4-2010

Maximal Class Numbers of CM Number Fields

Ryan C. Daileda
Trinity University, Ryan.Daileda@trinity.edu

Raju Krishnamoorthy

Anton Malyshev

Repository Citation

Daileda, R.C., Krishnamoorthy, R., & Malyshev, A. (2010). Maximal class numbers of CM number fields. *Journal of Number Theory, 130*(4), 936-943. doi: 10.1016/j.jnt.2009.09.013

Maximal Class Numbers of CM Number Fields

Ryan C. Daileda*,[a], Raju Krishnamoorthy[b,1], Anton Malyshev[c,1]

[a] *Trinity University, Mathematics Department, One Trinity Place, San Antonio, TX 78212-7200*
[b] *Massachusetts Institute of Technology, Department of Mathematics, 77 Massachusetts Avenue, Cambridge, MA 02139-4307*
[c] *Princeton University, Department of Mathematics, Fine Hall, Washington Road, Princeton NJ 08544-1000*

Abstract

Fix a totally real number field F of degree at least 2. Under the assumptions of the generalized Riemann hypothesis and Artin's conjecture on the entirety of Artin L-functions, we derive an upper bound (in terms of the discriminant) on the class number of any CM number field with maximal real subfield F. This bound is a refinement of a bound established by Duke in 2001. Under the same hypotheses, we go on to prove that there exist infinitely many CM-extensions of F whose class numbers essentially meet this improved bound and whose Galois groups are as large as possible.

Key words: class number, CM number field, Artin L-function, generalized Riemann hypothesis
2000 MSC: 11R29, 11R21, 11R42, 11R32

1. Introduction

Questions about the maximal size of the class numbers go back at least to Gauss, who conjectured that as $d \to -\infty$ through fundamental discriminants one should have that the class number h of $\mathbb{Q}(\sqrt{d})$ tends to infinity. Siegel obtained a proof of this result by establishing that $h > c_1(\epsilon)|d|^{\frac{1}{2}-\epsilon}$ for all $\epsilon > 0$. This lower bound on h is almost the best possible, for a classical result of Landau tells us that we have the inequality

$$h < c_2(n)|d|^{\frac{1}{2}} \log(|d|)^{n-1} \tag{1}$$

*Corresponding author
Email addresses: rdaileda@trinity.edu (Ryan C. Daileda), krishnamoorthy@alum.mit.edu (Raju Krishnamoorthy), amalyshe@princeton.edu (Anton Malyshev)

[1] The second and third authors received support from the National Science Foundation under grant DMS-0648390.

for the class number h of any number field of discriminant d and degree n over $\mathbb{Q}$. To show that the upper bound (1) is essentially sharp, Ankeny, Brauer and Chowla succeeded in proving what can be viewed as a generalization of Siegel's result. Their theorem states that for any $\epsilon > 0$ there are infinitely many number fields of any fixed signature and degree whose class numbers satisfy

$$h > |d|^{\frac{1}{2}-\epsilon}. \tag{2}$$

While the upper bound (1) and the lower bound (2) are remarkably close, they are not of the same order of magnitude as $|d|$ tends to infinity. However, if additional hypotheses are imposed upon the fields in question, it is possible to improve both (1) and (2) in certain cases, thereby obtaining more precise information about the maximal size of h.

For example, a technique due to Littlewood shows that, under the assumption of the generalized Riemann hypothesis (GRH) for certain Dirichlet L-functions, the class number of a quadratic number field satisfies

$$h \leq C_1 d^{1/2} \frac{d^{1/2} \log\log d}{\log d}. \tag{3}$$

More generally, Duke has shown that for families of number fields in which the degree, signature and Galois group are fixed one can use GRH for the associated L-functions to deduce bounds of the form

$$h \leq C_2 \frac{|d|^{1/2} (\log\log |d|)^{n-1}}{(\log |d|)^b} \tag{4}$$

in which the constants C_2 and $b \geq 0$ depend on the family under consideration (see Corollary 2). This inequality provides a specialized improvement of Landau's result (1), but of course is only hypothetical as it requires the assumption of GRH.

A natural question to ask is whether or not the hypothetical bound (4) is actually sharp. That is, do there exist fields in any such family with arbitrarily large discriminant whose class numbers satisfy the reverse of inequality (4), up to the constant C_1? Montgomery and Weinberger [5] showed that this is indeed the case for the family of real quadratic fields, Duke [3] established the analogous result for abelian cubic number fields, and the author [1] proved a similar result in the non-abelian cubic setting. It should be noted that while (4) is conditional on GRH, these results on its sharpness are actually unconditional. On the other hand, under GRH Duke [2] was able show sharpness for a large collection of families of arbitrary degree.

This body of evidence suggests that we might conjecture that the answer to the question posed above is always "yes." It is the purpose of this note to show that this is in fact not the case. Our first main result, Proposition 3, shows that for families of CM number fields, the bound (4) is never sharp in the sense described earlier, again under the assumption of GRH. However, in the course of the proof we will be led to a natural reformulation of (4) for families of CM

fields, in which we hold the maximal totally real subfield fixed. After deriving upper bounds on the class number in this setting, we prove in our second main result (Theorem 1) that this revised estimate is, in a certain sense, the best possible.

2. Class Numbers and GRH

If K is a number field of degree n over $\mathbb{Q}$ with Galois closure $\widehat{K}$, and we let $G = G(\widehat{K}/\mathbb{Q})$, then the action of $G(\widehat{K}/\mathbb{Q})$ on the cosets of $H = G(\widehat{K}/K)$ gives rise to an embedding $\iota : G(\widehat{K}/\mathbb{Q}) \hookrightarrow S_n$. As in [3], given a transitive subgroup $\mathcal{G} \subset S_n$ we let $\mathcal{K}(\mathcal{G})$ denote the set of all number fields K of degree n that have an ordering of their cosets so that the image of ι is exactly $\mathcal{G}$. Given a conjugacy class $\mathcal{C}$ of $\mathcal{G}$ we let $\mathcal{K}_{\mathcal{C}}(\mathcal{G})$ denote the subset of $\mathcal{K}(\mathcal{G})$ consisting of fields for which the image of complex conjugation under ι lies in C. Assuming that the associated L-functions are entire (Artin's conjecture) and satisfy GRH, Duke noted [3] that one can obtain a uniform upper bound for the class numbers of fields belonging to $\mathcal{K}_C(G)$ in terms of their discriminants. For the convenience of the reader, we include the details below.

The embedding $\iota : G(\mathcal{K}/\mathbb{Q}) \hookrightarrow S_n$ gives rise to an n-dimensional representation Λ_K of the Galois group which decomposes as $\Lambda_K = 1 \oplus \pi_K$, for a certain representation π_K of dimension $n-1$ that is free from trivial components. While Λ_K and π_K will depend on ι, their characters ψ_K and χ_K, respectively, do not. It is well known that the Artin L-function associated to ψ_K is precisely $\zeta_K(s)$ and functoriality of L-functions then gives $\zeta_K(s) = \zeta(s)L(s, \chi_K)$. The class number formula then tells us that the class number h of K is given by

$$h = \frac{w|d|^{1/2}L(1, \chi_K)}{2^{r_1}(2\pi)^{r_2}R} \tag{5}$$

where R is the regulator of K, d is its discriminant, and (r_1, r_2) its signature , and w is the number of roots of unity contained in K.

The constants w, r_1 and r_2 are bounded for fixed n, so we find that for $K \in \mathcal{K}_C(G)$ the class number depends, essentially, only on d, $L(1, \chi_K)$ and R. In order to get an upper bound on h in terms of d alone we need to bound R and $L(1, \chi_K)$ in terms of d. A general bound for R was given by Silverman [7]:

$$R \gg (\log |d|)^{r(K)-\rho(K)} \tag{6}$$

where $r(K)$ is the rank of the unit group of K and $\rho(K)$ denotes the maximum rank of the unit group of any proper subfield of K. To bound $L(1, \chi_K)$ we begin with the following result, which is proven as Proposition 5 of [2].

Proposition 1. *Let $L(s, \chi)$ be an entire Artin L-function that satisfies GRH, where χ has degree n and conductor N. Then*

$$\log L(1, \chi) = \sum_{p \leq (\log N)^{1/2}} \chi(p)p^{-1} + O_n(1). \tag{7}$$

Here

$$\chi(p) = \frac{1}{|I_p|} \sum_{\iota \in I_p} \chi(\sigma_p \iota)$$

where I_p is the inertia group and σ_p is the Frobenius of any of the primes over p.

Since χ_K has conductor $|d|$ and satisfies $\chi_K(p) \leq n-1$, one can immediately use this Proposition to deduce an upper bound for $L(1, \chi_K)$. However, we will later require a slightly more specialized bound that takes in to account the presence of subfields of K. This we deduce from the next group theoretic lemma.

Lemma 1. *Let K/F be number fields. For any $\sigma \in G(\widehat{K}/\mathbb{Q})$ we have*

$$\psi_K(\sigma) \leq [K:F] \psi_F(\sigma \,\big|_{\widehat{F}}).$$

Proof. As above, let $n = [K:\mathbb{Q}]$, $G = G(\widehat{K}/\mathbb{Q})$ and $H = G(\widehat{K}/K)$. Choose and ordering of the cosets of H in G and let $\iota_K : G \to S_n$ be the associated embedding. If we let f denote the function that returns the number of fixed points of a permutation, then it is clear that $\psi_K = f \circ \iota_K$. Setting $m = [F:\mathbb{Q}]$, $I = G(\widehat{K}/F)$ and $J = G(\widehat{K}/\widehat{F})$, Galois theory tells us that $\psi_F = f \circ \iota_F$, where $\iota_F : G/J \to S_m$ is obtained from the action of G/J on the cosets of I/J.

Let $\sigma \in G$. The fixed points of $\iota_K(\sigma)$ correspond to those cosets ρH for which $\sigma \rho H = \rho H$. Given such a coset, since $H \subseteq I$, we find that $\rho H \subset \rho I \cap \sigma \rho I$, which implies that $\rho I = \sigma \rho I$. But implies that $(\sigma \rho J)(I/J) = (\rho J)(I/J)$, i.e. $(\rho J)(I/J)$ corresponds to a fixed point of $\iota_F(\sigma J)$. The assignment $\rho H \mapsto (\rho J)(I/J)$ therefore gives a map from the fixed points of $\iota_K(\sigma)$ to those of $\iota_F(\sigma J)$ that is at most $[H:I]$-to-one. Since $[H:I] = [K:F]$ we see that

$$\psi_K(\sigma) = f(\iota_K(\sigma)) \leq [K:F] f(\iota_F(\sigma J)) = [K:F] \psi_F(\sigma \,\big|_{\widehat{F}}) \tag{8}$$

as claimed. □

Corollary 1. *Let K/F be number fields. For any $\sigma \in G(\widehat{K}/\mathbb{Q})$ we have*

$$\chi_K(\sigma) \leq [K:F] \psi_F(\sigma \,\big|_{\widehat{F}}) - 1.$$

Proof. This follows immediately from the lemma since $\chi_K(\sigma) = \psi_K(\sigma) - 1$. □

We can now deduce the bound we will need for $L(1, \chi_K)$.

Proposition 2. *Let K/F be number fields with $n = [K:\mathbb{Q}]$, $d = \operatorname{disc} K$. If $L(s, \chi_K)$ is entire and satisfies GRH, then*

$$L(1, \chi_K) \ll_{n,F} (\log \log |d|)^{[K:F]-1+o(1)} \tag{9}$$

as $|d| \to \infty$. If $F = \mathbb{Q}$ the $o(1)$ term may be omitted.

Proof. According to Proposition 1 we have

$$\log L(1,\chi_K) = \sum_{p\le(\log|d|)^{1/2}} \chi_K(p)p^{-1} + O_n(1). \tag{10}$$

Since $\chi_K(p) \le n-1$ and

$$\sum_{p\le x} p^{-1} = \log\log x + O(1)$$

we are finished in the case that $F=\mathbb{Q}$. Otherwise, given a rational prime p that is unramified in F, let $\sigma_p \in G(\widehat{F}/\mathbb{Q})$ denote its Frobenius. If we let C denote an arbitrary conjugacy class in $G(\widehat{F}/\mathbb{Q})$ then for any $x>0$ we have

$$\sum_{p\le x} \chi_K(p)p^{-1} = \sum_C \sum_{\substack{p\le x\\ \sigma_p\in C}} \chi_K(p)p^{-1} + O_{F,n}(1), \tag{11}$$

the error term arising from those primes that ramify in F. By Corollary 1

$$\chi_K(p) \le [K:F]\psi_F(\sigma_p) - 1.$$

Since ψ_F is constant on each conjugacy class, we can write $\psi_F(\sigma_p) = s_C$ for $\sigma_p \in C$ and so

$$\begin{aligned}\sum_C \sum_{\substack{p\le x\\ \sigma_p\in C}} \chi_K(p)p^{-1} &\le [K:F]\sum_C s_C \sum_{\substack{p\le x\\ \sigma_p\in C}} p^{-1} - \sum_C \sum_{\substack{p\le x\\ \sigma_p\in C}} p^{-1} &(12)\\ &= [K:F]\sum_C s_C \sum_{\substack{p\le x\\ \sigma_p\in C}} p^{-1} - \log\log x + O_F(1). &(13)\end{aligned}$$

The Čebotarev Density Theorem tells us that for each C

$$\lim_{x\to\infty} \frac{\sum_{\substack{p\le x\\ \sigma_p\in C}} p^{-1}}{\sum_{p\le x} p^{-1}} = \frac{|C|}{|G(\widehat{F}/\mathbb{Q})|}.$$

Therefore

$$\begin{aligned}\sum_{\substack{p\le x\\ \sigma_p\in C}} p^{-1} &= \left(\frac{|C|}{|G(\widehat{F}/\mathbb{Q})|} + o(1)\right)\sum_{p\le x} p^{-1}\\ &= \left(\frac{|C|}{|G(\widehat{F}/\mathbb{Q})|} + o(1)\right)\log\log x + O_F(1)\end{aligned}$$

as $x\to\infty$. Substituting this into (12) and (13), and the resulting expression into (11) we end up with

$$\sum_{p\le x} \chi_K(p)p^{-1} \le \left(\frac{[K:F]}{|G(\widehat{F}/\mathbb{Q})|}\sum_C s_C|C| - 1 + o(1)\right)\log\log x + O_{F,n}(1). \tag{14}$$

Since

$$\sum_C s_C|C| = |G(\widehat{F}/\mathbb{Q})|$$

we arrive at the conclusion. □

Taking $F = \mathbb{Q}$ in Proposition 2, the regulator estimate (6) and equation (5) now immediately imply the following.

Corollary 2. *Let $\mathcal{G}$ be a subgroup of S_n, $\mathcal{C}$ be a conjugacy class in $\mathcal{G}$, $K \in \mathcal{K}_{\mathcal{C}}(\mathcal{G})$ and $m_{\mathcal{C}}(\mathcal{G}) = r(K) - \rho(K)$. If $L(s, \chi_K)$ is entire and satisfies GRH then*

$$h \ll_n |d|^{1/2} \frac{(\log\log|d|)^{n-1}}{(\log|d|)^{m_{\mathcal{C}}(\mathcal{G})}}. \tag{15}$$

3. CM Number Fields

It has been shown that when $\mathcal{G} = S_2$ or $\mathcal{G} \subseteq S_3$ the bound (15) of Corollary 2 is sharp [1, 2, 3, 4, 5]; this is also the case when $\mathcal{G} = S_n$ and K is totally real ($\mathcal{C} = \{(1)\}$), under the additional assumption of GRH [2]. There is one general situation, however, in which the bound *cannot* be sharp, at least if we are still willing to accept the truth of the GRH. This is the case when the members of $\mathcal{K}_{\mathcal{C}}(\mathcal{G})$ are all CM fields.

A *CM field* is a totally imaginary quadratic extension of a totally real field. One can easily formulate conditions on $\mathcal{G}$ that will guarantee that $\mathcal{K}_{\mathcal{C}}(\mathcal{G})$ contains only CM fields, and we leave this to the reader (the first nontrivial case occurs when $\mathcal{G} \cong D_4$). Note that $m_{\mathcal{C}}(\mathcal{G}) = 0$ in this situation. If K is a CM field, it and its maximal totally real subfield essentially have the same regulator, and as we will see in the next proposition, this creates an obstruction to meeting the bound (15).

Proposition 3. *If $n \geq 4$ and the family $\mathcal{K}_{\mathcal{C}}(\mathcal{G})$ contains only CM fields then the bound (15) is not sharp in the following sense. For any fixed $c > 0$ there are only finitely many $K \in \mathcal{K}_{\mathcal{C}}(\mathcal{G})$ such that $L(s, \chi_K)$ is entire, satisfies GRH and*

$$h \geq c|d|^{1/2}(\log\log|d|)^{n-1}. \tag{16}$$

Proof. Let $K \in \mathcal{K}_{\mathcal{C}}(\mathcal{G})$ be a CM field with maximal real subfield F. The regulators of K and F are related by $\mathrm{Reg}(K) = c_0(K, F)\,\mathrm{Reg}(F)$, where $c_0(K, F)$ is a power of two bounded by $2^{r_1+r_2-1}$. Therefore, if $L(s, \chi_K)$ is entire and satisfies GRH, and h satisfies (16), the class number formula combined with Corollary 2 tells us that both $\mathrm{Reg}(F)$ and $\mathrm{Reg}(K)$ are bounded (the bound will depend on n and c only). This and the regulator bound (6) applied to the field F imply that the discriminant of F is bounded. However, there are only finitely number fields with bounded degree and discriminant, so for fixed n and c there are only finitely many choices for F.

Now assume that the set S of K as described in the statement of the proposition is infinite. The preceding paragraph implies that we may assume that all

$K \in S$ share a *common* nontrivial maximal real subfield F_0. Setting $F = F_0$ in proposition 2 yields

$$L(1, \chi_K) \ll_n (\log\log|d|)^{1+o(1)}$$

for $K \in S$. Since the regulator of K is bounded, the class number formula now gives

$$h \ll_n |d|^{1/2}(\log\log|d|)^{1+o(1)}$$

which contradicts (16) as $|d| \to \infty$. □

We are then faced with the following questions. When $\mathcal{K}_{\mathcal{C}}(\mathcal{G})$ contains only CM fields, can we improve (15)? If so, is there more than one way in which this can be done? Here we will address only the first of these questions. Our guiding influence will be the proof of Proposition 3, which suggests that we work with families of CM number fields that share a common maximal totally real base field. To this end, fix a positive integer m, a subgroup $\mathcal{H}$ of S_m and a field $F \in \mathcal{K}_{(1)}(\mathcal{H})$. Such an F is a totally real number field, and if K is a totally imaginary quadratic extension of F, then K is a CM field. The embedding of $G(\widehat{F}/F)$ into S_m extends to an embedding of $G(\widehat{K}/K)$ into $(\mathbb{Z}/2\mathbb{Z})^m \rtimes S_m$, whose image is contained in $(\mathbb{Z}/2\mathbb{Z})^m \rtimes \mathcal{H}$. Given a subgroup $\mathcal{G}$ of $(\mathbb{Z}/2\mathbb{Z})^m \rtimes \mathcal{H}$ we let $\mathcal{K}^F(\mathcal{H}, \mathcal{G})$ denote the set of totally imaginary number fields K satisfying $K \cap \mathbb{R} = F \in \mathcal{K}_{(1)}(\mathcal{H})$, $[K:F] = 2$, and whose associated embedding of $G(\widehat{K}/K)$ has image $\mathcal{G}$.

The proof of Proposition 3 shows that if $K \in \mathcal{K}^F(\mathcal{H}, \mathcal{G})$ and $L(s, \chi_K)$ is entire and satisfies GRH then

$$h \ll_F |d|^{1/2}(\log\log|d|)^{1+o(1)}. \tag{17}$$

Under the same hypotheses, and with the additional assumption that $\mathcal{G} = (\mathbb{Z}/2\mathbb{Z})^m \rtimes \mathcal{H}$, the next result shows that the exponent occurring in (17) is asymptotically the best possible.

Theorem 1. *Let $m \in \mathbb{Z}^+$, $\mathcal{H} \leq S_m$, $F \in \mathcal{K}_{(1)}(\mathcal{H})$ and $\mathcal{G} = (\mathbb{Z}/2\mathbb{Z})^m \rtimes \mathcal{H}$. Suppose that $L(s, \chi_K)$ is entire and satisfies GRH for each $K \in \mathcal{K}^F(\mathcal{H}, \mathcal{G})$. Then there is a constant $c_F > 0$ such that there exist $K \in \mathcal{K}^F(\mathcal{H}, \mathcal{G})$ with arbitrarily large discriminants whose class numbers satisfy*

$$h \geq c_F|d|^{1/2}(\log\log|d|)^{1+o(1)}.$$

Before turning to the proof of Theorem 1, we need to construct a suitable family of number fields with which to work, and to prove a few lemmas about them. To that end, fix m, $\mathcal{H}$, $\mathcal{G}$ and F as in the hypotheses of the theorem. Choose an algebraic integer α so that $F = \mathbb{Q}(\alpha)$ and for $t \in \mathbb{Z}$ let $K_t = \mathbb{Q}(\sqrt{\alpha - t})$, $d_t = \operatorname{disc} K_t$ and $\chi_t = \chi_{K_t}$. Since the conjugates of α must all be real, there is a constant c_1 (depending on the choice of α) so that if $t > c_1$ then K_t is totally imaginary and quadratic over F. Moreover, if $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial for α over $\mathbb{Q}$ then $g_t(x) = f(x^2 + t)$ is the minimal polynomial of $\sqrt{\alpha - t}$, and $\operatorname{disc} g_t = (\operatorname{disc} f)^2(-4)^m f(t)$.

The heart of the idea is to make the approximation (7) to $L(s, \chi_t)$ of Proposition 1 as large as possible by forcing enough of the primes that split completely in F to split in K_t as well. Because the splitting behavior of most primes p in K_t is determined by the factorization of $g_t \bmod p$, we are able to reduce the splitting criterion to a congruence condition on $t \bmod p$, and an additional congruence on t is used to ensure that we get the correct Galois group.

Lemma 2. *If an odd prime $p \in \mathbb{Z}$ splits completely in F and does not divide* $\operatorname{disc} f$*, then there exists an integer a_p so that for all $t > c_1$ satisfying $t \equiv a_p \pmod{p^2}$, p ramifies in K_t.*

Proof. Since $p \nmid \operatorname{disc} f$ and p splits completely in F, $f(x)$ must have m distinct roots mod p, each of which lifts to a unique root of $f(x) \bmod p^2$. But each root actually has p distinct lifts to residue classes mod p^2; we can therefore find an integer a_p so that $f(a_p) \equiv 0 \pmod{p}$ and $f(a_p) \not\equiv 0 \pmod{p^2}$. If $t \equiv a_p \pmod{p^2}$ this implies that p divides $\operatorname{disc} g_t$ exactly once. Since the polynomial discriminant and field discriminant differ by a square, we see that if t is so large that g_t is irreducible, then p must divide d_t. That is, p ramifies in K_t. □

Lemma 3. *Let $\alpha_1, \alpha_2, \dots, \alpha_m$ denote the conjugates of α over $\mathbb{Q}$. There are positive integers u and v so that for all t satisfying $t \equiv u \pmod{v}$, $\mathbb{Q}(\{\sqrt{\alpha_i - t}\}_{i=1}^m)$ has degree 2^m over $\mathbb{Q}(\{\alpha_i\}_{i=1}^m)$.*

Proof. Choose odd prime integers $p_1, p_2, \dots, p_m$ satisfying the hypotheses of Lemma 2 and let $v = p_1^2 p_2^2 \cdots p_m^2$. For each i, choose a prime $\mathfrak{p}_i$ of $\widehat{F} = \mathbb{Q}(\{\alpha_i\}_{i=1}^m)$ over p_i. Since each p_i splits completely in F, it does so in $\widehat{F}$, and hence if $\mathcal{O}$ denotes the ring of integers in $\widehat{F}$ we have $\mathbb{Z}/p_i\mathbb{Z} \cong \mathcal{O}/\mathfrak{p}_i$. We can therefore find positive integers a_i so that $a_i \equiv \alpha_i \pmod{\mathfrak{p}_i}$ for all i. This means we must have $f(a_i) \equiv 0 \pmod{p_i}$ and, as above, we can arrange it so that $f(a_i) \not\equiv 0 \pmod{p_i^2}$.

Let u be an integer that satisfies $u \equiv a_i \pmod{p_i^2}$ for every i. If $t \equiv u \pmod{v}$ we claim that for each i, $\mathfrak{p}_i$ exactly divides the ideal $(\alpha_i - t)$ in $\mathcal{O}$ but does not divide $(\alpha_j - t)$ for $j \neq i$. This is enough to prove the lemma, for it obviously implies that no subsequence of $\{\alpha_i - t\}_{i=1}^m$ can have a product equal to a square in $\widehat{F}$. It remains to prove the claim.

If $t \equiv u \pmod{v}$ then $t \equiv a_i \equiv \alpha_i \pmod{\mathfrak{p}_i}$ for each i so that $\mathfrak{p}_i$ divides $(\alpha_i - t)$. Furthermore, p_i exactly divides $f(t)$ and splits completely in $\widehat{F}$, so that $\mathfrak{p}_i$ exactly divides $(f(t))$ in $\mathcal{O}$. Since $f(t)$ is (up to its sign) the product of the $\alpha_j - t$, it must be that $\mathfrak{p}_i$ exactly divides $(\alpha_i - t)$, as claimed. □

Lemma 4. *Let $p \in \mathbb{Z}$ be an odd prime that splits completely in F and does not divide* $\operatorname{disc} f$*. There exists a constant c_2 (depending only on m) so that for each $p > c_2$ there is an integer b_p with the following property: for all $t > c_1$ satisfying $t \equiv b_p \pmod{p}$ one has $\chi_t(\sigma_p) = 2\psi_F(\sigma_p|_{\widehat{F}}) - 1$, where σ_p is any Frobenius element of p in $G(\widehat{K_t}/\mathbb{Q})$.*

Proof. Since $p \nmid \operatorname{disc} f$, p is unramified in F, and therefore $m_p = \psi_F(\sigma_p|_{\widehat{F}})$ is the number of degree 1 primes in F over p, which is in turn equal to the number of linear factors of $f(x)$ mod$p$. Let $r_1, r_2, \ldots, r_{m_p}$ denote the (distinct) roots of $f(x) \bmod p$. As in [6], one can use Weil's bound to show that there is a constant c_2, which depends only on m, so that if $p > c_2$ then there is an integer b_p so that $r_i - b_p$ is a quadratic residue of p for all i. In this situation, $t \equiv b_p \pmod p$ implies that $g_t(x)$ has exactly $2m_p$ roots mod p and that p does not divide $\operatorname{disc} g_t$. If $t > c_1$, so that $g_t(x)$ is irreducible over $\mathbb{Q}$, these conditions mean that there are exactly $2m_p$ primes of K_t over p. Thus

$$\chi_t(\sigma_p) = \psi_{K_t}(\sigma_p) - 1 = 2m_p - 1 = 2\psi_F(\sigma_p|_{\widehat{F}}) - 1.$$

□

Proof of Theorem 1. Choose u and v as in Lemma 3 and let c be a constant that is greater than c_2 of Lemma 4 and greater than every prime divisor of u. Given $x > c$ let P denote the largest prime less than x that splits completely in F and set

$$q = sP^2 \prod_{\substack{c \le p \le x \\ p \ne P}} p.$$

With a_P and b_p as in Lemmas 2 and 4, choose an integer t so that $t \equiv b_p \pmod p$ for all $p \ne P$ dividing q, $t \equiv a_P \pmod{P^2}$ and $t \equiv u \pmod v$. If x is sufficiently large we can furthermore assume that $c_1 < t \le 2q$. It then follows that $K_t \in \mathcal{K}^F(\mathcal{H}, \mathcal{G})$, that P divides the discriminant d_t of K_t, and that $\chi_t(p) = 2\psi_F(\sigma_p|_{\widehat{F}}) - 1$ for each prime $p \ne P$ with $c \le p \le x$.

Since $L(s, \chi_t)$ has conductor $|d_t|$ and we are assuming it is both entire and satisfies GRH, Proposition 1 gives

$$\log L(1, \chi_t) = \sum_{p \le (\log |d_t|)^{1/2}} \chi_t(p) p^{-1} + O_m(1). \tag{18}$$

Because $\operatorname{disc} g_t$ is polynomial in t and is a multiple of d_t we have

$$\log |d_t| \ll \log t \ll \log q \ll x \tag{19}$$

so that $(\log |d_t|)^{1/2} \le x$ for sufficiently large x. The conclusion of the preceding paragraph then gives

$$\log L(1, \chi_t) = \sum_{p \le (\log |d_t|)^{1/2}} (2\psi_F(\sigma_p|_{\widehat{F}}) - 1) p^{-1} + O_m(1). \tag{20}$$

Summing over the conjugacy classes of $G(\widehat{F}/\mathbb{Q})$ and applying the Čebotarev Density Theorem as in the proof of Proposition 2, this yields $L(1, \chi_t) \gg (\log \log |d_t|)^{(1+o(1))}$. Because of the relationship between the regulators of K_t and F, the class number formula (5) yields

$$h \gg |d_t| \, (\log \log |d_t|)^{(1+o(1))} \tag{21}$$

with the implied constant depending only on F. To conclude the proof we simply note that d_t is divisible by P, and that P tends to infinity with x. □

References

[1] Daileda, R. C., *Non-abelian number fields with very large class numbers*, Acta Arith. 125 (3) (2006), 215–255.

[2] Duke, W., *Extreme values of Artin L-functions and class numbers*, Compositio Math. 136 (1) (2003), 103–115.

[3] Duke, W., *Number fields with large class groups*, in Number Theory, CNTA VII, CRM Proceedings, 2004.

[4] Littlewood, J. E., *On the class number of the corpus* $P(\sqrt{-k})$, in Collected papers of J.E. Littlewood. Vol. II, The Clarendon Press, Oxford University Press, 1982, 920–934.

[5] Montgomery, H. L.; Weinberger, P. J., *Real quadratic fields with large class number*, Math. Ann. 225 (2) (1977), 173–176.

[6] Peralta, R., *On the distribution of quadratic residues and nonresidues modulo a prime number*, Math. Comp. 58 (197) (1992), 433–440.

[7] Silverman, J. H., *An Inequality Relating the Regulator and the Discriminant of a Number Field*, J. Number Theory 19 (3) (1984), 437–442.