THE CLASS NUMBER PROBLEM

JOSHIKA CHAKRAVERTY, ISABELLE HONG, ASHWIN RAJAN

1. Abstract

In this paper, we investigate the uses and the applications of the Gauss class number problem. The class number $h(-d)$, the number of reduced binary quadratic forms of discriminant d, is used in Gauss' conjecture where he claimed that as d tends to infinity, so does $h(-d)$. One of the uses of the class number problem is with the Heegner numbers, which satisfy $h(-d) = 1$ for a field $\mathbb{Q}(\sqrt{-d})$. The nine Heegner numbers have several interesting properties, including: being prime generators and producing almost integers (using the j-function). The j-function and the Heegner numbers were used by the Chudnovsky brothers to find an approximation for $\frac{1}{\pi}$. Overall, we discuss the the steps that were taken by many different mathematicians to prove that only 9 fields of class number one exist, and we also discuss the implications of the Heegner numbers in related fields of mathematics.

2. Introduction

The class number formula depends on an understanding on imaginary quadratic fields, which in turn depends on an understanding of the discriminant.

Definition 2.1 (Binary Quadratic Form Discriminants)**.** For a binary quadratic function $ax^2 + bxy + cy^2$, the discriminant d is $d \equiv 4ac^2 - b$.

Definition 2.2 (Imaginary Quadratic Field)**.** An imaginary quadratic field is represented as $\mathbb{Q}(\sqrt{-d})$ and includes all numbers in the form of $a + b\sqrt{-d}$, where $a, b \in \mathbb{Q}$ and $d \in \mathbb{Z}^+$.

Imaginary quadratic fields are used in many parts of mathematics. Two of the most common imaginary quadratic fields are the Eisenstein and Gaussian integers. The Eisenstein integers are $\mathbb{Q}(\sqrt{-3})$ and the Gaussian integers are $\mathbb{Q}(\sqrt{-1})$, the latter of which is equivalent to the complex numbers $a + bi$, where a and b are integers. With this background knowledge in mind, we can now introduce the class number problem.

Definition 2.3 (Gauss Class Number Problem)**.** For a given n, determine all of the imaginary quadratic fields in the form of $\mathbb{Q}(\sqrt{-d})$ with class number n.

Definition 2.4 (Class Number)**.** The class number $h(-d)$ is the number of reduced binary quadratic forms of discriminant d.

Definition 2.5 (Gauss Conjecture)**.** In his *Disquisitiones Arithmeticae* (1801), Gauss posed that $h(-d) \to \infty$ as $d \to \infty$.

The class number problem has only been solved for small values of n (specifically, for $n \leq 7$ and odd $n \leq 23$). When $n = 1$, the imaginary quadratic field has a unique factorization. Gauss was the first to make progress on the class number problem for $n = 1$ when he found imaginary quadratic fields for small class numbers and believed that he had found all of

them. He did not have a proof yet, so the next big breakthrough occurred when Heilbronn proved the Gauss Conjecture in 1934 [Hei34].

3. Class Number One

Definition 3.1 (Heegner Number)**.** A Heegner number is a squarefree positive integer d for which the field $\mathbb{Q}(\sqrt{-d})$ has the class number $h(-d) = 1$.

The term is named after Heegner, who developed a faulty proof of the values and quantity of Heegner numbers. Later, Stark and Baker independently came up with correct proofs and showed that there were exactly 9 Heegner numbers, contrary to a previous proof by Heilbronn and Linfoot that showed there could be a tenth, larger value of $-d$ [Hei34].

Theorem 3.2 (Baker-Stark-Heegner Theorem, [CG12])**.** *There are exactly 9 Heegner numbers. These can be expressed as* $-d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$*, or equivalently,* $\delta \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$*, where* δ *is the discriminant of the imaginary quadratic field* $\mathbb{Q}(\sqrt{-d})$*.*

These sets differ because the discriminant Δ is defined to be

$$\Delta = \begin{cases} -d & \text{if } -d = 1 \pmod 4 \\ -4d & \text{if } -d = 2, 3 \pmod 4 \end{cases}$$

for an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$.

Because the vast majority of cases with which we are concerned in this paper relate to the first case, where $-d = 1 \pmod 4$, the discriminant of the quadratic field is generally referenced as $-d$, although it is not always equivalent to the $-d$ used in $\mathbb{Q}(\sqrt{-d})$. Thus, the discriminant of $\mathbb{Q}(\sqrt{-1})$ is -4, and that of $\mathbb{Q}(\sqrt{-2})$ is -8.

A lot of work was done on this problem before a final solution was determined and proved. The first mathematician to make official progress was Alan Baker.

Theorem 3.3 (Baker, [Bak66])**.** *There is are only nine imaginary quadratic fields with class number one.*

In his paper, he proves a theorem that says that for a sequence of algebraic numbers whose logarithms are linearly independent over the rational numbers and a separate sequence of real algebraic numbers that are linearly independent over the rational numbers, the set that takes the sequence of rational numbers to the power of the sequence of the real algebraic numbers is transcendental. This theorem proves Gauss's conjecture that there are only 9 imaginary fields.

Theorem 3.4 (Stark, [S$^+$67])**.** *There is no tenth imaginary quadratic field with class number one.*

Stark attempted to do the opposite of what Baker did. He first proves that if $h(-p) = 1$ then it is impossible to have $p \geq 200$. He does this through constructing several Diophantine equations,

$$\begin{aligned} z_{2N+1} - 4y_N &= a^3 + 3 & \tfrac{p+1}{4} &\equiv 1 \pmod 8 \\ z_{2N+1} + 4y_N &= a^3 + 3 & \tfrac{p+1}{4} &\equiv 5 \pmod 8 \\ z_{2N+1} + 4y_{N+1} &= a^3 - 3 & \tfrac{p+1}{4} &\equiv 3 \pmod 8 \\ z_{2N+1} - 4y_{N+1} &= a^3 - 3 & \tfrac{p+1}{4} &\equiv 7 \pmod 8, \end{aligned}$$

one of which should hold true if $p \geq 200$, and where N is a nonnegative integer that satisfies $h(-8p) = 4N + 2$. However, he later shows that there are no solutions to those Diophantine equations. In a separate section, Stark shows that when $p \geq 19$ and has a class number of 1, p must be a prime that is congruent to 19 (mod 24). This includes the all the Heegner numbers greater than 19, but also includes 139 which is not a Heegner number. Luckily, 139 can be removed because it is the discriminant of two unequal polynomials, $x^2 + xy + 35y^2$ and $5x^2 + xy + 7y^2$. Thus, Stark shows that the only Heegner numbers are those listed in Theorem 3.2.

3.1. **Heegner's Proof.** Heegner had written proofs involving the Heegner numbers; initially, he started with a proof that, if there were another Heegner number not included in the list of 9 numbers he had found previously, then the value of that Heegner number must be greater than 10^9. However, his later and more important proof was an attempt in proving that the nine values above were the only possible values by constructed a function with an infinite product and then simplifying it using known representations of the algebraic values [Hee52].

The function that Heegner constructed was

$$f(\omega) = q^{-124} \prod_{v=1}^{\infty} (1 + q^{2v+1}),$$

where $q = e^{i\pi\omega}$.

He defined

$$\gamma_2 = f(\omega)^1 6 - 16 f(\omega)^{-8}.$$

He knew that when $p \equiv 3 \pmod 4$ and $h(-p) = 1$, $\gamma_2(\frac{-3+\sqrt{-p}}{2})$ was a rational integer. Because of this, he found an equivalency between $f(\frac{-3+\sqrt{-p}}{2})$ and a degree 24 polynomial with integer coefficients of

$$x^{24} - \zeta_2 x^8 - 16 = 0.$$

Heegner reduced this polynomial to

$$x^{12} + 2^8 + 2\zeta^2 x^4 - 4 = 0.$$

He then used the relation of

$$-4\zeta(\zeta^3 + 4) = \gamma_2$$

to reduce the 12 degree polynomial to a 6 degree polynomial of

$$x^6 + 2^4 + 2^2 - 2 = 0.$$

Mathematicians doubt this reduction because Heegner has no proof for it. He seems to have been misled by a paper by Weber that made many conjectures about Diophantine equations. Heegner reduced his polynomial again with the relations

$$\zeta = 2(\beta - \alpha^2) \text{ and } \zeta^2 = 2(\beta^2 + 2\alpha)$$

which leads to

$$(\beta^2 - 2\alpha^2)^2 = 2\alpha(\alpha^3 + 1)$$

. This equation should lead to correct values of p whenever α and β were rational integers, and in fact it works for

$$p = 3, 11, 19, 43, 67, 163.$$

According to Stark, who later on wrote a paper (see [Sta69]) which attempted to explain where Heegner's proof went wrong, the last equation in terms of α and β also works when they are very close to rational integers, so the final equation may have extra answers that are not Heegner numbers.

4. Properties of Heegner Numbers

4.1. **Prime Generators.** The Heegner numbers are related to Euler's prime generating formula $n^2 - n + p$, where p is a prime. This generator produces primes from $n = 0, 1, ..., p-2$ when the field $\mathbb{Q}(\sqrt{1-4p})$ has a class number of 1. This is only satisfied by $-7, -11, -19, -43, -67,$ and -163.

For example, one of the most famous of these polynomials is $n^2 + n + 41$. Its discriminant is $-1 + 4 \cdot 41 = -163$.

4.2. **Almost Integers.** When Heegner numbers are put into the j-function, they produce values that are very close to integers. The formula $e^{\pi\sqrt{d}}$ yields numbers that are close to integers.

Definition 4.1 (j-function)**.** The j-function is defined by $j(\tau) = 1728J(\tau)$, where $J(\tau) \equiv 4/27[1 - \lambda(\tau) + \lambda^2(\tau)]^3/\lambda(\tau)[1 - \lambda(\tau)]^3$.

The integer that it approximates is given by $-j(\frac{1+\sqrt{d}}{2}) + 744$.

Interestingly, fields of class number two (fields that satisfy $h(-d) = 2$) also provide share the quality of producing almost integers. However, they are not considered Heegner numbers because they do not share the other qualities of a Heegner number.

4.3. **Transcendental Numbers.** The transcendental numbers are numbers that are complex numbers but not algebraic numbers. This means that they cannot be written as a root of a monic polynomial with integer coefficients.

Definition 4.2 (Ramanujan's Constant)**.** $e^{\pi\sqrt{163}}$ is very close to $640320^3 + 744$.

This occurs because of a relationship between the q-expansion and j-invariant. When the j-invariant is an algebraic integer, then $\mathbb{Q}(\sqrt{-d})$ has to have a class number one, so d is a Heegner Number. Other Heegner numbers also approximate integers, but the larger the Heegner number is, the closer $e^{\pi\sqrt{d}}$ is to an integer.

5. Connection to Riemann Hypothesis

Definition 5.1 (Dirichlet Character)**.** A completely multiplicative arithmetic function χ where there exists a positive integer k with $\chi(n + k) = \chi(n)$ for all n, $\chi(n) = 0$ whenever $\gcd(n, k) > 1$.

Every Dirichlet character has a corresponding L-function called the Dirichlet L-function:

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for any complex number s where the real part of $s > 1$.

Definition 5.2 (Generalized Riemann Hypothesis)**.** For every Dirichlet character χ and every complex number s with $L(\chi, s) = 0$, as long as s is not a negative number then the real part of s is $1/2$.

The generalized Riemann Hypothesis implies Gauss's conjecture because the $h(-d)$ would grow with the absolute value of d. Thus, as d increases indefinitely, so will $h(-d)$.

Theorem 5.3 (Hecke)**.** *If $d > 0$ and $\chi \pmod d$ is odd, real and primitive, then when $L(\chi, s) \neq 0$ for a real s where $s > 1 - \frac{c}{\log d}$,*

$$h(-d) > \frac{c_1\sqrt{d}}{\log d}$$

where c_1 and c are fixed constants. This bound shows that $h(-d)$ grows as d grows. Deuring connected the class number problem and the Riemann Hypothesis even further.

Theorem 5.4 (Deuring)**.** *If the Riemann Hypothesis is false, then $h(-d) \geq 2$ for sufficiently large d.*

6. Class Number Two

In 1971, Baker and Stark independently solved Gauss's class number problem for n = 2. They were each able to prove the following:

Theorem 6.1. *For the class number two, where $h(-d) = 2$, then $-d$ must be one of* $-15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403, \text{or} -427$.

Both Baker and Stark's proofs depend on the logarithms of algebraic numbers and are quite similar in technique, so we will cover Baker's proof here. (See [Sta75] for Stark's proof.) Namely, it requires the following results:

Theorem 6.2 ([Bak71])**.** *Suppose that $\alpha, \alpha', \beta, \beta', \beta''$ are nonzero algebraic numbers with degrees less than or equal to d, where $|\alpha'| \neq 1$ and $\alpha'' = -1$. Additionally, let the heights (i.e. the magnitude of a polynomial's greatest coefficient) of α, α' be less than or equal to $A \geq 2$ and those of β, β', β'' be less than or equal to $H^{(\log H)^2}$. Let $\log\alpha$, $\log\alpha'$, $\log\alpha''$ be linearly independent and have principle values. Then, if $\varepsilon, \delta > 0$ and*

$$|\beta \log\alpha + \beta' \log\alpha' + \beta'' \log\alpha''| < e^{-\delta H},$$

then $H < C(\log A)^{1+\varepsilon}$, where $C = C(A', d, \varepsilon, \delta)$ is an effectively computable function.

Theorem 6.3 ([Bak71])**.** *Suppose that p, q are primes where $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$, and let $\mathbb{Q}(\sqrt{-pq})$ have class number two. Furthermore, let $k > 4$ represent the discriminant of $\mathbb{Q}(\sqrt{k})$, and let $\chi(n) = (k/n)$ be the Kronecker symbol. Additionally, let $\gcd(k, pq) = 1$ and define*

$$f = f(x, y) = x^2 + xy + \tfrac{1}{4}(1 + pq)y^2.$$

Then, we have

$$\frac{k\sqrt{pq}}{2\pi} \sum_{x=-\infty}^{\infty} \sum_{y=-\infty}^{\infty} \frac{\chi(f)}{f} = h(k)h(-kpq)\log\varepsilon + h(kp)h(-kq)\log\eta,$$

where $(x, y) \neq (0, 0)$, $h(l)$ represents the class number of $\mathbb{Q}(\sqrt{l})$ and ε, η represent the fundamental units of the fields $\mathbb{Q}(\sqrt{k})$ and $\mathbb{Q}(\sqrt{kp})$, respectively.

For brevity, the proofs of these theorems have been excluded, although both can be found in Baker's original paper [Bak71].

To prove that all imaginary quadratic fields for which $h(-d) = 2$ can be determined, Baker used the results of numerous past papers. After assuming that $d = pq$ and that $q > d^{1/4}$, he equated the left hand side of Theorem 6.3 with the results of [Bak69]:

$$\frac{k\sqrt{d}}{2\pi} \sum_{x=-\infty}^{\infty} \sum_{y=-\infty}^{\infty} \frac{\chi(f)}{f} = \frac{\pi k\sqrt{d}}{6} \prod_{p|k} (1 - p^{-2}) + B_0 + \sum_{r=-\infty, r\neq 0}^{\infty} B_r e^{\pi i r/k},$$

where $B_0 = -2 \log p$ for some prime p if k is a power of p, or B_0 is otherwise equal to 0. Additionally,

$$B_r = 2e^{-\pi |r| \sqrt{d}/k} \sum_{y|r, y>0} y^{-1} \sum_{j-1}^{k} \chi(f(j, y)) e^{2\pi i j r/(yk)}.$$

Then, taking $k = 21$ and class number $h(k) = 1$, and using the result of Theorem 6.3, Baker derived the inequality

$$\left| h(-21d) \log \varepsilon + h(21p) h(-21q) \log \eta - \frac{64}{21} \pi \sqrt{d} \right| < e^{-(1/10)\sqrt{d}}$$

for large d. Now, Theorem 6.2 can be used with $d = 2$, $\delta = 1/10$ and some $\varepsilon > 0$ to obtain the inequality

$$\sqrt{d} < C(\sqrt{p} \log p)^{1+\varepsilon},$$

in which $C = C(\varepsilon)$ is effectively computable. However, the original assumptions included statements that $d = pq$ and $q > d^{1/4}$, which combine to give $p < d^{3/4}$. According to the inequality above, this is not true for $\varepsilon < \frac{1}{3}$. This contradiction establishes the result that the determinants of all imaginary quadratic fields of class number two can be determined.

7. Higher Class Numbers

In 1985, Oesterlé was able to classify the imaginary quadratic fields with class number 3 [Oes85] through the application of the L-functions of elliptic curves, after similar discoveries by Goldfeld allowed for this breakthrough [Gol85]. Nearly two decades later, Watkins was able to extend this technique to calculate the imaginary quadratic fields of much higher class numbers [Wat04]. After extensive computation, he was able to obtain the classifications for imaginary quadratic fields of class numbers less than or equal to 100, which are summarized in his paper. In total, the process took seven months, at a rate of calculation of 2^{26} discriminants per second. For now, Watkins' computations are the most complete in solving the class number problem.

8. Conclusion

Gauss' class number problem is interesting because of how much work needs to be done. Although we have complete lists for some small class numbers, there are infinitely more integers with incomplete lists. The bounds can still be improved and more effective algorithms can be developed for shorter computation times.

References

[Bak66] A. Baker. Linear forms in the logarithms of algebraic numbers. *Mathematika*, 13(2):204–216, 1966.

[Bak69] A. Baker. A Remark on the Class Number of Quadratic Fields. *Bulletin of the London Mathematical Society*, 1(1):98–102, 03 1969.

[Bak71] A. Baker. Imaginary quadratic fields with class number 2. *Annals of Mathematics*, 94(1):139–152, 1971.

[CG12] John H Conway and Richard Guy. *The Book of Numbers*. Springer Science & Business Media, 2012.

[Gol85] Dorian Goldfeld. Gauss' class number problem for imaginary quadratic fields. *Bulletin of the American Mathematical Society*, 13(1):23–37, 1985.

[Hee52] Kurt Heegner. Diophantische analysis und modulfunktionen. *Mathematische Zeitschrift*, 56:227–253, 1952.

[Hei34] Hans Heilbronn. On the class-number in imaginary quadratic fields. *The Quarterly Journal of Mathematics*, (1):150–160, 1934.

[Oes85] Joseph Oesterlé. Nombres de classes des corps quadratiques imaginaires. *Astérisque*, 121-122:309–323, 1985.

[S$^+$67] Harold M Stark et al. A complete determination of the complex quadratic fields of class-number one. *The Michigan Mathematical Journal*, 14(1):1–27, 1967.

[Sta69] Harold M Stark. On the "gap" in a theorem of Heegner. *Journal of Number Theory*, 1(1):16–27, 1969.

[Sta75] H. M. Stark. On complex quadratic fields with class-number two. *Mathematics of Computation*, 29(129):289–302, 1975.

[Wat04] Mark Watkins. Class numbers of imaginary quadratic fields. *Mathematics of Computation*, 73:907–938, 2004.