GAUSS' CLASS NUMBER PROBLEMS AND THE DETERMINATION OF IMAGINARY QUADRATIC FIELDS WITH CLASS NUMBER ONE

MAXINE CALLE
MATH 361 FINAL PROJECT
MAY 13, 2019

ABSTRACT. This paper examines Gauss' class number problems for imaginary quadratic fields, with particular emphasis on the class number one problem. We develop the theory of binary quadratic forms and quadratic fields, and explore how the class number is represented in each of these contexts. This background allows us to outline the solution to the class number one problem through Gauss' original work and the Baker-Heegner-Stark theorem.

INTRODUCTION AND BACKGROUND

On our second exam, we encountered Euler's prime-producing polynomial

$$x^2 + x + 41$$

which takes on prime values for integers $-40 \leq x \leq 39$. Strikingly, our proof of this property relied upon the claim that -163 is not a quadratic residue for any positive prime $p < 41$. Encountering this material, one might wonder why the function has this fascinating property, where we might find other such functions, and why -163 is involved at all. A theorem of Rabinovitch, discussed in [4] and [8, Chapter 5, Section 7], makes the connection a bit more transparent.

Theorem (Rabinovitch). *For $D > 0$ with $D \equiv 3 \pmod 4$, the polynomial*

$$f(x) = x^2 - x + \frac{1+D}{4}$$

is prime for $x = 1, 2, \ldots, \frac{D-3}{4}$ if and only if every integer in $\mathbb{Q}(\sqrt{-D})$ factors uniquely into primes.

Ayoub and Chowla [1] show that a similar theorem holds for functions of the form $f(x) = x^2 + x + \frac{1+D}{4}$; noting that $f(x+1) = x^2 + x + \frac{1+D}{4}$ further verifies the intuitive claim. We see that the property of Euler's polynomial (with $\frac{1+D}{4} = 41$) is thus connected to the fact that the ring of integers of $\mathbb{Q}(\sqrt{-163})$ is a UFD. In fact, our familiar friend -163 is one of nine so-called Heegner numbers that gives rise to this phenomenon.

Determining the Heegner numbers is a special case of Gauss' class number problem, which originated in Gauss' *Disquisitiones Arithmeticae*. Written in 1798 when Gauss was 21 years old, *Disquisitiones* is one of the most influential texts in the history of algebraic number theory. The book consolidates the work of Gauss' predecessors, such as Euler, Lagrange, and Legendre, and presents interesting questions which even over 200 years later still occupy mathematicians. This paper seeks to give an overview of one such problem, known as the *class number one problem for imaginary quadratic fields*. However, in order to rigorously discuss this issue, we must first lay down some groundwork.

The first section discusses the theory of binary quadratic forms, as described in [3, Chapter 1, Section 2]. The notion of equivalence between forms allows us to define the class number. The main result of this section is that the class number is finite, although a proof is not supplied. Section 2 states Gauss' class number problem and some of its special cases, and discusses Gauss' original work on the class number one problem. We prove Landau's theorem, which verifies the completeness of Gauss' conjectured values giving rise to class number one. From here, we look beyond Gauss and move into imaginary quadratic fields. Section 3 recalls the material from lecture [9] to introduce the class number problem in this context. Finally, we discuss the Baker-Heegner-Stark theorem which gives the complete determination of imaginary quadratic fields with class number one. As some of this material is beyond the scope of this paper, we give only a rough sketch of the proof.

1. Binary Quadratic Forms

In the fifth section of *Disquisitiones Arithmeticae*, Gauss works with *binary quadratic forms*, which are those expressions

$$ax^2 + bxy + cy^2$$

for $a, b, c \in \mathbb{Z}$. The *discriminant* of the form is the term beneath the square root in the quadratic formula, which is $d = b^2 - 4ac$. Our focus will be primarily on forms with negative discriminants, so we assume both a and c to be non-zero. In particular, we are interested in *fundamental discriminants*, where $d \equiv 1 \pmod 4$ is square-free or $d = 4n$ where $n \equiv 2, 3 \pmod 4$ is square-free. For the remainder of this section, we let $f(x, y)$ denote the form $ax^2 + bxy + cy^2$ unless otherwise specified.

The study of binary quadratic forms began with Lagrange, as treated in his 1773-1775 work *Recherches d'Arithmétique*, in the context of trying to determine when an integer m can be represented by some form $f(x,y)$ for some integer x and y. The theory from *Recherches* was further developed by Gauss to whom most of the terminology is due, although many of the concepts are inspired by Lagrange. For further discussion of the origin of the study of binary quadratic forms and the more general theory, see the work by Cox [3, Chapter 1, Section 2] or Ribenboim [8, Chapter 6, Section 4].

A form $f(x,y)$ is called *primative* when $\gcd(a,b,c) = 1$. Since any form is an integer multiple of a primitive form, it is sufficient to concern ourselves exclusively with primitive forms. We also restrict our attention to *positive-definite* forms, which are those for which $f(x,y) \geq 0$ for all (x,y). Similarly, a form is *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* if there is a matrix of $\mathrm{GL}_2(\mathbb{Z})$ such that

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

Letting M denote the *pqrs*-matrix given above, we say this equivalence is *proper* if $M \in \mathrm{SL}_2(\mathbb{Z})$ and *improper* otherwise. It is clear that the equivalence of forms is an equivalence relation: the group action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of forms as given above partitions the set according to the orbits. Since $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$, proper equivalence is an equivalence relation in much the same way. Following Gauss, we say that two properly equivalent forms are in the same *class*, and denote the relation by $f(x,y) \sim g(x,y)$.

Proposition 1.1. *Any two equivalent forms $f(x,y) \sim g(x,y)$ have the same discriminant.*

Proof. Suppose $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = Ax^2 + Bxy + Cy^2$ are two equivalent forms of discriminant $d = b^2 - 4ac$ and $D = B^2 - 4AC$, respectively. Then there is a matrix $M \in \mathrm{GL}_2(\mathbb{Z})$ with $\det(M) = \pm 1$, such that $f(x,y) = g(px+qy, rx+sy)$. We will show that $d = (ps-qr)^2 D$, and hence that the discriminants are equal.

First, determine a,b,c in terms of A,B,C. Considering $g(px+qy, rx+sy)$, we expand $A(px+qy)^2 + B(px+qy)(rx+sy) + C(rx+sy)^2$ and group by like terms for x^2, xy, and y^2. A little bit of algebraic manipulation gives

$$\begin{aligned} a &= Ap^2 + Bpr + Cr^2, \\ b &= 2(Apq + Crs) + B(ps + qr), \\ c &= Aq^2 + Bqs + Cs^2. \end{aligned}$$

Now, we can expand b^2 and ac, rearranging alphabetically by A, B, C,

$$\begin{aligned}
b^2 =& 4(Apq + Crs)^2 + 4B(Apq + Crs)(ps + qr) + B^2(ps + qr)^2 \\
=& 4A^2p^2q^2 + 4AB(p^2qs + q^2pr) + 8ACpqrs + B^2(ps + qr)^2 \\
& + 4BC(s^2pr + r^2sq) + 4C^2r^2s^2, \\
ac =& (Ap^2 + Bpr + Cr^2)(Aq^2 + Bqs + Cs^2) \\
=& A^2p^2q^2 + AB(p^2qs + q^2pr) + AC(p^2s^2 + r^2q^2) + B^2(prqs) \\
& + BC(s^2pr + r^2sq) + C^2r^2s^2.
\end{aligned}$$

In the quantity $d = b^2 - 4ac$, it is easy to verify that everything cancels but the B^2 and AC terms. Thus

$$\begin{aligned}
b^2 - 4ac &= -4AC(p^2s^2 + r^2q^2 - 2pqrs) + B^2(p^2s^2 + q^2r^2 + 2pqrs - 4pqrs) \\
&= (ps - qr)^2(B^2 - 4AC),
\end{aligned}$$

and so $d = D$ as claimed. □

We can see that the converse of this proposition is not necessarily true – otherwise this paper would be quite a bit shorter! For example, consider $d = -20$ and the forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. We claim these forms are not equivalent. Using methods from the proof of Proposition 1.1 above, with $(a, b, c) = (2, 2, 3)$ and $(A, B, C) = (1, 0, 5)$, suppose we have a matrix M as given above. But then

$$\begin{aligned}
2 = a = Ap^2 + Bpr + Cr^2 &= p^2 + 5r^2, \\
2 = b = 2(Apq + Crs) + B(ps + qr) &= 2(pq + 5rs), \\
3 = c = Aq^2 + Bqs + Cs^2 &= q^2 + 5s^2,
\end{aligned}$$

and this is impossible for $p, q, r, s \in \mathbb{Z}$.

To examine the special case of Gauss' class number problem that we are interested in, we restrict our attention to positive-definite forms with negative discriminant, so $d < 0$ unless explicitly stated otherwise. The sign of the discriminant strongly restricts the behavior of the form.

Proposition 1.2. *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.*

Proof. The result follows by "completing the square" and some straight-foward manipulations:

$$\begin{aligned} ax^2+bxy+cy^2 &= a\left(x^2+\frac{b}{a}xy+\frac{c}{a}y^2\right) \\ &= a\left[x^2+2\frac{b}{2a}xy+\left(\frac{b}{2a}y\right)^2-\left(\frac{b}{2a}y\right)^2+\frac{4ac}{4a^2}y^2\right] \\ &= a\left[\left(x+\frac{by}{2a}\right)^2-(b^2-4ac)\left(\frac{y}{2a}\right)^2\right]. \end{aligned}$$

Since $b^2-4ac<0$, the quantity inside the brackets is positive regardless of choice of (x,y). Thus $f(x,y)$ is positive-definite if a is positive, and negative-definite otherwise. □

From this point on, we take a to be positive (and so $c>0$ as well), which provides an especially nice notion of a reduced form. 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 properly equivalent to a canonical unique reduced form [3, Theorem 2.8].

As a complement to the more classically-styled proof of Cox in [3], Gelfond gives a discussion of this result in [4] which builds nicely upon material from lecture [9, Part 2]. In particular, for a form $f(x,y)$ with discriminant d, we get an associated complex number $\omega=\frac{-b+\sqrt{d}}{2a}$. A form is thus reduced precisely when ω is in the fundamental domain of the modular group $\mathrm{SL}_2(\mathbb{Z})$. The fact that every form is equivalent to a unique reduced form is analogous to the idea from lecture that each complex lattice is homothetic to a lattice Λ_τ for τ in the fundamental domain.

Definition 1.1. *The class number, denoted $h(d)$, is the number of inequivalent forms $f(x,y)$ with discriminant $d=b^2-4ac$.*

Determining $h(d)$ for a given d can be a challenge in and of itself, although the task is made much easier via computer programs. Note that $-d=4ac-b^2\geq 3a^2$, and so we can bound the coefficients by $|b|\leq a\leq\sqrt{\frac{-d}{3}}$. This implies that there are only finitely many reduced forms for a given discriminant, and thus the number of proper equivalence classes is also finite. Hence we get the following theorem, which is analogous to Theorem 10.2 from lecture [9].

Theorem 1.1 ([3, Theorem 2.13])**.** *For fixed d, the number $h(d)$ of primitive, positive-definite forms of discriminant d is finite. Further, $h(d)$ is equal to the number of reduced forms of discriminant d.*

Remarkably, Gauss conjectured the same fact in *Disquisitiones*. Without knowing what a group is, Gauss proves that the classes of forms with a given discriminant form a finite group under composition as the group operation (see [3, Theorem 3.9]). This group is known as the *form class group* and denoted $C(d)$, and the order of $C(d)$ is clearly the class number $h(d)$. In article 303, Gauss' claims that the number of (negative) discriminants of a given class number is finite, and this is the advent of the class number problem.

2. Gauss' Class Number Problem

The class number problem can be stated roughly as follows:

> **Gauss' class number problem**: For a given n, determine all discriminants d such that $h(d) = n$.

This general problem grew and split into multiple questions over the years. For example, some of the more modern results and conjectures are given by:

(1) $\lim_{d\to-\infty} h(d) = \infty$.
(2) for $d < 0$,
  (i) $h(d) = 1 \Leftrightarrow d \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$
  (ii) determine all d such that $h(d) = n$ for small n.
(3) for $d > 0$, there are infinitely many d such that $h(d) = 1$.

While (1) and (2) were solved through the 20th century, (3) notably remains an open problem. Section 3 will discuss these problems in more detail, but the remainder of this section is devoted to Gauss' original work in the area of problem (2.i), called the class number one problem.

Disquisitiones Arithmeticae is not without its curiosities and differences from the modern theory. Notably, Gauss worked with forms with even middle coefficient, written $ax^2 + 2bxy + cy^2$, and defined the discriminant as $b^2 - ac$. We have already seen how properties of the discriminant can influence a form, and vice versa. Note that under the more general definitions from Section 1, $d = b^2 - 4ac \equiv b^2 \pmod 4$ so b is even iff $d \equiv 0 \pmod 4$ and odd iff $d \equiv 1 \pmod 4$. When the middle coefficient is $2b$, the general discriminant is $(2b)^2 - 4ac = 4(b^2 - ac)$ — four times the Gaussian discriminant. In this sense, Gauss' observations pertain only to even discriminants. Hence the modern class number problem explored in the next section is slightly more involved than his original conjectures given here.

For example, Gauss claimed that the complete set of negative discriminants with class number one is $\{-1, -2, -3, -4, -7\}$. Using Gauss' definitions, Landau verified the conjecture in 1902. Yet in the statement of 2(i) above, the modern set of values (the Heegner numbers) is almost entirely different! As noted, the Gaussian discriminant is a quarter of the modern version. Multiplying Gauss' original values by 4 we get $\{-4, -8, -12, -16, -28\}$, and discarding the non-fundamental discriminants leaves only -4 and -8. These two values are precisely the even Heegner numbers.

The remainder of this section is devoted to proving Landau's theorem as given in [3, Theorem 2.18]. The following section returns to the class number one problem in the context of odd discriminants.

Theorem 2.1 (Landau)**.** *Let n be a positive integer. Then $h(-4n) = 1$ if and only if $n \in \{1, 2, 3, 4, 7\}$.*

Proof. First note that $Q(x, y) = x^2+ny^2$ is a reduced form of discriminant $-4n$. Following the proof of the theorem in [3, Theorem 2.18], we proceed by cases. The goal in each case is to show that there is another reduced form of the same discriminant that is not equivalent to $Q(x, y)$, so the class number is at least 2.

Case 1: n is not a prime power. If n is not a prime power, then $n = ac$ for some $a, c \in \mathbb{Z}$. Since n is not a prime power, it must have at least two distinct prime factors. Thus without loss of generality, we can take $1 < a < c$ with $\gcd(a, c) = 1$, so the form $ax^2 + cy^2$ is also a reduced form of discriminant $-4n$. Since this form is not equivalent to $Q(x, y)$, we have $h(-4n) > 1$ for n which is not a prime power.

Case 2: n is a power of 2. If $n = 2^k$ for $k \geq 4$, then

$$4x^2 + 4xy + (2^{k-2} + 1)y^2$$

is a primitive, reduced form since $2^{k-2} + 1$ is odd and $4 \leq 2^{k-2} + 1$. Further, the discriminant is $4^2 - 4^2(2^{k-2} + 1) = 4^2(1 - 2^{k-2} + 1) = 4(-2^k) = -4n$. To show the forms are not equivalent, suppose that the form above could be represented by $Q(px + qy, rx + sy)$ with $p, q, r, s \in \mathbb{Z}$ and $ps - qr = \pm 1$. Then mimicking the work done for Proposition 1.1, we must have

$$\begin{aligned} 4 &= p^2 + nr^2 = p^2 + 2^k r^2, \\ 4 &= 2(pq + nrs) = 2pq + 2^{k+1}rs, \\ 2^{k-2} + 1 &= q^2 + ns^2 = q^2 + 2^k s^2. \end{aligned}$$

Since $k \geq 4$, this implies that $s = r = 0$. Then the first equation implies that $p = \pm 2$, and consequently the second equation implies that $q = \pm 1$. But then the third equation does not hold, and therefore there can be no such $p, q, r, s \in \mathbb{Z}$. Hence $h(-4n) > 1$ when $n = 2^k$ for $k \geq 4$.

Taking $k = 1, 2$ gives the even values of the set. For the remaining case when $k = 3$, we can compute directly that $h(-32) = 2$. To a primitive, reduced form $ax^2 + bxy + cy^2$ that is not equivalent to $Q(x, y)$, we recall the discussion prior to Theorem 1.1, which bounds $|b| \leq a \leq \sqrt{\frac{32}{3}} < 4$.

If $a = 1$, then $b = 0, 1$ ($b \neq -1$ otherwise the form is not reduced). Taking $b = 0$ gives $Q(x, y)$. Taking $b = 1$ gives a non-integer value of c, as $-32 = 1 - 4c$.

When $a = 2$, many of the possible values of b similarly give impossible non-integer values of c. The one exception is when $b = 0$, $-32 = -4(2c)$ so $c = 4$. But then the form is not primitive, since a, b, c are all even.

Finally, when $a = 3$, again most b-values give non-integer c-values, with the exception of $b = 2$. In this case, $-32 = 4 - 4(3c)$ so $c = 3$. Thus the form we've been searching for is $3x^2 + 2xy + 3y^2$. Similar methods as previously employed show that this form is not equivalent to $Q(x, y)$. Thus $h(-32) \neq 1$, so the only remaining even cases are the known values of 2 and 4.

Case 3: n is a power of an odd prime. Suppose $n = p^k$ for some odd prime p, so $n + 1$ is even. If $n + 1$ is not a prime power, and so can be written as $n = ac$ for some $2 \leq a < c$ with $\gcd(a, c) = 1$, then we consider $ax^2 + 2xy + cy^2$. By similar arguments as given previously, this form satisfies our requirements, with discriminant $4 - 4(ac) = 4 - 4(n + 1) = -4n$. Thus $n(-4n) > 1$ when $n + 1$ is not a prime power.

On the other hand, if $n+1$ is a prime power, it must be some power of 2. Suppose $n+1 = 2^k$, and note that taking $k = 1, 2, 3, 4, 5$ gives the values of $n = 1, 3, 7, 15, 31$, respectively. If $k \geq 6$, then $8x^2 + 6xy + (2^{k-3} + 1)y^2$ is a primitive, reduced form since the coefficients are relatively prime and $8 \leq 2^{k-3} + 1$. The discriminant is appropriately $36 - 32(2^{k-3} + 1) = 4 - 4 \cdot 2^k = 4(1 - (n + 1)) = -4n$. As before, we have $h(-4n) > 1$ in this case.

Now, to combat the unwanted values of $n = 15, 31$, we note that 15 is not a prime power and so is disposed of by Case 1. A short program (written by the author in Python) computes $h(-4 \cdot 31) = 3$, where the appropriate forms are $x^2 + 31y^2$ and $5x^2 \pm 4xy + 7y^2$. Thus we are left with only the desired values of n, which completes one direction of the proof. The other direction of implication follows computationally, as discussed on [3, p.31]. The author's Python program additionally confirmed the completeness of Tab. 1.

n	$-4n$	Reduced Forms of Discriminant $-4n$	$h(-4n)$
1	-4	x^2+y^2	1
2	-8	x^2+2y^2	1
3	-12	x^2+3y^2	1
4	-16	x^2+4y^2	1
5	-20	$x^2+5y^2,\ 2x^2+2xy+3y^2$	2
6	-24	$x^2+6y^2,\ 2x^2+3y^2$	2
7	-28	x^2+7y^2	1
8	-32	$x^2+8y^2,\ 2x^2+2xy+3y^2$	2
9	-36	$x^2+9y^2,\ 2x^2+2xy+5y^2$	2
13	-52	$x^2+13y^2,\ 2x^2+2xy+7y^2$	2
14	-56	$x^2+14y^2,\ 2x^2+7y^2,\ 3x^2\pm 2xy+5y^2$	4
27	-108	$x^2+27y^2,\ 4x^2\pm 2xy+7y^2$	3
31	-124	$x^2+31y^2,\ 5x^2\pm 4xy+7y^2$	3
64	-256	$x^2+64y^2,\ 4x^2+4xy+17y^2,\ 5x^2\pm 2xy+13y^2$	4

Table 1. Data for $-4n$ discriminants for various n.

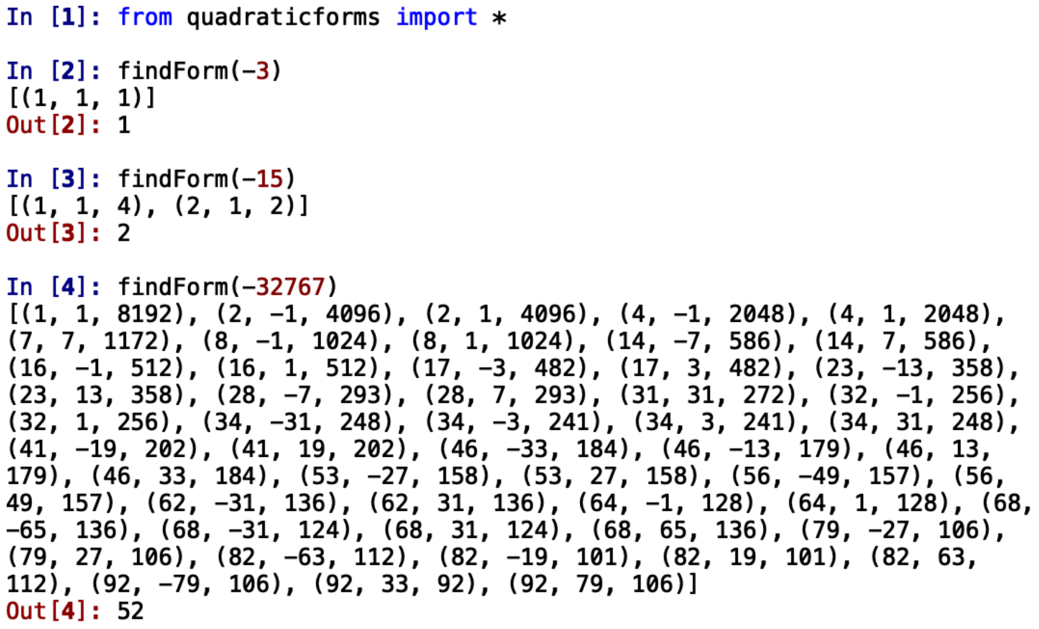
Having thus verified that $n \in \{1,2,3,4,7\}$ implies $h(-4n)=1$, the proof is complete. □

With the main work of this section done, we note the strong impact of computer programs on calculating these forms. Finding the forms by hand is not too difficult for relatively small discriminants, as demonstrated in the proof of Theorem 2.1, however a computer program can use the same methods to complete the task far more quickly. To emphasize this point, and to complete [3, Exercise 2.9], we implement the program to compute all reduced forms of discriminant -3, -15, and -32768, and Fig. 1 displays the results.

A call to the function findForm prints a list of all primitive, reduced forms of the given discriminant and returns the class number (which is the length of the list). Each tuple (a,b,c) represents the form $ax^2+bxy+cy^2$. While the -3 and -15 cases certainly seem manageable without a computer program, calculating all 52 reduced forms of discriminant -32767 by hand seems like a painful task.

3. After Gauss

Although Gauss worked only with even discriminants, the class number problem in its more general form has been tackled by various mathematicians over the years.



```
In [1]: from quadraticforms import *

In [2]: findForm(-3)
[(1, 1, 1)]
Out[2]: 1

In [3]: findForm(-15)
[(1, 1, 4), (2, 1, 2)]
Out[3]: 2

In [4]: findForm(-32767)
[(1, 1, 8192), (2, -1, 4096), (2, 1, 4096), (4, -1, 2048), (4, 1, 2048),
(7, 7, 1172), (8, -1, 1024), (8, 1, 1024), (14, -7, 586), (14, 7, 586),
(16, -1, 512), (16, 1, 512), (17, -3, 482), (17, 3, 482), (23, -13, 358),
(23, 13, 358), (28, -7, 293), (28, 7, 293), (31, 31, 272), (32, -1, 256),
(32, 1, 256), (34, -31, 248), (34, -3, 241), (34, 3, 241), (34, 31, 248),
(41, -19, 202), (41, 19, 202), (46, -33, 184), (46, -13, 179), (46, 13,
179), (46, 33, 184), (53, -27, 158), (53, 27, 158), (56, -49, 157), (56,
49, 157), (62, -31, 136), (62, 31, 136), (64, -1, 128), (64, 1, 128), (68,
-65, 136), (68, -31, 124), (68, 31, 124), (68, 65, 136), (79, -27, 106),
(79, 27, 106), (82, -63, 112), (82, -19, 101), (82, 19, 101), (82, 63,
112), (92, -79, 106), (92, 33, 92), (92, 79, 106)]
Out[4]: 52
```

FIGURE 1. Output of program calculating all primitive reduced forms for given discriminants -3, -15, and -32767.

The more modern view of the problem is from the perspective of quadratic fields rather than forms.

Most of the necessary tools were covered in lecture [9], so we recall only the most essential material. Additional discussion of this material can also be found in Ireland and Rosen [7, Chapters 12 and 13]. An *integer* in a quadratic field $K = \mathbb{Q}(\sqrt{d})$ is an element whose minimal monic polynomial has coefficients in $\mathbb{Z}$. These algebraic integers form a subring of K, denoted $\mathcal{O}_K$. The *discriminant* of K is defined to be d if $d \equiv 1 \pmod 4$ and $4d$ if $d \equiv 2, 3 \pmod 4$.

One might notice that this definition of discriminant is reminiscent of the fundamental discriminants of binary quadratic forms. The connection between these two concepts is as one would hope: d is a fundamental discriminant of a form if and only if d is the discriminant of a quadratic field K, and there is exactly one quadratic field (up to isomorphism) for each fundamental discriminant ($d \neq 1$) [8, Chapter 6, Section 16]. This connection also explains why we are interested in fundamental discriminants, whereas Gauss was not so concerned. Since we are interested in $d < 0$, we will restrict our attention to imaginary quadratic fields.

An ideal $\mathcal{I}$ of a quadratic field K is a *fractional ideal* if there is a non-zero algebraic integer $\alpha \in \mathcal{O}_K$ such that $\alpha\mathcal{I}$ is an ideal of $\mathcal{O}_K$, and a fractional ideal $\mathcal{I}$ said to be *principal* if $\alpha\mathcal{I}$ can be generated by a single element. The principal fractional ideals form a subgroup of the group of fractional ideals under ideal multiplication.

Definition 3.1. *The ideal class group of a quadratic field K is the quotient group*

$$C_K = \{\textit{fractional ideals}\}/\{\textit{principal fractional ideals}\}.$$

The class number for a quadratic field is the order of C_K, denoted h_K.

Note that $\mathcal{O}_K$ acts as the identity element on this group. It follows that $h_K = 1$ if and only if every ideal of $\mathcal{O}_K$ is principal, which is to say that $\mathcal{O}_K$ is a PID and hence a UFD. One might recall the discussion from the introduction, and note that the theorem of Rabinovitch can be restated to relate prime producing polynomials and imaginary quadratic fields of class number one.

At the end of Section 1, we briefly mention Gauss' remarkable work with the form class group $C(d)$, whose order is the class number $h(d)$. There is a striking relationship between the groups $C(d)$ and C_K.

Theorem 3.1 ([3, Theorem 5.30])**.** *Let K be an imaginary quadratic field of discriminant $d < 0$. Then the group homomorphism $\phi : C(d) \to C_K$ defined by*

$$ax^2 + bxy + cy^2 \mapsto \left(a,\ \frac{-b+\sqrt{d}}{2a}\right)$$

is an isomorphism. Hence the order of the ideal class group is the order of the form class group, which is to say $h(d) = h_K$.

This theorem allows us to compute ideal class groups using our knowledge of forms, or vice versa. For example, for $K = \mathbb{Q}(\sqrt{-5})$ with discriminant $d = -20$, the class group $C(-20)$ is cyclic of order 2, since Tab. 1 says there are only two reduced forms of discriminant -20. Then, by Theorem 3.1, C_K is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and the ideal class representatives are given by $\left(1, \sqrt{-5}\right) = \mathcal{O}_K$ and $\left(2, -1+\sqrt{-5}\right)$. We will now refer to the class number as $h(d)$, which encompasses both contexts.

With this understanding of imaginary quadratic fields and ideal class groups, mathematicians throughout the 20th century were able to build upon the work of Gauss, proving incredible results such as the Dirichlet class number formula presented in lecture [9], the divergence of the class number, and the complete determination of imaginary quadratic fields for small class numbers. The latter two are problems (1) and (2) from Section 2. The following section will focus on (2), in particular (2.i), but first we give a brief expository overview of (1) as it is both an amazing and amusing achievement of mathematics. Much of the following information is taken from Ireland and Rosen [7, Chapter 20, Section 6], Cox [3, Chapter 2, Section 7(D) and Chapter 3, Section 12(E)], and the article by Goldfeld [4].

The divergence of the class number was fully proved in a paper of Heilbronn published in 1934 [5], however the result is the combined effort of many mathematicians and utilizes the generalized Riemann hypothesis in a surprising way. Progress on the issue was first made by Hecke around 1918, who showed that if the generalized Riemann hypothesis is true, then $h(d) \to \infty$ as $d \to -\infty$ [5, Theorem IV]. In 1933, Deuring proved that if the Riemann hypothesis is *false*, then $\lim_{d\to-\infty} h(d) \geq 2$ so the class number at least begins to diverge [5, Theorem V]. Mordell improved upon this result in 1934 by showing that if the Riemann hypothesis is false, then indeed $h(d) \to \infty$ as $d \to -\infty$ [5, Theorem VI]. Hielbronn completed the circle of ideas by showing that if the *generalized* Riemann hypothesis is false, the class number must diverge [5, Theorem VII].

The overall method of proof of the divergence of the class number is a rather peculiar feat of logic: If the generalized Riemann hypothesis is true, then the class number diverges. But if the Riemann hypothesis is not true, the same consequence holds. Thus the class number must diverge, independent of the hypothesis. However, Heilbronn's method of proof is not effective in determining the exact nature of the divergence, and so sheds little light on Gauss' class number problem.

4. The Class Number One Problem

The class number one problem is the special case of Gauss' class number problem for $n = 1$. We saw in Section 2 that Gauss was able to make some progress for even d in 1798, but the more general problem was not completely resolved until the 1960s. By 1934, it was known that there were at least nine fundamental discriminants d with $h(d) = 1$, and Heilbronn and Linfoot were able to refine Heilbronn's earlier work to show that there could be *at most ten* such d [6]. The possible existence of this tenth discriminant incited feverish research in this area, but unexpectedly the first person to make significant progress was Heegner, a high school teacher. In 1952, he published *Diophantische Analysis und Modulfunktionen* which claims that there is no tenth discriminant with class number one. Thus there are exactly nine fundamental discriminants giving class number one. Unfortunately, his paper was considered to be incorrect and was largely discounted. This neglect was unwarranted, but Heegner died before receiving due credit for his accomplishment.

In 1966, Baker [2] and Stark [10] separately published proofs that corroborated Heegner's result. Stark's method is quite similar to Heegner's, although Baker's is totally different. At that time, Heegner's work was reexamined and Stark (among others) demonstrated that the "gap" in Heegner's proof is not hard to fill [11]. While the proof is mostly elementary, it is still quite complicated and involves concepts beyond our scope. The reader is invited to see Stark's treatment of Heegner's proof [11] as well as the work in [3, Theorem 12.34] for more rigorous explanation.

Theorem 4.1 (Baker-Heegner-Stark)**.** *There are exactly nine fundamental discriminants $d < 0$ for which $h(d) = 1$, namely*

$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Sketch of Proof. It has already been shown in Theorem 2.1 that the only even dicriminants with class number one are $-4, -8, -12, -16$ and -28, and only -4 and -8 are fundamental. Thus it is sufficient to consider $d \equiv 1 \pmod 4$. It follows that $d = -p$ where $p \equiv 3 \pmod 4$ is prime (see [3, Theorem 12.34] for an explanation involving basic genus theory). Thus p is congruent to either 3 or 7 modulo 8, and it is worth noting that the only $d = -p$ listed above with $p \equiv 7 \pmod 8$ is $d = -7$. So as a first step, we prove that if $p \equiv 7 \pmod 8$ with $h(-p) = 1$, then actually $p = 7$.

Suppose $p \equiv 7 \pmod 8$. Then Corollary 7.28 in [3] gives

$$\begin{aligned} h(-4p) &= h(-p)2\prod_{k|2}\left(1-\left(\frac{-p}{k}\right)\frac{1}{k}\right) \\ &= 2h(-p)\left[\left(1-\left(\frac{-p}{1}\right)\frac{1}{1}\right)\left(1-\left(\frac{-p}{2}\right)\frac{1}{2}\right)\right] \\ &= 2h(-p)\left[(1-0)\left(1-\frac{1}{2}\right)\right] \qquad \text{since } -p \equiv 1 \pmod 8, \\ &= h(-p), \end{aligned}$$

and so $h(-p) = 1$ if and only if $h(-4p) = 1$. Then Theorem 2.1 implies that $p = 7$.

Things get more complicated when $d = -p$ with $p \equiv 3 \pmod 8$, and we will only give a rough outline of the method. Very broadly, we can make use of modular forms—specifically the j-function—to show that a particular polynomial of degree 24 with rational coefficients has a degree-6 factor, from which we derive a set of Diophantine equations. The methods of Heegner and Stark use the solutions to the equations to determine the six remaining values of d. □

After this success story, significant progress was made on the same problem for relatively small class numbers, as discussed in [4, Section 5]. In 1971, Baker and

Stark determined that there are exactly eighteen imaginary quadratic fields with class number two. In 1985, Oesterlé determined the complete list for $h(d) = 3$. In 2003, Watkins completed the classification of $h(d) = n$ for $n \leq 100$ [13]. Despite all this work for imaginary quadratic fields, it should be noted that the class number one problem for real quadratic fields has not yet been solved. The summary presented by Stark in 2007 [12] gives a good discussion of how he envisions this work could proceed. With regards to the comments on the similarity of his and Heegner's proof of Theorem 4.1, he remarks [12, p.249],

> It is frequently stated that my proof and Heegners proof are the same. The two papers end up with the same Diophantine equations, but I invite anybody to read both papers and then say they give the same proof!

Unfortunately Heegner's paper is in German and rather difficult to find, but this fact should not undermine Stark's incredible contributions to this area of mathematics.

References

1. R.G. Ayoub and S. Chowla, "On Euler's Polynomial," *Jour. Num. Theory* **13** (1981): pp. 443–445.
2. A. Baker, "Linear Forms in the Logarithms of Algebraic Numbers," *Mathematika* **13** (1966): pp. 204–206.
3. D.A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, 2nd ed., John Wiley & Sons, Inc., New Jersey (2013).
4. D. Goldfeld, "Gauss' Class Number Problem for Imaginary Quadratic Fields," *Bull. Amer. Math. Soc.* **13** no. 1 (1985): pp. 23–38.
5. H. Heilbronn, "On the Class-Number in Imaginary Quadratic Fields," *Quart. Jour. Math. Oxford* **5** (1934): pp. 150–160.
6. H. Heilbronn and E.H. Linfoot, "On the Imaginary Corpora of Class-Number One," *Quart. Jour. Math. Oxford*, **5** (1934): pp. 293–301.
7. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Math. **84**, 2nd ed., Springer-Verlag, New York (2010).
8. P. Ribenboim, *My Numbers, My Friends: Popular Lectures on Number Theory*, Springer-Verlag, New York (2000): pp. 91–174.
9. J. Shurman, "The Dirichlet Class Number Formula for Imaginary Quadratic Fields," Math 361 Lectures at Reed College (2019), *http://people.reed.edu/∼jerry/361/lectures/iqclassno.pdf*.
10. H.M. Stark, "A Complete Determination of the Complex Quadratic Fields of Class Number One," *Michigan Math. J.* **14** (1967): pp. 1–27.
11. H.M. Stark, "On the 'Gap' in a Theorem of Heegner," *Jour. Num. Theory* **1** (1969): pp. 16–27.
12. H.M. Stark, "The Gauss Class-Number Problems," *Clay Math. Proc.* **7** (2007): pp. 247 – 256.
13. M. Watkins, "Class Numbers of Imaginary Quadratic Fields," *Math. Comp.* **73** no. 246 (2003): pp. 907 – 938.