UNIVERSITAT DE BARCELONA

Treball Final del Grau de Matemàtiques
Facultat de Matemàtiques i Informàtica

EL PROBLEMA DEL NOMBRE DE CLASSES 1

Guillem Garcia Tarrach

Director: Dr. Artur Travesa i Grau

Barcelona, 27 de juny de 2018

Abstract

The ring of integers is a unique factorization domain, but, in general, this isn't the case for the ring of integers of a number field. The class number 1 problem consists in giving a complete list of all imaginary quadratic fields whose ring of integers is a unique factorization domain. In this thesis we provide an adaptation of Kurt Heegner's original solution including an overview of the required theoretical tools, namely class field theory and the theory of elliptic curves with complex multiplication.

Resum

L'anell dels enters és un domini de factorització única, però els anells d'enters dels cossos de nombres no ho són en general. El problema del nombre de classes 1 consisteix a trobar quins anells d'enters de cossos quadràtics imaginaris sí que ho són. En aquest treball donem una adaptació de la solució original de Kurt Heegner, incloent-hi una visió general de les eines teòriques necessàries per a entendre-la: la teoria de cossos de classes i la teoria de corbes el·líptiques amb multiplicació complexa.

2010 Mathematics Subject Classification. 11E41, 11R04, 11R11, 11R29, 11R37, 11R65, 11G15

Continguts

Agraïments

M'agradaria agrair, en primer lloc, al meu tutor, el Dr. Artur Travesa i Grau, la seva ajuda i direcció durant el desenvolupament d'aquest treball. També m'agradaria agrair als meus amics i a la meva família el suport que m'han durant al llarg de tot el grau, especialment al meu pare, a qui li dedico aquest treball.

Introducció

Una interpretació del teorema fonamental de l'aritmètica és que l'anell dels nombres enters és un domini de factorització única. Si K és un cos de nombres, no és cert en general que l'anell d'enters de K, $\mathcal{O}_K$, també ho sigui. De fet, aquesta és una de les raons per les quals el teorema de Fermat no va ser demostrat en el segle XIX: Gabriel Lamé va presentar l'any 1847 una demostració en la qual suposava que els anells d'enters dels cossos ciclotòmics eren dominis de factorització única, però Ernst Kummer ja havia observat l'any 1844 que aquesta suposició era errònia.

El problema del nombre de classes 1 consisteix a trobar per a quins cossos quadràtics imaginaris, $\mathbb{Q}(\sqrt{N})$ amb $N < 0$ lliure de quadrats, l'anell d'enters és un domini de factorització única. Aquest problema va ser plantejat originalment per Gauss a les *Disquisicions Aritmètiques* (1801), i no va ser resolt fins l'any 1952 per Kurt Heegner. La solució de Heegner va ser rebutjada inicialment perquè feia referència a una secció de l'*Àlgebra* de Heinrich Weber que era incompleta i contenia imprecisions. De manera independent, Alan Baker i Harold Stark van arribar al mateix resultat els anys 1966 i 1967 respectivament, i l'any 1969 Stark va completar la prova de Heegner. Aquest resultat és coneix avui com el teorema de Heegner-Baker-Stark, i afirma que els únics $N < 0$ per als quals l'anell d'enters de $\mathbb{Q}(\sqrt{N})$ és un domini de factorització única són $-1, -2, -3, -7, -11, -19, -43, -67, -163$.

Aquest resultat també té algunes conseqüències sorprenents. Per exemple, explica per què el nombre $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925...$ és tan proper a un enter, o per què $n^2 - n + 41$ és primer per $n = 0, 1, ..., 40$, dos fets que a priori podrien semblar casualitat.

L'objectiu que ens plantegem en aquest treball és donar una adaptació de la solució original de Heegner, però cal que abans introduim algunes eines teòriques essencials per a poder entendre-la. La memòria està estructurada de la manera següent.

Al capítol 1 formulem el problema i definim el grup de classes d'ideals de l'anell d'enters dels cossos de nombres. De fet, definim el grup de classes d'ideals d'una classe més general d'anells, els ordres $\mathcal{O}$ de cossos quadràtics imaginaris, i reformulem el problema en termes d'aquest grup. Donem diverses descripcions d'aquest grup, i també alguns resultats elementals sobre el nombre de classes dels ordres de cossos quadràtics imaginaris utilitzant el llenguatge de les formes quadràtiques binàries enteres.

Als capítols 2 i 3 descrivim les eines que ens permetran desenvolupar la solució del problema. Al capítol 2 donem una visió general de la teoria de cossos de classes, que estudia les extensions abelianes dels cossos de nombres, enunciant-ne alguns dels resultats més imporants. A més, veiem la seva relació amb els grups de classes d'ideals. Més concretament, el grup de classes d'ideals d'un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K és isomorf al grup de Galois d'una extensió de K, anomenada cos de classes de l'ordre $\mathcal{O}$.

Al capítol 3 descrivim la teoria de corbes el·líptiques amb multiplicació complexa. Hi veiem la relació entre aquestes corbes i els ordres dels cossos quadràtics imaginaris, i per a estudiar-les definim diverses funcions i estudiem les seves propietats analítiques. El paper més important el juga l'anomenat invariant j, que fa possible donar una descripció explícita del cos de classes d'un ordre d'un cos quadràtic imaginari.

Al capítol 4, calculem l'invariant j d'alguns ordres que ja sabem que tenen nombre de classes 1, i reduim el problema de trobar tots els invariants j possibles a la resolució de l'equació diofantina $2X(X^3+1) = Y^2$. Finalment, resolem aquesta equació, trobant així la solució del problema.

En els tres primers capítols no s'inclouen algunes de les demostracions dels resultats que s'enuncien, però s'inclouen referències on es poden trobar. Tot i això, en els capítols 1 i 3, les demostracions que es troben en aquestes referències es poden seguir sense gaire dificultat amb els coneixements d'àlgebra i anàlisi obtinguts durant el grau i, tot i que no estan escrites en la memòria, han estat treballades a l'hora de fer aquest treball. En canvi, per a treballar amb detall el capítol 2 necessitaríem introduir noves eines teòriques més complicades, que requeririen en sí un treball propi. La continuació natural d'aquest treball seria, per aquesta raó, aprofundir en la teoria de cossos de classes, estudiant-la en detall i demostrant-ne els teoremes que aquí només hem enunciat.

El problema del nombre de classes 1 exemplifica clarament com, per a arribar a resultats profunds en una branca de les matemàtiques, s'acostuma a necessitar coneixements i tècniques d'altres. En aquest cas, per a resoldre un problema algebraic en teoria de nombres, és necessari utilitzar tècniques d'anàlisi complexa, per exemple. Per aquesta raó, aquest treball és una manera especialment adequada d'acabar el grau, ja que combina i relaciona coneixements adquirits en moltes de les assignatures cursades durant aquests quatre anys.

1 Formulació del problema

1.1 Enters algebraics i grup de classes d'ideals

El teorema fonamental de l'aritmètica precisa com, per a tot enter $n \in \mathbb{Z}$, podem descompondre n de manera única en un producte de la forma

$$n = \pm p_1^{e_1} \cdots p_r^{e_r},$$

on $p_1, ..., p_r$ són enters primers diferents i $e_1, ..., e_r$ són enters positius. En altres paraules, l'anell $\mathbb{Z}$ és un domini de factorització única.

De fet, podem estendre el resultat dient que, per a tot nombre racional $q \in \mathbb{Q}$, podem descompondre q de manera única en un producte de la forma

$$q = \pm p_1^{e_1} \cdots p_r^{e_r}, \tag{1.1.1}$$

on $p_1, ..., p_r$ són enters primers diferents i $e_1, ..., e_r$ són enters no nuls, no necessàriament positius.

Un cos de nombres K és un cos de característica 0 i tal que el grau $[K : \mathbb{Q}]$ és finit. Ens podem preguntar per a quins cossos de nombres tenim una propietat semblant a (1.1.1). En primer lloc, cal precisar exactament quina és aquesta propietat, és a dir, cal definir per a quin subanell de K han de ser primers els p_i.

Definició 1.1.2. Siguin A, B dominis d'integritat tals que $A \subseteq B$. Diem que un element $b \in B$ és enter de grau n sobre A si b és arrel d'un polinomi mònic irreductible de grau n de coeficients en A. El conjunt d'elements de B que són enters sobre A s'anomena la clausura entera de A en B.

Si $A = \mathbb{Z}$ i $B = K$ és un cos de nombres, els elements enters s'anomenen enters algebraics, i la clausura entera de A s'anomena l'anell d'enters de K, i es denota per $\mathcal{O}_K$.

Exemple 1.1.3. Un cos quadràtic K és un cos de la forma $K = \mathbb{Q}(\sqrt{N})$, on $N \notin \{0, 1\}$ és un enter lliure de quadrats. Si $N < 0$, diem que K és un cos quadràtic imaginari. Per a un cos quadràtic $K = \mathbb{Q}(\sqrt{N})$, l'anell d'enters és $\mathcal{O}_K = \mathbb{Z}[\omega]$, on

$$\omega := \begin{cases} \sqrt{N}, & \text{si } N \not\equiv 1 \mod 4, \\ \frac{1+\sqrt{N}}{2}, & \text{si } N \equiv 1 \mod 4. \end{cases}$$

De fet, també es té que $\mathcal{O}_K = \mathbb{Z}[\omega_K]$, on

$$d_K := \begin{cases} 4N, & \text{si } N \not\equiv 1 \mod 4, \\ N, & \text{si } N \equiv 1 \mod 4, \end{cases},$$

$$\omega_K := \frac{d_K + \sqrt{d_K}}{2},$$

L'enter d_K s'anomena el discriminant de K. Observem que $\mathbb{Z}[\sqrt{N}] \subseteq \mathcal{O}_K$, però l'altra inclusió no és certa en general. A més, $K = \mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{d_K})$.

En general, els anells d'enters dels cossos de nombres no són dominis de factorització única. Per exemple, l'anell d'enters de $K = \mathbb{Q}(\sqrt{-5})$ és $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, que no és un domini de factorització única: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ són dos descomposicions de 6 en producte d'elements irreductibles, i les dues descomposicions no són equivalents. Tot i així, sí que es compleix una propietat més feble.

Teorema 1.1.4. *Sigui K un cos de nombres. Aleshores, tot ideal no nul $\mathfrak{a}$ de $\mathcal{O}_K$ descompon de manera única en un producte de la forma*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r},$$

on $\mathfrak{p}_1, ..., \mathfrak{p}_r$ són ideals primers no nuls i diferents de $\mathcal{O}_K$ i $e_1, ..., e_r$ són enters positius.
DEMOSTRACIÓ. [7, teorema 2.4.5] □

Més generalment, diem que un domini d'integritat A és íntegrament tancat si és la seva pròpia clausura entera en el seu cos de fraccions. Els dominis d'ideals principals, per exemple, són íntegrament tancats.

Teorema 1.1.5. *Sigui A un domini d'integritat. Aleshores, són equivalents:*

(a) *Tot ideal no nul $\mathfrak{a}$ de A descompon de manera única en un producte de la forma*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r},$$

on $\mathfrak{p}_1, ..., \mathfrak{p}_r$ són ideals primers no nuls i diferents de A i $e_1, ..., e_r$ són enters positius.

(b) *A és noetherià, íntegrament tancat i de dimensió de Krull 1, és a dir, tot ideal de A és finitament generat, A és íntegrament tancat, no és un cos i tot ideal primer no nul és maximal.*

Si se satisfan aquestes propietats, diem que A és un anell de Dedekind.
DEMOSTRACIÓ. [9, capítol 16.3, teorema 15] □

Per tant, els anells dels enters dels cossos de nombres són anells de Dedekind. Aquesta classe d'anells té propietats especialment bones que fan possible l'estudi de la seva aritmètica. Per exemple, un anell de Dedekind és domini de factorització única si, i només si, és un domini d'ideals principals.

De forma semblant a com a (1.1.1) hem donat una versió del teorema fonamental de l'aritmètica per al cos dels nombres racionals en comptes de per a l'anell dels enters, podem fer el mateix amb el teorema 1.1.4 per als cossos de nombres, en comptes dels seus anells d'enters. Però de la mateixa manera que per als anells d'enters d'un cos de nombres K l'hem hagut d'expressar en termes d'ideals, hem de fer el mateix per al cos K. Això ens porta a la següent definició.

Definició 1.1.6. Sigui A un domini d'integritat. Un ideal fraccionari de A és un A-submòdul $\mathfrak{a}$ del cos de fraccions K de A i tal que existeix un element $a \in A \setminus \{0\}$ tal que $a\mathfrak{a} \subseteq A$.

Exemple 1.1.7. Sigui A un domini d'integritat.

- Tot ideal de A és un ideal fraccionari de A. Aquests ideals fraccionaris s'anomenen ideals enters de A.
- $\mathfrak{a} := \alpha A$ amb $\alpha \in K$ és un ideal fraccionari de A. Aquests ideals fraccionaris s'anomenen ideals fraccionaris principals.

Teorema 1.1.8. *Sigui A un anell de Dedekind. Aleshores, el conjunt d'ideals fraccionaris no nuls de A, que denotem per $\mathbf{I}(A)$ (també $\mathbf{I}(K)$ o $\mathbf{I}_K$ quan $A = \mathcal{O}_K$), és un grup abelià lliure respecte del producte de A-submòduls del cos de fraccions K de A. Els ideals primers no nuls de A en formen un sistema de generadors lliures.*

Demostració. [7, teorema 2.4.5] □

En particular, del fet que els ideals primers no nuls de A formin un sistema de generadors lliures d'aquest grup es dedueix l'equivalent de (1.1.1).

Corol·lari 1.1.9. *Sigui K un cos de nombres. Aleshores, tot ideal fraccionari no nul $\mathfrak{a}$ de K descompon de manera única en un producte de la forma*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r},$$

on $\mathfrak{p}_1, ..., \mathfrak{p}_r$ són ideals primers no nuls diferents de $\mathcal{O}_K$ i $e_1, ..., e_r$ són enters no nuls, no necessàriament positius. □

Ens interessa saber quan tenim el mateix resultat en termes d'elements en comptes d'ideals o, equivalentment, quan tots els ideals fraccionaris són principals.

Si A és un anell de Dedekind i K el seu cos de fraccions, el conjunt dels ideals fraccionaris principals, que denotem per $\mathbf{P}(A)$ (també $\mathbf{P}(K)$ o $\mathbf{P}_K$ quan $A = \mathcal{O}_K$ i K és un cos de nombres) forma un subgrup del grup d'ideals fraccionaris de $\mathbf{I}(A)$.

Definició 1.1.10. El grup quocient $\mathbf{I}(A)/\mathbf{P}(A)$ s'anomena grup de classes d'ideals de A, i es denota per $\mathbf{Cl}(A)$.

Un resultat molt important i que no és cert en general (per a anells de Dedekind que no són anells d'enters d'un cos de nombres) és el següent.

Teorema 1.1.11 (Dirichlet)**.** *Si K és un cos de nombres, el grup $\mathbf{Cl}(\mathcal{O}_K)$ és finit.*
Demostració. [7, teorema 4.4.4] □

L'ordre d'aquest grup s'anomena nombre de classes de K i es denota per $h(\mathcal{O}_K)$. Són equivalents:

(a) $\mathcal{O}_K$ és domini de factorització única.

(b) $\mathcal{O}_K$ és domini d'ideals principals.

(c) $\mathbf{P}(\mathcal{O}_K) = \mathbf{I}(\mathcal{O}_K)$.

(d) $\mathbf{Cl}(\mathcal{O}_K)$ és trivial.

(e) $h(\mathcal{O}_K) = 1$.

Així, podem pensar $h(\mathcal{O}_K)$ com una "mesura"de quant falla la factorització única en $\mathcal{O}_K$. Si $h(\mathcal{O}_K) = 1$, aleshores a $\mathcal{O}_K$ tenim factorització única, i com més gran és $h(\mathcal{O}_K)$ més lluny està $\mathcal{O}_K$ de tenir-ne.

En el cas dels cossos quadràtics, el problema que ens plantegem és el següent.

Problema 1.1.12. Per a quins enters $N < 0$ lliures de quadrats tenim que $h(\mathcal{O}_K) = 1$ per a $K = \mathbb{Q}(\sqrt{N})$?

Aquest problema es coneix com el problema del nombre de classes 1, i al capítol 4 en donarem la solució. A la següent secció definirem el grup de classes d'ideals per a una classe més general d'anells, i parlarem més a fons d'aquest problema.

1.2 Ordres de cossos quadràtics

Sigui K un cos de nombres.

Definició 1.2.1. Un ordre de K és un subanell (amb unitat) $\mathcal{O}$ de K que, com a grup abelià, és lliure de dimensió $n := [K : \mathbb{Q}]$. Equivalentment, un ordre de K és un subanell de K que, com a grup abelià, és finitament generat i conté una $\mathbb{Q}$-base de K.

Per exemple, l'anell dels enters algebraics de K, $\mathcal{O}_K$ és un ordre de K. De fet, si $\mathcal{O}$ és un ordre de K, el fet que $\mathcal{O}$ sigui finitament generat implica que tots els elements de $\mathcal{O}$ són enters algebraics. Per tant, $\mathcal{O} \subseteq \mathcal{O}_K$. Per aquesta raó, diem que $\mathcal{O}_K$ és l'ordre màxim (o maximal) de K. A més, $\mathcal{O}$ és un subgrup d'índex finit de $\mathcal{O}_K$, ja que $\mathcal{O}$ i $\mathcal{O}_K$ ón grups abelians lliures de la mateixa dimensió finita.

Definició 1.2.2. S'anomena conductor de $\mathcal{O}$ (o conductor de $\mathcal{O}_K$ en $\mathcal{O}$) a l'índex $f = [\mathcal{O}_K : \mathcal{O}]$ de $\mathcal{O}$ en $\mathcal{O}_K$ com a grups abelians.

Exemple 1.2.3. Sigui $K = \mathbb{Q}(\sqrt{-3})$. $\mathbb{Z}[\sqrt{-3}]$ és un ordre de K de conductor 2, i $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathcal{O}_K$ és un ordre de conductor 1.

Es satisfà $f\mathcal{O}_K \subseteq \mathcal{O}$, i per tant $\mathbb{Z} + f\mathcal{O}_K \subseteq \mathcal{O}$. En general no es satisfà la igualtat, però en el cas dels cossos quadràtics sí.

Proposició 1.2.4. *Siguin K un cos quadràtic. Llavors,*

(a) $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega_K$

(b) *Per a tot enter $f \geq 1$ existeix un únic ordre de conductor f en $\mathcal{O}_K$, que és $\mathcal{O}_{d_K f^2} := \mathbb{Z} \oplus \mathbb{Z} f\omega_K = \mathbb{Z} + f\mathcal{O}_K$, on d_K i ω_K són els nombres definits a l'exemple 1.1.3. L'enter $D = d_K f^2$ s'anomena el discriminant de $\mathcal{O}_{d_K f^2}$.*

Demostració. [1, lema 7.2] □

Observació 1.2.5. Amb les mateixes definicions que a la proposició anterior es compleix que $K = \mathbb{Q}(\sqrt{d_K}) = \mathbb{Q}(\omega_K) = \mathbb{Q}(f\omega_K)$ i $\mathcal{O}_K = \mathcal{O}_{d_K}$.

Observació 1.2.6. Els ordres dels cossos quadràtics estan unívocament determinats pel seu discriminant, que pot ser qualsevol enter no quadrat $D \equiv 0, 1 \mod 4$. Denotem per $\mathcal{O}_D$ l'ordre de discriminant D.

Els ordres d'un cos de nombres no són, en general, anells íntegrament tancats. Per tant, en general no són anells de Dedekind, i no hi ha factorització única dels ideals de l'ordre en ideals primers. Aquest fet fa que la construcció del grup de classes d'ideals d'un ordre $\mathcal{O}$ no sigui tan senzilla com la del grup de classes d'ideals d'un anell de Dedekind. Els ordres dels cossos de nombres són dominis d'integritat, de manera que té la definició 1.1.6 sentit. En aquest cas, diu el següent.

Definició 1.2.7. Siguin K un cos de nombres i $\mathcal{O}$ un ordre de K. Un $\mathcal{O}$-ideal fraccionari de K és un $\mathcal{O}$-submòdul $\mathfrak{a}$ de K no nul i tal que existeix $a \in \mathcal{O} \setminus \{0\}$ tal que $a\mathfrak{a} \subseteq \mathcal{O}$.

A diferència del cas dels anells de Dedekind, en general el conjunt dels $\mathcal{O}$-ideals fraccionaris de K no formen un grup amb el producte de $\mathcal{O}$-submòduls de K, ja que no tot $\mathcal{O}$-ideals fraccionari té un invers. Un $\mathcal{O}$-ideal fraccionari $\mathfrak{a}$ de K s'anomena invertible si existeix un $\mathcal{O}$-ideal fraccionari $\mathfrak{b}$ tal que $\mathfrak{ab} = \mathcal{O}$.

Proposició 1.2.8. *Siguin $\mathcal{O}$ un ordre d'un cos de nombres K i $\mathfrak{a} \subseteq K$ un $\mathcal{O}$-ideal fraccionari. Llavors, l'anell de multiplicadors de $\mathfrak{a}$, $\mathcal{O}(\mathfrak{a}) := \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$, és un ordre de K que conté $\mathcal{O}$ com a subordre. Si $\mathcal{O} = \mathcal{O}(\mathfrak{a})$, es diu que $\mathfrak{a}$ és propi. Si K és un*

cos quadràtic, aleshores $\mathfrak{a}$ *és invertible si, i només si, és propi.*
DEMOSTRACIÓ. [1, proposició 7.4] □

Sigui K un cos quadràtic i $\mathcal{O}$ un ordre de K. Denotem per $\mathbf{I}(\mathcal{O})$ el conjunt dels $\mathcal{O}$-ideals fraccionaris propis de K i per $\mathbf{P}(\mathcal{O})$ el conjunt dels $\mathcal{O}$-ideals fraccionaris principals de K. Amb aquestes definicions, de la proposició anterior es dedueix que $\mathbf{I}(\mathcal{O})$ és un grup commutatiu amb el producte d'ideals fraccionaris. De fet, tot ideal principal és propi, i $\mathbf{P}(\mathcal{O})$ és un subgrup de $\mathbf{I}(\mathcal{O})$.

Definició 1.2.9. El grup $\mathbf{Cl}(\mathcal{O}) := \mathbf{I}(\mathcal{O})/\mathbf{P}(\mathcal{O})$ s'anomena grup de classes d'ideals de $\mathcal{O}$.

En el cas en què $\mathcal{O} = \mathcal{O}_K$, aquesta definició coincideix amb la definició 1.1.10 del grup de classes d'ideals de $\mathcal{O}_K$.

A la secció 1.4 veurem que si K és un cos quadràtic imaginari, aleshores el grup $\mathbf{Cl}(\mathcal{O})$ és finit. Denotem per $h(\mathcal{O})$ l'ordre d'aquest grup. Ens podem plantejar una versió més general del problema del nombre de classes 1.

Problema 1.2.10. Per a quins discriminants $D < 0$ es té $h(\mathcal{O}_D) = 1$?

Al capítol 4 demostrarem que si $D < 0$, aleshores

$$h(\mathcal{O}_D) = 1 \iff D \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

En particular, si K és un cos quadràtic imaginari, aleshores

$$h(\mathcal{O}_K) = 1 \iff d_K = \{-4, -8, -3, -7, -11, -19, -43, -67, -163\}.$$

Cal observar que per als ordres no maximals $\mathcal{O}$ d'un cos quadràtic imaginari K, el fet que el seu nombre de classes sigui 1 no implica que $\mathcal{O}$ sigui un domini principal o factorial. Per exemple, l'ordre $\mathcal{O} = \mathcal{O}_{-12} = \mathbb{Z}[\sqrt{-3}]$ del cos $K = \mathbb{Q}(\sqrt{3})$ no és un domini de factorització única, però $h(\mathcal{O}) = 1$. De fet, els ordres dels cossos de nombres són dominis noetherians i de dimensió 1, de manera que són anells de Dedekind si, i només si, són integrament tancats. A més, si un ordre és un domini d'ideals principals, aleshores és íntegrament tancat, i per tant és un anell de Dedekind. Per tant, tots els ordres no maximals no són principals.

El problema del nombre de classes va ser plantejat inicialment per Gauss l'any 1801 a les *Disquisitiones Arithmeticae*, [5, punts 303, 304 i 305], on va conjecturar el següent:

(a) $h(\mathcal{O}_D) \to \infty$ quan $D \to -\infty$. En particular, per a un enter positiu n, $h(\mathcal{O}_D) = n$ per a un nombre finit de D.

(b) Si D és parell, aleshores $h(\mathcal{O}_D) = 1 \iff -D/4 \in \{1, 2, 3, 4, 7\}$.

(c) $h(\mathcal{O}_D) = 1$ per a infinits $D > 0$.

Les conjectures (a) i (b) han estat demostrades, però (c) encara és un problema obert.

Cal observar que, quan Gauss va conjecturar aquestes propietats, no utilitzava el llenguatge dels ordres de cossos quadràtics ni dels anells d'enters. A continuació veurem una altra descripició del grup de classes que apareix en un context totalment diferent, en què treballava Gauss: l'estudi de les formes quadràtiques enteres.

1.3 Formes quadràtiques binàries enteres

Una forma quadràtica binària entera és un polinomi en dues indeterminades i de la forma $f(X,Y) = aX^2 + bXY + cY^2$ amb $a, b, c \in \mathbb{Z}$. Diem que $f(X,Y)$ és primitiva si a, b i c són relativament primers.

Definició 1.3.1. Diem que dues formes $f(X,Y)$ i $g(X,Y)$ són pròpiament equivalents si existeix $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathbf{SL}(2,\mathbb{Z})$ tal que $f(X,Y) = g(pX+qY, rX+sY)$.

Del fet que $\mathbf{SL}(2,\mathbb{Z})$ és un grup es dedueix que la noció d'equivalència pròpia és una relació d'equivalència. Així, diem que dues formes quadràtiques binàries pertanyen a la mateixa classe si són pròpiament equivalents. Un invariant de les formes que pertanyen a una mateixa classe és el seu discriminant.

Definició 1.3.2. Sigui $f(X,Y) = aX^2+bXY+cY^2$ una forma quadràtica binària entera. Definim el discriminant de $f(X,Y)$ com $D = b^2 - 4ac$.

Si $D < 0$, aleshores $f(X,Y)$ només representa o bé enters positius, o bé enters negatius. En el primer cas, diem que $f(X,Y)$ és definida positiva, i en el segon diem que és definida negativa. Denotem per $\mathbf{Cl}(D)$ el conjunt de classes d'equivalència pròpia de formes primitives definides positives de discriminant D.

Lema 1.3.3. *Siguin $f(X,Y) = aX^2 + bXY + cY^2$ i $g(X,Y) = a'X^2 + b'XY + c'Y^2$ dues formes quadràtiques de discriminant $D < 0$ tals que $mcd(a, a', (b+b')/2) = 1$. Aleshores existeix un enter B únic mòdul $2aa'$ tal que*

$$B \equiv b \mod 2a, \qquad B \equiv b' \mod 2a', \qquad B^2 \equiv D \mod 4aa'.$$

Demostració. [1, lema 3.2] □

Siguin $f(X,Y)$ i $g(X,Y)$ dues formes que compleixen les hipòtesis del lema anterior. Es defineix la composició de $f(X,Y)$ i $g(X,Y)$ com la forma quadràtica

$$F(X,Y) = aa'X^2 + BXY + \frac{B^2 - D}{4aa'}Y^2,$$

on B és l'enter definit al lema anterior i de l'interval $0 \leq B \leq 2aa' - 1$.

Teorema 1.3.4. *Sigui $D \equiv 0, 1 \mod 4$ negatiu. Aleshores la composició de Dirichlet indueix una operació binària ben definida sobre $\mathbf{Cl}(D)$ i que dota $\mathbf{Cl}(D)$ d'estructura de grup abelià finit. Denotem per $h(D)$ l'ordre del grup $\mathbf{Cl}(D)$.*

Demostració. [1, proposició 3.8]. La finitud la veurem a la següent secció. □

El llenguatge i la notació que utilitzem per denotar el grup de classes de les formes quadràtiques enteres d'un discriminant donat ja suggereix una relació amb els grups de classes dels ordres de cossos quadràtics.

Teorema 1.3.5. *Siguin K un cos quadràtic imaginari, $\mathcal{O} \subseteq K$ un ordre de K i $D < 0$ el discriminant de $\mathcal{O}$.*

(a) *Sigui $f(X,Y) = aX^2 + bXY + cY^2$ una forma quadràtica binària entera primitiva definida positiva i de discriminant D. Aleshores, $I(f) := \mathbb{Z}a \oplus \mathbb{Z}\frac{-b+\sqrt{D}}{2}$ és un $\mathcal{O}$-ideal propi de K.*

(b) *L'aplicació I que envia la forma $f(X,Y)$ a l'ideal $I(f)$ indueix un isomorfisme entre el grup $\mathbf{Cl}(D)$ i el grup $\mathbf{Cl}(\mathcal{O})$. En particular, $h(\mathcal{O}) = h(D)$.*

Demostració. [1, teorema 7.7] □

1.4 Alguns resultats sobre el nombre de classes

El fet que tinguem dues descripcions dels grups de classes d'ideals i de formes quadràtiques ens permet utilitzar el llenguatge d'una de les dues per a demostrar coses de l'altra. En aquesta secció, enunciarem algunes propietats elementals de les formes quadràtiques enteres que seran de gran utilitat per a solucionar el problema del nombre de classes 1.

Definició 1.4.1. Diem que una forma quadràtica primitiva $f(X,Y) = aX^2+bXY+cY^2$ és reduïda si $|b| \leq a \leq c$ i, si alguna d'aquestes desigualtats és una igualtat, llavors $b \geq 0$.

Teorema 1.4.2. *Tota forma primitiva i definida positiva és pròpiament equivalent a una única forma reduïda.*

Demostració. Veurem que tota forma primitiva i definida positiva és pròpiament equivalent a una forma reduïda. Sigui $f(X,Y)$ una forma primitiva i definida positiva. Sigui $g(X,Y) = aX^2+bXY+Y^2$ una forma pròpiament equivalent a $f(X,Y)$ tal que $|b|$ sigui el mínim possible. Si $a < |b|$, aleshores, per a tot $m \in \mathbb{Z}$,

$$h(X,Y) = g(X+mY,Y) = aX^2 + (2am+b)XY + c'Y^2$$

és pròpiament equivalent a $g(X,Y)$, de manera que podem escollir m tal que $|2am+b| < |b|$, però havíem escollit $g(X,Y)$ tal que $|b|$ fos mínim. Per tant, hem de tenir que $a \geq |b|$, i amb un argument similar tenim que $c \geq |b|$. Si $a > c$, aleshores $h(X,Y) = g(-Y,X)$ és pròpiament equivalent a $f(X,Y)$, i satisfà $|b| \leq a \leq c$.

Per tant, $f(X,Y)$ és pròpiament equivalent a una forma amb $|b| \leq a \leq c$. Aquesta forma és reduïda excepte si $b < 0$ i, o bé $a = -b$, o bé $a = c$. En aquests casos, la forma $aX^2 - bXY + cY^2$ és reduïda, de manera que si veiem que és pròpiament equivalent a $aX^2 + bXY + cY^2$ haurem acabat.

- Si $a = -b$, aleshores el canvi de variables $(X,Y) \mapsto (X+Y,Y)$ envia la forma $aX^2-bXY+cY^2$ a $aX^2+bXY+cY^2$, de manera que les dues formes són pròpiament equivalents.

- Si $a = c$, aleshores el canvi de variables $(X,Y) \mapsto (-Y,X)$ envia $aX^2+bXY+cY^2$ a $aX^2 - bXY + cY^2$, de manera que les dues formes són pròpiament equivalents.

La demostració de la unicitat es pot trobar a [1, teorema 2.8]. □

Corol·lari 1.4.3. *$h(D)$ és finit per a tot $D < 0$.*

Demostració. Suposem que $f(X,Y) = aX^2 + bXY + cY^2$ és una forma reduïda de discriminant $D < 0$. Aleshores, $b^2 \leq a^2$ i $a \leq c$, de manera que $D = b^2 - 4ac \leq -3a^2$, és a dir, $a \leq \sqrt{-D/3}$. Així, si fixem D, a només pot prendre un nombre finit de valors. Com que $|b| \leq a$, b també pot prendre només un nombre finit de valors, i com que $D = b^2-4ac$, el mateix és cert per a c.

Per tant, només hi ha un nombre finit de formes reduïdes de discriminant D. Pel teorema 1.4.2 hi ha el mateix nombre de formes reduïdes que de classes de $\mathbf{Cl}(D)$, i per tant $\mathbf{Cl}(D)$ ha de ser finit. □

La demostració del corol·lari 1.4.3 ens proporciona un algoritme per calcular el nombre de classes d'un discriminant donat: només cal comptar per a quants a, b, c amb $|b| \leq a \leq \sqrt{-D/3}, c = (b^2 - D)/4a$ es té que $aX^2 + bXY + cY^2$ és una forma reduïda.

A l'apèndix A donem un exemple d'un programa que calcula el nombre de classes d'un discriminant negatiu donat utilitzant aquest algoritme.

A més, a l'apèndix B donem una taula del nombre de classes de discriminants negatius petits en valor absolut, que hem obtingut a partir del programa de l'apèndix A. Aquesta taula ens permet comprovar el següent.

Teorema 1.4.4. *Per a tot* $D \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$*, es té que* $h(D) = 1$*.*

Al capítol 4 veurem que els nombres del teorema 1.4.4 són els únics discriminants negatius de nombre de classes 1. De fet, ja estem en condició de provar la conjectura inicial de Gauss, que va ser demostrada per Landau l'any 1903.

Teorema 1.4.5 (Landau)**.** $h(-4n) = 1 \iff n \in \{1, 2, 3, 4, 7\}$.

Demostració. $X^2 + nY^2$ és una forma reduïda de discriminant $D = -4n$. Per a $n \notin \{1, 2, 3, 4, 7\}$ en construirem una diferent. Podem suposar que $n > 1$.

En primer lloc, suposem que n no és una potència d'un primer. Aleshores podem posar $n = ac$ amb $2 \leq a < c$ i $\mathrm{mcd}(a, c) = 1$, de manera que $aX^2 + cY^2$ és una forma reduïda de discriminant $-4ac = -4n$. Per tant, $h(-4n) > 1$.

Suposem ara que $n = 2^r$. Si $r \geq 4$, llavors la forma

$$4X^2 + 4XY + (2^{r-2} + 1)Y^2$$

és reduïda i de discriminant $4^2 - 4 \cdot 4(2^{r-2} + 1) = -2^{r+2} = -4n$. Si $r \leq 4$, amb la taula de l'apèndix B es pot comprovar que $h(-4n) = h(-4 \cdot 2^r) = 1$ només per a $r = 1, 2$, és a dir, per a $n = 2, 4$.

Suposem finalment que $n = p^r$ amb p primer senar. Si $n + 1$ no és una potència d'un primer, existeixen enters coprimers a, c tals que $n + 1 = ac$ i $2 \leq a < c$. Aleshores,

$$aX^2 + 2XY + cY^2$$

és una forma reduïda de discriminant $2^2 - 4ac = 4 - 4(n+1) = -4n$, i per tant $h(-4n) > 1$.

Si $n + 1$ és una potència d'un primer, com que $n = p^r$ és senar, ha de ser una potència de 2, $n + 1 = 2^s$. Per a $s \geq 6$, la forma

$$8X^2 + 6XY + (2^{s-3} + 1)Y^2$$

és primitiva i reduïda, i el seu discriminant és $6^2 - 4 \cdot 8(2^{s-3}+1) = 4 - 4 \cdot 2^s = 4 - 4(n+1) = -4n$, i per tant $h(-4n) > 1$. Per a $s < 6$, com abans, amb la taula de l'apèndix B podem comprovar que $h(-4n) = h(-4(2^s - 1)) = 1$ només per a $s = 1, 2, 3$, és a dir, per a $n = 1, 3, 7$. □

Proposició 1.4.6. *Sigui* $D < 0$ *un enter senar. Si* $-D$ *no és una potència d'un primer, aleshores* $h(D) > 1$*.*

Demostració. A fi d'estalviar-nos d'explicar la teoria de gèneres de formes quadràtiques enteres, hem fet una demostració independent d'aquesta teoria. Suposem que $-D$ no és una potència d'un primer, i posem $D = -mn$, on m i n són enters coprimers tals que $2 \leq m < n$. Com que D és un discriminant senar, ha de ser $D \equiv 1 \mod 4$. Per tant, $mn = -D \equiv 3 \mod 4$, de manera que tenim dues possiblitats:

- $m \equiv 1 \mod 4$ i $n \equiv 3 \mod 4$, o
- $m \equiv 3 \mod 4$ i $n \equiv 1 \mod 4$.

En els dos casos, $m+n \equiv 0 \mod 4$. Com que, a més, $D \equiv 1 \mod 4$, tenim que els nombres

$$c := \frac{m+n}{4}, \qquad d := \frac{1-D}{4},$$

són enters. Considerem les formes de discriminant D

$$\begin{aligned} f_1(X,Y) &= mX^2 + mXY + cY^2, \\ f_2(X,Y) &= cX^2 + (2c-m)XY + cY^2, \\ g(X,Y) &= X^2 + XY + dY^2. \end{aligned}$$

Clarament, $g(X,Y)$ és reduïda. A més,

- si $m \leq c$, aleshores $f_1(X,Y)$ és reduïda,
- si $m > c$, aleshores $2c-m = c+(c-m) < c$. A més, $2c-m = \frac{m+n}{2} - m = \frac{n-m}{2} > 0$. D'altra banda, $\mathrm{mcd}(2c-m,c) = \mathrm{mcd}(c,m) = \mathrm{mcd}(4c,m) = \mathrm{mcd}(m+n,m) = \mathrm{mcd}(m,n) = 1$. Per tant $f_2(X,Y)$ és reduïda.

Com que $f_1(X,Y) \neq g(X,Y) \neq f_2(X,Y)$, dues d'aquestes tres formes són reduïdes, diferents, i de discriminant D. Per tant, $h(D) \geq 2$. □

1.5 Ideals primers amb el conductor

Al següent capítol aplicarem la teoria de cossos de classes al nostre problema. La teoria de cossos de classes, però, tracta directament només amb els anells d'enters dels cossos de nombres, i no amb els seus ordres. Per a poder aplicar-la, donarem dues noves descripcions dels grup de classes d'un ordre d'un cos quadràtic K en termes de l'ordre màxim $\mathcal{O}_K$.

Definició 1.5.1. Siguin K un cos quadràtic, $\mathcal{O}$ un ordre de K i $\mathfrak{a}$ un $\mathcal{O}$-ideal enter no nul. Sigui f el conductor de $\mathcal{O}$. Es diu que $\mathfrak{a}$ és primer amb f si $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

Denotem per $\mathbf{I}(\mathcal{O},f)$ i $\mathbf{P}(\mathcal{O},f)$ als subgrups de $\mathbf{I}(\mathcal{O})$ i $\mathbf{P}(\mathcal{O})$ generats pels $\mathcal{O}$-ideals enters primers amb f i pels $\mathcal{O}$-ideals principals $\alpha\mathcal{O}, \alpha \in \mathcal{O}\backslash\{0\}$ tals que $\mathrm{mcd}(N(\alpha),f) = 1$ respectivament, on $N(\alpha) := |\mathcal{O}/\alpha\mathcal{O}| = |\alpha|^2$.

Definició 1.5.2. Siguin $m \in \mathbb{Z}$ un nombre enter no nul i $\mathfrak{a}$ un $\mathcal{O}_K$-ideal enter no nul. Es diu que $\mathfrak{a}$ és primer amb m si $\mathfrak{a} + m\mathcal{O}_K = \mathcal{O}_K$.

Denotem per $\mathbf{I}_K(m)$ al subgrup de $\mathbf{I}_K$ generat pels $\mathcal{O}_K$-ideals enters primers amb m. Denotem per $\mathbf{P}_{K,\mathbb{Z}}(f)$ el subgrup de de $\mathbf{I}_K(f)$ generat pels $\mathcal{O}_K$-ideals enters principals de la forma $\alpha\mathcal{O}_K$ on $\alpha \in \mathcal{O}_K, \alpha \equiv a \mod f$ per a un nombre enter a tal que $\mathrm{mcd}(a,f) = 1$.

Teorema 1.5.3. *Existeixen isomorfismes naturals*

$$\mathbf{Cl}(\mathcal{O}) \cong \frac{\mathbf{I}(\mathcal{O},f)}{\mathbf{P}(\mathcal{O},f)} \cong \frac{\mathbf{I}_K(f)}{\mathbf{P}_{K,\mathbb{Z}}(f)}.$$

Demostració. [1, proposició 7.22] □

De la mateixa manera que a la secció anterior hem utilitzat la descripció del grup de classes d'un ordre $\mathcal{O}$ d'un cos quadràtic imaginari K en termes de classes de formes quadràtiques enteres per a obtenir alguns resultats sobre $h(\mathcal{O})$, mitjançant aquestes dues noves descripcions es pot obtenir una relació entre $h(\mathcal{O})$ i $h(\mathcal{O}_K)$.

Teorema 1.5.4. *Siguin K un cos quadràtic imaginari, $\mathcal{O}$ l'ordre d'índex f en $\mathcal{O}_K$ i d_K el discriminant de $\mathcal{O}_K$. Aleshores, $h(\mathcal{O})$ és un múltiple de $h(\mathcal{O}_K)$ i se satisfà que*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right),$$

on $(\frac{d_K}{p})$ és el símbol de Kronecker, que és l'extensió del símbol de Jacobi tal que

$$\left(\frac{n}{2}\right) = \begin{cases} 0, & si\ 2|n, \\ 1, & si\ n \equiv \pm 1 \mod 8, \\ -1, & si\ n \equiv \pm 5 \mod 8. \end{cases}$$

Demostració. [1, teorema 7.24] □

2 Teoria de cossos de classes

La teoria de cossos de classes és una branca de la teoria algebraica de nombres que estudia les extensions abelianes d'alguns cossos, és a dir, aquelles que són de Galois i tenen un grup de Galois abelià. Un exemple d'un resultat clàssic en la teoria de cossos de classes és el teorema de Kronecker-Weber, que, de fet, és part de la motivació que hi ha darrere d'aquesta disciplina, i històricament marca el seu tret de sortida.

Teorema 2.0.1 (Kronecker-Weber)**.** *Sigui K una extensió abeliana de $\mathbb{Q}$. Aleshores existeix $m \in \mathbb{Z}$ tal que $K \subseteq \mathbb{Q}(\zeta_m)$, on $\zeta_m = e^{2\pi i/m}$ és una arrel primitiva de la unitat. En particular, l'extensió abeliana maximal de $\mathbb{Q}$ és el cos composició*

$$\prod_{m=1}^{\infty} \mathbb{Q}(\zeta_m).$$

En aquest capítol donarem una formulació clàssica de la teoria de cossos de classes per a cossos de nombres, enunciant-ne els resultats més importants. El resultat que més ens interessa per al nostre problema és el següent.

Teorema 2.0.2. *Sigui $\mathcal{O}$ un ordre d'un cos quadràtic imaginari K. Aleshores existeix una extensió de Galois $L|K$ tal que $Gal(L|K) \cong \mathbf{Cl}(\mathcal{O})$.*

Tots els resultats que no demostrem es poden trobar a [2] o a [1, capítols 5-9].

2.1 Ramificació

Siguin A un anell de Dedekind, K el seu cos de fraccions, $L|K$ una extensió finita i B la clausura entera de A en L. Aleshores, B és un anell de Dedekind. En particular, si $\mathfrak{p}$ és un ideal enter primer no nul de A, aleshores $\mathfrak{p}B$ és un ideal enter propi no nul de B, de manera que descompon de manera única en un producte de la forma

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

on els $\mathfrak{P}_i$ són els ideals enters primers de B que contenen a $\mathfrak{p}B$. Per a tot i, $\mathfrak{p} = \mathfrak{P}_i \cap A$. Anomenem índex de ramificació de $\mathfrak{P}_i$ sobre $\mathfrak{p}$ a l'enter e_i, i el designem per $e(\mathfrak{P}_i|\mathfrak{p})$.

El cos $A/\mathfrak{p}$ s'anomena cos residual de A en $\mathfrak{p}$, i l'extensió $B|A$ indueix una extensió finita dels cossos residuals $A/\mathfrak{p} \subseteq B/\mathfrak{P}_i$, anomenada extensió residual en $\mathfrak{P}_i$, de grau $f_i := [B/\mathfrak{P}_i : A/\mathfrak{p}] \leq [L : K]$. f_i s'anomena el grau residual en $\mathfrak{P}_i$ de l'extensió $B|A$, i escrivim $f_i := f(\mathfrak{P}_i|\mathfrak{p})$.

Els índexs de ramificació i graus residuals estan relacionats per les propietats següents.

Proposició 2.1.1. *Sigui $S := A \setminus \mathfrak{p}$. Si $L|K$ és separable o $S^{-1}B$ és un $S^{-1}A$-mòdul finitament generat, aleshores*

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Proposició 2.1.2. *Suposem ara que l'extensió $L|K$ és de Galois. Aleshores el grup de Galois $Gal(L|K)$ actua transitivament en el conjunt dels ideals primers $\mathfrak{P}$ de B que divideixen $\mathfrak{p}$. A més, els índexs de ramificació $e = e(\mathfrak{P}|\mathfrak{p})$ i els graus residuals $f = f(\mathfrak{P}|\mathfrak{p})$ no depenen de l'ideal primer $\mathfrak{P}$ de B que divideix a $\mathfrak{p}$. En particular, $efg = [L : K]$.*

A més, es pot comprovar fàcilment la proposició següent.

Proposició 2.1.3. *Sigui A un anell de Dedekind, K el seu cos de fraccions, $K'|K$ i $L|K'$ extensions finites, A' la clausura entera de A en K', B la clausura entera de A' en L, $\mathfrak{P} \subseteq B$ un ideal primer no nul de B, $\mathfrak{P}' := \mathfrak{P} \cap A'$ i $\mathfrak{p} := \mathfrak{P} \cap A$. Aleshores,*

$$\begin{aligned} e(\mathfrak{P}|\mathfrak{p}) &= e(\mathfrak{P}|\mathfrak{P}')e(\mathfrak{P}'|\mathfrak{p}), \\ f(\mathfrak{P}|\mathfrak{p}) &= f(\mathfrak{P}|\mathfrak{P}')f(\mathfrak{P}'|\mathfrak{p}), \\ g(\mathfrak{p}) &= \sum_{\mathfrak{P}' \cap A = \mathfrak{p}} g(\mathfrak{P}'). \end{aligned}$$

Sigui $\mathfrak{P}$ un ideal primer de B i $\mathfrak{p} := \mathfrak{P} \cap A$ la seva contracció a A. Diem que l'extensió $B|A$ és ramificada en $\mathfrak{P}$ quan l'extensió residual en $\mathfrak{P}$ no és separable o $e(\mathfrak{P}|\mathfrak{p}) > 1$, i que és ramificada en $\mathfrak{p}$ quan és ramificada en algun ideal primer de B que divideix $\mathfrak{p}B$. Diem que $\mathfrak{p}$ descompon completament quan $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ per a tot ideal primer $\mathfrak{P}$ de B que divideix $\mathfrak{p}$.

Sigui K un cos de nombres. Anomenem primer infinit real de K a tota $\mathbb{Q}$-immersió $\sigma : K \to \mathbb{R}$, i primer infinit complex de K a tot parell d'immersions conjugades $\sigma, \overline{\sigma} : K \to \mathbb{C}$ amb $\sigma \neq \overline{\sigma}$. En aquest context, diem que els ideals primers de $\mathcal{O}_K$ són primers finits de K. Observem que $\mathbb{Q}$ té un únic primer infinit real.

Donada una extensió $L|K$, diem que un primer infinit de K ramifica en L si és real i té una extensió complexa. Així, diem que una extensió $L|K$ és no ramificada si és no ramificada en tots els primers de K, tant finits com infinits.

El nombre de primers que ramifiquen en una extensió $L|K$ de cossos de nombres és finit. Per exemple, podem resumir la ramificació dels cossos quadràtics de la manera següent.

Teorema 2.1.4. *Sigui K un cos quadràtic. Aleshores,*

(a) *El primer infinit de $\mathbb{Q}$ ramifica en K si, i només si, $d_K < 0$, és a dir, si K és un cos quadràtic imaginari.*

(b) *Un primer finit p de $\mathbb{Q}$ ramifica en K, si i només si $p|d_K$, és a dir, si $(\frac{d_K}{p}) = 0$.*

(c) *Un primer finit p de $\mathbb{Q}$ descompon completament en K, si i només si $(\frac{d_K}{p}) = 1$.*

(d) *Un primer finit p de $\mathbb{Q}$ és primer en K (és a dir, $p\mathcal{O}_K$ és un ideal primer) si, i només si, $(\frac{d_K}{p}) = -1$.*

2.2 Grups generalitzats de classes d'ideals

Definició 2.2.1. Sigui K un cos de nombres. Un mòdul en K és un producte formal de la forma

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$$

sobre tots els primers de K, tant finits com infinits, tal que

(a) $n_\mathfrak{p} \geq 0$, i només un nombre finit de $n_\mathfrak{p}$ són no nuls,

(b) $n_\mathfrak{p} = 0$ per als primers infinits complexos $\mathfrak{p}$,

(c) $n_\mathfrak{p} \leq 1$ per als primers infinits reals $\mathfrak{p}$.

Si tots els $n_\mathfrak{p}$ són zero, posem $\mathfrak{m} = 1$.

Podem escriure un mòdul $\mathfrak{m}$ com $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, on $\mathfrak{m}_0$ és un ideal enter de $\mathcal{O}_K$ i $\mathfrak{m}_\infty$ és un producte de diferents primers infinits reals de K. En particular, si el cos K no admet primers infinits reals (per exemple, si K és quadràtic imaginari), podem considerar un mòdul com un ideal de $\mathcal{O}_K$.

Definició 2.2.2. Donat un mòdul $\mathfrak{m}$, definim $\mathbf{I}_K(\mathfrak{m})$ com el grup dels $\mathcal{O}_K$-ideals coprimers amb $\mathfrak{m}$ (és a dir, coprimers amb $\mathfrak{m}_0$), i $\mathbf{P}_{K,1}(\mathfrak{m})$ com el subrgup de $I_K(\mathfrak{m})$ generat pels ideals principals de la forma $\alpha\mathcal{O}_K$ on $\alpha \in \mathcal{O}_K$ i $\alpha \equiv 1 \mod \mathfrak{m}_0$ i $\sigma(\alpha) > 0$ per a tots els primers infinits reals σ que divideixen $\mathfrak{m}_\infty$.

Proposició 2.2.3. *$\mathbf{P}_{K,1}(\mathfrak{m})$ és d'índex finit en $\mathbf{I}_K(\mathfrak{m})$.*

Definició 2.2.4. Un subgrup $H \subseteq \mathbf{I}_K(\mathfrak{m})$ s'anomena subgrup de congruència per a $\mathfrak{m}$ si se satisfà que $\mathbf{P}_{K,1}(\mathfrak{m}) \subseteq H \subseteq \mathbf{I}_K(\mathfrak{m})$. En aquest cas, es diu que el quocient $\mathbf{I}_K(\mathfrak{m})/H$ és un grup generalitzat de classes d'ideals per a $\mathfrak{m}$.

Veiem-ne alguns exemples.

Exemple 2.2.5. Si prenem el mòdul $\mathfrak{m} = 1$, aleshores $\mathbf{I}_K = \mathbf{I}_K(1)$, i $\mathbf{P}_K = \mathbf{P}_{K,1}(1)$ és un subgrup de congruència, de manera que el grup de classes d'ideals $\mathbf{Cl}(\mathcal{O}_K)$ és un grup generalitzat de classes d'ideals.

Exemple 2.2.6. Sigui $\mathcal{O}$ l'ordre de conductor f d'un cos quadràtic imaginari K. Per la proposició 1.5.3 es té que

$$\mathbf{Cl}(\mathcal{O}) \cong \mathbf{I}_K(f)/\mathbf{P}_{K,\mathbb{Z}}(f),$$

on $\mathbf{P}_{K,\mathbb{Z}}(f)$ està generat pels ideals principals de la forma $\alpha\mathcal{O}_K$ amb $\alpha \equiv a \mod f\mathcal{O}_K, a \in \mathbb{Z}$ i $\mathrm{mcd}(a, f) = 1$. Per al mòdul $\mathfrak{m} = f\mathcal{O}_K$, tenim que

$$\mathbf{P}_{K,1}(f\mathcal{O}_K) \subseteq \mathbf{P}_{K,\mathbb{Z}}(f) \subseteq \mathbf{I}_K(f) = \mathbf{I}_K(f\mathcal{O}_K).$$

Per tant, $\mathbf{P}_{K,\mathbb{Z}}(f)$ és un subgrup de congruència per a $f\mathcal{O}_K$. En particular, $\mathbf{Cl}(\mathcal{O})$ és un grup generalitzat de classes d'ideals de K per al mòdul $f\mathcal{O}_K$.

2.3 El símbol d'Artin

Lema 2.3.1. *Siguin $L|K$ una extensió de Galois finita i $\mathfrak{p}$ un primer finit de $\mathcal{O}_k$ no ramificat en L. Si $\mathfrak{P}$ és un primer de $\mathcal{O}_L$ que divideix $\mathfrak{p}$, aleshores existeix un únic element $\sigma \in Gal(L|K)$ tal que $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{P}$ per a tot $\alpha \in \mathcal{O}_K$.*

Aquest element s'anomena símbol d'Artin o automorfisme de Frobenius, i es denota per $(\frac{L|K}{\mathfrak{P}})$. El símbol d'Artin té les propietats següents.

Proposició 2.3.2. *Sigui $L|K$ una extensió de Galois i no ramificada en un primer $\mathfrak{p}$ de K. Donat un primer $\mathfrak{P}$ de L que divideix a $\mathfrak{p}$, es compleix el següent:*

(a) *Si $\sigma \in Gal(L|K)$, aleshores*

$$\left(\frac{L|K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L|K}{\mathfrak{P}}\right)\sigma^{-1}.$$

(b) *L'ordre de $(\frac{L|K}{\mathfrak{P}})$ és el grau residual $f = f(\mathfrak{P}|\mathfrak{p})$.*

(c) $\mathfrak{p}$ *descompon completament en* L *si, i només si,* $(\frac{L|K}{\mathfrak{P}}) = 1$ *per a tot primer* $\mathfrak{P}$ *que divideix* $\mathfrak{p}B$.

(d) *Si* $L \supseteq L' \supseteq K$ *i* $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{L'}$, *aleshores* $(\frac{L|K}{\mathfrak{P}})_{|L'} = (\frac{L'|K}{\mathfrak{P}'})$.

Amb les mateixes hipòtesis que a la proposició anterior, si l'extensió $L|K$ és abeliana, aleshores $(\frac{L|K}{\sigma(\mathfrak{P})}) = \sigma(\frac{L|K}{\mathfrak{P}})\sigma^{-1} = (\frac{L|K}{\mathfrak{P}})$. Per tant, en aquest cas podem denotar el símbol d'Artin per $(\frac{L|K}{\mathfrak{p}})$, ja que no depèn del primer $\mathfrak{P}$ que divideix $\mathfrak{p}$.

Sigui $\mathfrak{m}$ un mòdul divisible per tots els primers ramificats d'una extensió abeliana $L|K$. Donat un ideal qualsevol $\mathfrak{a}$ primer amb $\mathfrak{m}$, podem expressar $\mathfrak{a}$ com

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

Definim el símbol d'Artin $(\frac{L|K}{\mathfrak{a}})$ com

$$\left(\frac{L|K}{\mathfrak{a}}\right) = \prod_{i=1}^{r} \left(\frac{L|K}{\mathfrak{p}_i}\right)^{e_i}.$$

Així, el símbol d'Artin defineix un morfisme $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L|K)$ anomenat aplicació d'Artin per a $L|K$ i $\mathfrak{m}$. Si cal, escriurem $\Phi_{L|K,\mathfrak{m}}$ en comptes de $\Phi_{\mathfrak{m}}$.

Teorema 2.3.3 (teorema de reciprocitat d'Artin)**.** *Siguin* $L|K$ *una extensió abeliana i* $\mathfrak{m}$ *un mòdul divisible per tots els primers de* K*, tant finits com infinits, que ramifiquen en* L*. Aleshores,*

(a) *L'aplicació d'Artin* $\Phi_{\mathfrak{m}}$ *és exhaustiva.*

(b) *Si els exponents dels primers finits a* $\mathfrak{m}$ *són suficientment grans, aleshores* $\ker(\Phi_{\mathfrak{m}})$ *és un subgrup de congruència per a* $\mathfrak{m}$*. En particular, l'isomorfisme* $I_K(\mathfrak{m})/\ker(\Phi_m) \to Gal(L|K)$ *ens diu que* $Gal(L|K)$ *és un grup de classes d'ideals generalitzat per al mòdul* $\mathfrak{m}$.

Observació 2.3.4. Un problema que podem tenir a l'hora d'aplicar aquest teorema és que el mòdul $\mathfrak{m}$ per al qual $\ker(\Phi_{\mathfrak{m}})$ és un subgrup de congruència no és únic. De fet, si $\ker(\Phi_{\mathfrak{m}})$ és un subgrup de congruència per a $\mathfrak{m}$ i $\mathfrak{m}$ divideix $\mathfrak{n}$ (és a dir, existeix un mòdul $\mathfrak{d}$ tal que $\mathfrak{n} = \mathfrak{d}\mathfrak{m}$), aleshores $\ker(\Phi_{\mathfrak{n}})$ és un subgrup de congruència per a $\mathfrak{n}$.

Teorema 2.3.5 (teorema del conductor)**.** *Sigui* $L|K$ *una extensió abeliana. Aleshores existeix un mòdul* $\mathfrak{f} = \mathfrak{f}(L|K)$ *tal que*

(a) *Un primer de* K*, finit o infinit, ramifica en* L *si, i només si, divideix* $\mathfrak{f}$.

(b) *Sigui* $\mathfrak{m}$ *un mòdul divisible per tots els primers de* K *que ramifiquen en* L*. Aleshores* $\ker(\Phi_m)$ *és un subgrup de congruència per a* $\mathfrak{m}$ *si, i només si,* $\mathfrak{f}|\mathfrak{m}$.

El mòdul $\mathfrak{f}(L|K)$ *s'anomena conductor de l'extensió* $L|K$.

Teorema 2.3.6 (teorema d'existència)**.** *Siguin* $\mathfrak{m}$ *un mòdul de* K *i* H *un subgrup de congruència per a* $\mathfrak{m}$*. Aleshores existeix una única extensió abeliana* L *de* K *tal que tots els primers que hi ramifiquen, finits o infinits, divideixen* $\mathfrak{m}$ *i l'aplicació d'Artin* $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to Gal(L|K)$ *de* $L|K$ *compleix* $H = \ker(\Phi_{\mathfrak{m}})$.

Corol·lari 2.3.7. *Tot grup generalitzat de classes d'ideals és el grup de Galois d'una certa extensió abeliana* $L|K$.

DEMOSTRACIÓ. Si H és un grup generalitat de classes d'ideals, i L és la extensió donada pel teorema d'existència, aleshores $\mathrm{Gal}(L|K) \cong I_K(\mathfrak{m})/H$. □

Exemple 2.3.8. Siguin $\mathfrak{m} = 1$ i $P_K = P_{K,1}(\mathfrak{m}) \subseteq I_K$. El teorema d'existència afirma que existeix una única extensió abeliana L de K no ramificada (ja que $\mathfrak{m} = 1$) tal que l'aplicació d'Artin indueix un isomorfisme $\mathbf{Cl}(\mathcal{O}_K) = \mathbf{I}_K/\mathbf{P}_K \cong \mathrm{Gal}(L|K)$. L s'anomena el cos de classes de Hilbert de K, i és la màxima extensió abeliana no ramificada de K.

Exemple 2.3.9. Sigui $\mathcal{O}$ l'ordre de conductor f d'un cos quadràtic imaginari K. Com hem vist a l'exemple 2.2.6, el grup de classes de $\mathcal{O}$, $\mathbf{Cl}(\mathcal{O})$, és un grup de classes generalitzat. Així, el teorema d'existència ens diu que existeix una única extensió abeliana $L|K$ no ramificada en els primers que no divideixen $f\mathcal{O}_K$ tal que $\mathrm{Gal}(L|K) \cong \mathbf{Cl}(\mathcal{O})$. Això demostra el teorema 2.0.2.

L s'anomena el cos de classes de l'ordre $\mathcal{O}$. Quan $f = 1$, aleshores el cos de classes de l'ordre $\mathcal{O} = \mathcal{O}_K$ és el cos de classes de Hilbert de K. El teorema d'existència, però, no és constructiu, de manera que no sabem obtenir de manera explícita el cos de classes d'un ordre d'un cos quadràtic imaginari.

Del teorema d'existència podem recuperar el teorema de Kronecker-Weber.

Teorema 2.0.1 (Kronecker-Weber)**.** *Sigui K una extensió abeliana de $\mathbb{Q}$. Aleshores existeix $m \in \mathbb{Z}$ tal que $K \subseteq \mathbb{Q}(\zeta_m)$, on $\zeta_m = e^{2\pi i/m}$ és una arrel primitiva de la unitat. En particular, l'extensió abeliana maximal de $\mathbb{Q}$ és el cos composició*

$$\prod_{m=1}^{\infty} \mathbb{Q}(\zeta_m).$$

DEMOSTRACIÓ. Siguin $\zeta_m = e^{2\pi i/m}$ i $\mathfrak{m} = m\infty$, on ∞ denota el primer infinit real de $\mathbb{Q}$. Els primers que ramifiquen a $\mathbb{Q}(\zeta_m)$ són aquells que divideixen m. Així, l'aplicació d'Artin

$$\Phi_{\mathfrak{m}} : \mathbf{I}_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)|\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$$

està ben definida. De fet, si $\frac{a}{b}\mathbb{Z} \in \mathbf{I}_{\mathbb{Q}}(\mathfrak{m})$ amb $\frac{a}{b} > 0$ i $\mathrm{mcd}(a, m) = \mathrm{mcd}(b, m) = 1$, aleshores

$$\Phi_{\mathfrak{m}}\left(\frac{a}{b}\mathbb{Z}\right) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*,$$

de manera que $\ker(\Phi_m) = \mathbf{P}_{\mathbb{Q},1}(\mathfrak{m})$.

Sigui K una extensió abeliana de $\mathbb{Q}$. Aleshores, pel teorema de reciprocitat d'Artin, existeix un mòdul $\mathfrak{m}$ tal que $\mathbf{P}_{\mathbb{Q},1}(\mathfrak{m}) \subseteq \ker(\Phi_{K|\mathbb{Q}})$. Si el primer infinit de $\mathbb{Q}$, ∞, no divideix $\mathfrak{m} = m$, com que $m|m\infty$, podem suposar que $\mathfrak{m} = m\infty$. Així, tenim que

$$\mathbf{P}_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)|\mathbb{Q},\mathfrak{m}}) \subseteq \ker(\Phi_{K|\mathbb{Q},\mathfrak{m}}).$$

Utilitzarem el lema següent, que és conseqüència del teorema d'existència.

Lema 2.3.10. *Siguin L i M extensions abelianes d'un cos K. Aleshores, $L \subseteq M$ si, i només si, existeix un mòdul $\mathfrak{m}$ divisible per tots els primers de K que ramifiquen en L o en M i tal que*

$$\mathbf{P}_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{M|K,\mathfrak{m}}) \subseteq \ker(\Phi_{L|K,\mathfrak{m}}).$$

Així, pel lema, tenim que $K \subseteq \mathbb{Q}(\zeta_m)$. □

2.4 Teorema de densitat de Txebotarev

Siguin K un cos de nombres i $\mathcal{P}_K$ el conjunt dels primers finits de K.

Donat dos subconjunts $\mathcal{S}, \mathcal{T} \subseteq \mathcal{P}_K$, si existeix un conjunt finit Σ tal que $\mathcal{S} \subseteq \mathcal{T} \cup \Sigma$, aleshores diem que $\mathcal{S}$ és quasicontingut en $\mathcal{T}$, i escribim $\mathcal{S} \subsetneq \mathcal{T}$ o $\mathcal{T} \supsetneq \mathcal{S}$. Si $\mathcal{S} \subsetneq \mathcal{T}$ i $\mathcal{T} \subsetneq \mathcal{S}$, aleshores diem que $\mathcal{S}$ i $\mathcal{T}$ són quasi iguals, i escrivim $\mathcal{S} \approx \mathcal{T}$.

Donat un subconjunt $\mathcal{S} \subseteq \mathcal{P}_K$, es defineix la densitat de Dirichlet de $\mathcal{S}$ com el límit

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

si aquest existeix. Les propietats bàsiques de la densitat de Dirichlet són les següents:

(a) $\delta(\mathcal{P}_K) = 1$.

(b) Si $\mathcal{S} \subseteq \mathcal{T}$ i $\delta(\mathcal{S})$ i $\delta(\mathcal{T})$ existeixen, aleshores $\delta(\mathcal{S}) \leq \delta(\mathcal{T})$.

(c) Si $\delta(\mathcal{S})$ existeix, aleshores $0 \leq \delta(\mathcal{S}) \leq 1$.

(d) Si $\mathcal{S}$ i $\mathcal{T}$ són disjunts i $\delta(\mathcal{S})$ i $\delta(\mathcal{T})$ existeixen, aleshores $\delta(\mathcal{S} \cup \mathcal{T}) = \delta(\mathcal{S}) + \delta(\mathcal{T})$.

(e) Si $\mathcal{S}$ és finit, aleshores $\delta(\mathcal{S}) = 0$.

(f) Si $\delta(\mathcal{S})$ existeix i $\mathcal{T} \approx \mathcal{S}$, aleshores $\delta(\mathcal{T})$ existeix i $\delta(\mathcal{T}) = \delta(\mathcal{S})$.

Sigui $L|K$ una extensió de Galois no necessàriament abeliana, i sigui $\mathfrak{p}$ un primer de K no ramificat en L. Els primers $\mathfrak{P}$ de L que contenen a $\mathfrak{p}$ formen una classe de conjugació del grup $\mathrm{Gal}(L|K)$, que anomenarem símbol d'Artin de $\mathfrak{p}$ i denotarem per $(\frac{L|K}{\mathfrak{p}})$.

Teorema 2.4.1 (teorema de densitat de Txebotarev)**.** *Siguin $L|K$ una extensió de Galois no necessàriament abeliana i $\langle\sigma\rangle$ la classe de conjugació d'un element $\sigma \in Gal(L|K)$. Aleshores, el conjunt*

$$\mathcal{S} = \left\{ \mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ és no ramificat en } L \text{ i } \left(\frac{L|K}{\mathfrak{p}}\right) = \langle\sigma\rangle \right\}$$

té densitat de Dirichlet

$$\delta(\mathcal{S}) = \frac{|\langle\sigma\rangle|}{|Gal(L|K)|} = \frac{|\langle\sigma\rangle|}{[L:K]}.$$

En particular, $\mathcal{S}$ és infinit.

En el cas en que l'extensió és abeliana, $\langle\sigma\rangle = \{\sigma\}$, de manera que tenim el següent.

Corol·lari 2.4.2. *Siguin L una extensió abeliana de K i $\mathfrak{m}$ un mòdul divisible per tots els primers ramificats en L. Aleshores, per a tot element $\sigma \in Gal(L|K)$ el conjunt de primers $\mathfrak{p}$ que no divideixen $\mathfrak{m}$ i tals que $(\frac{L|K}{\mathfrak{p}}) = \sigma$ té densitat de Dirichlet $1/[L:K]$ i, en particular, és infinit.*

Podem pensar en el teorema de densitat de Txebotarev com una generalització del teorema de Dirichlet dels primers en progressió aritmètica.

Corol·lari 2.4.3 (teorema de Dirichlet dels primers en progressió aritmètica)**.** *Siguin $m > 1$ i a enters coprimers. Aleshores, el conjunt de primers p tals que $p \equiv a \mod m$ té densitat de Dirichlet $1/\varphi(m)$.*

Demostració. Sigui ζ_m una arrel m-èssima primitiva de la unitat. Considerem l'extensió de cossos $\mathbb{Q}(\zeta_m)|\mathbb{Q}$. Tenim un isomorfisme $\Phi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)|\mathbb{Q})$ que envia $\overline{b}$ al $\mathbb{Q}$-automorfisme que envia ζ_m a ζ_m^b.

Els primers que ramifiquen en aquesta extensió són aquells que divideixen m. Veiem que, per a tot primer p que no divideix m es té $(\frac{L|K}{p}) = \Phi(\overline{p})$, on $\overline{p}$ denota la classe de p mòdul m. En efecte, per a tot $\alpha \in \mathbb{Q}(\zeta_m)$, posant $\alpha = a_0 + a_1\zeta_m + \cdots + a_{\varphi(m)}\zeta_m^{-1}$, tenim que $\Phi(\overline{p})(\alpha) = a_0 + a_1\zeta_m^p + \cdots + a_{\varphi(m)}\zeta_m^{-p} \equiv \alpha^p \mod p$.

Així, el conjunt de primers p tals que $p \equiv a \mod m$ és el conjunt de primers no ramificats amb $(\frac{L|K}{p}) = \Phi(\overline{p}) = \Phi(\overline{a})$, i pel corol·lari 2.4.2 aquest conjunt té densitat de Dirichlet $1/[L : K] = 1/\varphi(m)$. □

Una altra conseqüència important del teorema de densitat de Txebotarev és que els primers de K que descomponen completament en una extensió finita $L|K$ determinen unívocament el cos L. Donada una extensió finita $L|K$, definim

$$\mathcal{S}_{L|K} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ descompon totalment en } L\}.$$

Proposició 2.4.4. *Siguin L i M extensions finites de K. Aleshores,*

(a) *Si $M|K$ és de Galois, aleshores $L \subseteq M \iff \mathcal{S}_{M|K} \subsetneq \mathcal{S}_{L|K}$.*

(b) *Si $L|K$ és de Galois, aleshores $L \subseteq M \iff \tilde{\mathcal{S}}_{M|K} \subsetneq \mathcal{S}_{L|K}$, on*

$$\tilde{\mathcal{S}}_{M|K} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ és no ramificat en } M \text{ i } f(\mathfrak{P}|\mathfrak{p}) = 1 \text{ per a algun primer } \mathfrak{P} \text{ de } M \text{ que divideix } \mathfrak{p}\}$$

Demostració. Comencem veient (b). La proposició 2.1.3 ens diu que la implicació cap a la dreta és certa. Recíprocament, suposem que $\tilde{\mathcal{S}}_{M|K} \subsetneq \mathcal{S}_{L|K}$. Sigui N una extensió de Galois de K que contingui a L i a M. Si veiem que $\mathrm{Gal}(N|M) \subseteq \mathrm{Gal}(N|L)$, aleshores tindrem que $L \subseteq M$. Així, sigui $\sigma \in \mathrm{Gal}(N|M)$, i veiem que $\sigma_{|L}$ és la identitat.

Pel teorema de densitat de Txebotarev, existeixen infinits primers $\mathfrak{p}$ de K no ramificats en N tals que $(\frac{N|K}{\mathfrak{p}}) = \langle\sigma\rangle$, i per tant existeixen primers $\mathfrak{P}$ de N amb $(\frac{N|K}{\mathfrak{P}}) = \sigma$ i tals que $\mathfrak{P}$ divideix $\mathfrak{p}$.

Fixem un d'aquests primers, $\mathfrak{p}$, i veiem que $\mathfrak{p} \in \tilde{\mathcal{S}}_{M|K}$. Sigui $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_M$. Aleshores, per a tot $\alpha \in \mathcal{O}_M$ tenim que

$$\alpha = \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{P}'.$$

Per tant, $\mathcal{O}_M/\mathfrak{P}' \cong \mathcal{O}_K/\mathfrak{p}$, de manera que $f(\mathfrak{P}'|\mathfrak{p}) = 1$. Per tant, $\mathfrak{p} \in \tilde{\mathcal{S}}_{M|K}$.

Com que estem considerant infinits $\mathfrak{p}$ i estem suposant que $\tilde{\mathcal{S}}_{M|K} \subsetneq \mathcal{S}_{L|K}$, ha d'existir algun $\mathfrak{p}$ tal que $\mathfrak{p} \in \mathcal{S}_{L|K}$. Per tant, $(\frac{L|K}{\mathfrak{p}}) = 1$, i aleshores tenim que $\sigma_{|L} = (\frac{N|K}{\mathfrak{P}})_{|L} = (\frac{L|K}{\mathfrak{p}}) = 1$, com volíem veure.

Veiem (a). Com abans, la implicació cap a la dreta és conseqüència de la proposició 2.1.3. Recíprocament, suposem que $\mathcal{S}_{M|K} \subsetneq \mathcal{S}_{L|K}$. Sigui L' la clausura de Galois de L sobre K. Un primer de K descompon completament en L si, i només si, descompon completament en L'. Per tant, $\mathcal{S}_{L|K} = \mathcal{S}_{L'|K}$. Com que M és de Galois, aleshores $\tilde{\mathcal{S}}_{M|K} = \mathcal{S}_{M|K}$, de manera que tenim que $\tilde{\mathcal{S}}_{M|K} \subsetneq \mathcal{S}_{L'|K}$. Per (b), tenim que $L' \subseteq M$, de manera que $L \subseteq M$. □

Teorema 2.4.5. *Siguin L i M extensions de Galois de K. Aleshores,*

(a) $L \subseteq M \iff \mathcal{S}_{M|K} \subsetneq \mathcal{S}_{L|K}$

(b) $L = M \iff \mathcal{S}_{M|K} \eqsim \mathcal{S}_{L|K}$

DEMOSTRACIÓ. (a) és cert per l'apartat (a) de la proposició anterior, i (b) és una conseqüència de (a). □

Donada una extensió de cossos, en general és difícil determinar, llevat d'un nombre finit, quins primers descomponen completament. Tot i això, en alguns casos sí que podem donar-ne una descripció. Un exemple és el cas del cos de classes d'un ordre d'un cos quadràtic imaginari.

Teorema 2.4.6. *Sigui $\mathcal{O}$ un ordre d'un cos quadràtic imaginari, i $N(\alpha) = |\mathcal{O}/\alpha\mathcal{O}|$. Aleshores,*

$$\mathcal{S}_{L|\mathbb{Q}} \eqsim \{p \text{ primer } : p = N(\alpha) \text{ per a algun } \alpha \in \mathcal{O}\}.$$

3 Corbes el·líptiques amb multiplicació complexa

Al capítol anterior hem vist que per a tot ordre $\mathcal{O}$ d'un cos quadràtic imaginari K existeix un cos L, anomenat el cos de classes de $\mathcal{O}$, que conté K i tal que $\mathrm{Gal}(L|K) \cong \mathbf{Cl}(\mathcal{O})$. En aquest capítol descriurem com trobar L de forma explícita a través d'un invariant de les classes d'equivalència de $\mathcal{O}$-ideals fraccionaris propis, anomenat invariant j. El teorema principal d'aquest capítol és el següent:

Teorema 3.0.1. *Siguin $\mathcal{O}$ un ordre en un cos quadràtic imaginari K i $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionari propi. Aleshores, l'invariant j de $\mathfrak{a}$, és un enter algebraic de grau $h(\mathcal{O})$ i $K(j(\mathfrak{a}))$ és el cos de classes de l'ordre $\mathcal{O}$.*

Per a demostrar-lo, estudiarem algunes propietats de les xarxes de $\mathbb{C}$ i de les corbes el·líptiques complexes, així com les propietats analítiques de l'invariant j. Finalment, introduirem noves funcions per a fer viable el càlcul dels invariants j.

Tots els resultats que no demostrem en aquest capítol es poden trobar a [1, capítols 10, 11, 12] o a [3].

3.1 Xarxes i corbes el·líptiques

Una xarxa de $\mathbb{C}$ és un subgrup additiu L de $\mathbb{C}$ que està generat per dos nombres complexos ω_1, ω_2 linealment independents sobre $\mathbb{R}$. Escriurem $L = [\omega_1, \omega_2]$. També diem que $\mathbb{C}/L$ és la corba el·líptica generada per w_1 i w_2.

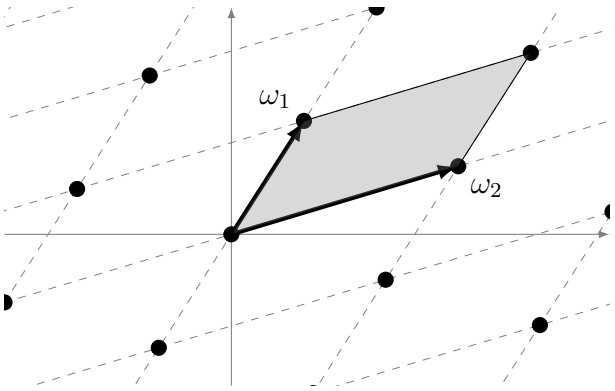

Figura 1: Una xarxa $L = [\omega_1, \omega_2]$.

Exemple 3.1.1. Sigui K un cos quadràtic imaginari i $\mathcal{O}$ l'ordre de K de conductor f. Aleshores, $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z} f\omega_k$ és una xarxa, $\mathcal{O} = [1, f\omega_K]$. De fet, si $\mathfrak{a}$ és un $\mathcal{O}$-ideal fraccionari, aleshores $\mathfrak{a}$ també és una xarxa.

$\mathbb{C}/L$ és una varietat analítica complexa de dimensió 1. També és un grup, i les operacions de grup són holomorfes. Diem que $\mathbb{C}/L$ és un grup de Lie complex. Com que, com a varietat analítica, és de gènere 1, diem que $\mathbb{C}/L$ és un tor complex.

Definició 3.1.2. Una funció el·líptica per a una xarxa L és una funció $f(z)$ meromorfa a $\mathbb{C}$ tal que $f(z + w) = f(z)$ per a tot $w \in L$.

Per tant, si $L = [w_1, w_2]$, aleshores una funció meromorfa $f(z)$ és el·líptica per a L si, i només si, $f(z + w_1) = f(z + w_2) = f(z)$, és a dir, si és doblement periòdica de períodes

ω_1, ω_2. D'altra banda, també podem pensar en les funcions el·líptiques per a L com les funcions meromorfes del tor complex $\mathbb{C}/L$. Hi ha una funció el·líptica per a L que ens interessa especialment.

Definició 3.1.3. Donada una xarxa L i $z \in \mathbb{C}$, definim la funció $\wp$ de Weierstrass per a la xarxa L per

$$\wp(z; L) = \frac{1}{z^2} + \sum_{w \in L \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Si fixem la xarxa L, escriurem $\wp(z)$ en comptes de $\wp(z; L)$.

Les propietats principals de la funció $\wp$ de Weierstrass són les següents.

Teorema 3.1.4. *Sigui L una xarxa.*

(a) *La sèrie $\wp(z)$ és absolutament convergent a $\mathbb{C} \setminus L$ i uniformement convergent en els compactes de $\mathbb{C} \setminus L$.*

(b) *$\wp(z)$ és una funció el·líptica parella per a L, i les seves singularitats són pols dobles als punts de L.*

(c) *La funció derivada de $\wp(z)$, $\wp'(z)$, també és una funció el·líptica per a L, i és una funció senar. A més,*

$$\wp'(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}.$$

(d) *Les funcions el·líptiques per a L formen un cos, que és $\mathbb{C}(\wp(z), \wp'(z))$. A més, les funcions el·líptiques parelles per a L en formen un subcòs, que és el cos $\mathbb{C}(\wp(z))$.*

(e) *Sigui $r > 2$. Les sèries $G_r(L) := \sum_{w \in L \setminus \{0\}} \frac{1}{w^r}$ són convergents, i en un entorn de l'origen se satisfà que*

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geq 1} (2n+1) G_{2n+2}(L) z^{2n}.$$

A més, els coeficients $(2n+1)G_{2n+2}(L)$ són polinomis de coeficients racionals en $G_4(L)$ i $G_6(L)$ i que no depenen de L.

(f) *$\wp(z)$ satisfà l'equació diferencial $\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$, on*

$$g_2(L) = 60 G_4(L) = 60 \sum_{w \in L \setminus \{0\}} \frac{1}{w^4},$$

$$g_3(L) = 140 G_6(L) = 140 \sum_{w \in L \setminus \{0\}} \frac{1}{w^6}.$$

(g) *Si $z, w \notin L$ són nombres complexos diferents i $z + w \notin L$, aleshores se satisfà que*

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4} \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2.$$

(h) *Si $z \notin L$ i $2z \notin L$, aleshores*

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2.$$

(i) *Si $z \notin L$, aleshores $\wp'(z) = 0$ si, i només si, $2z \in L$.*

Observació 3.1.5. Sigui $\mathbb{C}/L$ una corba el·líptica, i sigui E la corba del pla projectiu complex $\mathbb{P}^2_{\mathbb{C}}$ definida per l'equació

$$y^2z = 4x^3 - g_2(L)xz^2 - g_3(L)z^3.$$

E és una subvarietat analítica de $\mathbb{P}^2_{\mathbb{C}}$, i l'aplicació $\phi : \mathbb{C}/L \to E \subseteq \mathbb{P}^2_{\mathbb{C}}$ definida per $\phi(z) = (\wp(z) : \wp'(z) : 1)$ defineix un isomorfisme de varietats analítiques.

Per tant, la corba el·líptica $\mathbb{C}/L$, és una corba plana projectiva. A més, els punts (g) i (h) del teorema 3.1.4 donen equacions algebraiques per a la suma de punts de E. Per tant, una corba el·líptica té una estructura de grup compatible amb la seva estructura de varietat algebraica. En altres paraules, una corba el·líptica és una varietat abeliana.

3.2 Homotècies de xarxes, endomorfismes i multiplicació complexa

Siguin L i L' xarxes de $\mathbb{C}$. Diem que una aplicació $f : \mathbb{C}/L \to \mathbb{C}/L'$ és un morfisme de corbes el·líptiques si és un morfisme de grups de Lie complexos, és a dir, si és una aplicació holomorfa que és morfisme de grups.

Proposició 3.2.1. *Siguin L i L' xarxes de $\mathbb{C}$, $\pi_L : \mathbb{C} \to \mathbb{C}/L$ i $\pi_{L'} : \mathbb{C} \to \mathbb{C}/L'$ les projeccions canòniques, i $f : \mathbb{C}/L' \to \mathbb{C}/L$ un morfisme de corbes el·líptiques. Aleshores, existeix $\lambda \in \mathbb{C}$ tal que $\lambda L' \subseteq L$ i $f(\pi_{L'}(z)) = \pi_L(\lambda z)$.*

En particular, dues corbes el·líptiques $\mathbb{C}/L$ i $\mathbb{C}/L'$ són isomorfes si, i només si, existeix $\lambda \in \mathbb{C} \setminus \{0\}$ tal que $L = \lambda L'$. Si passa això, diem que les xarxes L, L' són homotètiques.

Si L, L' són homotètiques, $L' = \lambda L$, i f és una funció el·líptica per a L, aleshores $g(z) = f(\lambda z)$ és una funció el·líptica per a L'. A més, $\wp(\lambda z; L') = \lambda^{-2}\wp(z; L)$ i $\wp'(\lambda z; L') = \lambda^{-3}\wp'(z; L)$.

Observació 3.2.2. Si $L = [\omega_1, \omega_2] \subseteq \mathbb{C}$ és una xarxa, aleshores L és homotètica a les xarxes $L' = [1, \omega_2/\omega_1]$ i $L'' = [1, \omega_1/\omega_2]$. Com que o bé $\mathrm{Im}(\omega_2/\omega_1) > 0$ o bé $\mathrm{Im}(\omega_1/\omega_2) > 0$, tenim que tota xarxa és homotètica a una xarxa de la forma $[1, \tau]$ amb $\mathrm{Im}(\tau) > 0$.

Ens interessa estudiar els endomorfismes de les corbes el·líptiques.

Exemple 3.2.3. Veiem alguns exemples d'endomorfismes de corbes el·líptiques.

(a) Si L és una xarxa i n és un enter no nul, aleshores $nL \subseteq L$, de manera que la funció $f(z) = nz$ indueix un endomorfisme $\tilde{f} : \mathbb{C}/L \to \mathbb{C}/L$.

(b) Sigui $L = [1, i]$. Aleshores, $iL \subseteq L$, de manera que, per a la funció $f(z) = iz$, l'aplicació $\pi_L \circ f : \mathbb{C} \to \mathbb{C}/L$ també indueix un endomorfisme $\tilde{f} : \mathbb{C}/L \to \mathbb{C}/L$.

Fixem una xarxa L. Utilitzant la fórmula de duplicació per a la funció $\wp$ i l'equació diferencial entre $\wp$ i $\wp'$, obtenim que

$$\wp(2z) = -2\wp(z) + \frac{(12\wp(z)^2 - g_2(L))^2}{16(4\wp(z)^3 - g_2(L)\wp(z) - g_3(L))}.$$

Per tant, $\wp(2z)$ és una funció racional de $\wp(z)$. Utilitzant la fórmula de la suma per a $\wp$, obtenim per inducció que $\wp(nz)$ és una funció racional de $\wp(z)$ per a tot $n \in \mathbb{Z}, n \geq 1$. El següent teorema ens dóna una caracterització de quins $\alpha \in \mathbb{C}$ compleixen que $\wp(az)$ és una funció racional de $\wp(z)$.

Teorema 3.2.4. *Sigui $L \subseteq \mathbb{C}$ una xarxa i $\alpha \in \mathbb{C} \setminus \mathbb{Z}$. Són equivalents*

(a) *$\wp(\alpha z)$ és una funció racional de $\wp(z)$.*

(b) *$\alpha L \subseteq L$.*

(c) *Existeix un ordre $\mathcal{O}$ en un cos quadràtic imaginari K tal que $\alpha \in \mathcal{O}$ i L és una xarxa homotètica a un $\mathcal{O}$-ideal fraccionari propi de K.*

En aquest cas, existeixen polinomis $A(X)$ i $B(X)$ de coeficients a $\mathbb{C}$ tals que

$$\wp(z) = \frac{A(\wp(z))}{B(\wp(z))},$$

i $\deg(A(X)) = \deg(B(X)) + 1 = [L : \alpha L] = N(\alpha)$.

Definició 3.2.5. Donada una xarxa L, l'anell de multiplicació complexa de L és $\mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$. Si $\mathcal{O}(L) \neq \mathbb{Z}$, aleshores diem que la xarxa L (o la corba el·líptica $\mathbb{C}/L$) té multiplicació complexa per $\mathcal{O}(L)$.

Així, el teorema 3.2.4 ens diu que l'anell de multiplicació complexa d'una xarxa L, o equivalentment, l'anell d'endomorfismes de la corba el·líptica $\mathbb{C}/L$ és, o bé $\mathbb{Z}$, o bé un ordre $\mathcal{O} \subseteq K$ d'un cos quadràtic imaginari K.

Sigui $\mathcal{O}$ un ordre d'un cos quadràtic imaginari. Tota xarxa $L \subseteq \mathbb{C}$ que té $\mathcal{O}$ com a anell de multiplicació complexa és homotètica a un $\mathcal{O}$-ideal fraccionari propi, i, recíprocament, tot $\mathcal{O}$-ideal fraccionari propi és una xarxa que té $\mathcal{O}$ com a anell de multiplicació complexa. A més, dos $\mathcal{O}$-ideals fraccionaris pertanyen a la mateixa classe de $\mathbf{Cl}(\mathcal{O})$ si, i només si, són homotètics com a xarxes. Per tant, hem demostrat el següent:

Corol·lari 3.2.6. *Sigui K un cos quadràtic imaginari i $\mathcal{O}$ un ordre de K. Aleshores existeix una correspondència bijectiva entre el grup de classes d'ideals $\mathbf{Cl}(\mathcal{O})$ i el conjunt de classes d'homotècia de xarxes que tenen $\mathcal{O}$ com a anell complet de multiplicació complexa, i també amb el conjunt les classes d'isomorfisme de corbes el·líptiques que tenen $\mathcal{O}$ com a anell d'endomorfismes.*

Per tant, ens interessa poder determinar quan dues xarxes són homotètiques i classificar les classes d'homotècia.

Proposició 3.2.7. *Donada una xarxa $L \subseteq \mathbb{C}$, sigui $\Delta(L) := g_2(L)^3 - 27g_3(L)^2$. Llavors, $\Delta(L) \neq 0$.*

Definició 3.2.8. Donada una xarxa $L \subseteq \mathbb{C}$, definim l'invariant j de L (o de $\mathbb{C}/L$) com

$$j(L) := 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = 1728\frac{g_2(L)^3}{\Delta(L)}.$$

Per la proposició 3.2.7, $\Delta(L) \neq 0$, de manera que l'invariant j està definit per a tota xarxa L. Pot semblar estrany el 1728 que apareix a la definició de l'invariant j, però més endavant veurem per què és important que hi sigui.

Teorema 3.2.9. *Dues xarxes L i L' són homotètiques si, i només si, $j(L) = j(L')$.*

DEMOSTRACIÓ. Si $L' = \lambda L$ per a $\lambda \neq 0$, aleshores

$$g_2(L') = g_2(\lambda L) = \lambda^{-4} g_2(L),$$

$$g_3(L') = g_3(\lambda L) = \lambda^{-6} g_3(L).$$

En particular,

$$\Delta(L') = g_2(L')^3 - 27 g_3(L')^2 = \lambda^{-12} g_2(L)^3 - 27\lambda^{-12} g_3(L)^2 = \lambda^{-12}\Delta(L),$$

i per tant,

$$j(L') = \frac{g_2(L')^3}{\Delta(L')} = \frac{\lambda^{-12} g_2(L)^3}{\lambda^{-12}\Delta(L)} = \frac{g_2(L)^3}{\Delta(L)} = j(L).$$

Veiem el recíproc. Suposem que $j(L) = j(L')$ i veiem que existeix $\lambda \in \mathbb{C}$ tal que

$$\begin{aligned} g_2(L') &= \lambda^{-4} g_2(L), \\ g_3(L') &= \lambda^{-6} g_3(L). \end{aligned} \tag{3.2.10}$$

Comencem suposant que $g_2(L')$ i $g_3(L')$ no són nuls. Sigui λ un nombre complex tal que

$$\lambda^4 = \frac{g_2(L)}{g_2(L')}.$$

De la definició de $j(L)$ obtenim que

$$g_3(L)^2 = \frac{g_2(L)^3}{27}\left(1 - \frac{1728}{j(L)}\right).$$

Com que $j(L) = j(L')$, tenim que

$$\left(\frac{g_3(L)}{g_3(L')}\right)^2 = \frac{\frac{g_2(L)^3}{27}\left(1 - \frac{1728}{j(L)}\right)}{\frac{g_2(L')^3}{27}\left(1 - \frac{1728}{j(L')}\right)} = \frac{g_2(L)^3}{g_2(L')^3} = \lambda^{12},$$

i per tant

$$\lambda^6 = \pm\frac{g_3(L)}{g_3(L')}.$$

Canviant λ per $i\lambda$ si cal, podem suposar que el signe és positiu, i tenim (3.2.10).

Suposem ara que $g_2(L') = 0$. Aleshores $j(L') = 0$, i com que $j(L) = j(L')$, tenim que $j(L) = 0$. Per tant, $g_2(L) = 0$. A més, com que $\Delta(L') \neq 0$, tenim que $g_3(L) \neq 0$. Per tant, podem escollir $\lambda \in \mathbb{C} \setminus \{0\}$ tal que

$$\lambda^6 = \frac{g_3(L)}{g_3(L')},$$

de manera que se satisfà (3.2.10).

Finalment, suposem que $g_3(L') = 0$ i $g_2(L') \neq 0$. Aleshores

$$1728\frac{g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2} = j(L) = j(L') = 1728\frac{g_2(L')^3}{g_2(L')^3 - 27 g_3(L')^2} = 1728,$$

de manera que $g_2(L)^3 - 27g_3(L)^2 = g_2(L)^3$, és a dir, $g_3(L) = 0$. Per tant, podem escollir un nombre complex λ tal que

$$\lambda^4 = \frac{g_2(L)}{g_2(L')},$$

de manera que λ satisfà (3.2.10).

Per tant, en tots els casos se satisfà (3.2.10). Aleshores,

$$g_2(L') = \lambda^{-4} g_2(L) = g_2(\lambda L),$$

$$g_3(L') = \lambda^{-6} g_3(L) = g_3(\lambda L).$$

Utilitzant el punt (e) del teorema 3.1.4, tenim que $\wp(z, L')$ i $\wp(z, \lambda L)$ tenen el mateix desenvolupament sèrie de Laurent al voltant de l'origen. Per tant, $\wp(z, L') = \wp(z, \lambda L)$ per a tot $z \in \mathbb{C}$. Com que L' és el conjunt de pols de $\wp(z, L')$ i λL és el conjunt de pols de $\wp(z, \lambda L)$, tenim que $L' = \lambda L$. □

3.3 La funció j

Volem estudiar les propietats analítiques de l'invariant j, però per a poder-ho fer cal considerar j com una funció de variable complexa. Sigui $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ el semiplà superior. $\mathbf{SL}(2, \mathbb{Z})$ actua en $\mathbb{H}$ per l'acció $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$.

Definició 3.3.1. Sigui $\tau \in \mathbb{H}$. Considerem la xarxa $L_\tau = [1, \tau]$. Definim les funcions

$$\begin{aligned} g_2(\tau) &:= g_2(L_\tau) = 60 \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(m + n\tau)^4}, \\ g_3(\tau) &:= g_3(L_\tau) = 140 \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(m + n\tau)^6}, \\ \Delta(\tau) &:= \Delta(L_\tau) = g_2(\tau)^3 - 27 g_3(\tau)^2, \\ j(\tau) &:= \ j(L_\tau) = 1728 \frac{g_2(\tau)^3}{\Delta(\tau)}. \end{aligned}$$

Teorema 3.3.2. *Es compleixen les propietats següents.*

(a) *La funció $j : \mathbb{H} \to \mathbb{C}$ és holomorfa.*

(b) *Si $\tau, \tau' \in \mathbb{H}$, llavors $j(\tau) = j(\tau')$ si, i només si, existeix una matriu $\gamma \in \mathbf{SL}(2, \mathbb{Z})$ tal que $\tau' = \gamma\tau$. En particular, j és invariant per l'acció de $\mathbf{SL}(2, \mathbb{Z})$ en $\mathbb{H}$.*

(c) *L'aplicació $j : \mathbb{H} \to \mathbb{C}$ és exhaustiva.*

(d) *Per a $\tau \in \mathbb{H}$, es té $j'(\tau) \neq 0$ excepte per als casos*

  (a) *$\tau = \gamma i$, $\gamma \in \mathbf{SL}(2, \mathbb{Z})$, en què $j(\tau) = 0$, però $j''(\tau) \neq 0$,*

  (b) *$\tau = \gamma\rho, \rho = \frac{-1+\sqrt{3}}{2}$, i $\gamma \in \mathbf{SL}(2, \mathbb{Z})$, en què $j'(\tau) = j''(\tau) = 0$, però $j'''(\tau) \neq 0$.*

Corol·lari 3.3.3. *Siguin $g_2, g_3 \in \mathbb{C}$ tals que $g_2^3 - 27g_3^2 \neq 0$. Aleshores, existeix una xarxa $L \subseteq \mathbb{C}$ tals que $g_2(L) = g_2$ i $g_3(L) = g_3$.*

De la invariància de $j(\tau)$ respecte de $\mathbf{SL}(2,\mathbb{Z})$ es dedueix que

$$j(\tau+1) = j\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\tau\right) = j(\tau).$$

Per tant, podem considerar el desenvolupament en sèrie de Fourier de j,

$$j(\tau) = \sum_{n=-\infty}^{\infty} c_n q^n,$$

per a $q = e^{2\pi i\tau}$.

Teorema 3.3.4. *El desenvolupament en sèrie de Fourier de j és de la forma*

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n$$

on els c_n són enters per a $n \geq 0$. Els c_n per a $n \leq 4$ venen donats en la següent taula.

n	c_n
0	744
1	196884
2	21493760
3	864299970
4	20245856256

Així, $j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + ...$

Aquesta és una de les raons per les quals en definir la j multipliquem el quocient $g_2(L)^3/\Delta(L)$ per 1728: si no ho féssim, els coeficients de la sèrie de Fourier no serien enters, sinó enters dividits per 1728.

3.4 Els polinomis modulars

Considerem el conjunt de matrius

$$\Gamma_0(m) = \left\{ \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathbf{SL}(2,\mathbb{Z}) : c \equiv 0 \mod m \right\}.$$

$\Gamma_0(m)$ és un subgrup de $\mathbf{SL}(2,\mathbb{Z})$ d'índex

$$\psi(m) = m\prod_{p|m}\left(1+\frac{1}{p}\right).$$

Sigui $\{\gamma_1, ..., \gamma_{\psi(m)}\}$ un sistema qualsevol de representants de les classes laterals per l'esquerra de $\Gamma_0(m)$. Aleshores, la funció

$$\prod_{i=1}^{\psi(m)} (X - j(m\gamma_i\tau))$$

no depèn de l'elecció d'aquests representants.

Proposició 3.4.1. *$\prod_{i=1}^{\psi(m)}(X - j(m\gamma_i\tau))$ és un polinomi en X i en $j(\tau)$, que s'anomena el m-èsim polinomi modular i denotem per $\Phi_m(X, j)$.*

Les propietats principals dels polinomis modulars són les següents.

Teorema 3.4.2. *Sigui $m > 0$ un enter positiu.*

(a) $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.

(b) *$\Phi_m(X, Y)$ és irreductible com a polinomi en X.*

(c) *Per a $m > 1$, $\Phi_m(X, Y) = \Phi_m(Y, X)$.*

(d) *Si m no és un quadrat, aleshores $\Phi_m(X, X)$ és un polinomi de grau $d > 1$ amb coeficient dominant ± 1.*

(e) *(Congruències de Kronecker) Per a p primer, $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p)$ mod p.*

(f) *Si $x, y \in \mathbb{C}$, aleshores $\Phi_m(x, y) = 0$ si, i només si, existeixen una xarxa L i una subxarxa L' de L tals que $x = j(L')$ i $y = j(L)$ i el grup quocient L/L' és cíclic d'ordre m. Si L' i L compleixen aquesta última condició, diem que L' és una subxarxa cíclica d'índex m de L.*

Fent referència al punt (f), podem donar una caracterització de quan les subxarxes d'un $\mathcal{O}$-ideal fraccionari que són múltiples d'aquest són cícliques.

Lema 3.4.3. *Siguin $\mathcal{O}$ un ordre en un cos quadràtic imaginari i $\mathfrak{b}$ un $\mathcal{O}$-ideal fraccionari propi. Aleshores, donat $\alpha \in \mathcal{O}$, $\alpha\mathfrak{b}$ és una subxarxa de $\mathfrak{b}$ d'índex $N(\alpha)$, i $\alpha\mathfrak{b}$ és una subxarxa cíclica si, i només si, α no és de la forma $d\beta$, on $d > 1$ és un enter i $\beta \in \mathcal{O}$. Si α compleix aquesta última condició, diem que α és primitu.*

3.5 Multiplicació complexa i cossos de classes

Teorema 3.0.1. *Siguin $\mathcal{O}$ un ordre d'un cos quadràtic imaginari K i $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionari propi. Aleshores, l'invariant j de $\mathfrak{a}$, és un enter algebraic de grau $h(\mathcal{O})$ i $K(j(\mathfrak{a}))$ és el cos de classes de l'ordre $\mathcal{O}$.*

Demostració. En primer lloc, veiem que existeix un element $\alpha \in \mathcal{O}$ primitiu i no nul tal que $N(\alpha)$ no és un quadrat perfecte. Sigui f el conductor de $\mathcal{O}$, de manera que $\mathcal{O} = [1, f\omega_{d_K}]$ on $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$. Aleshores $\alpha := f\omega_{d_K}$ és un element no nul primitiu de $\mathcal{O}$, i

$$N(\alpha) = N(f\omega_{d_K}) = f^2\omega_{d_K}\overline{\omega_{d_K}} = f^2\frac{d_K(d_K - 1)}{4}.$$

Com que d_K no és un quadrat i $d_K, d_K - 1$ són relativament primers, tenim que $N(\alpha)$ no pot ser un quadrat.

Pel lema 3.4.3 tenim que $\alpha\mathfrak{a}$ és una subxarxa cíclica de $\mathfrak{a}$ d'índex $m := N(\alpha)$. Aleshores, utilitzant que $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$, el punt (f) del teorema 3.4.2 afirma que

$$0 = \Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = \Phi_m(j(\mathfrak{a}), j(\mathfrak{a})),$$

és a dir, que $j(\mathfrak{a})$ és una arrel del polinomi $\Phi_m(X, X)$. Pel teorema 3.4.2, $\Phi_m(X, X)$ és un polinomi de coeficients enters i de coeficient dominant ± 1, ja que m no és un quadrat. Per tant, $j(\mathfrak{a})$ és un enter algebraic.

Siguin L el cos de classes de l'ordre $\mathcal{O}$ i $M = K(j(\mathfrak{a}))$, i volem veure que $L = M$. Per a fer-ho, estudiarem quins primers de $\mathbb{Q}$ descomponen completament a L i a M. Sigui $\mathcal{S}_{L|\mathbb{Q}}$ el conjunt dels primers de $\mathbb{Q}$ que descomponen completament a L. Pel teorema 2.4.6,

$$\mathcal{S}_{L|\mathbb{Q}} \approx \{p \text{ primer} : p = N(\alpha) \text{ per a algun } \alpha \in \mathcal{O}\}.$$

Com que L és de Galois sobre $\mathbb{Q}$, per a veure $M \subseteq L$ és suficient veure $\mathcal{S}_{L|\mathbb{Q}} \lneq \mathcal{S}_{M|\mathbb{Q}}$. Sigui $p \in \mathcal{S}_{L|\mathbb{Q}}$. Podem suposar que p no és ramificat, ja que el nombre de primers que ramifiquen és finit. Com acabem de veure, tenim que $p = N(\alpha)$ per a algun $\alpha \in \mathcal{O}$. Així, $\alpha\mathfrak{a}$ és una subxarxa de $\mathfrak{a}$ d'índex $p = N(\alpha)$, i com que p és primer és cíclica. Per tant,

$$0 = \Phi_p(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\mathfrak{a}), j(\mathfrak{a})).$$

Utilitzant les congruències de Kronecker, tenim que existeix $\beta \in \mathcal{O}_K$ tal que

$$(j(\mathfrak{a})^p - j(\mathfrak{a}))^2 = p\beta.$$

Així, per a tot primer $\mathfrak{P}$ de M dividint p es té que

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \mathfrak{P}.$$

Com que $M = K(j(\mathfrak{a}))$ i $j(\mathfrak{a}) \in \mathcal{O}_M$, tenim que $\mathcal{O}_K[j(\mathfrak{a})]$ és un subgrup de $\mathcal{O}_M$. A més, com que els dos grups són grups abelians lliures de la mateixa dimensió, l'índex $[\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$ és finit. Veiem el següent lema.

Lema 3.5.1. *Si $p \nmid [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$, aleshores $\alpha^p \equiv \alpha \mod \mathfrak{P}$ per a tot $\alpha \in \mathcal{O}_M$.*

Demostració. Com que p descompon completament a L, també ho fa a K. $\mathfrak{p} := \mathfrak{P} \cap K$ és un ideal de $\mathcal{O}_K$ de norma p, i per tant per a tot $\alpha \in \mathcal{O}_K$ es té $\alpha^p \equiv \alpha \mod \mathfrak{p}$. Com que $\mathfrak{P}$ divideix $\mathfrak{p}$, tenim que $\alpha^p \equiv \alpha \mod \mathfrak{P}$ per a tot $\alpha \in \mathcal{O}_K$. Com que, a més, $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \mathfrak{P}$, tenim que $\alpha^p \equiv \alpha \mod \mathfrak{P}$ per a tot $\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$.

Suposem que p no divideix $n := [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$. Com que $n\mathcal{O}_M \subseteq \mathcal{O}_K[j(\mathfrak{a})]$, tenim que $n^p\alpha^p \equiv n\alpha \mod \mathfrak{P}$ per a tot $\alpha \in \mathcal{O}_M$. Com que p no divideix n, tenim que $n^p \equiv n \mod \mathfrak{P}$. Per tant $n\alpha^p \equiv n\alpha \mod \mathfrak{P}$, i com que n és invertible mòdul $\mathfrak{P}$, obtenim que $\alpha^p \equiv \alpha \mod \mathfrak{P}$ per a tot $\alpha \in \mathcal{O}_M$. □

D'aquest lema deduim que per a tot primer $\mathfrak{P}$ que divideix p, $f(\mathfrak{P}|\mathfrak{p}) = 1$, i per tant $\mathfrak{p}$ descompon completament en M. Per tant, $M \subseteq L$.

En particular, L conté els invarants j de tots els $\mathcal{O}$-ideals fraccionaris propis. Sigui $h = h(\mathcal{O})$, i siguin $\mathfrak{a}_1, ..., \mathfrak{a}_h$ representants de totes les classes de $\mathbf{Cl}(\mathcal{O})$. Aleshores, tot $j(\mathfrak{a})$ és algun $j(\mathfrak{a}_i)$, i $j(\mathfrak{a}_i) \neq j(\mathfrak{a}_j)$ per a $i \neq j$. Per tant,

$$\Delta := \prod_{i<j} (j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$$

és un element no nul de $\mathcal{O}_L$.

Per a veure que $L \subseteq M$, veurem que $\tilde{\mathcal{S}}_{M|\mathbb{Q}} \lneq \mathcal{S}_{L|\mathbb{Q}}$. Així, sigui $p \in \tilde{\mathcal{S}}_{M|\mathbb{Q}}$, és a dir, sigui p un primer no ramificat en M tal que $f(\mathfrak{P}|\mathfrak{p}) = 1$ per a algun primer $\mathfrak{P}$ de M que divideix p. En particular, p descompon completament en K, de manera que $p = N(\mathfrak{p})$, on $\mathfrak{p} = \mathfrak{P} \cap K$. Podem suposar que p és coprimer amb el conductor f de $\mathcal{O}$ i amb Δ, ja que això només exclou un nombre finit de primers p. Així, com que p és primer amb f, $\mathfrak{p} \cap \mathcal{O}$ és un ideal primer de $\mathcal{O}$, coprimer amb f i tal que $N(\mathfrak{p} \cap \mathcal{O}) = p$.

Si veiem que l'ideal $\mathfrak{p} \cap \mathcal{O}$ és un ideal principal $\alpha\mathcal{O}$, aleshores, com que $p = N(\alpha)$, tindrem que $p \in \mathcal{S}_{L|\mathbb{Q}}$, com volem. Sigui $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$. Com que $\mathfrak{p} \cap \mathcal{O}$ té norma p, $\mathfrak{a}'$ és una subxarxa de $\mathfrak{a}$ d'índex p, i per tant és cíclica. Per tant, $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$, i utlitizant les congruències de Kronecker, obtenim que existeix $Q(x, y) \in \mathbb{Z}[X, Y]$ tal que

$$0 = \Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = (j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pQ(j(\mathfrak{a}'), j(\mathfrak{a})),$$

Sigui $\tilde{\mathfrak{P}}$ un primer de L que divideix $\mathfrak{P}$. Com que $j(\mathfrak{a}'), j(\mathfrak{a}) \in \mathcal{O}_L$, tenim que $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in \tilde{\mathfrak{P}}$. Per tant,

$$j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \mod \tilde{\mathfrak{P}} \qquad \text{o} \qquad j(\mathfrak{a}') \equiv j(\mathfrak{a})^p \mod \tilde{\mathfrak{P}}.$$

D'altra banda, com que $f(\mathfrak{P}|\mathfrak{p}) = 1$, tenim que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \mathfrak{P}$, i com que $\mathfrak{P} \subseteq \tilde{\mathfrak{P}}$, obtenim que $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \mathfrak{P}$. Per tant,

$$j(\mathfrak{a}) \equiv j(\mathfrak{a}') \mod \tilde{\mathfrak{P}}.$$

Si $\mathfrak{a}, \mathfrak{a}'$ representessin classes diferents de $\mathbf{Cl}(\mathcal{O})$, aleshores $j(\mathfrak{a}) - j(\mathfrak{a}')$ dividiria Δ, i p i Δ no serien coprimers, contradient la nostra hipòtesi. Per tant, $\mathfrak{a}$ i $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$ representen la mateixa classe a $\mathbf{Cl}(\mathcal{O})$. En particular, la classe de $\mathfrak{p} \cap \mathcal{O}$ és l'element neutre de $\mathbf{Cl}(\mathcal{O})$, és a dir, $\mathfrak{p} \cap \mathcal{O}$ és un ideal principal, com volíem veure.

En particular, l'extensió $K(j(\mathfrak{a}))|K$ té grau $h(\mathcal{O})$, de manera que el grau de $j(\mathfrak{a})$ com a enter algebraic és, com a mínim, $h(\mathcal{O})$. Per a veure que és exactament $h(\mathcal{O})$, es veu que qualsevol $\mathbb{Q}$-automorfisme σ de $K(j(\mathfrak{a}))$ envia $j(\mathfrak{a})$ a $j(\mathfrak{b})$, on $\mathfrak{b}$ és un $\mathcal{O}$-ideal fraccionari. Per tant, només hi ha $h(\mathcal{O})$ possibilitats per a $\sigma(j(\mathfrak{a}))$, de manera que $j(\mathfrak{a})$ és de grau menor o igual que $h(\mathcal{O})$. Es poden trobar tots els detalls a [1, teorema 10.23]. □

Observació 3.5.2. En el cas en què $\mathcal{O}$ és un ordre de nombre de classes 1, el teorema ens diu que $j(\mathcal{O})$ és un enter algebraic de grau 1, és a dir, que $j(\mathcal{O})$ és un enter.

També podem descriure com actual el símbol d'Artin sobre $j(\mathfrak{a})$.

Teorema 3.5.3 (llei de reciprocitat)**.** *Sigui $\mathcal{O}$ un ordre d'un cos quadràtic imaginari K i L el cos de classes de $\mathcal{O}$. Si $\mathfrak{a}$ és un $\mathcal{O}$-ideal fraccionari propi i $\mathfrak{p}$ és un ideal primer de $\mathcal{O}_K$, aleshores*

$$\left(\frac{L|K}{\mathfrak{p}}\right)(j(\mathfrak{a})) = j(\overline{\mathfrak{p} \cap \mathcal{O}}\mathfrak{a}).$$

Corol·lari 3.5.4. *Sigui $\mathcal{O}$ un ordre d'un cos quadràtic imaginari K i L el cos de classes de $\mathcal{O}$. Donats dos $\mathcal{O}$-ideals fraccionaris $\mathfrak{a}$ i $\mathfrak{b}$, definim $\sigma_{\mathfrak{a}}(j(\mathfrak{b})) := j(\overline{\mathfrak{a}}\mathfrak{b})$. $\sigma_{\mathfrak{a}}$ està ben definit i és un element de $Gal(L|K)$, i $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ indueix un isomorfisme entre $\mathbf{Cl}(\mathcal{O})$ i $Gal(L|K)$.*

3.6 Una arrel cúbica de j i les funcions de Weber

Per a resoldre el problema del nombre de classes 1, haurem de calcular l'invariant j d'alguns ordres de cossos quadràtics imaginaris. De moment, però, no tenim bones eines per a fer-ho. Per això, en aquesta secció definirem altres funcions relacionades amb la funció j i amb les quals és més fàcil treballar, i enunciarem algunes de les seves propietats. Recordem que havíem definit $j(\tau)$ com

$$j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)}.$$

La funció $\Delta(\tau)$ no s'anul·la en $\mathbb{H}$, que és simplement connex, de manera que té una arrel cúbica holomorfa $\sqrt[3]{\Delta(\tau)}$. A més, $\Delta(\tau)$ és real quan τ és imaginari pur, de manera que podem escollir $\sqrt[3]{\Delta(\tau)}$ amb la mateixa propietat.

Definició 3.6.1. Definim $\gamma_2(\tau) = 12\frac{g_2(\tau)}{\sqrt[3]{\Delta(\tau)}}$.

Observació 3.6.2. Com que $g_2(\tau)$ també és real quan τ és imaginari pur, es té que $\gamma_2(\tau)$ és l'única arrel cúbica de $j(\tau)$ que és real quan τ és imaginari pur.

La propietat que més ens interessa de $\gamma_2(\tau)$ és la següent.

Teorema 3.6.3. *Sigui $\mathcal{O}$ un ordre de discriminant D no divisible per 3 en un cos quadràtic imaginari K. Posem $\mathcal{O} = [1, \tau_0]$ on*

$$\tau_0 = \begin{cases} \sqrt{-m}, & \text{si } D = -4m \equiv 0 \mod 4, \\ \frac{3+\sqrt{-m}}{2}, & \text{si } D = -m \equiv 1 \mod 4. \end{cases}$$

Aleshores, $\gamma_2(\tau)$ és un enter algebraic i $K(\gamma_2(\tau_0))$ és el cos de classes de $\mathcal{O}$. A més, $\mathbb{Q}(\gamma_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$.

En particular, si $\mathcal{O}$ és un ordre de discriminant D no divisible per 3 i de nombre de classes 1, definint τ_0 com al teorema tenim que $\gamma_2(\tau_0)$ és un enter i que $j(\tau_0)$ és un cub.

Definició 3.6.4. Siguin $\tau \in \mathbb{H}, q = e^{2\pi i\tau}, \zeta_{48} = e^{2\pi i/48}$. Definim les funcions

$$\begin{aligned} \eta(\tau) &:= q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \\ \mathfrak{f}(\tau) &:= \zeta_{48}^{-1}\frac{\eta((\tau+1)/2)}{\eta(\tau)}, \\ \mathfrak{f}_1(\tau) &:= \frac{\eta(\tau/2)}{\eta(\tau)}, \\ \mathfrak{f}_2(\tau) &:= \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)}. \end{aligned}$$

η s'anomena funció η de Dedekind, i $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$ s'anomenen funcions de Weber. El producte $\prod_{n=1}^{\infty}(1-q^n)$ convergeix absolutament, ja que $|q| < 1$, i uniformement sobre compactes de $\mathbb{H}$, de manera que $\eta(\tau) \neq 0$ i aquestes funcions estan ben definides.

Proposició 3.6.5. *Siguin $\tau \in \mathbb{H}, q = e^{2\pi i\tau}$. Aleshores,*

(a) $\mathfrak{f}(\tau) = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2})$,

(b) $\mathfrak{f}_1(\tau) = q^{-1/48}\prod_{n=1}^{\infty}(1-q^{n-1/2})$,

(c) $\mathfrak{f}_2(\tau) = \sqrt{2}q^{1/24}\prod_{n=1}^{\infty}(1+q^n)$,

(d) $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2} = \mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau)$.

Demostració. En substituir $\eta(\tau)$ pel seu desenvolupament en producte, i tenint en compte que tots els productes convergeixen absolutament i uniformement sobre compactes

de $\mathbb{H}$, tenim que

$$\begin{aligned}
\mathfrak{f}(\tau) &= \zeta_{48}^{-1}\frac{\eta((\tau+1)/2)}{\eta(\tau)} = \zeta_{48}^{-1}\frac{\zeta_{48}q^{1/48}\prod_{n=1}^{\infty}(1-(-1)^n q^{n/2})}{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)} = \\
&= q^{-1/48}\frac{\prod_{n=1}^{\infty}(1+q^{n-1/2})(1-q^n)}{\prod_{n=1}^{\infty}(1-q^n)} = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2}),\\
\mathfrak{f}_1(\tau) &= \frac{\eta(\tau/2)}{\eta(\tau)} = \frac{q^{1/48}\prod_{n=1}^{\infty}(1-q^{n/2})}{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)} = q^{-1/48}\prod_{n=1}^{\infty}(1-q^{n-1/2}),\\
\mathfrak{f}_2(\tau) &= \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2}\frac{q^{1/12}\prod_{n=1}^{\infty}(1-q^{2n})}{q^{1/24}\prod_{n=1}^{\infty}(1-q^n)} = \sqrt{2}q^{1/24}\frac{\prod_{n=1}^{\infty}((1-q^n)(1+q^n))}{\prod_{n=1}^{\infty}(1-q^n)}\\
&= \sqrt{2}q^{1/24}\prod_{n=1}^{\infty}(1+q^n).
\end{aligned}$$

A més, $\mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \frac{\eta(\tau)}{\eta(2\tau)}\cdot\sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2}$.

En substituir $\eta, \mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2$ pels seus desenvolupaments en productes, obtenim que

$$\begin{aligned}
&\eta(\tau)\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \\
&= \sqrt{2}\prod_{n=1}^{\infty}\left((1+q^{n-1/2})(1-q^{n-1/2})\right)\prod_{n=1}^{\infty}((1-q^n)(1+q^n)) = \\
&= \sqrt{2}\prod_{n=1}^{\infty}(1-q^{2n-1})\prod_{n=1}^{\infty}(1-q^{2n}) = \sqrt{2}\prod_{n=1}^{\infty}(1-q^n) = \sqrt{2}\eta(\tau).
\end{aligned}$$

Per tant, $\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \sqrt{2}$. □

Aquestes no són les úniques relacions entre les funcions de Weber.

Teorema 3.6.6. *Siguin $\tau \in \mathbb{H}, q = e^{2\pi i\tau}$. Aleshores, $\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}$ i*

$$\gamma_2(\tau) = \frac{\mathfrak{f}(\tau)^{24}-16}{\mathfrak{f}(\tau)^8} = \frac{\mathfrak{f}_1(\tau)^{24}+16}{\mathfrak{f}_1(\tau)^8} = \frac{\mathfrak{f}_2(\tau)^{24}-16}{\mathfrak{f}_2(\tau)^8}.$$

A més, si $\zeta_n = e^{2\pi i/n}$,

$$\begin{aligned}
\mathfrak{f}(\tau+1) &= \zeta_{48}^{-1}\mathfrak{f}_1(\tau), & \mathfrak{f}(-1/\tau) &= \mathfrak{f}(\tau),\\
\mathfrak{f}_1(\tau+1) &= \zeta_{48}^{-1}\mathfrak{f}(\tau), & \mathfrak{f}_1(-1/\tau) &= \mathfrak{f}_2(\tau),\\
\mathfrak{f}_2(\tau+1) &= \zeta_{24}\mathfrak{f}_2(\tau), & \mathfrak{f}_2(-1/\tau) &= \mathfrak{f}_1(\tau).
\end{aligned}$$

Així, les funcions de Weber estan relacionades amb la funció j, i per tant també tenen relació amb la teoria de cossos de classes.

Teorema 3.6.7. *Sigui m un enter positiu no divisible per 3. Aleshores $\mathcal{O} := [1, \sqrt{-m}]$ és un ordre de $K := \mathbb{Q}(\sqrt{-m})$ i*

(a) *si $m \equiv 6 \mod 8$, llavors $\mathfrak{f}_1(\sqrt{-m})^2$ és un enter algebraic i $K(\mathfrak{f}_1(\sqrt{-m})^2)$ és el cos de classes de l'ordre $\mathcal{O}$.*

(b) *si $m \equiv 3 \mod 4$, llavors $\mathfrak{f}(\sqrt{-m})^2$ és un enter algebraic i $K(\mathfrak{f}(\sqrt{-m})^2)$ és el cos de classes de l'ordre $\mathcal{O}$.*

4 La solució del problema del nombre de classes 1

En aquest capítol trobarem per a quins $D < 0$ tenim que $h(D) = 1$. El resultat principal és el següent.

Teorema 4.0.1 (Heegner-Baker-Stark)**.** *Siguin K un cos quadràtic imaginari i d_K el seu discriminant. Aleshores*

$$h(d_K) = 1 \iff d_k \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

El procediment serà el següent:

(1) Calcularem l'invariant j d'alguns dels ordres quadràtics que, pel teorema 1.4.4, ja sabem que tenen nombre de classes 1.

(2) Suposarem que $h(\mathcal{O}_K) = 1$. Utilitzant resultats del primer capítol, reduirem el problema al cas en què $d_K = -p$, on p és un primer amb $p \equiv 3 \mod 8$.

(3) Utilitzant les funcions de Weber, reduirem el càlcul dels possibles valors de $j(\mathcal{O}_K)$ a trobar les possibles solucions enteres de l'equació $Y^2 = 2X(X^3 + 1)$.

(4) Resoldrem aquesta equació, trobant així els possibles valors de $j(\mathcal{O}_K)$. Aquests valors seran alguns dels que hem calculat al primer pas, de manera que com que $j(\mathcal{O}_K)$ determina $\mathcal{O}_K$ (ja que dos ordres diferents no són homotètics com a xarxes), ja tindrem tots els possibles cossos K.

(5) Finalment, deduirem quins són tots els ordres, no necessàriament maximals, de cossos quadràtics imaginaris que tenen nombre de classes 1.

4.1 Invariants j dels ordres de nombre de classes 1

Volem calcular l'invariant j dels ordres quadràtics de discriminants $-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$. El teorema 1.4.4 diu que aquests ordres són de nombre de classes 1. En particular, el seu invariant j és un enter.

Si el discriminant de $\mathcal{O}$ no és múltiple de 3, el teorema 3.6.3 ens diu que $j(\mathcal{O})$ és un cub. Per tant, només haurem de calcular $\gamma_2(\tau_0)$, que és un enter, per a un τ_0 adequat.

Teorema 4.1.1. *Els invariants j dels ordres quadràtics de discriminants $-4, -7, -8, -11, -16, -19, -28, -43, -67, -163$ venen donats en la taula següent.*

D	τ_0	$\gamma_2(\tau_0)$	$j(\mathcal{O}) = j(\tau_0)$
-4	i	12	12^3
-7	$\frac{3+\sqrt{-7}}{2}$	-15	-15^3
-8	$\sqrt{-2}$	20	20^3
-11	$\frac{3+\sqrt{-11}}{2}$	-32	-32^3
-16	$2i$	66	66^3
-19	$\frac{3+\sqrt{-19}}{2}$	-96	-96^3
-28	$\sqrt{-7}$	255	255^3
-43	$\frac{3+\sqrt{-43}}{2}$	-960	-960^3
-67	$\frac{3+\sqrt{-67}}{2}$	-5280	-5280^3
-163	$\frac{3+\sqrt{-163}}{2}$	-640320	-640320^3

DEMOSTRACIÓ. Utilitarem les funcions de Weber per a aproximar $\gamma_2(\tau_0)$ amb un error de ± 0.5. Com que $\gamma_2(\tau_0)$ és un enter, serà l'enter més proper a la nostra aproximació.

Comencem pels casos de discriminant parell, $D = -4m$ per a $m = 1, 2, 4, 7$. En aquest cas, $\tau_0 = \sqrt{-m}$. Sigui $q = e^{2\pi i \tau_0} = e^{-2\pi\sqrt{m}}$. Veurem que $\gamma_2(\sqrt{-m}) = [[256q^{2/3} + q^{-1/3}]]$, on $[[x]]$ denota l'enter més proper a x.

Sabem pel teorema 3.6.6 que

$$\gamma_2(\sqrt{-m}) = \mathfrak{f}_2(\sqrt{-m})^{16} + \frac{16}{\mathfrak{f}_2(\sqrt{-m})^8}. \tag{4.1.2}$$

A més,

$$\mathfrak{f}_2(\sqrt{-m}) = \sqrt{2}q^{1/24}\prod_{n=1}^{\infty}(1+q^n). \tag{4.1.3}$$

Utilitzant que $1 + x < e^x$ per a tot $x \in \mathbb{R}$, tenim que

$$1 < \prod_{n=1}^{\infty}(1+q^n) < \prod_{n=1}^{\infty} e^{q^n} = e^{\sum_{n=1}^{\infty} q^n} = e^{q/(1-q)}. \tag{4.1.4}$$

Com que $q \leq e^{-2\pi}$, tenim que $q/(1-q) \leq q/(1-e^{-2\pi}) < 1.002q$. Combinant això amb (4.1.3) i (4.1.4), obtenim que

$$\sqrt{2}q^{1/24} < \mathfrak{f}_2(\sqrt{-m}) < \sqrt{2}q^{1/24}e^{q/(1-q)} < \sqrt{2}q^{1/24}e^{1.002q}.$$

En particular, per (4.1.2), tenim que

$$256q^{2/3} + q^{-1/3}e^{-8.016q} < \gamma_2(\sqrt{-m}) < 256q^{2/3}e^{16.032q} + q^{-1/3}.$$

Considerem la diferència entre aquestes cotes,

$$E(q) = 256q^{2/3}(e^{16.032q} - 1) + q^{-1/3}(1 - e^{-8.016q}).$$

Utilitzant que $1 - e^{-x} < x/(1-x)$ per a $0 < x < 1$, obtenim que

$$E(q) < 256q^{2/3}(e^{16.032q} - 1) + q^{-1/3} \cdot 8.016q/(1 - 8.016q) =$$

$$= 256q^{2/3}(e^{16.032q} - 1) + 8.016q^{2/3}/(1 - 8.016q).$$

Aquesta expressió és creixent respecte q. Com que $q < e^{-2\pi}$, tenim que $E(q) < E(e^{-2\pi}) < 0.25$. Per tant, per a tot x tal que

$$256q^{2/3} + q^{-1/3}e^{-8.016q} < x < 256q^{2/3}e^{16.032q} + q^{-1/3},$$

es té $[[x]] = \gamma_2(\sqrt{-m})$. Com que $x = 256q^{2/3} + q^{-1/3}$ satisfà aquestes desigualtats, tenim que $\gamma_2(\sqrt{-m}) = [[256q^{2/3} + q^{-1/3}]]$.

Considerem ara els discriminants senars. Sigui $\tau_0 = \frac{3+\sqrt{-m}}{2}$ per a $m = 7, 11, 19, 43, 67$ o 163. També utilitzarem (4.1.2), però no podem utilitzar el mateix mètode que al cas anterior, ja que ara $q = e^{2\pi i \frac{3+\sqrt{-m}}{2}} = -e^{-\pi\sqrt{m}}$ és negatiu. Sabem, però, que

$$\mathfrak{f}_2(\tau_0) = \frac{\sqrt{2}}{\mathfrak{f}_1(2\tau_0)},$$

i a més, si $\zeta_n := e^{2\pi i/n}$,

$$\mathfrak{f}_1(2\tau_0) = \mathfrak{f}_1(3+\sqrt{-m}) = \zeta_{48}^{-1}\mathfrak{f}(2+\sqrt{-m}) =$$
$$= \zeta_{48}^{-2}\mathfrak{f}_1(1+\sqrt{-m}) = \zeta_{48}^{-3}\mathfrak{f}(\sqrt{-m}) = \zeta_{16}^{-1}\mathfrak{f}(\sqrt{-m}).$$

Per tant,

$$\mathfrak{f}_2(\tau_0) = \frac{\zeta_{16}\sqrt{2}}{\mathfrak{f}(\sqrt{-m})},$$

d'on obtenim que

$$\gamma_2(\tau_0) = \frac{256}{\mathfrak{f}(\sqrt{-m})^{16}} - \mathfrak{f}(\sqrt{-m})^8.$$

Utilitzarem un mètode anàleg al cas anterior per a obtenir que, per a $q = e^{2\pi i\sqrt{-m}} = e^{-2\pi\sqrt{m}}$ (observem que ara $q > 0$), es compleix

$$\gamma_2(\tau_0) = [[-q^{-1/6} + 256q^{1/3}]].$$

Sabem que

$$\mathfrak{f}(\sqrt{-m}) = q^{-1/48}\prod_{n=1}^{\infty}(1+q^{n-1/2}).$$

Com abans, tenim que

$$1 < \prod_{n=1}^{\infty}(1+q^{n-1/2}) < \prod_{n=1}^{\infty} e^{q^{n-1/2}} = e^{q^{-1/2}\sum_{n=1}^{\infty} q^n} = e^{q^{1/2}/(1-q)}$$

i $q^{1/2}/(1-q) \leq q^{1/2}/(1-e^{-2\pi}) < 1.002q^{1/2}$. Per tant,

$$q^{-1/48} < \mathfrak{f}(\sqrt{-m}) < q^{-1/48}e^{1.002q^{1/2}},$$

d'on deduim que

$$256q^{1/3}e^{-16.032q^{1/2}} - q^{-1/6}e^{8.016q^{1/2}} < \gamma_2(\tau_0) < 256q^{1/3} - q^{-1/6}.$$

Considerem la diferència

$$E(q) = (256q^{1/3} - q^{-1/6}) - (256q^{1/3}e^{-16.032q^{1/2}} - q^{-1/6}e^{8.016q^{1/2}}).$$

De nou, tenim que $E(q) < 0.25$, i per tant per a tot x tal que

$$256q^{1/3}e^{-16.032q^{1/2}} - q^{-1/6}e^{8.016q^{1/2}} \leq x \leq 256q^{1/3} - q^{-1/6}$$

es té que $[[x]] = \gamma_2(\tau_0)$. Com que $x = -q^{-1/6} + 256q^{1/3}$ satisfà aquestes desigualtats, tenim que

$$\gamma_2(\tau_0) = [[-q^{-1/6} + 256q^{1/3}]].$$

Així, podem comprovar els valors de la taula fàcilment amb una calculadora de mà. □

Observació 4.1.5. Pel teorema 3.3.2, $j(\frac{-1+\sqrt{-3}}{2}) = 0$. Això ens diu que, per a l'ordre $\mathcal{O}$ de discriminant $D = -3$, tenim que $j(\mathcal{O}) = 0$.

Tot i que no ho utilitzarem per a donar la solució del problema del nombre de classes 1, donem l'invariant j dels ordres de nombre de classes 1 de discriminant divisible per 3.

Proposició 4.1.6. *Els invariants j dels ordres de nombre de classes 1 de discriminant un múltiple de 3 venen donats en la taula següent.*

D	τ_0	$j(\mathcal{O}) = j(\tau_0)$
-3	$\frac{1+\sqrt{-3}}{2}$	0
-12	$\sqrt{-3}$	54000
-27	$\frac{3+\sqrt{-3}}{2}$	-12288000

4.2 Solució del problema

Teorema 4.0.1 (Heegner-Baker-Stark)**.** *Siguin K un cos quadràtic imaginari i d_K el seu discriminant. Aleshores*

$$h(d_K) = 1 \iff d_k \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

Demostració. Sigui d_K el discriminant d'un cos quadràtic imaginari tal que $h(d_K) = 1$. Pel teorema de Landau (teorema 1.4.5) tenim que $h(-4n) = 1 \iff -4n = -4, -8, -12, -16$ o -28. Observem, però, que no existeix cap cos quadràtic K amb $d_K = -12, -16, -28$. Per tant, si d_K és parell, aleshores $h(d_K) = 1 \iff d_K = -4, -8$.

Suposem, per tant, que d_K és senar, $d_K \equiv 1 \mod 4$. La proposició 1.4.6 ens diu que $-d_K$ ha de ser una potència d'un primer. Com que d_K és el discriminant d'un cos, ha de ser lliure de quadrats, de manera que $d_K = -p$ on p és un primer, $p \equiv 3 \mod 4$.

Si $p \equiv 7 \mod 8$, aleshores pel teorema 1.5.4 tenim que

$$h(-4p) = 2h(-p)\left(1 - \left(\frac{-p}{2}\right)\frac{1}{2}\right) = h(-p) = 1.$$

Pel teorema de Landau, tenim que $p = 7$.

Suposem ara que $p \equiv 3 \mod 8$. Podem suposar que $p \neq -3$, ja que ja sabem que $h(-3) = 1$. Pel teorema 1.5.4, tenim que

$$h(-4p) = 2h(-p)\left(1 - \left(\frac{-p}{2}\right)\frac{1}{2}\right) = 3h(-p) = 3.$$

Per tant, $K(j(\sqrt{-p}))$, que és el cos de classes de l'ordre de discriminant $-4p$, és de grau 3 sobre K, de manera que $\mathbb{Q}(j(\sqrt{-p}))$ és de grau 3 sobre $\mathbb{Q}$. Pel teorema 3.6.7, tenim que $\mathfrak{f}(\sqrt{-p})^2 \in K(j(\sqrt{-p}))$. A més, com que tots els factors del desenvolupament en producte de $\mathfrak{f}(\sqrt{-p})$ donat a 3.6.5 són reals, tenim que $\mathfrak{f}(\sqrt{-p})^2$ és real, i per tant genera una extensió cúbica de $\mathbb{Q}$.

Siguin $\tau_0 = \frac{3+\sqrt{-p}}{2}$ i $\alpha = \zeta_8^{-1}\mathfrak{f}_2(\tau_0)^2$. Pel teorema 3.6.5 tenim que

$$\mathfrak{f}_1(2\tau_0)\mathfrak{f}_2(\tau_0) = \sqrt{2}$$

i pel teorema 3.6.6 tenim que

$$\mathfrak{f}_1(2\tau_0) = \mathfrak{f}_1(3 + \sqrt{-p}) = \zeta_{48}^{-3}\mathfrak{f}(\sqrt{-p}) = \zeta_{16}^{-1}\mathfrak{f}(\sqrt{-p}).$$

D'aquí deduim que $\alpha = 2/\mathfrak{f}(\sqrt{-p})^2$. Per tant, α genera l'extensió cúbica $\mathbb{Q}(\mathfrak{f}(\sqrt{-p})^2)$, i α^4 genera la mateixa extensió.

Estudiem el polinomi irreductible de α^4. Com que $\mathcal{O} = [1, \tau_0]$ i $h(-p) = 1$, tenim que $j(\tau_0)$ és un enter, i per tant $\gamma_2(\tau_0)$ també és un enter. A més,

$$\gamma_2(\tau_0) = \frac{\mathfrak{f}_2(\tau_0)^{24} + 16}{\mathfrak{f}_2(\tau_0)^8}.$$

Per tant, $\alpha^4 = -\mathfrak{f}_2(\tau_0)^8$ és una solució de l'equació

$$x^3 - \gamma_2(\tau_0) - 16 = 0,$$

i aquest és el seu polinomi irreductible.

D'altra banda, α també és un enter algebraic, de manera que és solució d'una equació de la forma $x^3 + ax^2 + bx + c = 0$. Movent els termes de grau parell al costat dret i elevant els dos costats als quadrats, obtenim

$$(x^3 + bx)^2 = (-ax^2 - c)^2.$$

Reordenant els termes, obtenim

$$x^6 + (2b - a^2)x^4 + (b^2 - 2ac)x^2 - c^2 = 0.$$

Per tant, α^2 és solució de l'equació

$$x^3 + ex^2 + fx + g = 0, \qquad \text{on } e = 2b - a^2, f = b^2 - 2ac, g = -c^2,$$

i repetint el procés obtenim que α^4 és solució de

$$x^3 + (2f - e^2)x^2 + (f^2 - 2eg)x - g^2.$$

Utilitzant que el polinomi irreductible de α^4 és únic, tenim que

$$\begin{cases} 2f - e^2 & = 0, \\ f^2 - 2eg & = -\gamma_2(\tau_0), \\ g^2 & = 16. \end{cases}$$

De la tercera equació, deduim que $g = \pm 4$, i com que $g = -c^2$ tenim que $g = -4$ i $c = \pm 2$. Si en comptes d'estudiar el polinomi mínim de α estudiéssim el de $-\alpha$, aleshores α^4 quedaria fix, pero a, b, c es canviarien per $-a, b, -c$. Per tant, podem suposar que $c = 2$. Aleshores,

$$\gamma_2(\tau_0) = -f^2 - 8e = -(b^2 - 4a)^2 - 8(2b - a^2).$$

D'altra banda, de l'equació $2f = e^2$ obtenim que $2(b^2 - 4a) = (2b - a^2)^2$. Per tant, a i b són enters parells. Prenent $x = -a/2$ i $y = (b - a^2)/2$, obtenim que x i y són solucions de l'equació diofantina $2X(X^3 + 1) = Y^2$. Les solucions d'aquesta equació ens venen donades pel lema següent, que demostrarem més endavant.

Lema 4.2.1. *Les solucions enteres de l'equació diofantina* $2X(X^3 + 1) = Y^2$ *són* $(0, 0)$, $(-1, 0), (1, \pm 2), (2, \pm 6)$.

Així, podem calcular tots els possibles valors per a a, b i $\gamma_2(\tau_0)$.

X	Y	$a=-2X$	$b=4X^2+2Y$	$\gamma_2(\tau_0)=-(b^2-4a)^2-8(2b-a^2)$
0	0	0	0	0
-1	0	2	4	-96
1	2	-2	8	-5280
1	-2	-2	0	-32
2	6	-4	28	-640320
2	-6	-4	4	-960

Tots aquests $\gamma_2(\tau_0)$ són alguns dels que hem calculat al teorema 4.1.1 i a la observació 4.1.5. Com que $j(\mathcal{O}_K)=\gamma_2(\tau_0)^3$ determina K, el cos K ha de ser un dels cossos que ja sabem que tenen nombre de classes 1. □

Corol·lari 4.2.2. *Sigui $D\equiv 0,1 \mod 4$. Aleshores,*

$$h(D)=1 \iff D\in\{-3,-4,-7,-8,-11,-12,-16,-19,-27,-28,-43,-67,-163\}.$$

Demostració. Suposem que $h(D)=1$. Posem $D=f^2d_K$, on K és el cos quadràtic imaginari que conté a l'ordre de discriminant D. Pel teorema 1.5.4 tenim que $h(d_K)|h(D)$, de manera que $h(d_K)=1$. Pel teorema anterior, tenim que $d_k\in\{-3,-4,-7,-8,-11,-19,-43,-67,-163\}$. Veiem per a quins conductors f tenim que $h(f^2d_K)=1$.

Les unitats dels anells d'enters de cossos quadràtics imaginaris venen donats per

$$\mathcal{O}_K^*=\begin{cases}\{\pm1\}, & \text{si } d_K\neq -3,-4,\\ \{\pm1,\frac{\pm1\pm\sqrt{-3}}{2}\}, & \text{si } d_K=-3,\\ \{\pm1,\pm i\}, & \text{si } d_K=-4.\end{cases}.$$

En particular, si $f>1$, aleshores $\mathcal{O}^*=\{\pm1\}$.

Comencem suposant que $d_K\neq -3,-4$. Aleshores $\mathcal{O}_K^*=\{\pm1\}$, de manera que $[\mathcal{O}_K^*:\mathcal{O}^*]=1$. Si $f>2$, sigui $f=p_1^{e_1}\cdots p_r^{e_r}$ la descomposició de f en factors primers. Llavors,

$$f\prod_{p|f}\left(1-\left(\frac{d_K}{p}\right)\frac{1}{p}\right)\geq f\prod_{p|f}\left(1-\frac{1}{p}\right)=\prod_{i=1}^{r}p_i^{e_i}\left(1-\frac{1}{p_i}\right)=\prod_{i=1}^{r}p_i^{e_i-1}(p_i-1)>1,$$

i pel teorema 1.5.4 tenim que $h(f^2d_K)>1$. Per a $f=2$, calculant tots els casos per a d_K veiem que $h(4d_K)=1$ si, i només si, $d_K=-7$, de manera que $D=-28$.

Suposem ara que $d_K=-3,-4$, de manera que $[\mathcal{O}_K^*:\mathcal{O}^*]\leq 3$. Si $f>3$, sigui $f=p_1^{e_1}\cdots p_r^{e_r}$ la descomposició en factors primers de f. Aleshores,

$$f\prod_{p|f}\left(1-\left(\frac{d_K}{p}\right)\frac{1}{p}\right)\geq\prod_{i=1}^{r}p_i^{e_i-1}(p_i-1)>3.$$

L'última desigualtat és certa perquè, per a que cap dels factors $p_i^{e_i-1}(p_i-1)$ sigui major que 3, els p_i han de ser 2 o 3 i els e_i menors o iguals que 2 i 1 respectivament. Comprovant manualment els casos $f=4,6,12$, veiem que la desigualtat és certa. Per tant, si $f>3$,

$$h(f^2d_K)=\frac{1}{[\mathcal{O}_K^*:\mathcal{O}^*]}f\prod_{p|f}\left(1-\left(\frac{d_K}{p}\right)\frac{1}{p}\right)>1.$$

Si $d_K = -3$, per a $f = 2$ i $f = 3$ es té que $h(f^2 d_K) = 1$, i per tant $D = -12$ o $D = -27$.

Per a $d_K = -4$, si $f = 3$ aleshores $h(f^2 d_K) > 1$. En canvi, si $f = 2$ aleshores $h(f^2 d_K) = 1$, i per tant $D = -16$. □

El teorema de Heegner-Baker-Stark té diverses conseqüències força interessants.

- En primer lloc, explica per què $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925...$ és tan proper a un enter.

  Recordem que $j(q)$ admet el desenvolupament en sèrie de Fourier $j(\tau) = \frac{1}{q} + 744 + 196884q + ...$ Es pot estudiar el comportament assimptòtic dels coeficients c_n d'aquesta sèrie, i s'obté que $c_n q^n$ convergeix ràpidament a 0.

  Siguin $\tau = \frac{1+\sqrt{-163}}{2}$ i $q = e^{2\pi i\tau} = -e^{-\pi\sqrt{163}}$. Tenim que $j(\tau) = -640320^3$. Aproximant $j(\tau)$ pels dos primers termes de la sèrie de Fourier, $j(\tau) \approx \frac{1}{q} + 744$, es pot demostrar que l'error és menor que 10^{-11}, de manera que

  $$-640320^3 = j(\tau) = \frac{1}{q} + 744 + \cdots \approx \frac{1}{q} + 744 = -e^{\pi\sqrt{163}} + 744,$$

  d'on es dedueix que $e^{\pi\sqrt{163}} \approx 640320^3 + 744 = 262537412640768744$.

- Euler va descobrir una propietat extraordinària del polinomi $x^2 - x + 41$: aquest polinomi pren valors primers per a $0 \leq x < 41$. De fet, 41 no és l'únic nombre amb aquesta propietat: 1, 2, 3, 5, 11, i 17 també la satisfan. La connexió d'aquest fet amb el problema del nombre de classes 1 és la següent.

  Proposició 4.2.3. *Sigui k un enter positiu. Són equivalents:*

  (a) *$x^2 - x + k$ és primer per a $0 \leq x < k$.*

  (b) *L'ordre quadràtic de discriminant el discriminant $D = 1 - 4k$ del polinomi té nombre de classes 1.*

  Demostració. [12] □

  Per tant, 1, 2, 3, 5, 11, 17 i 41 són els únics nombres amb aquesta propietat.

4.3 El càlcul final

Ens falta demostrar el lema que hem utilitzat a la demostració del teorema de Heegner-Baker-Stark.

Teorema 4.2.1. *Les solucions enteres de l'equació diofantina $2X(X^3 + 1) = Y^2$ són $(0, 0), (-1, 0), (1, \pm 2), (2, \pm 6)$.*

Demostració. Sigui (x, y) una solució entera. Com que x i $x^3 + 1$ són relativament primers, de $2x(x^3+1) = y^2$ obtenim que $\pm(x^3+1)$ és un quadrat o el doble d'un quadrat. Per tant, (x, y) dóna una solució entera a alguna d'aquestes equacions:

(a) $X^3 + 1 = Z^2$,

(b) $X^3 + 1 = -Z^2$,

(c) $X^3 + 1 = 2Z^2$,

(d) $X^3 + 1 = -2Z^2$,

Trobem-ne totes les solucions enteres. Treballarem en els anells $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-2}]$ i $\mathbb{Z}[\omega]$, on $\omega := e^{2\pi i/3}$, que són dominis euclidians i, per tant, de factorització única.

(a) Sigui (x, z) una solució de l'equació $X^3 + 1 = Z^2$. Observem que

$$\begin{cases} (1-z)(1+z)(-2) = -2(1-z^2) = 2x^3, \\ (1-z) + (1+z) + (-2) = 0. \end{cases}.$$

Utilitzarem el lema següent.

Lema 4.3.1. *Siguin $A, B, C \in \mathbb{Z}[\omega]$ no nuls tals que ABC és el doble d'un cub i $A + B + C = 0$. Aleshores, A, B i C no poden ser els tres diferents.*

Demostració. Suposem que existeixen tres nombres diferents A, B i C que compleixen la hipòtesi del lema. De totes les ternes (A, B, C) possibles, n'escollim una que faci que $d = \min(|A|, |B|, |C|)$ sigui mínim. En particular, tenim que A, B, C són coprimers dos a dos, de manera que, com que ABC és un cub, podem suposar que $A = 2ar^3, B = bs^3, C = ct^3$ on $a, b, c \in \mathbb{Z}[\omega]^* = \{1, \omega, \omega^2\}$ i $r, s, t \in \mathbb{Z}[\omega]$.

Tots els cubs de $\mathbb{Z}[\omega]$ són congru amb 0 o 1 mòdul 2, i com que $A \equiv 0 \mod 2$ tenim que $B, C \equiv 1 \mod 2$. Com que $b + c \equiv B + C = -A \equiv 0 \mod 2$, tenim que $b \equiv c \mod 2$, i per tant $b = c$, ja que $1, \omega, \omega^2$ són tots diferents mòdul 2. Com que $ABC = (abc)(rst)^3$ és un cub, tenim que $abc = 1$ i per tant $a = b = c$. Podem suposar que $a = b = c = 1$.

Per tant, $A = 2r^3, B = s^3, C = t^3$. Podem suposar multiplicant per una unitat que $s, t \equiv 1 \mod 2$. Observem que $|s|, |t| < \sqrt[3]{d}$. Siguin

$$A' = s + t, \qquad B' = \omega s + \omega^2 t, \qquad C' = \omega^2 s + \omega t.$$

La seva suma és 0 i el seu producte és $B + C = 2(-r)^3$. $B' \neq C'$, ja que $s \neq t$, i A' no pot ser igual a cap dels altres dos $A' \equiv 0 \mod 2$ i $B', C' \equiv 1 \mod 2$. A més, $|A'|, |B'|, |C'| \leq |s| + |t| < 2\sqrt[3]{d} < d$, la qual cosa contradiu la minimalitat de A, B, C. □

Per tant, tenim que o bé dos de $1 + z, 1 - z, -2$ són iguals, o bé que un dels tres és zero. Separem casos:

- Si $1 + z = 1 - z$, aleshores $z = 0$. En aquest cas, $x = -1$.
- Si $1 + z = -2$, aleshores $z = -3$. En aquest cas, $x = 2$.
- Si $1 - z = -2$, aleshores $z = 3$. En aquest cas, $x = 2$.
- Si $1 + z = 0$, aleshores $z = -1$. En aquest cas, $x = 0$.
- Si $1 - z = 0$, aleshores $z = 1$. En aquest cas, $x = 0$.

Per tant, totes les solucións (x, z) de l'equació són $(0, \pm 1), (-1, 0), (2, \pm 3)$.

(b) En aquest cas treballarem a l'anell $\mathbb{Z}[i]$. Sigui (x, z) una solució de l'equació $X^3 + 1 = -Z^2$. Aleshores $-x^3 = z^2 + 1 = (z + i)(z - i)$.

Veiem que $z+i$ i $z-i$ són relativament primers. Sigui $d = \text{mcd}(z+i, z-i)$, i suposem que no és una unitat. Com que $d|(z+i)$ i $d|(z-i)$, tenim que $d|i((z-i)-(z+i)) = 2$. Com que d divideix a $(z + i)(z - i) = -x^3$, tenim que d divideix a x^3, de manera que x ha de ser parell, ja que $d|2$. Però aleshores de $z^2 + 1 = -x^3$ obtenim que $z^2 + 1 \equiv 0 \mod 8$, la qual cosa no és possible.

Per tant, com que $(z + i)(z - i) = (-x)^3$, tenim que $z + i$ i $z - i$ han de ser cubs a $\mathbb{Z}[i]$. Posem $z+i = (a+bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i$. Aleshores, $b(3a^2 - b^2) = 1$, i llavors $a = 0$ i $b = -1$. Aleshores, $z + i = -i^3 = i$, de manera que $z = 0$ i $x = -1$.

(c) Si $x^3+1=2z^2$, aleshores tenim que $4xz^2=y^2$, de manera que x ha de ser un quadrat, $x=t^2$. Per tant, resoldrem l'equació $T^6+1=2Z^2$.

De nou, treballarem a $\mathbb{Z}[\omega]$. Recordem que la norma euclidiana d'aquest anell és $N(a+b\omega)=a^2-ab+b^2$. Sigui (t,z) una solució entera de $T^6+1=2Z^2$. Com que $t^6+1=2z^2$ és parell, tenim que t és senar.

Observem que $t^6+1=(t^2+1)(t^2+\omega)(t^2+\omega^2)$. Veiem que aquests factors són coprimers dos a dos. Suposem que $d\in\mathbb{Z}[\omega]$ divideix a t^2+1 i a $t^2+\omega$. Aleshores d divideix a $(t^2+1)-(t^2+\omega)=1-\omega$. Per tant, $N(d)|N(1-\omega)=3$. Com que d no és una unitat, tenim que $N(d)=3$. Per tant $3|N(t^2+1)=t^4+2t^2+1$, però això no es compleix per a cap $t\in\mathbb{Z}$. Amb arguments similars obtenim que t^2+1 i $t^2+\omega^2$ i que $t^2+\omega$ i $t^2+\omega^2$ són coprimers.

Com que $(t^2+1)(t^2+\omega)(t^2+\omega^2)=2z^2$, dos dels factors han de ser un quadrat per ±1 i l'altre un quadrat per ±2. Si tinguessim $t^2+1=\pm k^2$ amb $k\in\mathbb{Z}[\omega]$, com que $t\in\mathbb{Z}$ tindríem que $k\in\mathbb{Z}$. L'equació $t^2+1=-k^2$ no té solucions, i la única solució de $t^2+1=k^2$ és $(t,k)=(0,\pm1)$, però t ha de ser senar.

Per tant, t^2+1 ha de ser un quadrat per ±2, de manera que $t^2+\omega, t^2+\omega^2$ són un quadrat per ±1.

Si $t^2+\omega=+(a+b\omega)^2$, tenim que

$$a^2-b^2=1, \qquad b(2a-b)=1.$$

Les solucions de la primera equació són $(\pm1,0)$, però aquestes no satisfan la segona.

Si $t^2+\omega=-(a+b\omega)^2$, tenim que

$$a^2-b^2=-1, \qquad b(2a-b)=-1.$$

Les solucions de la primera equació són $(0,\pm1)$, i aquestes també són solucions de la segona equació.

Per tant, $t^2+\omega=-\omega^2$, de manera que $t=\pm1$ i $z=\pm1$. Com que $x=t^2$, les úniques solucions de $X^3+1=2Z^2$ són $(1,\pm1)$.

(d) Repetirem l'argument del cas (b), però en aquest cas treballarem a l'anell $\mathbb{Z}[\sqrt{-2}]$. Sigui (x,z) una solució de l'equació $X^3+1=-2Z^2$. Aleshores, $-x^3=2z^2+1=(1+z\sqrt{-2})(1-z\sqrt{-2})$.

Veiem que $1+z\sqrt{-2}$ i $1-z\sqrt{-2}$ són relativament primers. Suposem que $d=\mathrm{mcd}(1+z\sqrt{-2},1-z\sqrt{-2})$ no és una unitat. Com que $d|1+z\sqrt{-2}$ i $d|1-z\sqrt{-2}$, tenim que $d|(1+z\sqrt{-2})+(1-z\sqrt{-2})=2$. Com que d divideix a $(1+z\sqrt{-2})(1-z\sqrt{-2})=-x^3$, tenim que 2 divideix a $-x^3$, i per tant x ha de ser parell. D'altra banda, però, de $2z^2=x^3+1$ s'obté que és senar, la qual cosa contradiu el que acabem de veure.

Per tant, com que $(1+z\sqrt{-2})(1-z\sqrt{-2})=(-x)^3$, tenim que els dos factors han de ser cubs a $\mathbb{Z}[\sqrt{-2}]$. Posant $1+z\sqrt{-2}=(a+b\sqrt{-2})^3$ amb a,b enters i igualant els coeficients, obtenim que $a(a^2-6b^2)=1$ Per tant, hem de tenir que $a=1,b=0$, de manera que $z=0$ i $x=1$.

Així, si (x,y) és una solució de l'equació original, $2X(X^3+1)=Y^2$, aleshores $x\in\{-1,0,1,2\}$. Com que $y=\pm\sqrt{2x(x^3+1)}$, les úniques solucions són $(-1,0),(0,0),(1,\pm2),(2,\pm6)$. □

4.4 Més enllà

Ara que ja hem resolt el problema del nombre de classes 1, ens podem plantejar una versió més general: el problema del nombre de classes n.

Problema 4.4.1. Sigui $n \geq 1$ un enter. Per a quins discriminants $D < 0$ es té $h(D) = n$?

Recordem que Gauss va conjecturar que $h(D) \to \infty$ quan $D \to -\infty$. Això implicaria que, per a un enter n, existeix com a molt un nombre finit de discriminants de nombre de classes n. El primer pas cap a una demostració d'aquesta conjectura va ser fet per Hecke. Per a entendre'l, abans hem de definir alguns conceptes.

Un caràcter de Dirichlet mòdul un enter $m > 1$ és un morfisme de grups $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$. Un caràcter de Dirichlet mòdul m s'anomena primitiu si no factoritza a través de $(\mathbb{Z}/n\mathbb{Z})^*$ per a cap factor n de m, s'anomena real si la seva imatge està continguda en $\mathbb{R}$, i s'anomena senar si $\chi(-a) = -\chi(a)$ per a tot a.

Podem estendre un caràcter de Dirichlet a $\mathbb{Z}$ definint $\chi(a) = 0$ si $\mathrm{mcd}(a, m) > 1$. Donat un caràcter de Dirichlet χ, la funció L associada a χ és $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ per a $s \in \mathbb{C}$. Aquesta sèrie convergeix per a tot s tal que $\mathrm{Re}\, s > 1$, i admet una prolongació analítica meromorfa a tot el pla complex, que també denotem per $L(\chi, s)$.

Teorema 4.4.2 (Hecke, 1918)**.** *Sigui $D < 0$, i χ un caràcter de Dirichlet mòdul D que és real, primitiu i senar. Suposem que $L(\chi, s) \neq 0$ per a tot s real tal que $s > 1 - c/\log|D|$ per a una certa constant c que no depèn de D. Aleshores, si la hipòtesi generalitzada de Riemann és certa, existeix una constant c_1 que no depèn de D i tal que*

$$h(D) > c_1 \sqrt{|D|}/\log|D|.$$

Tot i això, aquest teorema suposa que la hipòtesi generalitzada de Riemann, que afirma que per a qualsevol caràcter de Dirichlet χ i nombre complex s tals que $L(\chi, s) = 0$ i $0 \leq \mathrm{Re}\, s \leq 1$ es té $\mathrm{Re}\, s = \frac{1}{2}$, és certa. Aquesta hipòtesi encara no ha estat demostrada o rebutjada.

Teorema 4.4.3 (Heilbronn, 1934)**.** *Si la hipòtesi de Riemann generalitzada és falsa, aleshores $h(D) \to \infty$ quan $D \to -\infty$.*

Així, tant si la hipòtesi. Des d'aleshores s'ha arribat a resultats més precisos.

Teorema 4.4.4 (Siegel, 1935)**.** $\lim\limits_{d_K \to \infty} \frac{\log h(d_K)}{\log |d_K|} = \frac{1}{2}$. *En particular, per a tot $\varepsilon > 0$ existeix una constant $C(\varepsilon)$ tal que $h(d_K) > C(\varepsilon)|d_K|^{\frac{1}{2}-\varepsilon}$ (per a $d_K < 0$).*

Malauradament, actualment no es tenen prou coneixements per a poder calcular les constants $C(\varepsilon)$ explícitament. Tot i així, existeixen altres cotes explícites.

Teorema 4.4.5 (Oesterlé, 1984)**.**

$$h(D) > \frac{1}{7000} \log|D| \prod_{p|D, p \neq D} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right)$$

Corol·lari 4.4.6. $|d_K| \leq \exp(21000 \cdot 2^{2+\nu_2(h(d_K))} h(d_K))$, *on ν_2 denota la valoració 2-àdica.*

Actualment, es coneixen tots els cossos quadràtics imaginaris de nombre de classes n per a $n \leq 100$. En un article publicat el 2004, Mark Watkins va trobar una cota superior per als possibles discriminants suficientment bona per a reduir el problema a un nombre de comprovacions suficientment petit per a que fos factible dur-les a terme amb l'ajuda d'ordinadors.

Apèndixs

A Programa per a calcular el nombre de classes

El programa següent en C conté una funció $h(D)$ que calcula el nombre de classes d'un discriminant negatiu donat D.

```
#include <stdio.h>
#include <math.h>

int gcd(int a, int b){
    if(a < 0) a = -a;
    if(b < 0) b = -b;
    if(a < b){
        int tmp = a;
        a = b;
        b = tmp;
    }
    while(b != 0){
        int d = a%b;
        a = b;
        b = d;
    };
    return a;
}

int h(int D){
    int a, b, c;
    int cota_superior_a = (int)(sqrt(-D/3.));
    int total = 0;
    for(a=1; a<=cota_superior_a; a++){
        for(b=-a; b<=a; b++){
            // De D = b^2 - 4ac deduim que c = (b^2-D)/4a. En particular, b^2-D ha de ser un múltiple de a
            if((b*b-D) % (4*a) != 0)
                continue;
            c = (b*b-D) / (4*a);

            // Per a que la forma sigui reduïda, hem de tenir a <= c
            if(a > c)
                continue;

            // Si a == c o a == |b|, aleshores ha de ser b >= 0
            if(a == c || a == b || a == -b)
                if(b < 0)
                    continue;

            // a,b,c han de ser coprimers
            if(gcd(a, gcd(b, c)) > 1)
                continue;
            total++;
        }
    }
    return total;
}
int main(){
    int D, h_D;

    D = -1;
    while(1){
        h_D = h(D);
        if(h_D != 0){
            printf("h(%i) = %i\n", D, h_D);
        }
        D--;
    }

    return 0;
}
```

B Taula del nombre de classes d'ordres de discriminant negatiu

$-D$	$h(D)$	$-D$	$h(D)$	$-D$	$h(D)$	$-D$	$h(D)$	$-D$	$h(D)$	$-D$	$h(D)$	$-D$	$h(D)$
3	1	92	3	183	8	272	8	363	4	452	8	543	12
4	1	95	8	184	4	275	4	364	6	455	20	544	8
7	1	96	4	187	2	276	8	367	9	456	8	547	3
8	1	99	2	188	5	279	12	368	6	459	6	548	8
11	1	100	2	191	13	280	4	371	8	460	6	551	26
12	1	103	5	192	4	283	3	372	4	463	7	552	8
15	2	104	6	195	4	284	7	375	10	464	12	555	4
16	1	107	3	196	4	287	14	376	8	467	7	556	9
19	1	108	3	199	9	288	4	379	3	468	8	559	16
20	2	111	8	200	6	291	4	380	8	471	16	560	12
23	3	112	2	203	4	292	4	383	17	472	6	563	9
24	2	115	2	204	6	295	8	384	8	475	4	564	8
27	1	116	6	207	6	296	10	387	4	476	10	567	12
28	1	119	10	208	4	299	8	388	4	479	25	568	4
31	3	120	4	211	3	300	6	391	14	480	8	571	5
32	2	123	2	212	6	303	10	392	8	483	4	572	10
35	2	124	3	215	14	304	6	395	8	484	6	575	18
36	2	127	5	216	6	307	3	396	6	487	7	576	8
39	4	128	4	219	4	308	8	399	16	488	10	579	8
40	2	131	5	220	4	311	19	400	4	491	9	580	8
43	1	132	4	223	7	312	4	403	2	492	6	583	8
44	3	135	6	224	8	315	4	404	14	495	16	584	16
47	5	136	4	227	5	316	5	407	16	496	6	587	7
48	2	139	3	228	4	319	10	408	4	499	3	588	6
51	2	140	6	231	12	320	8	411	6	500	10	591	22
52	2	143	10	232	2	323	4	412	5	503	21	592	4
55	4	144	4	235	2	324	6	415	10	504	8	595	4
56	4	147	2	236	9	327	12	416	12	507	4	596	14
59	3	148	2	239	15	328	4	419	9	508	5	599	25
60	2	151	7	240	4	331	3	420	8	511	14	600	8
63	4	152	6	243	3	332	9	423	10	512	8	603	4
64	2	155	4	244	6	335	18	424	6	515	6	604	7
67	1	156	4	247	6	336	8	427	2	516	12	607	13
68	4	159	10	248	8	339	6	428	9	519	18	608	12
71	7	160	4	251	7	340	4	431	21	520	4	611	10
72	2	163	1	252	4	343	7	432	6	523	5	612	8
75	2	164	8	255	12	344	10	435	4	524	15	615	20
76	3	167	11	256	4	347	5	436	6	527	18	616	8
79	5	168	4	259	4	348	6	439	15	528	8	619	5
80	4	171	4	260	8	351	12	440	12	531	6	620	12
83	3	172	3	263	13	352	4	443	5	532	4	623	22
84	4	175	6	264	8	355	4	444	8	535	14	624	8
87	6	176	6	267	2	356	12	447	14	536	14	627	4
88	2	179	5	268	3	359	19	448	4	539	8	628	6
91	2	180	4	271	11	360	8	451	6	540	6	631	13

Referències

[1] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, New York, 1989. ISBN: 0-471-50654-0.

[2] Gerald J. Janusz. *Algebraic Number Fields*. Academic Press, New York, 1973. ISBN: 0-12-380250-4.

[3] Segre Lang. *Elliptic Curves: Diophantine Analysis*. Springer-Verlag, Berlin Heidelberg New York, 1978. ISBN: 3-540-08489-4.

[4] Jean-Pierre Serre. *A course in Arithmetic* (Títol original: *Cours d'Arithmétique*). Springer-Verlag, New York, 1973. ISBN: 0-387-900-40-3.

[5] Carl Friedrich Gauss *Disquisicions Aritmètiques* (Títol original: *Disquisitiones Arithmeticae*). Societat Catalana de Matemàtiques, Barcelona, 1996. ISBN: 84-7283-313-5.

[6] Heinrich Weber. *Lehrbuch der Algebra*. Chelsea Publishing Company, New York, 1961. 3rd edition, reprint, with corrections (and some change of notations).

[7] Artur Travesa Grau. *Teoria de nombres*. Apunts de l'assignatura *Mètodes algebraics en teoria de nombres*. Universitat de Barcelona.

[8] Artur Travesa Grau. *Corbes el·líptiques amb multiplicació complexa i teoria de cossos de classes*. Capítol 3, p. 43-82 del llibre *Varietats abelianes amb multiplicació complexa*. Notes del Seminari de Teoria de Nombres (UB-UAB-UPC) volum 6, Barcelona, 200. ISBN: 84-923250-5-4.

[9] David S. Dummit, Richard M. Foote *Abstract Algebra*. Wiley, New York, 1973. ISBN: 0-471-43334-9.

[10] Mark Watkins. *Class numbers of imaginary quadratic fields.* Mathematics of Computation 73, 2004, p. 907-938.

[11] Harold Stark. *On the "gap" in a theorem of Heegner.* Journal of Number Theory 1(1), 1969, p. 16-27.

[12] Daniel Fendel. *Prime-Producing Polynomials and Principal Ideal Domains.* Mathematics Magazine Vol. 58, No. 4, 1985, p. 204-210.

[13] Jean-Pierre Serre. $\Delta = b^2 - 4ac$. Mathematical Medley 13(1), 1985, p. 1-10.