MATHEMATICS OF COMPUTATION
Volume 73, Number 246, Pages 907–938
S 0025-5718(03)01517-5
Article electronically published on October 2, 2003

CLASS NUMBERS OF IMAGINARY QUADRATIC FIELDS

MARK WATKINS

Abstract. The classical class number problem of Gauss asks for a classification of all imaginary quadratic fields with a given class number N. The first complete results were for $N = 1$ by Heegner, Baker, and Stark. After the work of Goldfeld and Gross-Zagier, the task was a finite decision problem for any N. Indeed, after Oesterlé handled $N = 3$, in 1985 Serre wrote, "No doubt the same method will work for other small class numbers, up to 100, say." However, more than ten years later, after doing $N = 5, 6, 7$, Wagner remarked that the $N = 8$ case seemed impregnable. We complete the classification for all $N \leq 100$, an improvement of four powers of 2 (arguably the most difficult case) over the previous best results. The main theoretical technique is a modification of the Goldfeld-Oesterlé work, which used an elliptic curve L-function with an order 3 zero at the central critical point, to instead consider Dirichlet L-functions with low-height zeros near the real line (though the former is still required in our proof). This is numerically much superior to the previous method, which relied on work of Montgomery-Weinberger. Our method is still quite computer-intensive, but we are able to keep the time needed for the computation down to about seven months. In all cases, we find that there is no abnormally large "exceptional modulus" of small class number, which agrees with the prediction of the Generalised Riemann Hypothesis.

1. Introduction

The classical class number problem of Gauss asks for a classification of all imaginary quadratic fields with a given class number N. We do not review the complete history here, but mention that important advances were made by Heilbronn and Linfoot [15], Siegel [37] following Landau [17], Tatuzawa [43], and Heegner [14], [41] before Baker [4], [5] and Stark [39], [42] independently and jointly [6] completed the classification for $N = 1$ and $N = 2$. See [12], [31], or [35] for a more complete history, including the vagaries regarding Heegner's work. Tatuzawa's work had shown that the classifications were complete with at most one possible exception, and the works of Heegner, Baker, and Stark eliminated this possibility when N was 1 or 2. For any given N, the problem was reduced to a finite computation by the work of Gross and Zagier [13], using a theorem due to Goldfeld [11]. The work of Oesterlé [30] greatly streamlined Goldfeld's argument, allowing him to handle $N = 3$. The latest results are Arno's thesis [2] and subsequent work with Robinson and Wheeler [3] and the work of Wagner [44], which together complete the classification for all $N \leq 7$ and odd $N \leq 23$. In this work, we handle all $N \leq 100$. The advance is mainly theoretical, though a long computation (seven months on desktop computers) is still necessary. Our argument is a modification of

Received by the editor February 27, 2002.
2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11M06, 11Y35.

the work of Oesterlé-Goldfeld, working with Dirichlet L-functions with a low-height zero instead of elliptic curve L-functions with a high-order zero at the critical point. Through this method, we reduce the amount of computational sieving needed by a factor of 1000 or more when compared to the bound obtained from previous work due to Montgomery and Weinberger [29].

Other work in a related direction has been undertaken by Setzer [36] who determined all imaginary quartic abelian number fields with class number one. Yamamura [48] first extended Setzer's work to all imaginary abelian number fields and later classified [49] all imaginary non-CM normal octic fields of class number one. Louboutin and Okazaki [24] have found all non-Galois quartic fields of class number one and all nonabelian Galois octic fields of type CM with class number one, and also have classified all quarternion CM-fields with ideal class group an exponent of two [25]. These last two authors have various other results, the most recent being a joint work with Lemmermeyer [20] on class number one for some nonabelian normal CM-fields of degree 24. Louboutin [23] has considered dihedral and dicyclic CM-fields (and extended this later with Park [26]), nonquadratic imaginary 2-power cyclic fields with class number equal to genus class number [22] (extending work of Miyada [28]), amongst many other various results. All of these results head in a different direction than our work, enlarging the degree of the field instead of the class number. We should also note that the Generalised Riemann Hypothesis implies that the class number of $\mathbf{Q}\big(\sqrt{-d}\big)$ is at least

$$\big(1+o(1)\big)(\pi/12e^{\gamma})\sqrt{d}/\log\log d$$

(see Littlewood [21]), and Paley [32] has shown that this is best possible except for a factor of two.

Let us outline this paper. In Section 2 we review the background material for binary quadratic forms, Dedekind zeta functions, etc. In Section 3 we describe how the method of Arno et al. and Wagner works and indicate how our argument shall differ. In Section 4 we prove various technical lemmata in preparation for the proof of a key inequality in Section 5. In Section 5 we prove our key inequality, which is similar in form to that of Montgomery and Weinberger [29], but is numerically superior due to the fact that we save a logarithm. In Sections 6 and 7 we use the key inequality of Section 5 to reduce our class number problems to a reasonable sieving problem. These sections, especially the latter, unfortunately become quite numeric at times, but we try to make the main ideas clear without getting lost in a slew of numbers. In Section 8 we describe our sieving process and comment on the possibilities for extending our method of analysis to handle higher class numbers. One can see the division of work between the last three sections as a splitting into large, mid-sized, and small discriminants. The large region is by far the easiest and is not novel in any respect besides the generation of sufficently many useful auxiliary moduli. The mid-sized region uses the same method as the large region, but pays much more attention to the tightness of bounds in order to reduce the amount of sieving needed in the small region.

This work had its beginnings in the dissertation of the author, in which he handled class numbers up to 16. The author would like to thank his dissertation advisor Carl Pomerance for support and helpful comments and also Andrew Granville and Daniel Shiu.

2. Background material

Here we review the background material for quadratic forms and lay the groundwork for a resolution of the class number N problem. Although we are most interested in $N \leq 100$, the method is general enough to allow attacks on larger N. We let $-d$ be a fundamental discriminant, $d > 4$. Recall that this means that d is congruent to one of $3, 7, 11, 15, 4, 8$ modulo 16. Furthermore d is squarefree if it is odd, and $d/4$ is squarefree if d is even. Given our specification of imaginary quadratic fields, the class group of the ring of integers can be realised in the guise of binary quadratic forms. A form $ax^2 + bxy + cy^2$ shall be abbreviated (a, b, c). We consider the **reduced** forms of discriminant $-d$; these are given by

$$Q_d = \{(a, b, c) : b^2 - 4ac = -d, -a < b \leq a < c \text{ or } 0 \leq b \leq a = c\},$$

which could be rephrased by saying that $(b + i\sqrt{d})/2a$ (as a point in the upper half-plane) is in the standard fundamental domain for the action of $\mathrm{SL}_2(\mathbf{Z})$.

We have that $|Q_d| = h(-d)$, the class number of $\mathbf{Q}(\sqrt{-d})$. We say that a form (a, b, c) represents a number $r \neq 0$ if there exist integers m and n with $am^2 + bmn + cn^2 = r$. We note that since $|b| \leq a \leq c$ and $b^2 - 4ac = -d$, it follows that $a \leq \sqrt{d/3}$ for reduced forms. Mostly we will be concerned with reduced forms which have $a \leq \sqrt{d/4}$, as the set of these has an additional multiplicative structure. Note that $am^2 + bmn + cn^2$ is a parabola in the m-coordinate. Its minimum occurs at $m = -bn/2a$, and the minimum is $dn^2/4a$, using $b^2 - 4ac = -d$. Hence if $n \neq 0$, then we have $am^2 + bmn + cn^2 \geq d/4a$. Thus if $a \leq \sqrt{d/4}$, we see that only when $n = 0$ can $am^2 + bmn + cn^2$ represent an integer less than $\sqrt{d/4}$. But, in fact, the same is true even in the range $\sqrt{d/4} \leq a \leq \sqrt{d/3}$. We see this as follows: if $|n| \geq 2$, then we are done since $am^2 + bmn + cn^2 \geq d/a \geq \sqrt{3d}$. On the other hand, if $|n| = 1$, then the m-coordinate of the vertex of the parabola is between 0 and ± 1, where the sign is that of bn. At $m = 0$, it is obvious that $am^2 + bmn + cn^2 = c \geq a \geq \sqrt{d/4}$, while at $m = \pm 1$, we have $am^2 + bmn + cn^2 = a - |b| + c \geq c \geq \sqrt{d/4}$. In fact, since $c \geq a$, this shows that a is the smallest integer represented by the form. Hence we have the following:

Lemma 1. *Let $am^2 + bmn + cn^2$ be a reduced binary quadratic form of discriminant $-d = b^2 - 4ac < 0$. Then a is the smallest integer represented by the form. Furthermore, no integer less than $\sqrt{d/4}$ has a representation with $n \neq 0$.*

The number a is called the minimum of the form. It shall play an important role in what follows. The principal form is the unique reduced form which represents 1. When d is even, the principal form is $x^2 + \frac{d}{4}y^2$, while if d is odd, it is given by $x^2 + xy + \frac{d+1}{4}y^2$. We define M_d to be the multi-set of minima of the reduced forms for the fundamental discriminant $-d$. It follows directly from the definition of Q_d that if $a \neq c$, $a \neq b$, and $b \neq 0$, then there is an inequivalent "conjugate" form to (a, b, c) given by $(a, -b, c)$. In fact, this conjugate form $(a, -b, c)$ is the inverse of (a, b, c) in the class group. Thus, in this case, a appears in M_d more than once. If we have $a = c$, $a = b$, or $b = 0$, then the form (a, b, c) is its own inverse.

The Dedekind zeta function $\zeta_{-d}(s)$ of $\mathbf{Q}(\sqrt{-d})$ is the product of $\zeta(s)$ and $L(s, \chi_{-d})$. Thus, it has a natural Euler product. However, if we write $\zeta_{-d}(s)$ as a Dirichlet series $\sum_l c_l/l^s$, then from the work of Dedekind (inherent already in Dirichlet) we know that c_l is the number of times that l is represented by members

of Q_d. Thus we can write the Dedekind zeta function as a sum over the reduced forms:

$$2\zeta(s)L(s,\chi_{-d}) = \sum_{(a,b,c)\in Q_d} \sum\sum_{(m,n)\neq(0,0)} (am^2+bmn+cn^2)^{-s}.$$

Here the factor of two simply accounts for the fact that $am^2+bmn+cn^2$ is unchanged if we negate both m and n, and we wish to avoid double-counting. The individual double sums are known as Epstein zeta functions. We define

$$Z_Q(s) = \frac{1}{2} \sum\sum_{(m,n)\neq(0,0)} (am^2+bmn+cn^2)^{-s},$$

for a reduced form $Q=(a,b,c)$. It follows from [7] or [34] that $Z_Q(s)$ extends to a meromorphic function, having only a simple pole at $s=1$, where the residue is $\pi/\sqrt{d}$. Furthermore, we have that $(\sqrt{d}/2\pi)^s Z_Q(s)\Gamma(s)$ is invariant under the map $s\mapsto 1-s$. Also, if we divide $Z_Q(s)$ by $\zeta(2s)$, this simply serves to remove terms in the double sum with $\gcd(m,n)>1$:

Lemma 2. *Let $Q=(a,b,c)$ be a binary quadratic form of discriminant $-d=b^2-4ac<0$. Then we have*

$$\frac{Z_Q(s)}{\zeta(2s)} = \frac{1}{2} \sum_{\substack{m\in\mathbf{Z}\\ \gcd(m,n)=1}} \sum_{n\in\mathbf{Z}} (am^2+bmn+cn^2)^{-s}. \tag{1}$$

Proof. This is equivalent to showing that

$$\sum\sum_{(m,n)\neq(0,0)} (am^2+bmn+cn^2)^{-s} = \zeta(2s) \sum_{\substack{m\in\mathbf{Z}\\ \gcd(m,n)=1}} \sum_{n\in\mathbf{Z}} (am^2+bmn+cn^2)^{-s}.$$

We consider the contribution to the l^{-s} term. On the left-hand side, this is the number of (m,n) pairs with $l=am^2+bmn+cn^2$. Let $y(k)$ be the number of coprime (m,n) pairs with $k=am^2+bmn+cn^2$. Then the right-hand side contribution to the l^{-s} term is $\sum_{j^2|l} y(l/j^2)$. Now each way of writing l/j^2 as $am^2+bmn+cn^2$ lifts to a unique way of writing l as $a(jm)^2+b(jm)(jn)+c(jn)^2$, and vice versa with $\gcd(m,n)=j$. Hence the l^{-s} terms on each side are equal. This shows the lemma. □

Call a representation $am^2+bmn+cn^2=r$ of r primitive if $\gcd(m,n)=1$, and let $2R(r)$ be the number of primitive representations of r by reduced forms of discriminant $-d$. Summing (1) over all the reduced forms, we get that

$$\frac{\zeta(s)L(s,\chi_{-d})}{\zeta(2s)} = \sum_{r=1}^{\infty} \frac{R(r)}{r^s}.$$

The left-hand side of this is given by the Euler product $\displaystyle\prod_p \frac{1+p^{-s}}{1-(-d|p)p^{-s}}$, so by expanding we see that $R(r)=\prod_{p|r}\bigl[1+(-d|p)\bigr]\prod_{p^2|r}(-d|p)$. We define the arithmetic function $\tilde{R}(r)$ to be the number of times that r appears in the multi-set of minima M_d, and we write $R^\star(r)=R(r)-\tilde{R}(r)$, so that $R^\star(r)$ is the number of

primitive nonminimum representations of r. We again sum (1) over the reduced forms, and then break off the terms with $n = 0$:

$$\begin{aligned} 2\frac{\zeta(s)L(s,\chi_{-d})}{\zeta(2s)} &= \sum_{(a,b,c)\in Q_d} \sum_{\substack{m\in\mathbf{Z}\\ \gcd(m,n)=1}} \sum_{n\in\mathbf{Z}} (am^2+bmn+cn^2)^{-s} \\ &= \sum_{(a,b,c)} \left[\frac{2}{a^s} + \sum_{\substack{\gcd(m,n)=1\\ n\neq 0}} \sum (am^2+bmn+cn^2)^{-s}\right] \\ &= 2\sum_{(a,b,c)} \left[\frac{1}{a^s} + \sum_{\substack{m\in\mathbf{Z}\\ \gcd(m,n)=1}} \sum_{n>0} (am^2+bmn+cn^2)^{-s}\right]. \end{aligned}$$

By Lemma 1, each member of the last double sum has $am^2+bmn+cn^2 \geq \sqrt{d/4}$ (note that we are assuming that $d > 4$, so that $\sqrt{d/4}$ is nonintegral; thus we can safely use either strict or nonstrict inequality in statements such as these). Thus any representation of a number $r \leq \sqrt{d/4}$ must have $n = 0$, and hence r must be the minimum of this form. Hence we see that for $r \leq \sqrt{d/4}$, we have

$$\tilde{R}(r) = R(r) = \prod_{p|r} \big[1 + (-d|p)\big] \prod_{p^2|r} (-d|p). \tag{2}$$

This equation is very important in that it says the counting function for minima is multiplicative if the product of the minima is less than $\sqrt{d/4}$; in other words $R^\star(r) = 0$ for $r \leq \sqrt{d/4}$. For instance, if we have $2, 5, 5 \in M_d$ and $\sqrt{d/4} > 10$, then we know that 10 appears twice in M_d. We define three types of prime minima. The Type I primes are those for which $p|d$, with $p \leq \sqrt{d/3}$ if d is odd, and with $p \leq \sqrt{d/4}$ if d is even. In the odd d case, we have that $\big(p, p, (p + d/p)/4\big)$ is a reduced form, and if d is even, then $(p, 0, d/4p)$ is a reduced form (except for $p = 2$, when the reduced form is $(2, 2, (d + 4)/8)$). Primes of this type appear once in the multi-set of minima. The Type II primes are the primes $p \leq \sqrt{d/3}$ with $\chi(p) = +1$ for which (p, b, c) is a reduced form of discriminant $-d$ for some b and c; if $p \leq \sqrt{d/4}$ and $\chi(p) = +1$, we know that such b and c exist. Such a p will appear twice in the multi-set of minima in the general case, but only once if $p = c$, which we shall distinguish by calling it a Type IIb prime; noting that these are at least $\sqrt{d/4}$, they will cause only a minor concern. From the above display we have the following:

Lemma 3. *Suppose that R appears r times in the multi-set M_d and that S appears s times. If $\gcd(R, S) = 1$ and $RS \leq \sqrt{d/4}$, then RS appears rs times in M_d. Furthermore, if P is a Type II prime and $P^l \leq \sqrt{d/4}$ for some $l \geq 1$, then P^l appears twice in M_d.*

Note that the number of minima (i.e., $\big|M_d\big|$) is exactly equal to $h(-d)$. This follows since the number of reduced forms (i.e., $\big|Q_d\big|$) is equal to $h(-d)$, and minima and forms are in an obvious one-to-one correspondence. From Gauss's theory of genera [10], [8], we know that $2^{\omega(d)-1}$ divides $h(-d)$ where $\omega(d)$ is the number of distinct prime factors of d, or more accurately, $G|h$ where G is the number of genera (which is a power of 2). We can calculate that $\log_2 G = G_1 + G_2 - 1$ where G_1 is the number of Type I primes, and G_2 is equal to the number of primes for which $p|d$, requiring $p \geq \sqrt{d/3}$ if d is odd, and $p \geq \sqrt{d/4}$ is d is even. It will also be useful to

know that any composite minimum can be written as the product of two minima both of which are each less than $\sqrt{d/4}$.

3. Previous methods and how our method compares

We now describe the general outline of our attack on the class number N problem for $N \le 100$. Using a result of Oesterlé [30] and the theory of genera due to Gauss [10], it is easy to conclude that if $h(-d) \le 100$, then $d \le e^{298368000}$. For the range $2^{162} \le d \le e^{298368000}$, we shall use a fairly mechanical method involving a variant of the Goldfeld-Oesterlé method and low-height zeros of various L-functions (see Table 1 at the end of this section). This dates back as far as Stark's early work on class number one [38]. We shall use a similar method for $2^{52} \le d \le 2^{162}$, but here it is not so mechanical. In fact, the lower part of this range is the most difficult part. If we were not able to go down as far as 2^{52}, we would need to sieve more numbers with our computational sieve. This is the main obstacle in doing the class number N problem. (In reality, we sieve slightly further for some d's of various specific forms.) Due to our reduction of this sieving bound to 2^{52}, we are able to handle the remaining range by a computational sieve in a reasonable amount of time. Using previous methods, it had appeared that the counterpart to our bound of 2^{52} would be more like 2^{62} or higher.

Our adaption of the Goldfeld-Oesterlé method gives a result that is similar in form to a formula of Montgomery and Weinberger [29], which was used by previous authors in attempts to reduce the sieving bound above. We now describe their result and indicate how ours will differ. The details of the derivation of the equation below can be found in [40], [29] or [34]; the main idea is to decompose the Dedekind zeta function as a sum of Epstein zeta functions and then expand each into a Fourier series and swap the order of summation. We state the result. Let $\chi_k(\cdot) = (k|\cdot)$ be a real primitive Dirichlet character modulo $|k|$ with $\gcd(k,d) = 1$. Then we have

$$\left(\frac{|k|\sqrt{d}}{2\pi}\right)^{s-1/2} \Gamma(s)L(s,\chi_k)L(s,\chi_{-kd}) = \tilde{T}_{k,d}(s) + \tilde{T}_{k,d}(1-s) + \tilde{U}_{k,d}(s)$$

where

$$\tilde{T}_{k,d}(s) = \left(\frac{|k|\sqrt{d}}{2\pi}\right)^{s-1/2} \Gamma(s)\zeta(2s)P_k(s)\tilde{A}(s),$$
$$P_l(s) = \prod_{p|l}(1 - 1/p^{2s}),$$

and

$$\tilde{A}(s) = \sum_{(a,b,c)\in Q_d} \frac{\chi_k(a)}{a^s},$$

while $\tilde{U}_{k,d}(s)$ is an error term given by

$$\tilde{U}_{k,d}(s) = \frac{4\sqrt{\pi}}{|k|} \sum_{(a,b,c)\in Q_d} \frac{1}{\sqrt{a}} \sum_{n=1}^{\infty} K_{s-1/2}\left(\frac{\pi n\sqrt{d}}{a|k|}\right) n^{s-1/2}$$
$$\times \sum_{y|n} \mathrm{Re}\left[\sum_{j=1}^{|k|} \chi_k(aj^2 + bjy + cy^2) \exp\left(i\frac{n\pi}{|k|}\left(\frac{2j}{y} + \frac{b}{a}\right)\right)\right],$$

where $K_\nu(z)$ is the standard K-Bessel function given by the formula $K_\nu(z) = \int_0^\infty e^{-z\cosh t}\cosh \nu t\, dt$ for any $\nu, z \in \mathbf{C}$ with $|\arg z| < \pi/2$ (see, e.g., [46]).

Some manageable upper bounds on $\left|\tilde{U}_{k,d}(s)\right|$ have been found. For $\operatorname{Re} s = 1/2$, we have

$$\left|\tilde{U}_{k,d}(s)\right| \le V_k \sum_{(a,b,c)\in Q_d} \sqrt{\frac{a}{d}} \tag{3}$$

where V_k is a number depending only on k; it can be taken to be (see [44])

$$V_k = 8\sqrt{\frac{|k|}{\pi}}\left(1+\log\left(1+\frac{2|k|}{\pi\sqrt{3}}\right)\right)\prod_{p|k}\left(2+\frac{3}{p^{3/2}}\right). \tag{4}$$

Our result is of the form (here $g = \gcd(d,k)$; we require k to be odd to ease problems with powers of 2)

$$\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{s-1/2}\Gamma(s)L(s,\chi_k)L(s,\chi_{-kd/g^2}) = T_{k,d}(s) + T_{k,d}(1-s) + U_{k,d}(s), \tag{5}$$

where $T_{k,d}(s) = \Gamma(s)\zeta(2s)P_{k/g}(s)A(s)\left(|k|\sqrt{d}/2\pi g\right)^{s-1/2}$ and $A(s)$ is an **admissible** Dirichlet series. We define this term. Recall our definition of $R^\star(n)$ as (half) the number of primitive nonminimum representions of n, so that

$$\sum_{n=1}^\infty \frac{R^\star(n)}{n^s} = \frac{\zeta(s)L(s,\chi_{-d})}{\zeta(2s)} - \sum_{a\in M_d}\frac{1}{a^s}.$$

Define

$$G_p(s) = \left(1+\frac{(-kd/g^2|p)}{p^s}\right) \quad \text{if } p|kp|d \tag{6}$$

and

$$G_p(s) = \frac{1+\chi_k(p)/p^s}{1-(-k^2d|p)/p^s} \quad \text{otherwise,}$$

and write $G(s) = \sum_n g(n)/n^s$. Then $A(s) = \sum_n a(n)/n^s$ is **admissible** if $|g(n)-a(n)| \le R^\star(n)$ for all n. Indeed, it will be shown that the above $\tilde{A}(s)$ is admissible, as are modifications of various truncations of the $G(s)$-Euler-product (see Lemma 8). These are the main types of admissible $A(s)$ we use. Our error term $U_{k,d}(s)$ can be given explicitly, but it is more useful just to give bounds on it, which we describe now.

For a given $(a,b,c) \in Q_d$, we have two different bounds on its contribution to $U_{k,d}(s)$, a generic bound $V^G_{k,d}$ and a specific bound $V^S_{k,d}(a)$. As the notation indicates, the former does not depend on a, while the latter does. From this, our bound for $|U_{k,d}(s)|$ when s is on the line $\operatorname{Re} s = 1/2$ can be written in the form $U^B_{k,d} = W_{k,d} + \sum_{a\in Q_d}\min\left(V^G_{k,d}, V^S_{k,d}(a)\right)$ (we actually only prove a result like this when s is a zero of $L(s,\chi_k)$, but it can be extended to the entire half-line). The generic bound $V^G_{k,d}$ is basically given by $2\sqrt{2\pi|k|}/d^{1/4}$. The specific bound $V^S_{k,d}(a)$ is more complicated; suffice it to say that it plays the role of the $\sqrt{a/d}$ in (3) above, making the small minima have a lesser contribution. Finally, $W_{k,d}$ is a contribution to our error term which involves $A(s)$ on a vertical line to the left of $\operatorname{Re} s = 1/2$; it is to control this error term in some difficult situations that we opt for the generality induced by the notion of admissibility. The main advantage that our generic bound

has over (4) is the loss of a logarithm, which is magnified to the fourth power when considered with the $d^{1/4}$. Through the use of Kloosterman sums to effect extra cancellation, one could improve the Montgomery-Weinberger method so that it is asymptotically better than our result, but unfortunately this would likely be unhelpful in our region of interest.

Our idea (following the lead of [29]) will be to choose a modulus k for which we know a low-height zero $1/2 + i\xi_0$ of $L(s, \chi_k)$ which is on the half-line. Then we will evaluate both sides of the formula (5) at this point. The left-hand side is obviously zero. By using the Schwarz Reflection Principle (see, e.g., [18]), we can see that $T_{k,d}(1/2+i\xi_0) = \overline{T_{k,d}(1/2 - i\xi_0)}$, and this gives us $2\operatorname{Re} T_{k,d}(s) = -U_{k,d}(s)$. From here, we derive a lower bound for $|2\operatorname{Re} T_{k,d}(s)|$ through consideration of the argument of $T_{k,d}(s)$. By showing that it is not close to a multiple of π, we find that the real part of $T_{k,d}(s)$ is not small. Under the assumption of $h(-d)$ being small, we can also show that $|U_{k,d}(s)|$ is smaller than this lower bound on $|2\operatorname{Re} T_{k,d}(s)|$, and thus our assumption of small class number must be incorrect.

We keep the notation that $L(1/2 + i\xi_0, \chi_k) = 0$. We rewrite $2\operatorname{Re} T_{k,d}(1/2 + i\xi_0)$ as

$$\begin{aligned} 2\operatorname{Re} T_{k,d}(1/2 + i\xi_0) &= 2|T_{k,d}(1/2 + i\xi_0)| \cos\bigl(\arg T_{k,d}(1/2 + i\xi_0)\bigr) \\ &= 2\bigl|\Gamma(1/2 + i\xi_0)\zeta(1 + 2i\xi_0)P_{k/g}(1/2 + i\xi_0)A(1/2 + i\xi_0)\bigr| \\ &\quad \times \sin\bigl(\arg iT_{k,d}(1/2 + i\xi_0)\bigr) \\ &= \xi_3|A(1/2 + i\xi_0)| \sin\bigl[\xi_1 \log d + \xi_2 + \arg A(1/2 + i\xi_0)\bigr], \end{aligned} \tag{7}$$

where $\xi_1 = \xi_0/2$, $\xi_3 = 2\bigl|\Gamma(1/2 + i\xi_0)\zeta(1 + 2i\xi_0)P_{k/g}(1/2 + i\xi_0)\bigr|$, and

$$\xi_2 = \xi_0 \log\left(\frac{|k|/g}{2\pi}\right) + \arg\bigl[i\Gamma(1/2 + i\xi_0)\zeta(1 + 2i\xi_0)P_{k/g}(1/2 + i\xi_0)\bigr]. \tag{8}$$

In many instances we shall require d and k to be coprime, in which case ξ_1, ξ_2, and ξ_3 are independent of d, depending only on k. And even if $(k, d) \neq 1$, there are only a few possibilities for this gcd. By combining the above equations, we have

$$\bigl|\sin\bigl[\xi_1 \log d + \xi_2 + \arg A(1/2 + i\xi_0)\bigr]\bigr| \leq \frac{U^B_{k,d}}{\xi_3|A(1/2 + i\xi_0)|}, \tag{9}$$

where $U^B_{k,d}$ is an upper bound for $\bigl|U_{k,d}(1/2 + i\xi_0)\bigr|$. Our assumption of small class number will imply a number of things about these formulae. Firstly, it will say that $\arg A(1/2 + i\xi_0)$ is rather small, and secondly that $|A(1/2 + i\xi_0)|$ is sufficiently bounded away from zero. Furthermore, this assumption will allow us to get an efficacious number for $U^B_{k,d}$. Unless we are in a range of d for which the argument of the sine function on the left-hand side of (9) is too close to a multiple of π, this will lead to a contradiction. By using enough different moduli k, it becomes unlikely that a given d would be problematic for all of them simultaneously. Also, a requirement of $\gcd(d, k) = 1$ is not a problem if we use sufficiently many mutually coprime k, since any fundamental discriminant $-d$ with $h(-d) \leq 100$ has at most 7 prime factors by the theory of genera. In this way, we are able to exclude large ranges of d from consideration.

Table 1 is a list of our various auxiliary fundamental discriminants k and their relevant statistics; these shall be used in our argument later. The latter 17 moduli

TABLE 1. Fundamental discriminants k used as auxiliary moduli

k	$\xi_0 = 2\xi_1$	ξ_2	ξ_3	g	factorisation
-163	0.2029013374988−	0.522143501	8.087	1	prime
-163	0.2029013374988−	−0.516764364	8.064	163	prime
-17923	0.0309857994985−	0.221562908	57.0	1	prime
-17923	0.0309857994985−	−0.081938880	57.0	17923	prime
-115147	0.0031576171546+	0.028750244	555	1	$113 \cdot 1019$
-1599847	0.0041700469535−	0.049107661	418	1	$61 \cdot 26227$
-1832763	0.0028914317622−	0.037221504	408	1	$3 \cdot 610921$
-8844707	0.0024525434632−	0.032821985	720	1	$349 \cdot 25343$
-11023787	0.0035551527795+	0.048238612	498	1	prime
-12461947	0.0024972078778+	0.034189907	709	1	prime
-17773807	0.0045817782246−	0.064357208	386	1	prime
-19420619	0.0033117362832+	0.047060003	531	1	$131 \cdot 148249$
-21614147	0.0022439934195+	0.032052511	786	1	$271 \cdot 79757$
-23311771	0.0048024717046−	0.072181068	314	1	$7 \cdot 163 \cdot 20431$
-24088843	0.0030464971137+	0.044586643	556	1	$23 \cdot 1047341$
-24463627	0.0045379439922−	0.065191189	390	1	prime
-26012207	0.0013588216455−	0.020184789	1204	1	$13 \cdot 2000939$
-28815295	0.0013731625949−	0.021056330	1032	1	$5 \cdot 5763059$
-31129723	0.0020616533726−	0.030114015	859	1	prime
-32438927	0.0044118919674+	0.065817481	387	1	$31 \cdot 317 \cdot 3301$
-175990483	0.0004752439954+	0.007926667	3530	1	$19 \cdot 1427 \cdot 6491$

shall only be used with $(k, d) = 1$, and so we list the ξ_i values for only $g = 1$ in these cases. In Table 1, $\xi_0 = 2\xi_1$ is an approximation to the imaginary part of a small height zero of $L(s, \chi_k)$, the zeros being computed as per the method of Weinberger [47]. This consists of taking a truncated approximation of the Dirichlet series for $L(s, \chi_k)$, weighted by incomplete Γ-integrals. Evaluation at one data point took around thirty minutes for the larger moduli using a program written in PARI-GP [33]. The secant method was used to locate the zeros, and usually converged to the indicated precision within five steps. The $+/-$ in Table 1 indicates whether the zero is larger/smaller than the 13-digit approximation. The 9-digit accuracy for ξ_2 is very much overkill. The values of ξ_2 given in Table 1 are correct to within one in the last digit given. The values given for ξ_3 are lower bounds. The choice of the larger moduli was motivated by a related computer experiment [45]. There is no particular significance to them other than that $L(s, \chi_k)$ has a low height zero and $|k|$ is not overly large. No claim is made that they are the optimal moduli for this purpose, or for that matter, even what optimal in this sense might mean.

4. Technical reductions

We now turn to some technical lemmata. The first gives an upper bound for an Epstein zeta function on the 3/2-line, the second and third are a revisiting of lemmata of Oesterlé [30] involving the comparison of two measures relating lattice-point counting inside an ellipse to the area of the ellipse, the fourth is a simple residue calculation for which there seemed no better place, and the fifth gives us a nice collection of admissible choices for $A(s)$.

Lemma 4. *Let $Q = (a, b, c)$ be a (reduced) binary quadratic form with discriminant $b^2 - 4ac = -d < 0$. Let $Z_Q(s) = \frac{1}{2} \sum\sum_{(m,n)\neq(0,0)} \frac{1}{(am^2+bmn+cn^2)^s}$ be the Epstein zeta-function corresponding to Q. Then on the line $\operatorname{Re} s = 3/2$, we have $|Z_Q(s)| \leq 13/a^{3/2}$.*

Proof. Note first that the terms with $n = 0$ contribute $\zeta(3)/a^{3/2} \leq 1.21/a^{3/2}$. For the other terms, we need only consider $n \geq 1$ by symmetry and doing so will remove the coefficient of $1/2$ in the $Z_Q(s)$ definition. Note that $am^2+bmn+cn^2$ is minimized at $m = -bn/2a$, and the minimum is $dn^2/4a$. Since we have $|b| \leq a \leq \sqrt{d/3}$, we see that $4ac = b^2 + d \leq 4d/3$. Hence $d/4a \geq 3c/4$, so that $am^2 + bmn + cn^2 \geq 3cn^2/4$. Thus for each $n \geq 1$, we bound the contribution from each $|m| < 2n$ by

$$\frac{1}{(3cn^2/4)^{3/2}} \leq \frac{(4/3)^{3/2}}{a^{3/2}n^3}.$$

Hence the total contribution from these m and n is

$$\frac{(4/3)^{3/2}}{a^{3/2}} \sum_{n=1}^{\infty} \frac{(4n-1)}{n^3} \leq \frac{8.28}{a^{3/2}}.$$

For $|m| \geq 2n$, we note that $am^2 + bmn + cn^2 \geq am^2 + bmn \geq \frac{am^2}{2}$ since $a \geq |b|$. Hence the total contribution over m and n here is bounded by

$$\sum_{n=1}^{\infty} 2 \sum_{m=2n}^{\infty} \frac{2^{3/2}}{(am^2)^{3/2}} \leq \frac{2^{3/2}}{a^{3/2}} \sum_{n=1}^{\infty} \frac{1}{(2n-1)^2}.$$

Now this last sum is just $\pi^2/8$, so that this part is bounded by $3.49/a^{3/2}$. Adding up the three parts, we get the result of the lemma. If a is small, we could likely do better, but this is unnecessary for our purposes. □

The Dirichlet series $Z_Q(s)$ converges for $\operatorname{Re}(s) > 1$ and can be analytically continued to $\mathbf{C} \setminus \{1\}$; furthermore, we have that $(\sqrt{d}/2\pi)^s Z_Q(s)\Gamma(s)$ is invariant under the map $s \mapsto 1 - s$, and the residue at $s = 1$ is $\pi/\sqrt{d}$ (see [7], [34]). We define Dirichlet series coefficients $b_l^\star$ by

$$Z_Q(s) - \frac{\zeta(2s)}{a^s} = \sum_{l=1}^{\infty} \frac{b_l^\star}{l^s}.$$

Note that Lemma 1 implies that if $l \leq \sqrt{d/4}$, then $b_l^\star = 0$. Write $\delta(x)$ for the point-mass measure at x. Let

$$\mu = \sum_{l>0} b_l^\star \delta(l) \quad \text{and} \quad \nu = \pi\delta(\sqrt{d/4}) + \frac{\pi}{\sqrt{d}} \operatorname{Leb}\big([\sqrt{d/4}, \infty)\big), \tag{10}$$

where $\operatorname{Leb}\big([x, \infty)\big)$ is the standard Lebesgue measure restricted to the interval $[x, \infty)$. We have the following lemma.

Lemma 5. *With the above notation, for all $X \geq 0$ we have*

$$\int_0^X \int_0^{t_3} \int_0^{t_2} \left[\int_0^{t_1} \mu \right] dt_1\, dt_2\, dt_3 \leq \int_0^X \int_0^{t_3} \int_0^{t_2} \left[\int_0^{t_1} \nu \right] dt_1\, dt_2\, dt_3.$$

Note. Oesterlé [30] claims a version of this with only double integrals. He also has $\frac{\pi}{2}\delta(\sqrt{d/4})$ as the foremost term of ν. With more effort, the method below should work for triple integrals and Oesterlé's ν. Perhaps one could even get a singly integrated result by using more sophisticated lattice point counting methods. Unfortunately, the implicit constants in these methods are typically not very efficacious. The result here suffices for our purposes.

Proof. This is trivial for $X \le \sqrt{d/4}$, as the left-hand side is 0. We can rewrite the lemma statement as

$$\begin{aligned}(11)\qquad &\int_0^X \int_0^{t_3} \int_0^{t_2} \sum_{l \le t_1} b_l^\star \, dt_1 \, dt_2 \, dt_3 \\ &\qquad \le \int_{\sqrt{d/4}}^X \int_{\sqrt{d/4}}^{t_3} \int_{\sqrt{d/4}}^{t_2} \left[\pi + \frac{\pi}{\sqrt{d}}(t_1 - \sqrt{d/4})\right] dt_1 \, dt_2 \, dt_3.\end{aligned}$$

We first work with the left-hand side. By a thrice-integrated form of Perron's formula (see [16]), we see that the left-hand side is equal to

$$\frac{1}{2\pi i} \int_{(2)} \left[Z_Q(s) - \frac{\zeta(2s)}{a^s} \right] \frac{X^{s+3} \, ds}{s(s+1)(s+2)(s+3)}.$$

Here the $\int_{(2)}$ notation for the integral indicates the path $2 - i\infty$ to $2 + i\infty$. Moving the contour to $\operatorname{Re} s = -1/2$, we get contributions from the poles at $s = 1$, $s = 1/2$ and $s = 0$. The sums of these residues is equal to

$$\frac{\pi}{\sqrt{d}} \frac{X^4}{24} - \frac{X^{7/2}}{\sqrt{a}} \frac{8}{105} + \frac{Z_Q(0)}{6} X^3 - \frac{\zeta(0)}{6} X^3.$$

By the functional equation, we have $Z_Q(0) = 1/2$, while $\zeta(0) = -1/2$. Thus the last two terms sum to $X^3/6$. We next bound the integral on $\operatorname{Re} s = -1/2$. For the

$$\frac{1}{2\pi i} \int_{(-1/2)} \frac{Z_Q(s) X^{s+3} \, ds}{s(s+1)(s+2)(s+3)}$$

term, we use the functional equation to relate $Z_Q(-1/2 + it)$ with $Z_Q(3/2 - it)$. We get that the absolute value is bounded by

$$\frac{d}{4\pi^2} \frac{2}{2\pi} \int_0^\infty \left| \frac{\Gamma(3/2 + it)}{\Gamma(-1/2 - it)} \right| \left| \frac{X^{5/2} Z_Q^B(3/2)}{(-1/2 + it)(1/2 + it)(3/2 + it)(5/2 + it)} \right| dt,$$

where $Z_Q^B(3/2)$ is a bound for $Z_Q(s)$ on the line $\operatorname{Re} s = 3/2$. We have

$$\begin{aligned}|(-1/2 + it)(1/2 + it)\Gamma(-1/2 - it)| &= |(-1/2 + it)(1/2 + it)\Gamma(-1/2 + it)| \\ &= |\Gamma(3/2 + it)|,\end{aligned}$$

the first step following by the Schwarz Reflection Principle, while the second step follows from applying the functional equation $s\Gamma(s) = \Gamma(s + 1)$ twice. Hence the above becomes

$$\frac{d}{4\pi^3} X^{5/2} Z_Q^B(3/2) \int_0^\infty \frac{dt}{\sqrt{(9/4 + t^2)}\sqrt{(25/4 + t^2)}},$$

and the integral can be numerically bounded by $4/5$ (in fact, the integral is $\frac{2}{5}K(4/5)$ $\approx .7981211$ where $K(k) = \int_0^1 \frac{dt}{\sqrt{1-t^2}\sqrt{1-k^2t^2}}$ is the complete elliptic integral of the first kind; see [1]). Furthermore, from Lemma 2 we have $Z_Q^B(3/2) \le 13/a^{3/2}$. Hence

the contribution from this term is less than $dX^{5/2}/11a^{3/2}$. We move the contour of the term

$$\frac{-1}{2\pi i}\int_{(-1/2)}\frac{\zeta(2s)}{a^s}\frac{X^{s+3}\,ds}{s(s+1)(s+2)(s+3)}$$

to $\operatorname{Re} s = -3/4$; then its absolute value is less than

$$\frac{2a^{3/4}X^{9/4}}{2\pi}\int_0^\infty\left|\frac{\zeta(-3/2+2it)}{(-3/4+it)(1/4+it)(5/4+it)(9/4+it)}\right|dt.$$

We recall that $\zeta(s)\Gamma(s/2)\pi^{-s/2}$ is invariant under the $s\mapsto 1-s$ map, so that this is equivalent to

$$\begin{aligned}\frac{2a^{3/4}X^{9/4}}{2\pi}\int_0^\infty\frac{1}{\pi^2}\left|\frac{\Gamma(5/4+it)}{\Gamma(-3/4+it)}\right|\left|\frac{\zeta(5/2+2it)}{(-3/4+it)(1/4+it)(5/4+it)(9/4+it)}\right|dt\\ \le\frac{\zeta(5/2)}{\pi^3}a^{3/4}X^{9/4}\int_0^\infty\left|\frac{1}{(5/4+it)(9/4+it)}\right|dt\le .04a^{3/4}X^{9/4}.\end{aligned}$$

The last step is by numerical integration, the integral being $\frac{4}{9}K\left(\frac{2\sqrt{14}}{9}\right)\approx .916808$. Thus the left-hand side of (11) is less than

$$\frac{\pi}{\sqrt{d}}\frac{X^4}{24}-\frac{X^{7/2}}{\sqrt{a}}\frac{8}{105}+\frac{X^3}{6}+\frac{dX^{5/2}}{11a^{3/2}}+\frac{a^{3/4}X^{9/4}}{25}.$$

The right-hand side of (11) is trivially

$$\begin{aligned}&\frac{\pi(X-\sqrt{d/4})^3}{6}+\frac{\pi}{\sqrt{d}}\frac{(X-\sqrt{d/4})^4}{24}\\ &\quad=\frac{\pi X^4}{24\sqrt{d}}+\frac{\pi X^3}{12}-\frac{3\pi X^2\sqrt{d}}{16}+\frac{5\pi Xd}{48}-\frac{7\pi d^{3/2}}{384}.\end{aligned}$$

We put $a=\sqrt{d}/\kappa$ and $X=\lambda d/a=\kappa\lambda\sqrt{d}$. Note that since $a<\sqrt{d/3}$, we need only consider $\kappa>\sqrt{3}$. We see that the statement of the lemma holds if we can show that

$$-\frac{8\kappa^4\lambda^{7/2}}{105}+\frac{\kappa^3\lambda^3}{6}+\frac{\kappa^4\lambda^{5/2}}{11}+\frac{\kappa^{3/2}\lambda^{9/4}}{25}\le\frac{\pi\kappa^3\lambda^3}{12}-\frac{3\pi\kappa^2\lambda^2}{16}+\frac{5\pi\kappa\lambda}{48}-\frac{7\pi}{384}.$$

Calculus implies that the above inequality holds for $\kappa>\sqrt{3}$ and $\lambda\ge 9/4$. Hence the lemma is shown for $X\ge 9d/4a$.

We now consider $\sqrt{d/4}\le X=\rho d/4a$ where $\rho<9$. Here we shall show that

$$\sum_{l\le X}b_l^\star\le\pi+\frac{\pi}{\sqrt{d}}(X-\sqrt{d/4})=\frac{\pi}{2}+\frac{\pi X}{\sqrt{d}}\tag{12}$$

holds, and thus the statement of the lemma immediately follows, as (12) is the result if we integrate only once in the statement of the lemma instead of four times. We shall deal with the left-hand side by lattice point counting. For a reduced form $Q=(a,b,c)$, we wish to count the points with $am^2+bmn+cn^2\le X$, but we ignore the $n=0$ terms since these do not contribute to $b_l^\star$. Furthermore we only count terms with positive n, as the formula for $Z_Q(s)$ has a factor of $1/2$ to prevent double-counting.

Now for $n \geq 1$, we wish to count the number of integers m for which we have $am^2 + bmn + cn^2 \leq X = \rho d/4a$. By completing the square, this inequality is the same as

$$a\left(m^2 + \frac{bmn}{a} + \frac{b^2n^2}{4a^2}\right) \leq \frac{\rho d}{4a} - cn^2 + \frac{b^2n^2}{4a}$$

or

$$a\left(m + \frac{bn}{2a}\right)^2 \leq \frac{\rho d}{4a} - \frac{n^2}{4a}(4ac - b^2) = \frac{d}{4a}(\rho - n^2).$$

Thus we see that we need $n \leq \sqrt{\rho}$ for there to be any m-solutions. Furthermore, when $n \leq \sqrt{\rho}$, the number of m-solutions for a given n is bounded by $1 + \frac{\sqrt{d}}{a}\sqrt{\rho - n^2}$. Thus the number of lattice points (and hence the left-hand side of (12)) is bounded by

$$\sum_{n=1}^{\lfloor\sqrt{\rho}\rfloor}\left[1 + \frac{\sqrt{d}}{a}\sqrt{\rho - n^2}\right].$$

We wish to show that this is less than $\frac{\pi}{2} + \pi\rho\sqrt{d}/4a$. This is trivial for $\rho < 1$. We next claim that this is clear for $1 \leq \rho < 4$. In this range, we have one contributor to the sum. Since $1 \leq \pi/2$, we need only show that $\sqrt{\rho - 1} \leq \pi\rho/4$, which is easily verified. Now for $4 \leq \rho < 9$, we see that we wish to establish

$$2 + (\sqrt{\rho - 1} + \sqrt{\rho - 4})x \leq \frac{\pi}{2} + \frac{\pi}{4}\rho x$$

where $x = \sqrt{d}/a \geq \sqrt{3}$. Again this is routine via calculus, the relevant minimum occuring when $x = \sqrt{3}$ and $\rho = 4 + \phi^2 \approx 4.884$ where $\phi \approx .94038$ satifies the quartic equation $\pi^2\phi^4 - 4\pi\phi^3 + 3\pi^2\phi^2 - 12\pi\phi + 12 = 0$. Hence we have established the lemma for $X < 9d/4a$, and thus we have completed the proof. So Lemma 5 is shown. □

We next prove a couple of lemmata in the spirit of Oesterlé [30]. Our starting point is the inverse Mellin transform

$$\int_{(2)} x^{-s}\Gamma(s)\frac{ds}{2\pi i} = e^{-x}.$$

The idea shall be to get a factor of $(s - 1/2)$ into the denominator of the integral by integrating both sides of the above with respect to x. To this end we define (for $x > 0$)

$$\begin{aligned} I(x) = \int_{(2)} x^{-s}\frac{\Gamma(s)}{(s-1/2)}\frac{ds}{2\pi i} &= \frac{1}{\sqrt{x}}\int_{(2)}\int_x^\infty y^{-s-1/2}\,dy\,\frac{\Gamma(s)\,ds}{2\pi i} \\ &= \frac{1}{\sqrt{x}}\int_x^\infty\int_{(2)} y^{-s-1/2}\,\Gamma(s)\frac{ds}{2\pi i}\,dy \\ &= \frac{1}{\sqrt{x}}\int_x^\infty \frac{e^{-y}}{\sqrt{y}}\,dy, \end{aligned} \tag{13}$$

where the integral switch is justified by a theorem of Fubini (see [19]); the fact that the integrand is in $L^1(ds, dy)$ follows from the exponential decay of the Γ-function as the imaginary part heads to infinity. Note that $I(x)$ is strictly positive, and in fact for the kth derivative we have $(-1)^k I^{(k)}(x) > 0$ for all x. Also, as $x \to \infty$ we have $|I^{(k)}(x)| \ll_k e^{-x}/x$ and as $x \to 0$ we have $|I^{(k)}(x)| \ll_k 1/x^{k+1/2}$. These

assertions are all easily established by induction. In the sequel, we shall only need these facts for $0 \le k \le 4$.

We next turn to an integral transform used by Oesterlé [30]. Let α be a nonnegative measure on $\mathbf{R}_+ = [0,\infty)$, with

$$\alpha\big([0,y]\big) \ll y \quad \text{as } y \to \infty, \qquad \text{and} \qquad \alpha\big([0,y]\big) \ll e^{-1/y} \quad \text{as } y \to 0. \tag{14}$$

These are not the optimal conditions on α, but they will suffice for our purposes. We next define the function $P_s : t \mapsto t^{-s}$, and for $\operatorname{Re} s > 1$ note that P_s is integrable with respect to α. We let $\hat{\alpha}(s) = \int_{\mathbf{R}_+} P_s \alpha$ and define the function $\tilde{I}_y : t \mapsto I(yt)$. Finally we define

$$E_\alpha(y) = \int_{(2)} \frac{\Gamma(s)}{(s-1/2)} y^{-s} \hat{\alpha}(s) \frac{ds}{2\pi i} = \int_{\mathbf{R}_+} \tilde{I}_y \alpha, \tag{15}$$

where again the validity of the integral switch follows Fubini's theorem and the conditions (14). We have the following lemma:

Lemma 6. *Suppose that μ and ν are nonnegative measures on $[0,\infty)$ satisfying (14) with*

$$\int_0^Y \int_0^{t_3} \int_0^{t_2} \left[\int_0^{t_1} \mu \right] dt_1\, dt_2\, dt_3 \le \int_0^Y \int_0^{t_3} \int_0^{t_2} \left[\int_0^{t_1} \nu \right] dt_1\, dt_2\, dt_3$$

for all $Y \ge 0$. Then we have $E_\mu(y) \le E_\nu(y)$ for all $y > 0$.

Proof. We define $\mu^1(u) = \int_0^u \mu$, and recursively $\mu^{l+1}(u) = \int_0^u \mu^l(t)\, dt$ for $l \ge 1$. We then integrate $E_\mu(y) = \int_{\mathbf{R}_+} \tilde{I}_y \mu$ by parts four times. This gives

$$\begin{aligned} E_\mu(y) = I(yt)\mu^1(t) \Big|_{t=0}^{\infty} - I'(yt)\mu^2(t) \Big|_{t=0}^{\infty} + I''(yt)\mu^3(t) \Big|_{t=0}^{\infty} - I'''(yt)\mu^4(t) \Big|_{t=0}^{\infty} \\ + \int_0^\infty I''''(yt)\mu^4(t)\, dt. \end{aligned}$$

Here the derivatives are with respect to t. A similar formula holds for $E_\nu(y)$. The conditions (14) on μ and ν and the behaviour of the derivatives of $I(x)$ at 0 and infinity imply that the first four terms are all zero. Hence we need only show that

$$\int_0^\infty I''''(yt)\mu^4(t)\, dt \le \int_0^\infty I''''(yt)\nu^4(t)\, dt,$$

which is obvious since the assumption of the lemma implies that $\mu^4(t) \le \nu^4(t)$ while we recall that $I''''(yt)$ is nonnegative. This proves the lemma. □

Note that Lemma 5 verifies the hypothesis of Lemma 6 for the μ and ν we have defined in (10), with the conditions (14) following from the easily verified fact (e.g., using Perron's formula as in Lemma 5) that $\sum_{l \le Y} b_l^\star \sim \pi Y/\sqrt{d}$ as $Y \to \infty$. Thus we have

$$E_\mu(y) = \int_{(2)} \frac{\Gamma(s)}{(s-1/2)} y^{-s} \hat{\mu}(s) \frac{ds}{2\pi i} \le E_\nu(y) = \int_{(2)} \frac{\Gamma(s)}{(s-1/2)} y^{-s} \hat{\nu}(s) \frac{ds}{2\pi i}$$

where (for a given form Q)

$$\hat{\mu}(s) = Z_Q(s) - \frac{\zeta(2s)}{a^s} \quad \text{and} \quad \hat{\nu}(s) = \frac{\pi}{2} \frac{2s-1}{s-1} \frac{2^s}{d^{s/2}}.$$

Lemma 7. *Let $\xi \geq 0$ and $x > 0$. Then*

$$\int_{(2)} x^s \Gamma(s) \frac{(s-1/2)}{(s-1/2)^2+\xi^2} \frac{ds}{2\pi i} = \int_{1/x}^{\infty} \frac{e^{-t}}{t} \sqrt{xt} \cos(\xi \log xt)\, dt.$$

Proof. This is probably just an exercise, but there is a delicacy, as blindly unraveling the Γ-function in the left-hand-side followed by a switch of integrals seems not to be valid. Call the left-hand side $F(x,\xi)$, and take its derivative with respect to ξ. Differentiating under the integral sign is justified as in [19]. This gives

$$\begin{aligned} F'(x,\xi) &= \int_{(2)} x^s \Gamma(s) \frac{(s-1/2)(-2\xi)}{\left[(s-1/2)^2+\xi^2\right]^2} \frac{ds}{2\pi i} \\ &= \int_0^{\infty} \frac{e^{-t}}{t} \int_{(2)} (xt)^s \frac{(s-1/2)(-2\xi)}{\left[(s-1/2)^2+\xi^2\right]^2} \frac{ds}{2\pi i}\, dt, \end{aligned}$$

as the second step is now justifiable. We now evaluate the inner integral by moving the contour off to infinity either to the right or left. If $xt \leq 1$, we move it to the right and get 0 for the integral, while if $xt \geq 1$, moving the contour all the way to the left picks up the two poles on the half-line. Thus we have

$$\begin{aligned} F'(x,\xi) &= -\int_{1/x}^{\infty} \frac{e^{-t}}{t} \sqrt{xt} \log(xt) \frac{(xt)^{i\xi} - (xt)^{-i\xi}}{2i}\, dt \\ &= -\int_{1/x}^{\infty} \frac{e^{-t}}{t} \sqrt{xt} \log(xt) \sin(\xi \log xt)\, dt. \end{aligned}$$

Integrating with respect to ξ (again with the integral switch justified) gives the result up to a constant of integration, which is seen to be zero as in (13). Hence the lemma is proven. □

We now give a method of constructing admissible choices for $A(s)$. Recall the definition of an admissible Dirichlet series $A(s)$ given with (6) and that

$$\sum_{n=1}^{\infty} \frac{R(n)}{n^s} = \frac{\zeta(s)L(s,\chi_{-d})}{\zeta(2s)}, \qquad \sum_{a \in M_d} \frac{1}{a^s} = \sum_{n=1}^{\infty} \frac{\tilde{R}(n)}{n^s},$$

and

$$R^{\star}(n) = R(n) - \tilde{R}(n).$$

Lemma 8. *Let $-d$ and k be fundamental discriminants with $g = \gcd(k,d)$ odd. Let $\mathbf{P}$ be a set of primes, $\mathbf{P}^{\star}$ the positive integers which have all of their prime factors in $\mathbf{P}$, and $\mathbf{Q}$ the sub-multi-set of M_d consisting of minima that have no prime factor which is in $\mathbf{P}$ (note that $1 \in \mathbf{Q}$). Define*

$$A(s) = \prod_{p \in \mathbf{P}} G_p(s) \cdot \sum_{a \in \mathbf{Q}} \frac{\chi^{\star}(a)}{a^s} = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} \tag{16}$$

where $\chi^{\star}(n)$ is the completely multiplicative function defined by $\chi^{\star}(q) = (-kd/g^2|q)$ for a prime q with $q|g$ and $\chi^{\star}(q) = (k|q)$ otherwise. Under these conditions, $A(s)$ is an admissible Dirichlet series.

Proof. By comparison of Euler products (indeed, this was the reason to define $G(s)$ as we did) we have $\zeta(2s)P_{k/g}(s)G(s) = L(s,\chi_k)L(s,\chi_{-kd/g^2})$. Thus (writing $G(s) = \sum_n g(n)/n^s$ as before) it follows that $g(n) = \chi^{\star}(n)R(n)$ where $R(n)$ is as

above. For $A(s)$ to be admissible, we need verify for each n that $|g(n)-a(n)| \le R^\star(n)$. There is a natural division of n's into two types. The first are the n which cannot be written as uv with $u \in \mathbf{P}^\star$ and $v \in \mathbf{Q}$. We have $a(n)=0$ in this case and also that $n \notin M_d$. The fact that $n \notin M_d$ implies that $R^\star(n)=R(n)$, whence the admissibility condition holds for these n. We next consider the n which can be written as uv in the manner indicated above. We have $a(n)=g(u)\chi^\star(v)\tilde{R}(v)$. Note that $g(v)$ and $\chi^\star(v)\tilde{R}(v)$ do not have differing signs, though one or both could be zero. Thus $a(n)$ and $g(u)g(v)$ do not have differing signs, and the latter is $g(n)$ since $\gcd(u,v)=1$. So $|g(n)-a(n)| \le |g(n)| \le R(n)$. When $n \ge \sqrt{d/3}$, this gives us admissibility, since we then have $R(n)=R^\star(n)$. Thus we are left with the $n \le \sqrt{d/3}$. When $v \le \sqrt{d/4}$, we recall that (2) implies $R(v)=\tilde{R}(v)$ and thus $\chi^\star(v)\tilde{R}(v)=\chi^\star(v)R(v)=g(v)$. So we have $a(n)=g(u)\chi^\star(v)\tilde{R}(v)=g(u)g(v)=g(n)$, implying the admissibility condition in this subcase. Finally we have the case where $n \le \sqrt{d/3}$ and $v \ge \sqrt{d/4}$. Necessarily we must have $u=1$ in this instance. Thus $a(n)=\chi^\star(n)\tilde{R}(n)$ and so $g(n)-a(n)=\chi^\star(n)R^\star(n)$, again giving the admissibility condition. This shows the lemma. □

Lemma 9. *Suppose that $A(s)$ is admissible in the sense of the above. Define Dirichlet series coefficients from $[G(s)-A(s)]\zeta(2s)P_{k/g}(s)=\sum_l h(l)/l^s$ and*

$$\zeta(s)L(s,\chi_{-d}) - \sum_{(a,b,c)\in Q_d} \frac{\zeta(2s)}{a^s} = \sum_{(a,b,c)\in Q_d} \sum_{m\in\mathbf{Z}} \sum_{n>0} \frac{1}{(am^2+bmn+cn^2)^s} = \sum_{l=1}^{\infty} \frac{H(l)}{l^s}.$$

Then $|h(l)| \le H(l)$ for all l.

Proof. We multiply $[G(s)-A(s)]$ by $\zeta(2s)P_{k/g}(s)$ and $\sum_r R^\star(r)/r^s$ by $\zeta(2s)$ to get

$$h(l)=\sum_{p^2|l}{}^\star [g(l/p^2)-a(l/p^2)] \quad \text{and} \quad H(l)=\sum_{p^2|l} R^\star(l/p^2),$$

where the star in the first sum prohibits p which divide k/g, and the $H(l)$-equality holds as in Lemma 2. Taking absolute values and using admissibility implies the second claim of the lemma. □

5. Proof of the key inequality

We next do the proof of the key inequality (9). Using this inequality, we shall then eliminate large ranges of d's from consideration. This lemma is fairly general and could be used for attacks on larger class numbers.

Lemma 10. *Let $-d$ be a fundamental discriminant. Let the ξ_i's be defined as in (8) and $G(s)$ as in (6), and let $A(s)$ be admissible in the sense above. Let χ_k be a real primitive character modulo $|k|$ with k odd. Let $L(s,\chi_k)$ have a zero at $s=1/2+i\xi_0$ (with $0 \le \xi_0 < 0.21$). Let $g=\gcd(d,k)$ and suppose that either $g=|k|$ or $|k| \ge \pi g$. Writing $\xi_1=\xi_0/2$, we then have*

$$\xi_3 |A(1/2+i\xi_0)| \big|\sin[\xi_1 \log d + \xi_2 + \arg A(1/2+i\xi_0)]\big| \le U^B_{k,d} \tag{17}$$

where

$$U^B_{k,d} = W_{k,d} + \sum_{a\in Q_d} \min(V^G_{k,d}, V^S_{k,d}(a)) \qquad \text{where} \quad V^G_{k,d} = \frac{2\sqrt{2\pi}}{d^{1/4}} \sqrt{\frac{|k|}{g}} e^{-\pi g/|k|}$$

and

$$V^S_{k,d}(a) = \frac{2\sqrt{2\pi}}{d^{1/4}}\sqrt{\frac{g}{|k|}}\left(\sum_{n=1}^{\infty}(1+2\beta n)I^\star\left(\frac{\pi g\beta n^2}{|k|}\right) + 2\sum_{n=1}^{\infty}\left\lfloor\frac{n}{\beta}\right\rfloor I^\star\left(\frac{\pi g\gamma n^2}{|k|}\right)\right)$$

where $I^\star(x) = \min\bigl(e^{-x}/x, \sqrt{\pi/x}\bigr)$, $\beta = \sqrt{d}/2a$, $\gamma = (1-1/2\beta)^2/\beta$, *and*

$$W_{k,d} = \left|\frac{2}{2\pi i}\int_{(1/4)}\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{s-1/2}\frac{\Gamma(s)A(s)P_{k/g}(s)\zeta(2s)(s-1/2)}{(s-1/2+i\xi_0)(s-1/2-i\xi_0)}\,ds\right|.$$

Proof. Since d is fundamental and $d<0$, we have $(-d|-1) = -1$. This implies that $(k|-1) = -(-kd|-1)$, so that χ_k and χ_{-kd/g^2} have different Γ-factors in their functional equations. So from the functional equation for Dirichlet L-functions, we have that

$$\left(\frac{|k|}{\pi}\right)^{s/2}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi_k)\cdot\left(\frac{|k|d}{\pi g^2}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)L(s,\chi_{-kd/g^2})$$

is invariant under the $s\mapsto 1-s$ map. We recall Legendre's duplication formula for $\Gamma(s)$, namely that $2\sqrt{\pi}\Gamma(s) = 2^s\Gamma(s/2)\Gamma\bigl((s+1)/2\bigr)$. Using this, we see that $\bigl(|k|\sqrt{d}/2\pi\bigr)^s\Gamma(s)L(s,\chi_k)L(s,\chi_{-kd/g^2})$ is also invariant under the $s\mapsto 1-s$ map. From this we can deduce that

(18)
$$\frac{2}{2\pi i}\int_{(2)}\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{s-1/2}L(s,\chi_k)L(s,\chi_{-kd/g^2})\frac{\Gamma(s)(s-1/2)\,ds}{(s-1/2+i\xi_0)(s-1/2-i\xi_0)} = 0.$$

This follows from moving the contour to $\operatorname{Re} s = 1/2$ and using symmetry. Here the integrand is entire since $L(1/2\pm i\xi_0,\chi_k) = 0$. As in Lemma 8, we have $L(s,\chi_k)L(s,\chi_{-kd/g^2}) = G(s)P_{k/g}(s)\zeta(2s)$ by comparison of Euler products. We insert this into (18). Our idea shall be to get a main term by replacing $G(s)$ by $A(s)$ and then to bound the residual term induced by $[G(s)-A(s)]$. Hence we replace $G(s)$ by $A(s)$ and evaluate

$$\frac{2}{2\pi i}\int_{(2)}\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{s-1/2}A(s)P_{k/g}(s)\zeta(2s)\frac{\Gamma(s)(s-1/2)\,ds}{(s-1/2+i\xi_0)(s-1/2-i\xi_0)}$$

via residue theory, moving the line of integration to $\operatorname{Re} s = 1/4$. The residues from the poles give a contribution

$$\begin{aligned}&\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{i\xi_0}\Gamma\left(\frac{1}{2}+i\xi_0\right)A\left(\frac{1}{2}+i\xi_0\right)P_{k/g}\left(\frac{1}{2}+i\xi_0\right)\zeta(1+2i\xi_0)\\ &\quad+\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{-i\xi_0}\Gamma\left(\frac{1}{2}-i\xi_0\right)A\left(\frac{1}{2}-i\xi_0\right)P_{k/g}\left(\frac{1}{2}-i\xi_0\right)\zeta(1-2i\xi_0),\end{aligned}\tag{19}$$

which in the notation of (5) is $T(1/2+i\xi_0)+T(1/2-i\xi_0)$. From (7), we see that this is the left-hand side of (17), while the resulting integral on the 1/4-line becomes the $W_{k,d}$ term of the lemma statement.

We now wish to bound the residual term (using R to denote its absolute value)

$$\frac{2}{2\pi i}\int_{(2)}\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{s-1/2}[G(s)-A(s)]P_{k/g}(s)\zeta(2s)\frac{\Gamma(s)(s-1/2)\,ds}{(s-1/2+i\xi_0)(s-1/2-i\xi_0)}.$$

If we write $[G(s)-A(s)]P_{k/g}(s)\zeta(2s)=\sum_l h(l)/l^s$, this becomes

$$\frac{2}{2\pi i}\int_{(2)}\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^{s-1/2}\sum_{l=1}^{\infty}\frac{h(l)}{l^s}\frac{\Gamma(s)(s-1/2)\,ds}{(s-1/2)^2+\xi_0^2}$$
$$=\frac{\sqrt{2\pi g}}{\sqrt{|k|}d^{1/4}}\sum_{l=1}^{\infty}h(l)\cdot\frac{2}{2\pi i}\int_{(2)}\left(\frac{|k|\sqrt{d}}{2\pi gl}\right)^{s}\frac{\Gamma(s)(s-1/2)\,ds}{(s-1/2)^2+\xi_0^2}.$$

The interchange of sum and integral is justified since $\sum_{l\le Y}|c(l)|\ll Y$ as $Y\to\infty$ as before. Putting $x=|k|\sqrt{d}/2\pi gl$ and using Lemma 7, we get

$$R\le\left|\frac{2\sqrt{2\pi g}}{\sqrt{|k|}d^{1/4}}\sum_{l=1}^{\infty}h(l)\int_{1/x}^{\infty}\frac{e^{-t}}{t}\sqrt{xt}\cos(\xi_0\log xt)\,dt\right|$$
$$\le\frac{2\sqrt{2\pi g}}{\sqrt{|k|}d^{1/4}}\sum_{l=1}^{\infty}H(l)\int_{1/x}^{\infty}\frac{e^{-t}}{t}\sqrt{xt}\,dt=\frac{2\sqrt{2\pi g}}{\sqrt{|k|}d^{1/4}}\sum_{l=1}^{\infty}H(l)I\left(\frac{2\pi gl}{|k|\sqrt{d}}\right).$$

where the $H(l)$ (as in Lemma 9) bound the $h(l)$ in absolute value and $I(x)$ is as in (13). We next split this sum over forms $(a,b,c)\in Q_d$. From the definition of the $H(l)$ in Lemma 9 we have

$$\begin{aligned}R&\le\frac{2\sqrt{2\pi g}}{\sqrt{|k|}d^{1/4}}\sum_{(a,b,c)\in Q_d}\sum_{m_1\in\mathbf{Z}}\sum_{m_2>0}I\left(\frac{2\pi g(am_1^2+bm_1m_2+cm_2^2)}{|k|\sqrt{d}}\right)\\&=\frac{2\sqrt{2\pi g}}{\sqrt{|k|}d^{1/4}}\sum_{(a,b,c)\in Q_d}T\big((a,b,c)\big).\end{aligned}\tag{20}$$

We shall bound $T\big((a,b,c)\big)$ in two ways, obtaining the generic bound $V_{k,d}^G$ and the specific bound $V_{k,d}^S(a)$.

The specific bound is derived by using lattice-point counting as in Lemma 5. Writing $\beta=\sqrt{d/4}/a$, we see (similar to Lemma 4) that the quadratic form $am_1^2+bm_1m_2+cm_2^2$ is given by

$$\sqrt{d/4}\left[\beta m_2^2+\frac{1}{\beta}\left(m_1+\frac{bm_2}{2a}\right)^2\right].$$

For $|m_1|\le\beta m_2$, we lower-bound the above simply by $\beta m_2^2\sqrt{d/4}$, and for $|m_1|\ge\beta m_2$, we use the fact that $|b|\le a$ to derive a lower-bound of $m_1^2\sqrt{d/4}\cdot(1-1/2\beta)^2/\beta=\gamma m_1^2\sqrt{d/4}$. Hence (since I is decreasing)

$$\begin{aligned}T\big((a,b,c)\big)&\le\sum_{m_2=1}^{\infty}\big(1+2\beta m_2\big)I\left(\frac{\pi g\beta m_2^2}{|k|}\right)+2\sum_{m_2=1}^{\infty}\sum_{m_1\ge\beta m_2}^{\infty}I\left(\frac{\pi g\gamma m_1^2}{|k|}\right)\\&\le\sum_{m_2=1}^{\infty}\big(1+2\beta m_2\big)I\left(\frac{\pi g\beta m_2^2}{|k|}\right)+2\sum_{m_1=1}^{\infty}\left\lfloor\frac{m_1}{\beta}\right\rfloor I\left(\frac{\pi g\gamma m_1^2}{|k|}\right).\end{aligned}\tag{21}$$

Noting that

$$I(x)=\frac{1}{\sqrt{x}}\int_x^{\infty}\frac{e^{-t}}{\sqrt{t}}\,dt\le\frac{e^{-x}}{x}\quad\text{and}\quad I(x)\le\frac{1}{\sqrt{x}}\int_0^{\infty}\frac{e^{-t}}{\sqrt{t}}\,dt=\sqrt{\pi/x},$$

we multiply by $2\sqrt{2\pi g}/\sqrt{|k|}d^{1/4}$ and get the bound $V_{k,d}^S(a)$ in the statement of the lemma as desired.

For the generic bound we reinterpret $T\big((a,b,c)\big)$ in the spirit of (10) and (15) as $E_\mu\big(2\pi g/|k|\sqrt{d}\big)$, where

$$\mu = \sum_{l=1}^{\infty} b_l^\star \delta(l) \qquad \text{where} \quad \sum_{l=1}^{\infty} \frac{b_l^\star}{l^s} = Z_Q(s) - \frac{\zeta(2s)}{a^s}.$$

Now by Lemmata 5 and 6, we can upper-bound E_μ by E_ν where

$$\nu = \pi\delta\big(\sqrt{d/4}\big) + \frac{\pi}{\sqrt{d}}\mathrm{Leb}([\sqrt{d/4},\infty)).$$

Note that ν is *independent* of (a,b,c). We have $T\big((a,b,c)\big) = E_\mu\big(2\pi g/|k|\sqrt{d}\big) \le E_\nu\big(2\pi g/|k|\sqrt{d}\big)$, and again we rewrite this as an integral using (15). Recalling that $\hat\nu(s) = \frac{\pi}{2}\frac{2s-1}{s-1}\frac{2^s}{d^{s/2}}$, we have

$$\begin{aligned} T\big((a,b,c)\big) &\le \int_{(2)} \frac{\Gamma(s)}{s-1/2}\left(\frac{|k|\sqrt{d}}{2\pi g}\right)^s \frac{\pi}{2}\frac{2s-1}{s-1}\frac{2^s}{d^{s/2}}\frac{ds}{2\pi i} \\ &= \pi\int_{(2)} \frac{\Gamma(s)}{s-1}\left(\frac{|k|}{\pi g}\right)^s \frac{ds}{2\pi i} = \frac{|k|}{g}e^{-\pi g/|k|}, \end{aligned} \tag{22}$$

and multiplication by $2\sqrt{2\pi g}/\sqrt{|k|}d^{1/4}$ gives the $V_{k,d}^G$ term. By combining equations (18), (19), (20), (21) and (22), we derive the statement of Lemma 9. □

6. Eliminating large discriminants

We shall first get bounds on the distribution of minima assuming the class number is small, recalling the definition of types of primes preceding Lemma 3.

Lemma 11. *Let $-d < 4$ be a fundamental discriminant, and put $D = \sqrt{d/4}$. Let m_0 be the number of Type I primes less than $D^{1/4}$ and m_1 the number of Type I primes greater than $D^{1/4}$. For Type II primes, let n_0 be the number of such primes less than $D^{1/4}$, n_1 the number between $D^{1/4}$ and $D^{1/2}$, n_2 the number greater than $\sqrt{D}$ (excluding the Type IIb primes), and let n_3 be the number of Type IIb primes. Then we have*

$$\begin{aligned} h \ge\ & 1 + m_0 + m_1 + 2n_0 + 2n_1 + 2n_2 + n_3 + 2n_0 + 2n_1 + 2n_0 + 2n_0 \\ & + \binom{m_0}{2} + 2m_0n_0 + 2m_0n_1 + 4\binom{n_0}{2} + 4n_0n_1 + 4\binom{n_1}{2} + 2m_0n_0 \\ & + 2\cdot 4\binom{n_0}{2} + 4n_0n_1 + 4\binom{n_0}{2} + 2m_0n_0 + 2\cdot 4\binom{n_0}{2} \\ & + \binom{m_0}{3} + 2\binom{m_0}{2}n_0 + 2\binom{m_0}{2}n_1 + 4m_0\binom{n_0}{2} + 4m_0n_0n_1 \\ & + 8\binom{n_0}{3} + 8\binom{n_0}{2}n_1 + 2\binom{m_0}{2}n_0 + 2\cdot 4m_0\binom{n_0}{2} + 3\cdot 8\binom{n_0}{3} \\ & + \binom{m_0}{4} + 2n_0\binom{m_0}{3} + 4\binom{n_0}{2}\binom{m_0}{2} + 8m_0\binom{n_0}{3} + 16\binom{n_0}{4}. \end{aligned}$$

Proof. This comes from nothing but the multiplicativity of minima when their product is less than D (see Lemma 3), the rest being straightforward bookkeeping. The first line accounts for all possible products of zero or one powers of prime

minima, while the second and third lines account for possible products of two powers of minima, etc. This proves the lemma. □

Next we get large ranges of d where the class number cannot be small. We first note that we can get an upper bound on the possible size of d with $h(-d) \le 100$ by using the result of Oesterlé [30]. By Gauss's theory of genera, there are at most 7 primes dividing d. Thus Oesterlé's result implies that if $h(-d) \le 100$, then

$$\log d \le (7000)(100) \prod_{p \le 13} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right)^{-1} \le 268800000.$$

One can do better by using the traces of Frobenius from the elliptic curve used in Oesterlé's proof (or by considering the case where $\gcd(d, 5077) = 1$ separately with a different elliptic curve), but such a gain is not very important. The main significance of this result is that it gives an upper bound on the size of d. We shall handle the fundamental discriminants d with $2^{162} \le d \le e^{268800000}$ by using Lemma 10. It is really no difficulty to go much higher on the upper range of d here. The idea is that the condition of Lemma 10 eliminates large periodic ranges of $\log d$ from consideration. Only if the sine term on the left-hand side of (17) is nearly zero can h possibly be small. If we use many auxiliary moduli k, the sine is unlikely to be near zero for all of them. Using seventeen moduli k with low height zeros, we eliminate these possibilities:

Lemma 12. *If $2^{162} \le d \le \exp(268800000)$, then $h(-d) > 100$. By the work of Oesterlé, we need not consider larger d, and thus if $h(-d) \le 100$, we have $d \le 2^{162}$.*

Proof. We shall take $A(s) = \prod_p G_p(s)$ where the product is over primes of Type I, II, or IIb. This choice of $A(s)$ is admissible by Lemma 8. We assume that $\gcd(d, k) = g = 1$ and simply bound the $W_{k,d}$ term in Lemma 10 by

$$\begin{aligned} W_{k,d} &\le 2\left(\frac{2\pi}{|k|\sqrt{d}}\right)^{1/4} A_{UB} \prod_{p|k} \left(1 + \frac{1}{p^{1/2}}\right) \\ &\quad \times \frac{2}{2\pi} \int_0^\infty \left| \Gamma(1/4 + it)\zeta(1/2 + 2it) \frac{t^2 + 1/16}{(\xi_0^2 - t^2 + 1/16)^2 + t^2/4} \right| dt \\ &\le 11\left(\frac{2\pi}{|k|\sqrt{d}}\right)^{1/4} A_{UB} \prod_{p|k} \left(1 + \frac{1}{p^{1/2}}\right), \end{aligned} \tag{23}$$

where A_{UB} is an upper bound for $A(s)$ on the line $\operatorname{Re} s = 1/4$. Here the integral in the second line of (23) can be bounded in absolute value by 17 (maximized at $\xi_0 = 0$) using analytic estimates on $\Gamma(s)$ and $\zeta(s)$ to bound the tails. We first turn to a sublemma involving the size of minima.

Sublemma 12.1. *Suppose $d \ge 2^{162}$ and $h(-d) \le 100$. Let $\operatorname{Re} s = 1/2$. Then we have*

$$|A(s)| \ge .016, \qquad A_{UB} \le 62, \quad \text{and} \quad \left|\frac{A'}{A}(s)\right| \le 8.31.$$

Proof. We shall use the notation $D = \sqrt{d/4}$ throughout the remainder of the paper. In this case, we have $D \ge 2^{80}$. We first note that neither 2 nor 3 can be a Type II

prime, since its powers would create more than 100 minima by multiplicativity by Lemma 3 (since $3^{50} \le D$). We define

$$P(p) = 1 - \frac{1}{\sqrt{p}}, \qquad Q(p) = \frac{1 - 1/\sqrt{p}}{1 + 1/\sqrt{p}}, \qquad L(p) = \frac{\log p}{\sqrt{p} - 1},$$

$$R(p) = 1 + \frac{1}{p^{1/4}}, \qquad \text{and} \qquad S(p) = \frac{1 + 1/p^{1/4}}{1 - 1/p^{1/4}}.$$

Let m_0, n_0, etc., be as in Lemma 10. By the theory of genera there are no more than seven Type I primes (see discussion after Lemma 3). And any purported seventh must be at least $d^{1/7}/4$, so that $m_0 \le 6$. We recall from (6) that when $\gcd(d, k) = 1$, we have that

$$A(s) = \prod_{\substack{p \text{ of Type} \\ \text{I, II or IIb}}} \frac{1 + \chi_k(p)/p^s}{1 - \chi_{-kd}(p)/p^s}.$$

From this, we see that we have (for any real t)

$$|A(1/2 + it)| \ge \prod_{\substack{\text{first } m_0 \\ \text{primes}}} P(p) \cdot P(D^{1/4})^{(7-m_0)} Q(5)^{n_0} Q(D^{1/4})^{n_1} Q(D^{1/2})^{50} Q(D)^{50}$$

$$\left|\frac{A'}{A}(1/2 + it)\right| \le \sum_{\substack{\text{first } m_0 \\ \text{primes}}} L(p) + (7 - m_0) L(D^{1/4})$$

$$+ \; 2n_0 L(5) + 2n_1 L(D^{1/4}) + 100 L(D^{1/2}) + 100 L(D)$$

$$A_{UB} \le \prod_{\substack{\text{first } m_0 \\ \text{primes}}} R(p) \cdot R(D^{1/4})^{(7-m_0)} S(5)^{n_0} S(D^{1/4})^{n_1} S(D^{1/2})^{50} S(D)^{50}. \tag{24}$$

Here the stray $Q(D)^{50}$ term (and others of that sort) comes from the possibility of Type IIb primes; it will have little effect. We are now set to use Lemma 11. Under the assumption that $h(-d) \le 100$, Lemma 11 gives us an upper bound on n_1 for a given (m_0, n_0) pair. We enumerate the various extermal (m_0, n_0, n_1) triples, and verify the conclusion of the lemma in each case.

Various gains can be made compared to above simplistic accounting, such as noting that when $m_0 \ge 3$, we can gain a little since a small prime like 5 cannot be both a Type I and Type II prime, but these minutiae are unneeded at the current time. The sublemma is shown, as can be evinced from Table 2. □

TABLE 2.

m_0	n_0	n_1	$\lvert A\rvert_L$	$\lvert A'/A\rvert^U$	A_{UB}	m_0	n_0	n_1	$\lvert A\rvert_L$	$\lvert A'/A\rvert^U$	A_{UB}	m_0	n_0	n_1	$\lvert A\rvert_L$	$\lvert A'/A\rvert^U$	A_{UB}
0	0	6	.981	.261	2	1	2	0	.042	6.97	62	4	0	3	.042	5.79	13
0	1	4	.376	2.82	9	2	0	5	.121	3.39	6	4	1	0	.016	8.31	54
0	2	1	.144	5.34	37	2	1	2	.046	5.91	24	5	0	1	.029	6.76	17
1	0	6	.287	1.92	4	3	0	4	.067	4.65	9	6	0	0	.021	7.70	24
1	1	3	.110	4.45	15	3	1	1	.025	7.17	37						

We now prove Lemma 12. By Lemma 10, we have

$$\bigl|\sin\bigl[\xi_1 \log d + \xi_2 + \arg A(1/2 + i\xi_0)\bigr]\bigr| \le \frac{U^B_{k,d}}{\xi_3 |A(1/2 + i\xi_0)|}, \tag{25}$$

where $U^B_{k,d}$ is as stated in the lemma. We assume $d \ge 2^{162}$, $h(-d) \le 100$, and k is one of the last seventeen moduli in Table 1 with $\gcd(d,k) = 1$. Using the sublemma-bound for the $A(s)$-quantities along with the implied bounds on k and d, we conclude from Lemma 10 and (23) (with $W_{k,d}$ being the biggest term) that

$$\begin{aligned} U^B_{k,d} &\le 11 \cdot \left(\frac{2\pi}{115147 \cdot \sqrt{2^{162}}}\right)^{1/4} \cdot 62 \cdot \left(1 + \frac{1}{\sqrt{3}}\right)\left(1 + \frac{1}{\sqrt{610921}}\right) \\ &\quad + \frac{200\sqrt{2\pi \cdot 175990483}}{2^{162/4}} \\ &\le .00002. \end{aligned}$$

Now $\xi_3 \ge 314$ for all of our k, and thus we see that

$$\bigl|\sin[\xi_1 \log d + \xi_2 + \arg A(1/2 + i\xi_0)]\bigr| \le \frac{.00002}{(314)(.016)} \le 0.000004.$$

Furthermore, since $\xi_0 \le .0049$ for each of the moduli, we have (see e.g., [3] for the first step)

$$|\arg A(1/2 + i\xi_0)| \le \xi_0 \left|\frac{A'}{A}(1/2 + i\xi_0)\right| \le (.0049)(8.41) \le .042.$$

Exploiting the near-linearity of the sine function near zero, it is easy to derive that for (25) to be true, we must have

$$\bigl|\sin[\xi_1 \log d + \xi_2]\bigr| \le .043. \tag{26}$$

Thus k eliminates periodic ranges of $\log d$ from consideration; only when $(\xi_1 \log d + \xi_2)$ is close to a multiple of π could we possibly have $h(-d)$ be small. If a fundamental discriminant satisfies (26) for a given k, we say that k **misses** d. We list below the ranges of d which each k misses, noting also the factorisation of k.

Here the Miss Period column records the period of the exponents (to base 10) that each k misses; the Miss Period is simply $\pi/\bigl(\xi_1 \log 10\bigr)$. The Shift column records the relative difference from the multiples of the Miss Period. The listed value for the Shift is in general a rather conservative bounding. Table 3 works as follows: for $k = -1832763$ and $p = 943.7375432$, the table tells us that if $2^{162} \le d \le \exp(268800000)$ and $\gcd(k,d) = 1$, then we can conclude that the left-hand side of (26) is greater than .043 for all d which are not in some interval of the form $10^{mp-25} \le d \le 10^{mp+10}$ for some integer m. For these d we can hence assert that $h(-d) > 100$. Thus for each k, we get periodic ranges of d which cannot have small class number. It is in this step that we require the 13-digit precision on the location of the zeros of the L-functions.

It is now a routine computer check (less than five hours) to ensure that each modulus d appears in no more than nine of the miss ranges. We checked up to $10^{130000000}$ and found that in fact none were in more than eight. Now if a discriminant d is missed by no more than nine moduli k, we see that it must have nontrivial gcd with the other eight if we are to have $h(-d) \le 100$. But then our count of Type I primes is at least 8, making $h(-d) \ge 128$ by the theory of genera. Thus we

TABLE 3.

k	Miss Period	Shift	Factors of k
-115147	864.1809865	$[-25, 10]$	$113 \cdot 1019$
-1599847	654.3697800	$[-25, 5]$	$61 \cdot 26227$
-1832763	943.7375432	$[-30, 10]$	$3 \cdot 610921$
-8844707	1112.6215493	$[-35, 10]$	$349 \cdot 25343$
-11023787	767.5486475	$[-30, 5]$	prime
-12461947	1092.7214878	$[-35, 10]$	prime
-17773807	595.5663007	$[-25, 0]$	prime
-19420619	823.9643723	$[-30, 5]$	$131 \cdot 148249$
-21614147	1216.0252718	$[-40, 15]$	$271 \cdot 79757$
-23311771	568.1975607	$[-25, 0]$	$7 \cdot 163 \cdot 20431$
-24088843	895.7017210	$[-30, 5]$	$23 \cdot 1047341$
-24463627	601.3191684	$[-25, 0]$	prime
-26012207	2008.1757725	$[-55, 30]$	$13 \cdot 2000939$
-28815295	1987.2029123	$[-55, 25]$	$5 \cdot 5763059$
-31129723	1323.5749248	$[-40, 15]$	prime
-32438927	618.4994392	$[-25, 0]$	$31 \cdot 317 \cdot 3301$
-175990483	5741.7931296	$[-125, 100]$	$19 \cdot 1427 \cdot 6491$

are left to conclude that there is no d in the range $2^{162} \leq d \leq \exp(268800000)$ with $h(-d) \leq 100$, completing the proof of Lemma 12. □

7. Eliminating mid-sized discriminants

In this section, we reduce our possibilities for $h(-d) \leq 100$ down to a number of computational sieving problems. Largely the method shall be the same as for the larger discriminants as in Section 6, but we shall make sharper bounds in many instances. We shall exclusively use the auxiliary moduli $k = -163$ and $k = -17923$, the latter for (typically) the range $2^{62} \leq d \leq 2^{162}$, and the former for the lesser d, down all the way to 2^{52} in the best circumstances. We shall also have another bifurcation due to the necessity of considering situations for which $g = \gcd(k, d) \neq 1$. We always assume that $h(-d) \leq 100$, so that anything which implies otherwise will not trouble us.

We first define a **Legendre symbol specification**. This is simply a 3-tuple of mutually disjoint sets (X, Y, Z), with each set containing only primes. We say that a negative fundamental discriminant $-d$ is **admissible** for a Legendre symbol specification if $(-d|p) = +1, 0, -1$ for all $p \in X, Y, Z$, respectively, so that the three sets of primes specify Legendre-symbol behaviour. We next define a **sieving problem**. This is a triple (L, m, B) where L is a Legendre symbol specification, m is a multiplier, and B is a positive integer. We also have a notion of admissibility for a sieving problem; this means that $-d$ is admissible for the Legendre symbol specification, $m|d$, and $d \leq B$. One of our computational sieving problems will be $\mathbf{S}_0 = \big((\emptyset, \emptyset, \emptyset), 1, 2^{52}\big)$, and so we can always take $d \geq 2^{52}$ in the argument below.

We shall effect a division of labour using the notion of a Legendre symbol specification. Let P be the set of partitions of the smallest ten primes into three sets. For such a partition $Q \in P$, let us identify Q with the induced Legendre symbol specification. For every fundamental discriminant $-d$, there is exactly one partition

$Q \in P$ such that $-d$ is admissible for Q. These break the problem into 3^{10} pieces. However, many of these can be eliminated from consideration rather quickly; for instance, we see that if $p = 2, 3$ are specified as having $(-d|p) = +1$, then (since we can assume $d \geq 2^{52}$) we already have 173 minima from Lemma 3. So for each $Q \in P$, we use Lemma 3 and our assumption $d \geq 2^{52}$ to determine the number of minima we already have; if this is greater than 100, we can ignore Q. We can also do the same upon adding the additional specification that either 163 or 17923 divides d (i.e., is a Type I prime). If there are eight specified prime divisors of d, the class number is divisible by 128 and we are done. The maximal product with seven specified prime divisors of d is $17923 \cdot 163 \cdot 29 \cdot 23 \cdot 19 \cdot 17 \cdot 13 < 2^{43}$ while $d \geq 2^{52}$; hence we know that $\log_2 G$ (where G is the number of genera) is always at least as large as the number of Type I primes which have been specified. The results of this process are that there are only 1741 different partitions $Q \in P$ we need consider; we call the set of remaining partitions P_1. We shall eliminate many of these through a crude process and then do a finer analysis for the more difficult partitions.

We now go through an example of our next process in some detail with a specific partition. We take

$$A(s) = \prod_{p \in \mathbf{P}} G_p(s) \sum_{a \in \mathbf{Q}} \frac{\chi^\star(a)}{a^s},$$

where $\mathbf{P}$ is the set of prime minima which are less than a parameter T_1 (which shall be taken as 10000 in the case we describe here) and $\mathbf{Q}$ is the set of minima with no prime divisor in $\mathbf{P}$, with $\chi^\star$ as in Lemma 8. Note that (if $T_1 \leq D$) all the Type IIb primes will appear in $\mathbf{Q}$ here, and so we can basically ignore the differentation between Type II and Type IIb primes, the former simply being double-counted in the sum over $\mathbf{Q}$. This choice of $A(s)$ (compared to the previous one in Lemma 12) has a relatively small effect on $A(1/2 + i\xi_0)$ while reducing the bound A_{UB} quite substantially in the case where there are a cluster of minima slightly larger than $\sqrt{D}$. Let $E \in P_1$ be a partition, with some given (k, g) pair. Write $A(s) = A_1(s) \cdot A_2(s) \cdot A_3(s)$ where $A_1(s)$ is the Euler product of $G_p(s)$ over the first ten primes, $A_2(s)$ is the Euler product over the other primes up to $\sqrt{D}$, and $A_3(s)$ is the sum over $\mathbf{Q}$. We note that $A_1(s)$ is determined by (E, k, g). Letting T_2 be a parameter (which we shall also take to be 10000 here), denote by m the number of Type I primes between 30 and T_2; this results in another division of the problem based upon the various possibilities for m (which is no more than 7). We then construct bounds as in (24), though we also use the extra information about E. We use this in a number of ways; we can compute $|A_1(1/2+i\xi_0)|$ and $\arg A_1(1/2+i\xi_0)$ directly and hence get much sharper bounds on these quantities. Secondly, in a bound like (23) of $W_{k,d}$, we can put $A_1(1/4 + it)$ into the integral. Furthermore, we can exploit the existence of small minima through the use of the specific bound $V^S_{k,d}(a)$ in Lemma 10. Finally (and perhaps most importantly), we can use the structure of E to determine lower bounds on the other minima. We describe how this all works for a specific partition E, say $(\{29\}, \{2, 3\}, \{5, 7, 11, 13, 17, 19, 23\})$. Here we have $A_1(s) = (1 - 1/2^s)(1 - 1/3^s)(1 + 1/29^s)(1 - 1/29^s)^{-1}$. We consider the case where $k = -17923$ and $d \in [2^{60}, 2^{162}]$ with $g = \gcd(k, d) = 1$, taking $T_1 = 10000$ and $m = 0$, so that T_2 is irrelevant. There are 44 minima formed by the various products of $2, 3, 29$ that are no greater than $2^{29} < D$. In order for the class number not to exceed 100, any additional Type II prime must be

at least 7349; if 7333 were a Type II prime, there would be at least 104 minima by Lemma 3. Similarly, the second smallest additional Type II prime must be at least 319201, and the third at least 6170933, and so on, ending when the addition of additional Type II primes would imply that $h(-d) > 100$. What about additional Type I primes? Since we have taken $m = 0$, there are no Type I primes less than 10000. And arguing as above, the third additional Type I prime must be at least 212827, and the fourth at least 638437, etc., with there being a limit of five additional Type I primes due to genera considerations. In general, we let p_i be a lower bound on the ith additional Type I prime, and we let q_j be a lower bound on the jth additional Type II prime, with Type II primes being double-counted in contrast with Type IIb primes. Recalling the definitions of P, Q, R, S, and T from Sublemma 12.1, this gives us

$$|A(1/2+i\xi_0)| \geq |A_1(1/2+i\xi_0)| \cdot \prod_{p_i<T} P(p_i) \prod_{q_j<T} Q(q_j) \cdot \left(1 - \sum_{p_i \geq T} \frac{1}{\sqrt{p_i}} - \sum_{q_j \geq T}^{\star} \frac{1}{\sqrt{q_j}}\right),$$

$$|\arg A_2(1/2+i\xi_0)| \leq \xi_0 \left|\frac{A_2'}{A_2}(1/2+it)\right| \leq \xi_0 \left(\sum_{p_i<T} L(p_i) + 2\sum_{q_j<T} L(q_j)\right),$$

$$|\arg A_3(1/2+i\xi_0)| \leq \arcsin\left(\sum_{p_i \geq T} \frac{1}{\sqrt{p_i}} + \sum_{q_j \geq T}^{\star} \frac{1}{\sqrt{q_j}}\right),$$

and

$$|A_2(1/4+it)A_3(1/4+it)| \leq \prod_{p_i<T} R(p_i) \prod_{q_j<T} S(q_j) \cdot \left(1 + \sum_{p_i \geq T} \frac{1}{\sqrt{p_i}} + \sum_{q_j \geq T}^{\star} \frac{1}{\sqrt{q_j}}\right),$$

where the starred sums recall the double-counting of Type II primes. For our specific (X, k, g) triple we have

$$|A(1/2+i\xi_0)| \geq (.180)(.976)(.988) \geq .173,$$
$$|\arg A_2(1/2+i\xi_0)| \leq 0.22\xi_0 \leq 0.007,$$
$$|\arg A_3(1/2+i\xi_0)| \leq 0.012,$$

and

$$|A_2(1/4+it)A_3(1/4+it)| \leq (1.25)(1.93) \leq 2.42.$$

We have $\arg A_1(1/2+i\xi_0) \approx 0.058155$, and so $\arg A(1/2+i\xi_0) \in [0.039, 0.078]$. Finally we compute $U^B_{k,d}$. We have that

$$W_{k,d} \leq \frac{0.088 \cdot A_2^U A_3^U}{d^{1/8}} \int_0^\infty \left|\frac{\Gamma(1/4+it)\zeta(1/2+2it)A_1(1/4+it)(t^2+1/16)}{(\xi_0^2 - t^2 + 1/16)^2 + t^2/4}\right| dt,$$

where A_2^U and A_3^U upper-bound $|A_2(s)|$ and $|A_3(s)|$ on the line $\operatorname{Re} s = 1/4$. The integral can be bounded numerically by 1.99, so that we have $W_{k,d} \leq 0.42/d^{1/8}$. For the 44 minima we already have directly from the partition E, we can use the bound $V^S_{k,d}(a)$ (computing a lower bound for β via $d \geq 2^{60}$) if this results in something

superior to the generic bound. For the other 56 possible minima, we simply use the generic bound. This gives that

$$U^B_{k,d} = W_{k,d} + \sum_{a\in Q_d} \min(V^G_{k,d}, V^S_{k,d}(a)) \le \frac{0.42}{d^{1/8}} + \frac{49396}{d^{1/4}} \le 1.51.$$

We can now show that the above estimates imply that (17) cannot hold for the d under consideration; namely, we have

$$\bigl|\sin[\xi_1 \log d + \xi_2 + \arg A(1/2 + i\xi_0)]\bigr| > \frac{U^B_{k,d}}{\xi_3 |A(1/2 + i\xi_0)|} \tag{27}$$

for all $d \in [2^{60}, 2^{162}]$, our conditions being that d is coprime to 17923 and admissible for our partition X, with there being no Type I primes between 30 and 10000 (the $m = 0$ condition). In particular, the left-hand side of (27) is at least 0.786 while the right-hand side is no more than $\frac{1.51}{(57.0)(.173)} \le 0.154$ (in general, we might not have such a uniform statement for all d under consideration, but we can use the fact that for d near 2^{162}, we get a much better bound on $U^B_{k,d}$). Since (17) cannot hold, our assumption that $h(-d) \le 100$ must be fallacious. We can then repeat this argument for various m-values; in general (for a given partition E), the $m = 0$ case is the most difficult, in the sense that for it the inequality (17) comes closest to being possible. Except for the case when $E = (E_X, E_Y, E_Z)$ has $E_X = E_Y = \emptyset$, the above (always taking $T_1 = T_2 = 10000$) will suffice to show that $h(-d) > 100$ for all the $d \in [2^{60}, 2^{162}]$ with $g = \gcd(k, d) = 1$. When $E_X = E_Y = \emptyset$, we proceed as in the paragraph below to get a better bound on the q_j — the main difficulty here is that the argument of $A(s)$ is not sufficiently controlled. In a similar manner, we can also try to show that $h(-d) > 100$ for all $d \in [2^{60}, 2^{162}]$ with $g = 17923$ (again separately considering the case $E_X = E_Y = \emptyset$ using the methods of the next paragraph) by a slight modification of the above; here if $|E_Y| = 1$ and $E_X = \emptyset$, we first need to split into more sub-cases (as in the m-division) by restricting the number of small Type II primes. We let n be the number of Type II primes less than a parameter T_3 and then consider all possible (m, n) pairs separately; it suffices to take $T_3 = 800$ and $T_1 = T_2 = 4300$, the latter choice made to help lower the bound for $|A(s)|$ on the line $\operatorname{Re} s = 1/4$ (of course, there is interplay with the bounds for $|\arg A(s)|$; the most difficult case is $E_X = \{29\}$ and $(m, n) = (4, 1)$). We can note that (prior to this n-division) for a fixed E, we actually usually get a better bound for the right side of (27) in the $g = 17923$ case compared to the $g = 1$ case, but the fact that ξ_2 is now $-0.081\ldots$ instead of $0.221\ldots$ means that the sine-value on the left side of (27) can be smaller, and hence we have these instances which require the finer division. So at this point we have shown (subject to the consideration of the $E_X = E_Y = \emptyset$ case) that we cannot have $h(-d) \le 100$ for any $d \in [2^{60}, 2^{162}]$. Our next task will be to consider the range $d \in [2^{52}, 2^{60}]$ by using the modulus $k = -163$ in a manner similar to the above; however, we will not be quite so successful in our end result. We first turn to the promised consideration of the case where $E_X = E_Y = \emptyset$ in the above.

The following lemma is included here rather than earlier as the lower bound it gives for the 26th smallest Type II prime is only useful when $E_X = E_Y = \emptyset$.

Lemma 13. *The number of Type II primes less than $D^{2/3}$ is not more than $h/4$.*

Proof. Let l be the number of Type II primes less than $D^{2/3}$. For each such prime p, there is at least one power (call it q) of it which is in $[D^{1/3}, D^{2/3}]$. For each q, we

take a form which has q as its minimum. Each such form is nonself-conjugate, so we have $2l$ binary forms which we denote $f_1, \bar{f}_1, \ldots, f_l, \bar{f}_l$; we also write $f_i = (a_i, b_i, c_i)$ in its reduced form. Next we form the products $f_1 f_1, f_1 \bar{f}_1, f_1 f_2, f_1 \bar{f}_2, \ldots, f_1 f_l, f_1 \bar{f}_l$. All of these are distinct, due to the existence of inverses under the group law. We ignore the second form since it is the principal form. Now [8] tells us (noting that $\gcd(a_1, a_i) = 1$ for $i \neq 1$) that $f_1 f_i$ can be written as $(a_1 a_i, x_i, y_i)$ for some x_i and y_i. Since a_1 and a_i are both in $[D^{1/3}, D^{2/3}]$, this implies that $f_1 f_i$ represents a number in $[D^{2/3}, D^{4/3}]$. This representation is primitive, and primitivity persists under reduction of the form, since a reduction is a unimodular change of variables. We next note that no form with a minimum less than $D^{2/3}$ can primitively represent any number less than $D^{4/3}$ which is not the minimum. This follows since $am^2 + bmn + cn^2 \geq dn^2/4a \geq D/a$ when $n \neq 0$. So the intersection of our list of products of forms with the list of forms themselves must be empty, as the former represent something in $[D^{2/3}, D^{4/3}]$, while the latter cannot. Adding in the principal form, we have at least $1 + 2l + (2l - 1)$ forms at this point, giving us the desired bound in terms of the class number. This shows the lemma. □

In particular, this lemma tells us that the 26th smallest Type II prime must be at least 660563 when $h \leq 100$ and $D \geq 2^{29}$. This now allows us to find a contradiction with (27) when $h \leq 100$. For the case where $g = 1$, we take $T_1 = T_2 = 10000$ and again use the additional n-splitting with $T_3 = 800$. Every (m, n) possibility has $U^B_{k,d} \leq 3.6$ and $|A(s)| \geq 0.181$, making the right side of (27) no more than 0.35, while we always have $|\arg A(s)| \leq 0.478$, so that the left side is greater than 0.37. Things are so ornery in the $g = 17923$ case that we decided to make the additional restriction $d \geq 2^{65}$; upon doing this and taking $T_1 = T_2 = 4300$ with $T_3 = 800$, we can show that having $h(-d) \leq 100$ cannot happen. So we need to add the sieving problem $\mathbf{T} = \big((\emptyset, \emptyset, P_{30}), 17923, 2^{65}\big)$ (where $\mathbf{P}_{30}$ is the set of primes less than 30) to our list of sieving problems; this is reasonable due to the great savings we achieve from the condition that $17923|d$.

We now turn to range $d \in [2^{52}, 2^{60}]$. Here we use $k = -163$. First we consider the d with $\gcd(d, 163) = 1$. Taking $T_1 = T_2 = 2500$ (with no n-division), we eliminate all but 323 of our 1741 partitions E. Changing the lower limit to 2^{54} eliminates 148 more, leaving 175, and a further increasing of the lower limit to 2^{56} leaves only 108. A final heightening of the lower limit to 2^{58} eliminates 45 more partitions, but for the remaining 63, nothing is efficacious. So to our list of sieving problems, we append 148 more (labeled $\mathbf{S}_1$ through $\mathbf{S}_{148}$) which have a bound of 2^{54}, an additional 67 (labeled $\mathbf{S}_{149}$–$\mathbf{S}_{215}$) with a bound of 2^{56}, another 45 more ($\mathbf{S}_{216}$–$\mathbf{S}_{260}$) with a bound of 2^{58}. There are 63 partitions left over for which nothing can be done via this method, leaving us only the previous bound of 2^{60}. For these partitions, we further sub-divide each into nine sub-paritions, using the primes 31 and 37. With this new group of 567 partitions, 168 of them already have more than 100 minima less than 2^{25}, and another 227 are eliminated through an argument as above. Of the remaining 172 sub-partitions, 39 are eliminated upon increasing the lower limit to 2^{54} (sieving problems $\mathbf{S}_{261}$–$\mathbf{S}_{299}$), another 35 by increasing the lower limit to 2^{56} (labeled $\mathbf{S}_{300}$–$\mathbf{S}_{334}$), and another 31 with a lower limit of 2^{58} (named $\mathbf{S}_{335}$–$\mathbf{S}_{365}$), leaving 67 sub–partitions ($\mathbf{S}_{366}$–$\mathbf{S}_{432}$) which have a sieving limit of 2^{60}. This concludes the discussion of the $d \in [2^{52}, 2^{60}]$ with $\gcd(d, 163) = 1$.

For the d with $163|d$, we only consider $d \in [2^{56}, 2^{60}]$ (adding $\mathbf{U}_0 = \big((\emptyset, \emptyset, \emptyset), 163, 2^{56}\big)$ to the list of sieving problems) and take $T_1 = T_2 = 1100$. This eliminates

all but 64 of the 1741 partitions. Of these 64 partitions, six have $E_X \neq \emptyset$, namely those with $E_Y = \emptyset$ and E_X having a single element larger than 10. The other 58, all with $E_X = \emptyset$, are given by the 56 partitions with $|E_Y| \leq 2$, and also $E_Y = \{17, 23, 29\}$ and $E_Y = \{19, 23, 29\}$. We denote the corresponding sieving problems (which have a multiplier of 163 and a bound of 2^{60}) as $\mathbf{U}_1$ through $\mathbf{U}_{64}$.

8. Sieving small discriminants

We are hence left with a number of sieving problems (L, m, B), where L is a Legendre symbol specification, m a multiplier, and B a bound on the sieving level. Recall that a fundamental discriminant $-d$ is admissible for a sieving problem if it is admissible for the Legendre symbol specification, has d a multiple of the multiplier, and has $d \leq B$. We give a full description of the situation for

$$\mathbf{S}_0 = \big((\emptyset, \emptyset, \emptyset), 1, 2^{52}\big),$$

the others being similar. Given a negative fundamental discriminant $-d$, the idea shall be to take sets of (say) 35 small primes and find at least one prime p in each set with $(-d|p) = +1$. These will then generate a lot of minima, hopefully more than 100. Our sets of primes shall be 31–197, 199–409, 419–631, 641–863, 877–1103, 1109–1373, and 1381–1613, which we call the sieving sets. Suppose, to start, that $d \geq 2^{48}$ (if not, we have reduced the problem by a factor of 16, and it is hence substantially easier) and at least one prime in each sieving set has $(-d|p) = +1$. Then there are at least 98 minima from products of the primes (since $1613^2 \leq 2^{23}$), and 14 minima from the primes themselves (plus one for the principal minimum), making 112 already. If a discriminant has $(-d|p) \neq +1$ for all primes in the sieving set, we say that this discriminant is **missed** by the sieving set. Note that the miss rate for our sieving sets is about 1 in 2^{35}. Even if we sieve about 2^{55} things, we can still easily handle all the misses simply by directly computing the class numbers (which takes less than a second) for the recalcitrant discriminants missed by a sieve. This use of sieving sets shall be the main idea of our sieving process, though we also use information about the smallest 10 primes to lighten the load. To this end, we divide the d's into congruence classes modulo

$$Q = 155272637520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29.$$

Sieving in a congruence class still possesses useful periodic conditions, and so is not any more difficult. We could use a larger modulus than Q, but we are nearing the point of diminishing returns; with our method we have about $2^{52}/Q \approx 29000$ discriminants under consideration in each congruence class, and reducing this much further would start to make overhead costs the dominant factor. There are negative fundamental discriminants in $Q/3$ of these congruence classes. For each congruence class, we ask how many sieving sets (starting with the smallest) we need to use before we can conclude that the resulting class number is more than 100. For instance, if 2 is a Type I prime and 13 is a Type II prime (with the other small primes having $(-d|p) = -1$), we need to sieve with the smallest two sieving sets (again assuming that $d \geq 2^{48}$; we have at least 74 minima after using the first sieving set and 138 after including the second). An accounting of the congruence classes gives the following data about how many sieving sets are needed: 50222242532 of the congruence classes need *zero* sieving sets, 955240658 need one sieving set, 361124966 need two, 128134380 need three, 39728376 need four, 38244528 need

five, 855360 need six, and 11975040 need seven. Thus the number of fundamental discriminants to be sieved here is about

$$\frac{2^{52}}{Q}\Big(955240658 + 722249932 + 384403140 + 158913504 + 191222640 + 5132160 + 83825280\Big) \le 73 \cdot 10^{12}.$$

Our raw sieving rate is about 2^{26} discriminants per second, and so this will take around two weeks (neglecting overhead). As mentioned above, this works for $d \ge 2^{48}$; for the smaller discriminants we use a similar method with slightly more sieving sets. We do not dwell on the details here; suffice it to say that the highest range of discriminants takes more than 85% of the sieving time. Note also that Buell [9] has exhaustively handled the range $d \le 2^{31}$, so we need not consider those discriminants.

The other sieving problems go similarly. For

$$\mathbf{T} = \big((\emptyset, \emptyset, \mathbf{P}_{30}), 17923, 2^{65}\big),$$

we have about

$$\frac{2^{65}}{17923} \cdot \frac{6}{16} \cdot \prod_{3 \le p \le 29} \left(\frac{p-1}{2p}\right)$$

fundamental discriminants, and each shall need six sieving sets to be used. This gives less than $3 \cdot 10^{12}$ discriminants to be sieved. For $\mathbf{U}_0$, a computation as with $\mathbf{S}_0$ tells us that we need sieve only about $(2^{56}/163Q) \cdot 1674504636 \le 5 \cdot 10^{12}$ discriminants. An accounting of the other 64 $\mathbf{U}_i$ sieving problems implies that less than $42 \cdot 10^{12}$ discriminants need to be sieved here. The sieving problems $\mathbf{S}_1$–$\mathbf{S}_{260}$ involve about $160 \cdot 10^{12}$ discriminants (the 160 could be reduced to 90 with a little more effort), while $\mathbf{S}_{261}$–$\mathbf{S}_{365}$ involve only $23 \cdot 10^{12}$. The lion's share of sieving comes from $\mathbf{S}_{366}$–$\mathbf{S}_{432}$, which involve sieving about $784 \cdot 10^{12}$ discriminants. For these latter sieving problems, we enhance the modulus Q to $Q/3 \cdot 31 \cdot 37$, which is still sufficiently smaller than the sieving bound of 2^{60} to allow periodic congruence conditions to be exploited.

This gives a total of about $1.1 \cdot 10^{15}$ discriminants overall, which, with our sieving rate of 2^{26} discriminants per second, takes only about six months, almost seven when overhead is taken into account. As noted above, the number of discriminants which fail to be sieved should be less than a million, and these can be handled individually. Upon completing this computation, we conclude that the classical lists of small class numbers are indeed complete.

How much further can one take this type of analysis? Our sieving rate of 2^{26} per second is actually quite slow even though we use such tricks as using the 32-bit computer architecture to consider 32 discriminants at a time. A special-purpose machine in the spirit of the MSSU [27] might be able to run 1000 times as fast as our sieve. However, we have the advantage of being able to distribute the load in parallel across many machines, while building more than one super-siever would be more difficult (in fact, the parallelism is already built into the design). Suppose that we wanted to consider all class numbers up to 1000. The factor of 10 in class number (compared to our $h \le 100$) corresponds to at least a jump of 10^4 in the level of sieving needed, due to the $h/d^{1/4}$ term in the equations. But also the lower bounds on $|A(s)|$ (and the other quantities) become worse as the class number

TABLE 4.

N	#	large	N	#	large	N	#	large	N	#	large	N	#	large
1	9	163	21	85	61483	41	109	296587	61	132	606643	81	228	1030723
2	18	427	22	139	85507	42	339	280267	62	323	647707	82	402	1446547
3	16	907	23	68	90787	43	106	300787	63	216	991027	83	150	1074907
4	54	1555	24	511	111763	44	691	319867	64	1672	693067	84	1715	1225387
5	25	2683	25	95	93307	45	154	308323	65	164	703123	85	221	1285747
6	51	3763	26	190	103027	46	268	462883	66	530	958483	86	472	1534723
7	31	5923	27	93	103387	47	107	375523	67	120	652723	87	222	1261747
8	131	6307	28	457	126043	48	1365	335203	68	976	819163	88	1905	1265587
9	34	10627	29	83	166147	49	132	393187	69	209	888427	89	192	1429387
10	87	13843	30	255	134467	50	345	389467	70	560	811507	90	801	1548523
11	41	15667	31	73	133387	51	159	546067	71	150	909547	91	214	1391083
12	206	17803	32	708	164803	52	770	439147	72	1930	947923	92	1248	1452067
13	37	20563	33	101	222643	53	114	425107	73	119	886867	93	262	1475203
14	95	30067	34	219	189883	54	427	532123	74	407	951043	94	509	1587763
15	68	34483	35	103	210907	55	163	452083	75	237	916507	95	241	1659067
16	322	31243	36	668	217627	56	1205	494323	76	1075	1086187	96	3283	1684027
17	45	37123	37	85	158923	57	179	615883	77	216	1242763	97	185	1842523
18	150	48427	38	237	289963	58	291	586987	78	561	1004347	98	580	2383747
19	47	38707	39	115	253507	59	128	474307	79	175	1333963	99	289	1480627
20	350	58507	40	912	260947	60	1302	662803	80	2277	1165483	100	1736	1856563

grows. A more realistic guess would be that the difficulty of the sieving problem would increase by 10^5 (or even 10^6). This seems unreasonable at present.

In Table 4 we give for $N \leq 100$ the number of negative fundamental discriminants with class number N and the largest such discriminant (in absolute value).

REFERENCES

[1] M. Abramowitz, I. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables.* National Bureau of Standards Applied Mathematics, 55. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 1964 MR **29:**4814 (later ed.)

[2] S. Arno, *The imaginary quadratic fields of class number 4.* Acta Arith. **60** (1992), pp. 321–334. MR **93b:**11144

[3] S. Arno, M. Robinson, F. Wheeler, *Imaginary quadratic fields with small odd class number.* Acta Arith. **83** (1998), pp. 295–330. MR **99a:**11123

[4] A. Baker, *Linear forms in the logarithms of algebraic numbers I, II, III.* Mathematika **13** (1966), pp. 204–216; ibid. **14** (1967), pp. 102–107; ibid. **14** (1967) pp. 220–228. MR **36:**3732

[5] A. Baker, *Imaginary quadratic fields with class number 2.* Ann. of Math. (2) **94** (1971), pp. 139–152. MR **45:**8631

[6] A. Baker, H. Stark, *On a fundamental inequality in number theory.* Ann. of Math. (2) **94** (1971), pp. 190–199. MR **46:**1716

[7] P. Bateman, E. Grosswald, *On Epstein's zeta function.* Acta Arith. **9** (1964), pp. 365–373. MR **31:**3392

[8] D. Buell, *Binary quadratic forms. Classical theory and modern computations.* Springer-Verlag, New York, 1989. MR **99b:**11021

[9] D. Buell, *The last exhaustive computation of class groups of complex quadratic number fields.* Number Theory (Ottawa, ON, 1996), pp. 35–53. CRM Proc. Lecture Notes, 19. Amer. Math. Soc., Providence, RI, 1999. MR **2000d:**11156

[10] C. Gauss, *Disquisitiones Arithmeticae* (Latin). English translation by A. Clarke, revised by W. Waterhouse, 1986 Springer–Verlag reprint of the Yale University Press, New Haven, 1966 edition. MR **33:**5545; MR **87f:**01105

[11] 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), pp. 624–663. MR **56:**8529

[12] D. Goldfeld, *Gauss' class number problems for imaginary quadratic fields.* Bull. Amer. Math. Soc. **13** (1985), pp. 23–37. MR **86k:**11065

[13] B. Gross, D. Zagier, *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986), pp. 225–320. MR **87j:**11057

[14] K. Heegner, *Diophantische Analysis und Modulfunktionen* (German). Math. Z. **56** (1952), pp. 227–253. MR **14:**725j

[15] H. Heilbronn, E. Linfoot, *On the imaginary quadratic corpora of class-number one.* Quart. J. Math. Oxford Ser. **5** (1934), pp. 293–301.

[16] A. Ingham, *The Distribution of Prime Numbers.* Cambridge Tract 30, Cambridge University Press, 1990. MR **91f:**11064

[17] E. Landau, *Bemerkungen zum Heilbronnschen Satz* (German). Acta Arith. **1** (1935), pp. 1–18.

[19] S. Lang, *Real and functional analysis.* Third edition. Graduate Texts in Mathematics, 142. Springer-Verlag, New York, 1993. MR **94b:**00005

[18] S. Lang, *Complex Analysis.* Fourth edition. Graduate Texts in Mathematics, 103. Springer-Verlag, New York, 1999. MR **99i:**30001

[20] F. Lemmermeyer, S. Louboutin, R. Okazaki, *The class number one problem for some non-abelian normal CM-fields of degree 24.* J. Théor. Nombres Bordeaux **11** (1999), pp. 387–406. MR **2001j:**11104

[21] J. Littlewood, *On the class number of the corpus* $P(\sqrt{-k})$. Proc. London Math. Soc. **27** (1928), pp. 358–372.

[22] S. Louboutin, *The nonquadratic imaginary cyclic fields of 2-power degrees with class number equal to their genus class numbers.* Proc. Amer. Math. Soc. **127** (1999), pp. 355–361. MR **99c:**11134

[23] S. Louboutin, *The class number one problems for the dihedral and dicyclic CM-fields.* Colloq. Math. **80** (1999), pp. 259–265. MR **2000e:**11140

[24] S. Louboutin, R. Okazaki, *Determination of all nonnormal quartic CM-fields and of all non abelian normal octic fields with class number one.* Acta Arith. **67** (1994), pp. 47–62. MR **95g:**11107

[25] S. Louboutin, R. Okazaki, *Determination of all quarternion CM-fields with ideal class group of exponent 2.* Osaka J. Math. **36** (1999), pp. 229–257. MR **2001c:**11120

[26] S. Louboutin, Y.-H. Park, *Class number problems for dicyclic CM-fields.* Publ. Math. Debrecen **57** (2000), pp. 283–295. MR **2001m:**11196

[27] R. Lukes, C. Patterson, H. Williams, *Numerical sieving devices: their history and some applications.* Nieuw Arch. Wisk, (4) **13** (1995), pp. 113–139. MR **96m:**11082

[28] I. Miyada, *On imaginary abelian number fields of type* $(2, 2, \cdots, 2)$ *with one class in each genus.* Manuscripta Math. **88** (1995), pp. 535–540. MR **96j:**11146

[29] H. Montgomery, P. Weinberger, *Notes on small class numbers.* Acta Arith. **24** (1973), pp. 529–542. MR **50:**9841

[30] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaries* (French). Séminaire Bourbaki, Vol. 1983/84. Astérisque No. 121–122 (1985), pp. 309–323. MR **86k:**11064

[31] J. Oesterlé, *Le probléme de Gauss sur le nombre de classes.* (French). Enseign. Math **34** (1988), pp. 43–67. MR **89j:**11108

[32] R. Paley, *A theorem on characters.* J. London Math. Soc. **7** (1932), pp. 28–32.

[33] PARI-GP. By C. Batut, D. Bernardi, H. Cohen, and M. Olivier. Currently maintained by K. Belabas at the Université Paris-Sud Orsay. `http://www.parigp-home.de`

[34] A. Selberg, S. Chowla, *On Epstein's zeta-function.* J. Reine Angew. Math. **227** (1967), pp. 86–110. MR **35:**6632

[35] J.-P. Serre, $\Delta = b^2 - 4ac$. Math. Medley **13** (1985), pp. 1–10. MR **87g:**11148

[36] B. Setzer, *The determination of all imaginary, quartic, abelian number fields with class number 1.* Math. Comp. **35** (1980), pp. 1383–1386. MR **81k:**12005

[37] C. Siegel, *Über die Klassenzahl quadratischer Zahlkörper* (German). Acta Arith. **1** (1935), pp. 83–86.

[38] H. Stark, *On complex quadratic fields with class number equal to one.* Trans. Amer. Math. Soc. **122** (1966), pp. 112–119. MR **33:**4043

[39] H. Stark, *A complete determination of the complex quadratic fields of class-number one.* Michigan Math. J. **14** (1967), pp. 1–27. MR **36:**5102
[40] H. Stark, *L-functions and character sums for quadratic forms I, II.* Acta. Arith **14** (1967/68), pp. 35–50; ibid. **15** (1968/69), pp. 307–317. MR **37:**2707; MR **39:**4101
[41] H. Stark, *On the "gap" in a theorem of Heegner.* J. Number Theory **1** (1969), pp. 16–27. MR **39:**2724
[42] H. Stark, *A transcendence theorem for class-number problems I, II.* Ann. of Math. (2) **94** (1971), pp. 153–173; ibid. **96** (1972), pp. 174–209. MR **45:**6767; MR **46:**8983
[43] T. Tatuzawa, *On a theorem of Siegel.* Jap. J. Math **21** (1951), pp. 93–111 (1952). MR **14:**452c
[44] C. Wagner, *Class number 5, 6 and 7.* Math. Comp. **65** (1996), pp. 785–800. MR **96g:**11135
[45] M. Watkins, *Real zeros of real odd Dirichlet L-functions.* Math. Comp., **73** (2004), pp. 415–423.
[46] G. Watson, *A treatise on the theory of Bessel functions.* Cambridge Univ. Press, 1922. MR **6:**64a (2nd ed.)
[47] P. Weinberger, *On small zeros of Dirichlet L-functions.* Math. Comp. **29** (1975), pp. 319–328. MR **51:**12739
[48] K. Yamamura, *The determination of the imaginary abelian number fields with class number one.* Math. Comp. **62** (1994), pp. 899–921. MR **94g:**11096
[49] K. Yamamura, *Determination of the imaginary normal octic number fields with class number one which are not CM-fields.* Acta Arith. **86** (1998), pp. 133–147. MR **99h:**11127

Department of Mathematics, McAllister Building, The Pennsylvania State University, University Park, Pennsylvania 16802
E-mail address: watkins@math.psu.edu