Teoría de números algebraicos
Grupo de clases en cuerpos cuadráticos imaginarios

Trabajo Fin de Grado

Autor:
Marta Frías Guitérrez

Tutor:
Blas Torrecillas Jover

Grado en Matemáticas

Junio, 2016
Universidad de Almería

Índice general

Abstract in English

Attraction and interest by the numbers man goes back many centuries. Whether for practical reasons, because of its link in the calculation of time or astronomy were many ancient peoples who were interested in numbers. The Greeks were the first to discover the language of numbers thus developing the basic laws of arithmetic. Among other things, they had knowledge of the Euclidean division, prime numbers, calculating the least common multiple and the greatest common divisor. Advance knowledge of numbers and the significant outcomes studied over time they have allowed to construct a theory of numbers sustained in increasingly more solid foundation.

We will see in this essay as the subtlety of algebraic number theory shown in the simplest way possible in the quadratic fields. This has made the quadratic fields have been considered as ideal models to formulate hypotheses and get first tests. So much so that many of the most significant results of algebraic number theory were previously shown in the case of quadratic fields and then in a second stage were widespread.

Results like the finiteness of the class number were tested by Gauss for quadratic fields. The Gauss' theory studies binary quadratic forms, but is similar to the theory of quadratic fields because the relationship between modules and forms can be refined in the quadratic case in such a way that any facts about forms can be transmitted to modules and vice versa.

Most of the theory manifests itself most naturally in terms of modules, while there are some concepts of great theoretical importance that are completely natural in terms of forms and yet it takes deeply into the theory to fully understand its meaning in terms of modules. Therefore it is of great importance to study both approaches and the relationship between them.

The approach that we will give in this essay about quadratic forms will primarily come of the theory of Lagrange, published in 1773-1775 Recherches d'Arithmeticae and Gauss, who at 21 published his book Disquisitiones Arithmeticae in 1801. In this book, though most terminology is due to Gauss, many of the terms introduced by him refer to concepts presented by Lagrange. Lagrange introduced the idea of equivalence between quadratic forms, but only enunciated a form " could be transformed into one of the same type " . The terms of equivalence and proper equivalence were later due to Gauss.

Once submitted the quadratic fields and quadratic forms , we will only work on imaginary quadratic fields. In these terms , from the concepts of reduced quadratic forms we will see that in particular the class number is equal to the number of primitive reduced forms with discriminant D.

Finally , we will make a brief introduction of the discrete logarithm problem and see the resolution method "Giant step Baby step" for the discrete logarithm. Thanks to previous results , we will introduce the Terr's Algorithm which is based on Shanks Algorithm's ideas for computing the order of the class group elements of imginary

quadratic fields.

Resumen en español

La atracción y el interés del hombre por los números se remonta muchos siglos atrás. Ya sea por motivos prácticos, por su relación con el cálculo del tiempo o con la astronomía eran muchos los pueblos antiguos que se interesaban por los números. Los griegos fueron los primeros en descubrir el lenguaje de los números desarrollando así las leyes básicas de la aritmética. Entre otras cosas, tenían conocimiento sobre la división euclídea, los números primos, el cálculo de mínimo común múltiplo o el máximo común divisor. El avance del conocimiento de los números y los considerables resultados estudiados a lo largo del tiempo han permitido construir una teoría de números sustentada en unas bases cada vez más sólidas.

Veremos en este trabajo como la sutileza de la teoría algebraica de números se muestra de la forma más sencilla posible en los cuerpos cuadráticos. Esto ha hecho que los cuerpos cuadráticos hayan sido considerados como modelos ideales para formular hipótesis y obtener primeras pruebas. Tanto es así que muchos de los resultados más significativos de la teoría algebraica de números fueron previamente demostrados en el caso de cuerpos cuadráticos y posteriormente en una segunda etapa fueron generalizados.

Resultados como la finitud del número de clases fueron probados por Gauss para cuerpos cuadrático. La teoría de Gauss estudia las formas cuadráticas binarias, pero es semejante a la teoría de cuerpos cuadráticos debido a que la relación entre módulos y formas puede refinarse en el caso cuadrático hasta el punto de trasladar fielmente cualquier hecho sobre formas a un hecho análogo sobre módulos y viceversa. La mayor parte de la teoría se manifiesta de forma más natural en términos de módulos, mientras que hay algunos conceptos de gran importancia teórica que resultan completamente naturales en términos de formas y sin embargo se necesita profundizar mucho en la teoría para comprender completamente su sentido en términos de módulos. Por ello será interesante estudiar ambos planteamientos y la relación entre ambos.

El enfoque que le daremos en este trabajo a las formas cuadráticas vendrá fundamentalmente de la teoría de Lagrange, publicada en 1773-1775 Recherches dArithméticae y Gauss, quien a sus 21 años publicó su libro Disquisitiones Arithmeticae en 1801. En este libro aunque la mayoría de la terminología es debida a Gauss, muchos de los términos que introdujo hacen referencia a conceptos presentados por Lagrange. Así por ejemplo, Lagrange presentó la idea de equivalencia entre las formas cuadráticas, aunque únicamente enunció que una forma *"podía ser transformada en una del mismo tipo"* [1]. Los términos de equivalencia y equivalencia propia fueron posteriormente debidos a Gauss.

Una vez presentados los cuerpos cuadráticos y las formas cuadráticas, nos limitaremos a trabajar sobre cuerpos cuadráticos imaginarios. En estas condiciones, a partir de los conceptos de formas cuadráticas reducidas veremos que en particular, el número de clases es igual al número de formas reducidas primitivas con discriminante D.

Por último, haremos una breve introducción del problema del logaritmo discreto y veremos el método de resolución de "Paso de gigante paso de Bebé"para el logaritmo discreto. Gracias a los resultados previos, estudiaremos el algoritmo de Terr el cual se basa en las ideas del algoritmo de Shanks, para obtener el orden de los elementos de los grupos de clases de cuerpos cuadráticos imaginarios.

1 Introducción

En este primer capítulo estudiaremos algunas definiciones y nociones básicas del grupo de clases, los cuerpos cuadráticos y los ideales que son de capital importancia y nos serán de utilidad en capítulos posteriores.

1.1 Grupo de clases

Para proporcionar una definición adecuada del grupo de clases es necesario, en primer lugar, recordar la definición de ideal fraccionario.

Definición 1.1. *Sea A un dominio de integridad y sea K su cuerpo de fracciones. Un A-submódulo I de K es un ideal fraccionario de A si $\gamma I \subseteq A$ para algún $\gamma \in A\ \{0\}$, esto es, si I es un subconjunto no vacío de K con las siguientes propiedades:*

- $\alpha, \beta \in I \Longrightarrow \alpha + \beta \in I$.
- $\alpha \in I, r \in A \Longrightarrow r\alpha \in I$.
- *Existe $\gamma \in A$, con $\gamma \neq 0$, tal que $\gamma I \subseteq A$.*

Consideremos ahora un cuerpo numérico K y el grupo abeliano de los ideales fraccionarios de K, denotado por $\mathcal{F}(O)$. Entre estos módulos podemos establecer una relación de equivalencia:

Dos ideales fraccionarios I y J son equivalentes si, y sólo si existe $\alpha \in K$ no nulo tal que $J = \alpha I$. Podemos expresar $\alpha = \frac{a}{b}$, donde a y b son enteros. De este modo diremos que I y J son equivalentes si, y sólo si existen dos enteros a y b tal que $bJ = aI$.

En estas condiciones podemos pasar a definir el grupo de clases, como sigue.

Definición 1.2. *Sea K un cuerpo numérico y $\mathcal{O}_K$ el anillo de enteros de K. Diremos que dos ideales I y J de K son equivalentes si $\exists \alpha \in K^*$ de modo que $J = \alpha I$. Al conjunto de clases de equivalencia le damos el nombre de grupo de clases de $\mathcal{O}_K$ y lo denotaremos por $Cl(K)$.*

Todo ideal fraccional es de la forma $\alpha^{-1}I$, donde α es un entero no nulo e I un ideal de K. Evidentemente, $\alpha^{-1}I$ es equivalente a I, luego todo grupo de clases se puede expresar como la clase de un ideal.

Proposición 1.1. *Sea K un cuerpo numérico, n su grado tal que $n = s + 2t$, siendo s y t definidos por sus s inmersiones reales y $2t$ complejas y d su discriminante. En estas condiciones, toda clase de ideales de K contiene un ideal entero J satisfaciendo que:*

$$N(J) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |d|^{1/2}.$$

Al factor, $\left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}$ se le denomina cota de Minkowski.

Por el resultado anterior, podemos ver que toda clase de ideales de un cuerpo numérico K tiene un representante de norma menor o igual a cierta cota, la cota de Minkoski, y solo hay un número finito de ideales que cumplan dicha condición. Con lo que podemos deducir que el grupo de clases es finito y a su número de elementos $h(K)$ se le llama número de clases del cuerpo numérico K.

La determinación de la estructura de $Cl(K)$ y en particular la estructura de la clase de números de $h(K)$ es uno de los principales problemas en la teoría de números. Para abordar este problema introduciremos a continuación algunas ideas y definiciones de los cuerpos cuadráticos que nos serán de utilidad para el desarrollo de este trabajo.

1.2 Cuerpos cuadráticos

En esta sección definiremos uno de los cuerpos de números algebraicos más sencillos, los cuerpos cuadráticos. Un cuerpo cuadrático es un cuerpo de números K de grado dos sobre $\mathbb{Q}$, esto es $[K:\mathbb{Q}] = 2$.

Por ser K de grado dos sobre $\mathbb{Q}$, podemos expresarlo de la forma $k = \mathbb{Q}(\theta)$ donde θ es un entero algebraico, y además es raíz de un polinomio mónico irreducible de $\mathbb{Z}[X]$, es decir, de la forma $P(X) = X^2 + aX + b$, con $a,b \in \mathbb{Z}$. De este modo,

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

Si $a^2 - 4b = r^2 d$ donde $r,d \in \mathbb{Z}$, entonces

$$\theta = \frac{-a + r\sqrt{d}}{2}$$

por lo que podemos expresar $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$, donde d es libre de cuadrados y, por la irreducibilidad de $P(X)$, d no es un cuadrado. Que d sea libre de cuadrados significa que no es divisible por ningún cuadrado perfecto distinto de uno. Es decir, d es el producto de distintos primos. Cuando trabajemos en $\mathbb{Q}(\sqrt{d})$ supondremos que d es libre de cuadrados. Con ésto no perderemos generalidad pues:

$$Si\ D' = n^2 D,\ \text{entonces}\ a + b\sqrt{D'} = a + bn\sqrt{D},\ \text{y por tanto}\ \ \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'}).$$

Proposición 1.2. *Todo cuerpo cuadrático es de la forma:*

$$\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} : x,y \in \mathbb{Q}\},$$

donde $d \in \mathbb{Z}$ es libre de cuadrados.

Definición 1.3. *Diremos que un cuerpo cuadrático $K = \mathbb{Q}(\sqrt{d})$ es real si está contenido en $\mathbb{R}$ o, equivalentemente, si $d > 0$. En caso contario, si $d < 0$, diremos que es imaginario.*

Ejemplo: $\mathbb{Q}(\sqrt{2})$ es un cuerpo cuadrático real mientras que, $\mathbb{Q}(\sqrt{-23})$ es un cuerpo cuadrático imaginario.

En el desarrollo de este trabajo, trabajaremos en términos de cuerpos cuadráticos imaginarios. Una de las razones por las que los cuerpos cuadráticos imaginarios son más sencillos es que son el único cuerpo numérico, a parte de $\mathbb{Q}$, con un número finito de unidades (casi siempre dos).

Veamos ahora cómo son los anillos de enteros de los cuerpos cuadráticos.

Proposición 1.3. *Sea d un entero libre de cuadrados. Entonces el anillo de enteros de $K = \mathbb{Q}(\sqrt{d})$ es:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] \ \ si\ d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \ \ si\ d \equiv 1 \pmod 4 \end{cases} \tag{1.1}$$

Observación. Notemos que

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \sqrt{d}\mathbb{Z} = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

$$\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z} = \left\{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\}$$

con $d \equiv 1 (mod\ 4)$ en el segundo caso.

Los anillos de enteros $\mathcal{O}_K$, preservan ciertas propiedades de $\mathbb{Z}$, como por ejemplo que todo elemento no nulo y no invertible se factoriza como producto de irreducibles, aunque dicha factorización no es única en general.

Ejemplo: Los anillos de enteros más conocidos son los *enteros de Gauss* $\mathbb{Z}[\sqrt{-1}]$ y los *enteros de Eisenstein* $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, en los cuales se conserva la división como en $\mathbb{Z}$. Por lo general no ocurrirá esto, como es el caso de $\mathbb{Z}[\sqrt{-5}]$. Otros ejemplos de anillos cuadráticos son $\mathbb{Z}[\sqrt{2}]$ y $\mathbb{Z}[\sqrt{7}]$.

Proposición 1.4. *Sea $K = \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático con d libre de cuadrados, y no cuadrado, es decir, $d \neq 1$. Entonces $\{1, w\}$ es una base y $d(K)$ el discriminante de K. Luego,*

$$w = \begin{cases} \frac{1+\sqrt{d}}{2} \ \text{ si } d \equiv 1 \pmod 4 \\ \sqrt{d} \ \text{ si } \ d \equiv 2 \ o\ 3 \pmod 4 \end{cases} \tag{1.2}$$

Además cuando $d \equiv 1$ (mod 4) tendremos $d(K) = d$, y para $d \equiv 2$ o 3 (mod 4) tendremos $d(K) = 4d$.

Para evitar hacer distinciones de casos innecesarios, consideraremos una definición más adecuada para los cuerpos cuadráticos.

Definición 1.4. *Un entero D es llamado discriminante fundamental si D es el discriminante de un cuerpo cuadrático K. En otras palabras, $D \neq 1$ y ya sea $D \equiv 1$ (mod 4) y libre de cuadrados, o $D \equiv 0$ (mod 4), $D/4$ es libre de cuadrados y $D/4 \equiv 2$ o 3 (mod 4).*

Si K es un cuerpo cuadrático con discriminante D, haremos uso de la siguiente notación: $K = \mathbb{Q}(\sqrt{D})$, donde D es un discriminante fundamental. Por tanto, $D = d(K)$, y una base fundamental de K viene dada por $\{1, w\}$, donde:

$$w = \frac{D + \sqrt{D}}{2},$$

y por tanto, $\mathcal{O}_K = \mathcal{O}[w]$.

Hasta ahora hemos estudiado brevemente cómo es la estructura de los cuerpos cuadráticos. Veremos a continuación una serie de resultados de gran importancia en los cuerpos cuadráticos.

Definición 1.5. *Dado K un cuerpo cuadrático, tal que $[K : \mathbb{Q}] = 2$. La totalidad de K-automorfismos de $\mathbb{Q}$ (es decir, los automorfismos $\sigma : \mathbb{Q} \to \mathbb{Q}$ tal que $\sigma(a) = a$ para todo $a \in K$) es un grupo $Gal(K/\mathbb{Q})$, llamado grupo de Galois de la extensión cuadrática.*

Definición 1.6. *Si K es un cuerpo y G un grupo de automorfismos de K, sea*

$$K^G = \{a \in K : \sigma(a) = a \text{ para todo } \sigma \in G\}$$

el cual se llama cuerpo fijo de K bajo la acción de G. Por ser extensión de Galois se tendrá que $K^G = \mathbb{Q}$.

Definición 1.7. *Un orden en un cuerpo numérico K es un subconjunto $\mathcal{O} \subseteq K$ para el cual se satisfacen las siguientes propiedades:*

1. *$\mathcal{O}$ es un subanillo de K que contiene a 1.*
2. *$\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado.*
3. *$\mathcal{O}$ contiene una $\mathbb{Q}$-base de K.*

Definición 1.8. *Un orden maximal es un orden que no está contenido propiamente en ningún otro orden.*

Ejemplo: Un ejemplo de orden y orden maximal sería el siguiente:

$$\mathbb{Z}[\sqrt{5}] \subset \mathbb{Z}[\frac{1 + \sqrt{5}}{2}] \subseteq \mathbb{Q}(\sqrt{5})$$

El anillo de enteros $\mathcal{O}_K$ es también un orden maximal.

Recordadas las definiciones de orden y orden maximal, podemos pasar a enunciar la siguiente proposción.

Proposición 1.5. *Si K es un campo cuadrático con discriminante D, entonces cada orden R de K tiene discriminante Df^2 donde f es un entero positivo llamado conductor del orden. Por el contrario, si A es cualquier número entero no cuadrado tal que $A \equiv 0$ o 1 (mod 4), entonces A es únicamente de la forma $A = Df^2$ donde D es un discriminante fundamental, y existe un único orden de R del discriminante A (y R es un orden del discriminante del cuerpo cuadrático $\mathbb{Q}(\sqrt{D})$).*

Una consecuencia de ésto es que es bastante natural considerar los cuerpos cuadráticos junto con sus órdenes, ya que sus discriminantes forman una secuencia, la cual es resultado de la unión de al menos dos progresiones aritméticas.

Para terminar esta sección veremos un resultado muy importante: cómo descomponen los números primos en un cuerpo cuadrático. Para ello, necesitaremos previamente conocer la siguiente definición:

Definición 1.9. *Sea $\boldsymbol{p}$ un primo impar y $mcd(a,p) = 1$. El símbolo de Legendre $\left(\frac{a}{p}\right)$ esta definido por:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{a residuo cuadrático (mod p)} \\ 0 & \text{si } p|a \\ -1 & \text{a no es residuo cuadrático (mod p)} \end{cases} \tag{1.3}$$

Ejemplo: Los residuos cuadráticos de $\mathbb{Z}_7$ son 1, 2 y 4, es decir:

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$$

y

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

Proposición 1.6. *Sea $K = \mathbb{Q}(\sqrt{D})$ donde $D = d(K)$, $\mathcal{O}_K = \mathcal{O}[w]$ con $w = (D + \sqrt{D})/2$ el anillo de enteros y p un número primo. Entonces:*

1. *Si $p|D$, es decir, si $\left(\frac{D}{p}\right) = 0$, entonces p ramifica en K, y tendremos que $p\mathcal{O}_K = \boldsymbol{p}^2$, donde*

$$\boldsymbol{p} = p\mathcal{O}_K + w\mathcal{O}_K$$

excepto cuando $p = 2$ y $D = 12$ (mod 16). En este caso,

$$\boldsymbol{p} = p\mathcal{O}_K + (1 + w)\mathcal{O}_K.$$

2. *Si* $\left(\frac{D}{p}\right) = -1$, *entonces* p *es inerte en* K, *por tanto* $\boldsymbol{p} = p\mathcal{O}_K$ *es un ideal primo.*

3. *Si* $\left(\frac{D}{p}\right) = 1$, *entonces* p *descompone completamente en* K , *y tendremos* $p\mathcal{O}_K = \boldsymbol{p_1 p_2}$, *donde*

$$\boldsymbol{p_1} = p\mathcal{O}_K + \left(w - \frac{D+b}{2}\right)\mathcal{O}_K \text{ y } \boldsymbol{p_2} = p\mathcal{O}_K + \left(w - \frac{D-b}{2}\right)\mathcal{O}_K$$

siendo b *una solución de* $b^2 \equiv D\ (mod 4p)$.

1.3 Ideales

Los ideales constituyen un papel fundamental para el objetivo de este trabajo. Es por ello, que será necesario recordar algunos conceptos que utilizaremos posteriormenten para el razonamiento de ciertas ideas y resultados.

Veamos pues, como se define la norma y el discriminante de un ideal I y algunas de sus propiedades.

Definición 1.10. *Sea* I *un ideal no cero de* $\mathcal{O}$ *definimos la norma de* I *por*

$$N(I) = card(\mathcal{O}/I)$$

Definición 1.11. *Denominaremos discriminante de un ideal* I *de* $\mathcal{O}$ *con base* $[\alpha_1, \beta_1]$, *al valor*

$$D(I) = \begin{vmatrix} \alpha_1 & \beta_1 \\ \alpha_1' & \beta_1' \end{vmatrix}^2,$$

en donde, en general, $\alpha := \sigma(\alpha)$ *denota el conjugado de Galois.*

Proposición 1.7. *Sea* I *un ideal no cero de* $\mathcal{O}$ *y* $a \in \mathcal{O}$, *entonces*

1. $N(a\mathcal{O}) = |N(a)|$.

2. *La norma de* I *es finita.*

Proposición 1.8. *Se satisface que:*

1. $D(I) = N(I)^2 D$.

2. *Si* I *es principal,* $I = (\gamma)$, *entonces* $N(I) = \left|N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\gamma)\right|$.

Proposición 1.9. *Sean* I *y* J *dos ideales enteros no nulos de* $\mathcal{O}$, *se tiene que*

$$N(IJ) = N(I)N(J).$$

Lema 1.1. *Sea* $I \subseteq \mathcal{O}$ *un ideal. Entonces, exite un número entero* n *de modo que* $II' = (n)$, *en donde* $I' := \{\alpha' : \alpha \in I\}$.

Proposición 1.10. *Si* $I \subseteq \mathcal{O}$ *es un ideal no nulo, entonces* $II' = (N(I))$.

Para enunciar el siguiente resultado, necesitaremos definir previamente el concepto de forma normal de Hermite.

Definición 1.12. *Diremos que una matriz $M = (m_{i,j})$ de dimensión mxn, con coeficientes enteros esta en* ***forma normal de Hermite*** *si existe $r \leq n$ y un estricto incremento de la aplicación $f : [r+1, n] \to [1, m]$ que satisface las siguientes propiedades:*

1. *Para $r+1 \leq j \leq n$, $m_{f(j),j} \geq 1$, $m_{i,j} = 0$ si $i > f(j)$ y $0 \leq m_{f(k),j} < m_{f(k),k}$ si $k < j$.*
2. *Las primeras r columnas de M son cero.*

En general, si $n \geq m$, una matriz M en forma normal de Hermite tiene la siguiente forma

$$\begin{pmatrix} 0 & 0 & \dots & 0 & * & * & \dots & * \\ 0 & 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & * \end{pmatrix}$$

donde las últimas m columnas forman una matriz en forma normal de Hermite.

Ejemplos: La matriz

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

es una matriz en forma normal de Hermite.

Consideremos ahora un entero no cuadrado D congruente con 0 o 1 módulo 4. R es el único orden cuadrático del discriminante, $\{1, w\}$ una base estándar de R y K el único cuerpo cuadrático que contiene a R. En estas condiciones,

Proposición 1.11. *Cualquier ideal entero I de R tiene una única forma normal de Hermite con denominador igual a 1, y matriz*

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

Con respecto a w, donde c divide a a y b y $0 \leq b < a$. En otras palabras, $I = a\mathbb{Z} + (b + cw)\mathbb{Z}$. Además, $a = l(I)$ es el entero positivo más pequeño en I y $N(I) = ac$.

Definición 1.13. *Diremos que un ideal entero I de R es primitivo si $c = 1$, en otras palabras si I/n no es un ideal entero de R para ningún entero $n > 1$.*

2

Formas cuadráticas

Las formas cuadráticas son otro de los conceptos fundamentales. Nos centraremos especialmente en el caso de las formas cuadráticas definidas positivas. Por ello en este apartado estudiaremos su estructura junto a sus propiedades.

Definiremos una forma cuadrática binaria f como una función de la forma,

$$f(X,Y) = aX^2 + bXY + cY^2 \tag{2.1}$$

donde a, b, y ,c son enteros no nulos. Denotaremos por $f = (a,b,c)$ a la forma cuadrática f. De forma matricial, podemos expresar $f(X,Y)$ como,

$$f(X,Y) = \frac{1}{2} C^T A(f) C$$

donde $C = \begin{pmatrix} X \\ Y \end{pmatrix}$ y $A(f) := \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. En estas condiciones, llamaremos discriminante de f al determinante de la matriz definida anteriormente $A(f)$ cambiado de signo,

$$D(f) = -\begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = b^2 - 4ac$$

y lo denotaremos por $D(f)$. El discriminante cumple un papel esencial en el estudio de las formas cuadráticas, pues su signo tiene importantes efectos en sus comportamientos.

Ejemplos: Las formas

1. $x^2 + 2xy + y^2$, o equivalentemente, $\frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$
2. $x^2 + 2y^2$, o equivalentemente, $\frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$
3. $3x^2 - xy + 2y^2$, o equivalentemente, $\frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 6 & -1 \\ -1 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

son ejemplos de formas cuadráticas binarias.

Proposición 2.1. *Un entero m es representado por una forma cuadrática $f(X,Y)$ si la ecuación*

$$m = f(X,Y)$$

tiene una solución entera en X e Y. La representación de m por $f(x,y)$ se denomina propiamente representada si $mcd(X,Y) = 1$.

Ejemplo: 23 es representado por la forma cuadrática $f(x,y) = x^2 + xy + y^2$ pues para $f(2,3)$ se tiene que

$$f(2,3) = 4^2 + 2 \cdot 3 + 3^2 = 23.$$

Además es propiamente representado pues $mcd(2,3) = 1$.

Proposición 2.2. *Una forma cuadrática $f = (a,b,c)$ se denomina primitiva si a, b y c son primos relativos, es decir, $mcd(a,b,c) = 1$. Si $f' = (a',b',c')$ y $r = mcd(a',b',c')$, la forma $f = (a'/r, b'/r, c'/r)$ es primitiva y satisface que $D(f') = D(f)r^2$.*

Ejemplos:

1. $2x^2 + 3xy + 5y^2$ es una forma cuadrática primitiva ya que $mcd(2,3,5) = 1$.
2. Dado $f' = (6,9,18)$ se tiene que $mcd(6,9,18) = 3$. La forma cuadrática $f = (6/3, 9/3, 18/3) = (2,3,6)$ es primitiva y se satisface que:

$$D(f') = 9^2 - 4 \cdot 6 \cdot 18 = -351 = (3^2 - 4 \cdot 2 \cdot 6)3^2 = D(f)3^2$$

Proposición 2.3. *Sea $f = (a,b,c)$. Se satisface que*

1. *$D(f) \equiv 0, 1$ (mod 4)*
2. *$D(f)$ es un cuadrado perfecto si, y sólo si, existen $r,s,u,v \in \mathbb{Z}$ tales que*

$$(a,b,c) = (rX + sY)(uX + vY)$$

Para los siguientes resultados, consideraremos el discriminante de la forma f como no cuadrado perfecto. Veamos ahora cómo se clasifican las formas cuadráticas en función de los valores que toman.

Definición 2.1. *Sea f una forma cuadrática. Entonces,*

1. *f es definida positiva si, y sólo si, $f(X,Y) \geq 0$ para todo $x,y \in \mathbb{Z}$.*
2. *f es definida negativa si, y sólo si, $f(X,Y) \leq 0$ para todo $x,y \in \mathbb{Z}$.*
3. *f es indefinida si, y sólo si, f toma valores positivos y negativos.*

Existe una relación directa entre la clasificación de una forma cuadrática f y el signo de su discriminante D. Consideramos,

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

con $x,y \in \mathbb{Z}$. Tomemos $a \in \mathbb{Z}$ con $a \neq 0$, entonces:

$$4af(x,y) = 4a^2x^2 + 4abxy + 4acy^2$$

Haciendo cambios de cuadrados tendremos que:

$$4af(x,y) = 4a^2x^2 + 4abxy + 4acy^2 = 4a^2x + 4abxy + b^2y^2 + (4ac - b^2)y^2 =$$
$$(2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 + Dy^2$$

En estas condiciones,

- Si $D < 0$ y $a > 0$, entonces

$$4af(x,y) = (2ax + by)^2 - Dy^2 \geq 0$$

y por tanto $f(x,y) \geq 0$, luego f es definida positiva.

- Si $D < 0$ y $a < 0$, entonces

$$-4af(x,y) = -(2ax + by)^2 + Dy^2 \leq 0$$

y por tanto $f(x,y) \leq 0$, luego f es definida negativa.

- Si $D > 0$ basta observar que

$$f(1,0) = a$$

$$f(b,-2a) = ab^2 - b^2 2a + c4a^2 = -ab^2 + 4a^2 c = -aD$$

y por tanto f toma valores de signos opuestos, con lo que f es indefinida.

Como consecuencia de la definición anterior podemos enunciar el siguiente resultado.

Proposición 2.4. *Sean $f = (a,b,c), D = D(f)$. La forma cuadrática f, será definida positiva si $D < 0$, $a > 0$; definida negativa si $D < 0$, $a < 0$ e indefinida si $D > 0$.*

Definición 2.2. *Para cada $D \in \mathbb{Z}$ tal que $D \equiv 0,1 \ (mod\ 4)$, existe una forma cuadrática con discriminante igual a D. A dicha forma cuadrática se le denomina forma básica de discriminante D.*

Demostración:

Para probar dicha afirmación basta con definir la forma cuadrática $f_0(x,y)$ tal que

$$f_0(x,y) = x^2 - \frac{D}{4}y^2, \text{ si } D \equiv 0 \ (mod 4)$$

$$f_0(x,y) = x^2 - xy + \frac{1-D}{4}y^2, \text{ si } D \equiv 1 \ (mod 4)$$

En ambos casos, dado que el discriminante $D = b^2 - 4ac$, podemos observar que $D(f_o) = D$.

■

2.1 Equivalencia de formas cuadráticas

Mediante cambios de base sobre las formas cuadráticas, estudiaremos la relación de equivalencia en las formas cuadráticas binarias. Para ello, será necesario recordar previamente la definición de los grupos clásicos $\boldsymbol{SL}(2,\mathbb{Z})$ y $\boldsymbol{GL}(2,\mathbb{Z})$.

Definición 2.3. *Llamaremos grupo lineal especial* $\boldsymbol{SL}(2,\mathbb{Z})$ *al grupo definido por matrices invertibles 2x2 con coeficientes en* $\mathbb{Z}$ *y determinante igual a 1. En otras palabras*

$$\boldsymbol{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} :\ p,q,r,s \in Z,\ \ ps - rq = 1 \right\}$$

Definición 2.4. *Llamaremos grupo lineal general* $\boldsymbol{GL}(2,\mathbb{Z})$ *al grupo definido como el conjunto de matrices invertibles 2x2 sobre el anillo de enteros con determinante ± 1:*

$$\boldsymbol{GL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} :\ \alpha,\beta,\gamma,\delta \in Z,\ \ \alpha\delta - \gamma\beta = \pm 1 \right\}$$

Ejemplos:

$$A = \begin{pmatrix} -1 & 3 \\ 0 & -1 \end{pmatrix} \quad y \quad B = \begin{pmatrix} -3 & 2 \\ -7 & -5 \end{pmatrix}$$

La matriz A con coeficientes enteros y con determinante igual a 1 es una matriz del grupo lineal especial $\boldsymbol{SL}(2,\mathbb{Z})$. Mientras que la matriz A y B son matrices del grupo lineal general $\boldsymbol{GL}(2,\mathbb{Z})$, pues tienen coeficientes enteros y determinantes son 1 o −1.

Acontinuación vamos a definir la relación de equivalencia en las formas cuadráticas.

Definición 2.5. *Dadas dos formas cuadráticas* $f(x,y)$ *y* $g(x,y)$ *diremos que son equivalentes si existen enteros p, q, r y s de modo que*

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

Puesto que $\begin{vmatrix} p & q \\ r & s \end{vmatrix} = ps - qr = \pm 1$ es claro que $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \boldsymbol{GL}(2,\mathbb{Z})$, y la equivalencia de formas cuadráticas es una relación de equivalencia. Siguiendo la teoría de Gauss, diremos que una equivalencia es una equivalencia propia si $ps - qr = 1$, es decir, $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \boldsymbol{SL}(2,\mathbb{Z})$ e impropia si $ps - qr = -1$. Puesto que $\boldsymbol{SL}(2,\mathbb{Z})$ es un subgrupo de $\boldsymbol{GL}(2,\mathbb{Z})$, la equivalencia propia es también una relación de equivalencia.

Matricialmente, podemos expresar la equivalencia de las formas cuadráticas de la siguiente forma. Sea $C = \begin{pmatrix} X \\ Y \end{pmatrix}$, consideremos la forma cuadrática

$$f(X,Y) = \frac{1}{2} C^T A(f) C$$

Dada la matriz $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \boldsymbol{SL}(2,\mathbb{Z})$, sea $PC = \begin{pmatrix} X' \\ Y' \end{pmatrix}$. Mediante un cambio de base a partir de la forma f, definiremos la forma cuadrática $g = (a', b', c')$ tal que:

$$g(X,Y) = f(X',Y') = \frac{1}{2}(PC)^T A(f)(PC) = \frac{1}{2}C^T(P^T A(f)P)C.$$

Luego, $A(g) = P^T A(f)P$. Desarrollando la expresión:

$$A(g) = \begin{pmatrix} p & r \\ q & s \end{pmatrix}\begin{pmatrix} 2a & b \\ b & 2a \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix} =$$

$$= \begin{pmatrix} 2ap^2 + 2bpq + 2cq^2 & 2apr + b(ps+qr) + 2cqs \\ 2apr + b(ps+qr) + 2cqs & 2ar^2 + 2brs + 2cs^2 \end{pmatrix}$$

tendremos que los coeficientes de la forma $g = (a', b', c')$ son:

$a' = ap^2 + bpq + cq^2$
$b' = 2apr + b(ps + qr) + 2cqs$
$c' = ar^2 + brs + cs^2$

De forma general, diremos que dos formas cuadráticas f y g son equivalentes si existe una matriz $P \in \boldsymbol{GL}(2,\mathbb{Z})$ tal que $A(g) = P^T A(f)P$, y propiamente equivalentes si $P \in \boldsymbol{SL}(2,\mathbb{Z})$ cumpliendo la misma condición, $A(g) = P^T A(f)P$.

Ejemplo: Obtengamos una forma cuadrática equivalente a $f(x,y) = x^2 - 8xy + 6y^2$. De forma matricial tendremos que,

$$f(x,y) = \frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 2 & -8 \\ -8 & 12 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

Una forma equivalente será de la forma

$$g(x,y) = \frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}A(g)\begin{pmatrix} x \\ y \end{pmatrix}$$

donde $A(g) = P^T A(f)P$ con $P \in \boldsymbol{GL}(2,\mathbb{Z})$. Consideremos $P = \begin{pmatrix} -4 & 1 \\ -5 & 1 \end{pmatrix}$, entonces

$$A(g) = \begin{pmatrix} -4 & -5 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & -8 \\ -8 & 12 \end{pmatrix}\begin{pmatrix} -4 & 1 \\ -5 & 1 \end{pmatrix} = \begin{pmatrix} 12 & 4 \\ 4 & -2 \end{pmatrix}.$$

Por tanto:

$$g(x,y) = \frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 12 & 4 \\ 4 & -2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}.$$

La siguiente proposición pone de manifiesto que el discriminante de una forma cuadrática es un invariante de su clase de equivalencia.

Proposición 2.5. *Dada f y g dos formas cuadráticas equivalentes entonces*

1. $D(f) = D(g)$
2. $f(x,y) = m$ *si, y sólo si,* $g(x,y) = m$*, es decir, representan los mismos enteros.*

Demostración:

Probemos el resultado anterior:

1. Sean f y g dos formas cuadráticas equivalentes. Como hemos visto anteriormente, por ser equivalentes $A(g) = P^T A(f)P$. Recordemos que el discriminante $D(f)$ de una forma cuadrática f era el determinante de la su matriz $A(f)$ cambiado de signo, luego:

$$D(g) = -|A(g)| = -\left|P^T A(f)P\right|$$

Por las propiedades de los determinantes,

$$D(g) = -|A(g)| = -\left|P^T\right||A(f)||P|$$

$$D(g) = -|A(g)| = -(ps-qr)(4ac-b^2)(ps-qr)$$
$$D(g) = -|A(g)| = (ps-qr)^2(b^2-4ac)$$
$$D(g) = (ps-qr)^2 D(f)$$

Puesto que son equivalentes, $ps - qr = \pm 1$ con lo que $D(g) = D(f)$.

2. Sean $f(x,y)$ y $g(px+qy, rx+sy)$ dos formas cuadáticas equivalentes, tal que $P = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Para cada solución (x',y') tal que $f(x',y') = n$, se tiene que $g(px'+qy', rx'+sy') = n$. Cada solución (x,y) de $f(x,y) = n$ puede obtenerse de la siguiente manera

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = P^{-1}\begin{pmatrix} x \\ y \end{pmatrix}.$$

Además, dos souciones (x',y') y (x'',y'') dan el mismo (x,y) si, y sólo si

$$P\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} = P\begin{pmatrix} x'' \\ y'' \end{pmatrix}$$

es decir, si y sólo si $(x',y') = (x'',y'')$. Por tanto, f y g representan al mismo entero m.

■

Ejemplo: Sean $f(x,y) = x^2 + y^2$ y $g(x,y) = f(x+y,y) = x^2 + 2xy + 2y^2$ dos formas cuadráticas equivalentes. Podemos ver que efectivamente f y g tienen el mismo discrimante, pues

$$D(f) = b^2 - 4ac = -4$$
$$D(g) = b^2 - 4ac = 2^2 - 4{,}2 = -4$$

Por otro lado tenemos que, $g(2,-3) = 10$, y 10 es también representado por f tal que $10 = g(2,-3) = f(2+(-3),-3) = f(-1,3)$.

Este resultado también engloba el caso de formas cuadráticas propiamente equivalentes. Una observación importante es que dado que las formas equivalentes representan los mismos enteros, deben ser simultáneamente definidas positivas, negativas o indefinidas. Además, cualquier forma equivalente a una primitiva, es también primitiva, debido a que la equivalencia deja también perserva la primitividad.

Lema 2.1. *Una forma cuadrática $f(x,y)$ representa propiamente a un entero m si, y sólo si $f(x,y)$ es propiamente equivalente a una forma cuadrática de la forma $mx^2 + bxy + cy^2$ para algún b,$c \in \mathbb{Z}$.*

Demostración:

Veamos en primer lugar la implicación hacia la derecha. Consideremos $f(p,q) = m$, con p, q primos relativos. Podemos encontrar dos enteros r y s, de modo que se satisfaga que $ps - qr = 1$, entonces

$$f(px+ry, qx+sy) = f(p,q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r,s)y^2$$
$$= mx^2 + bxy + cy^2$$

como queríamos probar. Para probar la otra implicación, basta ver que la forma cuadrática $mx^2 + bxy + cy^2$ representa propiamente a m para $(x,y) = (1,0)$.

■

2.2 Correspondencia entre ideales y formas cuadráticas

En esta sección, veremos que trabajar con ideales y formas cuadráticas es esencialmente lo mismo pues existe una correspondencia biyectiva entre el conjunto de las clases de ideales y las formas cuadráticas. Además ciertos algoritmos son más eficientes en términos de formas cuadráticas, por lo que es importante estudiar esta relación con detalle.

En primer lugar observaremos que a toda clase de ideales fraccionarios se le asocia una clase de formas cuadráticas binarias equivalente con discriminante D. Recordemos que D es un entero no cuadrado congruente con 0 o 1 módulo 4, y R el único orden del discriminante D. Consideremos entonces un ideal fraccionario $I \in \mathcal{F}(O)$ y sea γ un elemento de I con conjugado γ'. Dado que $(\gamma) \subseteq I$ y por ser Dominio de Dedekind,

$I|(\gamma)$, es decir, $(\gamma) = IJ$, luego $N((\gamma)) = N(I)N(J)$ y por tanto $N(I)|N((\gamma))$. Podemos definir así la aplicación

$$\begin{array}{rccc} \phi\colon & I & \longrightarrow & \mathbb{Z} \\ & \gamma & \longmapsto & \frac{\gamma\gamma'}{N(I)} \end{array}$$

Supongamos que el ideal I es de la forma $I = [\alpha, \beta]$ tal que $\alpha\mathbb{Z} + \beta\mathbb{Z} \approx \mathbb{Z}^2$. Al tomar esta base, podemos definir la aplicación ,

$$f_I\colon \ \mathbb{Z}^2 \longrightarrow \mathbb{Z}$$

dada por

$$f_I(x,y) := \phi(x\alpha + y\beta) = \frac{(x\alpha + y\beta)(x\alpha' + y\beta')}{N(I)} = \frac{N(x\alpha + y\beta)}{N(I)}.$$

Del desarrollo de dicha expresión obtenemos

$$f_I(x,y) = \frac{(x\alpha + y\beta)(x\alpha' + y\beta')}{N(I)} = \frac{\alpha\alpha' x^2 + \alpha\beta' xy + \alpha'\beta xy + \beta\beta' y^2}{N(I)} = \frac{\alpha\alpha' x^2 + (\alpha\beta' + \alpha'\beta)xy + \beta\beta' y^2}{N(I)}$$

Definiendo a, b, y c como

$$a := \frac{\alpha\alpha'}{N(I)};\ \ b := \frac{\alpha\beta' + \alpha'\beta}{N(I)};\ \ c := \frac{\beta\beta'}{N(I)}$$

podemos asociar a la aplicación anterior la forma cuadrática binaria:

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

Es evidente que a y c son enteros. Veamos por tanto que $b \in \mathbb{Z}$. Observamos que el grupo de Galois deja invariante a $\alpha\beta' + \alpha'\beta$, pues $G(\alpha\beta' + \alpha'\beta) = \alpha'\beta + \alpha\beta'$. Luego podemos afirmar que $\alpha\beta' + \alpha'\beta \in K^G = \mathbb{Q}$, $\alpha\beta' + \alpha'\beta \in II' = (N(I))$ y por consiguiente $\alpha\beta' + \alpha'\beta = tN(I)$ con $t \in O$. Dado que $\frac{(\alpha\beta' + \alpha'\beta)}{N(I)} \in O \cap \mathbb{Q} = \mathbb{Z}$ probamos que $b \in \mathbb{Z}$.

Hallemos ahora el discriminante de la forma cuadrática $f_I = (a,b,c)$:

$$b^2 - 4ac = \frac{(\alpha\beta' + \alpha'\beta)^2 - 4(\alpha\alpha')(\beta\beta')}{N(I)^2} = \frac{(\alpha\beta')^2 + 2(\alpha\beta'\alpha'\beta) + (\alpha'\beta)^2 - 4(\alpha\alpha')(\beta\beta')}{N(I)^2} =$$
$$= \frac{(\alpha\beta')^2 - 2(\alpha\alpha')(\beta\beta') + (\alpha'\beta)^2}{N(I)^2} = \frac{(\alpha\beta' - \alpha'\beta)^2}{N(I)^2} = \frac{D(I)}{N(I)^2} = D.$$

A continuación analizaremos la dependencia de la forma cuadrática f_I respecto a la base tomada en I. Supongamos que I=$[\alpha,\beta]$=$[\alpha_1,\beta_1]$, donde $\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$; con $P := \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL(2,\mathbb{Z})$. Las formas cuadráticas $f_{[\alpha,\beta]} y f_{[\alpha_1,\beta_1]}$ serán $SL(2,\mathbb{Z})$ equivalentes si, y sólo si $ps - qr = 1$. En estas condiciones podemos dar la siguiente definición.

Definición 2.6. *Una base $\{\alpha, \beta\}$ de un ideal I diremos que esta positivamente orientada si*

$$\frac{\alpha'\beta - \alpha\beta'}{\sqrt{D}} > 0.$$

La definición tiene sentido pues $\left(\frac{\alpha'\beta-\alpha\beta'}{\sqrt{D}}\right)^2 = \frac{D(I)}{D} = N(I)^2$ *es un número real positivo.*

Es importante analizar qué sucede al cambiar el ideal I por otro ideal estrictamente equivalente $(\lambda)I$, con $N(\lambda) > 0$. Podemos ver que si $I = [\alpha, \beta]$ está expresado en una base positiva, el ideal $(\lambda)I = [\lambda\alpha, \lambda\beta]$ también lo está, pues

$$f_{(\lambda)I}(x,y) = \frac{(\lambda\alpha'\lambda\beta - \lambda\alpha\lambda\beta')^2}{\sqrt{D}} = \frac{(\lambda^2(\alpha'\beta - \alpha\beta'))^2}{\sqrt{D}} > 0$$

Además,

$$f_{(\lambda)I}(x,y) = \frac{N(x\lambda\alpha + y\lambda\beta)}{N((\lambda)I)} = \frac{N(\lambda)N(x\alpha + y\beta)}{N(\lambda)N(I)} = \frac{N(x\alpha + y\beta)}{N(I)} = f_I(x,y)$$

Por consiguiente, a cada clase de ideales fraccionarios en sentido estricto le hemos asociado una clase de formas cuadráticas binarias con coeficientes enteros. Las formas son definidas positivas si, y sólo si $D < 0$.

Para definir la correspondencia en sentido contrario, partamos ahora de la forma cuadrática $f(a,b,c) = ax^2 + bxy + cy^2$ y sea $D(f)$ su discriminante. Supongamos que f es definida positiva, luego $a > 0$ y $D < 0$. Consideremos la ecuación $ax^2 + bx + c = 0$, y definamos τ a partir de las soluciones de dicha ecuación,

$$\tau = \frac{b + \sqrt{D}}{2a}.$$

En estas condiciones, definimos

$$I_f = \mathbb{Z} + \mathbb{Z}\tau$$

Veamos que I_f es un ideal de $\mathcal{O}$. Para ello veamos que dado $\lambda = \frac{u+v\sqrt{D}}{2} \in \mathcal{O}$, con u, v enteros, $u \equiv vD \pmod 2$ y sea $\alpha = x + y\tau \in I$ entonces $\lambda\alpha \in I$ (es decir, es cerrado para el producto).

$$\lambda\alpha = \left(\frac{u+v\sqrt{D}}{2}\right)(x+y\tau) = \left(\frac{u+v\sqrt{D}}{2}\right)\left(x + \frac{yb+y\sqrt{D}}{2a}\right) =$$

$$= \frac{xu}{2} + \frac{ybu}{4a} + \frac{yvD}{4a} + \left(\frac{xv}{2} + \frac{ybv}{4a} + \frac{uy}{4a}\right)\sqrt{D} =$$

$$= \left(x\frac{u-vb}{2} - yvc\right) + \left(xva + y\frac{u+vb}{2}\right)\tau \in \mathbb{Z} + \mathbb{Z}\tau = I$$

puesto que $b^2 \equiv D \pmod{4a}$ implica que $b \equiv D \pmod 2$, luego $u \equiv vD \equiv vb \pmod 2$. Podemos ver que

$$\frac{\tau - \tau'}{\sqrt{D}} = \frac{\frac{b+\sqrt{D}}{2a} - \frac{b-\sqrt{D}}{2a}}{\sqrt{D}} = \frac{2\sqrt{D}}{2a\sqrt{D}} = \frac{1}{a} > 0$$

y como a era positivo, pues habíamos definido f postiva, podemos determinar que la base tomada $\{1, \tau\}$ esta orientada positivamente.
Por otro lado,

$$D(I) = \begin{vmatrix} 1 & \tau \\ 1 & \tau' \end{vmatrix}^2 = (\tau' - \tau)^2 = \left(\frac{\sqrt{D}}{a}\right)^2 = \frac{D}{a^2}$$

con lo cual,

$$N(I) = \sqrt{\frac{D(I)}{D}} = \frac{1}{a}$$

Calculemos ahora la forma cuadrática f_I asociada al ideal $I = [1, \tau]$:

$$f_I(x,y) = \frac{N(x+y\tau)}{N(I)} = \frac{(x+y\tau)(x+y\tau')}{N(I)} = \frac{(x+y\frac{b+\sqrt{D}}{2a})(x+y\frac{b-\sqrt{D}}{2a})}{\frac{1}{a}} =$$

$$= \frac{x^2 + \left(\frac{b-\sqrt{D}}{2a}\right)xy + \left(\frac{b+\sqrt{D}}{2a}\right)xy + \left(\frac{b-\sqrt{D}}{2a}\right)\left(\frac{b+\sqrt{D}}{2a}\right)y^2}{\frac{1}{a}} = \frac{x^2 + \frac{b}{a}xy + \frac{c}{a}}{\frac{1}{a}}$$

obteniendo de ese modo $f_I(x,y) = ax^2 + bxy + cy^2 = f(x,y)$.

Tenemos pues definidas aplicaciones tales que

$$\psi_1 : \quad I \quad \longrightarrow \quad f_I$$

y

$$\psi_2 : \quad f \quad \longrightarrow \quad I_f$$

Para acabar, comprobemos que si $I \to f = (a,b,c) \to [1,\tau]$, entonces los ideales I y $[1,\tau]$ son estrictamente equivalentes. Consideremos pues, $I = [\alpha, \beta], \alpha\alpha' > 0$. De la definición de $f_I = (a,b,c)$ se deduce que,

$$\tau = \frac{b+\sqrt{D}}{2a} = \frac{\alpha\beta' + \alpha'\beta + N(I)\sqrt{D}}{2\alpha\alpha'} = \frac{\beta}{\alpha}.$$

Esto implica que

$$\mathbb{Z} + \mathbb{Z}\frac{b+\sqrt{D}}{2a} = \mathbb{Z} + \mathbb{Z}\frac{\beta}{\alpha} = (\alpha)^{-1} I$$

por lo que el ideal $[1,\tau]$ es estrictamente equivalente a I.

Supongamos ahora que $a<0$,$D>0$. Escribimos $I=\mathbb{Z}\lambda+\mathbb{Z}\lambda\tau$, con $N(\lambda)>0$. La base $\lambda,\lambda\tau$ estará orientada positiva y formaremos f_I como en el caso precedente. Recíprocamente, si partimos de un ideal $I=[\alpha,\beta]$ cuya base viene dada por $[\alpha,\beta]$ orientada positivamente, entonces $\alpha\alpha'<0$ con lo cual la forma cuadrática $f=(a,b,c)$ satisface que $a<0$ y el ideal $\mathbb{Z}\lambda+\mathbb{Z}\lambda\tau$ será estrictamente equivalente a I. Las consideraciones previas nos permiten llegar al resultado deseado.

Teorema 2.1. *Sean D un discriminante fundamental y $K=\mathbb{Q}(\sqrt{D})$. El conjunto $\mathcal{H}(D)$ de las clases cuadráticas binarias de discriminante d (definidas positivas si $D<0$) y el grupo $Cl^+(\mathcal{O})$ de las clases de ideales de $\mathcal{O}$ en sentido estricto, están en correspondencia biyectiva:*

$$\begin{aligned} Cl^+(\mathcal{O}) &\longrightarrow \mathcal{H}(D) \\ I &\longrightarrow f_I \\ [1,\tau] &\longleftarrow f. \end{aligned}$$

Por tanto, el conjunto finito $\mathcal{H}(D)$ tiene una estructura de grupo abeliano y el grupo abeliano $Cl^+(\mathcal{O})$ es un conjunto finito.

Notemos que si $D<0$, entonces $Cl(\mathcal{O})=Cl^+(\mathcal{O})$ y $card(Cl(\mathcal{O}))=h(D)$.

2.3 Finitud del número de clases

A partir de ahora, trabajaremos en cuerpos cuadráticos imaginarios, donde trataremos de abordar el problema del cálculo del grupo de clases mediante un sencillo algoritmo basado en las formas cuadráticas.

Para ello, la correspondencia estudiada anteriormente entre clases de formas cuadráticas y grupos de clases de ideales nos será de gran ayuda. Normalmente, trabajar con ideales es de mayor utilidad en demostraciones, sin embargo para el cálculo computacional se trabaja de una forma más sencilla con las formas cuadráticas. Una de las ventajas de la relación entre las clases de ideales y la clases de formas formas cuadráticas es que el algoritmo que vamos a plantear será más sencillo.

Definición 2.7. *Una forma cuadrática definida postiva (a,b,c) de discriminante D se dice que es reducida si*

$$|b|\leq a\leq c$$

y si, además, cuando una de las dos desigualdades es una igualdad, es decir, $|b|=a$ o $a=c$, entonces $b\geq 0$.

Ejemplos:

1. x^2+xy+y^2 es una forma cuadrática definida positiva reducida:

- Es definida positiva pues $D = b^2 - 4ac = 1 - 4 = -3 < 0$ y además $a = 1 > 0$.
- Por ser definida positiva y dado que:

$$|1| \leq 1 \leq 1$$

como $a = c = 1$ y se cumple que $b = 1 > 0$ es reducida.

2. $2x^2 + xy + 2y^2$ es una forma cuadrática definida positiva reducida:

- Puesto que $D = b^2 - 4ac = 1 - 4 \cdot 2 \cdot 2 = -15 < 0$ y $a = 2 > 0$, es definida positiva.
- Por ser definida positiva y satisfacer que:

$$|1| \leq 2 \leq 2$$

como $a = c = 2$ y se cumple que $b = 1 > 0$ es reducida.

Proposición 2.6. *En cada clase de formas cuadráticas definidas positivas con discriminante $D < 0$ existe exactamente una única forma reducida. En particular, $h(D)$ es igual al número de formas reducidas primitivas con discriminante D.*

Demostración:

Debemos probar dos cosas. En primer lugar, que cada clase contiene al menos una forma reducida, y en segundo lugar que esta forma reucida es única en dicha clase.

Empezemos viendo que en cada clase hay una forma reducida. Sea $\mathcal{C}$ una clase de formas cuadráticas equivalentes definidas positivas con discriminante D. Consideremos (a, b, c) un elemento de dicha clase de modo que a minimal. Es claro que para cualquier forma tenemos que $c \geq a$ pues (a, b, c) es quivalente a $(c, -b, a)$. Basta ver que

$$f(x, y) = ax^2 + bxy + cy^2 \text{ luego } f = (a, b, c)$$

$$f(-y, x) = ay^2 - bxy + cx^2 \text{ luego } f = (c, -b, a)$$

Mediante el cambio de (x, y) a $(x + ky, y)$ para un entero $k = \lfloor \frac{(a-b)}{2a} \rfloor$, obtenemos una forma (a', b', c') tal que,

$$a(x + ky)^2 + b(x + ky)y + cy^2$$
$$ax^2 + (2ak + b)xy + (ak^2 + b + k + c)y^2$$

donde $a' = a$, $b' = 2ak + b$ y $c' = ak^2 + b + k + c$, y $b' \in]-a', a]$ pues:

$$k \leq \frac{a - b}{2a} < k + 1$$
$$2ak \leq a - b < 2a(k + 1)$$
$$(2ak + b) \leq a < (2ak + b) + 2a$$
$$b' \leq a' < b' + 2a'$$

Puesto que $a' = a$ es minimal, tendremos que $a' \leq c'$, luego (a', b', c') es casi una forma reducida. El único problema posible sería si $a' = c'$) y $b' < 0$. En este caso, haciendo el cambio (a', b', c') a $(c'', b'', a'') = (c', -b', a')$ obtenemos una forma equivalente con $b'' > 0$, por tanto (c'', b'', a'') es reducida.

Veamos que si (a, b, c) es una forma reducida, se trata de la única forma reducida en dicha clase. Es claro que a es minimal de entre todas las formas equivalentes a (a, b, c), pues ara cualquier otro a' se tiene que $a' = am^2 + bmn + cn^2$ con m, n coprimos enteros. Las identidades,

$$am^2 + bmn + cn^2 = am^2\left(1 + \frac{b}{a}\frac{n}{m}\right) + cn^2 = am^2 + cn^2\left(1 + \frac{b}{c}\frac{m}{n}\right)$$

implican nuestra afirmación, puesto que $|b| \leq a \leq c$. Además, cualquier otra forma reducida (a', b', c') equivalente a (a, b, c) cumple que $a' = a$. Pero la misma identidad implica que las únicas formas equivalentes a (a, b, c) con $a' = a$ son obtenidas por el cambio (x, y) a $(x + ky, y)$ haciendole corresponder $m = 1$ y $n = 0$. Además, $b' = b + 2ak$ para algún k. Dado que $a' = a$ tenemos que $b, b' \in (-a, a]$, luego $k = 0$. Finalmente

$$c' = \frac{(b')^2 - D}{4a'} = \frac{b^2 - D}{4a} = c,$$

por tanto $(a', b', c') = (a, b, c)$.

■

Lema 2.2. *Sea $f = (a, b, c)$ una forma cuadrática binaria definida positiva con discriminante $D = b^2 - 4ac < 0$.*

1. *Si f es reducida, tendremos la desigualdad*

$$a \leq \sqrt{|D|/3}$$

2. *Por el contrario, si*

$$a < \sqrt{|D|/4} \quad y \quad -a < b \leq a$$

entonces f es reducida.

Demostración:

Para probar 1 basta con ver que si f es reducida entonces $|D| = 4ac - b^2 \geq 4a^2 - a^2$ luego $a \leq \sqrt{|D|/3}$. Veamos que 2 es cierta pues, $c = (b^2 + |D|)/(4a) \geq |D|/(4a) > a^2/a = a$, y por tanto f es reducida.

■

A partir de estos resultados podemos obtener el número de clases, $h(D)$, en cuerpos cuadráticos imaginarios, es decir, para un $D < 0$. Esto es debido a que, como hemos enunciado anteriormente, $h(D)$ será el número de formas reducidas primitivas con discriminante $D < 0$. Veamos algunos ejemplos:

Ejemplo. Calcular el número de clases para $D = -15$. Dado que:

$$a \leq \sqrt{|D|/3}$$

tendremos que $a \leq \sqrt{5} \approx 2$. Con lo que $a = 1$ o $a = 2$, distingamos ambos casos.

- Si $a = 1$ como $|b| \leq a$, tendremos que $|b| = 1$. Pero como $|b| = a$, por la definición 2.7, $b > 0$ y por tanto $b = 1$. Calculemos el valor de c y veamos si se satisface la condición de forma reducida.

  $$c = \frac{-D + b^2}{4a} = \frac{15 + 1}{4} = 4$$

  con lo que $|b| \leq a \leq c$ y una forma reducida para $D = -15$ es

  $$f(x, y) = x^2 + xy + 4y^2$$

- Si $a = 2$, tendremos que distinguir casos:

  1. $|b| = 2$. En este caso tendríamos que $|b| = a$ y por tanto $b > 0$, luego $b = 2$. Calculemos c.
     $$c = \frac{-D + b^2}{4a} = \frac{15 + 4}{8} = \frac{19}{8}$$
     como c no es un número entero, $|b| = 2$ no es un caso posible.
  2. $|b| = 1$. Entonces o $b = 1$ o $b = -1$. Calculemos c.
     $$c = \frac{-D + b^2}{4a} = \frac{15 + 1}{8} = 2$$
     Pues que $c = a$ tendremo que $b > 0$, luego $b = 1$ y la forma reducida sería
     $$f(x, y) = 2x^2 + xy + 2y^2$$

Luego, como hay dos formas reducidas para $D = -15$, tendremos que $h(-15) = 2$.

Ejemplo. Calcular el número de clases para $D = -23$. En este caso, puesto que:

$$a \leq \sqrt{|-23|/3} \approx 2$$

distinguiremos los siguientes casos:

- Si $a = 1$ como $|b| \leq a$, tendremos que $|b| = 1$, luego $|b| = a$. Por tanto, calcularemos el valor de c para $b = 1$.
$$c = \frac{-D + b^2}{4a} = \frac{23 + 1}{4} = 6$$
con lo que $|b| \leq a \leq c$ y una forma reducida para $D = -23$ es
$$f(x, y) = x^2 + xy + 6y^2$$

- Si $a = 2$, tendremos que distinguir casos:

  1. Para $|b| = 2$, tendríamos que $|b| = a$ y por tanto $b > 0$, luego $b = 2$. Calculemos c.
  $$c = \frac{-D + b^2}{4a} = \frac{23 + 4}{8} = \frac{27}{8}$$
  como c no es un número entero, $|b| = 2$ no es un caso posible.
  2. $|b| = 1$. Entonces o $b = 1$ o $b = -1$. Calculemos c.
  $$c = \frac{-D + b^2}{4a} = \frac{23 + 1}{8} = 3$$
  Con lo que tendrámos dos formas reducidas
  $$f(x, y) = 2x^2 + xy + 3y^2 \quad y \quad f(x, y) = 2x^2 - xy + 3y^2$$

Luego, como hay tres formas reducidas para $D = -23$, tendremos que $h(-23) = 3$.

Algunos ejemplos más para algunos $D < 0$ son:

D	h(D)	Formas reducidas de discriminante D
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-15	2	$x^2 + xy + 4y^2,\ 2x^2 + xy + 2y^2$
-20	2	$x^2 + 5y^2,\ 2x^2 + 2xy + 3y^2$
-23	3	$x^2 + xy + 6y^2,\ 2x^2 \pm xy + 3y^2$
-56	4	$x^2 + 14y^2,\ 2x^2 + 7y^2,\ 3x^2 \pm 2xy + 5y^2$
-108	3	$x^2 27y^2,\ 4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2,\ 4x^2 + 4xy + 17y^2,\ 5x^2 \pm 2xy + 13y^2$

3

Grupo de clases en cuerpos cuadráticos imaginarios

En este capítulo estudiaremos el problema del logaritmo discreto y su resolución mediante el método de Shanks, *Baby's Step Giants Step*. De este modo introduciremos el algoritmo de Terr el cual se basa en la idea del algoritmo de Shanks.

En teoría de grupos, el algoritmo de *Baby's Step Giants Step* es uno de los diferentes algoritmos que tratan de abordar de manera más eficiente el problema del logaritmo discreto. Por tanto, será necesario estudiar en primer lugar el probelma del logaritmo discreto para llegar a tener una mayor concepción del algoritmo de *Baby's Step Giants Step*.

3.1 El problema del logaritmo discreto

Sea G un grupo abeliano y $g \in G$ un elemento de orden n. Dado $a \in \langle g \rangle \subseteq G$, definiremos en términos generales al logaritmo discreto de a en base g como el entero k con $0 \leq k \leq n-1$, tal que:

$$g^k = a$$

Se dice también que k es en índice de a en base g.

Un caso particular del logaritmo discreto sería tomar como grupo abeliano a los $\mathbb{Z}_p$. De este modo, para estos grupos la definición de logaritmo discreto sería la siguiente:

Sea p un número primo fijo y consideremos a, $b \neq 0$ con $a \in \mathbb{Z}_p$ tal que $\mathbb{Z}^*{}_p =< a >$ y $b \in \mathbb{Z}^*{}_p$. En estas condiciones, llamaremos logaritmo discreto de b en base a al único entero k, con $0 \leq k \leq n-1$, tal que.

$$a^k \equiv b \text{ (mod p)}.$$

Y lo denotaremos por $k = log_a b$. El problema de hallar k es llamado el problema del logaritmo discreto.

Ejemplo: Consideremos $p = 11$. Entonces, tendremos $\mathbb{Z}^*_{11}$ un grupo cíclilo de orden 10, y 7 será un generador de $\mathbb{Z}^*_{11}$. Así:

$$7^6 \equiv 4 \pmod{11}$$

y

$$log_7 4 = 6$$

en $\mathbb{Z}_{11}$.

La razón por la que tomamos a como un elemento primitivo, es decir $\mathbb{Z}_p^* =< a >$, es para poder definir bien el logaritmo discreto y evitar así que $b \equiv 0 \pmod{p}$.

Dado a un generador de $\mathbb{Z}^*{}_p$, b_1,$b_2 \in \mathbb{Z}^*{}_p$ y s un entero podemos definir las siguientes propiedades del logaritmo discreto como siguen:

1. $log_a(b_1 b_2) = log_a b_1 + log_a b_2$
2. $log_a {b_1}^s = s log_a b_1$

Si p es pequeño entonces es fácil calcular los logaritmos discretos, probando con todos los exponentes posibles. Sin embargo para valores muy grandes de p se vuelve complicado.

Del interés del logaritmo discreto como operación inversa a la exponenciación en un grupo, viene la importancia del estudio y análisis del problema del logaritmo discreto. La exponenciación modular es una operación sencilla, para la que se conocen métodos eficientes como el que expondremos a continuación. En cambio, para un módulo entero cualquiera, el logaritmo discreto no siempre puede obtenerse de forma eficiente.

Supongamos que deseamos calcular b^e en el grupo multiplicativo de los enteros módulo m. Primero, debemos escribir el exponente binario: $e = \sum_{i=0}^{n-1} a_i 2^i$ y posteriormente seguir los siguientes pasos:

- Se define $i := n - 1$ y $v := 1$.
- Para $i = n - 1$ hasta 0
  1. $v = \begin{cases} v = vb \pmod{m} \text{ si } a_i = 1 \\ v = v \text{ si } a_i \neq 1 \end{cases}$
  2. $v = \begin{cases} v = v \text{ si } i = 0 \\ v = v^2 \pmod{m} \text{ si } i \neq 0 \end{cases}$

  Tras la última iteración se obtiene $v = b$.

Ejemplo: Sea $\mathbb{Z}_{11}^*$ el grupo multiplicativo de enteros módulo 11. Calculemos 7^{27}. Esto puede hacerse de cualquiera de las formas explicadas:

- Realizando las 26 multiplicaciones: $7^{27} \equiv 6 \pmod{11}$.
- Utilizando el método binario de exponenciación modular. Como $27 = 2^4 + 2^3 + 2 + 1$, la representación binaria de 2 es 11011. Entonces, tomamos $i = 4$ y $v = 1$.

i	a_i	v
4	1	$(1 \cdot 7)^2 \equiv 5 \pmod{11}$
3	1	$(5 \cdot 7)^2 \equiv 4 \pmod{11}$
2	0	$4^2 \equiv 5 \pmod{11}$
1	1	$(5 \cdot 7)^2 \equiv 4 \pmod{11}$
0	1	$(4 \cdot 7) \equiv 6 \pmod{11}$

Por lo tanto, $7^{27} \equiv 6 \pmod{11}$. Con este método se reduce el número de multiplicaciones que se deben realizar de 26 a 8.

Como podemos apreciar la exponenciación podría considerarse una buena función "trampa". Es por ello que algunos criptosistemas, como el criptosistema de ElGamal, y sistemas de autentificación de mensajes e intercambio de claves basan su seguridad en el problema del logaritmo discreto.

3.2 Cálculo del logaritmo discreto

El algoritmo de Shanks paso de gigante paso de bebé es uno de los métodos utilizados para resolver el problema del logaritmo discreto. Nuestro objetivo en esta sección será conocer la idea general del algoritmo de Shanks para el cálculo del logaritmo discreto para, posteriormente, ver su aplicación en el algoritmo de Terr.

Problema: A partir de un grupo multiplicativo $\mathbb{Z}_p^*$ consideraremos un generador a y un elemento b de dicho grupo. Nuestro objetivo será calcular el logaritmo discreto de b en base a, es decir, $x = log_a b$.

Algoritmo: Sea n el orden de $\mathbb{Z}_p^*$, entonces

1. Ponemos $m = [\sqrt{n}]$.
2. Construimos una tabla con los valores (j, a^j) para $o \leq j < m$. Ordenamos la tabla usando la segunda componente.
3. Calculamos el inverso de a^{-m} módulo p y ponemos $d = b$.
4. Para los valores de i tal que $0 \leq i < m - 1$ hacemos lo siguiente:
   a) Comprobamos si d es una segunda componente de la tabla.
   b) Si $d = a^j$ entonces obtenemos $x = im + j$.
   c) Ponemos $d = d \cdot a^{-m}$.

Ejemplo: Consideremos el grupo $\mathbb{Z}_{13}^*$ de orden 12. Dado 2 un generador de $\mathbb{Z}_{13}^*$ y un elemento $5 \in \mathbb{Z}_{13}^*$, calculemos $x = log_2 5$.

1. Denotaremos $m = [\sqrt{12}] = 4$.
2. Construimos una tabla de valores $(j,\ 2^j)$ tal que $0 \leq j < 4$:

j	a^j
0	1
1	2
2	4
3	8

3. Calculamos 2^{-4} (mod 13). En primer lugar, debemos obtener el inverso de 2 módulo 13 mediante el algoritmo de Euclides.

$$13 = 6 \cdot 2 + 1$$

Dado que $1 = 13 - 6 \cdot 2$, el inverso es -6. Luego $2^{-4} \equiv (-6)^4 \equiv 4 \pmod{13}$ y denotamos $d = 5$.

4. Para $0 \leq i < 3$ buscamos el valor de i tal que el d esté en la tabla anterior.

   - Para $i = 0$ tenemos $d = 5$. No está en la tabla.
   - Para $i = 1$ tenemos $d = 5 \cdot 4 = 7$. No está en la tabla.
   - Para $i = 2$ tenemos $d = 7 \cdot 4 = 2$. Sí esta en la tabla.

   Luego:

$$x = 2 \cdot 4 + 1 = 9$$

   Y

$$log_2 5 = 9$$

   en $\mathbb{Z}_{13}^*$.

Ejemplo: Sea ahora el grupo $\mathbb{Z}_{97}^*$ de orden 96. Un generador es 5 y un elemento $35 \in \mathbb{Z}_{97}^*$, calculemos $x = log_5 35$.

1. Denotaremos $m = [\sqrt{96}] = 10$.
2. Construimos una tabla de valores $(j,\ 5^j)$ tal que $0 \leq j < 10$:

j	a^j
0	1
1	5
2	25
3	28
4	43
5	21
6	8
7	40
8	6
9	30

3. Hallamos 5^{-10} (mod 97), para ello obtenemos el inverso de 5 módulo 97 mediante el algoritmo de Euclides.

$$97 = 5 \cdot 19 + 2$$

$$5 = 2 \cdot 2 + 1$$

   Dado que

$$1 = 5 - 2 \cdot 2$$

$$2 = 97 - 5 \cdot 19$$

tendremos que

$$1 = 5 - 2(97 - 5 \cdot 19)$$
$$1 = 5 - 2 \cdot 97 + 38 \cdot 5$$
$$1 = 39 \cdot 5 - 2 \cdot 97$$

Luego el inverso es 39 y $5^{-10} \equiv 39^{10} \pmod{13}$. Llamamos $d = 35$.

4. Para $0 \leq i < 9$ estudiamos si d está en la tabla o no.
   - Para $i = 0$ tenemos $d = 35$. No está en la tabla.
   - Para $i = 1$ tenemos $d = 35 \cdot 39 = 94$. No está en la tabla.
   - Para $i = 2$ tenemos $d = 94 \cdot 39 = 64$. No esta en la tabla.
   - Pra $i = 3$ tenemos $d = 64 \cdot 11 = 25$. Sí está en la tabla.

   Luego:
   $$x = 3 \cdot 10 + 2 = 32$$
   Y
   $$log_5 35 = 32$$
   en $\mathbb{Z}_{97}^*$.

3.3 Algoritmo de Terr

El algoritmo de Terr se basa en el algoritmo de *Paso de gigante paso de bebé* y busca calcular el orden de un elemento en un grupo G. En nuestro caso, buscaremos obtener el orden de los elementos de los grupos de clases de cuerpos cuadráticos imaginarios. Para ello, trabajaremos de forma más sencilla en términos de clases de formas cuadráticas en lugar de con el grupo de clases de ideales lo cuál será posible pues como hemos visto anteriormente, existe una biyección entre ambas.

Al trabajar con la clase de formas cuadráticas será necesario estudiar un método de reducción mediante el cual a partir de cualquier forma cuadrática podamos obtener la única forma reducida en dicha clase.

Algoritmo: *(Reducción de formas cuadráticas definidas positivas)* Dada una forma cuadráticas (a, b, c) definida positiva con discriminante $D = b^2 - 4ac < 0$, este algortimo da la única forma reducida equivalente a f.

1. [Inicialización] If $-a < b \leq a$ ir al paso 3.
2. [División Euclides] Llamamos $b = 2aq + r$ con $0 \leq r < 2a$. If $r > a$, entonces $r \leftarrow r - 2a$ y $q \leftarrow q + 1$ (En otras palabras, queremos que $b = 2aq + r$ con $-a < r \leq a$.) Entonces $c \leftarrow c - \frac{1}{2}(b + r)q$, $b \leftarrow r$.
3. [Final] If $a > c$, $b \leftarrow -b$, cambiamos a y c y volvemos al paso 2. De otro modo, If $a = c$ y $b < 0$, $b \leftarrow -b$. Output (a, b, c) y termina el algoritmo.

Lema 3.1. *Sea (a,b,c) una forma cuadrática definida positiva de discriminante $D = b^2 - 4ac < 0$ de modo que $-a < b \leq a$ y $a < \sqrt{|D|}$. Entonces, o (a,b,c) es también reducida o la forma (a,r,s) donde $-b = 2cq + r$ con $-c < r < c$ obtenida por el algoritmo de redución será reducida.*

La estructura de grupo en la clase de ideales lleva sólo a clases de formas cuadráticas, sin embargo podemos definir una operación entre las formas cuadráticas a la que denominaremos composición. Ésta será la operación utilizada en el algoritmo de Terr.

Definición 3.1. *Sea $f_1 = (a_1, b_1, c_1)$ y $f_2 = (a_2, b_2, c_2)$ dos formas cuadráticas con el mismo discriminante D. Definimos $s = (b_1 + b_2)/2$, $n = (b_1 - b_2)/2$ y consideremos u, v, w y d tal que*

$$ua_1 + va_2 + ws = d = mcd(a_1, a_2, s)$$

Definiremos la composición de dos formas cuadráticas f_1 y f_2 como la forma

$$(a_3, b_3, c_3) = \left(d_0 \frac{a_1 a_2}{d^2}, b_2 + \frac{2a_2}{d}(v(s - b_2) - wc_2), \frac{b_3^2 - D}{4a_3} \right)$$

módulo la acción de $\Gamma_\infty := \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, m \in \mathbb{Z} \right\}$, *donde* $d_0 = mcd(d, c_1, c_2, n)$.

Una vez definida la composición entre dos formas cuadráticas y un algoritmo para hallar la forma reducida de una forma f, podemos introducir el algoritmo de Terr. La idea es la siguiente:

Proposición 3.1. *Sea $g \in G$. Entonces existe un $e \in \mathbb{N}$ y $f \in \{0, ..., e-1\}$ con $g^{e(e+1)/2} = g^f$. Si e es minimal con esta propiedad, entonces $e(e-1)/2 < orden(g) \leq e(e+1)/2$ y $orden(g) = e(e+1)/2 - f$.*

Para $e = 1, 2...$ este algoritmo calcula el conjunto

$$\text{babySet} = \{(g^f, f) : 0 \leq f < e\}$$

y revisa si existe algún par de la forma $\left(g^{e(e+1)/2}, f\right)$ en babySet para algún f. Por el lema anterior, ésto sucede. Si sucede en el primer caso, entonces $orden(g) = e(e+1)/2 - f$. En la e-sima iteración del algoritmo usaremos

$$\text{babyElement} = g^e, \quad \text{giantElement} = g^{e(e+1)/2}$$

Algoritmo de Terr

1. [Inicialización] babySet $\leftarrow \{(1,0)\}$, e $\leftarrow 1$, babyElement$\leftarrow$ g, giantElement $\leftarrow$ g
2. [Loop] If babySet contiene un par $(gianElement, f)$ entonces $n = e(e+1)/2 - f$
   Incluir $(babyElement, e)$ en BabySet
   BabyElement $\leftarrow g\cdot$ babyElement
   $e \leftarrow e+1$ giantElement $\leftarrow$ giantElement $\cdot$ babyElement

Ejemplo: Sea $D = -227$ y la forma cuadrática $f = (3,1,19)$. Determinemos el orden de la clase de equivalencia $C = [3,1,19]$ de f en el grupo de clases Cl_{-227}.

$$BabySet_1 = \{([1,1,5],0)\}$$
$$BabyElement_1 = giantElement_1 = [3,1,19]$$

- Para **e** = **1**: Podemos observar que el conjunto $babySet_1$ no contiene ningún par cuya primera componente este en $giantElement_1$. Luego definamos:
  1. $babySet_2 = \{([1,1,5],0),\ ([3,1,19],1)\}$
  2. $BabyElement_2 = g \cdot BabyElement_1 = (3,1,19)\cdot(3,1,19)$. Veamos la composición de la formas cuadrática $(3,1,19)$ con ella misma.

     $$s = \frac{1+1}{2} = 1 \quad \text{y} \quad n = \frac{1-1}{2} = 0$$

     Para $u = 0,\ v = 0$ y $w = 1$, tendremos

     $$3u + 3v + 1w = d = mcd(3,3,1) = 1.$$

     Como $d_0 = mcd(a_1, a_2 d, c_1, c_2, n) = mcd(3,3,1,19,19,0) = 1$, obtenemos que la forma cuadrática resultante de la composción es:

     $$(a_3, b_3, c_3) = \left(1\frac{3\cdot 3}{1^2}, 1 + \frac{2\cdot 3}{1}(-1\cdot 19), \frac{b_3^2 - D}{4a_3}\right) = (9, -113, 361)$$

     Utilizando el algoritmo de reducción reducimos la forma cuadrática dada por la composción. Como no se cumple que $-a < b \leq a$, tendremos que

     $$-113 = 18q + r \quad 0 \leq r < 18$$

     $$-113 = 18\cdot(-6) + (-5) \quad 0 \leq r < 18$$

     Con lo que $b = -5,\ a = 9$ y $c = 7$. Como $a > c$ tendríamos que la forma reducida es $(7,-5,9)$. Por tanto $BabyElement_2 = (7,-5,9)$.
  3. $giantElement_2 = giantElement_1 \cdot BabyElement_1 = (3,1,19)\cdot(3,1,19) = (7,-5,9)$, razonando de forma similar.

- Para **e=2** podemos ver que el conjunto $babySet_2$ no contiene ningún par con primera componente en $giantElement_2$. Luego volvemos a hacer otra iteración.

  1. $babySet_3 = \{([1,1,5],0),([3,1,19],1),([7,-5,9],2)\}$
  2. $BabyElement_3 = g \cdot BabyElement_2 = (3,1,19)\cdot(7,-5,9)$. Componiendo:

$$s = \frac{1+(-5)}{2} = -2 \quad \text{y} \quad n = \frac{1-(-5)}{2} = -3$$

  Para $u = 1$, $v = 0$ y $w = 1$, tendremos

$$3u + 7v + (-2)w = d = mcd(3,7,-2) = 1.$$

  Como $d_0 = mcd(a_1,a_2,d,c_1,c_2,n) = mcd(3,7,1,19,9,0) = 1$, obtenemos que la forma cuadrática resultante de la composción es:

$$(a_3,b_3,c_3) = \left(1\frac{3\cdot 7}{1^2},(-5)+\frac{2\cdot 7}{1}(-1\cdot 9),\frac{b_3^2-D}{4a_3}\right) = (21,-131,207)$$

  Reduciendo la forma obtenida por la composición, tenemos que

$$-131 = 42q + r \quad 0 \le r < 42$$

$$-131 = 42\cdot(-3)+(-5) \quad 0 \le r < 42$$

  Con lo que $b = -5$, $a = 21$ y $c = 3$. Como $a > c$ tendríamos que la forma reducida es $(3,-5,21)$. Por tanto $BabyElement_3 = (3,-5,21)$.

  3. $giantElement_3 = giantElement_2 \cdot BabyElement_2 = (7,-5,9)\cdot(7,-5,9)$, entonces

$$s = \frac{(-5)+(-5)}{2} = (-5) \quad \text{y} \quad n = \frac{(-5)+(-5)}{2} = 0$$

  Para $u = -2$, $v = 0$ y $w = -3$, tendremos

$$7u + 7v + (-5)w = d = mcd(7,7,-5) = 1.$$

  Como $d_0 = mcd(a_1,a_2,d,c_1,c_2,n) = mcd(7,7,1,9,9,0) = 1$, obtenemos que la forma cuadrática resultante de la composción es:

$$(a_3,b_3,c_3) = \left(1\frac{7\cdot 7}{1^2},(-5)+\frac{2\cdot 7}{1}(3\cdot 9),\frac{b_3^2-D}{4a_3}\right) = (49,373,711)$$

  Mediante el algoritmo de redución, observamos que

$$373 = 98q + r \quad 0 \le r < 98$$

$$373 = 98 \cdot 3 + 79 \quad 0 \leq r < 98$$

Como $r = 79 > a = 49$, $r = r - 2a = -19$ y $q = q + 1 = 4$. Entonces $b = -19$, $a = 49$ y $c = 3$. Como $a > c$ intercambiamos ambos valores y dado que aún podemos expresar $b = 2aq + r$, $b = -b = 19$.

$$19 = 9 \cdot q + r \quad 0 \leq r < 9$$

$$19 = 9 \cdot 2 + 1 \quad 0 \leq r < 9$$

Con lo que $b = 1$, $a = 3$ y $c = 19$. Por tanto $BabyElement_3 = (3, 1, 19)$.

- Para **e=3** podemos ver que $babySet_3$ contiene el par $([3, 1, 19], 1)$ cuya primera componente coincide con $giantElement_3 = (7, -5, 9)$,luego el orden de C es

$$n = e(e + 1)/2 - f = 3(3 + 1)/2 - 1 = 5.$$

4

Conclusión

Acabaremos este trabajo dedicando algo de tiempo a ensalzar aquellos resultados de gran importancia.

En primer, hemos recordado en la introdución los conceptos de grupo de clases, cuerpos cuadráticos e ideales los cuales han estado presentes en el desarrollo de los capítulos posteriores. A partir de aquí, nuestro punto de partida ha sido el estudio de las formas cuadráticas binarias. Hemos estudiado su definición y propiedades lo que nos ha permitido deternernos más profundamente en el análisis de ciertos resultados como la equivalencia de formas cuadráticas, la relación entre clases de ideales y formas cuadráticas y las formas reducidas.

La equivalencia entre dos formas cuadráticas es una relación de equivalencia que preserva el discriminante de una forma a otra y la primitividad. Además hemos podido probar que dos formas equivalentes representan al mismo entero con lo que ambas formas deben ser simltaneamente definidas igual.

La relación entre clases de ideales y formas cuadráticas es uno de los resultados más importantes de este apartado pues es la prueba de que podemos trabajar de igual forma con clases de ideales y formas cuadráticas, pues exite una biyección entre ambos. Este resultado es de gran utilidad pues en términos de algoritmos y computación suele ser más sencillo trabajar con formas cuadráticas.

También hemos podido profundizar un poco en la reducción de las formas cuadráticas definidas positivas, lo que hemos llegado al resultado de que el número de formas reducidas primitivas de una clase de formas cuadráticas definidas positivas nos determina el número de clases, $h(D)$ para un determinado D. Mediante unos ejemplos hemos ilustrado este resultado.

Por último, una vez conocido todo lo ensencial, hemos analizado el algoritmo de Terr para obtener el orden de los elementos de los grupos de clases de cuerpos cuadráticos imaginarios. Este algoritmo basa su idea en el algoritmo de Shanks, que hemos introducido e ilustrado anteriormente como método para resolver el problema del logaritmo discreto. Con una concepción más clara del algoritmo de Shanks hemos estudiado el algoritmo de Terr y explicado con un ejemplo.

Cabe destacar la importancia del logaritmo discreto en criptografía. El problema del logaritmo discreto cuenta con diversos métodos para su calculo, sin embargo no hay ningún algoritmo que lo resuelva de forma general. El hecho de que el cálculo del problema inverso, la exponenciación discreta, sea fácil en términos computacionales, mientras que el problema del logaritmo discreto es dificl en muchos grupos hace que se utilice en criptografia en el metodo de intercambio de claves de Diffie-Hellman o en el sistema de ElGamal.

5

Anexo

5.1 Matrices equivalentes

Código:

```
Clear[ a, b, c]
a = 1;
b = -8;
c = 6;
f = a x^2 + b xy + c y^2;
A = {{2 a, b}, {b , 2 c}};
X = {{x}, {y}};
Print["Dada la forma cuadrática f(x,y)=", f, "
podemos expresarla matricialmente de la forma
f(x,y)=(1/2) X'A(f)X tal que f(x,y)=",
 1 / 2, MatrixForm[Transpose[X]], MatrixForm[A], MatrixForm[X]]

Print["Una forma equivalente a f(x,y) será de la forma
g(x,y)=(1/2)X'A(g)X, donde A(g)=P'A(f)P. La matriz P
será una matriz del grupo lineal LG=[2,Z]. Hemos creado una
lista de matrices 2x2 aleatoria de las cuales nos quedaremos
con una cuyo det=1 o det=-1, es decir, pertenezca al grupo lineal:"]

lista = RandomInteger[{-10, 10}, {1000, 2}];
matrix = Partition[lista, 2];
For[i = 1, i < Dimensions[matrix][[1]], i++, valdet = Det[matrix[[i]]];
 If[valdet == 1 || valdet == -1, M = matrix[[i]], Unevaluated[Sequence[]]]]
Print[" P=", MatrixForm[M], " y A(g)=", MatrixForm[Transpose[M]],
 MatrixForm[A], MatrixForm[M], "=", MatrixForm[Transpose[M].A.M]]
H = MatrixForm[Transpose[M].A.M];
Print["Con lo que g(x,y)=", 1 / 2, MatrixForm[Transpose[X]], MatrixForm[H],
 MatrixForm[X]]
```

Dada la forma cuadrática $f(x,y)=x^2-8xy+6y^2$

podemos expresarla matricialmente de la forma $f(x,y)=(1/2)\ X'A(f)X$ tal que $f(x,y)=\frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 2 & -8 \\ -8 & 12 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

Una forma equivalente a $f(x,y)$ será de la forma $g(x,y)=(1/2)X'A(g)X$, donde $A(g)=P'A(f)P$. La matriz P será una matriz del grupo lineal $LG=[2,Z]$ cuyo determinante es 1 o -1. Hemos creado una lista de matrices 2x2 aleatoria de las cuales nos quedaremos con una cuyo determinante sea 1 o -1, es decir, pertenezca al grupo lineal:

$P=\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}$ y $A(g)=\begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}\begin{pmatrix} 2 & -8 \\ -8 & 12 \end{pmatrix}\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 2 & 4 \\ 4 & -12 \end{pmatrix}$

Con lo que $g(x,y)=\frac{1}{2}\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} 2 & 4 \\ 4 & -12 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

5.2 Método de Shanks para resolución del logaritmo discreto:

Código1:

```
Clear[p, f, α, β, j, i, b, x];
p = 13;
α = 2;
β = 5;
m = Floor[Sqrt[p - 1]] + 1;
Array[f, m - 1, 0];
Array[h, m - 1, 0];
b = PowerMod[α, -1, p];
j = 0;
i = 0;
flag = 0;
While[j < m, f[j] = Mod[α^j, p];
  Print["f[", j, "]=", f[j]]; j++];
While[(i < m) && (flag == 0), h[i] = Mod[β * b^(m * i), p];
 For[j = 0, j < m, j++, If[h[i] == f[j], flag = 1;
   Print["h[", i, "]=", h[i]];
   x = j + m * i]]; i++]
If[flag == 0, Print["No logaritmo"]];
If[flag == 1, Print["logaritmo en base ", α, " de ", β, " = ", x]]
```

```
f[0]=1
f[1]=2
f[2]=4
f[3]=8
h[2]=2
logaritmo en base 2 de 5 = 9
```

Código2:

```
Clear[p, f, α, β, j, i, b, x];
p = 97;
α = 5;
β = 35;
m = Floor[Sqrt[p - 1]] + 1;
Array[f, m - 1, 0];
Array[h, m - 1, 0];
b = PowerMod[α, -1, p];
j = 0;
i = 0;
flag = 0;
While[j < m, f[j] = Mod[α^j, p]; Print["f[", j, "]=", f[j]]; j++];
While[(i < m) && (flag == 0), h[i] = Mod[β * b^(m * i), p];
 For[j = 0, j < m, j++, If[h[i] == f[j], flag = 1;
   Print["h[", i, "]=", h[i]];
   x = j + m * i]]; i++]
If[flag == 0, Print["No logaritmo"]];
If[flag == 1, Print["logaritmo en base " , α , " de ", β, " = " , x]]
```

```
f[0]=1
f[1]=5
f[2]=25
f[3]=28
f[4]=43
f[5]=21
f[6]=8
f[7]=40
f[8]=6
f[9]=30
h[3]=25
logaritmo en base 5 de 35 = 32
```

Bibliografía

[1] Cox, David A. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Canada: John Wiley and sons, inc. 1989. [Consulta: 23 de Mayo de 2016]

[2] Cohen, H. *A course in computational algebraic number theory*. Springer-Verlag, Berlin, 1993. MR 94i:11105. https://archive.org/stream/springer_10.1007-978-3-662-02945-9/10.1007-978-3-662-02945-9#page/n0/mode/2up.[Consulta: 23 de Mayo de 2016]

[3] Riesel, H. *Prime numbers and computer methods for factorization*. Progress in Mathematics, vol. 126, 2nd ed, Birkhauser Boston, Inc., Boston, MA, 1994.[Consulta: 3 de Junio de 2016]

[4] Trifković, M. *Algebraic Theory of Quadratic Numbers*. New York: Springer Science and Business Media. 14 de septiembre, 2013.[Consulta: 3 de Junio de 2016]

[5] Weston, T. *Algebraic Number Theory*. https://www.math.wisc.edu/~mmwood/748Fall2014/weston.pdf. [Consulta: 5 de Junio de 2016]

[6] Ivorra Castillo, C. *Teoría de números*. https://www.uv.es/ivorra/Libros/Numeros.pdf. [Consulta: 5 de Junio de 2016]

[7] Bakker, B.*Lecture notes: quadratic forms*. https://www2.mathematik.hu-berlin.de/~bakkerbe/math248/quadforms.pdf. [Consulta: 11 de Junio de 2016]

[8] Ireland, K and Rosen, M, *A Classical Introduction to Modern Number Theory*. Springer Science and Business Media. 17 abril 2013. https://archive.org/stream/springer_10.1007-978-1-4757-2103-4/10.1007-978-1-4757-2103-4#page/n0/mode/2up. [Consulta: 14 de Junio de 2016]

[9] Milne, J.S. *Algebraic Number Theory*. Version 3.06. 28 de mayo , 2014. http://www.jmilne.org/math/CourseNotes/ANT.pdf. [Consulta: 15 de Junio de 2016]

[10] Santamaría Fernández, M. *El logaritmo discreto y sus aplicaciones en Criptografía*. Trabajo dirigido de estadística y computación. Universidad de Cantabría. 2012-2013. http://repositorio.unican.es/xmlui/bitstream/handle/10902/3101/Jennifer%20Santamaria%20Fernandez.pdf?sequence=1. [Consulta: 16 de Junio de 2016]

[11] Song Y. Yan. *Number Theory for Computing*. Berlin Heidelberg: Springer-Verlag. 2000-2002.http://tomlr.free.fr/Math%E9matiques/Math%20Complete/Number%20theory/Number%20theory%20for%20computing%20-%20Yan%20S%20Y..pdf. [Consulta: 22 de Junio de 2016]

[12] Dr. Abhijit Das. *Computational number theory*. Taylor and Francis Group, LLC. 2013. [Consulta: 22 de Junio de 2016]

[13] Flath, Daniel E. *Introduction to number theory*. New York: John Willey and sons. 1989. [Consulta: 22 de Junio de 2016]

[14] Borevich, Z.I and Shafarevich, I. R. *Number Theory*. New York: Academic Press. 1966. http://www.maths.ed.ac.uk/~aar/papers/borevich.pdf. [Consulta: 23 de Junio de 2016]

[15] Burton, W, Jones. *The Arithmetic Theory of Quadratic Forms*. University of Colorado: The mathematical association of America, 2nd ed. 1961. http://www.maths.ed.ac.uk/~aar/papers/bwjones.pdf. [Consulta: 25 de Junio de 2016]

[16] Alexánder Borbón A., Walter Mora F.. *Edición de texto científicos LATEX 2014*. Revista digital Matemática Educación e Internet, 2nd ed. http://tecdigital.tec.ac.cr/revistamatematica/Libros/LATEX/LaTeX_2013.pdf. [Consulta: 27 de Junio de 2016]

[17] Luis, Miniejercicios con latex[blog internet], Espanña: Luis. 2012,Abril. http://minisconlatex.blogspot.com.es/2012/04/escribir-codigo-de-programacion-en.htm. [Consulta:27 de Junio de 2016]