The Gauss Class Number One Problem

Evan Ashoori, Mira Lubashev, Muztaba Syed

December 8, 2024

Background

Definition

A **binary quadratic form** $\varphi(X, Y) = aX^2 + bXY + cY^2$ of discriminant $D = b^2 - 4ac < 0$ is *primitive* if $(a, b, c) = 1$.

We can also write

$$\varphi(X, Y) = a(X + z_a Y)(X + \overline{z_a} Y),$$

where $z_a = \frac{b+\sqrt{D}}{2a} \in \mathbb{C}$.

Background

We can perform a change of variables to primitive forms of discriminant D to get equivalent forms. For example, we say

$$\varphi(X, Y) = X^2 + Y^2$$

and

$$\varphi(X + Y, Y) = (X + Y)^2 + Y^2 = X^2 + 2XY + 2Y^2$$

are equivalent.

Background

We can perform a change of variables to primitive forms of discriminant D to get equivalent forms. For example, we say

$$\varphi(X, Y) = X^2 + Y^2$$

and

$$\varphi(X+Y, Y) = (X+Y)^2 + Y^2 = X^2 + 2XY + 2Y^2$$

are equivalent.

This defines equivalence classes of forms, each of which can be represented by one **reduced form** which is the "simplest".

Background

We can perform a change of variables to primitive forms of discriminant D to get equivalent forms. For example, we say

$$\varphi(X, Y) = X^2 + Y^2$$

and

$$\varphi(X + Y, Y) = (X + Y)^2 + Y^2 = X^2 + 2XY + 2Y^2$$

are equivalent.

This defines equivalence classes of forms, each of which can be represented by one **reduced form** which is the "simplest".

For each D, the number of reduced forms is finite. Under a composition defined by Dirichlet, these forms make up the **class group** (denoted by $\mathcal{H}$) which has order equal to the **class number** of a discriminant D (denoted by h).

Gauss Class Numbers Problem

$h(D)$	1	2	3	4	5
# of fields	9	18	16	54	25
largest $\|D\|$	163	427	907	1555	2683

For $h(D) = 1$:

D	-3	-4	-7	-8	-11	-19	-43	-67	-163

The Gauss class number h problem is to find an effective algorithm to determine all imaginary quadratic fields with class number h, which is needed to prove that this list is complete.

If an effective algorithm did not exist, then in fact the associated Dirichlet L-function would have a real zero, and the generalized Riemann Hypothesis would be false.

Class numbers and ideals

We will present an overview of the solution to the Gauss class number one problem.

For this we take a number theory approach, alternatively defining the class number of the number field $\mathbb{Q}(\sqrt{D})$ to be the size of the class group $\mathcal{H} = I/P$, where I is the group of non-zero fractional ideals and P is the subgroup of principal ideals.

Through a correspondence between the forms $\varphi(X, Y) = aX^2 + bXY + cY^2$ and primitive ideals $\mathfrak{a} = \left[a, \frac{b+\sqrt{D}}{2}\right]$ we see that these definitions of the class number are consistent.

Deuring–Heilbronn Phenomenon

The analog of a prime in $\mathbb{Q}$ for a general number field is a **prime ideal**. In a quadratic field $K = \mathbb{Q}(\sqrt{D})$, a prime p may factor into prime ideals. For example, $5 = (2+i)(2-i)$ in $\mathbb{Q}(\sqrt{-1})$. One of three things can occur for a prime p:

Deuring–Heilbronn Phenomenon

The analog of a prime in $\mathbb{Q}$ for a general number field is a **prime ideal**. In a quadratic field $K = \mathbb{Q}(\sqrt{D})$, a prime p may factor into prime ideals. For example, $5 = (2+i)(2-i)$ in $\mathbb{Q}(\sqrt{-1})$. One of three things can occur for a prime p:

1. p splits: $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, when the Kronecker character $\chi_D(p)$, which in this case is just the Legendre symbol $\left(\frac{D}{p}\right)$, is 1.

Deuring–Heilbronn Phenomenon

The analog of a prime in $\mathbb{Q}$ for a general number field is a **prime ideal**. In a quadratic field $K = \mathbb{Q}(\sqrt{D})$, a prime p may factor into prime ideals. For example, $5 = (2+i)(2-i)$ in $\mathbb{Q}(\sqrt{-1})$. One of three things can occur for a prime p:

1. p splits: $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, when the Kronecker character $\chi_D(p)$, which in this case is just the Legendre symbol $\left(\frac{D}{p}\right)$, is 1.
2. p is ramified: $(p) = \mathfrak{p}^2$, when $\chi_D(p) = 0$.

Deuring–Heilbronn Phenomenon

The analog of a prime in $\mathbb{Q}$ for a general number field is a **prime ideal**. In a quadratic field $K = \mathbb{Q}(\sqrt{D})$, a prime p may factor into prime ideals. For example, $5 = (2+i)(2-i)$ in $\mathbb{Q}(\sqrt{-1})$. One of three things can occur for a prime p:

1. p splits: $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, when the Kronecker character $\chi_D(p)$, which in this case is just the Legendre symbol $\left(\frac{D}{p}\right)$, is 1.
2. p is ramified: $(p) = \mathfrak{p}^2$, when $\chi_D(p) = 0$.
3. p is inert: (p) is a prime ideal in K, when $\chi_D(p) = -1$.

Deuring–Heilbronn Phenomenon

1. p splits: $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, when the Kronecker character $\chi_D(p)$, which in this case is just the Legendre symbol $\left(\frac{D}{p}\right)$, is 1.
2. p is ramified: $(p) = \mathfrak{p}^2$, when $\chi_D(p) = 0$.
3. p is inert: (p) is a prime ideal in K, when $\chi_D(p) = -1$.

Suppose K has class number one. Then if a prime p is not inert, we have $(p) = \pi \cdot \overline{\pi}$ for some $\pi = (\frac{m+n\sqrt{D}}{2})$. Thus

$$p = \frac{m^2 - n^2 D}{4} \implies p \geq \frac{1-D}{4}.$$

This implies that any $p < \frac{1-D}{4}$ is inert.

Prime Producing Polynomials

Theorem

If $h(D) = 1$*, then* $x^2 - x + \frac{1-D}{4}$ *is prime for all* $1 \leq x < \frac{1-D}{4}$.

Prime Producing Polynomials

Theorem

If $h(D) = 1$, then $x^2 - x + \frac{1-D}{4}$ is prime for all $1 \leq x < \frac{1-D}{4}$.

Proof.

Suppose $x^2 - x + \frac{1-D}{4}$ is not prime for some $1 \leq x < \frac{1-D}{4}$. Then there exists some prime $p < \frac{1-D}{4}$ dividing $x^2 - x + \frac{1-D}{4}$ so that

$$p \mid (4x^2 - 4x + 1 - D) = (2x-1)^2 - D.$$

Thus $\left(\frac{D}{p}\right) = 0$ or 1, which implies that p is not inert in $\mathbb{Q}(\sqrt{D})$, which is a contradiction. □

Prime Producing Polynomials

Theorem

If $h(D) = 1$, then $x^2 - x + \frac{1-D}{4}$ is prime for all $1 \leq x < \frac{1-D}{4}$.

Proof.

Suppose $x^2 - x + \frac{1-D}{4}$ is not prime for some $1 \leq x < \frac{1-D}{4}$. Then there exists some prime $p < \frac{1-D}{4}$ dividing $x^2 - x + \frac{1-D}{4}$ so that

$$p \mid (4x^2 - 4x + 1 - D) = (2x-1)^2 - D.$$

Thus $\left(\frac{D}{p}\right) = 0$ or 1, which implies that p is not inert in $\mathbb{Q}(\sqrt{D})$, which is a contradiction. □

For example, $h(-163) = 1$, so $x^2 - x + 41$ takes prime values for $x = 1, 2, \ldots, 40$.

Lower Bound on Class Number (Assuming GRH)

If we assume the Generalized Riemann Hypothesis, we can find a strong lower bound on the class number.
If $\chi : \mathcal{H} \to \mathbb{C}^*$ is a character of the class group of K (a function to $\{1, 0, -1\}$ with some restrictions), let

$$L_K(s, \chi) = \sum_{\mathfrak{a}} \chi(\mathfrak{a})(N\mathfrak{a})^{-s}.$$

Assuming that $L(s, \chi_D)$ has no real zeroes for $s > \frac{1}{2}$ (which is implied by the GRH), by the intermediate value theorem we have

$$L\left(\frac{1}{2}, \chi_D\right) \geq 0.$$

Lower Bound on Class Number (Assuming GRH)

Thus (note that $\zeta\left(\frac{1}{2}\right) < 0$)

$$L_K\left(\frac{1}{2}, \chi_D\right) = \zeta\left(\frac{1}{2}\right) L\left(\frac{1}{2}, \chi_D\right) \leq 0$$

from which we can show that $h(D) \gg |D|^{\frac{1}{4}} \ln |D|$, because the central value of $L_K(s, \chi_D)$ is explicitly related to $h(D)$. In fact, the implied constant is effectively computable! That is, one can find a c such that $\forall D,\ h(D) > c|D|^{\frac{1}{4}} \ln |D|$.

As a result, if an effective algorithm did not exist, then in fact the associated Dirichlet L-function would have a real zero, and the generalized Riemann Hypothesis would be false.

L-functions of Elliptic Curves with Triple Zeros

Since the Riemann hypothesis is unproven, we need a different approach. However, we can show the solution without assuming GRH using the theory of modular forms (special type of periodic function). The proof relies on the existence of a modular form whose L-function has a triple zero.

To find such a modular form, we must use the theory of elliptic curves. Letting E be an elliptic curve, we define the **Hasse-Weil L-function**

$$L(E;\ s) = \prod_{p \mid \Delta} (1 - a(p)p^{-s})^{-1} \prod_{p \nmid \Delta} (1 - a(p)p^{-s} + p^{1-2s})^{-1},$$

where $a(p) = p + 1 - |E(\mathbb{F}_p)|$ and $|E(\mathbb{F}_p)|$ is the number of solutions to the elliptic curve modulo p (including the point at infinity), and Δ is the discriminant of the elliptic curve.

Modularity Theorem

Wiles et al. proved that for all elliptic curves E, there exists some normalized newform, f, of weight 2 and level $N(E)$ such that $L(E\,;s) = L(f\,;s+\frac{1}{2})$ where

$$L(f\,;s) = \sum_{n\geq 1} a_f(n)n^{-s}$$

for some cusp form $f \in S_2(q,\chi)$ with Fourier expansion

$$f(z) = \sum_{n\geq 1} a_f(n)e^{2\pi inz}.$$

Modularity Theorem

Wiles et al. proved that for all elliptic curves E, there exists some normalized newform, f, of weight 2 and level $N(E)$ such that $L(E\,; s) = L(f\,; s + \frac{1}{2})$ where

$$L(f\,; s) = \sum_{n \geq 1} a_f(n) n^{-s}$$

for some cusp form $f \in S_2(q, \chi)$ with Fourier expansion

$$f(z) = \sum_{n \geq 1} a_f(n) e^{2\pi i n z}.$$

The details are less important for this presentation. The idea is that we can use knowledge about elliptic curves to learn about L-functions of modular forms.

(Wiles used this to prove Fermat's last theorem: $X^n + Y^n = Z^n$ has no positive integer solutions for $n \geq 3$.)

Functional Equation for $L(f, s)$

If we let

$$\Lambda(f;s) = \left(\frac{\sqrt{q}}{2\pi}\right)^s \Gamma(s)L(f;s),$$

we have $\Lambda(f;s) = \pm\Lambda(f;2-s)$, where the sign can be determined.

The gamma function here is $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}\mathrm{d}t$ for $\mathrm{Re}(s) > 0$, and is well understood.

As a result, we can find a functional equation for $L(E, s)$.

This sign of the functional equation is important: if it is 1, then $L(f; s)$ has even order of vanishing at $s = 1$, and if it is -1, then $L(f; s)$ has odd order of vanishing at $s = 1$.

L-function of an Elliptic Curve

Suppose:

- E is an elliptic curve over $\mathbb{Q}$ such that $L_E(s) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}$ vanishes at $s = 1$ with order 3.

L-function of an Elliptic Curve

Suppose:

- E is an elliptic curve over $\mathbb{Q}$ such that $L_E(s) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}$ vanishes at $s = 1$ with order 3.
- D is the fundamental discriminant of an imaginary quadratic field with class number one.

L-function of an Elliptic Curve

Suppose:

- E is an elliptic curve over $\mathbb{Q}$ such that $L_E(s) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}$ vanishes at $s = 1$ with order 3.
- D is the fundamental discriminant of an imaginary quadratic field with class number one.
- $L_E(\chi_D; s) = \prod_p \left(1 - \frac{\alpha_p \chi_D(p)}{p^s}\right)^{-1} \left(1 - \frac{\beta_p \chi_D(p)}{p^s}\right)^{-1}$ is the L-function twisted by the quadratic character χ_D with conductor D.

L-function of an Elliptic Curve

Suppose:

- E is an elliptic curve over $\mathbb{Q}$ such that $L_E(s) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}$ vanishes at $s = 1$ with order 3.
- D is the fundamental discriminant of an imaginary quadratic field with class number one.
- $L_E(\chi_D; s) = \prod_p \left(1 - \frac{\alpha_p \chi_D(p)}{p^s}\right)^{-1} \left(1 - \frac{\beta_p \chi_D(p)}{p^s}\right)^{-1}$ is the L-function twisted by the quadratic character χ_D with conductor D.

Assuming D to be sufficiently large(effectively), we will heuristically derive a contradiction to the order of the zero at $s = 1$.

Gross–Zagier Curve

Define the completed L-function

$$\Lambda_D(s) = \left(\frac{N|D|}{4\pi^2}\right)^s \Gamma(1+s)^2 L_E(s) L_E(\chi_D; s).$$

We consider the convenient elliptic curve E:

$$-139y^2 = x^3 + 10x^2 - 20x + 8.$$

Proof that $L_E(s, \chi_D)$ Has a Double Zero

From the functional equation of $L_{\mathbb{Q}(\sqrt{D})}(E, s)$, we can prove that $L_{\mathbb{Q}(\sqrt{D})}(E, 1) = 0$, and by the **Gross–Zagier formula** we have

$$L'_{\mathbb{Q}(\sqrt{D})}(E, s)|_{s=1} = c_E \langle P_D, P_D \rangle = 0$$

where P_D is a **Heegner point**, which is torsion for this E. Without details just take this to be true.

Proof that $L_E(s, \chi_D)$ Has a Double Zero

From the functional equation of $L_{\mathbb{Q}(\sqrt{D})}(E, s)$, we can prove that $L_{\mathbb{Q}(\sqrt{D})}(E, 1) = 0$, and by the **Gross–Zagier formula** we have

$$L'_{\mathbb{Q}(\sqrt{D})}(E, s)|_{s=1} = c_E \langle P_D, P_D \rangle = 0$$

where P_D is a **Heegner point**, which is torsion for this E. Without details just take this to be true.

Thus, $L_{\mathbb{Q}(\sqrt{D})}(E, s)$ has at least a double zero at $s = 1$. We also have that

$$L_{\mathbb{Q}(\sqrt{D})}(E, s) = L_E(s) L_E(s, \chi_D).$$

Furthermore, we can check that $L(E, 1) \neq 0$ so that $L_E(s, \chi_D)$ has at least a double zero at $s = 1$.

Proof that $L_{E/\mathbb{Q}(\sqrt{D})}(s)$ Has at Least a Quadruple Zero

We can show the functional equation Additionally, the root number of $L_E(s,\chi_D)$ is negative, $L_E(s,\chi_D)$ has a zero of order at least 3 at $s=1$.

$$\Lambda_D(1+s) = w \cdot \Lambda_D(1-s),$$

where $w = \chi_D(-37 \cdot 139^2) = 1.$ This implies that

$$L_{E/\mathbb{Q}(\sqrt{D})}(s) = L_E(s)L_E(\chi_D; s)$$

has a zero of even order at $s=1$, and since $L_E(\chi_D; s)$ has a zero of order at least 3 at $s=1$, $L_{E/\mathbb{Q}(\sqrt{D})}(s)$ must have a zero of order at least 4.

Heuristic Solution of the Class Number One Problem

Write the Euler products:

$$L_E(s) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1},$$

$$L_E(\chi_D; s) = \prod_p \left(1 - \frac{\alpha_p \chi_D(p)}{p^s}\right)^{-1} \left(1 - \frac{\beta_p \chi_D(p)}{p^s}\right)^{-1}.$$

where $|\alpha_p|^2 = |\beta_p|^2 = \alpha_p \beta_p = p$.

Heuristic Solution of the Class Number One Problem

Write the Euler products:

$$L_E(s) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1},$$

$$L_E(\chi_D; s) = \prod_p \left(1 - \frac{\alpha_p \chi_D(p)}{p^s}\right)^{-1} \left(1 - \frac{\beta_p \chi_D(p)}{p^s}\right)^{-1}.$$

where $|\alpha_p|^2 = |\beta_p|^2 = \alpha_p \beta_p = p$.

From earlier, $h(D) = 1$ implies $\chi_D(p) = -1$ for all primes $p < \frac{1-D}{4}$, which allows us to approximate the behavior of the Euler product of $L_E(s)L_E(\chi_D; s)$.

Heuristic Solution of the Class Number One Problem

We define

$$\phi(s) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 + \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1} \left(1 + \frac{\beta_p}{p^s}\right)^{-1}$$

$$= \prod_p \left(1 - \frac{\alpha_p^2}{p^{2s}}\right)^{-1} \left(1 - \frac{\beta_p^2}{p^{2s}}\right)^{-1}$$

So that

$$\phi(s) \approx L_E(s) L_E(\chi_D; s)$$

by substituting $\chi_D(p) = -1$ (which is only true for $p < \frac{1-D}{4}$).
Thus $L_E(s) L_E(\chi_D; s)$ should analytically behave like $\phi(s)$.

Heuristic Solution of the Class Number One Problem

By the modularity theorem, there is a weight two Hecke eigenform (f) associated to E, and we have

$$\begin{aligned} L(sym^2(f); s) := &\prod_p \left(1 - \frac{\alpha_p^2}{p^s}\right)^{-1} \left(1 - \frac{\alpha_p \beta_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p^2}{p^s}\right)^{-1} \\ = &\prod_p \left(1 - \frac{\alpha_p^2}{p^s}\right)^{-1} \left(1 - \frac{1}{p^{s-1}}\right)^{-1} \left(1 - \frac{\beta_p^2}{p^s}\right)^{-1}. \end{aligned}$$

Thus $\phi(s)$ is essentially $\dfrac{L(sym^2(f); 2s)}{\zeta(2s-1)}$.

Heuristic Solution of the Class Number One Problem

It is known that $L(sym^2(f); s)$ is holomorphic on the whole plane and $L(sym^2(f); 1) \neq 0$. However, $\zeta(2s-1)$ has a simple pole at $s = 1$, meaning that $\phi(s)$ has a simple zero at $s = 1$, which contradicts the fact that $L_E(s)L_E(\chi_D; s)$ has a fourth-order of zero at $s = 1$.

Therefore our assumption that D was sufficiently large must have been wrong, so there is only a finite number of discriminants D such that $\mathbb{Q}(\sqrt{D})$ has class number one.

Acknowledgments

- We would like to thank our mentor Hao Peng for teaching us throughout the year and answering all our questions
- We also thank the PRIMES program for giving us this opportunity
- Additionally we'd like to thank our parents for spending their Sunday nights driving us to MIT

References

Kowalski, E., & Iwaniec, H. (2004). Analytic number theory. American Mathematical Society.

The argument in this presentation is taken from Dorian Goldfeld's paper "The Gauss Class Number Problem for Imaginary Quadratic Fields."