Two new proofs of class number one

Mark Watkins

1.

Gauss (1801) conjectured that there are exactly 9 imaginary quadratic fields of class number one. This was proven independently by Heegner (1952), Baker (1966), and Stark (1967). The proof of Baker used transcendence theory, while the proofs of Heegner and Stark used modular functions, eventually reducing to finding all rational points on a finite list of genus 2 curves. Later works by various authors used different modular curves to give alternate proofs in this genre.

A third type of proof was proposed by Goldfeld (1976), involving the central vanishing of the L-function of a suitable elliptic curve. Indeed, given an elliptic curve with analytic rank 3 or more (again satisfying various technical conditions), it would be possible to show that the class number diverged effectively. Moreover, the famed conjecture of Birch and Swinnerton-Dyer suggested that such an L-function should in fact exist. The (difficult) work of Gross and Zagier (1986) then showed that such a triple central vanishing of an elliptic curve L-function did indeed occur.

2.

Our work herein takes an opposite point of view, desiring to prove the class number one result via the use of an elliptic curve of analytic rank 2. This is much easier to verify than analytic rank 3, requiring only a modular symbols calculation rather than the Gross-Zagier theorem.

Let $-q$ be a negative fundamental discriminant and χ its character. Given a weight 2 Hecke newform $F = \sum_n c(n)e^{2\pi inz}$ of level N with $\gcd(N,q) = 1$, we let $\Lambda(s) = (Nq/4\pi^2)^{s-1}\Gamma(s)^2 L_F(s)L_{F\chi}(s)$ be the scaled and completed product L-function for F and $F\chi$, satisfying a functional equation $\Lambda(s) = \epsilon\Lambda(2-s)$. Goldfeld's argument starts from Cauchy's residue theorem, noting that

$$\frac{\Lambda^{(l)}(1)}{l!} = \left(\int_{(2)} - \int_{(0)}\right)\frac{\Lambda(s)}{(s-1)^{l+1}}\frac{\partial s}{2\pi i} = (1+\epsilon^l)\int_{(2)}\frac{\Lambda(s)}{(s-1)^{l+1}}\frac{\partial s}{2\pi i},$$

and then expands the Dirichlet series in terms of a Mellin transform to get

$$\frac{\Lambda^{(l)}(1)}{l!} = (1+\epsilon^l)\sum_{n=1}^{\infty} c(n)R_\chi(n)W_l\Big(\frac{n}{Nq}\Big) \quad \text{with} \quad W_l(x) = \int_{(2)}\frac{\Gamma(s)^2}{(4\pi^2 x)^s}\frac{\partial s/2\pi i}{(s-1)^{l+1}},$$

while $R_\chi(n)$ is half the number of representations of n by reduced binary quadratic forms (A,B,C) of discriminant $-q$. Expanding this definition gives $\Lambda^{(l)}(1)/l!$ as

$$\frac{1+\epsilon^l}{2}\sum_{(A,B,C)}\sum_{(X,Y)\neq(0,0)}\sum c\big(AX^2+BXY+CY^2\big)W_l\Big(\frac{AX^2+BXY+CY^2}{Nq}\Big).$$

The main term comes from the $Y=0$ contributions, which are given in terms of the symmetric square L-function for F (with Euler adjustments for $p|N$ included),

while the error term can be bounded crudely for each form as $O(\sum_A 1/A)$ using nothing more than the density $1/\sqrt{q}$ of represented integers and the length Nq of the approximate functional equation, in conjunction with Deligne's bound on $c(n)$ and/or the Hasse bound for elliptic curves.

Under suitable technical conditions so that $\epsilon(F\chi) = -1$, we take $l + 1 = r$ to be the analytic rank of F, and writing h for the class number the above gives

The A-sum here should actually be $\sum_A c(A)\nu(A)/A$ where $\nu(p) = p/(p+1)$, with more technical conditions about F for non-squarefree A.

$$\frac{\Lambda^{(r-1)}(1)}{(r-1)!} = 0 = 2L^{[N]}_{S^2F}(2)\frac{(\log q)^{r-2}}{(r-2)!}\sum_A \frac{c(A)}{A} + O_F\big(h\sum_A \frac{1}{A}\big).$$

The symmetric-square evaluation at the edge of its critical strip is nonzero, and so the effective divergence of the class number then follows when taking a suitable elliptic curve of analytic rank $r = 3$, such as the -139th quadratic twist of 37b.

Perhaps initially as a curiousity, given an elliptic curve with analytic rank 2 we find that $h \gg 1$. However, a numerical computation with 446d (the first curve to meet the technical conditions regarding root number variation) obtains roughly only $h \geq 2/3$ as $q \to \infty$, indicating that more work must be done if this is to achieve a useful result.

We instead show that for n represented by the principal form there is suitable cancellation in the $c(n)$, so that when $h = 1$ the error term is negligible as $q \to \infty$.

3.

We have two different methods to show such cancellation in the $c(n)$ when n is restricted to representations by the principal form.

3.1. The first method is applicable for elliptic curves with complex multiplication by $\mathbf{Q}(\sqrt{-1})$, with an example of analytic rank 2 being the 136th quadratic twist of 32a. Here we recall that $c(n)$ can be written in terms of representations of n as a sum of two squares as

$$c(n) = \theta(n) \sum_{\substack{a=-\infty \\ (4a+1)^2+(2b)^2=n}}^{\infty} \sum_{b=-\infty}^{\infty} (4a+1)(-1)^b$$

where θ is either quadratic character of conductor 136.

We then write $n = X^2 + XY + \frac{q+1}{4}Y^2$ as a representation by the principal form with $Y \geq 1$, and upon completing the square we have $4n = (2X+Y)^2 + qY^2$. This then gives the error term as a sum similar to

$$\frac{1}{q}\sum_{Y=1}^{\infty} \sum_{\substack{X \\ n=(4a+1)^2+(2b)^2 \\ 4n=(2X+Y)^2+qY^2}} \sum_a \sum_b (4a+1)(-1)^b\theta(n)\, W\Big(\frac{n}{Nq}\Big).$$

The Y-sum can be truncated at small height by the decay of the Mellin transform.

Upon equating the n-expressions we get $4(4a+1)^2-(2X+Y)^2 = -4(2b)^2+qY^2$, where we can factor the left-side as tu with t and u as $2(4a+1) \pm (2X+Y)$, and switch variables from (a, X) to (t, u). Furthermore, we can then implicitly have

the u-variable occur via a congruence of $-4(2b)^2 + qY^2$ modulo t. Splitting into congruence classes modulo 272, an analysis of 2-adic and 17-adic conditions leads us to consider

$$\sum_{r_b=1}^{34}\sum_{r_t=1}^{272} z(Y, r_b, r_t) \sum_{t\equiv r_t\,(16\cdot 17)} \sum_{\tilde{b}} \frac{t+u}{4} W\Big(\frac{n}{Nq}\Big)$$
$$-4(68\tilde{b}+2r_b)^2+qY^2\equiv 0\,(t)$$

where $|z(Y, r_b, r_t)| \le 4$, while u and n are derived from t as above.

Here we wish to show that the inner double sum over t and $\tilde{b}$ has some cancellation. Let us note that its crude bounding would be $\ll q$, coming from noting that $|t|$ and $|u|$ can be curtailed at size around $\sqrt{q}$ by the W-decay, while the expectation is that there are a constant number of $\tilde{b}$-roots of the congruence on average. Thus (roughly) the double sum over $(t, \tilde{b})$ has $\ll \sqrt{q}$ members, each of size $\ll |t + u| \ll \sqrt{q}$.

In order to rigidify the contributions from $(t + u)/4$ and the W-term, we split t and $\tilde{b}$ into intervals of size Z (slightly smaller than $\sqrt{q}$), in practice using a smooth partition of unity on $\tilde{b}$. We are essentially left to consider for various (T, B) the expressions

$$\frac{G(T,B)}{4} \times \sum_{\substack{|t-T|<Z/2\\ t\equiv r_t\,(272)}} \sum_{|\tilde{b}-B|<Z/2} 1,$$
$$-4(68\tilde{b}+2r_b)^2+qY^2\equiv 0\,(t)$$

where

$$G(T,B) = \Big(T + \frac{qY^2 - 136^2B^2}{T}\Big) W\Big(\frac{1}{Nq}\Big[\frac{1}{4}\Big(T - \frac{qY^2 - 136^2B^2)}{T}\Big)^2 + qY^2\Big]\Big)$$

is an odd function of T.

We then recall a result of Hooley (1964) regarding equi-distribution of roots of a polynomial congruence to varying moduli. Our adaptation therein then gives an equi-distribution of the roots of the congruence $-4(68\tilde{b} + 2r_b)^2 + qY^2 \equiv 0\,(t)$ as t varies, implying the above double sum over $(t, \tilde{b})$ is sufficiently well-approximated as proportional to $Z^2/|T|$. This then shows the necessary cancellation, e.g. via pairing T with $-T$.

This proof rather crucially exploits the principal form in achieving the beneficial factorization of the difference of squares into tu. More generally such a factorization is plausible when the binary quadratic form represents a square (i.e., is in the principal genus), though some consideration must be given to uniformity considerations therein.

3.2. Our second method of proof codifies various work over the last decade concerning Hecke eigenvalues over quadratic sequences. This was studied by Blomer (2008), and then Templier and Tsimerman (2013). Indeed, we can almost read the desired result from the latter, though in practice (as they go rather in a different direction) it seems better to re-derive our needed estimate from their methods.

The multiplier on the right should be $(4\pi)^s/\Gamma(s)$.

We first note that, following Selberg (1965) and Sarnak's work (1984) with Goldfeld, the method of unfolding gives that

$$\sum_{X=-\infty}^{\infty} \frac{c(X^2+qY^2)}{(X^2+qY^2)^s} = \frac{\Gamma(s)}{(4\pi)^s}\langle P_{\tilde{s}}^{qY^2}, F\bar{\theta}\rangle$$

as an inner product involving a Poincaré series at the parameter $\tilde{s} = s - 1/4$, where here the standard θ-function is given by $\theta(z) = \sum_n e^{2\pi i n^2 z}$ and an analogous formula (involving the θ-series for the odd squares) is applicable more directly to the principal form. Here the mth Poincaré series for weight $3/2$ and congruence subgroup $\mathbf{\Gamma}$ is defined as

$$P_s^m = \sum_{\gamma \in \mathbf{\Gamma}_\infty \backslash \mathbf{\Gamma}} \bar{\nu}(\gamma) e(m\gamma z) \Big(\frac{cz+d}{|cz+d|}\Big)^{-3/2} \mathrm{Im}(\gamma z)^s,$$

where ν is the standard θ-multiplier system.

We then use the spectral decomposition for Maass forms of level $4N$ to write

$$\langle P_{\tilde{s}}^{qY^2}, F\bar{\theta}\rangle = \sum_{j=1}^{\infty} \langle P_{\tilde{s}}^{qY^2}, \phi_j\rangle\langle \phi_j, F\bar{\theta}\rangle + \sum_{\mathfrak{a}} \int_{(\frac{1}{2})} \langle P_{\tilde{s}}^{qY^2}, E_w^{\mathfrak{a}}\rangle\langle E_w^{\mathfrak{a}}, F\bar{\theta}\rangle \, \frac{\partial w}{4\pi i}.$$

Considering the discrete spectrum, the first inner product can be written (again by an unfolding argument via the Poincaré series) in terms of the qY^2-th Fourier coefficient of ϕ_j, and this coefficient can in turn be bounded by a result of Duke (1988), which generalizes the bound of Iwaniec (1987) for coefficients of holomorphic forms of half-integral weight. For our application, the second inner product $\langle \phi_j, F\bar{\theta}\rangle$ can be bounded almost trivially (unlike Templier and Tsimerman who in fact show the expected exponential decay in the eigenvalue parameter), while the continuous spectrum can again be handled by Duke's result.

This proof also exploits the principal form, though in general we could perhaps work at a level depending on the minimum A, and upon taking level-uniformity into account, we should be able to obtain a result when A is smaller than some explicit (small) power of q. In any case, the main difficulty in class number problems is when the minima are of size $\sqrt{q}$, and our methods do not avail for such.

Hooley's result only saves a small power of logarithm, while the use of the Iwaniec-Duke bound saves $1/28$ in the q-exponent.

Added later. It must be said that for all practical purposes Templier (2011) in his Theorem 2 (equation 1.6) already exposes the idea that analytic rank 2 implies class number 1, as when f has analytic rank 2 (with suitable root number variation) and $h = 1$ the left side is zero, while when $h = 1$ the right side is proportional to $L'_\chi(1) \sim \pi^2/6$ as $D \to \infty$. The given path to this result is rather involved (and much simplified by Templier and Tsimerman (2013) as they note in their §1.4), and although it largely avoids spectral theory and instead uses the δ-symbol method, the bound of Iwaniec and Duke is again ultimately the driving force.

Added later. I consider it quite likely that the method of our first proof could be reworked into the schema of Friedlander and Iwaniec (2013), which would thus ultimately be reliant on Iwaniec's bound (and thus get a slight power savings) rather than Hooley's work. See in particular the change of variables right after their equation (2.2). However, similar to the above comment regarding Templier (2011), this would seem to be a more circuitous path in the end.

Indeed, to my understanding, they rely on a result for *Weyl Sums for Quadratic Roots* (joint with Duke), which involves spectral theory (and thus the Duke-Iwaniec bound) when considering a sum of Kloosterman sums.

Added later in 2019. Yet another method could be to adapt Blomer's framework (for convergence, one needs to work in weight 4 or more). Here his Lemma 7 notes that integral weight Kloosterman sums over quadratic sequences yield Kloosterman sums in half-integral weight (see the discussion after his (1.6)). However, after doing this, it seems that his replacement of $g(h;c)$ by $g^\star(h;c)$ would not be wise in our setting due to lack of uniformity, and instead one should aim to simply estimate $\sum_c K(4m-h^2,-\Delta,c)/c\cdot g(h;c/4)/\sqrt{c}$ as a weighted sum of Kloosterman sums. For this to work, one needs a uniform version *à la* Sarnak and Tsimerman (2009), generalized to the setting of half-integral weight (and nontrivial level), needing in particular to beat the exponent $1/4$ on the mn dependence.

An analogous result appears in recent work of Dunn (2018), though for the η-multiplier rather than the Θ-multiplier. Also, he only beats the $1/4$ exponent in the case of opposite signs of m, n. Here I think the issue is that the same-sign case has a contribution from holomorphic forms, and this *prima facie* loses $(mn)^{1/4}$ from the lack of a Deligne bound in half-integral weight (compare (59) in Sarnak-Tsimerman to (7.2) of Dunn). Thus he sees no reason to use the same trick as in (9.5) since (10.2) is already losing the $(mn)^{1/4}$.

I am now told by Dunn that it is not so straightforward (as simply invoking Iwaniec) due to the arbitrarily large weights that will appear in the Kuznetsov formula, but that he and Ahlgren have fashioned a suitable version for a different application in arxiv.org/abs/1806.01187

However, one can presumably again rely on Iwaniec's $3/14$ improvement to the trivial $1/4$ bound in half-integral weight. Thus it again seems this is ultimately "just" a rather circuitous path to reach the class number 1 conclusion (starting with analytic rank 2) via the Iwaniec-Duke bound.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*. Mathematika **13** (1966), no. 2, 204–216. http://doi.org/10.1112/S0025579300003971

[2] V. Blomer, *Sums of Hecke eigenvalues over values of quadratic polynomials*. Int. Math. Res. Not. **2008**, no. 16. http://doi.org/10.1093/imrn/rnn059

[3] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*. Invent. Math. **92** (1988), no. 1, 73–90. http://doi.org/10.1007/BF01393993

[4] W. Duke, J. B. Friedlander, H. Iwaniec, *Weyl sums for quadratic roots*. IMRN **2012**, no. 11, 2453–2549. http://doi.org/10.1093/imrn/rnr112

[5] A. Dunn, *Uniform bounds for sums of Kloosterman sums of half integral weight*. Research in Number Theory, **4** (2018), paper 45, 21pp. http://doi.org/10.1007/s40993-018-0138-6

[6] J. B. Friedlander, H. Iwaniec, *Small Representations by Indefinite Ternary Quadratic Forms*. In *Number Theory and Related Fields*, edited by J. M. Borwein, I. Shparlinski, W. Zudilin, Springer PROMS **43** (2013), 157–164. http://doi.org/10.1007/978-1-4614-6642-0_7

[7] C. F. Gauss, *Disquisitiones Arithmeticae*. (Latin) [Arithmetical investigations] (1801). From his complete works (1863): http://eudml.org/doc/202621
English translation: A. A. Clarke, *Disquisitiones Arithmeticae*, Yale Univ. Press (1965).

[8] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **3** (1976), no. 4, 624–663. http://eudml.org/doc/83732

[9] B. H. Gross, D. B. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84** (1986), no. 2, 225–320. http://eudml.org/doc/143341

[10] K. Heegner, *Diophantische Analysis und Modulfunktionen*. (German) [Diophantine analysis and modular functions]. Math. Z. **56** (1952), 227–253. http://eudml.org/doc/169287

[11] C. Hooley, *On the distribution of the roots of polynomial congruences*. Mathematika **11** (1964), 39–49. http://doi.org/10.1112/S0025579300003466

[12] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*. Invent. Math. **87** (1987), 385–402. http://eudml.org/doc/143426

[13] P. Sarnak, *Additive number theory and Maass forms*. In *Number theory (New York, 1982)*, edited by D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn, and M. B. Nathanson. Springer LNM **1052** (1984), 286–309. http://doi.org/10.1007/BFb0071548

[14] P. Sarnak, J. Tsimerman, *On Linnik and Selberg's conjecture about sums of Kloosterman sums*. In *Algebra, arithmetic, and geometry: in honor of Yu. I. Manin, vol. II,* edited by Y. Tschinkel and Y. Zarhin. Progress in Mathematics **270** (2009), 619–635. http://doi.org/10.1007/978-0-8176-4747-6_20

[15] A. Selberg, *On the estimation of Fourier coefficients of modular forms*. Proc. Sympos. Pure Math. **8** (1965), 1–15. http://bookstore.ams.org/pspum-8

[16] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*. Michigan Math. J. **14** (1967), no. 1, 1–27. http://doi.org/10.1307/mmj/1028999653

[17] N. Templier, *A nonsplit sum of coefficients of modular forms*. Duke. Math. J. **157** (2011), no. 1, 109–165. http://doi.org/10.1215/00127094-2011-003

[18] N. Templier, J. Tsimerman, *Non-split sums of coefficients of $GL(2)$-automorphic forms*. Israel J. Math. **195** (2013), no. 2, 677–723. http://doi.org/10.1007/s11856-012-0112-2

[19] M. Watkins, *Class number one from analytic rank two*. Mathematika **65** (2019, to appear), 333–374. http://doi.org/10.1112/S0025579318000517

[20] M. Watkins, *A spectral proof of class number one*. Math. Z., to appear, 2019. http://doi.org/10.1007/s00209-018-2183-1