CLASS NUMBER ONE FROM ANALYTIC RANK TWO

MARK WATKINS

Abstract. We aim to re-prove a theorem conjectured by Gauss, namely there are exactly 9 imaginary quadratic fields $\mathbf{Q}(\sqrt{-q})$ with class number 1: specifically the list is $q \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$. Our method initially follows an idea of Goldfeld, but rather than using an elliptic curve of analytic rank 3 (provided by the Gross-Zagier theorem), we instead use an elliptic curve of analytic rank 2, where this L-function vanishing can be proven by modular symbols rather than a difficult height formula. It is already clear that Goldfeld's work yields a constant lower bound for the class number by such means, but unfortunately it seems that even for the best choice of elliptic curve this numerical constant is less than 1, unless one can show nontrivial cancellation in the L-function coefficients restricted to values taken by quadratic forms.

To show the latter, we consider a specific analytic rank 2 elliptic curve with complex multiplication by $\mathbf{Q}(\sqrt{-1})$, and then by adapting a result of Hooley's regarding equidistrbution of roots of a quadratic polynomial to varying moduli, are able to show that there is indeed sufficient coefficient cancellation, giving an effective resolution of class number one. As we use various aspects of the principal form, our proof seems inapplicable for larger class numbers.

We also comment on the possibility of using spectral techniques (following Templier and Tsimerman) to show the desired coefficient cancellation, though postpone the details of this to elsewhere.

1. Introduction

Let $\mathbf{Q}(\sqrt{-q})$ be an imaginary quadratic field, with $-q$ a fundamental discriminant. The *class number* (commonly denoted by h) is the number of reduced binary quadratic forms $ax^2 + bxy + cy^2$ with discriminant $b^2 - 4ac = -q$. This was studied by Gauss [24, §303], who noted h tended to grow with q, and indeed seemed to be of size proportional to $\sqrt{q}$ on average. However, while he computed that $h = 1$ for $q \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$, he was unable to show this list was complete.

1.1. There are sundry histories about class numbers of imaginary quadratic fields, in particular the events around the solutions of the class number one problem given in the second half of the 20th century, but we give our own eclectic version herein. (Amongst works we have cited for other reasons, see e.g. [68], [14, §21], [41, §22.4].)

1.1.1. The Dirichlet class number formula [19, 20] connects the class number to the special value at $s = 1$ of the associated Dirichlet L-function, namely that (as conjectured in part by Jacobi [42]) we have $L_\chi(1) = \pi h/\sqrt{q}$ for $q > 4$. In the wake of various work on the prime number theorem (including variants in arithmetic progressions), Gronwall appears to be the first to explicitly relate a type of zero-free region for $L_\chi(s)$ to the largeness of the class number [27, §3], noting in 1913 that a zero-free interval $1-c/\log q \le \sigma < 1$ for $L_\chi(\sigma)$ implies $h \gg \sqrt{q}/(\log q)(\log\log q)^{3/8}$.

Exploiting an "auxiliary modulus" idea attributed to Remak, in 1918 Landau [45] showed imaginary quadratic fields with small class number are statistically rare. Specifically, fixing $\delta > 0$ and letting $-q_n$ be the (putative) nth fundamental discriminant with $h(-q_n) \ll_\delta q_n^{1/2-\delta}$, he showed $q_{n+1} \gg q_n^C$ for any C. The ensuing paper [46] improved the range to $h(-q_n) \ll \sqrt{q_n}/\log q_n$, and *inter alia* gave Hecke's argument that improved Gronwall's result (removing the log-log factor).

Moreover, it was shown by Littlewood [49, §9] in 1928 that under the Generalized Riemann Hypothesis we have (where γ is Euler's constant)

$$\frac{1}{2}\cdot\frac{\pi^2}{6e^\gamma}\frac{\sqrt{q}}{\log\log q}\lesssim \pi h(-q)\lesssim 2\cdot e^\gamma\sqrt{q}\log\log q \quad\text{as } q\to\infty,$$

and these bounds are best possible [49, §10] except for the factors of 2.

1.2. In 1933, Deuring [15, 16] produced a decomposition of the Dedekind ζ-function for $\mathbf{Q}(\sqrt{-q})$ which implies some rather remarkable properties when $h = 1$, notably that the Riemann hypothesis is true up to height approximately $\sqrt{q}$. By including a twist by an auxiliary Dirichlet L-function, Heilbronn [34] showed that $h(-q)\to\infty$ as $q\to\infty$ (as conjectured by Gauss), though this result was *ineffective*, in that one could not say as what rate the divergence occurred. The method was soon improved by Landau [47] and Siegel [58], but the result remained ineffective. One source of this ineffectivity is the usage of the auxiliary modulus (cf. [45, §4, (13)]), namely consideration of the bi-quadratic field $\mathbf{Q}(\sqrt{-q},\sqrt{-k})$ for some $k > 0$. For k, q sufficiently large, it can be shown that at most one of $h(-q)$ and $h(-k)$ is small, but dispensing with the possibility that one of them is in fact equal to 1 cannot be attained by the method. Indeed it could be said: there was possibly a 10th imaginary quadratic field, but no one could say how large its discriminant might be, and in any case there was definitely not an 11th (as shown by Heilbronn and Linfoot [35]).

This was the state of affairs for another couple of decades, and then a somewhat obscure paper of Heegner [33] in 1952 claimed to resolve the class number 1 problem. His work was largely ignored, as it was quite idiosyncratic in many ways, and appeared to rely on work of Weber on modular functions that was "known" to be in error. The problem was settled in the 1960s, by two different methods. Baker [2] used his transcendence theory with linear forms in logarithms[1] to give an explicit upper bound (in theory) on a 10th possible q. Independently, Stark [62] used a variant[2] of modular functions to show $q > 200$ implies $h(-q) > 1$. Furthermore, Stark [63] resolved the "gap" in Heegner's work (as did Birch and Deuring in similar works, cited therein), and Siegel [59] also produced a slightly different proof using modular functions around this time. Similar proofs include [18, 43, 12, 5, 6, 54], demonstrating an observation of Serre [56, §A.5], that an imaginary quadratic field with class number one gives rise to an integral point on various modular curves.

1.2.1. Of course, once $h = 1$ has been resolved then it is logical to progress next to $h = 2\ldots$ Here Gauss found the largest example as 427. In fact, neither Baker [3] nor Stark [66] was necessarily optimistic initially about $h = 2$, but soon each had produced a proof [4, 67] via linear forms in logarithms. However, it *was* truly the case that $h = 3$ was a different animal, where the largest example of Gauss was 907.

1.2.2. A paper of Goldfeld [26] then proposed a plan to solve the class number problem effectively for any fixed h (this was done ineffectively by Tatuzawa [70], who showed that the "expected" list coming from $q \geq 2100(h\log 13h)^2$ always

---

[1] As pointed out by Stark [64], one can instead use a decomposition (as he derived at about this time) involving a twisted Dedekind ζ-function so that one only needs linear forms in *two* logarithms, when the result was already known from 1949 work [25] of Gelfond and Linnik.

[2] See [65] and [68, §3, Paragraph 3ff] for his comments regarding what aspect "modular functions" play in his proof (via the Kronecker Limit Formula), as compared to Heegner's work.

had at most one exceptional discriminant missing), which at the same time could incidentally hope to provide a new method of proof for $h = 1$.

Goldfeld's idea was to avoid the ineffectivity problems arising from the auxiliary modulus of Landau *et al.* by instead employing an L-function of higher degree, namely an elliptic curve L-function of degree 2. Additionally, unlike Dirichlet L-functions which are not expected to vanish at $s = 1/2$, the Birch–Swinnerton-Dyer conjecture suggests that there should be elliptic curve L-functions with high orders of central vanishing. For instance, there is an elliptic curve $E/\mathbf{Q}$ of conductor 5077 of rank 3, and one expects its L-function $L_E(s)$ to have a triple zero at the center of the critical strip. One could verify that $L'_E(1) \approx 0.00000\ldots$ to high precision (possibly assuming a modularity conjecture), but a proof was lacking.

This obstacle was then overcome by the deep work of Gross and Zagier [28], who used the theory of Heegner points to show that $L'_E(1)$ was zero for a specific elliptic curve (the -139th quadratic twist of a rank 0 elliptic curve of conductor 37). Oesterlé [52] then greatly streamlined Goldfeld's work and with Mestre did the computations (involving modularity) to show that $L'_E(1) = 0$ for the above E of conductor 5077. The obtained bound, unfortunately, is nowhere near the expectation $h \gg \sqrt{q}/\log\log q$, being merely $\frac{1}{55}\log q$ for q prime, with a mild Euler product over $p|q$ appended for q composite. This is, however, sufficient to show 907 is the last case with $h = 3$, and in a popular article Serre [55] wrote: "No doubt the same method will work for other small class numbers, up to 100, say." This challenge of proving the lists were complete for all $h \leq 100$ was completed 20 years later in [75].

1.3. Our work takes a different direction and seeks to provide an alternative proof of class number 1, by using Goldfeld's method with an L-function of a suitable elliptic curve (or modular form) of analytic rank 2. Since we can verify that such an L-function does indeed have analytic rank 2 by a modular symbols calculation, this is thus substantially simpler than invoking the Gross-Zagier theorem, as is (currently) necessitated to show that a given elliptic curve has analytic rank 3.

1.3.1. From an elliptic curve (or modular form) L-function $L_F(s)$ of analytic rank $r \geq 2$ and conductor/level N, and assuming the $-q$th quadratic twist $L_{F\chi}(s)$ has odd parity and $\gcd(q, N) = 1$, as per Goldfeld's work the symmetry of the functional equation in conjunction with the central vanishing then implies that

$$0 = \int_{(2)} \Lambda_F(s)\Lambda_{F\chi}(s)\frac{\partial s/2\pi i}{(s-1)^r} = \int_{(2)} \Big(\frac{Nq}{4\pi^2}\Big)^s \Gamma(s)^2 L_\chi^{[N]}(2s-1)\sum_{l=1}^{\infty}\frac{c_l R_\chi(l)}{l^s}\frac{\partial s/2\pi i}{(s-1)^r},$$

the latter step by comparing Euler products, with $L_\chi^{[N]}$ removing $p|N$. Here c_l is the lth Dirichlet series coefficient of the L-function of F, with $R_\chi(l)$ as half the number of representations of l by reduced binary quadratic forms of discriminant $-q$.

Under an assumption of sufficiently small class number, and in particular for class number 1 (when indeed, the induced error is exponentially small in $\sqrt{q}$), we can approximate $L_\chi(2s-1)$ by a quotient of ζ-functions and get

$$0 \approx \int_{(2)} \Big(\frac{Nq}{4\pi^2}\Big)^s \Gamma(s)^2 \frac{\zeta^{[N]}(4s-2)}{\zeta^{[N]}(2s-1)}\sum_{l=1}^{\infty}\frac{c_l R_\chi(l)}{l^s}\frac{\partial s/2\pi i}{(s-1)^r} = \sum_{k=1}^{\infty}\xi_k\sum_{l=1}^{\infty} c_l R_\chi(l)\tilde{W}_r\Big(\frac{k^2 l}{Nq}\Big),$$

the latter step by Mellin inversion. Here the ξ_k are the Dirichlet coefficients for the ζ-quotient, while $\tilde{W}_r$ is a weighting function with rapid decay. The contribution from square l is bounded away from 0, roughly proportional to $q(\log q)^{r-2}$ for $r \geq 2$.

In the case of class number 1 (and $q > 8$, so q is prime) there is only the principal form $x^2 + xy + \frac{q+1}{4}y^2$ so that we have $R_\chi(l) = 0$ for nonsquare $l < q/4$, and moreover R_χ is supported on a thin set beyond that.[3] Simply by taking absolute values, this already gives that the nonsquare l contribute no more than q times a constant (depending on N) which unfortunately even for the best choice (446d) with analytic rank 2 appears to exceed the main term (see Remark 2.3.1).[4]

1.3.2. Thus we aim instead to detect some cancellation in the Dirichlet coefficients c_l of an elliptic curve L-function as l runs over values taken by a quadratic form, or by fixing one variable, as l runs over the values of a quadratic polynomial, the model case being $x^2 + x + \frac{q+1}{4}$. This problem has been approached in the last decade by spectral techniques [7, 71, 72], but it was only after this paper's original submission that we realized the scope of results therein, and thus relegate our comments on this potentiality to the Remark at the end of §2.4. Herein we give a more elementary argument to show Dirichlet coefficient cancellation, which exploits the specific form of the c_l for an elliptic curve with complex multiplication by $\mathbf{Q}(\sqrt{-1})$.

Considering the 34th quadratic twist of the elliptic curve $Y^2 = X^3 - X$ (this twist has analytic rank 2) and putting θ for a corresponding quadratic character mod 136, we write $l = (4a+1)^2 + (2b)^2$ so that $c_l = \theta(l)\sum_{a,b}(4a+1)(-1)^b$ when summing over such (a,b)-representations. After splitting into congruence classes to fix the character, we simply compare this form of l with $4l = (2x+1)^2 + q$ to get

$$4(4a+1)^2 - (2x+1)^2 = -4(2b)^2 + q, \tag{1}$$

and then factor the left side as tu, changing variables from (a,x) to (t,u).

This leads us to consider roots of the congruence $P(w) = -4(2w)^2 + q \equiv 0\,(t)$ for varying moduli t, where this polynomial corresponds to the real quadratic field $\mathbf{Q}(\sqrt{q})$. By a method of Hooley [38] we can show that the roots ν have ν/t suitably equi-distributed, allowing us to split into ranges that smooth the weights from $4a+1$ and the $\tilde{W}_r$-function. This then shows the error term is asymptotically negligible as $q \to \infty$, effectively answering the class number 1 problem of Gauss.

1.4. We wish to provide some perspective for our result. Firstly, the exploitation of an elliptic curve of analytic rank 2 rather than analytic rank 3 avoids the difficult Gross-Zagier theorem, replacing it by a rather straightforward modular symbols calculation [51, 13]. However, we still need some central vanishing of the L-function beyond what is simply forced by the root number.

Stark inquires in a survey article [68] whether it is possible to provide a "purely analytic" proof of class number 1, and while he is ambivalent [68, §4] about the status of Goldfeld's work as such, I cannot see how reducing the strain from analytic rank 3 to analytic rank 2 would suddenly allow this "purely analytic" moniker to be applicable (whereas analytic rank 1, being forced by odd parity, could conceivably induce such a terminological distinction).

[3] The effective length of the approximate functional equation is of size Nq (due to the L-function having degree 2), with a density of nonzero coefficients of approximately $\pi h/\sqrt{q}$.

[4] This part of the argument can also be done considering only *primitive* representations of l by the principal form (which leads more directly to the symmetric-square L-function of F appearing in the numerator instead of $\zeta(4s-2)$), and indeed our presentation in §6 following the original method of Goldfeld (as adapted by Oesterlé) will be closer to this, but in retrospect I think the above version more clearly emphasizes the importance of $\sum_l c_l R_\chi(l)/l^s$.

1.4.1. Additionally, it also seems that we fail with the second part of Stark's hope, namely that once a "purely analytic" proof of class number 1 was found it would generalize and give a decent-sized effective lower bound on the class number. Indeed, at least with the presentation given here, we use the class number 1 assumption in various ways, and most notably the above method to detect cancellation of coefficients appears only to work usefully with the principal form (in slightly more generality we can achieve a factorization as with (1) for any form that represents a square (thus is in the principal genus), but it seems to me there is a resulting lack of uniformity that limits its efficacy). Furthermore, Hooley's equidistribution result only saves a small power of logarithm; here it must be said that he has a "superior" result [37] for quadratic polynomials that obtains a power-savings, albeit my analysis was that its lack of uniformity implies it is un-useful for our setting.

1.4.2. It goes without saying that all our implicit constants will be effective. Let us give some idea of what size to expect for them.

The bound from Hooley's work for moduli t up to size T is of the form

$$\frac{T(\log\log T)^{(5-\sqrt{2})/2}}{(\log T)^{1-\sqrt{2}/2}},$$

and while I have not computed the optimal balance between exponents, I expect (see Remarks 7.6.2 and 7.7.1) that the log-exponent here will be reduced by a factor of at least 3 in the final comparison, so that the ultimate error term (from representations $x^2+xy+\frac{q+1}{4}y^2$ with $y\neq 0$) will be no smaller than $Cq/(\log q)^{1/10}$. Furthermore, my guess is that the constant C will not be too small, probably at least $\sqrt{2^6 17^2/4\pi^2}\approx 21.6$ from just the conductor of the elliptic curve lengthening the l-sum, and evidently some more from the extra log-log power in Hooley's work. Although we improve his exponent therein, we deal with a range of $T\approx\sqrt{q}$ where $\log\log T\approx 200$ (or more) cannot be neglected. There is also another factor of perhaps 136^2 coming from splitting a and b into arithmetic progressions to fix the character value.

In any case, and perhaps this is already optimistic, if we have $C=10^9$ while the main term is of size 1, this would necessitate handling $q\le\exp(10^{90})$ by alternative means. A more mechanical approach toward the explicit constants would perhaps leave $q\le\exp(10^{10000})$. However, even this would (nowadays) be essentially routine to handle by the method of Stark's thesis [61], which would use Deuring's theorem [15, 16] and high-precision computation of the first two Riemann ζ-zeros to D digits to get a putative bound of $\log q\gg 10^{D/2}$ for $q>163$ with class number 1.

1.5. **Notation.** Our most novel piece of notation is using ∂ when integrating – I suspect at one point the letter "d" was clashing, and upon switching, I've never found a reason to go back. We also denote L-functions with subscripts, for instance $L_E(s)$ for the L-function of an elliptic curve E. More substantially, we use a different scaling in the completed L-function, namely for (say) a primitive even Dirichlet character η of conductor k we have $\Lambda_\eta(s)=L_\eta(s)\Gamma(s/2)(\sqrt{k/\pi})^{s-1/2}$, whereas the usual ansatz would have s for the final exponent. In general we scale by the center of the critical strip, so for elliptic curve L-functions (and those of weight 2 modular forms) we will have $\Lambda_E(s)=L_E(s)\Gamma(s)(\sqrt{N}/2\pi)^{s-1}$.

Another oddity is that h will typically *not* stand for the class number in the sequel, but rather for a harmonic in a Fourier decomposition.

We write $-q$ for the fundamental discriminant of (assumed) class number 1, with χ its quadratic character and K the corresponding imaginary quadratic field. The generic Dirichlet character will be labelled η, and we use η_s to denote the Kronecker character for s a fundamental discriminant (also allowing $s = 1$).

The number of distinct prime divisors of n will be denoted $\omega(n)$, while $\Omega(n)$ counts these with multiplicity. The number of (positive) divisors of n is $\tau_2(n)$.

We write $\int_{(2)}$ for (e.g.) a line integral up the 2-line, while we retain the typical $s = \sigma + it$ decomposition of a complex variable where applicable. Finally, in the congruential notation $a \equiv b\,(c)$ we allow c to be negative.

2. Outline of proof

We give a somewhat long-winded outline of our methods, in particular taking some pains to note in §2.3 and §2.3.1 that a more simplistic argument (forgoing detecting of Dirichlet series coefficient cancellation and instead just taking absolute values) does not seem to work.

We assume that $K = \mathbf{Q}(\sqrt{-q})$ has class number 1 where $-q$ is a fundamental discriminant with $q > 163$. By the theory of genera of Gauss [24, §257] we know that q is prime. We let χ be the quadratic character corresponding to K, so that $\chi(p) = -1$ for all primes $p \le q/4$.

2.1. We first briefly recall Goldfeld's work [26], in its rendition by Oesterlé [52]. Let f be a weight 2 modular newform of level $\Gamma_0(N)$ whose L-function vanishes to order r at its central point. In the context of class number 1 we can assume that $\gcd(N, q) = 1$, as otherwise the theory of genera implies (for $q > N$) that the class number is even.

Writing $\Lambda_f(s) = L_f(s)\Gamma(s)(\sqrt{N}/2\pi)^{s-1}$ for the (scaled) completed L-function and $\Lambda_{f\chi}(s)$ for its twist by χ, we consider the integral

$$0 = \left(\int_{(2)} - \int_{(0)}\right)\Lambda_f(s)\Lambda_{f\chi}(s)\frac{\partial s/2\pi i}{(s-1)^u}.$$

For $u \le r$ this is zero by Cauchy's integral theorem since the integrand is entire and there is rapid decay in vertical strips. Substituting $s \to 2 - s$ in the second integral and using the functional equations $\Lambda_f(s) = \epsilon_1\Lambda_f(2-s)$ and $\Lambda_{f\chi}(s) = \epsilon_2\Lambda_{f\chi}(2-s)$ we get

$$0 = I_f(u) - \epsilon_1\epsilon_2(-1)^u I_f(u)$$

where

$$I_f(u) = \int_{(2)} \Lambda_f(s)\Lambda_{f\chi}(s)\frac{\partial s/2\pi i}{(s-1)^u} = \int_{(2)} L_f(s)L_{f\chi}(s)\Gamma(s)^2\Big(\frac{Nq}{4\pi^2}\Big)^{s-1}\frac{\partial s/2\pi i}{(s-1)^u}.$$

The coprimality of q and N implies that $\epsilon_2 = \chi(-N)\epsilon_1$ (see [52, §2.2] for instance).

2.1.1. *Root numbers.* Again in the context of class number 1 we have $\chi(p) = -1$ for all $p|N$, so that $\chi(N) = (-1)^{\Omega(N)}$ and since $\chi(-1) = -1$ for odd characters (applicable for imaginary quadratic fields), we get $\epsilon_2 = \chi(-N)\epsilon_1 = \epsilon_1(-1)^{\Omega(N)+1}$. We write

$$0 = I_f(u) + \kappa(u)I_f(u) \text{ where } \kappa(u) = \epsilon_1^2(-1)^{u+\Omega(N)} \tag{2}$$

and in our orthogonal case have $\epsilon_1 = \pm 1$, so we should take $\Omega(N)$ to be of the same parity as u, as else the above (2) is uninteresting. In particular, for $u = 2$ we cannot use $N = 389$ (or $N = 433$).

Remark. This facet of root number variation already appears in Goldfeld's work (see the choice of μ in his Theorem 1). Indeed, when using the rank 3 curve 5077a one has a condition that $\gcd(q, 5077) = 1$, and Gross and Zagier only achieve a "clean" theorem by working out the root number variation when f is the -139th quadratic twist of 37a, and showing Goldfeld's condition is suitably applicable (see [52, §4.3]).

2.2. We employ Oesterlé's notation and write

$$\Psi_f(s) = L_f(s)L_{f\lambda}(s) \text{ and } G_f(s) = \frac{L_{f\chi}(s)}{L_{f\lambda}(s)}$$

where λ is the completely multiplicative Liouville function which is -1 on all primes. For class number 1 we have $\chi(p) = \lambda(p) = -1$ for all $p < q/4$. Here the notation $f\lambda$ means to negate all terms in the Euler product, so that writing

$$L_f(s) = \prod_p \Bigl(1 - \frac{\alpha_p}{p^s}\Bigr)^{-1}\Bigl(1 - \frac{\beta_p}{p^s}\Bigr)^{-1} \text{ and } L_{f\lambda}(s) = \prod_p \Bigl(1 + \frac{\alpha_p}{p^s}\Bigr)^{-1}\Bigl(1 + \frac{\beta_p}{p^s}\Bigr)^{-1}$$

we see $\Psi_f(s) = \prod_p (1-\alpha_p^2/p^{2s})^{-1}(1-\beta_p^2/p^{2s})^{-1}$ is naturally a function of $2s$. Up to bad Euler factors, the product $\Psi_f(s)$ equals $L_{S^2f}(2s)/L_{A^2f}(2s)$ where S^2f and A^2f are respectively the symmetric and alternating squares of f (at the level of motivic L-functions), and moreover $L_{A^2f}(2s) = \zeta(2s-1)$ has a pole at $s = 1$.

Writing $G_f(s) = \sum_l g_l/l^s = 1+\tilde{G}_f(s)$ we find $g_l = 0$ unless all $p|l$ have $\chi(p) \neq -1$ and in particular in the context of class number 1 we have $g_l = 0$ for $1 < l < q/4$. From the above equation (2), when $\kappa(u) = +1$ we have

$$\begin{aligned} 0 = I_f(u) &= \int_{(2)} \Psi_f(s)G_f(s)\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1}\frac{\partial s/2\pi i}{(s-1)^u} \\ &= \int_{(2)} \Psi_f(s)\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1}\frac{\partial s/2\pi i}{(s-1)^u} + \int_{(2)} \Psi_f(s)\tilde{G}_f(s)\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1}\frac{\partial s/2\pi i}{(s-1)^u}. \end{aligned}$$

2.2.1. The first integral (call it $J_f(u)$) can be computed by moving the path of integration to the left, with the decay from the q^s-term dominating. The main term comes from the residue at $s = 1$, while the resulting error term is easily estimated via a standard zero-free region of ζ and the vertical decay of $\Gamma(s)^2$. Writing $B_f(2s)$ for a (possible) correction from bad Euler factors, upon combining with f, we have

$$J_f(u) \approx 2L_{S^2f}(2)B_f(2)(\log q)^{u-2}.$$

Although it will prove fruitless in the end, we can note that there is a weight 2 modular eigenform f of level 446 with analytic rank 2 corresponding to the elliptic curve 446d, and for f this main term is $J_f(2) \approx 2L_{S^2f}(2)\frac{2\cdot 223}{1\cdot 222} \approx 20.2$.

2.3. The second integral above (call it $E_f(u)$) can be bounded via the thin support of series coefficients for $\tilde{G}_f(s)$. For this, Oesterlé elegantly uses a positivity argument in conjunction with the fact that the Dirichlet series coefficients of $\Psi_f(s)\tilde{G}_f(s)$ are bounded by those of $\zeta_K(s-1/2)^2 - \zeta(2s-1)^2$, which we can write as

$$[\zeta_K(s-1/2) - \zeta(2s-1)]^2 + 2\zeta_K(s-1/2)\zeta(2s-1) - 2\zeta(2s-1)^2.$$

The first term is negligible as every n^{-s} in its support has $n \geq (q/4)^2$, while the third term can be dropped by positivity. Indeed the inverse Mellin transform of $z^{-s}\Gamma(s)^2/(s-1)^u$ is positive, decreasing, and concave for $u \geq 0$, and by accounting $\zeta_K(s-1/2)$ in terms of the density of integers represented by quadratic forms, namely replacing it by $\frac{\pi h}{2}(\sqrt{q}/2)^{1/2-s}\,\frac{s-1/2}{s-3/2}$ (see [52, §3.4]), the error $E_f(u)$ is essentially bounded by

$$2\int_{(2)}\zeta(2s-1)\Gamma(s)^2\cdot\frac{\pi h}{2}\Big(\frac{\sqrt{q}}{2}\Big)^{1/2-s}\,\frac{s-1/2}{s-3/2}\cdot\Big(\frac{Nq}{4\pi^2}\Big)^{s-1}\,\frac{\partial s/2\pi i}{(s-1)^u}$$
$$\approx 2\zeta(2)\Gamma(3/2)^2\cdot\frac{\pi h}{2}\frac{2}{\sqrt{q}}\frac{\sqrt{Nq}}{2\pi}\frac{1}{(1/2)^u}=h\frac{\pi^2}{6}\Gamma(3/2)^2 2^u\sqrt{N},$$

with the residue from the pole at $s=3/2$ the main contributor to this error. For the above f of level 446 and $u=2$ this is $\approx 109.1h$, and comparing to the main term in §2.2.1 gives a colloquial notion that this method of proof can show that the class number is $\geq 20.2/109.1\approx 1/5.4\approx 0.185$.

2.3.1. Although it turns out to be fruitless, with $h=1$ one can propose an attempt to go further in this vein, upon noting Oesterlé's method is not too sharp in the error term when it bounds the contribution of $\Psi_f(s)\tilde{G}_f(s)$ for the principal form (wherein the eccentricity of the ellipse plays a substantial rôle with respect to lattice point counting, as the asymptotic count (as $T\to\infty$) of $\pi T/\sqrt{q}$ is not too accurate for T of size q). Writing $\Psi_f(s)=\sum_k \xi_k/k^{2s}$ an alternative method is to expand in terms of an inverse Mellin transform as

$$E_f(u)=\int_{(2)}\Psi_f(s)\tilde{G}_f(s)\Gamma(s)^2\Big(\frac{Nq}{4\pi^2}\Big)^{s-1}\frac{\partial s/2\pi i}{(s-1)^u}=\frac{4\pi^2}{qN}\sum_{k=1}^{\infty}\xi_k\sum_{l\geq q/4}g_l W_u\Big(\frac{4\pi^2k^2l}{Nq}\Big)$$

where $W_u(z)$ is given by

$$W_u(z)=\int_{(2)}z^{-s}\Gamma(s)^2\frac{\partial s/2\pi i}{(s-1)^u}.$$

Specializing to $u=2$, in terms of K-Bessel functions we have $W_2(z)=2K_0(2\sqrt{z})/z$, so in particular $W_2(z)=O(e^{-\sqrt{z}})$ as $z\to\infty$. The rapid decay of W_u combined with the assumption of class number 1 together imply the l that have more than one prime factor p with $\chi(p)\neq -1$ give a negligible contribution, as all such l will exceed $(q/4)^2$. Thus with negligible error we can replace the l-sum by a sum over p with $\chi(p)\neq -1$. Moreover, we have $g_p=[1+\chi(p)](\alpha_p+\beta_p)$, which for p with $\chi(p)=+1$ is twice the pth Dirichlet series coefficient of f.

With f of level 446 and analytic rank 2 as above, by using the regularity of the p with $\chi(p)\neq -1$, namely coming from $p=x^2+xy+\frac{q+1}{4}y^2$ with $\gcd(x,y)=1$, one can obtain a bound for $E_f(2)$ of about 32 and my recollection is by additionally exploiting the vanishing of $J_f(u)$ for $u=0$ that I was able to achieve approximately 26, still less than the goal of 20.2. One could attempt to use other modular forms, such as 159k4a, or a nonorthogonal form (with unitary root number) with single central vanishing; my investigation concluded that the above choice of 446k2d is the best, yet still insufficient.[5]

[5] An alternative interpretation here is that there are "good reasons" why such an attempt via crude bounding does not suffice, for instance the existence of 163. While we have elided it above, in both the residue approximation for $J_f(2)$ and the bounding of $E_f(2)$ there is some q-dependence that goes to zero as $q\to\infty$ (somewhat rapidly in fact, for instance $\ll 1/q^{1/4}$). If it were the case that a crude bounding of $E_f(2)$ could show it to be much smaller than $J_f(2)$ asymptotically, then the question of whether this would already exclude $q=163$ could arise.

Indeed, it is perhaps not a fruitless numerical peregrination to consider 446d and $q=163$, and observe how $E_f(2)$ works to offset $J_f(2)$.

2.4. Our improvement shall come from detecting sufficient cancellation in the g_l for a specific elliptic curve, in particular one with complex multiplication. For this, we use the 34th quadratic twist of the elliptic curve 32a, namely $Y^2 = X^3 - 34^2X$, which has analytic rank 2 (via a modular symbols calculation), and write θ for a corresponding quadratic character modulo 136. Note that the conductor here is $N = 2^6 17^2$ which has $\Omega(N) = 8$, so the root numbers work out as desired.

We write c_l for the lth Dirichlet series coefficient of this elliptic curve. The modular newform of level 32 can be written as a **q**-series as

$$\sum_{a=-\infty}^{\infty} \sum_{b=-\infty}^{\infty} (4a+1)(-1)^b \mathbf{q}^{(4a+1)^2+(2b)^2},$$

so that upon taking the 34th quadratic twist we have

$$c_l = \theta(l) \sum_{\substack{a=-\infty \\ (4a+1)^2+(2b)^2=l}}^{\infty} \sum_{b=-\infty}^{\infty} (4a+1)(-1)^b.$$

2.4.1. As above, we have $g_p = [1+\chi(p)]c_p$, while the contribution from nonprime l to the error $E_f(2)$ is negligible by the decay of $W_2(z) = 2K_0(2\sqrt{z})/z$. Thus we want to estimate

$$E_1 = \sum_{k=1}^{\infty} \xi_k \sum_p c_p \bigl[1+\chi(p)\bigr] W_2\Bigl(\frac{4\pi^2k^2p}{Nq}\Bigr),$$

and show this is smaller than q in size. Since the coefficients ξ_k play no arithmetic rôle in the end (only their size matters), we can first multiply and divide by a Dirichlet series supported on squares that replaces the above sum over p by a sum over pm^2, with c_p replaced by c_{pm^2}. Indeed, an accounting shows that we have

$$E_1 \approx \sum_{k=1}^{\infty} \tilde{\xi}_k \sum_{l=1}^{\infty} c_l \tilde{R}_\chi(l) W_2\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr),$$

where the $\tilde{\xi}_k$ are adequately bounded, and $h = 1$ implies that $\tilde{R}_\chi(l)$ is the number of representations of l by the principal form $x^2 + xy + \frac{q+1}{4}y^2$ with $y \geq 1$.

Expanding c_l from the above, we thus want to bound $\sum_k |\tilde{\xi}_k||E_1^k|$ where

$$E_1^k = \sum_{\substack{a=-\infty \\ l=(4a+1)^2+(2b)^2}}^{\infty} \sum_{b=-\infty}^{\infty} \tilde{R}_\chi(l)(4a+1)(-1)^b\theta(l)W_2\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr).$$

We can note the W_2-decay allows us to curtail k at some height, say $K = (\log q)^{1/10^9}$.

Also note that it is not merely "generic" cancellation in $\sum_l c_l\tilde{R}_\chi(l)$ that we require, as this would already follow when weighting by W_0 (or more generally W_{-2k} for positive integers k), but this does not suffice for the desired W_2-weighting.

2.4.2. We then consider $l = x^2 + xy + \frac{q+1}{4}y^2$ with $y \geq 1$, which by rearrangement says $4l = (2x+y)^2 + qy^2$. By the accounting of $\tilde{R}_\chi(l)$ we have

$$E_1^k = \sum_{y=1}^{\infty} \sum_{\substack{x \\ l=(4a+1)^2+(2b)^2 \\ 4l=(2x+y)^2+qy^2}} \sum_a \sum_b (4a+1)(-1)^b\theta(l)\, W_2\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr)$$

The above conditions on l imply that

$$4(4a+1)^2 - (2x+y)^2 = -4(2b)^2 + qy^2.$$

We can factor the left side with

$$t = 2(4a+1) + (2x+y), \;\; u = 2(4a+1) - (2x+y),$$

so that $tu = -4(2b)^2 + qy^2$ while

$$2(4a+1) = (t+u)/2, \;\; 2x+y = (t-u)/2$$

and

$$4l = (t-u)^2/4 + qy^2, \;\; l = (t+u)^2/16 + (2b)^2.$$

A quite similar idea appears with (2.2) of a paper by Friedlander and Iwaniec doi.org/10.1007/978-1-4614-6642-0_7

Indeed their argument (based on related joint work with Duke) can likely be turned into a proof of class number 1 with sufficient effort, though would ultimately rely on the Iwaniec-Duke bound (and so save a power instead of a log-power) in place of our utilization of Hooley's result.

2.4.3. We then switch variables from (a,x) to (t,u). An analysis modulo 16 gives conditions ensuring the integrality of (a,x), and when combined with a similar analysis modulo 17 suffices to fix the effect of the character θ.

We are then left to consider sums (for $k \le K$) such as

$$\sum_{y\le K}\sum_{r_b=1}^{34}\sum_{r_t=1}^{272} z(y,r_b,r_t) \sum_{\substack{t\equiv r_t\,(16\cdot 17)\\ -4(68\tilde b+2r_b)^2+qy^2\equiv 0\,(t)}}\sum_{\tilde b} \frac{t+u}{4}\, W_2\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr)$$

where $|z(y,r_b,r_t)| \le 4$, while u and l 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 by the W-decay at size around $\sqrt{q}$, 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 $\ll |t+u| \ll \sqrt{q}$.

2.4.4. In order to rigidify the contributions from $(t+u)/4$ and the W-term, we split t and $\tilde b$ into intervals of size $Z = \sqrt{q}/S$ where $S = (\log q)^{1/100}$, in practice using a smooth partition of unity on $\tilde b$. The small t, say those with $|t| \ll \sqrt{q}/S^{1/5}$, contribute a negligible amount (by a crude estimate), and we are essentially left to consider for various (T,B) the expressions

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

where

$$G(T,B) = \Bigl(T + \frac{qy^2-136^2B^2}{T}\Bigr) W_2\biggl(\frac{4\pi^2k^2}{Nq}\Bigl[\frac14\Bigl(T-\frac{qy^2-136^2B^2}{T}\Bigr)^2 + qy^2\Bigr]\biggr)$$

is an odd function of T.

Our adaptation of Hooley's methods 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, namely that the above double sum over $(t,\tilde b)$ is sufficiently well-approximated as proportional to $Z^2/|T|$, and this shows the necessary cancellation, e.g. via pairing T with $-T$.

Remark. As noted in the introduction, it was only belatedly that we became aware of relevant work regarding sums of Hecke eigenvalues over quadratic sequences, most notably the work of Templier and Tsimerman [72].

In particular, returning to

$$E_1 \approx \sum_{k=1}^{\infty} \tilde{\xi}_k \sum_{l=1}^{\infty} c_l \tilde{R}_\chi(l) W_2\Big(\frac{4\pi^2 k^2 l}{Nq}\Big),$$

it appears that [72, (1.5)] almost shows the type of cancellation that we desire. Replicating their result directly, for $X \gg \sqrt{d}$ they show

$$\sum_n a_\pi(n^2+d)V(n/X) \ll_{\pi,\epsilon} X^{1/2+\epsilon} d^\delta \Big(1+\frac{X^2}{d}\Big)^{\theta/2},$$

where a_π are unitary normalized coefficients of an automorphic cuspidal representation π and V is a smooth function on $[1,2]$, while $\delta = 3/16$ comes from bounds on half-integral weight coefficients (alternatively interpreted as a q-subconvexity parameter) and $\theta = 7/64$ involves Selberg's eigenvalue conjecture. Transposing to our genre with $X \approx \sqrt{d}$, this analogously indicates $|E_1| \ll \sqrt{q} \cdot q^{1/4+\epsilon} q^\delta \ll q^{15/16+\epsilon}$ and moreover there is no restriction concerning complex multiplication.

Taking d to be our qy^2, it is only the fact that n^2+qy^2 does not quite give us our desired representations (involving an extra factor of 4 when e.g. n and y are odd) that prevents us from using this result in the form given. In [72, Remark (ii)] they mention that their methods should be applicable to other quadratic polynomials, and indeed n^2+n+d can be handled via using the Θ-function of the odd squares, namely $\Theta(z) - \Theta(4z)$. We give the details in [76], though for technical reasons we use $\delta = 3/14$ coming from the work of Iwaniec [39] and Duke [21].[6]

Note that their result gives a power-savings (since $\delta < 1/4$) in the region of interest; however, for larger class numbers the difficulty typically is with the minima a near $\sqrt{q/3}$, where uniformity considerations will arise since the spectral analysis would then be applied on $\Gamma_0(aN)$. As in our proof here, I don't see any way to generalize beyond class number one (where control of a is obvious).

2.5. **Hooley's equi-distribution of roots.** We can first note there are two papers by Hooley on equi-distribution of roots of polynomials to varying moduli. The first one [37] might seem to be more relevant to our problem, as it is attuned to quadratic polynomials and attains a power-savings, but unfortunately it seems to me that the uniformity is inadequate for the current purposes. Hooley's second paper [38] is for general polynomials and only saves a small power of logarithm; although he does not consider questions of uniformity, in the context of class number 1 we can handle this without much difficulty.

[6]Another observation is that Templier's left side in [71, Theorem 2, (1.6)] is 0 for f of analytic rank 2 when $h = 1$, while $h = 1$ implies his right side is proportional to $L_\chi'(1) \sim \pi^2/6$ as $D \to \infty$, and this thus implies the class number 1 result. Moreover, [71] uses the δ-symbol method (and spectral theory only appears tangentially); I apologize for not mentioning these matters in [76].

My analysis is that the bound in [71] ultimately also comes from Iwaniec's bound for Fourier coefficients, though through a long and winding process. The last paragraph of [72, §1.4] explains that one of their goals therein is to simplify the argument. They mention a slight generalization of [71, (1.6)] in [72, (1.9)], though it seems to me that α and β should include a factor of $L_\chi(1)$ (and thus not be dependent only on π). Note also that the $O(1/|D|^\eta)$ is in its more natural position here, in not being multiplied by $L_\chi(1)$. Indeed [71, §7] implicitly proves such a version, and then multiplies the $O(1/D^\eta)$ by $L_\chi(1)$ via Siegel's ineffective lower bound for the latter.

There is also a minor (and irrelevant) error in [71, (7.2)] in that the Γ-factor of the functional equation needs to be squared (thus of degree 4).

In the form given in [38], Hooley's result on the congruential root distribution for an irreducible polynomial P considers for nonzero harmonics h the exponential sum over the roots ν modulo m as

$$S_P(h,m) = \sum_{P(\nu)\equiv 0\,(m)} \exp(2\pi i h\nu/m),$$

and for P quadratic and primitive shows that

$$R_{P,h}(x) = \sum_{m\le x} S_P(h,m) \ll_{P,h} \frac{x(\log\log x)^{5/2}}{(\log x)^{(2-\sqrt{2})/2}}.$$

One can bound the h-dependence for $h\neq 0$ crudely as $\sqrt{|h|}$, which will suffice for our application. We need to consider m in an arithmetic progression (modulo 272), which ends up largely being a non-issue, as the method of proof subsumes it. Similarly, the fact that our polynomials might be nonprimitive is easily handled (indeed, I must admit to not seeing exactly where Hooley demands this).

2.5.1. We briefly describe Hooley's method. He writes each modulus as $m = m_1m_2$ where m_1 consists of primes less than $x^{1/200\log\log x}$ with m_2 the complement, and notes that an elementary upper-bound sieve shows that the contribution from m with $m_1 \ge x^{1/3}$ (say) is negligible. For the remaining m, he applies the factorization

$$S_P(h,m) = S_P(h\bar{m}_2, m_1)S_P(h\bar{m}_1, m_2),$$

so that (with m_1, m_2 having the above meaning)

$$|R_{P,h}(x)| = \Bigl|\sum_{\substack{m_1m_2\le x\\ m_1\le x^{1/3}}}\sum S_P(h\bar{m}_2,m_1)S_P(h\bar{m}_1,m_2)\Bigr| \le \sum_{\substack{m_1m_2\le x\\ m_1\le x^{1/3}}}\sum \rho_P(m_2)\bigl|S_P(h\bar{m}_2,m_1)\bigr|$$

where $\rho_P(k)$ is number of roots of P modulo k, and the m_2-sum is (much) longer than the modulus m_1. He then applies Cauchy's inequality and the basic estimate

$$\sum_{a=1}^{k} \bigl|S_P(ah,k)\bigr|^2 \le k\rho_P(k)\cdot \gcd(h,k),$$

which gives a (slight) savings on average compared to the trivial bound $k\rho_P(k)^2$. Combined with a result on the number of primes that split, this then gives the stated savings of a small power of $\log x$.

It could be noted that the smallness of the upper bound does not come from equi-distribution to *varying* moduli as such, but rather: to each *fixed* modulus the S_P-sum over the roots evinces some cancellation on average,[7] and this is then used with a factorization of $S_P(h,m)$ with respect to $m = m_1m_2$ to conclude the result.

2.5.2. To handle the q-dependence (in P) we need to show that there are sufficiently many small primes which do not split in the real quadratic field $\mathbf{Q}(\sqrt{q})$. Here we can note that class number 1 (together with quadratic reciprocity) implies that up to $q/4$ the splitting primes are exactly the primes that are 3 mod 4.

Similarly, in the application back to our above double $(t,\tilde{b})$ sum, we proceed by a Fourier expansion in h, with the main term from $h=0$. This main term then is simply the number of roots of the congruence when the modulus varies (over an

[7]Heath-Brown essentially notes this aspect with his final comment in a 2011 review [30] of a paper which included a Hooley-type result for equidistribution of roots of reducible quadratics.

arithmetic progression mod 272, though this aspect is essentially harmless). The effective range here is for moduli of roughly size $\sqrt{q}$, and to achieve an asymptotic formula we need a subconvexity bound for Dirichlet L-functions in the q-aspect. Although we could just quote such a result from the literature ([10] for instance), again in the context of class number 1 we argue alternatively, using that $L_\eta(s)L_{\eta\chi}(s)$ is well-approximated as an Euler product by $L_{\eta^2}(2s)$ (up to bad factors).

Remark. When considering either the splitting of primes in $\mathbf{Q}(\sqrt{q})$ or the above subconvexity bound the most blunt tool would be to exploit the Deuring-Heilbronn phenomenon [48], which will show that our class number 1 assumption implies the relevant Dirichlet L-functions satisfy a Riemann hypothesis up to a significant height (roughly $\sqrt{q}$). However, this is unnecessary, and the extent to which proofs of class number 1 rely on Deuring's work [15, 16] is a historical point that seems in some confusion. For instance, the survey article [69] says that "Deuring's theorem was an essential first step in solving the [class number 1] problem."

What is likely meant here is that Deuring's theorem gives a regular spacing of zeros of the Dedekind ζ-function of $\mathbf{Q}(\sqrt{-q})$, which can be compared to computations of zeros of the Riemann ζ-factor. Indeed, Stark in his thesis[8] used the computation of the first two zeros of the Riemann ζ-function to 20 digits to show [61] that a putative 10th fundamental discriminant with class number 1 had to satisfy the bound $q > \exp(2.2 \cdot 10^7)$. However, in his subsequent actual proof [62, §4] of class number 1 he only needs to assume $q > 200$, which leaves a mere hand calculation (already done by Gauss!) to give the entire list. The other proofs in the genre of "modular functions" similarly do not rely on Deuring's theorem to handle small q.

A bound of $q \le e^{160000}$ from an explicit Baker's method was given by Bundschuh and Hock [9], though in a comparable restricted problem (for class number 2) Baker [3] obtains a rather smaller bound of $q \le 10^{500}$; anyway, Deuring's theorem and computations of zeros would indeed be needed to finish the proof here.

Finally, Goldfeld's method as finished by Gross and Zagier (and computed by Oesterlé) implies directly that $h > 1$ for $q > e^{55}$, though my recollection (see the comparison with §2.3, where $L_{S^2 f}(2) \approx 7.546$ for $f = 5077a$ while $E_f(3) \approx 736.43$) is that with some effort one can reduce 55 to 50 (or 49) if desired, and a more exacting analysis for the principal form as in §2.3.1 would certainly allow the class number 1 proof to be finished by direct sieving. Here even $e^{55} \approx 10^{24} \approx 2^{80}$ can likely be handled by a computational sieve if necessary,[9] though this is of course heavily exploiting technological advances of the past few decades.

As noted in §1.4.2, the bound given by our proof is likely quite large, yet still should succumb to the method of Stark's thesis with (routine) computation of the first two Riemann ζ-zeros to 200 or perhaps 20000 digits.

Remark. As described more fully in [76, §3.9, Remark], one should be able to derive a "Deuring decomposition" for $\Lambda_f(s)\Lambda_{f\chi}(s)$, but this doesn't seem to be of much use except at the central point $s = 1$.

[8] I recall Stark has said that he didn't exploit a trick that would allow the exponent to essentially be squared, while D. B. Zagier indicates using more than two zeros increases the method's power.

[9] For instance, one can break up the sieving into congruence classes modulo M as the product of 8 with the odd primes up to 43, leaving $e^{55}/M \approx 15 \cdot 10^6$ discriminants to be sieved for each class, which takes less than a second. There are about 226 billion residue classes of interest, so the computation (which parallelizes perfectly) would take time on the order of a few core-millennia. Compare [60], which used around a core-century to sieve up to about 10^{25} in an analogous problem.

3. Binary quadratic forms and consequences of class number 1

We recall some basic facts about binary quadratic forms, and the consequences therein for class number 1. This is essentially due to Gauss [24] (see e.g. [41, §22]).

3.1. Let $-q$ be a negative fundamental discriminant, so q mod 4 is either 0 or 3. A reduced binary quadratic form $ax^2+bxy+cy^2$ of discriminant $-q=b^2-4ac<0$ has $-a<b\le a<c$ or $0\le b\le a=c$, which incidentally means that $(b+i\sqrt{q})/2a$ as a point in the upper half-plane is in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$. There is always the principal form ($a=1$), namely $x^2+xy+\frac{q+1}{4}y^2$ when q is 3 mod 4, and $x^2+\frac{q}{4}y^2$ when q is 0 mod 4. The class number of $\mathbf{Q}(\sqrt{-q})$ is the number of such reduced forms.

3.1.1. The theory of genera [24, §257] corresponds to divisors of q. It says that the class number is divisible by $2^{\omega(q)-1}$, and perhaps more directly in the context of class number 1, one can simply write down a nonprincipal reduced form corresponding to a nontrivial factorization of q.

Writing (a,b,c) for a form, when $q=tu$ is odd with $1<t<u$, we find that either $(t,t,(t+u)/4)$ or $((t+u)/4,(u-t)/2,(t+u)/4)$ is reduced and non-principal.

For $4\|q$ and $q>4$ we always have the reduced non-principal form $(2,2,(q+4)/8)$, and factorizations $q/4=tu$ with $1<t<u$ yield $(t,0,u)$ and either $(2t,2t,(t+u)/2)$ or $((t+u)/2,(u-t),(t+u)/2)$.

For $8\|q$ and $q>8$ we always have the reduced non-principal form $(2,0,q/8)$, and factorizations $q/8=tu$ by $1<t<u$ yield $(t,0,2u)$ and either $(2t,0,u)$ or $(u,0,2t)$.

Thus we find that if the class number is 1 and $q>8$, then q is prime. Similarly, we see 2 splits for q that are 7 mod 8, namely $(2,1,(q+1)/8)$ is a non-principal reduced form for $q>7$, so the class number 1 assumption implies that q is 3 mod 8.

3.1.2. Writing χ for the quadratic character associated to $K=\mathbf{Q}(\sqrt{-q})$, we then put $R^\star_\chi(l)$ for half the number of primitive representations of l with $\gcd(x,y)=1$ by reduced binary quadratic forms of discriminant $-q$, so that

$$R^\star_\chi(l)=\prod_{p|l}\bigl[1+\chi(p)\bigr]\cdot\prod_{p^2|l}\chi(p).$$

This is 0 if $\chi(p)=-1$ for some $p|l$. Moreover, we have $\zeta_K(s)/\zeta(2s)=\sum_l R^\star_\chi(l)/l^s$.

The class number 1 assumption (for $q>8$) thus says $R^\star_\chi(l)=0$ for $1<l\le q/4$, as for $y\ne 0$ the values of the principal form $x^2+xy+\frac{q+1}{4}y^2$ exceed $q/4$. In particular, we have $\chi(p)=-1$ for all $p\le q/4$. Similarly, the l with $q/4\le l\le (q/4)^2$ that are primitively represented must be prime, due to the multiplicativity of $R^\star_\chi(l)$.

4. Results on roots of quadratic congruences

We derive some simple results about roots of quadratic congruences. The relevant background concerning Dirichlet characters can be found in texts such as [14].

4.1. For fixed (r,q,y) we consider the quadratic polynomial given by

$$P(w)=-4(68w+2r)^2+qy^2.$$

Here we can assume $0\le r<34$, while in our situation of interest we have $q>163$ is prime and $0<|y|<q$ (simply to avoid $q|y$).

We let $\rho_P(t)$ be the number of roots of P modulo t, and $\bar\rho_P(t)$ be the number of roots of w^2-q modulo t, so that $\bar\rho_P(t)$ is the tth coefficient of the so-called "primitivized" Dedekind ζ-function $\zeta_{\sqrt{q}}(s)/\zeta(2s)$ of the real quadratic field $\mathbf{Q}(\sqrt{q})$, that is

$$\frac{\zeta_{\sqrt{q}}(s)}{\zeta(2s)} = \frac{\zeta(s)L_{\eta_{4q}}(s)}{\zeta(2s)} = \prod_{\bar{\rho}_P(p)=2} \frac{1+1/p^s}{1-1/p^s} \prod_{\bar{\rho}_P(p)=1} \Bigl(1+\frac{1}{p^s}\Bigr) = \prod_p U_p(s),$$

where η_{4q} is the primitive real Dirichlet character of modulus $4q$.

4.1.1. The Chinese remainder theorem implies ρ_P is multiplicative, and for prime powers p^e with $p\nmid 34y$ we have $\rho_P(p^e)=\rho_P(p)=\bar{\rho}_P(p)$.

For $p\notin\{2,17\}$ with $p|y$ we write $v=v_p(y)$ and then get $\rho_P(p^e)=p^{\lceil e/2\rceil}$ for $e\le 2v$, while $\rho_P(p^e)=p^v\bar{\rho}_P(p)$ for $e>2v$.

One can write down similar bounds for $\rho_P(p^e)$ with $p\in\{2,17\}$, but we can avoid needing such in the sequel in any event.

By multiplicativity, for t coprime to 34 we thus have $\rho_P(t)\le \gcd(t,y)2^{\omega(t)}$.

4.1.2. We next introduce some notation to deal with imprimitivities.

We write $E_P(s)$ for the distinction between $\bar{\rho}_P$ and ρ_P, so that as Dirichlet series

$$\sum_m \frac{\rho_P(m)}{m^s} = E_P(s)\sum_m \frac{\bar{\rho}_P(m)}{m^s}$$

and we have

$$E_P(s) = \prod_{p|34y} \left(U_p(s)^{-1}\sum_{e=0}^{\infty} \frac{\rho_P(p^e)}{p^{es}}\right) \tag{3}$$

where the $U_p(s)^{-1}$ removes the Euler factor for $\bar{\rho}_P$ corresponding to $\zeta_{\sqrt{q}}(s)/\zeta(2s)$, and the sum over e replaces it by the enumeration for ρ_P. We can also take a version of this when twisted by a Dirichlet character η, namely that

$$\sum_m \frac{\rho_P(m)\eta(m)}{m^s} = E_P^\eta(s)\sum_m \frac{\bar{\rho}_P(m)\eta(m)}{m^s}$$

where the Euler factor of $E_P^\eta(s)$ at $p|34y$ is

$$U_p^\eta(s)^{-1}\sum_{e=0}^{\infty}\frac{\rho_P(p^e)\eta(p^e)}{p^{es}} \quad \text{with} \quad U_p^\eta(s) = \begin{cases} \frac{1+\eta(p)/p^s}{1-\eta(p)/p^s} & \text{for } \bar{\rho}_P(p)=2,\\ 1+\eta(p)/p^s & \text{for } \bar{\rho}_P(p)=1,\\ 1 & \text{for } \bar{\rho}_P(p)=0.\end{cases}$$

We write $\tilde{E}_P(s)$ for $E_P(s)$ twisted by the principal character modulo 272, which has the effect of removing the Euler factors at 2 and 17.

We can moreover derive a simple bound for $|E_P^\eta(s)|$ for $\sigma\ge 4/5$ when twisting by a character η of modulus divisible by 2 and 17 (which again removes those Euler factors), namely $\rho_P(p^e)\le 2p^{\lceil e/2\rceil}$ implies the pth Euler factor is bounded by $10p^{1/5}$ (the $e=1$ term dominating), and then multiplying over $p|y$ crudely gives $\ll |y|^{1/4}$.

For a Dirichlet character η we denote its associated primitive character by $\eta_\star$, and write

$$V_\eta(s) = \frac{L_\eta(s)}{L_{\eta_\star}(s)} = \prod_p \frac{1-\eta_\star(p)/p^s}{1-\eta(p)/p^s}.$$

The Euler factor is possibly nontrivial only at p dividing the modulus, and we have that $|V_\eta(s)|, |V_\eta(s)^{-1}| \ll_\eta 1$ for $\sigma\ge 4/5$.

4.2. **Analytic estimates.** We need an asymptotic result regarding the summation of $\rho_P(m)$ when m is restricted to a coprime congruence class a modulo either 68 or 272. Our planned application will use this with x roughly of size $\sqrt{q}$, and in order to achieve a beneficial result we need a slight sub-convexity bound in the q-aspect for Dirichlet L-functions, which would be provided by Burgess [10] for instance.

However, our class number 1 assumption allows us to argue more directly.

Lemma 4.2.1. *Suppose that* $\mathbf{Q}(\sqrt{-q})$ *has class number 1, and let* P *be as above with* $0 < |y| \le Y = (\log q)^{1/10^9}$*, and let* a *be given with* $\gcd(a, 272) = 1$*. Then for* $1 \le x \le q/4$ *we have*

$$\sum_{\substack{1\le m\le x\\ m\equiv a\,(272)}} \rho_P(m) = \frac{x}{2\phi(272)}\frac{\tilde{E}_P(1)}{L_{\eta_{-4}}(1)} + O\bigl(xYe^{-0.1\sqrt{\log 3x}}\bigr),$$

and by combining together four such arithmetic progressions, thus also

$$\sum_{\substack{1\le m\le x\\ m\equiv a\,(68)}} \rho_P(m) = \frac{x}{2\phi(68)}\frac{\tilde{E}_P(1)}{L_{\eta_{-4}}(1)} + O\bigl(xYe^{-0.1\sqrt{\log 3x}}\bigr).$$

Remark. One can improve the error term via the Deuring-Heilbronn phenomenon (using that the L-functions have their zeros on the half-line up to height of size $\sqrt{q}$).

Remark. The upper bound given here on y is of no real significance, but is what appears later in any event.

Proof. We consider the Dirichlet series

$$A(s) = \sum_{m=1}^{\infty} \frac{\rho_P(m)}{m^s} = E_P(s)\cdot\frac{\zeta_{\sqrt{q}}(s)}{\zeta(2s)} = E_P(s)\prod_{\bar\rho_P(p)=2}\frac{1+1/p^s}{1-1/p^s}\prod_{\bar\rho_P(p)=1}\Bigl(1+\frac{1}{p^s}\Bigr),$$

Our assumption of class number 1 implies that for $p \le q/4$ we have $\bar\rho_P(p) = 0, 1, 2$ for primes $p \equiv 1, 2, 3\,(4)$ respectively (by quadratic reciprocity [24]). Thus we have

$$A(s) \cong E_P(s)\Bigl(1+\frac{1}{2^s}\Bigr)\prod_{p\equiv 3\,(4)}\frac{(1+1/p^s)}{(1-1/p^s)}$$

where the "$\cong$"-symbol indicates equality on Dirichlet series coefficients up to $q/4$. Via re-arrangement we find that this is

$$E_P(s)\prod_p\Bigl(1-\frac{1}{p^s}\Bigr)^{-1}\cdot\Bigl(1-\frac{1}{4^s}\Bigr)\prod_{p\equiv 1\,(4)}\Bigl(1-\frac{1}{p^s}\Bigr)\prod_{p\equiv 3\,(4)}\Bigl(1+\frac{1}{p^s}\Bigr) = E_P(s)\frac{\zeta(s)(1-1/4^s)}{L_{\eta_{-4}}(s)}.$$

Similarly, when twisting by a character η mod 272 we have

$$A_\eta(s) = \sum_{m=1}^{\infty}\frac{\rho_P(m)\eta(m)}{m^s} \cong E_P^\eta(s)\frac{L_\eta(s)(1-\eta(4)/4^s)}{L_{\eta\eta_{-4}}(s)},$$

and since $\eta(4) = 0$, writing this in terms of primitive characters says

$$A_\eta(s) \cong E_P^\eta(s)\frac{L_{\eta_\star}(s)}{L_{(\eta\eta_{-4})_\star}(s)}\frac{V_\eta(s)}{V_{\eta\eta_{-4}}(s)}.$$

4.2.2. For $1 \le x \le q/4$ a truncated Perron's formula (see [53, §5] or [14, §17]) with $\sigma_0 = 1 + 1/\log 3x$ yields

$$\sum_{m \le x} \rho_P(m)\eta(m) = \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{x^s}{s} E_P^\eta(s) \frac{L_{\eta_\star}(s)}{L_{(\eta\eta_{-4})_\star}(s)} \frac{V_\eta(s)}{V_{\eta\eta_{-4}}(s)} \frac{\partial s}{2\pi i} + O\Big(\frac{x^{\sigma_0} Y (\log 3x)^2}{T}\Big).$$

Writing $t^\star = |t| + 5$ we then move the line of integration to $\sigma = 1 - c/\log t^\star$, and by standard zero-free regions and bounds for Dirichlet L-functions [14] get that

$$\sum_{m \le x} \rho_P(m)\eta(m) = \delta_\eta \frac{\tilde{E}_P(1)}{L_{\eta_{-4}}(1)} \frac{V_{\eta_1}(1)}{V_{\eta_{-4}}(1)} + O\Big(x^{1-c/\log T} Y (\log T)^2\Big) + O\Big(\frac{xY(\log 3x)^2}{T}\Big),$$

where we can take $c = 1/200$ (see [50]), while δ_η is 1 when η is principal and else 0.

Upon choosing $T = e^{\sqrt{c \log 3x}}$, by character orthogonality we thus get

$$\begin{aligned}\sum_{\substack{1 \le m \le x \\ m \equiv a\,(272)}} \rho_P(m) &= \frac{1}{\phi(272)} \sum_{\eta\,(272)} \bar{\eta}(a) \sum_{1 \le m \le x} \rho_P(m)\eta(m) \\ &= \frac{x}{2\phi(272)} \frac{\tilde{E}_P(1)}{L_{\eta_{-4}}(1)} + O\big(xYe^{-0.1\sqrt{\log 3x}}\big),\end{aligned}$$

since $V_{\eta_1}(1) = (1-1/2)(1-1/17)$ and $V_{\eta_{-4}}(1) = (1-\eta_{-4}(17)/17) = (1-1/17)$. $\square$

Corollary 4.2.3. *Suppose that* $\mathbf{Q}(\sqrt{-q})$ *has class number 1 and let* P *be as above with* $0 < |y| \le Y = (\log q)^{1/10^9}$. *Then for* $1 \le x \le q/4$ *we have*

$$\sum_{\substack{1 \le m \le x \\ \gcd(m,34)=1}} \rho_P(m) \ll xY.$$

5. Hooley's equidistribution

We recall our setting of the quadratic polynomial

$$P(w) = -4(68w + 2r)^2 + qy^2,$$

where $0 \le r < 34$, and we have $q > 163$ is prime, with $0 < |y| < q$.

We retain the notation $\rho_P(t)$ for the number of roots of P modulo t. The basic information that we shall use about $\rho_P(t)$ is embodied in §4.1.1, namely that we have $\rho_P(t) \le \gcd(t,y)2^{\omega(t)}$ for t coprime to 34, and $\rho_P(p^e) = \bar{\rho}_P(p)$ for $p \nmid 34y$.

Most of the argument in this section is a recapitulation of Hooley's work, and we refer to [38] for some details.

5.1. We define $S_P(h,m) = \sum_\nu \exp(2\pi i h\nu/m)$ as the sum over the roots ν of the congruence $P(\nu) \equiv 0\,(m)$. We replicate the key (yet easy) Lemma 1 of Hooley.

Lemma 5.1.1. *For any integer* h *we have*

$$\sum_{a=1}^{k} |S_P(ah,k)|^2 \le k\rho_P(k) \cdot \gcd(h,k).$$

Proof. By the definition of S_P we have

$$\sum_{a=1}^{k} |S_P(ah,k)|^2 = \sum_{a=1}^{k} \sum_{\substack{0 \le \nu,\nu' < k \\ P(\nu) \equiv P(\nu') \equiv 0\,(k)}} \sum \exp\Big(2\pi i(\nu - \nu')\frac{ah}{k}\Big).$$

Inverting the summation order and noting the a-sum is k when $h(\nu-\nu')\equiv 0\,(k)$ and zero otherwise, we get

$$\sum_{a=1}^{k}|S_P(ah,k)|^2 = k \sum\sum_{\substack{0\le\nu,\nu'<k\\ P(\nu)\equiv P(\nu')\equiv 0\,(k)\\ h(\nu-\nu')\equiv 0\,(k)}} 1 \;\le\; k \sum_{\substack{0\le\nu<k\\ P(\nu)\equiv 0\,(k)}}\;\sum_{\substack{0\le\nu'<k\\ h(\nu-\nu')\equiv 0\,(k)}} 1.$$

The latter inner sum is simply $\gcd(h,k)$, which gives the result. $\square$

5.2. For r_t with $\gcd(r_t,34)=1$, we now proceed to estimate

$$R_h(x) = R_{P,h}^{r_t}(x) = \sum_{\substack{1\le t\le x\\ t\equiv r_t\ (272)}} S_P(h,t) \;=\; \sum_{\substack{1\le t\le x\\ t\equiv r_t\ (272)}}\;\sum_{\substack{0\le\nu<t\\ P(\nu)\equiv 0\,(t)}} \exp(2\pi i h\nu/t).$$

By summing over four such arithmetic progressions we can achieve a similar result when the modulus is replaced by 68.

Lemma 5.2.1. *Suppose that* $\mathbf{Q}(\sqrt{-q})$ *has class number 1 and let* P *be as above with* $0<|y|\le Y\le(\log q)^{1/10^9}$, *and let* r_t *be given with* $\gcd(r_t,272)=1$. *Then for* $h\ne 0$ *and* $q^{1/100}\ll x\ll q^{100}$ *we have*

$$\left|R_{P,h}^{r_t}(x)\right| \ll Y\sqrt{|h|}\,\frac{x(\log\log x)^{(5-\sqrt{2})/2}}{(\log x)^{1-\sqrt{2}/2}},$$

Proof. We write $\mathbf{P}$ for the set of primes $\le X = x^{1/200\log\log x}$ and can split $t=t_1t_2$ with t_1 in the monoid $\mathbf{P}^\star$ and t_2 in the complementarily-generated monoid $\bar{\mathbf{P}}^\star$. We additionally write $\mathbf{P}_{34}$ for $\mathbf{P}$ with 2 and 17 removed. Here our assumptions that $x\gg q^{1/100}$ and $0<|y|\le Y$ ensure for large q that 2, 17, and all $p|y$ are in $\mathbf{P}$.

By a Chinese remainder theorem ([38, Lemma 3]) we factor $S_P(h,t)$ and have

$$R_h(x) = \sum_{\substack{t_1\in\mathbf{P}_{34}^\star\\ t_1t_2\le x,\, t_1t_2\equiv r_t\ (272)}}\;\sum_{t_2\in\bar{\mathbf{P}}^\star} S_P(h\bar{t}_2,t_1)S_P(h\bar{t}_1,t_2),$$

where the bars indicate reciprocal residues modulo the second argument. As with Hooley's argument, the $t_1\ge x^{1/3}$ contribute negligibly. More precisely, dropping the congruence condition on t_1t_2, since $\rho_P(t)\le\gcd(t,y)2^{\omega(t)}$ they contribute

$$\le \sum_{\substack{t_1\in\mathbf{P}_{34}^\star\\ t_1t_2\le x,\, t_1\ge x^{1/3}}}\;\sum_{t_2\in\bar{\mathbf{P}}^\star}\rho_P(t_1t_2)\le Y\sum_{\substack{t_1\in\mathbf{P}_{34}^\star\\ t_1t_2\le x,\, t_1\ge x^{1/3}}}\;\sum_{t_2\in\bar{\mathbf{P}}^\star} 2^{\omega(t_1t_2)},$$

and t_1 must either have $\ge 200(\log\log x)/6$ distinct prime factors or a square divisor exceeding $(x^{1/12})^2$. As per Hooley, a result of Hardy and Ramanujan [29] suffices to bound the contribution from the former as $\ll Yx/\log x$, while the latter's contribution is much smaller, indeed saving a factor of nearly $x^{1/12}$.

5.2.2. We then consider the t with $t_1\le x^{1/3}$, and again can readily drop the congruential t-condition, getting a contribution Σ_2 with

$$(4)\qquad \left|\Sigma_2\right| \le \sum_{\substack{t_1\in\mathbf{P}_{34}^\star\\ t_1t_2\le x,\, t_1\le x^{1/3}}}\;\sum_{t_2\in\bar{\mathbf{P}}^\star}\rho_P(t_2)\left|S_P(h\bar{t}_2,t_1)\right| = \sum_{\substack{t_1\in\mathbf{P}_{34}^\star\\ t_1\le x^{1/3}}} T(x/t_1,t_1)$$

where (for $z \geq x^{2/3}$) we have written

$$T(z,t_1) = \sum_{\substack{t_2 \in \bar{\mathbf{P}}^\star \\ t_2 \leq z}} \rho_P(t_2) \big| S_P(h\bar{t}_2, t_1) \big|.$$

By Cauchy's inequality we see that

$$T(z,t_1)^2 \leq \Bigg(\sum_{\substack{t_2 \in \bar{\mathbf{P}}^\star \\ t_2 \leq z}} \rho_P(t_2)^2 \Bigg) \Bigg(\sum_{\substack{t_2 \in \bar{\mathbf{P}}^\star \\ t_2 \leq z}} \big| S_P(h\bar{t}_2, t_1) \big|^2 \Bigg). \tag{5}$$

As noted by Hooley, the first sum can be bounded by the sparsity of t_2 via an upper-bound sieve as

$$\sum_{\substack{t_2 \in \bar{\mathbf{P}}^\star \\ t_2 \leq z}} \rho_P(t_2)^2 \leq \sum_{\substack{t_2 \in \bar{\mathbf{P}}^\star \\ t_2 \leq z}} 4^{\omega(t_2)} \ll \frac{z}{\log X} \cdot \Big(\frac{\log z}{\log X} \Big)^{4-1} \ll \frac{z (\log\log x)^4}{\log x}.$$

The second sum similarly goes by an upper-bound sieve, as we have

$$\sum_{\substack{t_2 \in \bar{\mathbf{P}}^\star \\ t_2 \leq z}} \big| S_P(h\bar{t}_2, t_1) \big|^2 = \sum_{\substack{a=1 \\ (a,t_1)=1}}^{t_1} \big| S_P(ah, t_1) \big|^2 \sum_{\substack{t_2 \leq z,\, t_2 \in \bar{\mathbf{P}}^\star \\ t_2 \equiv a\,(t_1)}} 1 \ll \frac{z/\phi(t_1)}{\log X} \sum_{\substack{a=1 \\ (a,t_1)=1}}^{t_1} \big| S_P(ah, t_1) \big|^2.$$

The remaining sum here is bounded by Lemma 5.1.1 as $\leq \rho_P(t_1) t_1 \cdot \gcd(h,t_1)$ which is crudely $\leq |h| t_1 \rho_P(t_1)$. Putting these back into (5) we find (for $h \neq 0$) that

$$\big| T(z,t_1) \big| \ll \sqrt{|h|}\, \frac{z (\log\log x)^{5/2}}{\log x} \sum_{\substack{t_1 \in \mathbf{P}^\star_{34} \\ t_1 \leq x^{1/3}}} \rho_P(t_1)^{1/2} \sqrt{\frac{t_1}{\phi(t_1)}}$$

and thus an overall bound in (4) of

$$\big| \Sigma_2 \big| \ll \sqrt{|h|}\, \frac{x (\log\log x)^{5/2}}{\log x} \sum_{\substack{t_1 \in \mathbf{P}^\star_{34} \\ t_1 \leq x^{1/3}}} \frac{\rho_P(t_1)^{1/2}}{\sqrt{t_1 \phi(t_1)}}.$$

5.2.3. We can note that there is no q-dependence in the above bound yet. Indeed, this only comes into play when we show there are not too many small primes p with $\rho_P(p) = 2$, which we shall obtain from our class number 1 hypothesis combined with standard results about the distribution of primes modulo 4, essentially relating the natural field $\mathbf{Q}(\sqrt{q})$ for the form P to our imaginary quadratic field $\mathbf{Q}(\sqrt{-q})$ via twisting by the Dirichlet character of conductor 4.

We can slightly improve Hooley's argument to save an additional log-log power, writing Σ_7 for the above t_1-sum and noting that

$$\Sigma_7 = \sum_{\substack{t_1 \in \mathbf{P}^\star_{34} \\ t_1 \leq x^{1/3}}} \frac{\rho_P(t_1)^{1/2}}{\sqrt{t_1 \phi(t_1)}} \leq \prod_{\substack{p \leq X \\ p \notin \{2,17\}}} \left(1 + \Big(1 - \frac{1}{p} \Big)^{-1} \sum_{e=1}^{\infty} \frac{\rho_P(p^e)^{1/2}}{p^e} \right),$$

whereas Hooley here takes $p \leq x$.

We then take the logarithm of the right side, bounding it as

$$\leq \sum_{\substack{p\leq X\\ p\nmid 34y}} \Bigl(1-\frac{1}{p}\Bigr)^{-2}\frac{\sqrt{\rho_P(p)}}{p} + \sum_{p|y}\frac{O(1)}{\sqrt{p}} + O(1) \leq \sum_{\substack{p\leq X\\ \bar\rho_P(p)=2}} \frac{\sqrt{2}}{p} + O\bigl(\sqrt{\log Y}\bigr).$$

Since $\mathbf{Q}(\sqrt{-q})$ has class number 1 and $X\leq q/4$ (from $x\ll q^{100}$), the primes $p\leq X$ with $\bar\rho_P(p)=2$ are precisely those congruent to 3 mod 4. By standard results about primes in arithmetic progressions [44] we thus have

$$\sum_{\substack{p\leq X\\ \bar\rho(p)=2}} \frac{\sqrt{2}}{p} = \frac{\sqrt{2}}{2}\sum_{\substack{p\leq X\\ p\equiv 3(4)}}\frac{2}{p} = \frac{\sqrt{2}}{2}\log\log X + O(1).$$

Re-exponentiating (crudely in Y) gives $\Sigma_7 \ll Y(\log X)^{\sqrt{2}/2}$, so that

$$\bigl|\Sigma_2\bigr| \ll Y\sqrt{|h|}\,\frac{x(\log\log x)^{(5-\sqrt{2})/2}}{(\log x)^{1-\sqrt{2}/2}},$$

which is the desired result. □

Remark. We have already remarked above that Hooley's earlier work [37] for quadratic congruences is inapplicable in our context, due to a lack of suitable uniformity in the polynomial discriminant (which is of size qy^2).

We can also comment on spectral theory methods that obtain a power-savings, notably work of Duke, Friedlander, and Iwaniec [22] in the case of negative discriminant (inspired by Bykovskii [11], and alternatively presented in [41, §21.4ff]), and Tóth [73] for our case of positive discriminant.[10] It is not readily apparent to me what the uniformity in the discriminant is, but in the negative discriminant case the class number appears, while in Tóth's work (cf. Lemma 4.2) the fundamental unit also presumably plays a rôle (similar to its effect on Hooley's result).

There is also a result of Hejhal [36, (7.25)] regarding the congruence $w^2\equiv A$ to varying moduli, where a power-savings is similarly obtained (by spectral methods) for positive odd fundamental discriminants A of the form u^2-4 with class number 1 (said set is finite by Siegel's ineffective theorem [58], and includes $\{5,21,77,437\}$).

6. Goldfeld's argument

Let f be the weight 2 modular form of level $N=2^6 17^2$ corresponding to the elliptic curve $Y^2=X^3-34^2X$. By a modular symbols calculation (e.g. [13, §2.8]) we find that its L-function $L_f(s)$ has a double zero at its central point $s=1$.

Remark. As this curve has complex multiplication, the modular correspondence already follows from (say) Deuring's work [17], independently of Wiles and his school. Indeed, we could simply drop all reference to the elliptic curve.

Remark. The modular symbols calculation can proceed via twisting level 32 by 34 (or 64 by 17) if desired, rather than working directly at level 18496. (Another method to show the L-function vanishing, which I hesitate to mention due to its difficulty – indeed, comparable to the Gross-Zagier height formula in generality, would be via Waldspurger's work [74] and the associated weight 3/2 Shintani lift).

[10] The principal statements in [22, 73] are made for what corresponds to our case of $r_t=0$, but as characters are apparent in the proofs, one can generalize to nonzero residue classes.

6.1. We let θ be a primitive real character of conductor 136 (there are two, and it does not matter which we choose, as they differ for l that are 3 mod 4, for which we have $c_l = 0$ anyway). Recalling that the modular cuspidal eigenform of level 32 can be written (see [40, §8.4] for instance) as a $\mathbf{q}$-series as

$$\sum_{a=-\infty}^{\infty} \sum_{b=-\infty}^{\infty} (4a+1)(-1)^b \mathbf{q}^{(4a+1)^2+(2b)^2},$$

upon taking the 34th quadratic twist the lth Dirichlet series coefficient of $L_f(s)$ is

$$c_l = \theta(l) \sum_{\substack{a=-\infty \\ (4a+1)^2+(2b)^2=l}}^{\infty} \sum_{b=-\infty}^{\infty} (4a+1)(-1)^b.$$

We have $|c_p| \le 2\sqrt{p}$ as $(4a+1)^2 + (2b)^2 = p$ has at most 2 solutions [23, Prop. VII]. We can also note that $c_l = 0$ for all l which are not 1 mod 4.

By either Hecke's theory of Grössencharacter L-functions [31] or his theory of modular form L-functions [32], we have

$$L_f(s) = \sum_{l=1}^{\infty} \frac{c_l}{l^s} = \prod_p \Bigl(1 - \frac{\alpha_p}{p^s}\Bigr)^{-1} \Bigl(1 - \frac{\beta_p}{p^s}\Bigr)^{-1}$$

where $\alpha_p \beta_p = p$ for $p \notin \{2, 17\}$. We have $c_p = \alpha_p + \beta_p$, so $|c_p| \le 2\sqrt{p}$ says $\beta_p = \bar{\alpha}_p$, and thus $|\alpha_p| = \sqrt{p}$. We also have $c_2 = c_{17} = \alpha_2 = \alpha_{17} = \beta_2 = \beta_{17} = 0$.

6.2. We assume that $K = \mathbf{Q}(\sqrt{-q})$ has class number 1 where $-q$ is a fundamental discriminant with $q > 163$. Recalling §3, by the theory of genera of Gauss we know q is prime. In particular, we have $\gcd(q, N) = 1$. We let χ be the quadratic character corresponding to K, so that $\chi(p) = -1$ for all primes $p \le q/4$.

Writing $\Lambda_f(s) = L_f(s)\Gamma(s)(\sqrt{N}/2\pi)^{s-1}$ and similarly for the completed twisted L-function $\Lambda_{f\chi}(s)$, the central vanishing of $L_f(s)$ then implies by Cauchy's integral theorem that

$$0 = \Bigl(\int_{(2)} - \int_{(0)}\Bigr) \Lambda_f(s)\Lambda_{f\chi}(s) \frac{\partial s/2\pi i}{(s-1)^2}.$$

By [1, §6] the twist of f by χ has level $q^2 N$ and root number $\chi(-N) = \chi(-1) = -1$ (see [77, Satz 2] or the last statement of [1, Theorem 6]), so that the integral on the 0-line is the additive inverse of that on the 2-line by the functional equations(s) for $\Lambda_f(s)\Lambda_{f\chi}(s)$ relating $s \leftrightarrow 2 - s$, and we have

$$0 = \int_{(2)} \Lambda_f(s)\Lambda_{f\chi}(s) \frac{\partial s/2\pi i}{(s-1)^2} = \int_{(2)} L_f(s)L_{f\chi}(s)\Gamma(s)^2 \Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1} \frac{\partial s/2\pi i}{(s-1)^2}.$$

6.2.1. Following Oesterlé [52], we next define

$$\Psi_f(s) = L_f(s)L_{f\lambda}(s) \quad\text{and}\quad G_f(s) = \frac{L_{f\chi}(s)}{L_{f\lambda}(s)} \tag{6}$$

where λ is the Liouville function, which is completely multiplicative and -1 on all primes. Hence

$$L_{f\lambda}(s) = \prod_p \Bigl(1 + \frac{\alpha_p}{p^s}\Bigr)^{-1} \Bigl(1 + \frac{\bar{\alpha}_p}{p^s}\Bigr)^{-1} \quad\text{so that}\quad \Psi_f(s) = \prod_p \Bigl(1 - \frac{\alpha_p^2}{p^{2s}}\Bigr)^{-1} \Bigl(1 - \frac{\bar{\alpha}_p^2}{p^{2s}}\Bigr)^{-1}$$

is naturally a function of $2s$, and up to bad Euler factors at $p \in \{2, 17\}$ it is in fact equal to $L_{S^2f}(2s)/L_{A^2f}(2s)$ where S^2f and A^2f are respectively the symmetric and alternating squares of f (at the level of motivic L-functions), where moreover $L_{A^2f}(2s) = \zeta(2s-1)$ has a pole at $s = 1$.

More specifically, the motivic symmetric-square L-function $L_{S^2f}(s)$ here is

$$L_{S^2f}(s) = \prod_p \Bigl(1 - \frac{\tilde{\alpha}_p^2}{p^s}\Bigr)^{-1}\Bigl(1 - \frac{\tilde{\alpha}_p\bar{\tilde{\alpha}}_p}{p^s}\Bigr)^{-1}\Bigl(1 - \frac{\bar{\tilde{\alpha}}_p^2}{p^s}\Bigr)^{-1}$$

with $\tilde{\alpha}_p = \alpha_p$ for all p except $p = 17$, where instead we have $\tilde{\alpha}_{17} = 1 + 4i$ (co-opting this from the twisted modular form of level 32). Since $\tilde{\alpha}_p\bar{\tilde{\alpha}}_p = p$ for all $p \neq 2$, the middle term corresponds to the Riemann ζ-function, and we find that

$$\Psi_f(s) = \frac{L_{S^2f}(2s)}{\zeta(2s-1)} \cdot \Bigl(1 - \frac{2}{2^{2s}}\Bigr)^{-1}\Bigl(1 + \frac{30}{17^{2s}} + \frac{17^2}{17^{4s}}\Bigr),$$

where we shall notate the contribution from the exceptional Euler factors by $B_f(2s)$.

6.2.2. We define $\tilde{G}_f(s) = G_f(s) - 1$ and write g_l for the Dirichlet series coefficients of $G_f(s)$, so that by the above Euler quotient $G_f(s) = L_{f\chi}(s)/L_{f\lambda}(s)$ we have

$$G_f(s) = \sum_{l=1}^{\infty} \frac{g_l}{l^s} = 1 + \tilde{G}_f(s) = \Bigl(1 + \frac{\alpha_q}{q^s}\Bigr)\Bigl(1 + \frac{\bar{\alpha}_q}{q^s}\Bigr) \prod_{p:\chi(p)=+1} \frac{(1 + \alpha_p/p^s)(1 + \bar{\alpha}_p/p^s)}{(1 - \alpha_p/p^s)(1 - \bar{\alpha}_p/p^s)}.$$

We see that $g_l = 0$ unless all $p|l$ have $\chi(p) \neq -1$, and thus in the context of class number 1 we have $g_l = 0$ for $1 < l \leq q/4$. For p prime with $\chi(p) = +1$ we have that $g_p = 2(\alpha_p + \bar{\alpha}_p) = 2c_p$, while $c_q = g_q = 0$ since q is 3 mod 4. We also note that $|g_{p^v}| \leq 4vp^{v/2}$ as follows from $|\alpha_p| \leq \sqrt{p}$ and $[(1+x)/(1-x)]^2 = 1 + \sum_n 4nx^n$.

6.2.3. From $L_f(s)L_{f\chi}(s) = \Psi_f(s)G_f(s)$ and $G_f(s) = 1 + \tilde{G}_f(s)$ we have

$$\begin{aligned} 0 &= \int_{(2)} \Psi_f(s)G_f(s)\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1} \frac{\partial s/2\pi i}{(s-1)^2} \\ &= \int_{(2)} \Psi_f(s)\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1} \frac{\partial s/2\pi i}{(s-1)^2} + \int_{(2)} \Psi_f(s)\tilde{G}_f(s)\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1} \frac{\partial s/2\pi i}{(s-1)^2}. \end{aligned}$$

The first integral is estimated by moving the path of integration to the left and using Cauchy's residue theorem, with the decay from q^s dominating the error. Via the standard zero-free region [44] and estimates for ζ (here for $|t| \ll \log q$, as the vertical decay of $\Gamma(s)^2$ suffices otherwise), and analytic properties of the symmetric-square L-function we get

$$\begin{aligned} \int_{(2)} \Psi_f(s)\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1} \frac{\partial s/2\pi i}{(s-1)^2} &= \int_{(2)} \frac{B_f(2s)L_{S^2f}(2s)}{\zeta(2s-1)}\Gamma(s)^2\Bigl(\frac{Nq}{4\pi^2}\Bigr)^{s-1} \frac{\partial s/2\pi i}{(s-1)^2} \\ &= 2B_f(2)L_{S^2f}(2) + O(1/q^{1/100 \log\log q}) \gg 1. \end{aligned}$$

In fact, in this CM case we have $L_{S^2f}(s) = L_{\eta_{-4}}(s-1)L_{\psi_\star^2}(s)$ where ψ is the Hecke Grössencharacter corresponding to the elliptic curve isogeny class of conductor 32. Thus the analytic properties of the symmetric-square are immediate (see [31], or [57] in general) and in any case we can compute $L_{S^2f}(2) \approx 0.674969789$.

6.3. We are thus left to estimate

$$\frac{4\pi^2}{Nq}\int_{(2)}\Psi_f(s)\tilde{G}_f(s)\Gamma(s)^2\Big(\frac{Nq}{4\pi^2}\Big)^s\frac{\partial s/2\pi i}{(s-1)^2}=\frac{4\pi^2}{Nq}E,$$

and wish to show that E is asymptotically dominated by q as $q\to\infty$.

With $\Psi_f(s)=\sum_k \xi_k/k^{2s}$ and $\tilde{G}_f(s)=-1+\sum_l g_l/l^s$ we then expand out the above integral E as a Mellin transform to get

$$E=\sum_{k=1}^{\infty}\xi_k\sum_{l>1}g_lW\Big(\frac{4\pi^2k^2l}{Nq}\Big)$$

where

$$W(z)=\int_{(2)}z^{-s}\,\Gamma(s)^2\frac{\partial s/2\pi i}{(s-1)^2}=\int_{(2)}z^{-s-1}\,\Gamma(s)^2\frac{\partial s}{2\pi i}.$$

To determine the decay rate of W one can either note that $W(z)=2K_0(2\sqrt{z})/z$ (by Mellin convolution of e^{-z} with itself) and use known bounds for K-Bessel functions, or work directly (e.g. [8]) by noting the quotient of $\sqrt{2\pi}\,\Gamma(2s-1/2)/2^{2s-1}$ by $\Gamma(s)^2$ tends to 1 uniformly as $|s|\to\infty$ away from the negative real axis, so that changing variables $2s-1/2\to s$ gives $W(z)\sim\sqrt{\pi}/z^{5/4}e^{2\sqrt{z}}\ll e^{-\sqrt{z}}$. Also, $l\geq q/4$ implies $4\pi^2k^2l/Nq\geq 1/1875$, so W and W' are absolutely bounded for l we consider. Although it's unneeded, the convolution interpretation shows W is positive.

6.3.1. The Dirichlet series $\tilde{G}_f(s)$ is not directly in a form where we can easily detect cancellation of the coefficients, and we shall make some modifications to ameliorate our efforts. What we wish to do is replace

$$\sum_{k=1}^{\infty}\xi_k\sum_{l>1}\frac{g_l}{(k^2l)^s}\qquad\text{by}\qquad\sum_{k=1}^{\infty}\tilde{\xi}_k\sum_{n=1}^{\infty}\frac{c_n\tilde{R}_\chi(n)}{(k^2n)^s}$$

where $\tilde{R}_\chi(n)$ counts representations of n by the principal form $x^2+xy+\frac{q+1}{4}y^2$ with $y\geq 1$. We similarly notate by $\tilde{R}^\star_\chi(n)$ the number of primitive such representations with $\gcd(x,y)=1$. This resulting inner sum over n is more suitable for showing cancellation by our methods.

From above we have $g_p=2c_p=\tilde{R}^\star_\chi(p)c_p$ for p with $\chi(p)\neq -1$. The nonprime l with $g_l\neq 0$ or $\tilde{R}^\star_\chi(l)\neq 0$ have $l\geq (q/4)^2$ and thus contribute negligibly due to the W-decay (by crude estimates $|\xi_k|\leq k\tau_2(k)$ and $|g_l|,|c_l\tilde{R}^\star_\chi(l)|\leq\tau_2(l)^2\sqrt{l}$), giving

$$E=\sum_{k=1}^{\infty}\xi_k\sum_{l>1}g_lW\Big(\frac{4\pi^2k^2l}{Nq}\Big)=\sum_{k=1}^{\infty}\xi_k\sum_{l=1}^{\infty}c_l\tilde{R}^\star_\chi(l)W\Big(\frac{4\pi^2k^2l}{Nq}\Big)+O(1/q^{99}).$$

Remark. In fact, we have $g_l=c_l\prod_{p|l}[1+\chi(p)]=c_l\tilde{R}^\star_\chi(l)$ for squarefree $l>1$.

6.3.2. We then write

$$\begin{aligned}\sum_{k=1}^{\infty}\frac{\xi_k}{k^{2s}}\sum_{l=1}^{\infty}\frac{c_l\tilde{R}^\star_\chi(l)}{l^s}&=\sum_{j=1}^{\infty}\frac{\xi_j}{j^{2s}}\Big(\sum_{m=1}^{\infty}\frac{c_{m^2}}{m^{2s}}\Big)^{-1}\cdot\sum_{m=1}^{\infty}\frac{c_{m^2}}{m^{2s}}\sum_{l=1}^{\infty}\frac{c_l\tilde{R}^\star_\chi(l)}{l^s}\\&=\sum_{k=1}^{\infty}\frac{\tilde{\xi}_k}{k^{2s}}\cdot\sum_{m=1}^{\infty}\frac{c_{m^2}}{m^{2s}}\sum_{l=1}^{\infty}\frac{c_l\tilde{R}^\star_\chi(l)}{l^s}\end{aligned}$$

where we have

$$\sum_{k=1}^{\infty}\frac{\tilde{\xi}_k}{k^{2s}}=\prod_p\biggl(\sum_{v=0}^{\infty}\sum_{e=0}^{v}\frac{\alpha_p^{2e}\bar{\alpha}_p^{2v-2e}}{p^{2vs}}\biggr)\biggl(\sum_{v=0}^{\infty}\sum_{e=0}^{2v}\frac{\alpha_p^{a}\bar{\alpha}_p^{2v-e}}{p^{2vs}}\biggr)^{-1}.$$

We can then bound the p^{2u}-coefficient of the reciprocated Dirichlet series by noting that $1/(1-3z-5z^2-7z^3+\ldots)=1/F(z)$ has its uth coefficient bounded by λ^u where $1/\lambda\approx 0.2192$ satisfies $F(1/\lambda)=0$, so that

$$|\tilde{\xi}_{p^w}|\le\sum_{i=0}^{w}(i+1)p^i\cdot\lambda^{w-i}p^{w-i}\le(\lambda+2)^w p^w\le 7^w p^w\le p^{4w},$$

implying $|\tilde{\xi}_k|\le k^4$ by multiplicativity (this can be improved, but we do not bother).

This Dirichlet series replacement gives us

$$E=\sum_{k=1}^{\infty}\tilde{\xi}_k\sum_{l=1}^{\infty}c_l\tilde{R}^{\star}_{\chi}(l)\sum_{m=1}^{\infty}c_{m^2}W\Bigl(\frac{4\pi^2k^2lm^2}{Nq}\Bigr)+O(1/q^{99}),$$

where the contributing m with $\gcd(l,m)\neq 1$ have $lm^2\ge(q/4)^3$ and thus are negligible by W-decay. So we can replace $c_lc_{m^2}=c_{lm^2}$, and since $\tilde{R}^{\star}_{\chi}(l)=\tilde{R}_{\chi}(lm^2)$ for $m\le q/4$, inserting this and putting $n=lm^2$ gives the desired re-arrangement

$$E=\sum_{k=1}^{\infty}\tilde{\xi}_k\sum_{n=1}^{\infty}c_n\tilde{R}_{\chi}(n)W\Bigl(\frac{4\pi^2k^2n}{Nq}\Bigr)+O(1/q^{99}).$$

Moreover, using $|c_n|\le\sqrt{n}\tau_2(n)$ and the easy bound (e.g. from lattice points in an ellipse) that the summation of $\tilde{R}_{\chi}(n)$ up to x is $\ll x/\sqrt{q}$, we can curtail the k-sum at $K=(\log q)^{1/10^9}$ by W-decay, with an error that is $\ll qe^{-K/100}\ll q/(\log q)^{999}$.

Remark. An alternative schema for this section appears in [76, §3], which notes that $L_f(s)L_{f\chi}(s)=\tilde{B}_f(s)L_{\chi}(2s-1)\sum_l c_lR_{\chi}(l)/l^s$ for some bad Euler factors $\tilde{B}_f(s)$, and then approximates $L_{\chi}(2s-1)$ by $\zeta(4s-2)/\zeta(2s-1)$.

7. Estimation of the error term

We are left to estimate the sum

$$E_1=\sum_{k\le K}\tilde{\xi}_k\sum_{l=1}^{\infty}c_l\tilde{R}_{\chi}(l)W\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr)$$

where c_l is the lth Dirichlet series coefficient of $L_f(s)$ and $\tilde{R}_{\chi}(l)$ is the number of representations of l by the form $x^2+xy+\frac{q+1}{4}y^2$ with $y\ge 1$, while $|\tilde{\xi}_k|\le k^4$ and $K=(\log q)^{1/10^9}$, and $W(z)=2K_0(2\sqrt{z})/z$ has rapid decay $\ll e^{-\sqrt{z}}$ as $z\to\infty$.

We wish to show that E_1 is negligible compared to q, as by the computation of §6.2.3 this will contradict the assumption of class number 1.

7.1. As in §6.1 we have

$$c_l=\theta(l)\sum_{a=-\infty}^{\infty}\sum_{\substack{b=-\infty\\(4a+1)^2+(2b)^2=l}}^{\infty}(4a+1)(-1)^b,$$

and thus want to bound $\sum_k k^4|E_1^k|$ for $k \le K$, where (with l merely as a shorthand)

$$E_1^k = \sum_{\substack{a=-\infty \\ l=(4a+1)^2+(2b)^2}}^{\infty} \sum_{b=-\infty}^{\infty} \tilde{R}_\chi(l)(4a+1)(-1)^b\theta(l)W\Big(\frac{4\pi^2k^2l}{Nq}\Big).$$

7.1.1. We then consider $l = x^2 + xy + \frac{q+1}{4}y^2$ with $y \ge 1$. By rearrangement this says $4l = (2x+y)^2 + qy^2$, and so by the accounting of $\tilde{R}_\chi(l)$ we thus find

$$E_1^k = \sum_{y=1}^{\infty} \sum_{\substack{x \\ l=(4a+1)^2+(2b)^2 \\ 4l=(2x+y)^2+qy^2}} \sum_{a} \sum_{b} (4a+1)(-1)^b\theta(l)\,W\Big(\frac{4\pi^2k^2l}{Nq}\Big).$$

7.1.2. Equating the above conditions on l implies that

$$4(4a+1)^2 - (2x+y)^2 = -4(2b)^2 + qy^2.$$

It is a feature of working with the principal form that the left side factors in a particular nice way as tu with

$$t = 2(4a+1) + (2x+y), \;\; u = 2(4a+1) - (2x+y).$$

(In general we can achieve a similar factorization for any form in the principal genus, though the resulting uniformity is unclear). We thus have $tu = -4(2b)^2 + qy^2$ and

$$2(4a+1) = (t+u)/2, \;\; 2x+y = (t-u)/2. \tag{7}$$

Moreover we have

$$4l = \frac{(t-u)^2}{4} + qy^2, \;\; l = \frac{(t+u)^2}{16} + (2b)^2.$$

7.2. We now switch variables from (a,x) to (t,u). We wish to determine whether a given (t,u) yields an *integral* (a,x)-pair, which are 2-adic conditions by (7).

Firstly, we can note that l must be 1 mod 4 by $l = (4a+1)^2 + (2b)^2$. On the other hand, for $l = x^2 + xy + \frac{q+1}{4}y^2$ we see that $y \equiv 2\,(4)$ give l that are 3 mod 4 for odd x and even l for even x. Similarly, when $4|y$ the even x yield even l.

7.2.1. For odd y, since q is 3 mod 8 we have

$$tu = -4(2b)^2 + qy^2 \equiv qy^2 \equiv 3, 11 \pmod{16},$$

so in particular $t - u \equiv 2$ (4), implying that the condition $2x + y = (t-u)/2$ gives an integral x since y is odd.

In dealing with a, when $qy^2 \equiv 3$ (16) we see that $t \equiv 1, 3, 9, 11$ (16) determines $u \equiv 3, 1, 11, 9$ (16), so $(4a+1) = (t+u)/4$ gives an integral a from $t + u \equiv 4$ (16). On the other hand, the other t yield a nonintegral a by the same calculation, and so we ignore these t. For $qy^2 \equiv 11$ (16) the situation is similar, with the residue classes $t \equiv 5, 15, 7, 13$ (16) being those that yield integral a.

Thus for odd y there is a set of residue classes modulo 16 (depending on y) for t corresponding exactly to integral values of a, while x is always integral.

7.2.2. When $4|y$, the analysis is only slightly more complicated. We have x is odd, so that $(t-u) = 2(2x+y) \equiv 4\,(8)$. On the other hand, $(t+u) = 4(4a+1) \equiv 4\,(16)$ and thus one of t, u is 0 mod 8 and the other is 4 mod 8. By symmetry, we can assume t is the latter. In particular, we find that $(t/4)(u/4) = -b^2 + q(y/4)^2$ must be even, so that b and $y/4$ must have the same parity. When these are both odd, we find that $(t/4)(u/4) \equiv 2\,(8)$, implying $8\|u$ so that $u/4 \equiv 2\,(4)$ whence $t \equiv 12\,(16)$ to ensure integrality of a. Similarly, when b and $y/4$ are both even we have $4|(u/4)$ and so $t \equiv 4\,(16)$.

As a result of the above integrality considerations, with $2b = 4\tilde{b} + 2r_b$ we have

$$E_1^k = \sum_{y=1}^{\infty}\sum_{r_b=1}^{2}\sum_{r_t=1}^{16} z_2(y,r_b,r_t) \sum_{\substack{t\equiv r_t\ (16)\\ tu=-4(4\tilde{b}+2r_b)^2+qy^2}} \sum_{u}\sum_{\tilde{b}} \frac{t+u}{4}(-1)^{r_b}\theta(l)\, W\Big(\frac{4\pi^2k^2l}{Nq}\Big)$$

where

- $z_2(y,r_b,r_t) = 0$ when y is odd with $qy^2 \equiv 3\,(16)$ and $r_t \notin \{1,3,9,11\}$,
- $z_2(y,r_b,r_t) = 0$ when y is odd with $qy^2 \equiv 11\,(16)$ and $r_t \notin \{5,15,7,13\}$,
- $z_2(y,r_b,r_t) = 1$ when $qy^2 \equiv 3\,(16)$ and $r_t \in \{1,3,9,11\}$,
- $z_2(y,r_b,r_t) = 1$ when $qy^2 \equiv 11\,(16)$ and $r_t \in \{5,15,7,13\}$,
- $z_2(y,r_b,r_t) = 0$ when $y \equiv 2\,(4)$,
- $z_2(y,r_b,r_t) = 0$ when $4|y$ and r_b and $y/4$ have differing parity,
- $z_2(y,r_b,r_t) = 0$ when $4|y$ and r_b and $y/4$ are odd and $r_t \neq 12$,
- $z_2(y,r_b,r_t) = 2$ when $4|y$ and r_b and $y/4$ are odd and $r_t = 12$,
- $z_2(y,r_b,r_t) = 0$ when $4|y$ and r_b and $y/4$ are even and $r_t \neq 4$,
- $z_2(y,r_b,r_t) = 2$ when $4|y$ and r_b and $y/4$ are even and $r_t = 4$.

We could combine some of the congruence classes when y is odd via the t-u symmetry (thereby doubling z_2), but choose not to do so.

7.3. Next we need to consider the effect of $\theta(l)$, which induces an additional analysis at the prime 17. We can assume the residue class $2r_b$ mod 68 of $2b$ is fixed.

7.3.1. We consider the effect of fixing t modulo 17. When $\gcd(t,17) = 1$ this determines u mod 17 by the relation $tu \equiv -4(2r_b)^2 + qy^2$ (17), and thus also a mod 17 from $(t+u)/4 = 4a+1$. Writing r_a for this residue class, the character contribution $\theta((4a+1)^2 + (2r_b)^2)$ is thereby fixed, since $(4a+1)^2 \equiv (4r_a+1)^2$ (136).

Similarly to the analysis with $4|y$, when $17|t$ we can essentially switch t and u. Indeed, we note that $-4(2b)^2 + qy^2 \equiv 0$ (17) has no solutions other than the "trivial" solution $(b,y) \equiv (0,0)$ (17), due to the fact that q is non-square modulo 17 (using that $-q$ is a non-square by our class number 1 assumption, and exploiting quadratic reciprocity since 17 is 1 mod 4).

This allows us to note that 17 divides at most one of t and u, or else the character evaluation is zero. Indeed, when $17|tu$ we have $17|b$, and so if $17|t$ and $17|u$ then $17|(4a+1)$, so that $\theta((4a+1)^2 + (2b)^2) = 0$ as the argument is divisible by 17.

Therefore, the contribution from $17|t$ is just the contribution from $17|r_b$ and $17|y$ when running over u-classes coprime to 17.

We then get

$$E_1^k = \sum_{y=1}^{\infty}\sum_{r_b=1}^{34}\sum_{r_t=1}^{272} z(y,r_b,r_t) \sum_{\substack{t\equiv r_t\ (16\cdot 17)\\ tu=-4(68\tilde{b}+2r_b)^2+qy^2}} \sum_{u}\sum_{\tilde{b}} \frac{t+u}{4}\, W\Big(\frac{4\pi^2k^2l}{Nq}\Big)$$

where $z(y, r_b, r_t) = z_2(y, r_b, r_t \bmod 16) \cdot z_{17}(y, r_b, r_t) \cdot \tilde{\theta}(y, r_b, r_t)$ and

- $z_{17}(y, r_b, r_t) = 0$ when $17 | r_t$,
- $z_{17}(y, r_b, r_t) = 2$ when $17 \nmid r_t$, $17 | r_b$, and $17 | y$,
- $z_{17}(y, r_b, r_t) = 1$ otherwise,

with

$$\tilde{\theta}(y, r_b, r_t) = (-1)^{r_b} \theta\big((r_t + u)^2/16 + (2r_b)^2\big)$$

where u is determined by the congruence $r_t u \equiv -4(2r_b)^2 + qy^2 \,(2 \cdot 272)$ (here the extra 2-power is necessary when $4 \| r_t$ (so $4|y$) to ensure $8|u$).

7.4. We can now write the free u-sum as a congruence modulo t; it is also slightly nicer to remove factors of 4 when $4|y$ (so $4\|r_t$) so that for $i \in \{1, 2\}$ we consider

$$E_1^{k,i} = \sum_{y \in Y_i} \sum_{r_b=1}^{34} \sum_{r_t=1}^{M_i} z(y, r_b, m_i r_t) \sum_{\substack{t \equiv r_t \,(M_i) \\ P(\tilde{b})/m_i \equiv 0 \,(t)}} \sum_{\tilde{b}} \frac{m_i t + u}{4} W\Big(\frac{4\pi^2 k^2 l}{Nq}\Big)$$

where Y_1 is the odd positive integers and Y_2 is the positive multiples of 4. Meanwhile, we have $(M_1, M_2) = (272, 68)$ and $(m_1, m_2) = (1, 4)$, while the quadratic polynomial is $P(w) = -4(68w + 2r_b)^2 + qy^2$ and u and l are implicitly defined by

$$m_i t u = -4(68\tilde{b} + 2r_b)^2 + qy^2 \tag{8}$$

and

$$4l = \frac{(m_i t - u)^2}{4} + qy^2, \;\; l = \frac{(m_i t + u)^2}{16} + (68\tilde{b} + 2r_b)^2. \tag{9}$$

Note that $\gcd(r_t, M_i) = \gcd(r_t, 34) = \gcd(t, 34) = 1$ for all r_t with nonzero z-value. In particular, we can remove the denominator m_i in the congruence $P(\tilde{b})/m_i \equiv 0\,(t)$.

7.4.1. We proceed to eliminate the $y > K = (\log q)^{1/10^9}$ by W-decay via the first expression in (9). For this, we first consider $y \gg (\log q)^2$, where the W-decay of $W(z) \ll e^{-\sqrt{z}}$ is so strong that we can simply ignore the $P(\tilde{b}) \equiv 0\,(t)$ condition and sum over all $(y, t, \tilde{b})$, getting a sufficient bound. Indeed, the same argument works when any of $|\tilde{b}|, |t|, |u| \gg \sqrt{q}(\log q)^2$, as each implies $l \gg q(\log q)^4$. To handle the remaining terms, we use the bounds $W(\cdot) \ll e^{-K/100}$ and $\rho_P(t) \le y 2^{\omega(t)}$ for an overall error in E_1 of

$$\ll K^5 \cdot (\log q)^2 \cdot \frac{\sqrt{q}(\log q)^2}{e^{K/100}} \sum_{\substack{|t| \ll \sqrt{q}(\log q)^2 \\ \gcd(t,34)=1}} \rho_P(t) \frac{\sqrt{q}(\log q)^2}{|t|} \ll \frac{q}{(\log q)^{999}}.$$

7.4.2. For future reference, we can similarly note there is negligible contribution when any of $|t|, |u|, |\tilde{b}| \ge \sqrt{q}K$. Indeed by the above l-expressions (9) each implies that $l \ge qK^2/16$, while we already saw that when one of $|\tilde{b}|, |t|, |u| \gg \sqrt{q}(\log q)^2$ there is negligible contribution, and so as before we get a bound in E_1 of

$$\ll K^5 \cdot K \cdot \frac{\sqrt{q}(\log q)^2}{e^{K/400}} \cdot \sum_{\substack{|t| \ll \sqrt{q}(\log q)^2 \\ \gcd(t,34)=1}} \rho_P(t) \frac{\sqrt{q}(\log q)^2}{|t|} \ll \frac{q}{(\log q)^{999}}.$$

7.5. We are thus left to estimate

$$E_2 = \sum_{k\le K} k^4 \Bigl|\sum_{i=1}^{2}\sum_{\substack{y\le K\\ y\in Y_i}}\sum_{r_b=1}^{34}\sum_{r_t=1}^{M_i} z(y,r_b,m_ir_t)\sum_{\substack{t\equiv r_t\,(M_i)\\ P(\tilde b)\equiv 0\,(t)}}\sum_{\tilde b}\frac{m_it+u}{4}\,W\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr)\Bigr|.$$

Letting $S=(\log q)^{1/100}$ we first show that the small $|t|\ll\sqrt{q}/S^{1/5}$ (say) give a negligible contribution. From §7.4.2 we need only consider $|u|\ll\sqrt{q}K$. By (8) we must have one of $|\tilde b\pm\sqrt{q}y/136|\ll|tu|/\sqrt{q}y$, and so when $|u|\ll\sqrt{q}K$ this restricts $\tilde b$ to relatively small intervals of size $\ll|t|K/y$. The number of $\tilde b$'s is thus bounded as $\ll K\rho_P(t)$ so the contribution to the inner double sum above in E_2 is

$$\ll\sqrt{q}K\cdot\sum_{\substack{|t|\ll\sqrt{q}/S^{1/5}\\ \gcd(t,34)=1}} K\rho_P(t)\ll\sqrt{q}K^3\frac{\sqrt{q}}{S^{1/5}},$$

where we changed the t-congruence condition modulo M_i to a coprimality restriction, and used $W(\cdot)\ll 1$ and Corollary 4.2.3 with $Y=K$. We can then sum over the "fixed" parameters (k,i,y,r_b,r_t) which gives an extra factor of $\ll K^6$ in E_2. This is sufficiently small since $K=(\log q)^{1/10^9}$, and indeed with the choice of S above, this will essentially be the largest of our error contributions (up to K-factors).

7.6. Next we split the t into intervals of size $\sqrt{q}/S$ centered at $T_j=j\sqrt{q}/S$, and proceed to estimate for $S^{4/5}\ll|j|\ll SK$ the double sum

$$B_2^j=B_2^j(k,i,y,r_b,r_t)=\sum_{\substack{|t-T_j|<\sqrt{q}/2S\\ t\equiv r_t\,(M_i)}}\ \sum_{\substack{\tilde b\\ P(\tilde b)\equiv 0\,(t)}}\frac{m_it+u}{4}\,W\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr).$$

We make a smooth partition of unity of size S with $\sum_s F_s(z)\equiv 1$ for all z. Here[11] we index $0\le s\le S-1$, and have each F_s as nonnegative with period 1, with periodic support contained in an interval of length $2/S$ that is centered at s/S. Furthermore, the nth derivatives are bounded by $|F_s^{(n)}(z)|\ll_n S^n$. This gives

$$B_2^j=\sum_{\substack{|t-T_j|<\sqrt{q}/2S\\ t\equiv r_t\,(M_i)}}\ \sum_{\substack{\tilde b\\ P(\tilde b)\equiv 0\,(t)}}\ \sum_{s=0}^{S-1}F_s(\tilde b/|t|)\,\frac{m_it+u}{4}\,W\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr).$$

We can then write $\tilde b=c|t|+w$ with $0\le w<|t|$ and note $|\tilde b|\gg\sqrt{q}K$ contribute negligibly by W-decay (§7.4.2) so $|c|\gg C_j=\sqrt{q}K/|T_j|=SK/|j|$ can be ignored. Similarly, we can write $\tilde b=\tilde c|t|+\tilde w$ with $|\tilde w|<|t|/2$, which will be used for $s=0$.

For each s, we are then left to estimate either

$$B_3^{j,s}=\sum_{\substack{|t-T_j|<\sqrt{q}/2S\\ t\equiv r_t\,(M_i)}}\ \sum_{\substack{0\le w<|t|\\ P(w)\equiv 0\,(t)}}F_s(w/|t|)\sum_{|c|\ll C_j}\frac{m_it+u}{4}\,W\Bigl(\frac{4\pi^2k^2l}{Nq}\Bigr)\tag{10}$$

[11] I must admit to not knowing an applicable citation for this. One can follow an idea popularized by B. J. Green: namely, let $f(z)$ be 1 on its support $[-1/2,1/2]$ and take the infinite convolution $f_\infty(z)$ of $2^nf(2^nz)$ for $n\ge 0$, which has $\sum_m f_\infty(z+m)\equiv 1$ for all z. In our context, we take $H_s(z)=f_\infty(Sz-Ss)$ and then $F_s(z)=\sum_m H_s(z+m)$ has the desired properties.

or

$$\tilde{B}_3^{j,s} = \sum_{\substack{|t-T_j|<\sqrt{q}/2S \\ t\equiv r_t\,(M_i)}} \sum_{\substack{|\tilde{w}|<|t|/2 \\ P(\tilde{w})\equiv 0\,(t)}} F_s(\tilde{w}/|t|) \sum_{|\tilde{c}|\ll C_j} \frac{m_i t + u}{4} W\Big(\frac{4\pi^2 k^2 l}{Nq}\Big),$$

with these two expressions essentially the same, just parametrizing $\tilde{b}$ differently.

7.6.1. For $s \neq 0$ the values of $w/|t|$ are restricted to a region of size $2/S$ about s/S, and thus we can aim to approximate

$$u = \frac{-4(68\tilde{b}+2r_b)^2 + qy^2}{m_i t} \quad \text{by} \quad U_{j,c,s} = \frac{-4\big[68(c|T_j| + s|T_j|/S)\big]^2 + qy^2}{m_i T_j},$$

while for $s = 0$ we instead wish to approximate by $U_{j,\tilde{c},s}$.

This leads us to approximate $B_3^{j,s}$ by

$$B_4^{j,s} = G_s^j \sum_{\substack{|t-T_j|<\sqrt{q}/2S \\ t\equiv r_t\,(M_i)}} \sum_{\substack{0\le w<|t| \\ P(w)\equiv 0\,(t)}} F_s(w/|t|) \tag{11}$$

where the w-sum can be over any period of length $|t|$, and we have

$$G_s^j = \sum_{|c|\ll C_j} \frac{m_i T_j + U_{j,c,s}}{4} W\Big(\frac{4\pi^2 k^2}{Nq}\big[(m_i T_j - U_{j,c,s})^2/4 + qy^2\big]\Big),$$

with G_s^j thus also depending on (k, i, y), which we suppress from the notation.

7.6.2. We now analyze the approximation error in $B_4^{j,s}$ to $B_3^{j,s}$. When $s \neq 0$ we avoid endpoints and have $\big|w/|t| - s/S\big| \le 1/S$, so that $\big|w - s|t|/S\big| \ll |T_j|/S$ and thus $\big|w - s|T_j|/S\big| \ll |T_j|/S + \sqrt{q}/S \ll \sqrt{q}K/S$. Since $|t - T_j| \ll \sqrt{q}/S \ll |T_j|/S^{4/5}$ we get

$$u = \frac{-4\big[68(c|T_j| + s|T_j|/S) + O(C_j\cdot\sqrt{q}/S) + O(\sqrt{q}K/S) + O(1)\big]^2 + qy^2}{m_i T_j\big(1 + O(1/S^{4/5})\big)},$$

so from $C_j = SK/|j| \ll KS^{1/5} = C$ and using $\sqrt{q}/S^{1/5} \ll |T_j| \ll \sqrt{q}K$ we have

$$|u - U_{j,c,s}| \ll \frac{C_j|T_j|\cdot C_j(\sqrt{q}/S)}{|T_j|} + \frac{(C_jT_j)^2}{|T_j|S^{4/5}} + \frac{qK^2}{|T_j|S^{4/5}} \ll \frac{\sqrt{q}K^2}{S^{3/5}} + \frac{\sqrt{q}K^3}{S^{2/5}} + \frac{\sqrt{q}K^2}{S^{3/5}}.$$

Replacing the $(m_i t + u)$ term in $B_3^{j,s}$ of (10) by $(m_i T_j + U_{j,c,s})$, for the error therein we see that summing over $s \neq 0$ still leaves $\sum_s F_s(\cdot) \le 1$ everywhere, while summing over j gives a bound via $|W(\cdot)| \ll 1$ and Corollary 4.2.3 of

$$\sum_{S^{4/5}\ll|j|\ll SK} \sum_{\substack{|t-T_j|<\sqrt{q}/2S \\ t\equiv r_t\,(M_i)}} \sum_{\substack{0\le w<|t| \\ P(w)\equiv 0\,(t)}} \sum_{|c|\ll C_j} \frac{\sqrt{q}K^3}{S^{2/5}} \ll \frac{C\sqrt{q}K^3}{S^{2/5}} \sum_{\substack{|t|\ll\sqrt{q}K \\ (t,34)=1}} \rho_P(t) \ll \frac{qK^6}{S^{1/5}},$$

which is acceptable, as summing over (k, i, y, r_b, r_t) multiplies by the bound by K^6.

Next we have to replace the argument of W involving t and u by the corresponding approximations. We first note that $|t|, |u| \ll \sqrt{q}K$ by W-decay, and so $(m_i t - u)^2$ differs from $(m_i T_j - U_{j,c,s})^2$ by $\ll \sqrt{q}K \cdot (\sqrt{q}K^3/S^{2/5}) = qK^4/S^{2/5}$. The boundedness of the derivative of W along with $|m_i T_j|, |U_{j,c,s}| \ll \sqrt{q}K$ imply (again with the s-sum being harmless) that the error herein when summing over all j is bounded as

$$K^2\frac{K^4}{S^{2/5}}\cdot C\sqrt{q}K\sum_{\substack{|t|\ll\sqrt{q}K\\(t,34)=1}}\rho_P(t)\ll\frac{qK^{10}}{S^{1/5}},$$

which again is acceptable. Thus we find that $B_4^{j,s}$ is a good approximant to $B_3^{j,s}$.

The same argument holds for $\tilde{B}_3^{j,s}$ and $s=0$, as we start with $\big|\tilde{w}/|t|-s/S\big|\le 1/S$, and the rest follows *mutatis mutandis*, the re-naming of c to $\tilde{c}$ in G_s^j being irrelevant.

Remark. We have been somewhat sloppy here, and a finer analysis could plausibly allow us to remove the S-dependence from C, whence a bound of $\ll q/\sqrt{S}$ both here and in §7.5 might follow.

7.7. We return to $B_4^{j,s}$ given by (11) and expand $F_s(z)=\sum_h c_s(h)\exp(2\pi ihz)$ as a Fourier series with $c_s(h)=\int_0^1 F_s(z)\exp(-2\pi ihz)\,\partial z$ to get

$$B_4^{j,s}=G_s^j\sum_{\substack{|t-T_j|<\sqrt{q}/2S\\t\equiv r_t\,(M_i)}}\sum_{\substack{0\le w<|t|\\P(w)\equiv 0\,(t)}}\sum_h c_s(h)\exp\bigl(2\pi ihw/|t|\bigr).$$

For $s\neq 0$ we see that F_s on $[0,1]$ is supported on $[(s-1)/S,(s+1)/S]$, so integrating twice by parts and using $|F_s''(\cdot)|\ll S^2$ gives $|c_s(h)|\ll\int_0^1|F_s''(z)|\,\partial z/|h|^2\ll S/|h|^2$ for $h\neq 0$ (and similarly for $s=0$). Thus we can remove the $|h|\gg H=S^3$ via the bound $|G_s^j|\ll C_j\sqrt{q}K$, giving an acceptable error when summing over s and j of

$$S\cdot C\sqrt{q}K\sum_{\substack{|t|\ll\sqrt{q}K\\(t,34)=1}}\rho_P(t)\cdot\frac{S}{H}\ll\frac{qK^4S^{11/5}}{H}=\frac{qK^4}{S^{4/5}}.$$

7.7.1. For each j with $S^{4/5}\ll|j|\ll SK$ this leaves us with

$$\sum_{s=0}^{S-1}G_s^j\sum_{|h|\ll H}c_s(h)\sum_{\substack{|t-T_j|<\sqrt{q}/2S\\t\equiv r_t\,(M_i)}}\sum_{\substack{0\le w<|t|\\P(w)\equiv 0\,(t)}}\exp(2\pi ihw/|t|),$$

where the inner double sum for $h\neq 0$ can be estimated by Hooley's methods. Noting that $|c_s(h)|\ll 1/S$, by Lemma 5.2.1 the contribution from $h\neq 0$ is bounded as

$$\ll C_j\sqrt{q}K\cdot KH^{3/2}\biggl(\frac{|T_j|(\log\log|T_j|)^{(5-\sqrt{2})/2}}{(\log|T_j|)^{(2-\sqrt{2})/2}}\biggr),$$

and crudely using $|T_j|\ll\sqrt{q}K$ while $|j|\ll SK$ the overall bound when summing over j is

$$\ll SK\cdot S^{1/5}\sqrt{q}K^2\cdot KS^{9/2}\frac{\sqrt{q}K}{(\log q)^{29/100}}=\frac{qS^{57/10}K^5}{(\log q)^{29/100}},$$

which by our choice of $S=(\log q)^{1/100}$ and $K=(\log q)^{1/10^9}$ is sufficient.

Remark. A more refined argument would take $H=S^{1+\epsilon}$ via higher derivatives and reduce the h-dependence in Hooley's result to a divisor function. Moreover, the S-dependence from C might also be lessened as commented in Remark 7.6.2, while the S-factor coming from splitting t into intervals (via j) could plausibly be handled in Hooley's argument somehow (perhaps at least taking its square root in a usage of Cauchy's inequality). In the rosiest scenario, we would get $qS^{1+\epsilon}/(\log q)^{(2-\sqrt{2})/2}$ as the quantity here to be balanced against the putative $q/\sqrt{S}$ from Remark 7.6.2.

7.8. We are thus left to consider the contribution from $h = 0$, which is given by

$$\sum_{S^{4/5}\ll|j|\ll SK}\sum_{s=0}^{S-1} c_s(0)\, G_s^j \sum_{\substack{|t-T_j|<\sqrt{q}/2S\\ t\equiv r_t\,(M_i)}}\ \sum_{\substack{0\le w<|t|\\ P(w)\equiv 0\,(t)}} 1$$

for fixed (k, i, y, r_b, r_t). Here we will use Lemma 4.2.1 and pair j with $-j$.

We have that the above is

$$\sum_{S^{4/5}\ll j\ll SK}\sum_{s=0}^{S-1} c_s(0) H_s^j$$

where (upon writing $t^\star = -t$) we have

$$H_s^j = G_s^j \sum_{\substack{|t-T_j|<\sqrt{q}/2S\\ t\equiv r_t\,(M_i)}}\ \sum_{\substack{0\le w<t\\ P(w)\equiv 0\,(t)}} 1 + G_s^{-j} \sum_{\substack{|t^\star-T_j|<\sqrt{q}/2S\\ t^\star\equiv -r_t\,(M_i)}}\ \sum_{\substack{0\le w<t^\star\\ P(w)\equiv 0\,(t^\star)}} 1.$$

With Lemma 4.2.1 the specific coprime residue class makes no difference in the asymptotic formula, and since $|G_s^j|, |G_s^{-j}| \ll C_j\sqrt{q}K$ we have

$$H_s^j = \big[G_s^j + G_s^{-j}\big]\frac{\sqrt{q}/S}{2\phi(M_i)}\frac{\tilde{E}_P(1)}{L_{\eta_{-4}}(1)} + O\Big(C\sqrt{q}K\frac{\sqrt{q}K^2}{(\log q)^{999}}\Big),$$

and summing the error over $(k, i, y, r_b, r_t, j, s)$ gives an acceptable bound.

Meanwhile, G_s^j is an odd function of j, so that the main term is simply zero.

Thus we have shown that the $h = 0$ contribution is negligible, and conclude that $|E| \ll q/(\log q)^{1/10^3}$. By the comparison of integrals in §6.2.3, this is a contradiction to $\mathbf{Q}(\sqrt{-q})$ having class number 1 for sufficiently large q.

References

[1] A. O. L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$. Math. Ann. **185** (1970), no. 2, 134–160. `http://eudml.org/doc/161948`

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

[3] A. Baker, *A remark on the class number of quadratic fields.* Bull. LMS **1** (1969), 98–102. `http://doi.org/10.1112/blms/1.1.98`

[4] A. Baker, *Imaginary Quadratic Fields with Class Number 2.* Ann. Math. **94** (1971), no. 1, 139–152. `http://doi.org/10.2307/1970739`

[5] B. Baran, *A modular curve of level 9 and the class number one problem.* J. Number Theory **129** (2009), no. 3, 715–728. `http://doi.org/10.1016/j.jnt.2008.09.013`

[6] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem.* J. Number Theory **130** (2010), no. 12, 2753–2772. `http://doi.org/10.1016/j.jnt.2010.06.005`

[7] 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`

[8] B. L. J. Braaksma, *Asymptotic expansions and analytic continuations for a class of Barnes-integrals.* Compositio. Math. **15** (1962-4), 239–341. `http://eudml.org/doc/88877`

[9] P. Bundschuh, A. Hock, *Bestimmung aller imaginär-quadratischen Zahlkörper der Klassenzahl Eins mit Hilfe eines Satzes von Baker.* (German) [Determination of all imaginary quadratic fields of class number one with the help of a theorem of Baker]. Math. Z. **111** (1969), no. 3, 191–204. `http://doi.org/10.1007/BF01113285`

[10] D. A. Burgess, *On character sums and L-series. II.* Proc. London Math. Soc. **13** (1963), 524–536. `http://doi.org/10.1112/plms/s3-13.1.524`

[11] V. A. Bykovskii, *A trace formula for the scalar product of Hecke series and its applications.* J. Math. Sciences **89** (1998), no. 1, 915–932. `http://doi.org/10.1007/BF02358528`

[12] I. Chen, *On Siegel's modular curve of level 5 and the class number one problem.* J. Number Theory **74** (1999), no. 2, 278–297. `http://doi.org/10.1006/jnth.1998.2320`

[13] J. E. Cremona, *Algorithms for modular elliptic curves.* Cambridge University Press, 1992. `http://homepages.warwick.ac.uk/~masgaj/book/amec.html`

[14] H. Davenport, *Multiplicative Number Theory.* Springer GTM **74**, 2000, 3rd edition. `http://doi.org/10.1007/978-1-4757-5927-3`

[15] M. Deuring, *Imaginäre quadratische Zahlkörper mit der Klassenzahl 1.* (German) [Imaginary quadratic fields with class number 1]. Math. Z. **37** (1933), 405–415. `http://eudml.org/doc/168455`

[16] M. Deuring, *Zetafunktionen quadratischer Formen.* (German) [Zeta-functions of quadratic forms]. J. reine Angew. Math. **172** (1935), 226–252. `http://eudml.org/doc/149913`

[17] M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins.* (German) [The zeta-function of an algebraic curve of genus one]. Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. Math.-Phys.-Chem. Ab **1953**, 85–94.

[18] M. Deuring, *Imaginäre quadratische Zahlkörper mit der Klassenzal Eins.* (German) [Imaginary quadratic fields with class number one]. Invent. Math. **5** (1968), 169–179. `http://doi.org/10.1007/BF01425548`

[19] G. Lejeune Dirichlet, *Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres.* (French) [Some diverse applications of the infinitesimal analysis in number theory]. J. reine Angew. Math. **19** (1839), 324–369, *ibid.* **21** (1840), 134–155.
`http://resolver.sub.uni-goettingen.de/purl?GDZPPN002142007`
`http://resolver.sub.uni-goettingen.de/purl?GDZPPN002142473`

[20] P. G. Lejuene Dirichlet, with supplement by R. Dedekind, *Vorlesungen über Zahlentheorie.* (German) [Lectures on number theory]. Vieweg und Sohn, 1871. `http://archive.org/details/vorlesungenberz04dedegoog`

[21] 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`

[22] W. Duke, J. B. Friedlander, H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli.* Ann. Math. **141** (1995), no. 2, 423–441. `http://doi.org/10.2307/2118527`

[23] L. Eulero [L. Euler], *De numeris, qui sunt aggregata duorum quadratorum.* (Latin) [On numbers which are the sum of two squares]. Novi Commentarii academiæ scientiarum Petropolitanæ **4** (1758), 3–40. `http://eulerarchive.maa.org/pages/E228.html`

[24] 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).

[25] A. O. Gelfond, *Transcendental and algebraic numbers.* Translated from the first Russian edition (1952) by L. F. Boron, Dover (1960, 2015).

[26] 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`

[27] T. H. Gronwall, *Sur les séries de Dirichlet correspondant à des caractéres complexes.* (French) [On Dirichlet series of complex characters]. Rend. Circ. Matem. Palermo **35** (1913), 145–159. `http://doi.org/10.1007/BF03015596`

[28] 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`

[29] G. H. Hardy, S. Ramanujan, *The normal number of prime factors of a number n.* Quart. J. Math. **48** (1917), 76–92.

[30] D. R. Heath-Brown, *Mathematical Reviews #2764153*, 2011m:11071. `http://mathscinet.ams.org/mathscinet-getitem?mr=2764153`

[31] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. I, II.* (German) [A new kind of zeta-function and its relation to the distribution of prime numbers]. Math. Z. **1** (1918), no. 4, 357–376, *ibid.* **6** (1920), 11–51. `http://eudml.org/doc/167468` `http://eudml.org/doc/167556`

[32] E. Hecke, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. I-II.* (German) [On modular functions and Dirichlet series with Euler products]. Math. Ann. **114** (1937), 1–28, 316–351.
http://eudml.org/doc/159899 http://eudml.org/doc/159919

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

[34] H. Heilbronn, *On the class number in imaginary quadratic fields.* Quart. J. Math. Oxford **5** (1934), no. 1, 150–160. http://doi.org/10.1093/qmath/os-5.1.150

[35] H. Heilbronn, E. H. Linfoot, *On the imaginary quadratic corpora of class-number one.* Quart. J. Math. Oxford **5** (1934), no. 1, 293–301. http://doi.org/10.1093/qmath/os-5.1.293

[36] D. A. Hejhal, *Roots of quadratic congruences and eigenvalues of the non-Euclidean Laplacian.* In *The Selberg trace formula and related topics*, ed. D. A. Hejhal, P. Sarnak, A. A. Terras. Contemp. Math. **53** (1986). http://doi.org/10.1090/conm/053/853563

[37] C. Hooley, *On the number of divisors of a quadratic polynomial.* Acta Math. **110** (1963), 97–114. http://doi.org/10.1007/BF02391856

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

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

[40] H. Iwaniec, *Topics in classical automorphic forms.* Grad. Studies in Math. **17**, AMS, 1997. http://doi.org/10.1090/gsm/017

[41] H. Iwaniec, E. Kowalski, *Analytic Number Theory.* Colloq. Publ. AMS **53** (2004). http://doi.org/10.1090/coll/053

[42] C. G. J. Jacobi, *Observatio arithmetica de numero classium divisorum quadraticorum formae $yy + Azz$, designante A numerum primum formae* $4n + 3$. (Latin) [An arithmetic observation on the class number of quadratic forms $y^2 + Az^2$ where A is a prime congruent to 3 mod 4]. J. reine angew. Math. **9** (1832), 189–192.
http://www.digizeitschriften.de/dms/resolveppn/?PID=GDZPPN002138727

[43] M. A. Kenku, *A note on the integral points of a modular curve of level 7.* Mathematika **32** (1985), no. 1, 45–48. http://doi.org/10.1112/S0025579300010846

[44] Ch.-J. de La Vallée Poussin, *Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premieres inférieurs a une limite donnée.* (French) [On the Riemann ζ-function and the number of prime numbers less than a given limit]. Mem. Courronnes et Autres Mem. Pub. Acad. Roy. Sci. Lettres Beaux-Arts Belgique **59** (1899/1900).
https://archive.org/details/surlafonctionze00pousgoog

[45] E. Landau, *Über imaginär-quadratischer Zahlkörper mit gleicher Klassenzahl.* (German) [On imaginary quadratic fields with the same class number]. Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. (1918), 277–284.
http://www.digizeitschriften.de/dms/resolveppn/?PID=GDZPPN002505134

[46] E. Landau, *Über die Klassenzahl imaginär-quadratischer Zahlkörper.* (German) [On the class number of imaginary quadratic fields]. Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. (1918), 285–295. http://www.digizeitschriften.de/dms/resolveppn/?PID=GDZPPN002505142

[47] E. Landau, *Bemerkungen zum Heilbronnschen Satz.* (German) [Remarks about Heilbronn's theorem]. Acta Arithmetica **1** (1935), 1–18. http://eudml.org/doc/205049

[48] U. V. Linnik, *On the least prime in an arithmetic progression II. The Deuring–Heilbronn phenomenon.* Rec. Math. [Mat. Sbornik.] **15** (1944), no. 3, 347–368.
http://mi.mathnet.ru/eng/msb6202

[49] J. E. Littlewood, *On the class number of the corpus $P(\sqrt{-k})$.* Proc. London. Math. Soc. **27** (1928), 358–372. http://plms.oxfordjournals.org/content/s2-27/1/358.full.pdf+html

[50] K. S. McCurley, *Explicit zero-free regions for Dirichlet L-functions.* J. Number Theory **19** (1984), no. 1, 7–32. http://doi.org/10.1016/0022-314X(84)90089-1

[51] Ju. I. Manin, *Parabolic points and zeta-functions of modular curves.* (Translated). Math. USSR Izvestia. **6** (1972), 19–64. http://doi.org/10.1070/IM1972v006n01ABEH001867

[52] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires.* (French) [Class numbers of imaginary quadratic fields]. Sém. Bourbaki **26** (1983–1984), 309–323.
http://eudml.org/doc/110032

[53] O. Perron, *Zur Theorie der Dirichletschen Reihen.* (German) [On the theory of Dirichlet series]. J. reine Angew. Math. **134** (1908), 95–143. http://eudml.org/doc/149285

[54] R. Schoof, N. Tzanakis, *Integral points of a modular curve of level 11.* Acta Arith. **152** (2012), no. 1, 39–49. http://doi.org/10.4064/aa152-1-4
[55] J.-P. Serre, $\Delta = ab^2 - 4ac$. Math. Medley (Singapore Math. Soc.) **13** (1985), 1–10. http://sms.math.nus.edu.sg/smsmedley/smsmedley.aspx#Vol-13
[56] J.-P. Serre, *Lectures on the Mordell-Weil Theorem.* Translated and edited by M. Brown from notes by M. Waldschmidt. Friedr. Vieweg & Sohn, Braunschweig, Aspects of Mathematics **15** (1989, 1997), x+218pp. http://doi.org/10.1007/978-3-663-10632-6
[57] G. Shimura, *On the holomorphy of certain Dirichlet series.* Proc. London Math. Soc. **31** (1975), no. 1, 79–98. http://doi.org/10.1112/plms/s3-31.1.79
[58] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper.* (German) [On the class number of quadratic fields]. Acta Arithmetica **1** (1935), 83–86. https://eudml.org/doc/205054
[59] C. L. Siegel, *Zum Beweise des Starkschen Satzes.* (German) [Some remarks on Stark's theorem]. Invent. Math. **5** (1968), no. 3, 180–191. http://eudml.org/doc/141914
[60] J. P. Sorenson, *Sieving for Pseudosquares and Pseudocubes in Parallel Using Doubly-Focused Enumeration and Wheel Datastructures.* In *Algorithmic Number Theory* (ANTS 2010), edited by G. Hanrot, F. Morain, E. Thomé, Springer LNCS **6197**, 331–339. http://doi.org/10.1007/978-3-642-14518-6_26
[61] H. Stark, *On complex quadratic fields with class number equal to one.* Trans. Amer. Math. Soc. **122** (1966), 112–119. http://doi.org/10.1090/S0002-9947-1966-0195845-4
[62] 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
[63] H. M. Stark, *On the "gap" in a theorem of Heegner.* J. Number Theory **1** (1969), 16–27. http://doi.org/10.1016/0022-314X(69)90023-7
[64] H. M. Stark, *A historical note on complex quadratic fields with class-number one.* Proc. Amer. Math. Soc. **21** (1969), 254–255. http://doi.org/10.1090/S0002-9939-1969-0237461-X
[65] H. M. Stark, *The role of modular functions in a class-number problem.* J. Number Theory **1** (1969), no. 2, 252–260. http://doi.org/10.1016/0022-314X(69)90044-4
[66] H. M. Stark, *Recent advances in determining all complex quadratic fields of a given class-number.* Proc. Sympos. Pure Math. **XX** (1971), 401–414. Edited by D. J. Lewis. http://www.ams.org/books/pspum/020/0316421
[67] H. M. Stark, *A Transcendence Theorem for Class-Number Problems.* Ann. Math. **94** (1971), no. 1, 153–173. http://doi.org/10.2307/1970740
[68] H. M. Stark, *The Gauss class-number problems.* Clay Math. Proc. **7** (2007), 247–256. Published by AMS as *Analytic Number Theory*, edited by W. Duke and Y. Tschinkel. http://www.uni-math.gwdg.de/tschinkel/gauss-dirichlet/stark.pdf
[69] J. Stopple, *Notes on the Deuring-Heilbronn phenomenon.* Notices AMS **53** (2006), no. 8, 864–875. http://www.ams.org/notices/200608/fea-stopple.pdf
[70] T. Tatuzawa, *On a theorem of Siegel.* Jap. J. Math. **21** (1951), 163–178. http://www.jstage.jst.go.jp/article/jjm1924/21/0/21_0_163/_pdf
[71] 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
[72] 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
[73] Á. Tóth, *Roots of quadratic congruences.* IMRN **2000**, no. 14, 719–739. http://doi.org/10.1155/S1073792800000404
[74] J.-L. Waldspurger, *Correspondance de Shimura.* (French) [The Shimura correspondence]. J. Math. Pures Appl. **59** (1980), no. 1, 1–132.
———, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier.* (French) [On the Fourier coefficients of modular forms of half-integral weight]. J. Math. Pures Appl. **60** (1981), no. 1, 375–484.
[75] M. Watkins, *Class numbers of imaginary quadratic fields.* Math. Comp. **73** (2004), no. 246, 907–938. http://doi.org/10.1090/S0025-5718-03-01517-5
[76] M. Watkins, *A spectral proof of class number one.* Math. Z., to appear, 2019. http://doi.org/10.1007/s00209-018-2183-1
[77] A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen.* (German) [On Dirichlet series satisfying functional equations]. Math. Ann. **168** (1967), 149–156. http://eudml.org/doc/161499