RIMS Kôkyûroku Bessatsu
B64 (2017), 19–32

Real cyclotomic fields of prime conductor and their class numbers II

By

John C. Miller*

Abstract

In the author's previous paper, it was proven that the plus part of the class number is 1 for cyclotomic fields with prime conductors between 71 and 151. Furthermore, under the assumption of the generalized Riemann hypothesis, the class number was determined for prime conductors between 167 and 241. In this paper, we extend our work to higher conductors and determine the class number for prime conductors 251, 257 and 263 under the assumption of GRH.

§ 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, i.e. the class number of the maximal real subfield (also called the real cyclotomic field). The problem of determining the class number of a cyclotomic field goes back to Kummer, who recognized that calculation of the plus part presents substantial difficulties.

Until the author's recent work [5], the class number of real cyclotomic fields of prime conductor had only been determined unconditionally up to conductor 67 by Masley [3], and up to conductor 163 by van der Linden [2] under the assumption of GRH. For fields of larger conductor, Minkowski bounds are far too large to be useful, and their discriminants are too large for their class numbers to be treated by Odlyzko's discriminant bounds. Following the method introduced in [4], the problem of large

Received April 12, 2015. Revised April 13, 2016.
2010 Mathematics Subject Classification(s): Primary 11R29, 11R18; Secondary 11R80, 11Y40.
Key Words: *class number, cyclotomic field.*
*Johns Hopkins University, Baltimore, Maryland, USA.
e-mail: jmill268@jhu.edu

discriminants can be overcome by establishing nontrivial lower bounds for sums over the prime ideals of the Hilbert class field, allowing us to obtain an upper bound for the class number.

In this paper, we extend our work to higher conductors. Under GRH, the real cyclotomic fields of conductors 251 and 263 are shown to have class number 1. The real cyclotomic field of conductor 257, shown in [1] to have class number greater than 2, is shown under GRH to have class number 3.

Theorem 1.1. *Under the assumption of the generalized Riemann hypothesis, the class numbers of the real cyclotomic fields of conductors* 251, 257 *and* 263 *are* 1, 3 *and* 1 *respectively.*

Together with earlier results in [2, 3, 5], we have the following corollary.

Corollary 1.2. *Let p be a prime integer, and let $\mathbb{Q}(\zeta_p)^+$ denote the maximal real subfield of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. Then the class number of $\mathbb{Q}(\zeta_p)^+$ is* 1 *for $p \leq 151$.*

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

$$h_p^+ = \begin{cases} 1 & \text{if } p \leq 263 \text{ and } p \neq 163, 191, 229 \text{ and } 257, \\ 4 & \text{if } p = 163, \\ 11 & \text{if } p = 191, \\ 3 & \text{if } p = 229 \text{ or } 257. \end{cases}$$

§ 2. Upper bounds for class numbers of fields of large discriminant

We may obtain an upper bounds for class numbers of number fields of large discriminant by establishing lower bounds for sums over the prime ideals of the Hilbert class field. The author's earlier paper [4] treats this in detail.

Definition 2.1. 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:

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

Theorem 2.2 (Miller [4, Lemma 5.2])**.** *Let K be a totally real field of degree n, and let*

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

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

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

where γ is Euler's constant. If $B > 0$ then we have, under the generalized Riemann hypothesis, an upper bound for the class number h of K,

$$h < \frac{2c\sqrt{\pi} e^{(c/4)^2}}{nB}.$$

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

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

If x is in the ring of integers of K, and if its norm is a prime 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. If we find sufficiently many such primes which totally split into principal ideals, the preceding theorem establishes an upper bound for the class number. After establishing an upper bound, we can use the results of Schoof [7] to determine a precise class number h. In his "Main Table," for each prime conductor less than 10000, Schoof gives a number $\tilde{h}$ such that either $h = \tilde{h}$ or $h > 80000 \cdot \tilde{h}$. In particular, if $h < 80000$, then $h = \tilde{h}$.

The real cyclotomic field $\mathbb{Q}(\zeta_p)^+$ of prime conductor has degree $n = (p-1)/2$. We will use the integral basis $\{b_0, b_1, \ldots, b_{n-1}\}$, with $b_0 = 1$ and $b_j = 2\cos(2\pi j/p)$ for $j = 1, \ldots, n-1$. We also will use the alternative basis

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

To find integral elements of small norm, our strategy will be to search over a large number of "sparse" vectors, i.e. vectors where almost all the coefficients are zero, with respect to the bases (b_j) and (c_k). For the following results, each took several days running a C program on a single laptop to find sufficiently many elements of small norm. The author also uses the Maple computer program to perform algebraic manipulations.

§ 3. The class number of $\mathbb{Q}(\zeta_{251})^+$

Proposition 3.1. *Under the generalized Riemann hypothesis, the class number of $\mathbb{Q}(\zeta_{251})^+$ is 1.*

Proof. Unlike the number fields encountered in [5], a brute force search of $\mathbb{Q}(\zeta_{251})^+$ for integral elements of small prime norm, or a chain of almost primes, does not seem to easily yield sufficiently many elements. We must apply a more subtle approach. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following integral elements α, β, γ and their norms:

Element	Norm
$\alpha = b_1 - b_7 + b_{65} - b_{71} - b_{78} + b_{100}$	$251 \cdot 503 \cdot 242467$
$\beta = c_0 + c_3 - c_{13} - c_{25} - c_{61} + c_{81} + c_{84}$	$503 \cdot 23593$
$\gamma = b_1 - b_2 - b_9 - b_{49} + b_{66} - b_{69} + b_{77}$	$23593 \cdot 242467$

Since the prime over 251 is totally ramified, we can divide α by $2b_0 - b_1$, which has norm 251, to get an integral element

$$\delta = \frac{\alpha}{2b_0 - b_1}$$

with norm $503 \cdot 242467$.

Now we can twist β and δ by the Galois action until their product is divisible by γ. In other words, for each σ_1, σ_2 in $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, we check the quotient

$$\eta = \frac{\beta^{\sigma_1}\delta^{\sigma_2}}{\gamma}$$

until we find a pair σ_1, σ_2 that yields an element η in the ring of integers of $\mathbb{Q}(\zeta_{251})^+$, which will necessarily have norm 503^2. In fact, σ_1 is the Galois action that sends ζ_p to ζ_p^{37} and σ_2 sends ζ_p to ζ_p^{40}. Explicitly, using the basis (b_j), the element η is

$\eta = [12361, -299, -4678, 7860, 5135, -654, 290, 3096, 7695, -679, -4289, 10334, 5167, -7050, 4990, 8471, -1102, 6, 3245, 6161, 2843, -4756, 5924, 9728, -5878, -160, 10844, 442, -2286, 3846, 4983, 3912, -2833, 1433, 11201, -1386, -4897, 10529, 4739, -4464, 3298, 5686, 3334, -554, -1084, 9171, 3767, -7179, 6497, 9435, -4639, 431, 7459, 3093, 497, -841, 5928, 7433, -5541, 935, 12102, -1634, -3836, 7978, 4357, -409, 164, 3439, 8007, -1608, -3461, 11276, 3857, -6697, 6032, 7604, -1210, 189, 2980, 6483, 2024, -5046, 7109, 8797, -6540, 1252, 10542, -85, -1514, 3836, 5244, 3927, -3430, 2397, 11137, -2740, -3992, 10825, 3424, -4115, 3578, 5307, 3537, -969, -650, 9977, 2667, -6850, 7860, 8400, -4874, 1368, 6986, 2931, 326, -1175, 6659, 6690, -6339, 2335, 11750, -2656, -2704, 8155, 3965].$

Therefore the principal ideal generated by η factors as

$$(\eta) = PP^\tau$$

for some prime ideal P of norm 503 and some τ in $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$. From here it is not difficult to argue abstractly that P must be a principal ideal. However, we prefer here to proceed explicitly to find an actual generator for P.

The idea is as follows. Suppose that τ generates the entire Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, which is cyclic of order 125. Since the ideal generated by 503 totally splits, it would factor as:

$$(503) = PP^\tau P^{\tau^2} \cdots P^{\tau^{124}}.$$

Therefore the element

$$\frac{503}{\eta^{\tau}\eta^{\tau^3}\eta^{\tau^5}\cdots\eta^{\tau^{123}}}$$

would be an integral element that generates the prime ideal P of norm 503. However, when we check the quotient

$$\frac{503}{\eta^{\sigma}\eta^{\sigma^3}\eta^{\sigma^5}\cdots\eta^{\sigma^{123}}}$$

for each σ that generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, we never get an integral element. Thus we conclude that τ can not generate the entire Galois group.

Proceeding similarly, we now assume that τ generates the index 5 subgroup of the Galois group. We can easily search in the quintic subfield for an element of norm 503 and lift it to an element λ in $\mathbb{Q}(\zeta_{251})^+$ of norm 503^{25}. In fact, using the basis $b_0, b_1, \ldots, b_{124}$, the element λ is

$\lambda = [15, 0, 0, 4, 0, 0, 4, 2, 0, 4, 0, 4, 4, 4, 2, 4, 0, 2, 4, 2, 0, 2, 4, 2, 4, 0, 4, 2, 2, 2, 4, 4, 0, 4, 2, 2, 4, 4, 2, 2, 0, 2, 2, 4, 4, 4, 2, 0, 4, 4, 0, 0, 0, 4, 2, 2, 4, 2, 2, 2, 4, 4, 2, 4, 0, 0, 4, 4, 2, 2, 0, 2, 4, 4, 2, 4, 4, 2, 2, 2, 4, 0, 2, 2, 2, 2, 2, 4, 2, 4, 2, 4, 0, 2, 4, 0, 2, 4, 2, 4, 2, 0, 4, 0, 4, 4, 2, 2, 4, 2, 4, 4, 2, 2, 0, 2, 2, 2, 2, 4, 4, 4, 4, 2, 0, 4]$.

Now assuming that τ generates the index 5 subgroup of the Galois group, then the ideal generated by λ factors as

$$(\lambda) = PP^{\tau}P^{\tau^2}\cdots P^{\tau^{24}}$$

and the quotient

$$\frac{\lambda}{\eta^{\tau}\eta^{\tau^3}\eta^{\tau^5}\cdots\eta^{\tau^{23}}}$$

would be an integral element that generates the prime ideal P of norm 503. Indeed, we check the quotient

$$\theta = \frac{\lambda}{\eta^{\sigma}\eta^{\sigma^3}\eta^{\sigma^5}\cdots\eta^{\sigma^{23}}}$$

for every σ that generates the index 5 subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, and we do find such a σ that produces a quotient θ which is integral. Explicitly, using the basis (b_j), we find θ to be

$\theta = [29525608, 43553782, 54974405, 56758423, 22817830, 3665682, 27831104, 19279490, 21218318, -2806749, -22243683, 20248512, 24979411, 22270503, 13310103, 13980496, 42339501, 58097905, 52307380, 23800535, 45747322, 56983451, 50586512, 43520016, -3222986, 14213830, 30756307, 18770862, 10733689, -15326037, 2901922, 20991200, 24999724, 7943313, 12753694, 44440883, 52132909, 63675840, 28580934, 21643473, 58900838, 51500518, 50509614, 21983827, 4744116, 23512990, 21685403, 4880618, -13493327, 5214120, 20538934, 30286173, 19085108, -7502983, 29547177, 52528414, 58132760, 56167623, 23524185, 44674300, 54805868, 42003040, 25057614, 11894497, 25575933, 27903173, 19072870, -19256464, -14489922, 20438942, 21708086, 36960123, 7038865, 9557849, 49923836, 49197318, 51528625, 35018615, 42970510, 55900254, 54300085, 27671065, 145857, 24507518, 25628130, 27145403, 4561988, -27496147, 10045624, 20712414, 26250716, 21404521, 9275422, 37163356, 54965798, 50501403, 30082338, 41988513, 56539005, 54200482, 47239715, -714414, 6502707, 33897859, 22338937, 19422824, -13376824, -10601439, 17875588, 22462536, 17899396, 14250075, 38431915, 50357625, 56335074, 32582673, 17402561, 59986501, 58443554, 57097257, 28134026, -8283917, 19123511, 21699008, 14563903]$.

Moreover, it can be explicitly verified that this element θ has norm 503. Setting $S = \{503\}$ and $c = 10.5$, we apply Theorem 2.2 to show a class number upper bound of 6998. Using Schoof's table [7], this proves that the class number is 1.

□

§ 4. The class number of $\mathbb{Q}(\zeta_{257})^+$

First, we introduce a useful lemma for cyclic number fields that have 2-power degree.

Lemma 4.1. *Let K be a cyclic number field of degree 2^k, and let p be a prime number that totally splits in K. Suppose that there exist elements α and β in the ring of integers $\mathcal{O}_K$ such that*

$$|N_{K/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(\beta)| = p^2$$

and such that β/α^σ is not a unit of $\mathcal{O}_K$, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Suppose further that β lies in the index 2 subfield of K. Then for any prime ideal P of K lying above p, the ideal P^2 is principal.

Proof. Since β lies in the index 2 subfield, it generates a principal ideal

$$(\beta) = PP^\eta$$

for some prime ideal P over p and where η is the order 2 element of $\mathrm{Gal}(K/\mathbb{Q})$. For a suitably chosen $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have a principal fractional ideal

$$\left(\frac{\beta}{\alpha^\sigma}\right) = \frac{P}{P^\tau}$$

for the same prime ideal P and some $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Since β/α^σ is not a unit, τ is not the identity automorphism.

Suppose that τ has order m in the Galois group. Since τ is not the identity, m must be even, so

$$\frac{P}{P^\eta} = \frac{P}{P^{\tau^{m/2}}} = \frac{P}{P^\tau}\frac{P^\tau}{P^{\tau^2}} \cdots \frac{P^{\tau^{m/2-1}}}{P^{\tau^{m/2}}}$$

is a principal fractional ideal. We conclude that

$$P^2 = (\beta)\frac{P}{P^\eta}$$

is a principal ideal. □

Proposition 4.2. *Under the generalized Riemann hypothesis, the class number of $\mathbb{Q}(\zeta_{257})^+$ is 3.*

Proof. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following integral elements of $\mathbb{Q}(\zeta_{257})^+$ and their norms:

Element	Norm
$\alpha_1 = c_0 + c_8 - c_{48} - c_{78} - c_{81} + c_{119}$	$130043 \cdot 231299$
$\alpha_2 = b_0 + b_1 - b_{114}$	$130043 \cdot 529933$
$\alpha_3 = b_1 + b_4 - b_{48} - b_{49}$	$257 \cdot 231299 \cdot 529933$

Since the prime over 257 is totally ramified, we can divide α_3 by $2b_0 - b_1$, which has norm 257, to get an integral element α_4 with norm $231299 \cdot 529933$. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{257})^+/\mathbb{Q})$, which is cyclic of order 128. By choosing appropriate σ_1, σ_2 in G, we can construct an integral element

$$\beta_1 = \frac{\alpha_1^{\sigma_1}\alpha_2^{\sigma_2}}{\alpha_4}$$

of norm 130043^2. In fact, σ_1 is the Galois action that sends ζ_p to ζ_p^{58} and σ_2 sends ζ_p to ζ_p^{110}. Explicitly, using the basis (b_j), the element β_1 is

$\beta_1 =$ [-395, 138, -176, 181, -361, 58, -164, 177, -266, -40, -140, 119, -130, -139, -97, 16, 24, -223, -45, -115, 160, -273, 12, -241, 248, -282, 58, -336, 266, -246, 87, -372, 210, -179, 88, -344, 98, -97, 64, -258, -44, -20, 17, -132, -182, 38, -46, 7, -292, 68, -116, 135, -350, 75, -189, 224, -353, 62, -246, 257, -297, 32, -275, 221, -199, -10, -260, 123, -73, -62, -202, -21, 52, -114, -108, -178, 149, -158, 1, -312, 197, -185, 101, -392, 185, -193, 166, -396, 122, -180, 186, -334, 25, -155, 156, -216, -79, -120, 81, -73, -172, -81, -26, 71, -234, -36, -150, 184, -263, 12, -264, 247, -256, 55, -344, 245, -217, 85, -369, 179, -154, 87, -330, 60, -75, 59, -228, -88].

Let K be the index 2 subfield of $\mathbb{Q}(\zeta_{257})^+$. Inspired by the result of Lemma 4.1, we search for an integral element of K that has norm (in K) 130043. It is useful to have an integral basis for K. Let g be the automorphism that sends ζ_{257} to ζ_{257}^3, so that g generates G. Let $d_0 = 1$ and let

$$d_j = (\zeta_{257} + \zeta_{257}^{-1})^{g^{j-1}} + (\zeta_{257} + \zeta_{257}^{-1})^{g^{64+j-1}}$$

for $1 \le j \le 63$. Then $d_0, d_1, \ldots, d_{63}$ is an integral basis for K. To find elements in the ring of integers $\mathcal{O}_K$, we both search over sparse vectors in K using the basis (d_i), as well as searching sparse vectors in $\mathbb{Q}(\zeta_{257})^+$ using bases (b_j) and (c_k), and then taking the relative norm $\alpha \mapsto \alpha\alpha^{g^{64}}$ to get an element of K. We find the following integral elements of K and $\mathbb{Q}(\zeta_{257})^+$ and their respective absolute norms:

Field	Element	Norm
$\mathbb{Q}(\zeta_{257})^+$	$b_1 + b_2 - b_{18}$	1100175367
K	$d_1 - d_2 - d_5 + d_{13} + d_{14} - d_{20} - d_{53} - d_{61}$	$1100175367 \cdot 485731$
$\mathbb{Q}(\zeta_{257})^+$	$c_0 - c_4 + c_7 + c_{54} + c_{60} + c_{83}$	$485731 \cdot 227189$
K	$d_1 + d_3 + d_9 - d_{13} + d_{27} + d_{33} + d_{44} - d_{55}$	$227189 \cdot 777167$
K	$d_1 + d_2 - d_7 - d_{11} - d_{12} + d_{17} - d_{24}$	$777167 \cdot 1461301$
$\mathbb{Q}(\zeta_{257})^+$	$c_0 + c_6 - c_{18} - c_{24} + c_{75}$	$1461301 \cdot 559015091$
$\mathbb{Q}(\zeta_{257})^+$	$b_1 + b_{28} - b_{68} - b_{69}$	$257 \cdot 559015091 \cdot 30841$
$\mathbb{Q}(\zeta_{257})^+$	$c_0 - c_{17} + c_{39} + c_{45} + c_{116}$	$30841 \cdot 446142233$
K	$d_0 + d_1 + d_4 - d_{18} + d_{46} + d_{52} - d_{58} + d_{60}$	$446142233 \cdot 140837$
$\mathbb{Q}(\zeta_{257})^+$	$b_1 + b_2 - b_{43}$	$140837 \cdot 130043$

As usual, we can divide by $2b_0 - b_1$, which has norm 257, to get an integral element with norm $559015091 \cdot 30841$. For elements in $\mathbb{Q}(\zeta_{257})^+$, we take relative norms to produce elements of the same absolute norm in K. Finally, by taking quotients by

appropriate Galois conjugates, we can construct an integral element β_2 of K, which has norm 130043, and which has norm 130043^2 when considered as an element of $\mathbb{Q}(\zeta_{257})^+$.

We can explicitly calculate that β_2/β_1^σ is not a unit for all σ in G. Thus we can apply Lemma 4.1 to show that, for any prime P lying above 130043, the ideal P^2 is principal. We can use the Parity Check Theorem [3, Theorem 2.21] to see that the class number of $\mathbb{Q}(\zeta_{257})^+$ is odd, therefore P itself must be principal. From here it is relatively straightforward to find integral elements α of the form

$$(\alpha) = PQ$$

where Q is a prime ideal of small prime norm, thereby establishing a class number upper bound. However, we prefer to proceed more explicitly, finding actual generators for the prime ideals of small prime norm.

First we find σ in G such that

$$\gamma = \frac{\beta_2}{\beta_1^\sigma}$$

generates a principal fractional ideal of the form

$$(\gamma) = \frac{P}{P^\tau}$$

where P is a prime ideal of norm 130043, and $\tau \in G$. By taking certain products of Galois conjugates of γ, we can determine that τ generates G. This element γ is useful in the following situation: Suppose that there exist integral elements x and y with norms pqr and pq respectively, where $p = 130043$, and q and r are prime numbers that totally split in the field. Then x generates an ideal of the form

$$(x) = PQR$$

where P, Q and R are prime ideals of norms p, q and r respectively. Similarly, a Galois conjugate of y generates the ideal

$$(y^{\sigma_1}) = P^{\sigma_2}Q$$

for some $\sigma_1, \sigma_2 \in G$. Suppose that $\sigma_2 = \tau^k$. Then $\gamma\gamma^\tau \cdots \gamma^{\tau^{k-1}} y^{\sigma_1}$ generates the ideal PQ. Therefore, we can construct an integral element

$$\frac{x}{\gamma\gamma^\tau \cdots \gamma^{\tau^{k-1}} y^{\sigma_1}}$$

of norm r. In other words, we have used the element γ to "twist" the prime ideal P by a Galois action, when P is a factor of a composite ideal.

To make use of this idea, we use the following elements of $\mathbb{Q}(\zeta_{257})^+$ and their norms:

Element	Norm
$\alpha_2 = b_0 + b_1 - b_{114}$	$130043 \cdot 529933$
$\alpha_5 = c_0 + c_{54} + c_{59} + c_{112}$	$529933 \cdot 16205393$
$\alpha_6 = c_0 - c_7 - c_{19} + c_{36} - c_{88} + c_{115} + c_{123}$	$16205393 \cdot 8737$
$\alpha_7 = c_0 - c_1 + c_{13} - c_{52} + c_{106} - c_{121} + c_{122}$	$1275749 \cdot 8737^2$

By choosing the appropriate σ_1 and σ_2 in G, we can construct an element

$$\beta_3 = \frac{\alpha_2^{\sigma_1}\alpha_6^{\sigma_2}}{\alpha_5}$$

that has norm $130043 \cdot 8737$. Next we choose σ_3 and σ_4 in G such that the element

$$\beta_4 = \frac{\alpha_7\beta_1}{\beta_3^{\sigma_3}\beta_3^{\sigma_4}}$$

generates the ideal

$$(\beta_4) = \frac{P^{\sigma_5}P^{\sigma_6}Q}{P^{\sigma_7}P^{\sigma_8}}$$

where P and Q are prime ideals of norm 130043 and 1275749 respectively. Now by multiplying β_4 by the appropriate Galois conjugates of γ, we can construct an integral element β_5 of norm 1275749.

Next we use the following integral elements and their norms.

Element	Norm
$\alpha_8 = c_1 - c_{18} + c_{40} + c_{56} - c_{75} + c_{105}$	$1275749 \cdot 4111 \cdot 16447$
$\alpha_9 = b_0 + b_1 - b_9 - b_{30} + b_{58} - b_{75} + b_{84}$	$130043 \cdot 16447$
$\alpha_{10} = b_1 + b_3 + b_{39} + b_{56} - b_{120}$	$1615501 \cdot 4111^2$
$\alpha_{11} = c_0 + c_{57} - c_{84} - c_{95} + c_{115}$	$1615501 \cdot 4454086019$
$\alpha_{12} = b_1 + b_{12} + b_{20} + b_{27} - b_{88} + b_{106}$	$4454086019 \cdot 4111$

By dividing α_8 by the appropriate conjugate of β_5, we can construct an integral element β_6 of norm $4111 \cdot 16447$. We can choose $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in G$ such that

$$\beta_7 = \frac{\alpha_{10}\alpha_9^{\sigma_1}\alpha_9^{\sigma_2}}{\beta_6^{\sigma_3}\beta_6^{\sigma_4}}$$

is an integral element of norm $1615501 \cdot 130043^2$. Now we can use the idea discussed above to divide β_7 by β_1 (which has norm 130043^2) after "Galois twisting" β_1 via multiplying by the appropriate conjugates of γ. This constructs an integral element β_8 of norm 1615501. Now we can divide α_{11} by the appropriate conjugate of β_8 to produce an element β_9 of norm 4454086019, and finally we can divide α_{12} by the appropriate conjugate of β_9 to construct an integral element β_{10} of norm 4111. Moreover, the foregoing calculations, while rather elaborate, do construct β_{10} explicitly. Using our basis (b_j), the following integral element has norm 4111:

[10428599412, −14580350932, −3376865511, −3282951359, 16341675835, 1606498420, 8793062613, −10418031177, −6534149268, 3959823353, 2343001669, 10405410440, −159350108, 1294971873, 14581294173, −21855534611, −10953699563, 1523537643, −1917408750, 5120471172, 3796206827, 9634551567, 13161733282, −2891642657, 16236634832, 5812863383, 2291902524, −927271498, 12344458809, −5339104130, −10449175119, 15360571789, 6867130480, 5172508006, −7549973967, 211995255, −3763953981,−11433299663, −13615962461, 5355009796, −11297606817, −2556433074, 6233677121, 3183108998, 9711268884, 1358917812, −13181014917, −460664187, −9867390849, −7057095944, −1231901880, 17841337326, 6865141087, 7050234913, 3378609799, 2597830021, −1832197251, 3819792880, −6992348742, −5130633052, 14306839471, 12887464234, −18866257486, 25559309930, 15012086950, 7342448392, −1447037609, 10925064191, −2871628392, 13674056414, −12763449177, 6465755479, −8530847721, 357435101, −5870464205, −1053588258, −6264126033, 3519819872, −10418872203, 1209803322, 18036790420, −16494298977, −895762797, 6908038386, −6385671655, 2210043491, 14099425376, −102885514, 6525479595, −4275376660, 20281603850, 21656361938, −41020296, 1764621668, −1128485911, 2185909622, −3173565968, −8361116079, −16226275883, 6027752153, −16755055836, 714323813, 6857278901, 10406224009, 30155528, 9622569750, −14207419941, 790856920, −6259612995, −4506190723, −22604391522, 7208517345, 13498834899, 12234015974, 6816024743, −8841527344, −7546114709, −5966609027, 9218589829, −52711198, −939675580, −3878241077, −10089568359, −3270719023, 3458120705, −11928861316, 5827650658, 8477718634].

We can examine the quadratic subfield $\mathbb{Q}(\sqrt{257})$ (which has class number 3) to confirm that 4111 must be the smallest prime which totally splits into principal ideals in $\mathbb{Q}(\zeta_{257})^+$. We can also use $\beta_{10}, \beta_6, \alpha_9$ and β_3 to produce integral elements of norms 8737, 16447 and 130043. Setting $S = \{4111, 8737, 16447, 130043\}$ and $c = 12$, we apply Theorem 2.2 to show a class number upper bound of 58532. Using Schoof's table [7], this proves that the class number is 3. □

§ 5. The class number of $\mathbb{Q}(\zeta_{263})^+$

Proposition 5.1. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{263})^+$ *is* 1.

Proof. As the conductor of the real cyclotomic field gets larger, it becomes much more difficult to directly find integral elements of small prime norm. The smallest prime norm that we found directly is 19062767, which is too large to be useful, so more elaborate methods must be used. Using our alternative basis of cyclotomic integers, we find the following element and its norm, which will prove critical to our calculations:

$$N(c_0 - c_1 + c_{30} + c_{50} + c_{57} + c_{125}) = 263 \cdot 90473^2.$$

The prime 263 is totally ramified, and the element $2b_0 - b_1$ has norm 263, so the quotient

$$\beta_1 = (c_0 - c_1 + c_{30} + c_{50} + c_{57} + c_{125})/(2b_0 - b_1)$$

is integral and has norm 90473^2. Finding an element of square of prime norm is quite useful. It generates a principal ideal of the form PP^σ, where P is an prime ideal of norm 90473 and σ is a Galois automorphism (possibly trivial). Suppose that σ is nontrivial. Since the field is cyclic and of odd prime degree, P would have to be principal. Indeed, if σ is nontrivial, then σ generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{263})^+/\mathbb{Q})$, and we would have $P = (\beta_2)$, where

$$\beta_2 = \frac{90473}{\beta_1^\sigma \beta_1^{\sigma^3} \beta_1^{\sigma^5} \cdots \beta_1^{\sigma^{129}}}.$$

To verify that σ really is nontrivial and to calculate β_2 explicitly, we can, by trial and error, calculate the above quotient for each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{263})^+/\mathbb{Q})$ until we find an element that is integral. We successfully find an element β_2 with norm 90473. Explicitly, using our basis (b_j), we have

β_2 = [91093658332149, 46685768271369, 68361335338819, 70449701906399, 31843826845597, 71908870045208, 27348493133994, 33754439477092, 44962750769433, −1508515343175, 38936510401862, 5192389684002, 3856782750979, 30811441093606, −13800153606985, 29501013048266, 12698371445207, 5972682159799, 47522592180973, 6984009026336, 47796072467378, 45431238836744, 28923021502479, 76508506511574, 36427352941694, 65288348301432, 70729148827096, 39222853791302, 83890582919007, 42561006315902, 54359680367799, 65856630526478, 21771108627025, 62485586062044, 26270613224325, 25094463692233, 47568054578494, 125103582406, 40199642477044, 17255996070330, 8020908354451, 43727515821674, −1224030726933, 36725858965513, 28721683898737, 11059835997195, 55772756914003, 13963391285317, 44428872659723, 48817768645436, 20806767869799, 68256402498630, 29533198999197, 47647209752074, 61820560465718, 23399606060785, 68941541644779, 35080264238375, 39477647868923, 62954375684249, 17926845492145, 60044369932817, 35355012024759, 27811028989986, 61007592764110, 14202408842359, 51237426002148, 38049808198331, 19048314247332, 59172601836849, 12845180380311, 41215485711317, 39372324585845, 9507804081257, 53457153938823, 11150392769067, 29804191547363, 40985902129113, 4145466953423, 51035020787945, 17645569166106, 27171632487894, 51999047781356, 11617148558946, 58380593320006, 35709375065281, 34271393487151, 69329058912370, 26009828407571, 66912441681898, 53689198914325, 38297029552571, 78021970342828, 31559126022913, 60846711527437, 55304155983289, 24952006088441, 65163951384176, 18339935726356, 34630357356142, 39133556811954, −982220989357, 41344881716202, 2613790588508, 10778478428163, 31190967040067, −9846880977122, 37002211890541, 13289474010174, 15539069958255, 51634030002302, 11894975122939, 57793409741762, 46922638944671, 37965909423900, 81212332710005, 38872529472440, 73929528055148, 70028966094730, 44443940224036, 86511154348392, 40219032166425, 58939087815398, 60743505389903, 20146235684074, 59689390807667, 15613793165531, 21298434543273, 34515562251936, −11239938639024, 30781542318124].

This element has prime norm that is relatively small, so we can take quotients with it to find several other useful elements. Searching over sparse vectors, we find the following elements and their norms:

Element	Norm
$\alpha_1 = b_1 - b_2 - b_6 + b_{39} - b_{45} - b_{130}$	$90473 \cdot 123083$
$\alpha_2 = c_0 + c_{11} - c_{59} - c_{62} + c_{67}$	$123083 \cdot 699581$
$\alpha_3 = b_0 + b_1 - b_3 + b_{30} + b_{72} - b_{113} + b_{117}$	$123083 \cdot 4900741$
$\alpha_4 = b_1 + b_5 + b_9 - b_{34} - b_{38} - b_{65}$	$263 \cdot 4900741 \cdot 64930493$
$\alpha_5 = b_0 + b_1 + b_8 + b_{10} - b_{33} - b_{35} - b_{37}$	$64930493 \cdot 12308399$
$\alpha_6 = b_0 + b_1 + b_{51} - b_{100}$	$12308399 \cdot 1713181$
$\alpha_7 = b_0 + b_1 + b_2 + b_{27} - b_{57} + b_{115} + b_{119}$	$1713181 \cdot 476213047$
$\alpha_8 = c_0 + c_1 - c_{11} - c_{68} - c_{73} + c_{75} + c_{91}$	$476213047 \cdot 5458303$

As usual, we can divide α_4 by $2b_0 - b_1$ to get an integral element of norm $4900741 \cdot 64930493$. Then we can take quotients by the appropriate Galois conjugates to construct integral elements of β_3, β_4 and β_5 of prime norms 123083, 699581 and 5458303 respectively.

We recall an idea introduced in Section 3. If we have 3 elements of "almost prime" norms p_1p_2, p_2p_3 and p_3p_1 (where p_1, p_2 and p_3 are distinct primes), then we can take products and quotients by the appropriate Galois conjugates to construct an element of p_1^2. This generalizes to a sequence of elements of norms

$$p_1p_2, p_2p_3, p_3p_4, \ldots, p_{2k}p_{2k+1}, p_{2k+1}p_1.$$

We can think of this in terms of graph theory: Let every prime number p_i correspond to a vertex v_i, and draw edges between vertices v_i and v_j whenever we find an element of norm p_ip_j. Then our goal is to find a cycle in the graph of *odd* length. In such a

case, we can construct elements of square of prime norm p_i^2 for each vertex v_i in the cycle. We can then exploit this square of prime norm as before. To carry out this idea, we search over the sparse vectors and find:

Element	Norm
$(b_1 + b_6 + b_{74} + b_{81} - b_{111})/\beta_2^{\sigma_1}$	$1051 \cdot 970469$
$b_0 + b_1 - b_3 + b_{50} - b_{78}$	$970469 \cdot 127817$
$(c_0 - c_2 - c_{12} - c_{15} + c_{32} + c_{126})/\beta_3^{\sigma_2}$	$127817 \cdot 53653$
$c_0 - c_{13} + c_{63} + c_{77} + c_{96} + c_{102} + c_{111}$	$53653 \cdot 13166917739$
$b_1 + b_8 - b_{35}$	$13166917739 \cdot 1458599$
$(b_0 + b_1 - b_{13} - b_{59} + b_{85} - b_{120})/\beta_4^{\sigma_3}$	$1458599 \cdot 87317$
$(b_1 + b_2 - b_8 + b_{61} - b_{100} - b_{101})/(2b_0 - b_1)$	$87317 \cdot 44711$
$(b_0 + b_1 + b_3 - b_{12} - b_{14} - b_{55} - b_{62})/\beta_5^{\sigma_4}$	$44711 \cdot 6311$
$(c_0 + c_4 + c_{10} - c_{19} + c_{38} - c_{64} + c_{118})/\beta_3^{\sigma_5}$	$6311 \cdot 23143$
$c_0 - c_5 - c_{37} + c_{63} - c_{93} + c_{114} + c_{123}$	$23143 \cdot 4733$
$(b_1 + b_7 + b_{13} + b_{27} - b_{34} + b_{104})/\beta_2^{\sigma_6}$	$4733 \cdot 61453$
$(b_1 - b_7 + b_{26} - b_{97} + b_{103} - b_{118})/(2b_0 - b_1)$	$61453 \cdot 29983$
$b_0 + b_1 - b_{32} - b_{34} - b_{51} - b_{80}$	$29983 \cdot 213557$
$(b_0 + b_1 - b_{11} + b_{23} - b_{94} - b_{111} - b_{116})/\beta_2^{\sigma_7}$	$213557 \cdot 58802591$
$(b_1 - b_3 - b_{29} + b_{30})/(2b_0 - b_1)$	$58802591 \cdot 1051$

Note that, where necessary, we divided by the appropriate Galois conjugates of $\beta_2, \beta_3, \beta_4$ and β_5, or by the generator $2b_0 - b_1$ of the totally ramified prime over 263, in order to obtain quotients with our desired norms. We now have a cycle of odd length:

$$1051 \to 970469 \to 127817 \to 53653 \to 13166917739 \to 1458599 \to 87317 \to 44711$$

$$\to 6311 \to 23143 \to 4733 \to 61453 \to 29983 \to 213557 \to 58802591 \to 1051$$

From this cycle of elements almost prime norms, we can construct an integral element β_6 of norm 1051^2. Then we can proceed as we did earlier, checking the quotient

$$\frac{1051}{\beta_6^{\sigma} \beta_6^{\sigma^3} \beta_6^{\sigma^5} \cdots \beta_6^{\sigma^{129}}}$$

for each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{263})^+/\mathbb{Q})$ until (possibly) finding an integral element which has norm 1051. Indeed, using our basis (b_j), we can explicitly find such an element of norm 1051:

[4937323371016121050282685, 7580985651254745650097999, −1545422806020001019458536 1, 1160825091089121697776618 1, 8296951211820526848129067, −9495171525321871549373872, 1764542225425146364532466 6, 5037486883361967412831486, 8226092826053271032519287, −1523834764351580765360 01, 7435157508565396487106611, −1618920159858211534673095 6, −7375143169639161472468879, 1826804428372966652888281 1, 4815485446067692852689706, 1917716558190010585952870 2, 1169877275219572189106800 3, 1041424353963302055215132, −2382318783343172818953068, 1704429263164780331801612 9, 3627486085528583685696700, 5661403194326210808810951, −6859888720765748512851989, −8044209564042405580987222, 4037227107411631544423822 1, 1351451562356258350386833 3, 1721876421192351601694493, 1854130892721851476750639, −1068188079417355817395 42, −2218828528121283034199024 6, 1210771330436383884831905 7, 2787638890005007604630438 2, −2506542865353264837787205 3, −5391498367582091631608 74, −2328448882933695126666404, 1972045119272216236271561 4,

518340248159477627207305 6, 307007961323658847334830 8, 557404178221304169517505, −156714213465306457520368 88, 244655432549655527423811 72, −323919405006584334877400 7, 276877299686731618749149 41, −695690545030024968912572 8, −931087572883338014868870 6, 289500463972087979794701 58, 262820930362015307322378 2, 288788882659265425451879 37, 601413153089417265217601 6, 878632464348198287306945 0, −765905260176176559652978 9, 865186440321179931646790 9, 157635593084971634692124 81, −154627470892116992090738 11, 729845647875306685339834 5, 813188006661581606504049 7, 221433884396378334898607 92, −862499360632592065438016 1, 861654370428550637457637 9, 643973543319527091901928 9, −274413545701164058157004 67, 808341265136183704047944 8, 714014645894996909744479 6, 283108741134524235531498 8, −474243153338246374543354 35, 894007600372722790344895 2, 216312765175771978235051 8, 350229397316122180420928 3, −362096683439023622623737, −622788792941330728725351 8, 295042614112215091384445 8, −609971314234453618551296 7, −678353389737319825663644 5, 730881153534521857262356 7, 158684913550709576660703 38, −182519713869672510838475 96, 121495651069762020467756 09, −130615237535109853187008, −237302591428027850605929 22, 280052132620792613334498 84, 197660272530804123582523 20, −348162909370259237257957 4, −172082708956934814468562 05, 913585417789615508780881 7, −686946366880013214544361 8, 137056135902309717183534 62, 359650416217215747487130 73, 175580593893615992199777 2, 130827375642091334101053 5, −188982963411359446629994 56, 172988792322959341898792 51, 207980198598095225714493 13, −872761379481393715377052 0, −639151699399904790369470 7, 100535843107481335778487 1, 203568660903848057855821 36, −596686302892959523868089 9, 257084592481061537578033 72, 335262608986349736213531 4, −173713583988656912836516 55, 106795723424966875324486 8, 689573949862160455264260 9, 946526264459734743914242 4, −101305582786993104959082 96, 133209066481231093938353 254, 717181328223638207149435 0, 185773045210078866138643 06, 215196589023536200309595 75, 506775115262556965067945 4, −727092668013974624305303 8, −140754616072637551390922 4, 278048459756613243846000 67, 728977436778906707648879 5, 991175850365536740213528 7, 480602627753936721271685 1, −410140108043502949290 13, 147966962510908757257 76, 246469344422609445684444 07, 170043953630606681351235 84, −360936204663186484156159 7, 693704887978210227156818 0, −196172043696427350680523 76, 198982519795256302281755 96, −554627710386619237474824 6, −143178589891190132153706 53, 140258218728153391632865 43, −179687183842892098555902 1, 516299369798211631320898 0, 705970482749541595813636 6, 211231399755753699932660 70, −261084074634183082517990 58]

We can now conclude that all the primes in the cycle given above totally split into principal ideals. Setting $S = \{1051, 4733, 6311\}$ and $c = 10$, we apply Theorem 2.2 to show a class number upper bound of 2152. Using Schoof's table [7], this proves that the class number is 1. □

This completes the proof of Theorem 1.1.

§ 6. Concluding remarks

Although the difficulty of finding generators for principal prime ideals seems to grow exponentially with the degree of the field, the author hopes that further ideas can be found that would allow the calculation of the class number of cyclotomic fields of larger conductor than is currently possible.

§ 7. Acknowledgments

I would like to thank my advisor, Henryk Iwaniec, for introducing me to the class number problems of cyclotomic fields, and for his steadfast encouragement. The contents of this paper comprise a part of my Ph.D. thesis [6] written under Professor Iwaniec's guidance and supervision. I thank Professors Hoshi, Takahashi and Tsuji, the organizers of the 2014 RIMS Workshop on Algebraic Number Theory held in Kyoto, for their generous hospitality. It was a great pleasure to attend their wonderful conference. I sincerely appreciate the careful reading and suggestions of the editors and the anonymous referee.

References

[1] Ankeny, N. C., Chowla, S. and Hasse, H., On the class-number of the maximal real subfield of a cyclotomic field, *J. Reine Angew. Math.*, **217** (1965), 217–220.

[2] Van der Linden, F. J., Class number computations of real abelian number fields, *Math. Comp.*, **39**, no. 160 (1982), 693–707.

[3] Masley, J. M., Class numbers of real cyclic number fields with small conductor, *Compositio Math.*, **37**, no. 3 (1978), 297–319.

[4] Miller, J. C., Class numbers of totally real fields and applications to the Weber class number problem, *Acta Arith.*, **164**, no. 4 (2014), 381–397.

[5] Miller, J. C., Real cyclotomic fields of prime conductor and their class numbers, *Math. Comp.*, **84**, no. 295 (2015) 2459–2469.

[6] Miller, J. C., Class numbers of totally real number fields, Thesis (Ph.D.), Rutgers University, 2015.

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