DORIAN M. GOLDFELD

The conjectures of Birch and Swinnerton-Dyer and the class numbers of quadratic fields

Astérisque, tome 41-42 (1977), p. 219-227
<http://www.numdam.org/item?id=AST_1977__41-42__219_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.219-227

THE CONJECTURES OF BIRCH AND SWINNERTON-DYER AND THE CLASS NUMBERS OF QUADRATIC FIELDS

by

Dorian M. GOLDFELD

1. The Class Number Problem

Let χ be a real, primitive, Dirichlet character (mod d) . Associated to χ we have a quadratic field

$$K = Q(\sqrt{\chi(-1)d})$$

which is real or imaginary according as $\chi(-1) = +1$ or -1 . If we let

$$H = \begin{cases} h & \text{if } \chi(-1) = -1 \\ h.\log \epsilon_o & \text{if } \chi(-1) = +1 \end{cases}$$

where h is the class number and ϵ_o is the fundamental unit of K , then C.L. Siegel [4], [10] has proved the important result

$$H > c(\epsilon) d^{\frac{1}{2}-\epsilon}$$

where for all $\epsilon > 0$, $c(\epsilon) > 0$ is an ineffectively computable constant.

Actually, one expects even more to be true, since if $H = o(\sqrt{d} / \log d)$, there exists a real number β satisfying (see [5], [7])

$$1 - \beta \sim \frac{6}{\pi^2} L(1,\chi) \Bigg(\sum_{\substack{a,b,c \\ -a<b\leqq a<\frac{1}{4}\sqrt{d} \\ b^2-4ac=\chi(-1)d}} a^{-1} \Bigg)^{-1}$$

for which

$$L(\beta,\chi) = 0 \quad .$$

This, of course, contradicts the Riemann Hypothesis, and it is, therefore, likely that $H.\log d / \sqrt{d}$ never gets too small.

The strongest known effective lower bounds for H have been obtained by Stark [11] and Baker [1], who established that there are only 9 imaginary quadratic fields with class number one, and that there are exactly 18 imaginary quadratic fields with class number two. As a consequence, the lower bound

$$H \geqq 3 \qquad (d > 427 \ , \ \chi(-1) = -1)$$

was obtained. The general Gauss problem of effectively determining how many imaginary quadratic fields have a given class number $h > 2$ still remains open.

S. Chowla has raised an analogous problem for real quadratic fields. If d is of the form $d = m^2 + 1$ so that the fundamental unit is minimal, Chowla has conjectured that there will be only finitely many real quadratic fields of this type with a given class number, and that these fields can be effectively determined.

2. The Birch-Swinnerton-Dyer Conjectures

Let E be an elliptic curve over Q, with conductor N (see [13]). If p does not divide N, the reduction of E modulo p is an elliptic curve over Z/pZ; let N_p be its number of points, and put $t_p = p + 1 - N_p$. The Hasse-Weil L-function of E is defined to be :

$$L_E(s) = \prod_{p|N} (1-a_p p^{-s})^{-1} \prod_{p\nmid N} (1-t_p p^{-s}+p^{1-2s})^{-1} = \sum E_n n^{-s} \quad ,$$

where the a_p's (for $p|N$) are equal to $0,1$ or -1 (cf. [13]).

Weil (loc. cit.) has conjectured that $L_E(s)$ is entire and satisfies the functional equation

$$(\sqrt{N}/2\pi)^s \, \Gamma(s) L_E(s) = \pm \, (\sqrt{N}/2\pi)^{2-s} \, \Gamma(2-s) L_E(2-s) \quad ,$$

and that

$$\sum E_n e^{2\pi i n z}$$

is a cusp form of weight 2 for the congruence subgroup $\Gamma_o(N)$.

Let $E(Q)$ denote the group of rational points on E . Then if $E(Q)$ has g independent generators of infinite order, Birch and Swinnerton-Dyer have conjectured [2]

CONJECTURE $L_E(s)$ has a zero of order g at $s = 1$.

This conjecture may prove useful in the class number problem (for both real and imaginary fields), for we can show [6]

THEOREM 1 - If $L_E(s)$ satisfies Weil's conjecture and $L_E(s)$ has a zero of order g at $s = 1$, then for $(d,N) = 1$

$$H > \frac{c_2}{g^4 g_N{}^{13}} (\log d)^{g-u-1} \exp(-21g^{\frac{1}{2}} (\log\log d)^{\frac{1}{2}}) \quad , \quad \left(d > e^{e^{c_1 N g^3}} \right)$$

where $u = 1,2$ is suitably chosen so that

$$\chi(-N) = (-1)^{g-u}$$

and the constants $c_1, c_2 > 0$ can be effectively computed and are independent of g , N , and d .

If we simply take $u = 2$ in the above Theorem, then the condition $(d,N) = 1$ can be dispensed with. In this case, however, the proof of Theorem (1) will have to be slightly modified to take into account a finite number of bad primes dividing (d,N) .

3. Example 1

Stephens [12] has shown that the elliptic curve

$$E_1 : y^2 = x^3 - 2^4 . 3^7 . 73^2$$

satisfies

$$g = \text{rank of } E_1(\mathbb{Q}) = 3 \quad , \qquad N = 3^3 . 73^2$$

$$(\sqrt{N}/2\pi)^s \, \Gamma(s) L_{E_1}(s) = - (\sqrt{N}/2\pi)^{2-s} \, \Gamma(2-s) L_{E_1}(2-s) \quad .$$

$L_{E_1}(s)$ satisfies Weil's conjecture since E_1 has complex multiplication by $\sqrt{-3}$ so that by a Theorem of Deuring [3] $L_{E_1}(s)$ is a Hecke L-series with Grössencharakter of $\mathbb{Q}(\sqrt{-3})$. Moreover, since the functional equation has the - sign, $L_{E_1}(s)$ must have a zero of odd order at $s = 1$. It immediately follows that

$$L_{E_1}(1) = 0 \quad .$$

As a consequence of Theorem (1), we have

THEOREM 2 - _If_ $L'_{E_1}(1) = 0$, _then for every_ $\varepsilon > 0$ _there exists_ $c(\varepsilon) > 0$ _such that_

$$H > c(\varepsilon)(\log d)^{1-\varepsilon} \quad , \qquad (d, 3.73) = 1$$

in the case $\chi(-1) = -1$, $\chi(3) = -1$. _The constant_ $c(\varepsilon)$ _can be effectively computed and is independent of_ d .

4. _Example_ 2

Consider the curve

$$E_2 : y^2 = x^3 + (3.7.11.17.41)^2 x$$

found by Wiman [14]. For this example

$$g = \text{rank of } E_2(\mathbb{Q}) = 4 \quad , \qquad N = 2^6 (3.7.11.17.41)^2$$

$$(\sqrt{N}/2\pi)^s \, \Gamma(s) L_{E_2}(s) = + (\sqrt{N}/2\pi)^{2-s} \, \Gamma(2-s) L_{E_2}(2-s) \quad .$$

Since E_2 has complex multiplication by $\sqrt{-1}$, Weil's conjecture is again satisfied. The + sign in the functional equation shows that $L_{E_2}(s)$ has a zero of even order at $s = 1$. Since $L_{E_2}(1)$ must be an integral multiple of a predictable number, one can show by computer computation that

$$L_{E_2}(1) = 0 \quad , \qquad L'_{E_2}(1) = 0 \quad .$$

THEOREM 3 - <u>If</u> $L''_{E_2}(1) = 0$, <u>then for every</u> $\varepsilon > 0$, <u>there exists</u> $c(\varepsilon) > 0$ <u>such that</u>

$$H > c(\varepsilon)(\log d)^{2-\varepsilon} \quad , \qquad (d, 2.3.7.11.17.41) = 1$$

<u>and</u>

$$H > c(\varepsilon)(\log d)^{1-\varepsilon} \qquad (\text{no condition on } d\ )$$

<u>in the case</u> $\chi(-1) = 1$. <u>The constant</u> $c(\varepsilon)$ <u>can be effectively computed and is independent of</u> d .

It immediately follows that the vanishing of $L''_{E_2}(1)$ would allow one to effectively determine all imaginary quadratic fields having a given class number, and, therefore, provide a solution to the class number problem. Unfortunately, the curves E_1 and E_2 provide no information in the case of real quadratic fields. To get a solution to Chowla's conjecture, for example, one would require an elliptic curve E for which $L_E(s)$ has a zero of order 5 at $s = 1$.

5. <u>Some Generalizations</u>

Theorem (1) can be generalized to a rather wide class of L-functions associated to modular forms of arithmetic type. If

$$L_1(s) = \prod_p \prod_{i=1}^{k} (1-\alpha_{p,i}p^{-s})^{-1} \quad , \qquad |\alpha_{p,i}| \leq 1$$

is such an L-function satisfying a functional equation of type

$$M^s\, T(s)L_1(s) = wM^{1-s}T(1-s)L_1(1-s) \quad , \qquad |w| = 1$$

where M is a positive real number and $T(s)$ is some finite product of Γ-functions $(T(s) = \prod \Gamma(s+a_i))$, and if the twisted series

$$L_1(s,\chi) = \prod_p \prod_{i=1}^{k} (1-\chi(p)\,\alpha_{p,i}p^{-s})^{-1}$$

satisfies

$$M_\chi^s T_\chi(s) L_1(s,\chi) = w_\chi M_\chi^{1-s} T_\chi(1-s) L_1(1-s,\chi) \quad , \qquad |w_\chi| = 1$$

where $T_\chi(s)$ is again some finite product of Γ-functions and

(*) $$M_\chi << dM \quad ,$$

one can in general show that for every $\epsilon > 0$, there exists an effectively computable constant $c(\epsilon) > 0$ such that

(**) $$H > c(\epsilon)(\log d)^{g-u-\rho-\epsilon} \quad .$$

Here, g is the order of the zero of $L_1(s)$ at $s = \frac{1}{2}$; $u = 1$ or 2 according as

$$1 + (-1)^{g-1} w w_\chi \neq 0 \quad \text{or} = 0 \quad ,$$

and ρ is the order of the zero of

$$L_2(s) = \prod_p \prod_{i=1}^{k} (1-\alpha_{p,i}^2 p^{-s})^{-1}$$

at $s = 1$. The condition (*) seems to force $k \leqq 2$.

If $L_1(s)$ is an L-function associated to an elliptic curve, one can show by Rankin's method [9] that $\rho = 1$, and this is the main reason why zeros of order $\geqq 3$ are needed to get non-trivial lower bounds for H . It would be of considerable interest to find examples of L-functions for which $g - \rho \geqq 2$ and $\rho < 1$.

The proof of these results is based on the general principle that if H is too small then $\chi(n)$ behaves like Liouville's function $\lambda(n)$

(where $\zeta(2s)/\zeta(s) = \sum \lambda(n) n^{-s}$)

for $n << d$. This can easily be seen in the case of an imaginary quadratic field with class number one. If the field has discriminant $-d$, then for a prime $p < d$, $\chi(p) = +1$ if and only if we have the representation

$$p = x^2 + xy + \frac{(d+1)}{4} y^2 ,$$

from which it follows that $\chi(p) = -1$ for all $p < (d+1)/4$. This implies that $\chi(n) = \lambda(n)$ for $n < (d+1)/4$.

If one writes

$$L_1(s)L_1(s,\chi) = G(s)L_2(2s) ,$$

then $G(s)$ measures the deviation by which $\chi(n)$ differs from Liouville's function $\lambda(n)$. We show that this deviation can be measured in terms of H. Let

$$G(s) = \sum g_n n^{-s} , \qquad G(s,x) = \sum_{n<x} g_n n^{-s} .$$

It is not hard to see that $G(s)$ is majorized by

$$F(s) = (\zeta(s)L(s,\chi)/\zeta(2s))^k ,$$

that is to say $|g_n|$ is bounded by the n^{th} coefficient in the Dirichlet series expansion for $F(s)$. By expanding $F(s)$ into a rapidly converging series of Bessel functions it is possible to estimate $G(\frac{1}{2},d)$ in terms of $L(1,\chi)$.

On using a general method of A.F. Lavrik [8] one can expand

$$M^s M_\chi^s T(s)T_\chi(s)L_1(s)L_1(s,\chi)$$

into a rapidly converging series of incomplete Γ-functions whose main contribution comes from the terms $n \ll MM_\chi$, and in this way it can be proved that

$$\left(\frac{d}{ds}\right)^{g-1} [(MM_\chi)^s T(s)T_\chi(s)L_1(s)L_1(s,\chi)]_{s=\frac{1}{2}} =$$

$$= \delta\left(\frac{d}{ds}\right)^{g-1} [(MM_\chi)^s T(s)T_\chi(s)G(s,U)L_2(2s)]_{s=\frac{1}{2}} + O(MM_\chi L(1,\chi)(\log d)^c) .$$

where

$$\delta = 1 + (-1)^{g-1} w w_{\chi}$$

and U is a power of $\log d$. Since $L_1(s)$ has a zero of order g at $s = \frac{1}{2}$ and $G(\frac{1}{2}, U)$ can be bounded from below if H is sufficiently small it follows that one can obtain results of type (**) . Note that there will be a loss of ρ powers of $\log d$ if $L_2(s)$ has a zero of order ρ at $s = 1$, and a loss of one $\log d$ if $\delta = 0$.

BIBLIOGRAPHY

[1] BAKER A. - Imaginary quadratic fields with class number two. Annals of Math. 94 (1971), 139-152.

[2] BIRCH B.J. and SWINNERTON-DYER H.P.F. - Notes on elliptic curves. J. reine angewandte Math. 218 (1965), 79-108.

[3] DEURING M. - Die Zetafunktion einer algebraischer Kurve von Geschlechte Eins. I, II, III, IV, Nachr. Akad. Wiss. Göttingen (1953), 85-94 ; (1954), 13-42 ; (1956), 37-76 ; (1957), 55-80.

[4] GOLDFELD D.M. - A simple proof of Siegel's theorem. Proc. Nat. Acad. Sci. U.S.A., 71 (1974), 1055.

[5] GOLDFELD D.M. - An asymptotic formula relating the Siegel zero and the class number of quadratic fields. Annali Scuola Normale Superiore, Serie IV, Vol. II (1975), 611-615.

[6] GOLDFELD D.M. - The class number of quadratic fields and the conjectures of Birch-Swinnerton-Dyer. To appear in Annali Scuola Normale Superiore.

[7] GOLDFELD D.M. and SCHINZEL A. - On Siegel's zero. Annali Scuola Normale Superiore, Serie IV, Vol. II (1975), 571-585.

[8] LAVRIK A.F. - Functional equations of Dirichlet functions. Soviet Math. Dokl. 7 (1966), 1471-1473.

[9] OGG A.P. - On a convolution of L-series. Inventiones Math. 7 (1969), 297-312.

[10] SIEGEL C.L. - Über die Classenzahl quadratischer Zahlkörper. Acta Arith. 1 (1935), 83-86.

[11] STARK H.M. - A transcendence theorem for class number problems. Annals of

Math. 94 (1971), 153-173.

[12] STEPHENS N.M. - The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer. J. reine angewandte Math. 231 (1968), 121-162.

[13] WEIL A. - Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann. 168 (1967), 149-156.

[14] WIMAN A. - Über rational Punkte auf Kurven $y^2 = x(x^2 - c^2)$. Acta Math. 77 (1945), 281-320.

Dorian M. GOLDFELD
Math. Dept.
M.I.T.
CAMBRIDGE, MA 02139
(U.S.A.)