CONJECTURES ON ELLIPTIC CURVES

OVER QUADRATIC FIELDS.

by Dorian Goldfeld

§A. The average order of the Tate-Shafarevich group

In §302 of Gauss' Disqusitiones Arithmeticae one finds an interesting conjecture which states that the average order of the number of classes of binary quadratic forms with given discriminant $-D$ is $\frac{2\pi}{7\zeta(3)}\sqrt{D}$. Gauss supports this conjecture with numerical evidence he has obtained but never gives any indication of where the constant $\frac{2\pi}{7\zeta(3)}$ came from. In a later section he alludes to the problem of the average order of the number of classes of binary quadratic forms with a given positive discriminant, but does not formulate a precise conjecture.

Gauss' conjecture was first proved by I. M. Vinogradov [1918] and the subject has been subsequently dealt with by various authors: (B.V. Stepanov [1959]), (M.B. Barban [1962]), (A.F. Lavrik [1966]), (E. Hecke [1926]), (Shintani [1971]). Hecke's approach is most interesting as he interprets class numbers as Fourier coefficients of an Eisenstein series of weight $\frac{3}{2}$.

In (Goldfeld and Viola [1979]) a vast generalization of Gauss' conjecture was formulated. I should like to report on this work in the special case of an elliptic curve and this should be thought of as the elliptic analogue of Gauss' original conjecture as formulated in §302 of the Disqusitiones.

Let $\Gamma_0(N)$ denote the set of all two-by-two matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for which $a,b,c,d \in \mathbb{Z}$, $ad-bc = 1$, $c \equiv 0 \pmod N$. Consider a modular form $f(z)$ for $\Gamma_0(N)$ satisfying

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

We also take $f(z)$ to be a cusp form so that it vanishes at all the parabolic vertices of the compact Riemann surface $R_N = \Gamma_0(N)\backslash H^*$. Here H denotes the upper half plane and $H^* = H \cup \{\text{rational numbers}\}$. Then $f(z)dz$ is a holomorphic differential 1-form on R_N. If $f(z)$ is an eigenfunction for all the Hecke operators with rational Fourier coefficients, i.e.,

$$F(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi i n z} \qquad (a_n \in Q)$$

then it is known (Shimura [1971]), (Birch and Swinnerton-Dyer [1975]) that the associated L-function

$$L_f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

is the Hasse-Weil L-function for some elliptic subvariety E of the Jacobian variety of R_N. That is to say, for almost all rational primes p, $a(p)$ is just $p + 1 - N_p$ where N_p denotes the number of integer points on E (mod p). Here E is an elliptic curve of genus one which is also an elliptic subfield of finite index of the modular field $X_o(N)$ generated by $j(z)$ and $j(Nz)$, where $j(z)$ is the modular function satisfying

$$j\left(\frac{az+b}{cz+d}\right) = j(z) \qquad \text{for all} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z).$$

As pointed out by B. Gross, a convenient way of explicitly determining E is to compute all the integrals

$$\int_{\alpha}^{\beta} f(z)\, dz$$

where α, β range over the cusps of $\Gamma_o(N)$. These integrals are modular symbols and turn out to be rational multiples of the periods of E.

Now, we consider our elliptic curve E over an arbitrary quadratic field $Q(\sqrt{D})$. Let χ be a real primitive multiplicative character of $\mathbb{Z}/D\mathbb{Z}$, and define

$$f_\chi(z) = \sum_{n=1}^{\infty} a(n)\chi(n)e^{2\pi i n z}$$

$$L_f(s,\chi) = \sum_{n=1}^{\infty} a(n)\chi(n)n^{-s}$$

to be twists (by χ) of $f(z)$ and $L_f(s)$, respectively. Then $L_f(s)L_f(s,\chi)$ is the Hasse-Weil L-function of E over $Q(\sqrt{D})$ and we have the functional equations

$$\left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L_f(s) = w \left(\frac{\sqrt{N}}{2\pi}\right)^{2-s} \Gamma(2-s)L_f(2-s)$$

$$\left(\frac{D\sqrt{N}}{2\pi}\right)^{s}\Gamma(s)L_{f}(s,\chi) = w\chi(-N)\left(\frac{D\sqrt{N}}{2\pi}\right)^{2-s}\Gamma(2-s)L_{f}(2-s,\chi)$$

$$w = \pm 1 .$$

Let

$$\tau(\chi) = \sum_{a=1}^{D} \chi(a)e^{\frac{2\pi i a}{D}}$$

denote the Gauss sum.

An argument first introduced by Birch shows that

$$\begin{aligned}
\frac{-\tau(\chi)L_{f}(1,\chi)}{2\pi i} &= \tau(\chi)\int_{0}^{i\infty} f_{\chi}(z)\,dz \\
&= \sum_{n=1}^{\infty} a(n)\chi(n)\tau(\chi)\int_{0}^{i\infty} e^{2\pi i n z}\,dz \\
&= \sum_{r=1}^{D} \chi(r) \sum_{\substack{n=1 \\ (n,D)=1}}^{\infty} a(n)\int_{0}^{i\infty} e^{2\pi i n(z + r/D)}dz \\
&= \sum_{r=1}^{D} \chi(r)\int_{\frac{r}{D}}^{\frac{r}{D}+i\infty}\left(\sum_{\substack{n=1 \\ (n,D)=1}}^{\infty} a(n)e^{2\pi i n z}\right)dz
\end{aligned}$$

from which one can deduce that $\tau(\chi)L_{f}(1,\chi)$ must be a rational number multiplied by one of the periods of E. The particular period one gets depends only on whether χ is an even or odd character; that is to say, on whether the quadratic field in question is real or imaginary. According to the conjecture of Birch and Swinnerton-Dyer, this rational number should essentially be Ш_{D}, the order of the Tate-Shafarevich group of E over $Q(\sqrt{D})$. This is the elliptic analogue of Dirichlet's class number formula.

Since $L_{f}(s)$ is an eigenfunction for all the Hecke operators it has an Euler product

$$L_{f}(s) = \prod_{p|N}\left(1 - \frac{a(p)}{p^{s}}\right)^{-1}\prod_{p\nmid N}\left(1 - \frac{\alpha_{p}}{p^{s}}\right)^{-1}\left(1 - \frac{\overline{\alpha}_{p}}{p^{s}}\right)^{-1}$$

where $a(p) = \pm 1$ or 0 if $p|N$ and $|\alpha_{p}| = p^{1/2}$ for $p \nmid N$. It follows that the twisted L-series has the Euler product

$$L_f(s,\chi) = \prod_{p|N}\left(1 - \frac{\chi(p)a(p)}{p^s}\right)^{-1} \prod_{p\nmid N}\left(1 - \frac{\chi(p)\alpha_p}{p^s}\right)^{-1}\left(1 - \frac{\chi(p)\bar{\alpha}_p}{p^s}\right)^{-1} .$$

Putting

$$\lambda = \lim_{s\to 2} (s-2) \sum_{n=1}^{\infty} \frac{|a(n)|^2}{n^s}$$

to be the residue of the Rankin zeta function at $s = 2$, it is now possible to formulate our main conjecture:

MAIN CONJECTURE: *If Σ denotes a sum over discriminants of quadratic fields, we have*

$$\sum_{|D|\leq X} L_f(1,\chi) \sim \lambda \prod_{p|N} (1 - \tfrac{1}{p})^{-1} \sum_{|D|\leq X} (1+w\chi(-N)) \prod_{p|D}\left(1 - \frac{\alpha_p^2}{p^2}\right)\left(1 - \frac{\bar{\alpha}_p^2}{p^2}\right)\left(1 + \frac{1}{p}\right)^{-1}$$

where $w = (-1)^r$ and r is the rank of the Mordell-Weil group of E over Q .

It follows from this that

$$\text{Average order } \tau(\chi)L_f(1,\chi) \sim C\sqrt{|D|}$$

where

$$C = \lambda(1 + w\chi(-N)) \prod_{p|N} (1 - \tfrac{1}{p})^{-1} \prod_{p|D}\left(1 - \frac{\alpha_p^2}{p^2}\right)\left(1 - \frac{\bar{\alpha}_p^2}{p^2}\right)(1 + \tfrac{1}{p})^{-1} .$$

Since

$$\int_0^{\infty}\int_0^1 |f(z)|^2 y^s \, dxdy = (4\pi)^{-(s+1)}\Gamma(s+1) \sum_{n=1}^{\infty} \frac{|a(n)|^2}{n^{s+1}}$$

and

$$\int_0^{\infty}\int_0^1 = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_o(N)} \int\int_{\gamma D_o(N)}$$

where $D_o(N)$ is a fundamental domain for $\Gamma_0(N)$ and $\Gamma_\infty = \{\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix}; m\in\mathbb{Z}\}$ it follows that (see Rankin [1939])

$$\iint_{D_o(N)} |f(z)|^2 E(z,s) \, dxdy = (4\pi)^{-(s+1)}\Gamma(s+1) \sum_{n=1}^{\infty} \frac{|a(n)|^2}{n^{s+1}}$$

where

$$E(z,s) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_o(N)} (\operatorname{Im} \gamma z)^s .$$

Now $E(z,s)$ has a simple pole at $s = 1$ with residue independent of z. After a simple computation we get

$$\lambda = \frac{96\pi}{N} \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \langle f, f \rangle$$

where

$$\langle f, f \rangle = \iint_{D_o(N)} |f(z)|^2 \, dxdy$$

is the Petersson inner product of f with itself. It is now possible to express λ in terms of the periods of E.

Let $E_1(z)$ be a holomorphic Eisenstein series of weight one for $\Gamma_0(N)$ with multiplier χ_N where χ_N is a real primitive character of $\mathbb{Z}|N\mathbb{Z}$, so that $E_1(z)$ satisfies $E_1\left(\frac{az+b}{cz+d}\right) = \chi_N(d)(cz+d)E_1(z)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Consequently, $E_1(z)^2$ is a weight two modular form for $\Gamma_0(N)$. Hence, after taking inner products with f,

$$\langle E_1^2, f \rangle = a \langle f, f \rangle$$

for some constant a. A tedious calculation shows that

$$\langle E_1^2, f \rangle = bL_f(1)L_f(1,\chi_N)$$

for some other constant b. Since $L_f(1)$ and $L_f(1,\chi_N)$ are expressible in terms of the periods of E and a and b are easily calculated, one can in this way express λ in terms of the periods of E.

For example, consider the elliptic curve with conductor $N = 11$ with two periods

$$\Omega^+ = 0.6346047, \qquad \Omega^- = 1.4588166.$$

In this case one obtains

$$\lambda = \frac{2}{\pi} \Omega^+ \Omega^- .$$

There is a unique cusp form $f(z)$ for $\Gamma_0(11)$ and our conjecture predicts

Average value $\tau(\chi)L_f(1,\chi) \sim \frac{22}{5\pi}\,\Omega^+\,\Omega^- \cdot \sqrt{|D|}$.

For prime values of D, the Birch and Swinnerton-Dyer conjecture states

$$\text{Ш}_D = \begin{cases} \dfrac{\tau(\chi)L_f(1,\chi)}{2\Omega^-} & \chi(-1) = -1 \\[2ex] \dfrac{\tau(\chi)L_f(1,\chi)}{10\,\Omega^+} & \chi(-1) = +1\,. \end{cases}$$

We then have

<u>CONJECTURE</u> (A)

$$\text{Average value } \text{Ш}_D \sim \begin{cases} \dfrac{11\,\Omega^+}{5\pi}\,\sqrt{|D|}\,, & \chi(-1) = -1 \\[2ex] \dfrac{11\,\Omega^-}{25\pi}\,\sqrt{|D|}\,, & \chi(-1) = +1\,. \end{cases}$$

Glenn Stevens of Harvard University has provided a lot of numerical evidence supporting the above conjecture (see Goldfeld-Viola [1979]). A possible way to prove conjecture (A) would be to find some kind of modular form whose Fourier coefficients contain Ш_D.

§B. The average order of the rank

Let m_χ be the multiplicity of the zero of $L_f(s,\chi)$ at $s = 1$. According to the conjecture of Birch and Swinnerton-Dyer, this should be the rank of the Mordell-Weil group of E over $Q(\sqrt{D})$ minus the rank of E over Q. Numerical evidence supports the conjecture

<u>CONJECTURE</u> (B) $\sum\limits_{|D|\leq X} m_\chi \sim \frac{1}{2} \sum\limits_{|D|\leq X} 1.$

Put $\tilde{X} = \sum\limits_{|D|\leq X} 1$, to be the number of $\{$discriminants of quadratic fields$\} \leq X$.

It is not hard to show

<u>Proposition</u> (1) <u>As</u> $X \longrightarrow \infty$

$$\sum_{|D|\leq X} m_\chi \gtrsim \frac{1}{2}\tilde{X} .$$

To prove this just look at the functional equation

$$\psi(s,\chi) = \left(\frac{D\sqrt{N}}{2\pi}\right)^s \Gamma(s)L_f(s,\chi)$$

$$= w\chi(-N)\ \psi(2-s,\chi) .$$

Now, for about one half of the discriminants, $w\chi(-N) = -1$, from which it follows that $\psi(1,\chi) = 0$. It is relatively easy to prove the above proposition in this manner.

A more interesting problem is to obtain an upper bound for $\sum_{|D|\leq X} m_\chi$. In this direction we have:

<u>Proposition</u> (2) <u>Assuming the Riemann hypothesis for</u> $L_f(s,\chi)$

$$\sum_{|D|\leq X} m_\chi \leq (3.25 + \varepsilon)\ \tilde{X}$$

<u>and this holds for every</u> $\varepsilon > 0$ <u>and</u> X <u>sufficiently large</u>.

<u>Proof</u>: First of all note that

$$\frac{\psi'}{\psi}(s,\chi) = -\frac{\psi'}{\psi}(2-s,\chi).$$

Consider a function $F(s)$ satisfying

(i) $F(s)$ is entire in some strip $-c_0 \leq \mathrm{Re}(s) \leq c_0$

(ii) $\int_{c-i\infty}^{c+i\infty} |F(s)|\ |s|^\varepsilon |ds| = O(1), \quad -c_0 \leq c \leq c_0$

(iii) $F(s) = F(-s)$

(iv) $F(s)$ is real and positive if s is pure-imaginary.

By Cauchy's theorem and the functional equation for $\frac{\psi'}{\psi}(s,\chi)$ it follows that

$$\frac{1}{\pi i}\int_{c-i\infty}^{c+i\infty} \frac{\psi'}{\psi}(1+s,\chi)F(s)ds = \sum_{L_f(1+i\gamma,\chi)=0} F(i\gamma) .$$

Noting that

$$\frac{\psi'}{\psi}(s,\chi) = \log\left(\frac{D\sqrt{N}}{2\pi}\right) + \frac{\Gamma'}{\Gamma}(s) - \sum_{p|N}\sum_{k=1}^{\infty}\frac{a(p)^k(\log p)}{p^{ks}}\ \chi(p)^k$$
$$- \sum_{p\nmid N}\sum_{k=1}^{\infty}\frac{\alpha_p^k+\bar{\alpha}_p^k}{p^{ks}}\ (\log p)\ \chi(p)^k$$

and putting

$$\hat{F}(x) = \frac{1}{\pi}\int_{-\infty}^{\infty} e^{-ixt}\ F(it)\ dt$$

we obtain (by the positivity of $F(i\gamma)$)

$$\sum_{|D|\le X} m_\chi \le \frac{1}{F(0)}\left\{\tilde{X}\ \left(\log \frac{X\sqrt{N}}{2\pi}\right)\ \hat{F}(0) + \frac{\tilde{X}}{\pi}\int_{-\infty}^{\infty}\left|\frac{\Gamma'}{\Gamma}(1+it)\right|\,|F(it)|\,dt\right.$$
$$-\left(\sum_{|D|\le X}\ \sum_{p/N}\ \sum_{k=1}^{\infty}\frac{a(p)^k}{p^k}(\log p)\ \chi(p)^k\ \hat{F}(k\ \log p)\right.$$
$$\left.\left.+\sum_{p\nmid N}\ \sum_{k=1}^{\infty}\frac{\alpha_p^k+\bar{\alpha}_p^k}{p^k}\ (\log p)\ \chi(p)^k\ \hat{F}(k\ \log p)\right)\right\}\ .$$

Now, we have the estimate (see Goldfeld-Viola [1979])

$$\sum_{|D|\le X}\chi(p) \ll X^{\frac{1}{2}}\ (\log X)\ p^{\frac{3}{16}+\varepsilon}\ .$$

Applying this bound, we get

$$\sum_{|D|\le X}\ \sum_{p\nmid N}\frac{\alpha_p+\bar{\alpha}_p}{p}(\log p)\chi(p)\hat{F}(\log p) \ll X^{\frac{1}{2}}\log X\sum_p\frac{\hat{F}(\log p)}{p^{5/16-\varepsilon}}\ .$$

Similarly, for $k \ge 3$ and odd

$$\sum_{|D|\le X}\ \sum_{\substack{\ell=1\\ k=2\ell+1}}\frac{\alpha_p^k+\alpha_p^k}{p^k}\ (\log p)\chi(p)^k\ \hat{F}(k\ \log p) \ll X^{\frac{1}{2}}\ \log X\ \sum_{k\ge 3}\frac{\log p}{p^{\frac{k}{2}-\frac{3}{16}-\varepsilon}}\ \hat{F}(k\ \log p)$$

The case k is even (especially $k = 2$) is more delicate. Define

$$L_f^{**}(s) = \prod_{p|N}\left(1-\frac{a(p)^2}{p^s}\right)\prod_{p\nmid N}\left(1-\frac{\alpha_p^2}{p^s}\right)^{-1}\left(1-\frac{\bar{\alpha}_p^2}{p^s}\right)^{-1}\ .$$

We have

$$-\sum_{|D|\leq X} \sum_{k=1}^{\infty} \left(\sum_{p|N} \frac{a(p)^{2k}}{p^{2k}} (\log p) + \sum_{p\nmid N} \frac{\alpha_p^{2k}+\bar{\alpha}_p^{2k}}{p^{2k}} (\log p)\right) \hat{F}(2k \log p) =$$

$$= \frac{\tilde{X}}{\pi i} \int_{c-i\infty}^{c+i\infty} \frac{L_f^{**\,\prime}}{L_f^{**}} (2 + 2s)\ F(s)\ ds\ .$$

Combining these results gives

$$\sum_{|D|\leq X} m_X \leq \frac{\tilde{X}}{F(0)} \left[(\log \frac{X\sqrt{N}}{2\pi})\ \hat{F}(0) + \frac{1}{\pi}\int_{-\infty}^{\infty} \left| \frac{\Gamma'}{\Gamma} (1+it)\right| |F(t)|\, dt \right]$$

$$+ 0\left(\frac{X^{\frac{1}{2}} \log X}{F(0)} \sum_{p} \sum_{\substack{\ell=0 \\ k=2\ell+1}}^{\infty} \frac{\hat{F}(k \log p)}{p^{k/2-3/16-\varepsilon}} \right)$$

$$+ \frac{\tilde{X}}{F(0)\pi i} \int_{c-i\infty}^{c+i\infty} \frac{L_f^{**\,\prime}}{L_f^{**}} (2 + 2s)\ F(s)\ ds.$$

We have now run into a complicated extremal problem in Fourier transforms. One wants to minimize $\frac{\hat{F}(0)}{F(0)}$ subject to the restraint

$$\sum_{p} \sum_{\substack{\ell=0 \\ k=2\ell+1}}^{\infty} \frac{\hat{F}(k \log p)}{p^{k/2-3/16-\varepsilon}} \ll X^{1/2}\ \hat{F}(0).$$

It is also interesting that $L_f^{**}(s)$ has a zero at $s = 2$ so that in general

$$\frac{1}{F(0)\pi i} \int_{c-i\infty}^{c+i\infty} \frac{L_f^{**\,\prime}}{L_f^{**}} (2 + 2s)\ F(s)\ ds \sim \frac{1}{2}\ .$$

A choice of $F(s)$ that works fairly well is

$$F(s) = \left(\frac{e^{Ys} - e^{-Ys}}{s} \right)^2$$

where for the moment Y is a large variable to be chosen shortly. We have

$$\hat{F}(\log X) = \frac{1}{\pi i} \int_{c-i\infty}^{c+i\infty} X^{-s} \left(\frac{e^{Ys} - e^{-Ys}}{s} \right)^2 ds$$

$$= \frac{1}{\pi i} \int_{c-i\infty}^{c+i\infty} X^{-s}\ \frac{e^{2Ys} - 2 + e^{-2Ys}}{s^2}\ ds\ .$$

Consequently

$$\hat{F}(\log X) = \begin{cases} 4Y - 2\log X & 1 < X < e^{2Y} \\ 0 & e^{2Y} < X \\ 4Y & X = 1 . \end{cases}$$

Also,

$$F(0) = 4Y^2$$
$$\hat{F}(0) = 4Y .$$

It now follows that

$$\sum_{|D| \leq X} m_\chi \leq \frac{\tilde{X}(\log \frac{(\sqrt{N})X}{2\pi})}{Y} + \frac{\tilde{X}}{2} + 0\left(Y\, X^{\frac{1}{2}} \log X \sum_{p \leq e^{2Y}} \frac{1}{p^{5/16-\varepsilon}} \right) .$$

Choosing

$$Y = \left(\frac{4}{11} - \varepsilon\right) \log x$$

gives

$$\sum_{|D| \leq X} m_\chi \leq (3.25 + \varepsilon)\tilde{X} .$$

It would be nice if one could reduce the constant 2.75 in the above bound. Actually, any constant less than 2 would be most interesting. For example, if one had

$$\sum_{|D| \leq X}{}' m_\chi \leq (2-\varepsilon) \sum_{|D| \leq X}{}' 1$$

where the prime on the summation symbol means D is restricted to discriminants where $w\chi(-N) = +1$ (i.e., a plus sign in the functional equation) then this would imply that there are infinitely many quadratic fields $Q(\sqrt{D})$ for which E (if E has complex multiplication) does not have a non-rational point of infinite order lying in $Q(\sqrt{D})$. To see this, note that a recent theorem of Coates and Wiles [1977] implies that $L_f(s,\chi)$ vanishes if E has a non-rational point of infinite order lying in $Q(\sqrt{D})$. Since the sign in the functional equation is plus one, this implies that $L_f(s,\chi)$ actually has a double zero.

BIBLIOGRAPHY

M. B. Barban, "Linnik's 'large sieve' and a limit theorem for the class number of ideals of an imaginary quadratic field," Izk. Nauk SSSR, Ser. Mat. [1962], 573-78.

Birch and Swinnerton-Dyer, "Elliptic curves and modular functions," Modular functions of one variable, Springer Lecture Notes 476 [1975], 2-32.

J. Coates and A. Wiles, "On the conjecture of Birch and Swinnerton-Dyer," Inventiones Math. 39, [1977], 223-251.

D. Goldfeld and C. Viola, "Mean values of L-functions associated to elliptic, Fermat and other curves at the center of the critical strip," to appear J. Number Theory [1979].

E. Hecke, "Neue Herleitung der Klassenzahlrelationen von Hurwitz und Kronecker, Nachrichten der K. Gesellschaft der Wissenschaften zu Göttingen, Math.-Phys. Klasse [1926], 244-249.

A. F. Lavrik, "Functional equations of Dirichlet functions," Soviet Math. Dokl. 7 [1966], 1471-1473.

R. A. Rankin, "Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetic functions," Proc. Cambridge Philos. Soc. 35 [1939], 357-375.

G. Shimura, Arithmetic theory of automorphic functions, Princeton Univ. Press [1971], 183-184.

T. Shintani, "On zeta functions associated with prehomogeneous vector spaces," Seminar on Modern Methods in Number Theory, Inst. Statist. Math. Tokyo [1971], paper no. 40.

B. V. Stepanov, "On the mean value of the k^{th} power of the number of classes for an imaginary quadratic field," Dokl. Akad. Nauk SSSR 124 [1959], 984-986.

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139