On Chowla's conjecture for class numbers of real quadratic fields

by

Tsuneo Arakawa

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Strasse 26
D-5300 Bonn 3

and

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro
Tokyo 171 Japan

MPI/89-62

On Chowla's conjecture for class numbers of real quadratic fields

Tsuneo Arakawa

§ 0. *Introduction*

The class number problem of obtaining an effective estimate for class numbers of imaginary quadratic fields was a classical but fundamental problem and has recently been settled by Goldfeld [Go1, 2] and Gross-Zagier [G-Z] with the use of an extremely ingenious method.

Class number problems for real quadratic fields with some additional condition on discriminants can be considered. It seems that along this line a typical interesting problem is a conjecture of S. Chowla [Ch], [C-F]. In the sequel let D always denote a square free positive integer and h(D) the class number of the real quadratic field $\mathbb{Q}(\sqrt{D})$. Chowla's conjecture predicts that

$h(D)=1$ and $D=q^2+4$ (resp. $4q^2+1$) with $q \in \mathbb{N}$ if and only if
$D= 5, 13, 29, 53, 173, 293$ (resp. $D= 5, 17, 37, 101, 197, 677$).

Chowla's conjecture has been proved by Mollin ([Mo]) and Lachaud [La] under the generalized Riemann hypothesis. Kim-Leu-Ono [K-L-O] proved that if $D=q^2+4$ or $4q^2+1$ $(q \in \mathbb{N})$, then there exists at most one $D \geq e^{16}$

with $h(D)=1$.

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N and $L(E,s)=\sum_{n=1}^{\infty} a_n n^{-s}$ the L-function associated with E. The Taniyama-Weil conjecture predicts that

(0.1) the function $f(z)=\sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ is a new form of weight two with respect to the congruence subgroup $\Gamma_0(N)$ of $SL_2(\mathbb{Z})$.

In this case the L-function $L(E,s)=L(f,s)$ is analytically continued to an entire function of s which satisfies the functional equation

$$L^*(E,2-s)=\epsilon_E L^*(E,s) \qquad \text{with} \quad \epsilon_E=\pm 1,$$

where $L^*(E,s)=(\sqrt{N}/2\pi)^s\Gamma(s)L(E,s)$. Denote by $r(E)$ the Mordell-Weil rank of E. We moreover assume that the Birch and Swinnerton-Deyer conjecture holds for the elliptic curve E;

(0.2) $L(E,s)$ has a zero at $s=1$ of order $r(E)$.

Let $\chi=\chi_D$ be a Dirichlet character associated with the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Concerning Chowla's conjecture, Goldfeld's result [Gol, Theorem 1] implies the following.

THEOREM (Goldfeld). *Let E be an elliptic curve over $\mathbb{Q}$ satisfying* (0.1), (0.2). *Let D be of the form* $D=q^2+4$ *or* $4q^2+1$ $(q \in \mathbb{N})$ *with* $h(D)=1$. *Then for any positive number ε, there exists a certain positive constant $C(\varepsilon,E)$ depending only on ε and E such that*

(0.3) $$(\log D)^{r-\mu-2} < C(\varepsilon,E)(\log D)^{\varepsilon},$$

where $\mu=1$ *or* 2 *so that* $\chi(N)=(-1)^{r-\mu}$.

The aim of this note is to obtain a better estimate for logD than that of (0.3). We follow the method of Goldfeld (or more precisely its modified version due to Oesterlé [Oe]). We obtain

THEOREM 1. *Assume that an elliptic curve* E *over* $\mathbb{Q}$ *satisfies the conditions* (0.1), (0.2). *Let* D *be a square free positive integer with* $D = q^2+4$ *or* $4q^2+1$ $(q \in \mathbb{N})$ *satisfying the conditions*

$$h(D) = 1 \quad \text{and} \quad (D,N)=1.$$

Define a positive integer g *by*

$$(0.4) \qquad g = \begin{cases} r(E)+1 & \ldots \text{ if } \chi_D(N) = -\varepsilon_E \\ r(E) & \ldots \text{ if } \chi_D(N) = \varepsilon_E. \end{cases}$$

Moreover assume that $g \geq 4$. *Then there exist positive constants* C_1, λ *and real constants* $C_2, \ldots, C_{g-1}$ *depending only on* E *such that, if* $q > 4$,

$$C_1 \left\{ \frac{(\log D)^{g-2}}{(g-2)!} + \sum_{j=2}^{g-1} C_j \frac{(\log D)^{g-1-j}}{(g-1-j)!} \right\} - \lambda$$

$$< \frac{N^{3/2} 2^{g-4}}{3} \log\varepsilon_0 \cdot \left(1 + \frac{4}{\sqrt{D}} \log\varepsilon_0\right) + N^{5/4} 2^{2(g-4)} \left(18 + \frac{67}{D^{1/4}}\right)$$

$$+ N^{3/2} \cdot \frac{(\log\varepsilon_0)^2}{\sqrt{D}} \cdot 2^{g-7} \cdot (4\mathrm{Max}(2, \log M)+9),$$

where $M = N/(4\pi^2)$ *and* ε_0 *is the fundamental unit* of $\mathbb{Q}(\sqrt{D})$ *with* $\varepsilon_0 > 1$ *which is given in this case by*

$$\varepsilon_0 = \left(q + \sqrt{q^2+4}\right)/2 \quad (\textit{resp.}\ 2q + \sqrt{4q^2+1}\ ) \quad \textit{if}\ D = q^2+4 \quad (\textit{resp.}\ 4q^2+1).$$

The constants C_1, λ, *and* $|C_2|, \ldots, |C_{g-1}|$ *are effectively computable and the precise definition is given by* (2.6), (2.8) *in this paper.*

By this theorem, Goldfeld's estimate (0.3) is improved as follows:

$$(0.5) \qquad (\log D)^{r-\mu-1} < C(E)$$

with a certain positive constant $C(E)$ depending only on E (note that $\epsilon_E=(-1)^r$ and $g=r+2-\mu$).

As a corollary of Theorem 1, one can obtain a result in the case of E over $\mathbb{Q}$ with $r(E)=3$ (and accordingly, $\epsilon_E=-1$).

COROLLARY. *Let* E *satisfy the conditions* (0.1), (0.2) *with* $r(E)=3$ *and* $\epsilon_E=-1$. *Write the conductor* N *as a product of distinct prime factors:* $N= p_1^{e_1}\cdots p_k^{e_k}$. *Assume that* $e_1+ \cdots +e_k \equiv 0 \bmod 2$. *Let* D *be a square free positive integer with* $h(D)=1$ *and* $D=q^2+4$ *or* $4q^2+1$ $(q \in \mathbb{N})$. *Assume moreover that* $q > \mathrm{Max}(4,p_1,\ldots,p_k)$. *Then,*

$$C_1\log D < 2C_1\left(|C_2|+ \frac{|C_3|}{\log D}\right) + \frac{2\lambda}{\log D} + \frac{2N^{3/2}\log\varepsilon_0}{3\log D}\cdot\left(1+ \frac{4\log\varepsilon_0}{\sqrt{D}}\right)$$

$$+ \frac{2N^{5/4}}{\log D}\cdot\left(18+ \frac{67}{D^{1/4}}\right) + N^{3/2}\cdot\frac{(\log\varepsilon_0)^2}{4\sqrt{D}}\cdot(4\mathrm{Max}(2,\log M)+9),$$

where C_1, C_2, C_3, λ *and* ε_0 *are the same as in* THEOREM 1.

REMARK. It is known that, if $D=q^2+4$ or $4q^2+1$ $(q \in \mathbb{N},\ q>2)$ and $h(D)=1$, then, D is a prime integer congruent to one modulo 4 and moreover $\chi_D(p)= -1$ for any prime p less than q ([Yo, Theorem 1, Proposition 2]).

A key to the proof is the inequality (2.9) and moreover to employ some convenient expression due to Zagier [Za] for the Dedekind zeta function of $\mathbb{Q}(\sqrt{D})$.

The author would like to thank Max-Planck-Institut für Mathematik in Bonn for supporting him financially in 1989 and thank Professor D. Zagier for his kind advice.

§ 1. *Real quadratic fields and continued fractions*

Let D be a square free positive integer and set $F=\mathbb{Q}(\sqrt{D})$. Let h(D) denote the class number of F. For any x of F, x' denotes the conjugate of x. A number x of F is called reduced if $x>1$ and $0>x'>-1$. Any number x of F can be expanded in a unique way as a continued fraction:

$$(1.1) \qquad x= a_1+ \cfrac{1}{a_2+ \cfrac{1}{\ddots}} \qquad (a_i \in \mathbb{Z},\ a_i \geq 1 \text{ if } i \geq 2).$$

Then the sequence $\{a_1, a_2, \ldots\}$ becomes periodic. Let m be the period of x. Then, x is reduced, if and only if the continued fraction expansion of x is pure periodic, i.e., $a_{i+m}=a_i$ $(i\geq 1)$. In this case we write for simplicity

$$(1.2) \qquad x=[a_1, \ldots, a_m] \qquad \text{instead of } (1.1).$$

Now we recall a theorem of Zagier [Za] concerning partial zeta functions of real quadratic fields. A partial zeta function $\zeta_F(s,B)$ associated with a narrow ideal class B of $F=\mathbb{Q}(\sqrt{D})$ is given by

$$\zeta_F(s,B)=\sum_{\mathfrak{b}} N(\mathfrak{b})^{-s} \qquad (\mathrm{Re}(s)>1),$$

where $\mathfrak{b}$ runs over all integral ideals of B. A number z of F is called reduced in the sense of [Za], if $z>1>z'>0$. Let B be a narrow ideal class of F. There exists a reduced number w in the sense of [Za] for which $\{1,w\}$ gives a basis of some ideal $\mathfrak{b}$ in B. Then, w has a purely periodic continued fraction expansion with period r of the form

$$(1.3) \qquad w=b_1-\cfrac{1}{b_2-\cfrac{1}{\ddots}} \qquad (b_j\in\mathbb{Z},\quad b_j\geq 2)$$

with $b_{j+r}=b_j$ for any $j\in\mathbb{N}$ ([Za, p. 162]). We write simply

$$w=[[b_1,\ldots,b_r]]$$

for the continued fraction expansion (1.3). The period r depends only on the class B and is denoted by $\ell(B)$. Set, for each j $(1\leq j\leq \ell(B))$,

$$w_j=[[b_j,b_{j+1},\ldots,b_{j+\ell(B)-1}]].$$

Then each continued fraction w_j is reduced in the sense of [Za] and $\{1,w_j\}$ also gives a basis of the ideal $\mathfrak{b}$. It is known that

$$(1.4) \qquad w_1\cdots w_{\ell(B)}=\varepsilon,$$

ε being the totally positive fundamental unit of F with $\varepsilon>1$. For each j $(1\leq j\leq \ell(B))$, we define a binary quadratic form $Q_j(x,y)$ by

$$(1.5) \qquad Q_j(x,y)=\frac{1}{w_j-w_j'}(y+xw_j)(y+xw_j') \qquad ([\text{Za, } (6.7)]),$$

which is an indefinite binary quadratic form with positive coefficients and discriminant 1. Zagier obtained the following decomposition for $\zeta_F(s,B^{-1})$.

THEOREM (Zagier [Za, p.166]). *Let* D_F *denote the discriminant of* F. *Then,*

$$D_F^{s/2}\zeta_F(s,B^{-1})=\sum_{j=1}^{\ell(B)} Z_{Q_j}(s) \qquad (\mathrm{Re}(s)>1),$$

where

$$Z_{Q_j}(s)=\sum_{p=1}^{\infty}\sum_{q=0}^{\infty}\frac{1}{Q_j(p,q)^s}.$$

For the later use we quote some results due to Yokoi. Assume that $D\equiv 1 \bmod 4$. Let $\left(\frac{D}{p}\right)^*$ be the extended Legendre symbol which coincides with $\left(\frac{D}{p}\right)$ for any odd prime integers p and is defined at p=2 by

$$\left(\frac{D}{p}\right)^*=\begin{cases} 1 & \ldots\ D\equiv 1 \bmod 8 \\ -1 & \ldots\ D\equiv 5 \bmod 8. \end{cases}$$

LEMMA 1 (Yokoi [Yo, Theorem 1, Proposition 2]). *Let* D *be a square free positive integer of the form* $D=q^2+4$ *or* $4q^2+1$ *with* $q\in\mathbb{N}$, $q>2$. *Assume moreover that* $h(D)=1$. *Then,* D, q *are odd primes and* $\left(\frac{D}{p}\right)^*=-1$ *for all prime integers* p *less than* q.

§ 2. *An estimate for* logD

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. The L-function

$L(E,s)=\sum_{n=1}^{\infty} a_n n^{-s}$ has an expression as Euler products:

$$L(E,s)=\prod_{p|N}(1-a_p p^{-s})^{-1}\prod_{p\nmid N}(1-a_p p^{-s}+p^{1-2s})^{-1}\qquad (\mathrm{Re}(s)>1),$$

where $a_p=0$ if $p^2|N$, $a_p=\pm 1$ if $p|N$, $p^2\nmid N$, and $|a_p|\le 2\sqrt{p}$ if $p\nmid N$. Assume that E satisfies the conditions (0.1), (0.2) in the introduction. In this case the function

$$f(z)=\sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

on the upper half plane $\mathfrak{H}$ is a new form of weight two with respect to $\Gamma_0(N)$, and

$$f\left(-\frac{1}{Nz}\right)=-\epsilon_E N z^2 f(z).$$

For a square free positive integer D, let $\chi=\chi_D$ denote a Dirichlet character associated with the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Assume for simplicity that

$$D\equiv 1 \bmod 4 \quad\text{and}\quad (N,D)=1.$$

We denote by $f\otimes\chi$ the twist of f with χ which is a new form of weight two with respect to $\Gamma_0(ND^2)$. Then,

$$a_n(f\otimes\chi)=a_n\chi(n)\qquad (n\in\mathbb{N}),$$

where $a_n(f\otimes\chi)$ is the n-th Fourier coefficient of $f\otimes\chi$. It is known that

$$(f\otimes\chi)\left(-\frac{1}{Nz}\right)=-\epsilon(f\otimes\chi)ND^2z^2(f\otimes\chi)(z)\qquad \text{with}\quad \epsilon(f\otimes\chi)=\chi(-N)\epsilon_E$$

(see for instance [Oe, 2.2]).

Let λ be the Liouville function which is a multiplicative function from $\mathbb{N}$ to $\{\pm 1\}$ characterized by $\lambda(p)=-1$ for any prime p. Let $L(f\otimes\lambda,s)$ be the twisted L-function of $L(f,s)$ by λ:

$$L(f\otimes\lambda,s)=\sum_{n=1}^{\infty}\frac{a_n\lambda(n)}{n^s},$$

which is absolutely convergent for $\mathrm{Re}(s)>3/2$. The L-function $L(\mathrm{Sym}^2 f,s)$ of symmetric square is given by

$$(2.1)\qquad L(\mathrm{Sym}^2 f,s)=\prod_{p\nmid N}(1-p^{1-s})^{-1}\cdot L(f,s/2)L(f\otimes\lambda,s/2)\qquad (\mathrm{Re}(s)>2)$$

It is known that $L(\mathrm{Sym}^2 f,s)$ can be continued to an entire function of s and moreover that

$$(2.2)\qquad L(\mathrm{Sym}^2 f,2)=\frac{(2\pi)^3}{N}\int_{\Gamma_0(N)\backslash\mathfrak{H}} y^2|f(z)|^2\,\frac{dxdy}{y^2}\qquad ([\mathrm{Og}]).$$

We set

$$\Psi(s)=L((f,s)L(f\otimes\lambda,s),$$

$$G(s)=L(f\otimes\chi,s)L((f\otimes\lambda,s)^{-1}.$$

The Dirichlet series $\Psi(s)$ (resp. $G(s)$) is absolutely convergent for $\mathrm{Re}(s)>1$ (resp. $\mathrm{Re}(s)>3/2$), and $\Psi(s)$ has a simple zero at $s=1$.
For two Dirichlet series

$$b(s)=\sum_{n=1}^{\infty}\frac{b_n}{n^s},\qquad c(s)=\sum_{n=1}^{\infty}\frac{c_n}{n^s},$$

we write $b\ll c$ if $|b_n|\le c_n$ for any $n\ge 1$. The following fact is known by Oesterlé [Oe, p.314, p.319]).

$$(2.3)\qquad \Psi(s)\ll\zeta(2s-1)^2 \quad\text{and}\quad G(s)\ll\left(\frac{\zeta_F(s-1/2)}{\zeta(2s-1)}\right)^2,\quad \text{where } F=\mathbb{Q}(\sqrt{D}).$$

Now following the method of Oesterlé [Oe], we give a proof of THEOREM 1 in the introduction.

Proof of THEOREM 1.

Let an elliptic curve E over $\mathbb{Q}$ and a square free positive integer D satisfy the assumptions of THEOREM 1. Define a positive integer g by (0.4). We set

$$\gamma(s) = M^s \Gamma(s)^2 \qquad \text{with} \quad M = N/(4\pi^2).$$

We consider the following integral J for $\sigma > 1$:

$$(2.4) \qquad J = \int_{\sigma-i\infty}^{\sigma+i\infty} D^{s-1}\gamma(s)\Psi(s)(s-1)^{-g} \frac{ds}{2\pi i}.$$

We note that the integral J is absolutely convergent. Since $\epsilon(f\otimes\chi) = \chi(-N)\epsilon_E$, by the assumption for E, the function

$$\Psi(s)G(s) = L(f,s)L(f\otimes\chi,s)$$

has a zero at s=1 of order at least g. Therefore using the functional equations of $L(f,s)$, $L(f\otimes\chi,s)$ and shifting the integral path to $\sigma \longrightarrow -\infty$, we get

$$(2.5) \qquad \int_{\sigma-i\infty}^{\sigma+i\infty} D^{s-1}\gamma(s)\Psi(s)G(s)(s-1)^{-g} \frac{ds}{2\pi i} = 0 \qquad (\sigma > 3/2).$$

We set

$$J^* = \int_{\sigma-i\infty}^{\sigma+i\infty} D^{s-1}\gamma(s)\Psi(s)(G(s)-1)(s-1)^{-g} \frac{ds}{2\pi i} \qquad (\sigma > 3/2),$$

Then, (2.4), (2.5) imply that

$$J^* = -J.$$

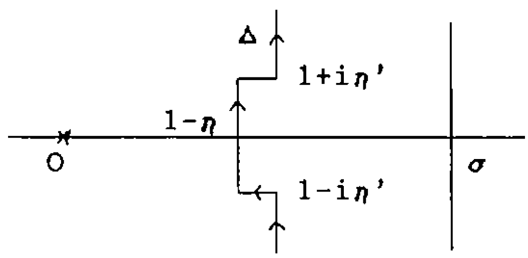
The function $\gamma(s)\Psi(s)/(s-1)$ has the Taylor expansion at s=1:

$$(2.6) \qquad \frac{\gamma(s)\Psi(s)}{s-1} = C_1\left(1+C_2(s-1)+\cdots+C_{g-1}(s-1)^{g-2}+\cdots\right)$$

with $C_1, C_2, \ldots, C_{g-1} \in \mathbb{R}$. By virtue of (2.1), (2.2), the first constant C_1 is given by

$$C_1 = 4\pi \prod_{p|N} (1-p^{-1})^{-1} \cdot \int_{\Gamma_0(N)\backslash\mathfrak{H}} |f(z)|^2 dxdy > 0.$$

Choose any positive numbers η, η' with $\eta \le 1/4$. Let Δ be the oriented integral path given in the figure.



Shifting the integral path in the integral (2.4) to Δ, we have

$$(2.7) \qquad J = C_1\left(\frac{(\log D)^{g-2}}{(g-2)!} + \sum_{j=2}^{g-1} C_j \frac{(\log D)^{g-j-1}}{(g-j-1)!} \right) + J_1,$$

where J_1 is the integral with the integral path $\mathrm{Re}(s)=\sigma$ replaced by Δ on the right side of (2.4).

Then, J_1 has the trivial estimate

$$(2.8) \qquad |J_1| \le \lambda, \qquad \lambda = \int_\Delta |\gamma(s)\Psi(s)(s-1)^{-g}| \frac{|ds|}{2\pi}.$$

On the other hand we have to estimate the absolute value $|J^*|$ from the above. Replacing s with $s+1/2$ yields

$$J^* = \int_{\sigma-i\infty}^{\sigma+i\infty} D^{s-1/2}\gamma(s+1/2)\Psi(s+1/2)(G(s+1/2)-1)(s-1/2)^{-g} \frac{ds}{2\pi i} \quad (\sigma>1).$$

We see from the property (2.3) of the Dirichlet series $\Psi(s)$, $G(s)$ that

$$\Psi(s+1/2)(G(s+1/2)-1) \ll \zeta_F(s)^2-\zeta(2s)^2.$$

Set, for each $n \in \mathbb{N}$,

$$\alpha_n = \int_{\sigma-i\infty}^{\sigma+i\infty} D^{s-1/2}\gamma(s+1/2)n^{-s}(s-1/2)^{-g} \frac{ds}{2\pi i} \qquad (\sigma>1).$$

Then it is known by Lemma 1 of [Oe, 3.3] that $\alpha_n>0$. Similarly as in (3.4.2) of [Oe],

$$(2.9) \qquad |J^*| \le \int_{\sigma-i\infty}^{\sigma+i\infty} D^{s-1/2}\gamma(s+1/2)(\zeta_F(s)^2-\zeta(2s)^2)(s-1/2)^{-g} \frac{ds}{2\pi i}.$$

In this step what we have to do is to get a useful expression of $\zeta_F(s)$ with the help of THEOREM of Zagier. Let P denote the principal ideal class of F. Since $h(D)=1$ and ε_0 is with norm -1, P is the unique ideal class of F which coincides with the narrow principal ideal class of F. We set

$$x= \varepsilon_0 \quad (\text{resp. } x= \left(2q-1+\sqrt{4q^2+1}\right)/2) \quad \text{if } D= q^2+4 \ (\text{resp. } D= 4q^2+1).$$

Then, x is reduced and the lattice $\mathbb{Z}+\mathbb{Z}x$ coincides with the ring of integers of F. The number $w=1+x$ is reduced in the sense of [Za]. The relation between the continued fraction expansion of x of the form (1.1) and that of w of the form (1.3) is given explicitly by [Za, (8.13)]. Since x has a continued fraction expansion

$$x= [q] \qquad (\text{resp. } x= [2q-1,1,1])$$

with the notation (1.2), we have, by [Za, (8.13)], if $D=q^2+4$ (resp. $D=4q^2+1$),

$$w= [[q+2,\underbrace{2,\dots,2}_{q-1}]] \qquad (\text{resp. } w= [[2q+1,3,\underbrace{2,\dots,2}_{2q-2},3]]).$$

and consequently

$$\ell(P)= q \qquad (\text{resp. } \ell(P)= 2q+1).$$

We set, for $D= q^2+4$ (resp. $D= 4q^2+1$),

$$b_1=2, \ \ldots, \ b_{q-1}=2, \ b_q=q+2$$

$$(\text{resp. } b_1=2, \ \ldots, \ b_{2q-2}=2, \ b_{2q-1}=3, \ b_{2q}=2q+1, \ b_{2q+1}=3).$$

Extending the numbers b_j to all $j \in \mathbb{N}$ by $b_{j'}=b_j$ if $j'\equiv j \bmod \ell(P)$, we define continued fractions w_j as follows:

$$w_j= [[b_j, b_{j+1}, \ldots, b_{j+\ell(P)-1}]] \qquad (1\leq j\leq \ell(P)).$$

Attached to these numbers w_j $(1\leq j\leq \ell(P))$, let $Q_j(x,y)$ be the indefinite quadratic forms given by (1.5). We write

$$Q_j(x,y)= A_jx^2 + B_jxy + C_jy^2 \qquad (1\leq j\leq \ell(P))$$

with A_j, B_j, $C_j>0$. Using the recursion formula

$$w_j= b_j-\frac{1}{w_{j+1}},$$

we can calculate explicitly the numbers w_j and hence A_j $(1\leq j\leq \ell(P))$. If $D=q^2+4$, then we obtain

$$A_j= \left(-j^2+(q+2)j-q\right)/\sqrt{D} \qquad \text{for } 1\leq j\leq q.$$

If $D=4q^2+1$, then,

$$A_j= \left(-j^2+(2q+1)j-q\right)/\sqrt{D} \qquad \text{for } 1\leq j\leq 2q \quad \text{and} \quad A_{2q+1}= 1/\sqrt{D}.$$

In virtue of THEOREM of Zagier we get a decomposition for $\zeta_F(s)$:

$$(2.10) \qquad D^{s/2}\zeta_F(s)= \zeta(2s)\sum_{j=1}^{\ell(P)} A_j^{-s} + \sum_{j=1}^{\ell(P)} \sum_{m,n=1}^{\infty} Q_j(m,n)^{-s},$$

For each j $(1\leq j\leq \ell(P))$, let μ_j be the measure on $\mathbb{R}_+$ given by

$$\mu_j = \sum_{m,n=1}^{\infty} \delta_{Q_j(m,n)},$$

where δ_a $(a>0)$ denotes the Dirac measure at the point a.

LEMMA 2. *Let* $1 \leq j \leq \ell(P)$. *If* $t \leq 1$, *then*, $\mu_j([0,t])=0$. *If* $t>1$, *then*,

$$\mu_j([0,t]) \leq \frac{t}{2}\log(w_j/w_j').$$

Proof. We note that

$$\mu_j([0,t]) = \#\{(m,n) \in \mathbb{N}^2 \mid Q_j(m,n) \leq t\}, \tag{2.11}$$

where $\#(S)$ denotes the cardinality of a finite set S. Since $A_j+B_j+C_j>1$, the first equality is clear. Suppose $t>1$. It is easy to see from (2.11) that

$$\mu_j([0,t]) \leq \int_{\{(x,y) \in \mathbb{R}_+^2 \mid Q_j(x,y) \leq t\}} dxdy.$$

An elementary calculation shows that the integral on the right side coincides with

$$\frac{t}{2} \log \frac{B_j+1}{B_j-1} = \frac{t}{2} \log\left(w_j/w_j'\right) \qquad \text{q.e.d.}$$

We define a measure ν on $\mathbb{R}_+$ to be the sum of the Dirac measure δ_1 at the point 1 and the Lebesgue measure on the interval $[1,\infty)$. Set, for each j $(1 \leq j \leq \ell(P))$,

$$\mu_j' = \frac{1}{2} \log\left(w_j/w_j'\right) \cdot \nu,$$

which gives a measure on $\mathbb{R}_+$. LEMMA 2 shows that

$$\mu_j([0,t]) < \mu_j'([0,t]) \quad \text{for any } t>0. \tag{2.12}$$

For any positive measure μ on $\mathbb{R}_+$, let $\widehat{\mu}$ be the Mellin transform of μ:

$$\mu(s)= \int_{\mathbb{R}_+} t^{-s}\ \mu,$$

if the integral on the right side exists. Then if Re(s)>1,

$$(2.13)\qquad \widehat{\mu}_j(s)= \sum_{m,n=1}^{\infty} Q_j(m,n)^{-s} \quad\text{and}\quad \widehat{\mu}_j'(s)= \frac{1}{2}\log\left(w_j/w_j'\right)\cdot\frac{s}{s-1}\ .$$

Thus Lemma 3 of [Oe, 3.3] and (2.9), (2.10), (2.12), (21.13) enable us to get the following estimate for $|J^*|$:

$$|J^*| \le D^{-1/2}\int_{\sigma-i\infty}^{\sigma+i\infty} \gamma(s+1/2)\Big[\zeta(2s)^2\Big\{\Big(\sum_{j=1}^{\ell(P)} A_j^{-s}\Big)^2 - D^s\Big\} +$$

$$2\zeta(2s)\Big(\sum_{j=1}^{\ell(P)} A_j^{-s}\Big)\Big(\sum_{j=1}^{\ell(P)} \widehat{\mu}_j'(s)\Big) + \Big(\sum_{j=1}^{\ell(P)} \widehat{\mu}_j'(s)\Big)^2\Big](s-1/2)^{-g}\ \frac{ds}{2\pi i}\ .$$

Let ε be the same as in (1.4). In our case, $\varepsilon= \varepsilon_0^2$. We set, if $D=q^2+4$ (resp. $D=4q^2+1$),

$$A(s)= \sum_{j=2}^{q} \left(-j^2+(q+2)j-q\right)^{-s} \qquad \left(\text{resp. } A(s)= \sum_{j=1}^{2q} \left(-j^2+(2q+1)j-q\right)^{-s}\right).$$

Since $\sum_{j=1}^{\ell(P)} A_j^{-s}= D^{s/2}(1+A(s))$, it is easy to see from (1.4) and (2.13) that

$$(2.14)\qquad |J^*| \le I_1+I_2+I_3,$$

where

$$I_1= D^{-1/2}\int_{\sigma-i\infty}^{\sigma+i\infty} \gamma(s+1/2)\zeta(2s)^2D^s(A(s)^2+2A(s))(s-1/2)^{-g}\ \frac{ds}{2\pi i}\ ,$$

$$I_2 = 2D^{-1/2}\log\varepsilon\cdot\int_{\sigma-i\infty}^{\sigma+i\infty} \gamma(s+1/2)\zeta(2s)D^{s/2}(1+A(s))\cdot\frac{s}{s-1}\cdot(s-1/2)^{-g}\,\frac{ds}{2\pi i}\ ,$$

$$I_3 = D^{-1/2}(\log\varepsilon)^2\int_{\sigma-i\infty}^{\sigma+i\infty} \gamma(s+1/2)\left(\frac{s}{s-1}\right)^2(s-1/2)^{-g}\,\frac{ds}{2\pi i}$$

$(\sigma>1)$.

We note that the value of the integral I_1 is positive and that the values of I_2, I_3 are real numbers ([Oe, Lemma 1 of 3.3]). Take any positive number ρ with $0<\rho\leq 1/2$. Shifting the integral path $Re(s)=\sigma$ to $Re(s)=1/2+\rho$ yields

$$I_1 = D^{-1/2}\int_{1/2+\rho-i\infty}^{1/2+\rho+i\infty} \gamma(s+1/2)\zeta(2s)^2D^s(A(s)^2+2A(s))(s-1/2)^{-g}\,\frac{ds}{2\pi i}$$

$$\leq D^{\rho}\gamma(1+\rho)\zeta(1+2\rho)^2(A(1/2+\rho)^2+2A(1/2+\rho))\int_{-\infty}^{\infty}(\rho^2+t^2)^{-g/2}\cdot\frac{dt}{2\pi}\ .$$

Hence,

$$(2.15)\qquad I_1\leq D^{\rho}\gamma(1+\rho)\zeta(1+2\rho)^2(A(1/2+\rho)^2+2A(1/2+\rho))\cdot\frac{\tau_g}{2\pi\rho^{g-1}}\ ,$$

where we put

$$\tau_g = \int_{-\infty}^{\infty}(1+t^2)^{-g/2}dt.$$

Similarly as in (3.4.8) of [Oe], a residue calculation implies that

$$\int_{\sigma-i\infty}^{\sigma+i\infty} x^s\cdot\frac{s}{s-1}\cdot(s-1/2)^{-g}\,\frac{ds}{2\pi i}\leq 2^g x\qquad (x>0,\ \sigma>1).$$

Therefore,

$$(2.16)\qquad I_2\leq \log\varepsilon\cdot\gamma(3/2)\zeta(2)2^{g+1}(1+A(1)).$$

Shifting the integral path of the integral I_3 to $Re(s)=1+\rho$, we have

$$|I_3| \le D^{-1/2}(\log\varepsilon)^2\gamma(3/2+\rho)\int_{-\infty}^{\infty} \frac{(1+\rho)^2+t^2}{\rho^2+t^2}\cdot\frac{1}{\{(\rho+1/2)^2+t^2\}^{g/2}}\cdot\frac{dt}{2\pi}$$

The integral on the right side is dominated by

$$\frac{1}{2\pi}\left(\frac{(1+2\rho)2^g\pi}{\rho} + \frac{\tau_g}{(\rho+1/2)^{g-1}} \right),$$

which is less than $2^{g-3}\left(\frac{4}{\rho} + 9\right)$, since $\tau_g \le \tau_4 \le \pi/2$. Taking $\rho = (\mathrm{Max}(2,\log M))^{-1}$ as in [Oe, Proposition 1, c)], we have the estimate

$$(2.17) \qquad I_3 \le D^{-1/2}(\log\varepsilon_0)^2 \frac{N^{3/2}}{\pi^3} \cdot 2^{g-4} e\cdot(4\mathrm{Max}(2,\log M)+9).$$

Now we have to estimate $A(1/2+\rho)$ $(0<\rho\le 1/2)$ from the above.

LEMMA 3. *Suppose that*

$$(2.18) \qquad q > \begin{cases} \dfrac{1-2\rho}{4\sqrt{\rho(1-\rho)}} & \dots \text{ if } 0<\rho<1/2, \\ 4 & \dots \text{ if } \rho=1/2. \end{cases}$$

Then,

$$A(1/2+\rho) \le \begin{cases} (4/D)^{\rho}.\dfrac{\Gamma(1/2-\rho)\sqrt{\pi}}{\Gamma(1-\rho)} & \dots \quad 0<\rho<1/2 \\ \dfrac{4}{\sqrt{D}}\log\varepsilon_0 & \dots \quad \rho=1/2. \end{cases}$$

REMARK. If $D=q^2+4$, the above estimate for $A(1/2+\rho)$ holds without the assumption (2.18) for q.

Proof. First let $D=q^2+4$. Set, for simplicity, $\alpha=1/2+\rho$. Then it is immediate to see that

$$A(\alpha) \leq \int_1^{q+1} (-x^2+(q+2)x-q)^{-\alpha}dx = (4/D)^{\rho}\cdot\int_{-q/\sqrt{D}}^{q/\sqrt{D}} (1-t^2)^{-\alpha}dt,$$

from which the estimate easily follws. Suppose $D=4q^2+1$. Then,

$$(2.19) \qquad A(\alpha) \leq 2q^{-\alpha} + \int_1^{2q} (-x^2+(2q+1)x-q)^{-\alpha}dx.$$

We put $\beta = \left(2q+1-\sqrt{D}\right)/2$. Note that $0<\beta<1/2$ and $\beta' = (2q+1+\sqrt{D})/2 > 2q+1/2$. If $0<\rho<1/2$,

$$\int_\beta^1 (-x^2+(2q+1)x-q)^{-\alpha}dx = (4/D)^{\rho}\cdot\int_{(2q-1)/\sqrt{D}}^1 (1-t^2)^{-\alpha}dt$$

Replacing the integrand $(1-t^2)^{-\alpha}$ with $t(1-t^2)^{-\alpha}$, we have

$$(2.20) \qquad \int_\beta^1 (-x^2+(2q+1)x-q)^{-\alpha}dx \geq \frac{q^{1-\alpha}}{(1/2-\rho)\sqrt{D}},$$

where the value on the right hand side is larger than $q^{-\alpha}$ if

$$q^2 > \frac{(1-2\rho)^2}{16\rho(1-\rho)} .$$

In the case of $\rho=1/2$, it is not difficult to see that, if $q>4$,

$$(2.21) \qquad \int_{1/2}^1 (-x^2+(2q+1)x-q)^{-1}dx > 1/q.$$

Thus by (2.19), (2.20), (2.21), the value $A(1/2+\rho)$ with $0<\rho<1/2$ (resp. $A(1)$) is dominated by the integral

$$\int_\beta^{\beta'} (-x^2+(2q+1)x-q)^{-\alpha}dx \qquad \left(\text{resp. } \int_{1/2}^{2q+1/2} (-x^2+(2q+1)x-q)^{-1}dx\right).$$

An elementary calculation of these integrals leads us to the assertion for $D=4q^2+1$. q.e.d.

We set

$$\omega = \Gamma(1/4)^2/(2\sqrt{2\pi}) = \int_{-1}^{1}(1-x^4)^{-1/2}dx.$$

Then, $\omega=2.62205\ldots$. The following inequality is based on (2.15), LEMMA 3 applied to $\rho=1/4$, an obvious estimate $\zeta(1+2\rho)<1+\frac{1}{2\rho}$, and the inequality $\tau_g\le\pi/2$:

$$(2.22) \qquad I_1 < N^{5/4}2^{2(g-4)}\left(\frac{2^{3/2}3^2\omega^2}{\pi^2}+\frac{2^2 3^2\omega^3}{D^{1/4}\pi^2}\right)$$

$$< N^{5/4}2^{2(g-4)}\left(18+\frac{67}{D^{1/4}}\right).$$

The inequality (2.16) and LEMMA 3 applied to $\rho=1/2$ imply that

$$(2.23) \qquad I_2 < N^{3/2}\,\frac{2^{g-3}}{3}\log\varepsilon_0\cdot\left(1+\frac{4}{\sqrt{D}}\log\varepsilon_0\right).$$

Taking a trivial estimate $e/\pi^3<2^{-3}$ into account in (2.17), we conclude from (2.7), (2.8), (2.14), (2.17), (2.22) and (2.23) that THEOREM 1 in the introduction holds. q.e.d.

Our final task is to derive COROLLARY from THEOREM 1 in the introduction.

Proof of COROLLARY. Let the assumption be the same as in the assertion of COROLLARY. Each p_j ($1\le j\le k$), a divisor of N, is less than q. Therefore, with the help of Lemma 1, $\chi_D(p_j)=\left(\frac{D}{p_j}\right)^*=-1$. Since $e_1+\ldots+e_k\equiv 0 \bmod 2$,

$$\chi_D(N)=\prod_{j=1}^{k}\chi_D(p_j)^{e_j}=(-1)^{e_1+\ldots+e_k}=1=-\epsilon_E,$$

from which $g=r(E)+1=4$. Thus CORILLARY follows from THEOREM 1.

q.e.d.

Referemces

[Ch] S. Chowla, L-series and elliptic curves, Number Theory Day, Lecture Notes in Math. 626. Berlin Heidelberg New York: Springer 1977.

[C-F] S. Chowla and J. B. Friedlander, Some remarks on L-functions and class numbers, Acta Arith. **28**(1976), 414-417.

[Go1] D. Goldfeld, The class numbers of quadratic fields and the conjectures of Birch and Swinnerton-Dyer, Ann. Sc. Norm. Super. Pisa **3**(1976), 623-663.

[Go2] D. Goldfeld, Gauss' class number problem for imaginary quadratic fields, Bull. AMS **13**(1985) 23-37.

[G-Z] B. H. Gross and D. B. Zagier, Heegner points and derivatives of L-series, Invent. Math. **84**(1986) 225-320.

[K-L-O] H. K. Kim, M. Leu and T. Ono, On two conjectures on real quadratic fields, Proc. Japan Acad. **63**, Ser. A(1987) 222-224.

[La] G. Lachaud, On real quadratic fields, Bull. AMS **17**(1987) 307-311.

[Mo] R. A. Mollin, Class number one criteria for real quadratic fields, Proc. Japan Acad. **63**, Ser. A(1987) 121-125.

[Oe] J. Oesterlé, Nombres de classes des corps quadratiques imaginaires, Seminaire Bourbaki No. **631**(1983-1984).

[Og] A. P. Ogg, On a convolution of L-series, Invent. Math. **7** (1969) 297-312.

[Yo] H. Yokoi, Class-number one problem for certain kind of real quadratic fields, Proc. International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields, 1986, Katata, Japan, pp. 125-137.

[Za] D. Zagier, A Kronecker limit formula for real quadratic fields, Math. Ann. **213**(1975) 153-184.

Tsuneo Arakawa

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro
Tokyo 171 Japan

and

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Strasse 26
D-5300 Bonn 3