BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 13, Number 1, July 1985

GAUSS' CLASS NUMBER PROBLEM FOR IMAGINARY QUADRATIC FIELDS

BY DORIAN GOLDFELD[1]

1. Early history. In 1772 Euler [11] thought it noteworthy to remark that

$$x^2 - x + 41 = \text{prime}, \qquad x = 1, 2, \ldots, 40.$$

This subject was again touched upon by Legendre [28] in 1798 when he announced

$$x^2 + x + 41 = \text{prime}, \qquad x = 0, 1, \ldots, 39.$$

These remarkable polynomials, which take on prime values for many values of x, are one of the earliest recorded instances of a phenomenon related to what is now commonly referred to as Gauss' class number one problem. In fact, at the Fifth International Congress of Mathematicians, Rabinovitch [34] stated the following

THEOREM (RABINOVITCH). $D < 0$, $D \equiv 1 \pmod 4$,

$$x^2 - x + \frac{1 + |D|}{4} = prime, \qquad x = 1, 2, \ldots, \frac{|D| - 3}{4},$$

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

A similar theorem holds for the polynomial $x^2 + x + (1 + |D|)/4$. It is known that $Q(\sqrt{-163})$ has the unique factorization property, and this accounts for the remarkable polynomials above.

Gauss' class number problem has a long, curious, and interesting history. Perhaps the subject really goes back to Fermat, who in 1654 stated theorems like (here p = prime)

$$p = 6n + 1 \Rightarrow p = x^2 + 3y^2,$$
$$p = 8n + 1 \Rightarrow p = x^2 + 2y^2,$$

which were first proved by Euler in 1761 and 1763. Many other representation theorems of integers as sums of squares were proved in the eighteenth century,

Received by the editors February 27, 1985.
1980 *Mathematics Subject Classification*. Primary 12A50, 12A25; Secondary 12-03.

[1] The author gratefully acknowledges the generous support of the Vaughn Foundation during the past year.

and in 1773 Lagrange [27], for the first time, developed a general theory of binary quadratic forms

$$(1) \qquad ax^2 + bxy + cy^2,$$

with discriminant $D = b^2 - 4ac$, to handle the general problem of when an integer m is representable by the form

$$(2) \qquad m = ax^2 + bxy + cy^2.$$

It is clear that under a linear change of variables

$$(3) \qquad \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}, \qquad \alpha\delta - \beta\gamma = +1, \qquad \alpha, \beta, \gamma, \delta \in \mathbf{Z},$$

we have

$$ax^2 + bxy + cy^2 = Ax'^2 + Bx'y' + Cy'^2,$$

where

$$\begin{aligned} A &= a\alpha^2 + b\alpha\gamma + c\gamma^2, \\ B &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \\ C &= a\beta^2 + b\beta\delta + c\delta^2, \end{aligned}$$

and, therefore, the two binary quadratic forms

$$ax^2 + bxy + cy^2, \qquad Ax'^2 + Bx'y' + Cy'^2$$

represent the same set of integers. Denoting these two forms as (a, b, c), (A, B, C), respectively, Lagrange defined them to be equivalent since he was primarily interested in the representation problem (2).

We shall also write $(a, b, c) \sim (A, B, C)$ if the binary quadratic form (A, B, C) can be obtained from (a, b, c) by a linear change in variables (3); and we reiterate Lagrange's basic principle that equivalent forms represent the same integers.

Lagrange developed a reduction theory for binary quadratic forms and showed that every form is equivalent to a certain canonically chosen reduced form. This idea was also further developed by Gauss. A modern account of reduction theory goes as follows.

Given two equivalent forms $(a, b, c) \sim (A, B, C)$ with discriminant

$$D = b^2 - 4ac = B^2 - 4AC < 0,$$

we can associate two complex numbers,

$$w = (-b + \sqrt{D})/2a, \qquad w' = (-B + \sqrt{D})/2A,$$

lying, say, in upper half-plane $\mathfrak{H}$. Then w is equivalent to w' ($w \sim w'$) in the sense that

$$w = (\alpha w' + \beta)/(\gamma w' + \delta),$$

where $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ is the unimodular transformation given by (3).

A form is called reduced if its associated complex number w lies in the fundamental domain for the modular group SL(2, **Z**), i.e.,

$$w \in \mathrm{SL}(2, \mathbf{Z}) \backslash \mathfrak{H}.$$

It is then easy to check that a reduced form satisfies $-a < b \leqslant a \leqslant c$ or $0 \leqslant b \leqslant a = c$. Every form is equivalent to a canonical unique reduced form.

DEFINITION 1. *Let $h(D)$ denote the number of inequivalent binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $D = b^2 - 4ac$.*

In his book of 1798 Legendre simplified Lagrange's work, proved the law of quadratic reciprocity assuming there exist infinitely many primes in an arithmetic progression, introduced a composition of two forms, and defined the Legendre symbol

$$\left(\frac{n}{p}\right) = \begin{cases} +1, & n \equiv x^2 \pmod{p}, \\ -1, & n \not\equiv x^2 \pmod{p}, \\ 0, & p | n. \end{cases}$$

His book [**28**] became almost immediately obsolete, however, with the publication in 1801 of Gauss' *Disquisitiones arithmeticae* [**12**].

Perhaps one of the most remarkable parts of the *Disquisitiones* is the section where Gauss defines the composition of two binary quadratic forms and (without knowing what a group is) proves that the classes of binary quadratic

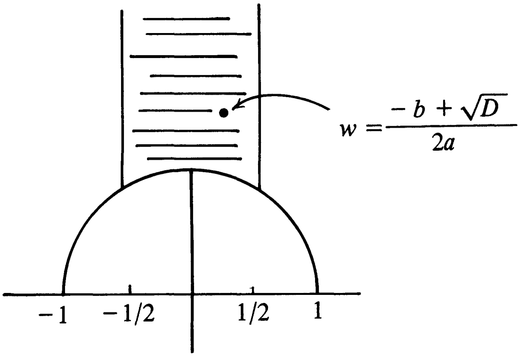

FIGURE 1

forms with given discriminant form a finite group with composition as a group law. In fact, he even proves that this group is a direct product of cyclic groups, and, as I understand from Mackey, Gauss' proof can be generalized to prove that any finite abelian group is a direct product of cyclic groups!

In article 303 of the *Disquisitiones*, Gauss enunciated the

CONJECTURE. *The number of negative discriminants $D < 0$ which have a given class number h is finite.*

It is important to point out that Gauss' definition of binary quadratic form is slightly different from Lagrange's in that he considers the form

$$ax^2 + 2bxy + cy^2 \tag{4}$$

with even middle coefficient and defines the discriminant as

$$D = b^2 - ac. \tag{5}$$

In article 303 he gives tables of discriminants having a given class number and conjectures that his tables are complete.

For the moment we shall stick to Gauss' notation (4), (5) and let $h(D)$ be the number of inequivalent forms of type (4). It is not well known that Gauss' class number one table was first shown to be complete by Landau [25] in 1902.

THEOREM (LANDAU). *For $D = b^2 - ac < -7$, $h(D) > 1$.*

This is due to the fact that Gauss' definitions (4), (5) really pertain to even discriminants, and, therefore, correspond to a much simpler problem.

Let us now state the modern version of the class number problem. It is convenient to return to the Lagrangian notation

$$ax^2 + bxy + cy^2, \qquad D = b^2 - 4ac < 0. \tag{6}$$

Gauss' class number problem: To find an effective algorithm for determining all negative discriminants with given class number h.

Lagrange's notation (6) is really better suited to the modern reinterpretation of the theory of binary quadratic forms in terms of the theory of quadratic fields. To each binary quadratic form

$$ax^2 + bxy + cy^2 \tag{7}$$

of discriminant D we can associate an ideal (see [7])

$$\left[a, (-b + \sqrt{D})/2\right] \quad \mathbf{Z}\text{-module} \tag{8}$$

in the ring of integers of $Q(\sqrt{D})$. Two ideals $\mathfrak{a}$, $\mathfrak{b}$ are equivalent ($\mathfrak{a} \sim \mathfrak{b}$) if there exist principal ideals (λ_1), (λ_2) such that $\mathfrak{a}(\lambda_1) = \mathfrak{b}(\lambda_2)$. It can then be shown that equivalent ideals of type (8) correspond to equivalent forms (in the Lagrangian sense) of type (7).

The ideal classes of $Q(\sqrt{D})$ form a group; we let $h(D)$ denote the order of this group. When $h(D) = 1$, every ideal in $Q(\sqrt{D})$ is principal, and the integers of $Q(\sqrt{D})$ have unique factorization.

Gauss' class number one problem: $h(D) = 1$ *for* $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$ *and for no other* $D < -163$.

2. Dirichlet's class number formula. The problem of the arithmetic progression, that there exist infinitely many primes in the arithmetic progression a, $a+q$, $a+2q$, $a+3q, \ldots$, where $(a,q)=1$, first fell in 1837 for the case $q=$ prime, and for arbitrary q in 1839 [**10**], in the now classic papers of Dirichlet. It was well known at the time that Euler's proof (1748),

$$\infty = \sum \frac{1}{n} = \prod \left(1 - \frac{1}{p}\right)^{-1},$$

of the infinitude of primes did not work for primes in an arithmetic progression since there is no natural series representation for the product

$$\prod_{p \equiv a \, (\mathrm{mod}\, q)} \left(1 - \frac{1}{p}\right)^{-1}.$$

Dirichlet remedied this situation by introducing, for the first time, group characters

$$\chi \colon \mathbf{Z}/q\mathbf{Z} \to \text{roots of unity}$$

which satisfy

$$\begin{aligned} &\chi(n+q) = \chi(n), && \forall n \in \mathbf{Z}, \\ &\chi(mn) = \chi(m)\chi(n), && \forall m, n \in \mathbf{Z}, \\ &\chi(n) = 0, && (n,q) > 1. \end{aligned}$$

There are $\phi(q)$ such characters $\chi \pmod q$, and they satisfy the orthogonality relation

$$(9) \qquad \frac{1}{\phi(q)} \sum_{\chi \, (\mathrm{mod}\, q)} \bar{\chi}(a)\chi(n) = \begin{cases} 1, & n \equiv a \pmod q, \\ 0, & n \not\equiv a \pmod q. \end{cases}$$

Dirichlet defined the L-function

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \qquad (\mathrm{Re}(s) > 1)$$

from which it follows, by logarithmic differentiation and (9), that

$$(10) \qquad -\frac{1}{\phi(q)} \sum_{\chi \, (\mathrm{mod}\, q)} \bar{\chi}(a) \frac{L'}{L}(s,\chi) = \sum_{p^m \equiv a \, (\mathrm{mod}\, q)} (\log p) p^{-ms}.$$

He considered the limit as $s \to 1$. Since

$$\sum_p \sum_{m \geqslant 2} (\log p) p^{-m} < \infty,$$

the existence of infinitely many primes in an arithmetic progression is reduced to showing that the left side of (10) blows up as $s \to 1$. The trivial character ($\chi(n) = 1$ for $(n,q) = 1$) occurs in (10) and contributes the logarithmic derivative of the Riemann zeta function which has a pole at $s = 1$. Since all other Dirichlet L-functions $L(s,\chi)$ are holomorphic at $s = 1$, it is enough to show that $L(1,\chi) \neq 0$. This Dirichlet did in a most remarkable way. We illustrate his argument for real characters, since the case of complex χ is much easier.

Let $D < 0$, D a fundamental discriminant; $\chi \pmod D$ a real, odd, primitive Dirichlet character. Let $h(D)$ denote the class number of $Q(\sqrt{D})$ and set

$$w = \begin{cases} 2, & D < -4, \\ 4, & D = -4, \\ 6, & D = -3, \end{cases}$$

to be the number of roots of unity in the field.

THEOREM (DIRICHLET). $L(1, \chi) = 2\pi h(D)/w\sqrt{|D|}$.

This is Dirichlet's famous class number formula, which was conjectured in simpler form by Jacobi [**24**, 7] in 1832 and proved in full by Dirichlet [**10**] in 1839. It is remarkable how the class number and special value $L(1, \chi)$ relate in this way.

Since $h(D) \geqslant 1$, this implies $L(1, \chi) \neq 0$, from which Dirichlet deduced the infinitude of primes in an arithmetic progression.

A brief sketch of Dirichlet's proof in modern notation goes as follows. For $z = x + iy$, $x \in \mathbf{R}$, $y > 0$, let

$$E(z, s) = \frac{1}{2} \sum_{(m,n)=1} \frac{y^s}{|mz + n|^{2s}} \tag{11}$$

be the Eisenstein series which satisfies the functional equation

$$E^*(z, s) = \pi^{-s}\Gamma(s)\zeta(2s)E(z, s) = E^*(z, 1 - s)$$

and has simple poles at $s = 0, 1$ with residue independent of z.

Although Eisenstein series hadn't been invented yet, Dirichlet did introduce zeta functions

$$\sum_{\substack{m,n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(am^2 + bmn + cn^2)^s}$$

associated with a binary quadratic form (a, b, c) of discriminant $b^2 - 4ac = D < 0$. These, however, are just special cases of the Eisenstein series (11) when $z = (-b + \sqrt{D})/2a$.

Dirichlet showed that

$$\left(\frac{\sqrt{|D|}}{2\pi}\right)^s \Gamma(s)\zeta(s)L(s, \chi) = \frac{1}{w} \sum_{\substack{b^2-4ac=D \\ -a<b\leqslant a\leqslant c \\ \text{or } 0<b\leqslant a=c}} E^*\left(\frac{-b + \sqrt{D}}{2a}, s\right), \tag{12}$$

from which he deduced the class number formula by comparing residues at $s = 1$. Formula (12) is simply stating that the zeta function of an imaginary quadratic field $Q(\sqrt{D})$, $D < 0$, is just the sum of the zeta functions of the $h(D)$ ideal classes.

3. The Deuring-Heilbronn phenomenon and Siegel's zero. Very little progress on Gauss' original class number conjecture was made until the twentieth century. In 1918 Landau [**26**] published the following theorem, which he attributed to a lecture given by Hecke.

THEOREM (HECKE). *Let* $D < 0$, $\chi \pmod D$ *odd, real, and primitive. If* $L(s, \chi) \neq 0$ *for* s *real and* $s > 1 - c/\log|D|$, *then*

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

where $c, c_1 > 0$ *are fixed absolute constants.*

Now, the generalized Riemann hypothesis asserts that the only nontrivial zeros of $L(s, \chi)$ are on the line $\mathrm{Re}(s) = 1/2$. So Hecke showed that the generalized Riemann hypothesis implies Gauss' conjecture, since the class number $h(D)$ would then grow with $|D|$.

In 1933, Deuring [**8**] proved the following unexpected and surprising result.

THEOREM (DEURING). *If the classical Riemann hypothesis is false, then* $h(D) \geqslant 2$ *for* $-D$ *sufficiently large.*

This was improved upon by Mordell [**30**] in 1934.

THEOREM (MORDELL). *If the classical Riemann hypothesis is false, then* $h(D) \to \infty$ *as* $D \to -\infty$.

Again in 1934, Heilbronn [**21**] went a step further.

THEOREM (HEILBRONN). *The falsity of the generalized Riemann hypothesis implies* $h(D) \to \infty$ *as* $D \to -\infty$.

When combined with Hecke's theorem, this gave an unconditional proof of Gauss' conjecture.

THEOREM (HECKE-DEURING-HEILBRONN). $h(D) \to \infty$ as $D \to -\infty$.

Here was the first known instance of a proof which first assumed that the generalized Riemann hypothesis was true and then that it was false, giving the right answer in both cases! Unfortunately, the method of proof was not effective, since if the generalized Riemann hypothesis were false, all constants would depend on an unknown zero of $L(s, \chi)$ located off the line $\mathrm{Re}(s) = 1/2$. This presumably nonexistent zero is now known as Siegel's zero.

Heilbronn and Linfoot [**22**] refined the proof to deal with Gauss' class number one problem. They showed

THEOREM (HEILBRONN-LINFOOT). *There are at most ten negative fundamental discriminants* $D < 0$ *for which* $h(D) = 1$: *namely,* $D = -3, -4, -7, -8, -11, -19, -43, -67, -163,$?

The possible existence of a tenth imaginary quadratic unique factorization field reflected the ineffectivity in the Deuring-Heilbronn proof. If such a field existed, the generalized Riemann hypothesis could not be true! This led to intense, fervent, and sometimes heated research on this problem.

In 1935, Siegel [35] practically squeezed the last drop out of the classical Hecke-Deuring-Heilbronn phenomenon.

THEOREM (SIEGEL). *For every $\varepsilon > 0$, there exists a constant $c > 0$ which cannot be effectively computed such that*

$$h(D) > c|D|^{1/2-\varepsilon}.$$

Tatuzawa [41] went a step further and showed that Siegel's theorem is true with an effectively computable constant $c > 0$ for all $D < 0$, except for at most one exceptional discriminant D.

Perhaps the simplest proof of Siegel's theorem is in Goldfeld's [15] half-page note. This method was further developed by Hoffstein [23] to yield a simple proof of Tatuzawa's theorem.

Due to its ineffectivity, the whole line of attack outlined in this section still did not solve Gauss' class number problem as stated in §1. Except for some simple cases, Gauss' tables of class numbers were not known to be complete. All that was known was that if Gauss was wrong then the generalized Riemann hypothesis had to be false. One can well imagine how this topic generated many a discussion in the coffee houses of Europe in the late 1940s and 1950s.

At the time, a high school teacher named Kurt Heegner was going around telling people he had solved the Gauss class number one problem. His paper [20], *Diophantische Analysis und Modulfunktionen*, was published in 1952. It is fitting to quote from the referee's report for *Mathematical Reviews*.

"*The author proves in addition, by extending certain results of Weber on complex multiplication, that the only quadratic fields with negative discriminant and class number unity are the known classical cases.*"

Heegner's paper contained some mistakes and was generally discounted at the time. He died before anyone really understood what he had done.

4. The Birch-Swinnerton-Dyer Conjecture. Let

$$E\colon y^2 = 4x^3 - ax - b \tag{13}$$

be an elliptic curve over Q with discriminant $\Delta = a^3 - 27b^2 \neq 0$. If $(x, y) \in E$, with x and y both rational numbers, we say (x, y) is a rational point on E. Let $E(Q)$ denote the set of rational points on E, including the point at ∞. Then $E(Q)$ is a finitely generated abelian group [31]. The group law is given as follows. The 0 element is the point at infinity. If $P = (x, y)$, then $-P = (x, -y)$, and the sum of three collinear points is 0.

If we graph E in the x-y plane, we have (Figure 2) $P_1 + P_2 = Q$, where $Q = -P_3$.

Let g denote the number of independent generators of infinite order of $E(Q)$. Then

$$E(Q) \cong \mathbf{Z}^g \oplus \{\text{torsion subgroup}\}, \tag{14}$$

where the torsion subgroup is also finitely generated and consists of points of finite order. A deep and beautiful theorem of Mazur [29] asserts that a torsion point can have order at most twelve.

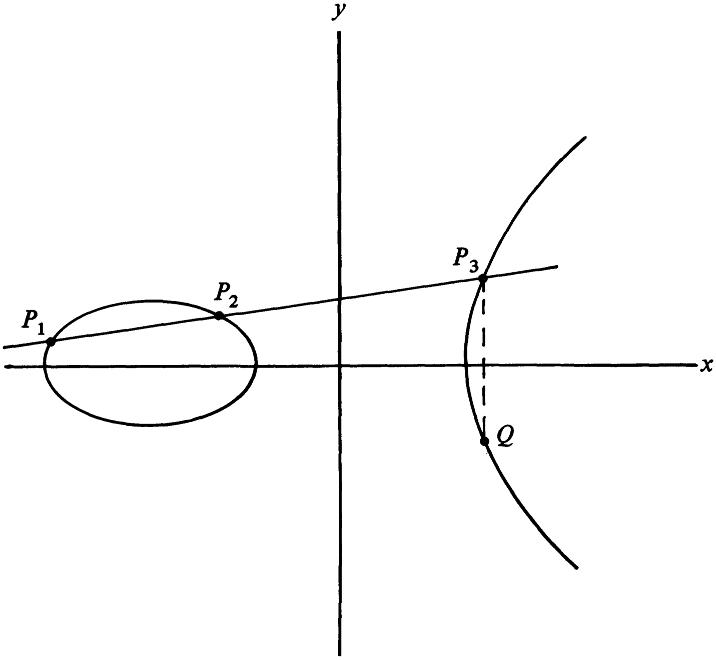

FIGURE 2

The decomposition (14) was essentially conjectured by Poincaré, first proved by Mordell [31], and generalized by Weil [42]. It was known to Diophantus that the line connecting two rational points on E must intersect at a third rational point. Then Poincaré's conjecture is equivalent to the fact that all the rational points on E can be obtained from a finite number of generators by drawing all possible chords and tangents between these points, generating new points, again drawing all possible chords and tangents, and continuing on ad infinitum.

Associated to the curve E given by (13) there is an integer N called the conductor of E. Here N is divisible only by primes dividing the discriminant Δ and the power of the prime that occurs depends only on the reduction of E by that prime.

We can now define the Hasse-Weil L-function associated with E.

$$L_E(s) = \prod_{p|N} \left(1 - t_p p^{-s}\right)^{-1} \prod_{p\nmid N} \left(1 - t_p p^{-s} + p^{1-2s}\right)^{-1}, \tag{15}$$

where

$$t_p = \begin{cases} p - N_p, & p \nmid N, \\ \pm 1 \text{ or } 0, & p|N, \end{cases}$$

and

$$N_p = \operatorname{Card}\{(x, y) \pmod{p} \colon y^2 \equiv 4x^3 - ax - b \pmod{p}\}.$$

By the Riemann hypothesis for curves over finite fields (Hasse [19] 1933, Weil [43]),

$$|t_p| \leqslant 2\sqrt{p}\,.$$

It follows that the Euler product given by (15) converges absolutely for $\mathrm{Re}(s) > 3/2$.

Now, Tanayama and Weil [44] have conjectured that $L_E(s)$ has a holomorphic continuation to the entire complex s-plane and satisfies the functional equation

$$\left(\frac{\sqrt{N}}{2\pi}\right)^{s}\Gamma(s)L_E(s) = \pm\left(\frac{\sqrt{N}}{2\pi}\right)^{2-s}\Gamma(2-s)L_E(2-s). \tag{16}$$

Moreover, the inverse Mellin transform of $L_E(s)$ should correspond to a holomorphic cusp form of weight two for the congruence subgroup of the modular group of level N. If this is the case, then E is called a modular curve and (16) is true.

We can now state

CONJECTURE (BIRCH-SWINNERTON-DYER [5]). *If* $\mathrm{rank}(E(Q)) = g$, *then*

$$L_E(s) \sim c_E(s-1)^g,$$

where the constant c_E *can also be explicitly conjectured in terms of the order of the Tate-Safarevic group and the determinant of the height pairing of the g generators of* $E(Q)$.

5. The solution of Gauss' class number problem. In this final part of our saga, I should like to describe, in chronological order, the series of papers that ultimately solved the class number problems.

1966	Baker [1]	*There is no tenth imaginary quadratic field with class number one.*
1967	Stark [37]	

REMARKS. Baker used an idea of Gelfond and Linnik [13], who showed that the class number one problem could be solved if one had linear independence of three logarithms. He reduced the problem to a finite amount of computation. Stark's proof was totally different from Baker's but very similar to Heegner's. He actually proved that a tenth field did not exist.

1968	Deuring [9]:	*Fills in gap in Heegner's proof.*
1968	Siegel [36]:	*Gives another proof of class number one.*
1969	Stark [39]:	*On the "gap" in a theorem of Heegner.*
1969	Stark [38]:	*He shows that Gauss' class number one conjecture could have been solved in* 1949 *by Gelfond and Linnik by showing that linear independence in only two logarithms is needed.*

1970 Chowla [**6**]: *Wrote the paper, "The Heegner-Stark-Baker-Deuring-Siegel theorem."*

1971 Baker [**2**]
1971 Stark [**40**] *There are exactly eighteen imaginary quadratic fields with class number two.*

REMARKS. In these papers, Stark and Baker solve the class number two problem and show that the possible nineteenth field does not exist. They use the method of linear independence of logarithms.

1975 Goldfeld [**16**]: *If $h(D) < \varepsilon\sqrt{|D|}/\log|D|$ with $\varepsilon > 0$ sufficiently small, then there exists a real number $\beta < 1$ such that, for $\chi \pmod D$ real, odd, primitive, $L(\beta, \chi) = 0$, and β is given asymptotically as $D \to -\infty$ by*

$$1 - \beta \sim \frac{6}{\pi^2}L(1,\chi) \sum_{\substack{b^2-4ac=D \\ -a<b\leqslant a\leqslant c \\ \text{or } 0\leqslant b\leqslant a=c}} \frac{1}{a}.$$

REMARK. This violently contradicts the generalized Riemann hypothesis. The number β is called the Siegel zero.

1976 Goldfeld [**16, 17**]: Let E be an elliptic curve over Q with Hasse-Weil L-function $L_E(s)$. Let $g = \text{rank}(E(Q))$, $N = \text{conductor}(E)$. Fix $D < 0$ a fundamental discriminant and $Q(\sqrt{D})$ an imaginary quadratic field. Let $\chi \pmod D$ be the real, odd, primitive Dirichlet character associated to $Q(\sqrt{D})$.

THEOREM (GOLDFELD). *Choose $\mu = 1, 2$ so that $\chi(-N) = (-1)^{g-\mu}$. If $L_E(s) \sim c_E(s-1)^g$ then, for $(D, N) = 1$,*

$$h(D) > \frac{c}{g^{4g}N^{13}}(\log|D|)^{g-\mu-1}\exp\{-21\sqrt{g\log\log|D|}\},$$

where c is an absolute constant independent of E.

REMARKS. There is a similar theorem if $(D, N) > 1$. If the Birch-Swinnerton-Dyer conjecture is true for a suitable fixed elliptic curve of rank $g = 3$, then this theorem effectively solves the general Gauss class number problem; i.e., the Gauss conjecture is reduced to showing that there exists an elliptic curve whose Hasse-Weil L-function has a triple zero at $s = 1$!

1981 Birch-Stephens [**4**]:

Birch [3], already in 1968, utilized the remarkable method of Heegner [**20**] for constructing canonical points of infinite order on certain classes of elliptic curves.

Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z}) : c \equiv 0 \pmod{N} \right\},$$

$$w = f(z)\,dz \text{ be invariant for } \Gamma_0(N),$$

so that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

For $z \in \Gamma_0(N) \backslash \mathfrak{H}$ set

$$\pi(z) = \int_z^\infty w \in E$$

for a certain elliptic curve E which occurs as an abelian subvariety of the Jacobian variety of $\Gamma_0(N) \backslash \mathfrak{H}$.

Now, fix $d < 0$ and choose (a, b, c) and $z \in \mathfrak{H}$ satisfying $b^2 - 4ac = d$, $a \equiv 0$ (N), $b \equiv r$ $(2N)$, $r^2 \equiv d$ $(4N)$, $az^2 + bz + c = 0$. There will be $h(d)$ such points $z = z_1, z_2, \ldots, z_h$. The Heegner point P_d is defined as the trace

$$P_d = \pi(z_1) + \cdots + \pi(z_h) \in E\big(Q(\sqrt{D})\big).$$

We quote from Birch and Stephens' paper [4], where they conjecture:

> If E is an elliptic curve over Q which is parametrised by modular functions, and K is a complex quadratic field such that the Mordell-Weil group $E(K)$ of K-rational points of E has odd rank, then the "canonical" K-rational point of E which is given by Heegner's construction has Tate height measured by $L'_{E/K}(1)$.
>
> Unhappily, it is a consequence of this conjecture that the Heegner point turns out to be trivial whenever the rank is more than one.

1983 Gross-Zagier [**18**]:

Let E: $my^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over Q with conductor N and odd rank g. For $d < 0$, $d \equiv \square \,(\mathrm{mod}\, 4N)$, let

$$E^{(d)}\colon\ mdy^2 = x^3 + ax^2 + bc + c.$$

THEOREM (GROSS-ZAGIER). *If $L_E(s)$ has an odd order zero at $s = 1$, then there exists a Heegner point $P_d \in E(Q)$ such that*

$$L'_E(1) L_{E^{(d)}}(1) = \big(\pi^2 w / \sqrt{|d|}\big) \langle P_d, P_d \rangle,$$

where w is a certain period of E and $\langle\ ,\ \rangle$ is the height pairing.

REMARKS. This theorem solves the conjectures of Birch-Stephens [**4**]. For the special example

$$E_0\colon\ -139y^2 = x^3 + 4x^2 - 48x + 80$$

with $N = 37 \cdot (139)^2$, $g = 3$, it can be shown that the Heegner point P_{-139} is trivial. The Gross-Zagier theorem then gives

COROLLARY (GROSS-ZAGIER). *$L_{E_0}(s)$ has a triple zero at $s = 1$.*

Combined with Goldfeld's theorem [**16**], this yields

THEOREM (GOLDFELD-GROSS-ZAGIER). *For every $\varepsilon > 0$ there exists an effectively computable constant $c > 0$ such that $h(D) > c(\log|D|)^{1-\varepsilon}$.*

REMARK. This theorem solves (up to a finite amount of computation) the general Gauss class number problem.

1984 Oesterlé [**33**]:

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

REMARKS. Oesterlé obtained this result by computing the constant in Goldfeld's theorem [**16**] for the special curve E_0 mentioned above. His method of proof is also simpler than [**16**] at various points. Using instead the elliptic curve of conductor 5077 found by Brumer and Kramer, Oesterlé computed 1/55 instead of 1/7000. It was only very recently shown by Mestre, Oesterlé and Serre that this curve is modular. Combined with the bounds of Montgomery-Weinberger [**32**] (that $h(D) \neq 3$ for $907 < -D < 10^{2500}$), this gives the complete list of all imaginary quadratic fields with class number three. The complete list of all imaginary quadratic fields with class number 1, 2, or 4 would determine the complete finite list of all integers n which have a unique representation as a sum of three squares:

$$n = x^2 + y^2 + z^2 \qquad (x \geqslant y \geqslant z \geqslant 0).$$

We conclude with a few remarks to elucidate some of the deep inherent difficulties underlying Gauss' class number conjectures. For fixed integers a, b, c with $b^2 - 4ac = D < 0$ and $|D|$ sufficiently large, the zeta function

$$\sum_{m=-\infty}^{\infty} \sum_{\substack{n=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \frac{1}{(am^2 + bmn + cn^2)^s}$$

has a functional equation similar to the zeta function of $Q(\sqrt{D})$ but, nevertheless, has a real zero near one. It does not have an Euler product, however. Associated to an Eisenstein series for a suitable noncongruence subgroup of SL(2, **Z**), there will be a zeta function (associated to the constant term in the Fourier expansion) which has a functional equation similar to the Riemann zeta function but has a real zero near one. Finally, there exist Selberg zeta functions of order two associated to discrete subgroups of SL(2, **R**) which satisfy the Riemann hypothesis and have functional equations, Euler products, and real zeros near one.

REFERENCES

1. A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), 204–216.

2. ______, *Imaginary quadratic fields with class number two*, Ann. of Math. (2) **94** (1971), 139–152.

3. B. J. Birch, *Diophantine analysis and modular functions*, Algebraic Geometry,(Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, 1969, pp. 35–42.

4. B. J. Birch and N. M. Stephens, *Heegner's construction of points on the curve* $y^2 = x^3 - 1728e^3$ (Séminaire de Théorie des Nombres, Paris, 1981–1982), Birkhäuser, Boston, 1983, pp. 1–19.

5. B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves*, J. Reine Angew. Math. **218** (1965), 79–108.

6. S. Chowla, *The Heegner-Stark-Baker-Deuring-Siegel theorem*, J. Reine Angew. Math. **241** (1970), 47–48.

7. H. Davenport, *Multiplicative number theory*, Graduate Texts in Math., vol. 74, 2nd ed., Springer-Verlag, New York, 1980, pp. 43–53.

8. M. Deuring, *Imaginär-quadratische Zahlkörper mit der Klassenzahl* (1), Math. Z. **37** (1933), 405–415.

9. ______, *Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins*, Invent. Math. **5** (1968), 169–179.

10. L. Dirichlet, *Recherches sur diverse applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. **19** (1839); ibid. **21** (1840).

11. L. Euler, Mém. de Berlin, année 1722, 36; Comm. Arith. **1**, 584.

12. C. F. Gauss, *Disquisitiones arithmeticae*, 1801.

13. A. O. Gelfond, *Transcendental and algebraic numbers*, Dover, New York, 1960.

14. D. M. Goldfeld, *An asymptotic formula relating the Siegel zero and the class number of quadratic fields*, Ann. Scuola Norm. Sup. Pisa (4) **2** (1975), 611–615.

15. ______, *A simple proof of Siegel's theorem*, Proc. Nat. Acad. Sci. U.S.A. **71** (1974), 1055.

16. ______, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa (4) **3** (1976), 623–663.

17. ______, *The conjectures of Birch and Swinnerton-Dyer and the class number of quadratic fields*, Journées Arith. de Caen (Univ. Caen, Caen, 1976), Astérisque nos. 41–42, Soc. Math. France, 1977, pp. 219–227.

18. B. Gross and D. Zagier, *Points de Heegner et derivées de fonctions L*, C. R. Acad. Sci. Paris **297** (1983), 85–87.

19. H. Hasse, *Beweis analogous der Riemannschen Vermutung für die Artinsche und F. K. Schmidtschen Kongruenz-zetafunktionen in gewisse elliptischen Fallen*, Nachr. Akad. Wiss. Göttingen (1933), 253–262.

20. K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253.

21. H. Heilbronn, *On the class number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. 2 **5** (1934), 150–160.

22. H. Heilbronn and E. H. Linfoot, *On the imaginary quadratic corpora of class number one*, Quart. J. Math. Oxford Ser 2 **5** (1934), 293–301.

23. J. Hoffstein, *On the Siegel-Tatuzawa theorem*, Acta Arith. **38** (1980), 167–174.

24. C. G. J. Jacobi, J. Math. **9** (1832), 189–192.

25. E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante*, Math. Ann. **56** (1902), 671–676.

26. ______, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Göttinger Nachr. (1918), 285–295.

27. J. L. Lagrange, *Recherches d'arithmétique*, Nouv. Mém. Acad. Berlin (1773), 265–312; Oeuvres, III, pp. 693–758.

28. A. M. Legendre, *Théorie des nombres*, Libraire Scientifique A. Hermann, Paris, 1798, pp. 69–76; 2nd ed., 1808, pp. 61–67; 3rd ed., 1830, pp. 72–80.

29. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. No. 47 (1978), 33–186.

30. L. J. Mordell, *On the Riemann hypothesis and imaginary quadratic fields with a given class number*, J. London Math. Soc. **9** (1934), 289–298.

31. ______, *On the rational solutions of the indeterminate equations of the* 3*rd and* 4*th degrees*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

32. H. L. Montgomery and P. J. Weinberger, *Notes on small class numbers*, Acta Arith. **24** (1973), 529-542.

33. J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Séminaire Nicolas Bourbaki, 1983–1984, Éxp. 631.

34. G. Rabinovitch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, Proc. Fifth Internat. Congress Math. (Cambridge), vo. I, 1913, pp. 418–421.

35. C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935), 83–86.

36. ______, *Zum Beweise des Starkschen Staz*, Invent. Math. **5** (1968), 180–191.

37. H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), 1–27.

38. ______, *A historical note on complex quadratic fields with class-number one*, Proc. Amer. Math. Soc. **21** (1969), 254–255.

39. ______, *On the "gap" in a theorem of Heegner*, J. Number Theory **1** (1969), 16–27.

40. ______, *A transcendence theorem for class number problems*, Ann. of Math. (2) **94** (1971), 153–173.

41. T. Tatuzawa, *On a theorem of Siegel*, Japan. J. Math. **21** (1951), 163–178.

42. A. Weil, *Sur un théorème de Mordell*, Bull. Sci. Math. (2) **54** (1930), 182–191.

43. ______, *Sur les fonctions algébriques à corps de constantes fini*, C. R. Acad. Sci. Paris **210** (1940), 592–594.

44. ______, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. **168** (1967), 149–156.

Department of Mathematics, University of Texas, Austin, Texas 78712

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138