos fijamos en que cualquier forma compuesta con ella misma va a tener todos los caracteres positivos, pues si nos fijamos en los caracteres χ_p siendo p un primo impar, al multiplicar dos restos no cuadráticos obtenemos un resto cuadrático módulo p. Si observamos χ_2, cualquier impar al cuadrado es congruente con 1 (mod 8) y los subconjuntos de impares de la forma $\{-1,-5\},\{5,-5\}$ y $\{-1,5\}$ módulo 8 cumplen que al multiplicarlos con ellos mismo devuelven el subconjunto restante de impares módulo 8, que será el que contiene al 1 y el representado por la forma principal. Es decir, las clases al cuadrado van a tener todos los caracteres positivos y por tanto están en el género principal; que es resultado del Teorema de Duplicación de Gauss.

2.4. Resolución de conjeturas iniciales

No podíamos terminar este trabajo sin dar una demostración a las conjeturas iniciales que llevaron al desarrollo de toda esta teoría, las cuales veremos que son casos muy directos dentro de la Teoría de géneros.

Teorema 2.40. *Sea* p *primo, entonces* $p=x^2+y^2$ *para ciertos* $x,y\in\mathbb{Z}$ *si y solo si* $p=2$ *o* $p\equiv 1 \pmod 4$.

Demostración. Llamemos $f_1(x,y)=x^2+y^2$, entonces el discriminante de f_1 es $D=-4$. La forma f_1 representa a $p=2$ pues $f_1(1,1)=2$. Por otro lado, dado

p un primo impar, sabemos por el Teorema 2.4 que p es representado por una forma de discriminante $D = -4$ si y solo si -4 es residuo cuadrático módulo p. Equivalentemente:

$$\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4.$$

Si vemos que la única forma reducida con este discriminante es f_1, entonces esta ha de representar a todo primo p con $p \equiv 1 \pmod 4$. Sea $g = (a, b, c)$ forma reducida de discriminante -4, entonces $a^2 \leq -D/3 = 4/3$ y b ha de ser par. Por tanto, la única opción es $a = 1$ y $b = 0$ se tiene que cualquier forma reducida es $g = x^2 + y^2$. □

Teorema 2.41. *Sea p primo, entonces $p = x^2 + 2y^2$ para ciertos $x, y \in \mathbb{Z}$ si y solo si $p \equiv 1, 3 \pmod 8$.*

Demostración. Llamemos $f_2(x, y) = x^2 + 2y^2$, entonces el discriminante de f_2 es $D = -8$. Dado p un primo impar, sabemos por el Teorema 2.4 que p es representado por una forma de discriminante $D = -4$ si y solo si $\left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right) = 1$. Por tanto hay dos opciones:

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = 1 \iff \left\{ \begin{array}{rc} p \equiv & 1, -1 \pmod 8 \\ p \equiv & 1 \pmod 4 \end{array} \right\} \to p \equiv 1 \pmod 8,$$

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = -1 \iff \left\{ \begin{array}{rc} p \equiv & 3, -3 \pmod 8 \\ p \equiv & 3 \pmod 4 \end{array} \right\} \to p \equiv 3 \pmod 8.$$

Por lo que si p primo es representado por una forma de discriminante -8 si y solo si $p \equiv 1, 3 \pmod 8$. Si vemos que la única forma reducida con este discriminante es f_2, entonces esta ha de representar a p y ya tendríamos el resultado que buscamos. Sea $g = (a, b, c)$ forma reducida de discriminante -8, entonces $a^2 \leq -D/3 = 8/3$ y b es par. Por tanto, la única opción es $a = 1$ y $b = 0$ y se tiene que $g(x, y) = x^2 + 2y^2$. □

Teorema 2.42. *Sea p primo, entonces $p = x^2 + 3y^2$ para ciertos $x, y \in \mathbb{Z}$ si y solo si $p = 3$ o $p \equiv 1 \pmod 3$.*

Demostración. Llamemos $f_3(x, y) = x^2 + 3y^2$, entonces el discriminante de f_3 es $D = -12$. El caso $p = 3$ es directo, pues $f_3(0, 1) = 3$. Si p es un primo impar, sabemos por el Teorema 2.4 que p es representado por una forma de discriminante $D = -12$ si y solo si

$$\left(\frac{-12}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1,$$

equivalentemente, $p \equiv 1 \pmod 3$.

Si vemos que la única forma reducida con este discriminante es f_3, entonces esta ha de representar a todo primo $p \equiv 1 \pmod 3$ y ya tendríamos el resultado que buscamos. Sea $g = (a, b, c)$ forma reducida de discriminante -12, entonces $a^2 \leq 12/3 = 4$ y b par. Si $a = 1$ y $b = 0$, $g = x^2 + 3y^2$, que es reducida. La otra opción sería $a = 2$, si $b = 0$, entonces no existe c tal que $c = (b^2 - D)/4a$, y si $b = 2$ entonces la forma que queda es $2x^2 + 2xy + 2y^2$, la cual no es primitiva y por tanto tampoco es reducida. Es decir, la única forma reducida es $f_3(x, y) = x^2 + 3y^2$. □

APÉNDICE A

Reciprocidad cuadrática. Símbolos de Legendre y de Jacobi

Esta primera sección del Apéndice la dedicaremos a repasar resultados vistos en el grado relativos a la Reciprocidad cuadrática y el Símbolo de Legendre y Jacobi, pues son de gran utilidad para este trabajo y se usan con relativa frecuencia.

Lema A.1. *Sean r, s enteros impares, entonces:*

$$\frac{r-1}{2} + \frac{s-1}{2} \equiv \frac{rs-1}{2} \pmod 2.$$

Demostración. Si $r \equiv s \pmod 4$, entonces $r + s \equiv rs + 1 \equiv 2 \pmod 4$ y si, en caso contrario $r \equiv 3 \pmod 4$ y $s \equiv 1 \pmod 4$, entonces $r + s \equiv rs + 1 \equiv 0 \pmod 4$. En cualquier caso, si r y s son impares, entonces $r + s \equiv rs + 1 \pmod 4$ y el lema es resultado directo de esta equivalencia. □

Lema A.2. *Sean r, s impares, entonces:*

$$\frac{r^2-1}{8} + \frac{s^2-1}{8} \equiv \frac{r^2s^2-1}{8} \pmod 2.$$

Demostración. Si r es impar, se puede comprobar que:

$$r^2 \equiv \begin{cases} 1 \pmod{16} & si\ r \equiv \pm 1 \pmod{16}, \\ 9 \pmod{16} & si\ r \equiv \pm 3 \pmod{16}, \\ 9 \pmod{16} & si\ r \equiv \pm 5 \pmod{16}, \\ 1 \pmod{16} & si\ r \equiv \pm 7 \pmod{16}. \end{cases}$$

Si $r^2 \equiv s^2 \pmod{16}$, entonces $r^2s^2 + 1 \equiv r^2 + s^2 \equiv 2 \pmod{16}$. Mientras que si $r^2 \not\equiv s^2 \pmod{16}$, se tiene que $r^2s^2 + 1 \equiv r^2 + s^2 \equiv 10 \pmod{16}$. En cualquier caso $r^2s^2 + 1 \equiv r^2 + s^2 \pmod{16}$, y directamente podemos obtener la igualdad del lema. □

Ahora ya comenzaremos la sección con la siguiente definición:

Definición A.3. *Sean m, n enteros con $n > 0$. Decimos que m es residuo cuadrático módulo n si $m \equiv x^2 \pmod n$ para algún entero x.*

En concreto, observamos que los residuos cuadráticos módulo p son:

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

Pues $(p-a)^2 \equiv a^2 \pmod{p}$, por lo que podemos suponer $a \leq \frac{p-1}{2}$. En general, la mitad de las unidades módulo p^n serán cuadrados.

Definición A.4. *Sea a entero y p primo impar. Definimos el Símbolo de Legendre de la siguiente forma:*

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

Vamos a ver ciertas propiedades que cumple el Símbolo de Legendre. La ley más importante es la siguiente:

Teorema A.5. *(Ley de Reciprocidad Cuadrática). Sean p y q primos impares, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Lema A.6. *(Leyes suplementarias) Sea p primo impar, entonces:*

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

Lema A.7. *(Criterio de Euler) Sea p primo impar y sea a un entero coprimo con p. Entonces*

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

Demostración. Las raíces de $x^{(p-1)} - 1$ en $\mathbb{Z}/p\mathbb{Z}$ son las clases $1, 2, ..., p-1$ (todas salvo el 0). Además

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

Si $x \equiv a^2 \pmod{p}$, anula el primer factor (por el pequeño teorema de Fermat) y si $x \not\equiv a^2 \pmod{p}$, debe anular el segundo factor. Por lo que en el primer caso tenemos que:

$$\left(\frac{x}{p}\right) = 1 \quad \text{y} \quad x^{\frac{p-1}{2}} = 1.$$

En el segundo caso:

$$\left(\frac{x}{p}\right) = -1 \quad \text{y} \quad x^{\frac{p-1}{2}} = -1.$$

□

El criterio de Euler nos permite obtener varios resultados:

Corolario A.8. *Sea p primo impar y a, b enteros cualesquiera. Entonces:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demostración. Si $p \mid a$ o $p \mid b$ entonces es trivial. Si $p \nmid a$ y $p \nmid b$, entonces:

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

Como el símbolo de Legendre es 1 o -1, probar la congruencia módulo p supone probar la igualdad.

Para $p = 2$ la igualdad se consigue gracias al Lema A.1. □

Gracias al criterio de Euler también podemos demostrar las leyes suplementarias.

Demostración. (Leyes suplementarias)

Para la primera Ley suplementaria basta sustituir $a = -1$ en el Criterio de Euler.

Para la segunda Ley suplementaria queremos ver que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Sea $P = \frac{p-1}{2}$, usando las siguientes igualdades

$$1 = (-1)(-1), \quad 2 = (2)(-1)^2, \quad 3 = (-3)(-1)^3, \quad \ldots \quad , P = (\pm P)(-1)^P,$$

y sacando factor común a -1 podemos escribir:

$$P! = (-1)^{1+2+\ldots+P} \cdot (-1) \cdot 2 \cdot (-3) \cdot \ldots \cdot (\pm P).$$

Nos fijamos en el lado derecho y sustituimos los términos impares de la siguiente forma:

$$-1 \equiv 2P \pmod{p}, -3 \equiv 2(P-1) \pmod{p}, \ldots$$

Nos queda:

$$(-1)^{1+\ldots+P} \cdot (-1) \cdot 2 \cdot \ldots \cdot (\pm P) \equiv (-1)^{\frac{P(P+1)}{2}} \cdot 2 \cdot 4 \cdot \ldots \cdot 2(P-1) \cdot 2P \pmod{p}.$$

Sacando factor común a 2 queda la siguiente igualdad:

$$P! \equiv (-1)^{\frac{P(P+1)}{2}} \cdot 2^P \cdot P! \pmod{p}.$$

Por lo tanto, $2^P \equiv (-1)^{\frac{P(P+1)}{2}} \pmod{p}$ y aplicando el criterio de Euler junto con la igualdad $\frac{P(P+1)}{2} = \frac{p^2-1}{8}$ concluimos lo que queríamos. □

Podemos observar que el Símbolo de Legendre solo está definido para números primos; es aquí donde aparece el Símbolo de Jacobi, que es una extensión para números impares:

Definición A.9. *Sean n, m enteros coprimos con $m > 0$ impar. Definimos el símbolo de Jacobi:*

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{k} \left(\frac{n}{p_i}\right)^{e_i}.$$

donde $p_1^{e_1} \dots p_k^{e_k} = m$ es su factorización en números primos.

Proposición A.10. *El Símbolo de Jacobi cumple la Ley de reciprocidad cuadrática y las Leyes suplementarias:*

- $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$,
- $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$,
- $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$.

Demostración. Demostramos la primera Ley suplementaria: si $m = p_1^{e_1} \dots p_k^{e_k}$ es la factorización en primos, tendríamos que

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)^{e_i} = (-1)^{\sum_{i=1}^{k} e_i (p_i - 1)/2}.$$

Aplicando el Lema A.1 sucesivamente a la suma obtenemos lo siguiente:

$$\sum_{i=1}^{k} \frac{e_i(p_i - 1)}{2} \equiv \frac{\prod_{i=1}^{k} p_i^{e_i} - 1}{2} \equiv \frac{m-1}{2} \pmod 2.$$

Para demostrar la segunda ley suplementaria el proceso es análogo pero apoyándonos en el Lema A.2. Finalmente para la demostración de la reciprocidad cuadrática en el Símbolo de Jacobi observamos que si $m = p_1 \dots p_k$ y $n = q_1 \dots q_l$ entonces:

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l} \left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{l} \frac{(p_i-1)}{2}\frac{(q_j-1)}{2}}.$$

Aplicando el Lema A.1 inductivamente llegamos a que:

$$\sum_{i=1}^{k}\sum_{j=1}^{l} \frac{(p_i-1)}{2}\frac{(q_j-1)}{2} \equiv \frac{n-1}{2}\sum_{i=1}^{k}\frac{(p_i-1)}{2} \equiv \frac{n-1}{2}\frac{m-1}{2} \pmod 2.$$

□

APÉNDICE B

Resultados relativos a discriminantes fundamentales

En este apartado daremos las demostraciones relativas a discriminantes fundamentales y discriminantes primos, recordemos las definiciones:

Definición B.1. *Sea $D \in \mathbb{Z}\backslash\{0,1\}$ con $D \equiv 0,1 \pmod 4$. Decimos que D es un discriminante fundamental si no es divisible por ningún cuadrado de un primo impar y es impar o $D \equiv 8$ o $D \equiv 12 \pmod{16}$. Decimos que d es un discriminante primo si es un discriminante fundamental divisible solo por un único primo.*

Antes de comenzar, daremos varios lemas previos que vamos a necesitar en las demostraciones:

Lema B.2. *Sea D un discriminante fundamental par. Entonces $D/4 \equiv 2 \pmod 4$ o $D/4 \equiv 3 \pmod 4$. En ambos casos, el entero $D/4$ es libre de cuadrados.*

Demostración. Si D es par entonces $D = 8 + 16k$ o $D = 12 + 16l$. En cualquier caso podemos dividir entre 4 obteniendo $D/4 = 2 + 8k$ en el primer caso, lo que implica $D/4 \equiv 2 \pmod 4$, y en el segundo caso, $D/4 = 3+4l$, y por tanto $D/4 \equiv 3 \pmod 4$. □

Lema B.3. *Sea d entero libre de cuadrados satisfaciendo $d \equiv 2,3 \pmod 4$, entonces $4d$ es un discriminante fundamental.*

Demostración. Obviamente $4d \equiv 0 \pmod 4$ y además $4d \neq 0,1$. Por otro lado, como d es libre de cuadrados, $4d$ no es divisible por un primo impar al cuadrado. Además, si $d = 2+4k$, entonces $4d \equiv 8 \pmod{16}$ y si $d = 3+4k$, entonces $4d \equiv 12 \pmod{16}$. □

Lema B.4. *Sea D discriminante fundamental divisible por 8. Si reordenamos su descomposición en discriminantes primos de la siguiente forma: $D = d_1 \dots d_t$ con $d_1 = \pm 8$, entonces si $d_1 = -8$, $D/4 \equiv 6 \pmod 8$ y si $d_1 = 8$, $D/4 \equiv 2 \pmod 8$.*

Demostración. Si $d_1 = -8$ entonces $D = -8 \cdot d_2 \dots d_t$ con $d_2 \dots d_t \equiv 1 \pmod 4$ pues cada d_i es un discriminante primos impar. Entonces existe un entero k tal que $\frac{D}{-8} = 1 + 4k$, y multiplicando por -2, obtenemos la congruencia $\frac{D}{4} \equiv 6 \pmod 8$. Para $d_1 = 8$, la prueba es análoga. □

Demostración de la Proposición 2.12

Demostración. Procedemos por inducción en t, el número de divisores primos de D. Si $t = 1$, entonces D es un discriminante fundamental primo. Suponemos la hipótesis cierta hasta t y consideramos D, discriminante fundamental divisible entre $t+1$ divisores primos. Esto significa que existe al menos un primo impar p que divide a D. Sea $d_p \equiv 1 \pmod 4$ el correspondiente discriminante primo. Si tomamos $D' = D/d_p$ y vemos que es un discriminante fundamental, entonces aplicando la hipótesis de inducción sobre D' obtenemos la factorización que buscábamos de D pues $D = D' \cdot d_p$.

Si $D \equiv 0 \pmod 4$ el Lema B.2 nos dice que $D = 4n$ con $n \equiv 2$ o $3 \pmod 4$ y libre de cuadrados y por tanto, $D' = 4n/d_p$. Si llamo $m = n/d_p$, entonces m es un entero libre de cuadrados y $m \equiv 2$ o $3 \pmod 4$. Como $D' = 4m$, el Lema B.3 nos dice que D' es un discriminante fundamental.

Si $D \equiv 1 \pmod 4$, entonces D es divisible por $t+1$ primos impares distintos y es libre de cuadrados. Por lo que $D' = D/d_p \equiv 1 \pmod 4$ y es libre de cuadrados, por tanto D' es discriminante fundamental.

□

Demostración del Teorema 2.13

Demostración. Antes de comenzar la demostración es conveniente observar que si d_i es un discriminante fundamental primo, entonces $d_i \equiv 0, 1 \pmod 4$ y por tanto está bien definido el homomorfismo χ_{d_i}. Sea m entero coprimo con D, separamos la prueba en casos:

1. Si $D \equiv 1 \pmod 4$ entonces, $\chi_D(m) = \left(\dfrac{m}{|D|}\right)$ con $|D| = |d_1| \dots |d_t|$, con d_i primo impar para $i = 1, \dots, t$. Por la definición del símbolo de Jacobi tenemos:

$$\chi_D(m) = \left(\frac{m}{|D|}\right) = \left(\frac{m}{|d_1|}\right) \dots \left(\frac{m}{|d_t|}\right) = \chi_{d_1}(m) \dots \chi_{d_t}(m).$$

2. Si $D \equiv 0 \pmod 4$, podemos reordenar la factorización y llamar d_1 al discriminante primo par ($d_1 = -4, 8$ o -8). Escribiendo $D = 2^c u$ con u impar, se puede comprobar caso a caso que $\chi_D(m) = \chi_{d_1}(m)\left(\frac{m}{|u|}\right)$ donde $|u| = |d_2| \dots |d_t|$. Tenemos lo siguiente:

$$\chi_D = \chi_{d_1}(m)\left(\frac{m}{|u|}\right) = \chi_{d_1}\left(\frac{m}{|d_2|}\right) \dots \left(\frac{m}{|d_t|}\right) = \chi_{d_1}(m)\chi_{d_2}(m) \dots \chi_{d_t}(m).$$

□

Bibliografía

[1] Duncan A. Buell. *Binary quadratic forms*. Classical theory and modern computations. Springer-Verlag, New York, 1989.

[2] Carlos Ivorra Castillo. *Introducción a la teoría algebraica de números*. URL: https://www.uv.es/~ivorra/Libros/ITAl.pdf.

[3] David A. Cox. *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication*. Third edition with solutions, With contributions by Roger Lipsett. AMS Chelsea Publishing, Providence, RI, 2022.

[4] Andrej Dujella. *Number theory*. Translated from the Croatian edition by Petra Švob. Školska Knjiga, Zagreb, 2021.

[5] C. F. Gauss. *Disquisitiones arithmeticae*. Traducido del Latin por Hugo Barrantes Campos, Michael Josephy y Ángel Ruiz Zúñiga. Colección Enrique Pérez Arbeláez, Vol. 10. Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá, 1995.

[6] Joseph Louis Lagrange. *Oeuvres*. Vol. 3. Gauthier-Villars, 1869.

[7] Federico Pintore. "Binary quadratic forms, elliptic curves and Schoof 's algorithm". Tesis doct. University of Trento, 2015. URL: https://core.ac.uk/download/pdf/35317485.pdf.

[8] Rick L. Shepherd. "Binary quadratic forms and genus theory". Tesis doct. The University of North Carolina, 2013. URL: https://libres.uncg.edu/ir/uncg/f/Shepherd_uncg_0154M_11099.pdf.