Growth Rate of the Class Number of Imaginary Quadratic Fields

William Zhang

Euler Circle

July 17, 2023

Overview

- The class number problem for quadratic fields was formulated by Gauss in his book *Disquisitiones Arithmeticae* [Gau01], written in 1798 when Gauss was 21 years old
- It has wide connections to number theory, algebra, analysis and a long history of results and theory development.
- It still attracts mathematicians' attention to this day

In this talk, we'll

- Introduce the background of the Gauss class number problem
- Present Dirichlet's class number formula for imaginary quadratic fields
- Outline the historical development of the works on the lower bound for the class number of imaginary quadratic fields, including the landmark Siegel's theorem and the Goldfeld-Gross-Zagier theorem, the first general result with an effective constant.

The Start

$x^2 - x + 41$ is a prime for all $x \in \{1, 2, \cdots, 40\}$ (Euler 1772) [Eul72]

$x^2 + x + 41$ is a prime for all $x \in \{0, 1, 2, \cdots, 39\}$ (Legendre 1798)

Theorem

(Rabinovitch) $D < 0, D \equiv 1$(mod 4),

$$x^2 - x + \frac{1+|D|}{4} \textit{ is a prime for all } x \in \{1, 2, \cdots, \frac{|D|-3}{4}\},$$

if and only if every integer of the field $\mathbb{Q}(\sqrt{D})$ has unique factorization into product of primes.

- -163 is the discriminant
- $\mathbb{Q}(\sqrt{-163})$ has the unique factorization property.
- -163 is one of nine so-called Heegner numbers.

Binary Quadratic Forms

In *Disquisitiones Arithmeticae*, Gauss works with binary quadratic forms:

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

The discriminant of the form is $d = b^2 - 4ac$. We consider only $d < 0$, in particular, the *fundamental discriminants*, where $d \equiv 1 \pmod 4$ is square-free or $d = 4n$ where $n \equiv 2, 3 \pmod 4$ is square-free (every form is equivalent to one such).

- $f(x, y)$ is called primitive when $gcd(a, b, c) = 1$
- $f(x, y)$ a positive-definite form if $f(x, y) \geq 0$ for all (x, y) (negative-definite if $f(x, y) \leq 0$ for all (x, y) and indefinite if neither positive- nor negative-definite).
- Two forms $f(x, y)$ and $g(x', y')$ are called equivalent, denoted as $f(x, y) \sim g(x', y')$, if there is a matrix in $SL_2(\mathbb{Z})$ such that

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{ and } ps - qr = 1.$$

Binary Quadratic Forms - *cont.*

- It can be shown that two forms are equivalent iff they represent the same set of integers (Lagrange 1773).
- Any two equivalent forms $f(x,y) \sim g(x,y)$ have the same discriminant.
- Let $f(x,y)$ be a form with discriminant $b^2 - 4ac < 0$. Then $f(x,y)$ is either positive- or negative-definite, as determined by the sign of a.
- A form $f(x,y)$ is reduced if $|b| \leq a \leq c$ and $b \geq 0$ if either $a = |b|$ or $a = c$.

It follows that every primitive, positive-definite form is equivalent to a canonical unique reduced form.

Definition

The *class number* for integer d, denoted $h(d)$, is the number of nonequivalent forms $f(x,y)$ with discriminant $d = b^2 - 4ac$.

Class Number Is Positive and Finite

For a reduced form, $-d = 4ac - b^2 \geq 3a^2 \implies |b| \leq a \leq \sqrt{\frac{-d}{3}}$. This implies that $h(d)$ is finite. Furthermore, since $d \equiv b^2 \equiv 0$ or $1 \pmod 4$, the following provides at least one binary quadratic form of discriminant d for any valid d, called the *principal form*:

$$\begin{cases} x^2 - \frac{1}{4}dy^2 & \text{if } d \equiv 0 \pmod 4 \\ x^2 + xy - \frac{1}{4}(d-1)y^2 & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{0.1}$$

Hence $h(d)$ is a positive integer, and together we get the following:

Theorem

[Cox22] For fixed d, the number $h(d)$ of primitive, positive-definite forms of discriminant d is positive and finite. Further, $h(d)$ is equal to the number of reduced forms of discriminant d.

The Gauss Class Number Problem

In the *Disquisitiones Arithmeticae* (1801) [Gau01], Gauss showed (using the language of binary quadratic forms) that $h(d)$ is finite. He conjectured

1. $h(d) = 1$ for $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$ and no others for $d < -163$, known as **Gauss' class number one problem**,
2. $\lim_{d \to -\infty} h(d) = \infty$,
3. There are infinitely many real quadratic fields with class number one (still an open problem!)

This set off a race of more than 200 years of finding an effective algorithm to determine all imaginary quadratic fields with a given class number h, known as the **Gauss class number problem**.

Connection to Abstract Algebra

- Given the form $f(x, y) = ax^2 + bxy + cy^2$ with $d < 0$, consider the *fractional ideal* $< a, \frac{-b+\sqrt{d}}{2} >$ of the algebraic integer subring of $\mathbb{Q}(\sqrt{d})$ ("fractional" because $< a, \frac{-b+\sqrt{d}}{2} >$ is not but $2 < a, \frac{-b+\sqrt{d}}{2} >$ is contained in the algebraic integer subring when b or d is odd).
- Two ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent, denoted as $\mathfrak{a} \sim \mathfrak{b}$, if $\exists$ principal ideals $(\lambda_1), (\lambda_2)$ such that $\mathfrak{a}(\lambda_1) = \mathfrak{b}(\lambda_2)$.
- It can be shown that equivalent ideals of the ideal generated from $f(x, y)$ above correspond to equivalent forms of $f(x, y)$.
- These ideal classes of $\mathbb{Q}(\sqrt{d})$ form a group, *i.e.*, the quotient group of $\{$nonzero fractional ideals$\}/\{$principal fractional ideals$\}$, called *ideal class group*, with order $h(d)$.
- When $h(d) = 1$, every ideal in $\mathbb{Q}(\sqrt{d})$ is principal, thus a principal ideal domain, and the algebraic integers of $\mathbb{Q}(\sqrt{d})$ have unique factorization.

Legendre and Kronecker Symbols

Definition

Legendre symbol: Let a be an integer and p be a prime.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \not\equiv 0 \text{ and } a \text{ is a quadratic residue} \pmod{p} \\ -1, & \text{if } a \text{ is not a quadratic residue} \pmod{p} \\ 0, & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

- Legendre symbol satisfies the quadratic reciprocity law

Definition

Kronecker symbol: Let n be a non-zero integer, with prime factorization $n = u \cdot p_1^{e_1} \cdots p_k^{e_k}$, where u is a unit (± 1). Let a be an integer. Define the Kronecker symbol $\left(\frac{a}{n}\right)$ recursively as

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

Legendre and Kronecker Symbols - *cont.*

For odd p_i, the number $\left(\frac{a}{p_i}\right)$ is simply the usual Legendre symbol. When $p_i = 2$, we define $\left(\frac{a}{2}\right)$ by

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } a \text{ is even} \\ 1, & \text{if } a \equiv \pm 1 \pmod 8 \\ -1, & \text{if } a \equiv \pm 3 \pmod 8 \end{cases}.$$

For $u = 1$, $\left(\frac{a}{1}\right) = 1$. For $u = -1$ and $n = 0$, we define as

$$\left(\frac{a}{-1}\right) = \begin{cases} -1, & \text{if } a < 0 \\ 1, & \text{if } a \geq 0 \end{cases} \qquad \left(\frac{a}{0}\right) = \begin{cases} 1, & \text{if } a = \pm 1 \\ 0, & \text{otherwise} \end{cases}$$

- Kronecker symbol generalizes the Jacobi symbol and satisfies its own quadratic reciprocity law.

Dirichlet Character

When Euler proved (1748) that there are infinitely many primes, he used the so-called Euler product

$$\sum_{1}^{\infty} \frac{1}{n} = \prod_{p \ \ prime} \sum_{k=0}^{\infty} \frac{1}{p^k} = \prod_{p \ \ prime} (1 - \frac{1}{p})^{-1}.$$

When Dirichlet proved that there are infinitely many primes in the arithmetic progression

$$a, a+q, a+2q, \cdots, \text{where } (a, q) = 1,$$

similar product $\prod_{p \equiv a \pmod{q}} (1 - \frac{1}{p})^{-1}$ could not be directly used as there is no known equality like the harmonic series. Dirichlet remedied the problem with the *Dirichlet character*.

Dirichlet Character - *cont.*

Definition

Dirichlet Character: A complex-valued arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character of modulus m (where m is a positive integer) if for all integers a and b:

1. $\chi(ab) = \chi(a)\chi(b)$; that is, χ is completely multiplicative.
2. $\chi(a) \begin{cases} = 0 & \text{if } \gcd(a, m) > 1 \\ \neq 0 & \text{if } \gcd(a, m) = 1. \end{cases}$
3. $\chi(a + m) = \chi(a)$; that is, χ is periodic with period m.

- The simplest possible character, called the principal character, usually denoted χ_0, exists for all moduli: $\chi_0(a) = \begin{cases} 0 & \text{if } \gcd(a, m) > 1 \\ 1 & \text{if } \gcd(a, m) = 1. \end{cases}$
- Real-valued characters are just Kronecker symbols

Dirichlet L-function

With a character χ, Dirichlet defined the L-function:

Definition

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_{p\ \ prime}\sum_{k=0}^{\infty}\frac{(\chi(p))^k}{(p^s)^k}=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}(Re(s)>1)$$

Before introducing Dirichlet's class number formula, we also need to look at the automorphs - $SL_2(\mathbb{Z})$ transformations keeping a form unchanged:

- Always two trivial automorphs, identity and its negative: $x=x',y=y'$; $x=-x',y=-y'$.
- If $d<0$, no others except for $d=-3$ or -4. For both, only the principal form. If $d=-3$, it is x^2+xy+y^2 with 4 more: $x=-y',y=x'+y'$; $x=x'+y',y=-x'$ and their negatives.
- If $d=-4$, it is x^2+y^2 with 2 more: $x=y',y=-x'$ and its negative.

Dirichlet's Class Number Formula

Let $w(d)$ denote the number of automorphs on a form of a given d. We have:

$$w(d) = \begin{cases} 2 & \text{if } d < -4 \\ 4 & \text{if } d = -4 \\ 6 & \text{if } d = -3 \end{cases} \tag{0.2}$$

Theorem

(Dirichlet's class number formula) [LD39] Let $d < 0$ be a fundamental discriminant and χ be the $\pmod{d}$ Kronecker symbol ($\chi(m) = \left(\frac{d}{m}\right)$). Then

$$h(d) = \frac{w(d)\sqrt{|d|}}{2\pi} L(1, \chi), \tag{0.3}$$

$$L(1, \chi) = -\frac{\pi}{|d|^{\frac{3}{2}}} \sum_{m=1}^{|d|-1} m \left(\frac{d}{m}\right). \tag{0.4}$$

Dirichlet's Class Number Formula - *cont.*

Combining the two formulas above gives the following finite sum of Kronecker symbols for $h(d)$ with $d < 0$:

$$h(d) = -\frac{w(d)}{2|d|} \sum_{m=1}^{|d|-1} m \left(\frac{d}{m} \right)$$

Examples

1. $d = -3, w(d) = 6, h(d) = -\frac{6}{2 \cdot 3} \sum_{m=1}^{2} m \left(\frac{-3}{m} \right) = -1(1 \left(\frac{-3}{1} \right) + 2 \left(\frac{-3}{2} \right)) = -1(1 \cdot 1 + 2 \cdot (-1)) = -1(-1) = 1.$ Therefore, the algebraic integers of $\mathbb{Q}(\sqrt{-3})$ form a PID, and its integers have unique factorizations.
2. For $\mathbb{Q}(\sqrt{-5})$, the fundamental discriminant $d = -20$ ($-5 \equiv 3 \pmod 4$), and similarly $h(-20) = 2$, so the algebraic integers of $\mathbb{Q}(\sqrt{-5})$ do not form a PID, and its integers may have multiple factorizations. For example, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Siegel's Theorem

In 1934, Heilbronn [Hei34] proved part of the Gauss class number conjecture:

$$\lim_{d \to -\infty} h(d) = \infty.$$

(Heilbronn proved this under the assumption of falsity of the generalized Riemann hypothesis while Hecke (1918) did it under the opposite assumption!)
In 1935, Siegel proved the following beautiful result about the growth rate of $h(d)$.

Theorem

(Siegel) [Sie35] Let $\mathbb{Q}(\sqrt{d})$, $d < 0$ be a quadratic field, and h(d) denote its class number. For every $\epsilon > 0$, we have

$$h(d) > C_\epsilon |d|^{\frac{1}{2}-\epsilon}$$

for some constant $C_\epsilon > 0$.

Siegel's Theorem - *cont.*

- Eastermann [Est48] (1948) has a short analytical proof.
- See Goldfeld [Gol74] (1974) for a short half-page proof.

Siegel's theorem gives a landmark result on the lower bound of the class number with respect to the magnitude of the discriminant. However, it has an *ineffective* constant C_ϵ in that, given ϵ, there is no way of computing a constant value that makes the inequality hold even though it exists.

Therefore, even with these results and the Dirichlet class number formula, we were still far from solving even the Gauss class number one problem.

The first important milestones were obtained by Heegner [Hee52] (1952), Stark [Sta67] (1967), Baker [Bak71] (1971), and Stark [Sta72] (1972), whose work led to the solution of the class number one and two problems.

Goldfeld-Gross-Zagier Theorem

The general Gauss class number problem was finally solved completely, at least theoretically, by Goldfeld–Gross–Zagier (Goldfeld [Gol76] (1975) and [Gol85] (1985), Gross and Zagier [GZ85] (1985)) in 1985. Their results combined to reduce the problem of finding all the $d < 0$'s with given $h(d)$ to a finite amount of computation in applying the Dirichlet class number formula.

Theorem

(Goldfeld-Gross-Zagier)[Gol85] For every $\epsilon > 0$ *there exists an effective computable constant* $c > 0$ *such that* $h(d) > c(\log(|d|)^{1-\epsilon}$.

Even though the GGZ theorem reduces the order of magnitude of the lower bound on the class number from almost $|d|^{\frac{1}{2}}$ to less than $\log(|d|)$, it gives an *effective* constant, which can be computed given ϵ.
Its *effectiveness* can be seen in that it can be utilized to limit the possible $d's$ to a finite number of choices, given a fixed class number.

The Current State

- Oesterl´e in 1985 [Oes88] improved the constant in GGZ that led to the solution of the class number 3 problem.
- Arno (1992) [Arn92] solved the class number four problem, and subsequently, work with Robinson and Wheeler (1998) [ARW98], and work of Wagner (1996) [Wag96] gave a solution to Gauss' class number problem for class numbers 5,6,7 and odd class numbers ≤ 23.
- Watkins (2004) [Wat04] obtained the complete list of all imaginary quadratic fields with class number ≤ 100 (the computation took seven months!).

It is worth noting that the Generalised Riemann Hypothesis implies that the class number $h(d)$ is at least

$$(1+o(1))\frac{\pi}{12e^{\gamma}}\frac{\sqrt{|d|}}{\log\log|d|}$$

by Littlewood (1928) [Lit28] (Paley (1932) [Pal32] has shown that this is best possible except for a factor of two).

Conclusion and Discussion

- The Gauss class number problem has been one of the main drivers in mathematical research for over 200 years in number theory, with wide connection to algebra and analysis, etc.
- Significant results such as Siegel's theorem and Goldfeld-Gross-Zagier theorem have been proven.
- Even though $h(d)$ grows approximately in the order of $|d|^{\frac{1}{2}}$, its constant is uncomputable, thus ineffective. The GGZ theorem gives a growth rate of approximately $\log(|d|)$ with a computable constant, thus effective.
- Complete lists of imaginary quadratic fields with class number ≤ 100 have been identified.

Future work: Can the order of growth be increased from log with an effective constant? Can the effective constant of the lower bound be increased? Compute the d's for $h(d) > 100$.

Acknowledgement

- Kishan Jani
- Dr. Simon Rubinstein-Salzedo
- Euler Circle
- All the guest speakers

REFERENCES

Steven Arno.
The imaginary quadratic fields of class number 4.
Acta Arithmetica, 60(4):321–334, 1992.

Steven Arno, M Robinson, and Ferrell Wheeler.
Imaginary quadratic fields with small odd class number.
Acta Arithmetica, 83(4):295–330, 1998.

Alan Baker.
Imaginary quadratic fields with class number 2.
Annals of mathematics, 94(1):139–152, 1971.

David A Cox.
Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions, volume 387.
American Mathematical Soc., 2022.

Th Estermann.
On dirichlet's l functions.

Journal of the London Mathematical Society, 1(4):275–279, 1948.

L. Euler.
Mém de berlin, année 1722, 36.
Comm. Arith., 1(584), 1772.

Carl Friedrich Gauss.
Disquisitiones Arithmeticae.
in commissis apud Gerh. Fleischer, jun., 1801.

Dorian M Goldfeld.
A simple proof of siegel's theorem.
Proceedings of the National Academy of Sciences, 71(4):1055–1055, 1974.

Dorian M Goldfeld.
The class number of quadratic fields and the conjectures of birch and swinnerton-dyer.
Annali della Scuola Normale Superiore di Pisa-Classe di Scienze, 3(4):623–663, 1976.

Dorian Goldfeld.
Gauss' class number problem for imaginary quadratic fields.
Bulletin of the American Mathematical Society, 13(1):23–37, 1985.

Benedict Gross and Don Zagier.
Heegner points and derivatives of l-series.
1985.

Kurt Heegner.
Diophantische analysis und modulfunktionen.
Mathematische Zeitschrift, 56(3):227–253, 1952.

Hans Heilbronn.
On the class-number in imaginary quadratic fields.
The Quarterly Journal of Mathematics, (1):150–160, 1934.

G Lejeune Dirichlet.
Recherches sur diverses applications de l'analyse infinitesimale à la théorie des nombres.
1839.

John E Littlewood.
On the class-number of the corpus p (- k).
Proceedings of the London Mathematical Society, 2(1):358–372, 1928.

Joseph Oesterlé.
Le problème de gauss sur le nombre de classes.
Enseign. Math, 34(1-2):43–67, 1988.

REAC Paley.
A theorem on characters.
Journal of the London Mathematical Society, 1(1):28–32, 1932.

Carl Siegel.
Über die classenzahl quadratischer zahlkörper.
Acta Arithmetica, 1(1):83–86, 1935.

Harold M Stark.
A complete determination of the complex quadratic fields of class-number one.
Michigan Mathematical Journal, 14(1):1–27, 1967.

Harold Mead Stark.
A transcendence theorem for class-number problems (ii).
Annals of Mathematics, 96(1):174–209, 1972.

Christian Wagner.
Class number 5, 6 and 7.
Mathematics of computation, 65(214):785–800, 1996.

Mark Watkins.
Class numbers of imaginary quadratic fields.
Mathematics of Computation, 73(246):907–938, 2004.