LMS J. Comput. Math. 17 (Special issue A) (2014) 404–417 © 2014 Author
doi:10.1112/S1461157014000382

Class numbers of real cyclotomic fields of composite conductor

John C. Miller

Abstract

Until recently, the 'plus part' of the class numbers of cyclotomic fields had only been determined for fields of root discriminant small enough to be treated by Odlyzko's discriminant bounds.

However, by finding lower bounds for sums over prime ideals of the Hilbert class field, we can now establish upper bounds for class numbers of fields of larger discriminant. This new analytic upper bound, together with algebraic arguments concerning the divisibility properties of class numbers, allows us to unconditionally determine the class numbers of many cyclotomic fields that had previously been untreatable by any known method.

In this paper, we study in particular the cyclotomic fields of composite conductor.

1. *Introduction*

Ever since mathematicians more than a century ago established connections between Fermat's Last Theorem and the unique factorization properties of cyclotomic integers, the class numbers of cyclotomic fields have been investigated intensively. Among the most mysterious aspects remains the 'plus part' of the class number, that is the class number of the maximal real subfield.

Exploiting Odlyzko's discriminant lower bounds, Masley [3] and van der Linden [2] were able to unconditionally establish the class numbers of all real cyclotomic fields of composite conductor m, provided that $m \leqslant 200$, $\phi(m) \leqslant 72$ and $m \neq 148, 152$. However, for fields of larger degree or conductor, the root discriminant becomes too large for their methods to handle. To overcome the problem of large root discriminants, we establish a lower bound on sums over prime ideals of the Hilbert class field, which in turn establishes an upper bound on the class number. We make further algebraic arguments concerning the divisibility of class numbers in order to prove our main result.

Theorem 1.1. *Let m be a composite integer, $m \not\equiv 2 \,(\mathrm{mod}\, 4)$, and let $\mathbb{Q}(\zeta_m)^+$ denote the maximal real subfield of the mth cyclotomic field $\mathbb{Q}(\zeta_m)$. Then the class number h_m^+ of $\mathbb{Q}(\zeta_m)^+$ is*

$$h_m^+ = \begin{cases} 1 & \text{if } \phi(m) \leqslant 116 \text{ and } m \neq 136, 145, 212, \\ 2 & \text{if } m = 136, \\ 2 & \text{if } m = 145, \\ 1 & \text{if } m = 256, \end{cases}$$

where ϕ is the Euler phi function. Furthermore, under the generalized Riemann hypothesis (GRH), $h_{212}^+ = 5$ and $h_{512}^+ = 1$.

For example, the real cyclotomic field of conductor 420 has class number 1. This is the largest conductor for which the class number of a cyclotomic field has been calculated unconditionally.

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11R18, 11R29 (primary), 11J71, 11R80, 11Y40 (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

This result on composite conductors complements our earlier results on real cyclotomic fields of prime conductor.

THEOREM 1.2 (Miller [5]). *Let p be a prime integer, and let $\mathbb{Q}(\zeta_p)^+$ denote the maximal real subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. Then the class number of $\mathbb{Q}(\zeta_p)^+$ is 1 for $p \leqslant 151$.*

Furthermore, under the assumption of the GRH, the class number h_p^+ of $\mathbb{Q}(\zeta_p)^+$ is

$$h_p^+ = \begin{cases} 1 & \textit{if } p \leqslant 241 \textit{ and } p \neq 163, 191, 229, \\ 4 & \textit{if } p = 163, \\ 11 & \textit{if } p = 191, \\ 3 & \textit{if } p = 229. \end{cases}$$

2. *Upper bounds for class numbers*

A critical step for determining the class number of fields of relatively large degree or discriminant is to find an upper bound for the class number. To accomplish this, Masley [3] and van der Linden [2] exploited Odlyzko's lower bounds of discriminants. Although Odlyzko's tables [7, 8] are unpublished, much information about his estimates for discriminants and related problems can be found in his survey [6].

DEFINITION 1. Let K denote a number field of degree n over $\mathbb{Q}$. Let $d(K)$ denote its discriminant. The *root discriminant* $\mathrm{rd}(K)$ of K is defined to be:

$$\mathrm{rd}(K) = |d(K)|^{1/n}.$$

We can use the relative discriminant formula to prove the following proposition.

PROPOSITION 2.1. *Let L/K be an extension of number fields. Then*

$$\mathrm{rd}(K) \leqslant \mathrm{rd}(L),$$

with equality if and only if L/K is unramified at all finite primes.

Consequently, the root discriminant has the following important property.

COROLLARY 2.2. *Let K be a number field. Then the Hilbert class field of K has the same root discriminant as K.*

Suppose K is a totally real number field of degree n. Odlyzko constructed a table [8] of pairs (A, E) such that the discriminant of K has the lower bound

$$|d(K)| > A^n e^{-E}.$$

If $\mathrm{rd}(K) < A$, we can use Odlyzko's discriminant bounds and Corollary 2.2 to get an upper bound for the class number h,

$$h < \frac{E}{n(\log A - \log \mathrm{rd}(K))}.$$

However, if the root discriminant of K is larger than the largest A in Odlyzko's table, the above method cannot be applied. The largest value for A in Odlyzko's table is 60.704 (or 213.626 if the GRH is assumed).

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

Example 1. The real cyclotomic field $\mathbb{Q}(\zeta_{212})^+$ has root discriminant approximately 98.2080. This root discriminant is too large for the class number to be treated by Odlyzko's unconditional discriminant bounds, but if we assume the GRH, then we can choose a pair $(A, E) = (119.296, 118.11)$ from Odlyzko's table [7] of GRH conditional discriminant bounds to get a class number upper bound

$$h_{212}^+ \leqslant 11$$

which is conditional on the GRH.

In the author's previous paper [4], we obtained unconditional upper bounds for class numbers for fields of root discriminant larger than 60.704 by establishing nontrivial lower bounds for sums over the prime ideals of the Hilbert class field. We repeat here a lemma that will be crucial to our investigation.

Lemma 2.3 (Miller [4]). *Let K be a totally real field of degree n, and let*

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh(x/2)}$$

for some positive constant c. Suppose S is a subset of the prime integers which totally split into principal prime ideals of K. Let

$$B = \frac{\pi}{2} + \gamma + \log 8\pi - \log \mathrm{rd}(K) - \int_0^\infty \frac{1-F(x)}{2}\left(\frac{1}{\sinh(x/2)} + \frac{1}{\cosh(x/2)}\right) dx \\ + 2\sum_{p\in S}\sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p).$$

If $B > 0$ then we have an upper bound for the class number h of K,

$$h < \frac{2c\sqrt{\pi}}{nB}.$$

Note that the above upper bound is unconditional on the GRH.

If x is in the ring of integers of K, and if its norm is a prime integer p which is unramified in K, then p totally splits into principal ideals, and we can take p to be in the set S above. Once we find sufficiently many such prime integers which totally split into principal ideals, so that $B > 0$, we can establish an upper bound for the class number.

3. *Real cyclotomic fields*

We briefly recall a few facts about real cyclotomic fields and establish some notation. More information can be found in Washington's *Introduction to Cyclotomic Fields* [11].

Let ζ_m be a primitive mth root of unity. Then $\mathbb{Q}(\zeta_m)$ is the cyclotomic field of conductor m. Its maximal real subfield, also known as the real cyclotomic field of conductor m, is $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, which we will usually denote by $\mathbb{Q}(\zeta_m)^+$. The degree of $\mathbb{Q}(\zeta_m)^+$ over $\mathbb{Q}$ is $\phi(m)/2$, where ϕ is the Euler phi function.

The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$, and the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})$ of the real cyclotomic field is isomorphic to the quotient group $(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$. Galois theory determines the subfields of $\mathbb{Q}(\zeta_m)^+$.

The ring of integers of $\mathbb{Q}(\zeta_m)^+$ is simply $\mathbb{Z}[\zeta_m + \zeta_m^{-1}] = \mathbb{Z}[2\cos(2\pi/m)]$. The prime integers which totally split in this field are precisely those which are congruent to ± 1 modulo m.

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

We will denote the class number of $\mathbb{Q}(\zeta_m)$ by h_m and the class number of its maximal real subfield (the 'plus part') by h_m^+. The 'minus part' h_m^- is defined to be the relative class number

$$h_m^- = \frac{h_m}{h_m^+}.$$

Let $n = \phi(m)/2$ and let $a_1, a_1, \ldots, a_n$ be those positive integers (in increasing order) that are less than $m/2$ and coprime to m. Until otherwise noted, the integral basis of $\mathbb{Q}(\zeta_m)^+$ that we will use is $\{b_0, b_1, \ldots, b_{n-1}\}$, with $b_0 = 1$ and $b_j = 2\cos(2\pi a_j/m)$ for $j = 1, \ldots, n-1$.

Given an element x of a Galois number field K, we define its *norm* to be

$$N(x) = \left| \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(x) \right|.$$

4. *Divisibility properties of the class numbers of real cyclotomic fields*

In the author's previous paper on cyclotomic fields of prime conductor [5], we were able to take advantage of the extensive work of Schoof [9] on the divisibility properties of class numbers h_p^+ for p prime. Real cyclotomic fields of prime power conductor have the special property that the index of the group of cyclotomic units $\mathcal{O}_{\mathrm{cyc}}^\times$ within the full group of units $\mathcal{O}^\times$ is equal to the class number. This allowed Schoof to study the Galois action on the quotient group $\mathcal{O}^\times/\mathcal{O}_{\mathrm{cyc}}^\times$, rather than class group itself, to extract information about the class number.

However, once we move away from prime power conductors, the size of the quotient group $\mathcal{O}^\times/\mathcal{O}_{\mathrm{cyc}}^\times$ is no longer equal to the class number. To some extent, Agathocleous, in her thesis [1], was able to get around this problem, but with the limitation of considering only composite conductors that are products pq of two distinct odd primes. This is actually quite a severe limitation for us: only 9 of the 50 fields we considered have such conductors.

Therefore, in the current paper, we return to the classical approach of exploiting the Galois action on the class group itself, as implemented by Masley [3] and van der Linden [2]. This approach has its limitations, especially when considering the p-part of the class number where p divides the degree of the field. Nevertheless, by establishing quite good upper bounds on the class numbers, we are able to successfully use these methods.

In order to carry out our strategy, we use several theorems described by van der Linden [2], Masley [3] and Washington [11].

Parity Check Theorem (Masley [3, Theorem 2.21]). *If h_m^- is odd, then h_m^+ is odd.*

Reflection Theorem (Masley [3, Theorem 2.22]). *Let p be a prime integer, and let M be the least common multiple of p and the conductor m. If p does not divide h_M^-, then p does not divide h_m^+.*

We will use the tables in Washington [11, p. 412] to find the minus part h_m^- of the class number.

Pushing Up Theorem (Washington [11, Proposition 4.11]). *Let L/K be an extension of number fields. If no intermediate field $M \neq K$ of L/K is abelian over K and unramified (at all primes, including the Archimedean ones) over K, then h_K divides h_L.*

Corollary 4.1. *h_m^+ divides h_{km}^+ for any positive integer k.*

Corollary 4.2. *If K is a subfield of a real cyclotomic field of prime power conductor p^k, then h_K divides $h_{p^k}^+$.*

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

Pushing Down Theorem (Washington [11, Theorem 10.4]). *Let L/K be a Galois extension of number fields whose degree is a power of a prime p. Suppose that there is at most one prime (finite or infinite) of K that ramifies in L. If p does not divide h_K, then p does not divide h_L.*

Theorem 4.3 (Masley [3, Theorem 2.10]). *Let $m = 4p, pq$ or $2^a q$, with $a \geqslant 3$, p and q odd primes, and $q \equiv 3 \pmod 4$. Then the maximal real abelian 2-extension K of $\mathbb{Q}$ with conductor m has odd class number.*

Rank Theorem (Masley [3, Corollary 2.15]). *Let L/K be a cyclic extension of degree n. Let p be a prime that does not divide h_E for all intermediate fields E with $K \subseteq E \subsetneq L$. If p divides h_L, then p^f divides h_L, where f is the order of p modulo n.*

We also give the more precise version of the Rank Theorem described by van der Linden [2]. Given a cyclic extension of number fields L/K of degree n, and a prime p not dividing n, we define $\mathrm{Cl}_p^*(L/K)$ to be

$$\mathrm{Cl}_p^*(L/K) = \{\alpha \in \mathrm{Cl}_p(L) : \alpha^{\Phi_n(\sigma)} = 1\},$$

where $\mathrm{Cl}_p(L)$ is the Sylow p-subgroup of the class group of L, σ is the generator of $\mathrm{Gal}(L/K)$, and Φ_n is the nth cyclotomic polynomial. For example, given the trivial extension K/K, we have $\mathrm{Cl}_p^*(K/K) = \mathrm{Cl}_p(K)$.

Theorem 4.4 (van der Linden [2, Theorem 8]). *Let L/K be a cyclic extension of degree n. Let p be a prime that does not divide n. Then $|\mathrm{Cl}_p^*(L/K)|$ is a power of p^f, possibly 1, where f is the order of p modulo n.*

Theorem 4.5 (van der Linden [2, Theorem 6]). *Let E/K be an abelian extension of number fields of degree n, and let p be a prime integer not dividing n. Then*

$$\mathrm{Cl}_p(E) \cong \oplus\, \mathrm{Cl}_p^*(L/K),$$

where the direct sum is over all the intermediate fields L for which L/K is cyclic.

Corollary 4.6. *Suppose p, K and E are as in the theorem above. If p divides h_E, then there exists a cyclic extension L/K, with $K \subseteq L \subseteq E$ and p dividing h_L.*

5. *The class number of the real cyclotomic field of conductor* 148

We give a detailed example of applying our upper bound to find the class number of the real cyclotomic field of conductor 148.

Van der Linden [2] proved that the class number of $\mathbb{Q}(\zeta_{148})^+$ has class number 1, conditional upon the GRH. The root discriminant of this field is approximately 66.94, which is greater than 60.704, so Odlyzko's discriminant bounds could not be used to establish an unconditional upper bound on the class number. However, using our class number upper bound, we can now unconditionally prove that the real cyclotomic field of conductor 148 has class number 1.

Proposition 5.1. *The class number of $\mathbb{Q}(\zeta_{148})^+$ is 1.*

Proof. First, using our integral basis $\{b_0, b_1, \ldots, b_{n-1}\}$, we search over 'sparse vectors' and find two elements of the ring of integers that have norms of 149 and 443:

$$N(b_0 + b_1 + b_8) = 149,$$
$$N(b_0 + b_1 + b_9) = 443.$$

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

Since the prime integers 149 and 443 are congruent to ±1 modulo 148, they totally split in $\mathbb{Q}(\zeta_{148})^+$, and split into principal ideals generated by the above elements and their conjugates. We define our set S to be

$$S = \{149, 443\}.$$

Let F be the function

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh(x/2)}$$

with $c = 20$. The contribution from prime ideals of the Hilbert class field is bounded below by

$$2 \sum_{p\in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p) > 2 \sum_{p\in S} \frac{\log p}{\sqrt{p}} F(\log p) > 0.1753.$$

The following integral can be estimated using numerical integration:

$$\int_0^{\infty} \frac{1 - F(x)}{2} \left(\frac{1}{\sinh(x/2)} + \frac{1}{\cosh(x/2)} \right) dx < 1.2825.$$

Thus we find a lower bound for B,

$$\begin{aligned} B = {} & \frac{\pi}{2} + \gamma + \log 8\pi - \log \operatorname{rd}(\mathbb{Q}(\zeta_{148})^+) - \int_0^{\infty} \frac{1 - F(x)}{2} \left(\frac{1}{\sinh(x/2)} + \frac{1}{\cosh(x/2)} \right) dx \\ & + 2 \sum_{p\in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p) > 0.0611. \end{aligned}$$

Now we can apply Lemma 2.3 to show that the class number has an upper bound

$$h_{148}^+ \leqslant 32.$$

It remains to use divisibility arguments to show that the class number is 1. We consider the possible prime divisors of h_{148}^+.

2-*part*. Since $h_{148}^- = 4\,827\,501$ is odd, the Parity Check Theorem shows that h_{148}^+ is odd.

3-*part*. The degree of $\mathbb{Q}(\zeta_{148})^+$ is 36. Consider its quartic subfield K_4. The prime integer 37 is totally ramified in K_4 and factors as

$$(37) = P^4$$

for a prime ideal P. The prime P is the only prime that ramifies in the degree 9 extension $\mathbb{Q}(\zeta_{148})^+/K_4$. Since K_4 has class number 1 (which has small enough degree that it can be calculated unconditionally in a software package such as Sage [10]), we can use the Pushing Down Theorem to show that 3 does not divide h_{148}^+.

p-part, $5 \leqslant p \leqslant 31$ $\mathbb{Q}(\zeta_{148})^+/\mathbb{Q}$ is a cyclic extension. Every proper subfield of $\mathbb{Q}(\zeta_{148})^+$ is either a subfield of $\mathbb{Q}(\zeta_{37})^+$, or is the degree 12 subfield K_{12}, or is the quartic subfield K_4. Using Sage, we can calculate unconditionally that K_4 and K_{12} have class number 1. Also, the subfield $\mathbb{Q}(\zeta_{37})^+$ has class number 1. Since $\mathbb{Q}(\zeta_{37})^+/\mathbb{Q}$ is totally ramified at 37, by the Pushing Up Theorem every subfield of $\mathbb{Q}(\zeta_{37})^+$ has class number 1. Thus, using the extension $\mathbb{Q}(\zeta_{148})^+/\mathbb{Q}$ and the upper bound $h_{148}^+ \leqslant 32$, we can apply the Rank Theorem to show that p does not divide h_{148}^+ for all p between 5 and 31.

Using the upper bound $h_{148}^+ \leqslant 32$, we conclude unconditionally that $h_{148}^+ = 1$. □

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

Note that the Minkowski bound of $\mathbb{Q}(\zeta_{148})^+$ is approximately 2.5×10^{18}. It is striking that, using our new approach, we needed to only check if *two* primes, 149 and 443, factored into principal ideals, in stark contrast to using the Minkowski bound, which would have required checking roughly 6×10^{16} primes!

As an alternative proof, in the following section we will show below that an upper bound of h^+_{148} is 1, thus showing that $h^+_{148} = 1$, without need for any additional algebraic arguments.

6. *Upper bounds for class numbers of real cyclotomic fields of degree less than or equal to* 58

Consider the real cyclotomic field of conductor m with degree n. For real cyclotomic fields of relatively small degree, it is possible to use relatively few prime ideals to find a class number upper bound. However, for fields of larger degree, the number of primes required is much greater. Our strategy will be to search over sparse vectors using both the basis $b_0, b_1, \ldots, b_{n-1}$ described above, as well as using an alternative basis,

$$c_k = \sum_{j=0}^{k} b_j, \quad k = 0, 1, \ldots, n-1.$$

The advantage of using the alternative basis is its tendency to find elements that are of different norm than those found using sparse vectors in the original basis.

We calculate the norm of every element of the ring of integers of the form

$$x = b_0 + b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5}$$

and

$$x = b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5},$$

where $1 < j_1 < j_2 < j_3 < j_4 < j_5 < n$ and $a_j \in \{-1, 0, 1\}$ for $1 \leqslant j \leqslant 5$. Similarly, using the alternative basis, we also calculate the norm of every element of the form

$$x = c_0 + a_1 c_{k_1} + a_2 c_{k_2} + a_3 c_{k_3} + a_4 c_{k_4} + c_5 b_{k_5},$$

where $1 \leqslant k_1 < k_2 < k_3 < k_4 < k_5 < n$ and $a_k \in \{-1, 0, 1\}$ for $1 \leqslant k \leqslant 5$.

Let T denote the set of all such elements x, and let S denote the set of norms that are prime, congruent to ± 1 modulo the conductor m, and less than 10^{10},

$$S = \{N(x) : x \in T, N(x) \text{ prime}, N(x) \equiv \pm 1 \pmod{m}, N(x) < 10^{10}\}.$$

We calculate the set S for every real cyclotomic field of composite conductor m of degree up to 58, that is, with $\phi(m) \leqslant 116$, except for the fields that have already been treated unconditionally by Masley or van der Linden. We also exclude the conductor 212, for reasons to be discussed later. We then apply Lemma 2.3. The results are given in Table 1 of conductors m, parameter c, and upper bounds of class numbers h^+_m.

We are free to choose the parameter c. Recall that our class number bound is $h < 2c\sqrt{\pi}/nB$. If c is chosen to be too small, then the lower bound for the denominator B would be nonpositive or very small. On the other hand, if c is too large, this leads directly to a large class number bound. Thus, there is an optimal c that provides the best possible bound. However, since the class number is an integer, the class number bound is usually not sensitive to the precise choice of c, so it is easy to just compute an optimal c by testing in a reasonable interval.

We should also remark that if we had calculated the table of class number upper bounds using summations over a larger number of principal prime ideals, then we could have improved upper bounds, obviating the need for some of the algebraic arguments in § 7. There is a trade-off between the amount of computation and the amount of algebraic argumentation.

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

7. *Class numbers of real cyclotomic fields of degree up to* 58

The above upper bounds are sufficiently strong to immediately show that the real cyclotomic fields of conductors

$$115, 147, 148, 152, 165, 195, 200, 204, 216, 220, 228, 240, 252, 264, 300, 420$$

have class number 1.

In the following, all invocations of the Parity Check Theorem and the Reflection Theorem use minus parts of the class numbers obtained from the table in Washington [11, p. 412]. In particular, an application of the Parity Check Theorem shows that the real cyclotomic fields of conductors

$$119, 129, 141, 125, 176, 196$$

also have class number 1.

For conductor 145, we will need a better upper bound, so the proof of that class number will be postponed until the next section. The remaining fields are treated below.

PROPOSITION 7.1. *The class number of* $\mathbb{Q}(\zeta_{121})^+$ *is* 1.

Proof. We have the upper bound $h^+_{121} \leqslant 4$. By the Parity Check Theorem, h^+_{121} is odd. The least common multiple of 3 and 121 is 363. Since 3 does not divide h^-_{363}, the Reflection Theorem shows that 3 does not divide h^+_{121}. □

PROPOSITION 7.2. *The class numbers of* $\mathbb{Q}(\zeta_{123})^+$, $\mathbb{Q}(\zeta_{153})^+$, $\mathbb{Q}(\zeta_{164})^+$ *and* $\mathbb{Q}(\zeta_{224})^+$ *are* 1.

Proof. Let L denote one of these fields, and let K denote the maximal 2-subextension of $L/\mathbb{Q}$. We have the upper bound for the class number $h(L) \leqslant 2$. By Theorem 4.3, the class number of K is odd. We apply the Rank Theorem to the extension L/K to show that $h(L)$ is odd. □

TABLE 1. *Upper bounds for class numbers* h^+_m *of real cyclotomic fields of conductor* m, *using parameter* c *in Lemma* 2.3.

m	c	$h^+_m \leqslant$
115	18	1
119	20	2
121	26	4
123	19	2
125	22	2
129	19	2
133	25	3
141	20	2
145	50	36
147	18	1
148	17	1
152	17	1
153	21	2
159	25	3
164	20	2
165	15	1
171	26	4
172	20	2
176	20	2
177	29	5
184	22	3
188	23	3
189	24	3
195	21	1
196	20	2
200	18	1
204	15	1
208	25	3
216	18	1
220	18	1
224	22	2
228	15	1
232	30	8
236	48	29
240	15	1
252	15	1
260	21	2
264	18	1
276	20	2
280	20	2
288	24	3
300	18	1
312	20	2
324	28	5
336	21	2
348	26	4
360	21	2
420	18	1

Proposition 7.3. *The class number of* $\mathbb{Q}(\zeta_{133})^+$ *is* 1.

Proof. We know $h^+_{133} \leqslant 3$. We apply Theorem 4.5 to the degree 27 extension $\mathbb{Q}(\zeta_{133})^+/\mathbb{Q}(\sqrt{133})$. The cyclic subextensions are of degree 1, 3 or 9. Since the class number of $\mathbb{Q}(\sqrt{133})$ is 1, by Theorems 4.4 and 4.5, the 2-part of h^+_{133} must be a power of 4. Since $h^+_{133} \leqslant 3$, we have that h^+_{133} is odd.

For the 3-part, consider the sextic subfield K of $\mathbb{Q}(\zeta_{133})^+$ that has discriminant $7^5 \cdot 19^3$. The class number of K is 1. The prime integer 19 factors as $(19) = P^2$ in K for a prime ideal P. The prime P is the only prime of K that ramifies in $\mathbb{Q}(\zeta_{133})^+$, so we can apply the Pushing Down Theorem to show that 3 does not divide h^+_{133}. □

Proposition 7.4. *The class number of* $\mathbb{Q}(\zeta_{159})^+$ *is* 1.

Proof. We know $h^+_{159} \leqslant 3$. By the Parity Check Theorem, h^+_{159} is odd. Every proper subfield of $\mathbb{Q}(\zeta_{159})^+$ is either the quartic subfield K_4, or is a subfield of $\mathbb{Q}(\zeta_{53})^+$. Using Sage [10], we can calculate unconditionally that the class number of K_4 is 1. Also, $\mathbb{Q}(\zeta_{53})^+$ has class number 1. Since $\mathbb{Q}(\zeta_{53})^+/\mathbb{Q}$ is totally ramified at 53, by the Pushing Up Theorem every subfield of $\mathbb{Q}(\zeta_{53})^+$ has class number 1. Therefore, we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{159})^+/\mathbb{Q}$ to show that 3 does not divide h^+_{159}. □

Proposition 7.5. *The class number of* $\mathbb{Q}(\zeta_{171})^+$ *is* 1.

Proof. We know $h^+_{171} \leqslant 4$. We apply Theorem 4.5 to the degree 27 extension $\mathbb{Q}(\zeta_{171})^+/\mathbb{Q}(\sqrt{57})$. The cyclic subextensions are of degree 1, 3 or 9. The class number of $\mathbb{Q}(\sqrt{57})$ is 1, and the four cubic extensions of $\mathbb{Q}(\sqrt{57})$ contained in $\mathbb{Q}(\zeta_{171})^+$ all have odd class number (either 1 or 3). So we need only concern ourselves with the degree 9 cyclic subextensions of $\mathbb{Q}(\zeta_{171})^+/\mathbb{Q}(\sqrt{57})$. Therefore, by Theorems 4.4 and 4.5, the 2-part of h^+_{171} must be a power of 64. Since $h^+_{171} \leqslant 4$, we have that h^+_{171} is odd.

The prime 3 factors as $(3) = P^2$ in $\mathbb{Q}(\zeta_{57})^+$ for a prime ideal P. The prime P is the only prime of $\mathbb{Q}(\zeta_{57})^+$ that ramifies in $\mathbb{Q}(\zeta_{171})^+$, so we can apply the Pushing Down Theorem to show that 3 does not divide h^+_{171}. □

Proposition 7.6. *The class number of* $\mathbb{Q}(\zeta_{172})^+$ *is* 1.

Proof. We know $h^+_{172} \leqslant 2$. $\mathbb{Q}(\zeta_{172})^+$ is of degree 42. Let K denote its sextic subfield. We can use Sage [10] to show unconditionally that the class number of K is 1. We apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{172})^+/K$ to show that h^+_{172} is odd. □

Proposition 7.7. *The class number of* $\mathbb{Q}(\zeta_{177})^+$ *is* 1.

Proof. We know $h^+_{177} \leqslant 5$. By the Parity Check Theorem, h^+_{177} is odd. Every proper subfield of $\mathbb{Q}(\zeta_{177})^+$ is either $\mathbb{Q}(\sqrt{177})$ or is a subfield of $\mathbb{Q}(\zeta_{59})^+$. The quadratic subfield $\mathbb{Q}(\sqrt{177})$ has class number 1. Also, $\mathbb{Q}(\zeta_{59})^+$ has class number 1, as do its subfields by the Pushing Down Theorem. Therefore we can apply the Rank Theorem to the degree 58 cyclic extension $\mathbb{Q}(\zeta_{177})^+/\mathbb{Q}$ to show that neither 3 nor 5 divides h^+_{177}. □

Proposition 7.8. *The class numbers of* $\mathbb{Q}(\zeta_{184})^+$ *and* $\mathbb{Q}(\zeta_{276})^+$ *are* 1.

Proof. These fields have degree 44. Let L denote either of these fields, and K denote the quartic subfield. We know $h(L) \leqslant 3$. We can use Sage [10] to show unconditionally that the class number of K is 1. We apply the Rank Theorem to the extension L/K to show that neither 2 nor 3 divide h_L. □

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

Proposition 7.9. *The class number of* $\mathbb{Q}(\zeta_{188})^+$ *is* 1.

Proof. We know $h_{188}^+ \leqslant 3$. By the Parity Check Theorem, h_{188}^+ is odd. The least common multiple of 3 and 188 is 576. Since 3 does not divide h_{576}^-, the Reflection Theorem shows that 3 does not divide h_{188}^+. □

Proposition 7.10. *The class number of* $\mathbb{Q}(\zeta_{189})^+$ *is* 1.

Proof. We know $h_{189}^+ \leqslant 3$. By the Parity Check Theorem, h_{189}^+ is odd. The least common multiple of 3 and 189 is 189. Since 3 does not divide h_{189}^-, the Reflection Theorem shows that 3 does not divide h_{189}^+. □

Proposition 7.11. *The class numbers of* $\mathbb{Q}(\zeta_{208})^+$ *and* $\mathbb{Q}(\zeta_{288})^+$ *are* 1.

Proof. Let $m = 208$ or 288. We know $h_m^+ \leqslant 3$. By the Parity Check Theorem, h_m^+ is odd. Consider the degree 4 cyclic extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}(\zeta_{m/4})^+$. Since we already know that $h_{m/4}^+ = h_{m/2}^+ = 1$, we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}(\zeta_{m/4})^+$ to show that 3 does not divide h_m^+. □

Proposition 7.12. *The class number of* $\mathbb{Q}(\zeta_{232})^+$ *is* 1.

Proof. We know $h_{232}^+ \leqslant 8$.

The prime integer 2 is inert in $\mathbb{Q}(\zeta_{29})^+$. The prime ideal (2) is the only prime that ramifies in the degree 4 extension $\mathbb{Q}(\zeta_{232})^+/\mathbb{Q}(\zeta_{29})^+$. Since $h_{29}^+ = 1$, the Pushing Down Theorem shows that h_{232}^+ is odd.

Now let K be the octic subfield of $\mathbb{Q}(\zeta_{232})^+$. Since the class number of K is 1, we can apply the Rank Theorem to the degree 7 extension $\mathbb{Q}(\zeta_{232})^+/K$ to find that h_{232}^+ is not divisible by 3 or 5.

The prime 29 factors as $(29) = P^2$ in K for a prime ideal P. P is the only prime of K that ramifies in $\mathbb{Q}(\zeta_{232})^+$, so we can apply the Pushing Down Theorem to show that 7 does not divide h_{232}^+. □

Proposition 7.13. *The class number of* $\mathbb{Q}(\zeta_{236})^+$ *is* 1.

Proof. We know $h_{236}^+ \leqslant 29$. Since the class number of $\mathbb{Q}(\sqrt{59})$ is 1, we can apply the Rank Theorem to the degree 29 cyclic extension $\mathbb{Q}(\zeta_{236})^+/\mathbb{Q}(\sqrt{59})$ to show that no prime less than 29 divides h_{236}^+.

It remains to show that 29 does not divide h_{236}^+. The only prime ideal of $\mathbb{Q}(\sqrt{59})$ that ramifies in $\mathbb{Q}(\zeta_{236})^+$ is $(\sqrt{59})$, so we can apply the Pushing Down Theorem to show that 29 does not divide h_{236}^+. □

Proposition 7.14. *The class number of* $\mathbb{Q}(\zeta_{260})^+$ *is* 1.

Proof. We know $h_{260}^+ \leqslant 2$, and $\mathbb{Q}(\zeta_{260})^+$ is of degree 48. Let L denote its degree 16 subfield. L has three octic subfields. Let K denote the octic subfield with discriminant $2^8 \cdot 5^4 \cdot 13^6$. Sage [10] can show unconditionally that K has class number 1. The prime integer 5 factors as $(5) = P^2$ in K for a prime ideal P. The only prime ideal of K that ramifies in L is P, so by the Pushing Down Theorem, the class number of L is odd. Now we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{260})^+/L$ to show that h_{260}^+ is odd. □

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

PROPOSITION 7.15. *The class numbers of* $\mathbb{Q}(\zeta_{280})^+$, $\mathbb{Q}(\zeta_{312})^+$ *and* $\mathbb{Q}(\zeta_{360})^+$*are* 1.

Proof. Let $m = 280$, 312 or 360. We know $h_m^+ \leqslant 2$. The prime integer 2 is inert in $\mathbb{Q}(\zeta_{m/8})^+$. The prime ideal (2) is the only prime that ramifies in the degree 4 extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}(\zeta_{m/8})^+$. Since $h_{m/8}^+ = 1$, the Pushing Down Theorem shows that h_m^+ is odd. □

PROPOSITION 7.16. *The class number of* $\mathbb{Q}(\zeta_{324})^+$ *is* 1.

Proof. We know $h_{324}^+ \leqslant 5$. By the Parity Check Theorem, h_{324}^+ is odd. The least common multiple of 3 and 324 is 324. Since 3 does not divide h_{324}^-, the Reflection Theorem shows that 3 does not divide h_{324}^+.

Finally, since $\mathbb{Q}(\zeta_{324})^+$ is cyclic of degree 54, every proper subfield of $\mathbb{Q}(\zeta_{324})^+$ is a subfield of $\mathbb{Q}(\zeta_{81})^+$, which has class number 1. Since $\mathbb{Q}(\zeta_{81})^+/\mathbb{Q}$ is totally ramified at 3, by the Pushing Up Theorem every subfield of $\mathbb{Q}(\zeta_{81})^+$ has class number 1. Therefore, we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{324})^+/\mathbb{Q}$ to show that 5 does not divide h_{324}^+. □

PROPOSITION 7.17. *The class number of* $\mathbb{Q}(\zeta_{336})^+$ *is* 1.

Proof. We know $h_{336}^+ \leqslant 2$. The prime integer 2 is inert in $\mathbb{Q}(\zeta_{21})^+$. The prime ideal (2) is the only prime that ramifies in the degree 8 extension $\mathbb{Q}(\zeta_{336})^+/\mathbb{Q}(\zeta_{21})^+$. Since $h_{21}^+ = 1$, the Pushing Down Theorem shows that h_{336}^+ is odd. □

PROPOSITION 7.18. *The class number of* $\mathbb{Q}(\zeta_{348})^+$ *is* 1.

Proof. We know $h_{348}^+ \leqslant 4$. The prime integer 2 is inert in $\mathbb{Q}(\zeta_{87})^+$. The prime ideal (2) is the only prime that ramifies in the quadratic extension $\mathbb{Q}(\zeta_{348})^+/\mathbb{Q}(\zeta_{87})^+$. Since $h_{87}^+ = 1$, the Pushing Down Theorem shows that h_{348}^+ is odd.

Now let K be the octic subfield of $\mathbb{Q}(\zeta_{348})^+$. Since the class number of K is 1, we can apply the Rank Theorem to the degree 7 extension $\mathbb{Q}(\zeta_{348})^+/K$ to find that h_{348}^+ is not divisible by 3. □

8. *The class number of the real cyclotomic field of conductor* 145

Under the assumption of the GRH, van der Linden [2] proved that the class number of $\mathbb{Q}(\zeta_{145})^+$ is 2, and he proved unconditionally that 2 divides h_{145}^+. So far, we have obtained the unconditional upper bound $h_{145}^+ \leqslant 36$. However, it is difficult to pin down the exact class number; the 2-parts and 7-parts of the class number pose difficulties. We will endeavor to find an improved upper bound.

We consider the sparse vectors

$$x = b_0 + b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5} + a_6 b_{j_6}$$

and

$$x = b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5} + a_6 b_{j_6},$$

where $1 < j_1 < j_2 < j_3 < j_4 < j_5 < j_6 < n$ and $a_j \in \{-1, 0, 1\}$ for $1 \leqslant j \leqslant 6$, and

$$x = c_0 + a_1 c_{k_1} + a_2 c_{k_2} + a_3 c_{k_3} + a_4 c_{k_4} + c_5 b_{k_5} + c_6 b_{k_6},$$

where $1 \leqslant k_1 < k_2 < k_3 < k_4 < k_5 < k_6 < n$ and $a_k \in \{-1, 0, 1\}$ for $1 \leqslant k \leqslant 6$.

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

Let T denote the set of all such elements x, and let U be the set of their norms, up to 10^{19}, that are congruent to ± 1 modulo the conductor m:

$$U = \{N(x) : x \in T, N(x) < 10^{19}, N(x) \equiv \pm 1 \,(\operatorname{mod} m)\}.$$

Let S_1 be the set of prime norms

$$S_1 = \{p : p \in U, p \text{ prime}, \, p \equiv \pm 1 \,(\operatorname{mod} m)\}.$$

For a field of such large discriminant and nontrivial class group, it is more difficult to find sufficiently many totally split primes of prime norm. An effective approach is to search for sparse vectors that have large composite norms, and then take quotients of appropriately chosen algebraic integers.

Following the above strategy, we define S_2 to be the set of primes defined by

$$S_2 = \{p : pq \in U, p \text{ prime}, \, p \notin S_1, q \in S_1\},$$

noting that if $N(x) = pq$ and $N(y) = q$, for x, y in the ring of integers $\mathcal{O}$, then $x/\sigma(y) \in \mathcal{O}$ with norm p for some Galois automorphism σ, and p is congruent to ± 1 modulo m.

Now put $S = S_1 \cup S_2$ and $c = 42$. We have the following lower bound for the contribution of prime ideals:

$$2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p) > 2\sum_{p\in S}\sum_{m=1}^{2}\frac{\log p}{p^{m/2}}F(m\log p) > 0.5410.$$

Applying Lemma 2.3, we have $B > 0.1906$, so the class number is bounded above by 13.95. Therefore,

$$h_{145}^{+} \leqslant 13.$$

Now we can prove the following unconditionally.

Proposition 8.1. *The class number of* $\mathbb{Q}(\zeta_{145})^{+}$ *is* 2.

Proof. Let K be the octic subfield of $\mathbb{Q}(\zeta_{145})^{+}$. Using Sage [**10**], we can show unconditionally that K has class number 2. We apply Theorems 4.4 and 4.5 to the degree 7 extension $\mathbb{Q}(\zeta_{145})^{+}/K$ to find that the 2-part of h_{145}^{+} is equal to

$$2 \cdot 8^{t}$$

for some nonnegative integer t. Since $h_{145}^{+} \leqslant 13$, we have shown that the 2-part of h_{145}^{+} is precisely equal to 2.

We can also apply the Rank Theorem to $\mathbb{Q}(\zeta_{145})^{+}/K$ to show that neither 3 nor 5 divides h_{145}^{+}. Finally, since h_{145}^{+} is even and less than or equal to 13, we know that primes greater than or equal to 7 do not divide the class number. □

9. *The class number of the real cyclotomic field of conductors* 212, 256 *and* 512

As we will see, the class group of the real cyclotomic field of conductor 212 is nontrivial, so it is of course more difficult to find principal prime ideals of small norm. The missing contribution from these primes of small norm must be replaced by a quite large number of primes of greater norm. In fact, so many principal prime ideals are required that it is difficult to establish an unconditional upper bound on the class number. However, if we assume the GRH, it is quite easy to find an upper bound, as we have already seen in Example 1.

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

PROPOSITION 9.1. *Under the assumption of the GRH, the class number of $\mathbb{Q}(\zeta_{212})^+$ is 5.*

Proof. Using Odlyzko's discriminant lower bounds, we have already shown in Example 1 that

$$h_{212}^+ \leqslant 11$$

conditional upon GRH.

Let K be the quartic subfield of $\mathbb{Q}(\zeta_{212})^+$. Using Sage [10], we can calculate the class number of K is 5. By the Pushing Up Theorem, 5 divides h_{212}^+. By the Parity Check Theorem, h_{212}^+ is odd, so we can conclude (conditional on GRH) that $h_{212}^+ = 5$. □

Finally, the calculation of the class numbers of the real cyclotomic fields of conductors 256 and 512 can be found in the author's earlier paper [4], concluding the proof of Theorem 1.1.

10. *Concluding remarks*

As part of our main result, we unconditionally calculated the class numbers of nine fields of conductor pq, with p and q distinct odd primes. The odd parts of their class numbers were all trivial, which confirms previous results of the thesis of Agathocleous [1].

Also, to reach our main result, we calculated the class numbers of 25 fields of composite conductor larger than 200, most of which had not previously had their class numbers calculated even conditionally on the GRH. Of those fields, only the real cyclotomic field of conductor 212 had a nontrivial class group. So the results match closely with our expectation that these fields should have small class number and be predominantly class number 1.

It is possible use the methods in this paper to unconditionally calculate the class numbers of even higher conductors, but the amount of required calculation of principal prime ideals would grow roughly exponentially with the conductor. This problem can be alleviated by assuming the GRH, requiring us to find far fewer principal prime ideals. However, even under GRH, the 'principal ideal problem' for fields of very large degree or discriminant becomes quite challenging.

It is possible to extend these techniques beyond cyclotomic fields. For example, the author is currently investigating the application of the methods of this paper to certain nonabelian number fields.

Acknowledgements. I would like to thank my advisor, Henryk Iwaniec, for introducing me to the class number problems of cyclotomic fields, and for his continuing encouragement. I am particularly thankful for the advice and support of Lawrence Washington and René Schoof. I sincerely appreciate the careful reading and suggestions of the three anonymous referees.

References

1. E. Agathocleous, 'Class Numers of Real Cyclotomic Fields of Conductor pq', PhD Thesis, University of Maryland, College Park, http://drum.lib.umd.edu/handle/1903/9832.
2. F. J. van der Linden, 'Class number computations of real abelian number fields', *Math. Comp.* 39 (1982) no. 160, 693–707.
3. J. M. Masley, 'Class numbers of real cyclic number fields with small conductor', *Compos. Math.* 37 (1978) no. 3, 297–319.
4. J. C. Miller, 'Class numbers of totally real fields and applications to the Weber class number problem', *Acta Arith.*, to appear, arXiv:1405.1094.
5. J. C. Miller, 'Real cyclotomic fields of prime conductor and their class numbers', *Math. Comp.*, to appear, arXiv:1407.2373.
6. A. M. Odlyzko, 'Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results', *Sém. Théor. Nombres Bordeaux* (2) 2 (1990) no. 1, 119–141.

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press

7. A. M. Odlyzko, 'Table 3: GRH bounds for discriminants', http://www.dtc.umn.edu/∼odlyzko/unpublished/discr.bound.table3.

8. A. M. Odlyzko, 'Table 4: Unconditional bounds for discriminants', http://www.dtc.umn.edu/∼odlyzko/unpublished/discr.bound.table4.

9. R. Schoof, 'Class numbers of real cyclotomic fields of prime conductor', *Math. Comp.* 72 (2003) no. 242, 913–937.

10. W. Stein *et al.*, Sage Mathematics Software (Version 5.11), The Sage Development Team, 2013, http://www.sagemath.org.

11. L. Washington, *Introduction to cyclotomic fields*, 2nd edn Graduate Texts in Mathematics 83 (Springer, New York, 1997).

John C. Miller
Department of Mathematics
Rutgers University
Hill Center for the Mathematical Sciences
110 Frelinghuysen Road
Piscataway, NJ 08854-8019
USA

jcmiller@math.rutgers.edu

https://doi.org/10.1112/S1461157014000382 Published online by Cambridge University Press