MATHEMATICS OF COMPUTATION
VOLUME 39, NUMBER 160
OCTOBER 1982, PAGES 693-707

Class Number Computations of Real Abelian Number Fields

By F. J. van der Linden

Abstract. In this paper we describe the calculation of the class numbers of most real abelian number fields of conductor $\leqslant 200$. The technique is due to J. M. Masley and makes use of discriminant bounds of A. M. Odlyzko. In several cases we have to assume the generalized Riemann hypothesis.

Introduction. It is well known that the class number h of an abelian number field can be written as $h = h^+ \cdot h^-$, where h^+ is the class number of the maximal real subfield K^+ of K and h^- is an integer. We can determine the *relative class number* h^- in a straightforward way, using the complex analytic class number formula (see [7, Kap. III], or [9, Chapter 3, Section 3]). For the full cyclotomic fields $\mathbf{Q}(\zeta_n)$, with $\phi(n) \leqslant 256$, and their subfields, one can deduce h^- from the tables of G. Schrutka von Rechtenstamm [15]; here ζ_n denotes a primitive nth root of unity, and ϕ is the Euler function.

For the class number factor h^+, the complex analytic class number formula is less useful, since it requires that the units of K^+ be known. Alternative techniques have been developed by J. M. Masley [13], who computed the class number of almost all real cyclic number fields of conductor $\leqslant 100$; here the *conductor* of K is the least f for which $K \subset \mathbf{Q}(\zeta_f)$.

In this paper we apply Masley's techniques, with a few additions, to determine the class numbers of a large collection of real abelian fields of conductor $\leqslant 200$; see Section 1 for a precise statement of our results, some of which assume the generalized Riemann hypothesis.

An important ingredient of Masley's method is the use of discriminant lower bounds proved by A. M. Odlyzko [14]. These lead to an upper bound for the class number of a real abelian number field, provided that its conductor, or more precisely its root discriminant (see [13, Section 1]), is sufficiently small. It follows that this method can only be used for a finite number of real abelian number fields. The existence of infinite class field towers shows that this remains true after any future improvement of Odlyzko's bounds. In fact, examples of J. Martinet [12] show that the method will never apply to fields whose root discriminant is larger than five times the present bound, under assumption of the generalized Riemann hypothesis.

The structure of this paper is as follows. Section 1 contains our results and Section 2 lists the theorems used in the proofs. The proofs themselves are largely suppressed.

Received October 24, 1980; revised December 24, 1981.
1980 *Mathematics Subject Classification.* Primary 12-04, 12A35, 12A55.
Key words and phrases. Class number, cyclotomic field, abelian number field.

©1982 American Mathematical Society
0025-5718/82/0000-0251/$03.75

Instead we present, in Section 3, a recipe which any reader can use to check our results for any given conductor. In Section 4 we illustrate this for the conductors 111, 136, 145, 163, 183; the last four of these are the only conductors for which we found class numbers greater than the genus factors; see Section 1. Finally, in an appendix we give an extract from unpublished tables of discriminant lower bounds due to A. M. Odlyzko [14]. We are grateful for his permisssion to reproduce these tables.

We denote the end of a proof by □.

1. Main Results. Let K be a real abelian number field with class number $h(K)$. The *conductor* $f(K)$ of K is the least m for which $K \subset \mathbf{Q}(\zeta_m)$, with ζ_m a primitive mth root of unity. By GRH we denote the generalized Riemann hypothesis for the zeta-function of the Hilbert class field of $\mathbf{Q}(\zeta_{f(K)})$.

THEOREM 1. *Suppose that* $f(K) = q$ *is a prime power. Then* $h(K) = 1$ *if* $\phi(q) \leqslant 66$.

THEOREM 2. *Suppose that* $f(K) = q$ *is a prime power, and assume GRH. Then*

$$h(K) = 4 \quad \text{if } q = 163,$$
$$h(K) = 1 \quad \text{for all other } K \text{ for which } \phi(q) \leqslant 162.$$

In order to state results for fields with a non prime power conductor we need some definitions. Let $G(K)$ be the *genus field* of K, i.e., the maximal totally unramified extension of K which is abelian over $\mathbf{Q}$. It is contained in $\mathbf{Q}(\zeta_{f(K)})$, and it can be determined as follows. Let $G^*(K)$ be the smallest field containing K which is a composite of abelian extensions of $\mathbf{Q}$ of prime power conductors. Then $G(K) = G^*(K) \cap \mathbf{R}$; see [13, Section 2]. It is clear that $K = G^*(K) = G(K)$ if $f(K)$ is a prime power. The equality $K = G(K)$ is true for many other fields as well. We write $g(K) = [G(K) : K]$.

By $H(K)$ we denote the *Hilbert class field* of K, i.e., the maximal totally unramified abelian extension of K. By class field theory,we have $h(K) = [H(K) : K]$. Clearly $H(K)$ contains $G(K)$, so $h(K)$ is divisible by the *genus factor* $g(K)$.

THEOREM 3. *Suppose that* $f(K) = f$ *is not a prime power. Then*

$$h(K) = 2 \cdot g(K) = 2 \quad \text{for } K = \mathbf{Q}(\zeta_{136})^+,$$
$$h(K) = g(K) \quad \text{for all other } K \text{ for which } f \leqslant 200, \phi(f) \leqslant 72, f \neq 148, f \neq 152,$$
$$h(K) = g(K) \quad \text{for } f = 165.$$

THEOREM 4. *Suppose that* $f(K) = f$ *is not a prime power, and assume GRH. Then*

$$h(K) = 2 \cdot g(K) = 2 \quad \text{for } K = \mathbf{Q}(\zeta_{136})^+,$$
$$h(K) = 2 \cdot g(K) \quad \text{if } f = 145 \text{ and } \sqrt{145} \in K,$$
$$h(K) = 4 \cdot g(K) = 4 \quad \text{if } f = 183 \text{ and } 12 \mid [K : \mathbf{Q}],$$
$$h(K) = g(K) \quad \text{for all other } K \text{ with } f \leqslant 200.$$

If we do not assume GRH in Theorems 2 and 4, then $h(K)$ is at least divisible by the value it is claimed to be, and there is a lower bound on the prime powers occurring in their quotient. This lower bound is found in the course of the proof.

2. Auxiliary Theorems. In this section we state some theorems used in the proofs of Theorems 1–4.

Let K be an algebraic number field with $[K:\mathbf{Q}] < \infty$. We denote by $\mathcal{O}(K)$ its rings of integers, and by $\mathcal{O}(K)^*$ the unit group of $\mathcal{O}(K)$. The discriminant of K over $\mathbf{Q}$ is denoted by Δ_K. The notations $h(K)$ and $H(K)$ have the same meaning as in Section 1. If L/K is a Galois extension we denote its Galois group by $\mathrm{Gal}(L/K)$.

The following theorem provides us with a good upper bound for the class number; for Tables 1 and 2, see the appendix.

THEOREM 5. *Let (A, E) be a pair appearing in Table* 1, *and K a totally real number field of degree n over $\mathbf{Q}$ for which $\Delta_K^{1/n} < A$. Then we have*

$$h(K) < E/(n \log A - \log \Delta_K).$$

If the zeta-function of $H(K)$ satisfies the generalized Riemann hypothesis, then the same is true for pairs (A, E) appearing in Table 2.

Usually the best results are not obtained by taking A to be the smallest value such that $A > \Delta_K^{1/n}$.

Proof. Tables 1 and 2 are abstracted from tables computed by A. M. Odlyzko [14]. He proved that lower bound $\Delta_K > A^n \cdot e^{-E}$ for any totally real number field K and any pair (A, E) from these tables, assuming GRH in case of Table 2. Applying the bound to $H(K)$, we find

$$\Delta_K^{h(K)} > A^{n \cdot h(K)} \cdot e^{-E}.$$

The theorem follows by taking logarithms. □

Let L/K be a cyclic extension of number fields with $[L:K] = n$. Denote by σ a generator of $\mathrm{Gal}(L/K)$. For a prime number p not dividing n, let $\mathrm{Cl}_p(L)$ be the p-primary part of the class group of L, and

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

where Φ_n is the nth cyclotomic polynomial. It can be shown, using [20, Theorem 1], that $\mathrm{Cl}_p^*(L/K)$ consists of all elements of $\mathrm{Cl}_p(L)$ with norm 1 to all intermediate fields $L' \neq L$ of L/K.

THEOREM 6. *Let M/K be an abelian extension of number fields, and p a prime number not dividing $[M:K]$. Then we have*

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

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

Proof. See Fröhlich [3, Theorem 3.1]. □

COROLLARY 7. *If M, K, and p are as in Theorem* 6, *then: $p \mid h(M) \Leftrightarrow \exists L/K$ cyclic (possibly $K = L$) with $L \subset M$ and $p \mid h(L)$.* □

THEOREM 8 (Rank). *Let L/K be a cyclic extension of number fields, and p a prime number not dividing $n = [L:K]$. Then $\#\mathrm{Cl}_p^*(L/K)$ is a power of p^f, where f is the smallest positive integer for which $p^f \equiv 1 \bmod n$.*

Proof. Let σ be as above, and $\alpha \in \mathrm{Cl}_p^*(L/K)$, $\alpha \neq 1$. Suppose that $\sigma^d(\alpha) = \alpha$, where d divides n, $d \neq n$. Denote by L' the intermediate field of L/K with $[L':K] = d$. Then on the one hand the norm $N_{L/L'}(\alpha)$ equals $\alpha^{n/d}$, and on the other hand $N_{L/L'}(\alpha) = 1$. From $p \nmid n/d$ it now follows that $\alpha = 1$, a contradiction.

This proves that the stabilizer of α in $\mathrm{Gal}(L/K)$ is $\{1\}$, so the orbit of α under $\mathrm{Gal}(L/K)$ contains n elements. This is true for all $\alpha \neq 1$, so $\#\mathrm{Cl}_p^*(L/K) \equiv 1 \bmod n$, and the theorem follows. □

Theorem 8 is a more precise version of the rank corollary of J. Masley [13, (2.15)]. It is a very useful theorem because for many primes, p^f exceeds the class number bound from Theorem 5.

THEOREM 9 (Reflection). *Let p be a prime number, and m a positive integer. If $M = \text{l.c.m.}(p, m)$ we have*

$$p \mid h^+(\mathbf{Q}(\zeta_m)) \Rightarrow p \mid h^-(\mathbf{Q}(\zeta_M)).$$

Proof. See Masley [13, (2.22)]. □

THEOREM 10. *If p is a prime number with $p < 125000$, then $p \nmid h^+(\mathbf{Q}(\zeta_p))$.*

Proof. See Wagstaff [19]. □

THEOREM 11. *Let L/K be a p-extension, i.e., a Galois extension with $\mathrm{Gal}(L/K)$ a p-group. Let P be a set of (finte or infinite) primes of K and $\mathfrak{q}$ a prime of K. Suppose that L/K is unramified outside $P \cup \{\mathfrak{q}\}$. If $p \mid h(L)$, then there exists a cyclic extension M/K of degree p that is unramified outside P.*

Proof. See Masley [13, (2.6)]. □

If we take $P = \varnothing$, we deduce

COROLLARY 12 (Pushing Down). *Let L/K be a p-extension with at most one ramifying prime. Then $p \mid h(L) \Rightarrow p \mid h(K)$.* □

THEOREM 13 (Pushing Up). *Let L/K be an extension of number fields. Then we have $h(K) \mid h(L) \cdot [L : K]$. If no intermediate field $M \neq K$ of L/K is unramified over K, then $h(K) \mid h(L)$.*

Proof. See Masley [13, (2.3)]. □

THEOREM 14. *Let L/K be an abelian extension. Suppose that M is a field with $L \subset M \subset H(L)$ for which M/K is an abelian extension. Then for the relative conductors we have*

$$\mathfrak{f}_{M/K} = \mathfrak{f}_{L/K}.$$

Proof. Immediate from the definition of relative conductors, see for example [8, IV, Section 7.3], and the fact that the conductor $\mathfrak{f}_{M/L} = 1$. □

For the next two theorems we need a definition. Let $K \neq \mathbf{Q}$ be a real, abelian number field of conductor f. One can show that $\eta_a = (\zeta_{2f} - \zeta_{2f}^{-1})/(\zeta_{2f}^a - \zeta_{2f}^{-a})$ is a unit in $\mathbf{Q}(\zeta_f)^+$ if $(a, 2f) = 1$. The group $C_K = \langle -1, N(\eta_a) : (a, 2f) = 1 \rangle$ where $N : \mathbf{Q}(\zeta_f)^+ \to K$ is the relative norm, is called the group of *cyclotomic units* of K. It is a subgroup of $\mathcal{O}(K)^*$. We denote by C_K' the subgroup of $\mathcal{O}(K)^*$ generated by the group C_L, with L ranging over all subfields $L \neq \mathbf{Q}$ of K (notice that different subfields can have different conductors).

Hasse has proved the following two theorems:

THEOREM 15. *Let K be a real abelian extension of degree n of $\mathbf{Q}$. Suppose that all primes that ramify in $K/\mathbf{Q}$ factorize as $p \cdot \mathcal{O}(K) = \mathfrak{p}^{n_p}$ in $\mathcal{O}(K)$. Then*

$$h(K) = \text{Index}[\mathcal{O}(K)^* : C_K] \cdot \prod_p \frac{n}{n_p},$$

where the product is taken over all primes that ramify in $K/\mathbf{Q}$.

Proof. See Hasse [7, II, Section 11, Satz 3]. □

THEOREM 16. *Let* $K/\mathbf{Q}$ *be a real cyclic extension of degree* n. *Then*

$$h(K) = \text{Index}[\mathcal{O}(K)^* : C_K'].$$

Proof. See Hasse [7, II, Section 19, Satz 9]. □

There are more ways to define "cyclotomic units" and to get information about the class number from them. See, for example, Leopoldt [10], Lang [9] or Sinnott [17], [18].

3. The Proofs. In this section we describe a method by which Theorems 1, 2, 3, and 4 can be proved.

Let a positive integer f be given. We wish to determine the class numbers of the subfields K of $\mathbf{Q}(\zeta_f)^+$.

Step 1. We use Galois theory to get a diagram of all subfields of $\mathbf{Q}(\zeta_f)^+$. In [7] one can find diagrams that occur often. We use existing tables to find the class number of some fields occurring in this diagram. For fields of degree 2 and 3 we use tables from [1] and [5]. For fields of degree 4 and 6 one can use tables from [6] and [11]. The latter two tables were not actually used in the proofs because they were not yet available. For fields with small conductors one uses the tables from [13].

For the remaining fields one determines the genus factors (see Section 1). Now, by using Theorem 13 (Pushing Up) we can get additional class number factors. Let us denote by $g'(K)$ the resulting class number factor.

Step 2. We calculate Δ_K for each $K \subset \mathbf{Q}(\zeta_f)^+$, e.g., by using the conductor discriminant product formula [8, Theorem 7.3]. We use Theorem 5 to get an upperbound $B(K)$ for $h(K)$, assuming GRH or not (only $\mathbf{Q}(\zeta_{128})^+$ is an exceptional case: see appendix).

In this stage the only possible prime divisors of $h(K)/g'(K)$ are the primes $p \leqslant B(K)/g'(K)$. Let such a prime p be fixed. In the following steps we determine whether p divides $h(K)/g'(K)$, and if so, to which power.

Step 3. For most primes p not dividing $[K:\mathbf{Q}]$ we can use Theorems 6 and 8 (Rank) and Corollary 7 to prove that p does not occur in $h(K)/g'(K)$. If p does divide $[K:\mathbf{Q}]$, it may be possible to apply these theorems to a base field different from $\mathbf{Q}$. In the case $K = \mathbf{Q}(\zeta_f)^+$ we can, for some primes, use Theorem 9 (Reflection) in combination with [15], or Theorem 10. for subfields of $\mathbf{Q}(\zeta_f)^+$ we can then apply Theorem 13 (Pushing Up).

Now we are left with only a few primes p. Typically these are primes p dividing $n = [K:\mathbf{Q}]$, or primes p of which a small power is 1 mod n.

Step 4. This step is only applicable if $p \mid n$. First use Corollary 12 (Pushing Down), when possible. In other cases, select a subfield K_0 of K for which K/K_0 is a p-extension. Using Theorem 11 or other group-theoretic arguments (cf. Section 4), we can prove that $p \mid h(K)/g'(K)$ implies the existence of an abelian extension M/K_0 with prescribed degree and ramification properties; here Theorem 14 is sometimes useful. Class field theory tells us that the existence of M as above is

equivalent to the existence of a quotient group of a ray class group of K_0 having certain specified properties; cf. [2, Chapter XI] or [8, Appendix 2, Section 2]. In many cases it is easy to disprove the existence of this group by calculations with units of K_0; for this it is convenient to choose K_0 as small as possible.

In a few cases, cf. Section 4, we find that such an M does exist. Then we may get an unramified extension of K, and a new class number factor. In this cases we update $g'(K)$, and we redo the previous steps, when necessary.

Step 5. In this step we use Theorems 15 and 16. This is the only step for which we use an electronic computer.

Let $G = \mathrm{Gal}(K/\mathbf{Q})$, $n = [K:\mathbf{Q}]$, and let p be a prime number not dividing $2n$. We know from Theorem 15 or 16 that $h(K) = m \cdot \#(E/C)$, where $E = \mathcal{O}(K)^*$ and $C \subset E$ is generated by cyclotomic units. Here m is a constant that is easy to determine, and that is built up from prime factors of n. Hence $p \nmid m$, and $p \mid h(K)$ if and only if $p \mid \#(E/C)$. So to prove that $p \nmid h(K)$, it suffices to prove that $E^p \cap C = C^p$.

To prove this we make use of the known structure of C/C^p as a $\mathbf{Z}[G]$-module. It follows from standard facts of representation theory of finite groups, cf. [16, III, Section 2], that C/C^p as a $\mathbf{Z}[G]$-module is isomorphic to $\mathbf{F}_p[G]/\mathbf{F}_p \cdot \mathrm{Tr}$, where $\mathrm{Tr} = \Sigma_{\sigma \in G} \sigma$. This makes it easy to determine the minimal submodules of C/C^p; cf. the example in Section 4. Let them be $C_1/C^p, \ldots, C_t/C^p$; then $t \leqslant n - 1$. We choose $\alpha_i \in C_i - C^p$ for $1 \leqslant i \leqslant t$.

If $E^p \cap C \neq C^p$, then $C_i \subset E^p$ for some i, so $\alpha_i \in E^p$. To obtain a contradition from this, it suffices to find, for each α_i, a prime $\mathfrak{q}$ of $\mathcal{O}(K)$ for which $p \mid N\mathfrak{q} - 1$ and $\alpha_i^{(N\mathfrak{q}-1)/p} \not\equiv 1 \bmod \mathfrak{q}$. To simplify the computations, we choose $\mathfrak{q}$ to be a prime lying over a prime number q that is $1 \bmod \mathrm{l.c.m.}(p, 2f)$. If the test fails for some i and many choices of $\mathfrak{q}$, it is likely that α_i is in fact a pth power, and this can then be verified by other means. This, however, did not occur for the cases needed in the proofs of Theorems 1, 2, 3, or 4.

4. Examples. In this section we give some examples of class number computations. These examples include all fields we found with class number greater than $g(K)$. We will also consider the fields with conductor 111 to illustrate step 5. For most fields the computations are analogous to this last example.

In the following we denote fields by capitals K, L, M, N, with an index indicating the degree of the field over $\mathbf{Q}$. The same letter is used for fields with the same conductor. A double index will be used if the degree and the conductor do not uniquely determine the field.

$f = 163$. There are four real fields with conductor 163:

$$\mathbf{Q} \subset K_3 \subset K_9 \subset K_{27} \subset K_{81}.$$

We have $K_3 = \mathbf{Q}(\omega)$, where ω is a zero of $x^3 + x^2 - 54x - 169$. Let α be a zero of $x^2 + (1 + \omega)x + 4 + \omega$, and let α' be a zero of $x^2 + (1 + \omega')x + 4 + \omega'$, where $\omega' = 37 + 3\omega - \omega^2$ is a conjugate of ω.

PROPOSITION 17. *Suppose that GRH holds. If* $K \subset \mathbf{Q}(\zeta_{163})^+$ *and* $K \neq \mathbf{Q}$, *then* $h(K) = 4$ *and* $H(K) = K(\alpha, \alpha')$.

Proof. M. N. Gras [5] gives $h(K_3) = 4$. Since the discriminant of $x^2 + (1 + \omega)x + 4 + \omega$ is a totally positive element, which generates the square of an ideal of norm 85, the extension $K_3(\alpha)/K$ must be unramified. The same argument shows that $K_3(\alpha')/K_3$ is unramified. Since $K_3(\alpha) \neq K_3(\alpha')$ we see that $H(K_3) = K_3(\alpha, \alpha')$. Because 163 is prime we have $g(K) = 1$ for all fields of conductor 163. By Theorem 13 (Pushing Up) we have $4 \mid h(K)$ for these fields.

We get the following class number bounds using Theorem 5 (assuming GRH):

$$h(K_9) \leqslant 51 \qquad \text{for } A = 112.863,$$
$$h(K_{27}) \leqslant 223 \qquad \text{for } A = 147.266,$$
$$h(K_{81}) \leqslant 386 \qquad \text{for } A = 162.826.$$

We use Theorem 8 (Rank) for 2 and all primes from 5 up to 89, and we use Theorem 12 (Pushing Down) for 3. So we find $h(K) = 4$ for all these fields. Because $K(\alpha, \alpha')/K$ is unramified we have $H(K) = K(\alpha, \alpha')$. □

$f = 183$. For the following proposition we need some notation. Let L_3 be the cubic field of conductor 61. Then $L_3 = \mathbf{Q}(\omega)$, where ω is a zero of $x^3 + x^2 - 20x - 9$. Let α be a zero of $x^2 + \omega x + \omega$, and α' be a zero of $x^2 + \omega' x + \omega'$, where $\omega' = \frac{1}{3}(12 - 2\omega - \omega^2)$ is a conjugate of ω.

PROPOSITION 18. *Assume GRH. Let K be a real abelian field of conductor* 183. *Then*
(a) $h(K) = g(K) = 1$ *if* $[K : \mathbf{Q}] \in \{4, 20\}$,
(b) $h(K) = 4$, $H(K) = K(\alpha, \alpha')$ *if* $[K : \mathbf{Q}] \in \{12, 60\}$.

Proof. We have the following diagram (Figure 1) of subfields of $\mathbf{Q}(\zeta_{183})^+ = K_{60}$. Here The K_i are of conductor 183 and the L_i are of conductor 61. Masley [13] gives $h(L_i) = 1$. All $g(K_i)$ are 1.

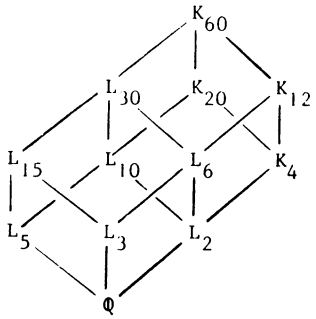

FIGURE 1

In L_3 we have 3 primes $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$ over 3. We choose them such that

$$\omega \equiv 0 \bmod \mathfrak{p}, \qquad \omega' \equiv 1 \bmod \mathfrak{p},$$
$$\omega \equiv 1 \bmod \mathfrak{q}, \qquad \omega' \equiv 1 \bmod \mathfrak{q},$$
$$\omega \equiv 1 \bmod \mathfrak{r}, \qquad \omega' \equiv 0 \bmod \mathfrak{r}.$$

Then $L_3(\alpha)/L_3$ ramifies only at $\mathfrak{q}$, $\mathfrak{r}$, and $L_3(\alpha')/L_3$ ramifies only at $\mathfrak{p}$, $\mathfrak{q}$. Since the ideals over $\mathfrak{p}$, $\mathfrak{q}$, and $\mathfrak{r}$ are ramified in K_{12}/L_6, the extensions $K_{12}(\alpha, \alpha')/K_{12}$ and $K_{60}(\alpha, \alpha')/K_{60}$ are unramified, and 4 divides $h(K_{12})$ and $h(K_{60})$. The class number

upper bound for K_{60}, assuming GRH, gives $h(K_{60}) \leqslant 10$. So $h(K_{60}) \in \{4, 8\}$. We use Theorem 13 (Pushing Up) for all odd primes to see that each $h(K_i)$ is a 2-power. If $2 \mid h(K_4)$, then, by using Theorem 11 for $K_4/\mathbf{Q}$, we get an extension of $\mathbf{Q}$ of degree 2 in which only 3 ramifies. This is impossible, so $h(K_4) = 1$. Now we use Theorem 6, with $K = K_4$, to get $h(K_{60}) = h^*(K_{60}) \cdot h(K_{20}) \cdot h(K_{12})$. From Theorem 8 with $K = K_4$ we know that $h(K_{12})$ is a power of 4 greater than 1, and that $h(K_{20})$ and $h^*(K_{60})$ are powers of 16. This leaves only one possibility: $h(K_{12}) = 4$, $h(K_{20}) = 1$, $h(K_{60}) = 4$. □

$f = 136$.

PROPOSITION 19. *Let K be a real abelian field of conductor* 136, *then*

(a) $h(K) = g(K)$ *if* $K \neq \mathbf{Q}(\zeta_{136})^+$,

(b) $h(K) = 2 \cdot g(K) = 2$, $H(K) = K(\sqrt{5 + 2\sqrt{2}})$ *if* $K = \mathbf{Q}(\zeta_{136})^+$.

Proof. We have the following diagram (Figure 2) of subfields of $K_{32} = \mathbf{Q}(\zeta_{136})^+$:

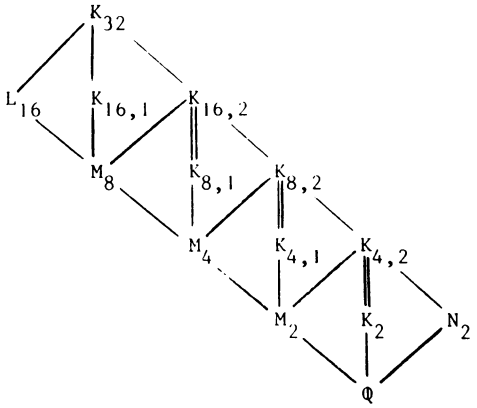

FIGURE 2

The K_i are of conductor 136, the field L_{16} is of conductor 68, the M_i are of conductor 17 and $N_2 = \mathbf{Q}(\sqrt{2})$ is of conductor 8. A double bar indicates an unramified extension.

Masley [13] gives $h(K) = 1$ for the fields with conductor < 136. The table of Borewicz-Šafarevič [1] gives $h(K_2) = 2$. For the remaining fields we have the following list:

K	$h(K) \leqslant$	$g(K)$	$G(K)$
$K_{4,1}$	5	2	$K_{8,2}$
$K_{4,2}$	2	1	$K_{4,2}$
$K_{8,1}$	6	2	$K_{16,2}$
$K_{8,2}$	2	1	$K_{8,2}$
$K_{16,1}$	5	1	$K_{16,1}$
$K_{16,2}$	3	1	$K_{16,2}$
K_{32}	44	1	K_{32}

Using Theorem 8 (Rank) for the odd primes, we see that each $h(K_i)$ is a 2-power.

Consider the extension $K_{16,2}/N_2$. In this extension only the two primes over 17 ramify. If $2 \mid h(K_{16,2})$, we can use Theorem 11 to get a quadratic extension of N_2 in which the only ramifying prime is a prime $\mathfrak{p}$ over 17. Class field theory then gives

$$2 \mid \text{Index}\left[(\mathcal{O}(N)/\mathfrak{p})^* : \mathcal{O}(N_2)^* \bmod \mathfrak{p}\right],$$

because $h(N_2) = 1$. But $1 + \sqrt{2} \in \mathcal{O}(N_2)^*$ has order 16 mod $\mathfrak{p}$, so this index is 1 and $2 \nmid h(K_{16,2})$. Now we can use Theorem 13 (Pushing Up) to get $h(K_{4,2}) = h(K_{8,2}) = 1$, $h(K_{4,1}) = h(K_{8,2}) = 2$.

It is known that K_2 has strict class number equal to 4. This means that $K_{4,2}$ has a quadratic extension in which precisely the infinite primes ramify: $K_{4,2}(\sqrt{-5-2\sqrt{2}})$. So also $K_{32}(\sqrt{-5+2\sqrt{2}})/K_{32}$ ramifies precisely at the infinite primes. Since the same is true for $K_{32}(\sqrt{-1})/K_{32}$, we find that $K_{32}(\sqrt{5+2\sqrt{2}})/K_{32}$ is totally unramified. So $H_{64} = K_{32}(\sqrt{5+2\sqrt{2}})$ satisfies $H_{64} \subset H = H(K_{32})$.

The group $A = \text{Gal}(H/K_{32})$ is isomorphic to the class group of K_{32}, and it is a module over $G = \text{Gal}(K_{32}/N_2)$. Let σ generate G. Let $H' \subset H$ be the fixed field of A^{σ^2-1}, and let $H'' \subset H$ be the fixed field of $A^{\sigma-1}$. Then H'' is the maximal subfield of H which is abelian over N_2, and H' is the maximal subfield of H which is abelian over $K_{4,2}$. Hence $H_{64} \subset H'' \subset H' \subset H$.

The primes ramifying in $H'/K_{4,2}$ are two primes $\mathfrak{p}_2, \mathfrak{q}_2$ lying over 2 and two primes $\mathfrak{p}_{17}, \mathfrak{q}_{17}$ lying over 17. Theorem 14 tells us that $\mathfrak{f} = \mathfrak{f}_{H'/K_{4,2}} = \mathfrak{f}_{K_{32}/K_{4,2}}$. Using the conductor-discriminant theorem [8, Chapter IV, Section 7.3, Theorem 7.3] we obtain $\mathfrak{f} = \mathfrak{p}_2^2\mathfrak{q}_2^2\mathfrak{p}_{17}\mathfrak{q}_{17}$. Class field theory then gives

$$[H' : K_{4,2}] \mid \text{Index}\left[(\mathcal{O}(K_{4,2})/\mathfrak{f})^* : \mathcal{O}(K_{4,2})^* \bmod \mathfrak{f}\right].$$

Using that

$$\langle -1, 1+\sqrt{2}, 4+\sqrt{17}, 3\sqrt{2}+\sqrt{17} \rangle \subset \mathcal{O}(K_{4,2})^*,$$

we calculate that this index is $\leqslant 16$. But we know $H' \supset H_{64}$, so this index is $\geqslant 16$ and $H' = H_{64}$. Then also $H'' = H_{64}$, and $A^{\sigma^2-1} = A^{\sigma-1}$, i.e., $(A^{\sigma-1})^{\sigma+1} = A^{\sigma-1}$. But $A^{\sigma-1}$ is a 2-group, and σ has 2-power order, so $(A^{\sigma-1})^{(\sigma+1)^N} = 1$ for some N. We conclude that $A^{\sigma-1} = 1$ and $H = H_{64}$.

If now $2 \mid h(K_{16,1})$, then $h(K_{16,1}) = 2$ by Theorem 13 (Pushing Up). Then $H(K_{16,1})/\mathbf{Q}$ is abelian which is impossible because $g(K_{16,1}) = 1$. □

f = 145.

PROPOSITION 20. *Assume GRH. Let K be a real abelian field of conductor* 145. *Then*
(a) $h(K) = g(K) = 1$ *if* $\sqrt{145} \notin K$,
(b) $h(K) = 2 \cdot g(K)$, $H(K) = G(K)(\alpha)$ *if* $\sqrt{145} \in K$,
where α *is a zero of* $X^2 + \theta X - 1$, *with* $\theta = \frac{1}{2}(1+\sqrt{5})$.

Proof. We have the following diagram (Figure 3) of subfields of $\mathbf{Q}(\zeta_{145})^+ = K_{56}$:

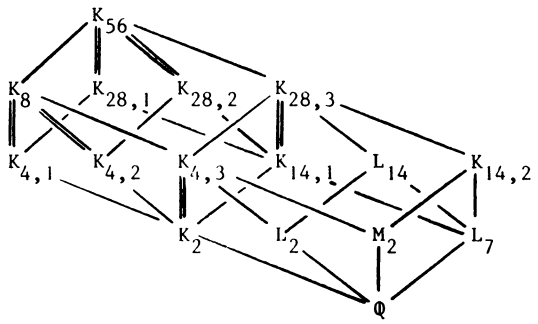

FIGURE 3

The K_i have conductor 145, the L_i have conductor 29 and $M_2 = \mathbf{Q}(\sqrt{5})$ has conductor 5. Unramified extensions are indicated by a double bar.

Borewicz and Šafarevič [1] give $h(K_2) = 4$, $h(M_2) = h(L_2) = 1$. Masley [13] gives $h(L_i) = 1$. For the other fields we have the following list, using GRH:

K	$h(K) \leqslant$	$g(K)$	$g'(K)$	$G(K)$
$K_{4,1}$	11	2	4	K_8
$K_{4,2}$	11	2	4	K_8
$K_{4,3}$	2	1	2	$K_{4,3}$
K_8	5	1	2	K_8
$K_{14,1}$	5	2	4	$K_{28,3}$
$K_{14,2}$	3	1	1	$K_{14,2}$
$K_{28,1}$	11	2	4	K_{56}
$K_{28,2}$	11	2	4	K_{56}
$K_{28,3}$	2	1	2	$K_{28,3}$
K_{56}	5	1	2	K_{56}

By Theorem 8 (Rank) we find that $h(K_{14,2}) = 1$. By the above table, all other class numbers are 2-powers, and $h(K_{4,3}) = h(K_{28,3}) = 2$.

The extension $M_2(\alpha)/M_2$ is only ramified at one prime over 29. The extension $M_2(\alpha')/M_2$ is only ramified at the other prime over 29, where α' is a zero of $X^2 + (1 - \theta)X - 1$. Because $K_{4,3}(\alpha) = K_{4,3}(\alpha')$, the extension $K_{4,3}(\alpha)/K_{4,3}$ is unramified, and for all fields K containing K_2 we get $K(\alpha) \subset H(K)$.

Let $H = H(K_8)$. The group $A = \mathrm{Gal}(H/K_8)$ is isomorphic to the class group of K_8, and it is a module over $G = \mathrm{Gal}(K_8/M_2)$. Let σ be a generator of G. We denote the fixed field of A^{σ^2-1} by H' and the fixed field of $A^{\sigma-1}$ by H''. Then H'' is the maximal subfield of H which is abelian over M_2 and H' is the maximal subfield of H which is abelian over $K_{4,3}$. Hence $H_{16} = K_8(\alpha) \subset H'' \subset H' \subset H$. The primes ramifying in $H'/K_{4,3}$ are two primes $\mathfrak{p}_5$ and $\mathfrak{q}_5$ lying over 5 and two primes $\mathfrak{p}_{29}$ and $\mathfrak{q}_{29}$ lying over 29. By Theorem 14 we get $\mathfrak{f}_{H'/K_{4,3}} = \mathfrak{p}_5\mathfrak{q}_5\mathfrak{p}_{29}\mathfrak{q}_{29}$.

Let $F \subset H'$ be the field corresponding to the inertia group of $\mathfrak{p}_5$ in $\mathrm{Gal}(H'/K_{4,3})$. Then $\mathfrak{f}_{F/K_{4,3}} \mid \mathfrak{q}_5\mathfrak{p}_{29}\mathfrak{q}_{29}$, and $[H' : F] = 2$. Class field theory gives: $[F : K_{4,3}] \mid 2 \cdot \mathrm{Index}[(\mathcal{O}(K_{4,3})/\mathfrak{q}_5\mathfrak{p}_{29}\mathfrak{q}_{29})^* : \mathcal{O}(K_{4,3})^* \bmod \mathfrak{q}_5\mathfrak{p}_{29}\mathfrak{q}_{29}]$, because $h(K_{4,3}) = 2$. Using that $\langle -1, \frac{1}{2}(1+\sqrt{5}), \frac{1}{2}(5+\sqrt{29}), \frac{1}{4}(13+7\sqrt{5}+3\sqrt{29}+\sqrt{145}\rangle \subset \mathcal{O}(K_{4,3})^*$, we find that this index is odd, so $[F : K_{4,3}] = 2$ and $[H' : K_{4,3}] = 4$. But then we have $H' = H'' = H_{16}$ and $A^{\sigma-1} = A^{\sigma^2-1}$. An argument as in the proof of Proposition 19 then shows that $A^{\sigma-1} = 1$. So $H = H_{16} = K_8(\alpha)$, and $h(K_8) = 2$.

Now we can use Theorem 13 (Pushing Up) to find $b(K_{4,1}) = h(K_{4,2}) = 4$, and Theorem 8 (Rank) plus Theorem 6 to find $h(K_{28,1}) = h(K_{28,2}) = 4$ and $h(K_{56}) = 2$. □

$f = 111$.

PROPOSITION 21. *Let K be a real abelian field of conductor* 111. *Then* $h(K) = 1$.

Proof. We have the following diagram (Figure 4) of subfields of $\mathbf{Q}(\zeta_{111})^+ = K_{36}$:

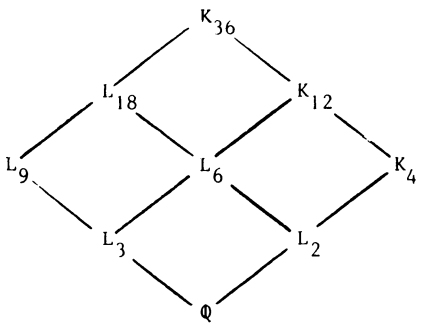

FIGURE 4

The K_i are of conductor 111 and the L_i are of conductor 37. From the tables of Masley [13] we see that $h(L_i) = 1$. Upper bounds for the remaining class numbers are:

K	$h(K) \leqslant$
K_4	6
K_{12}	15
K_{36}	63

Since $2 \cdot 3 \cdot 37 \mid h^-(\mathbf{Q}(\zeta_{111}))$, we cannot apply Theorem 9 (Reflection) for 2, 3, or 37 (presumably a refinement of Theorem 9 can be used for 37); and for the other primes the tables of Schrutka von Rechtenstamm [15] do not extend far enough. Using Theorem 8 (Rank) we see that the only possible primes dividing $h(K_4)$ are 2 and 5, the only possible primes dividing $h(K_{12})$ are 2, 3, 5, and 13 and the only possible primes dividing $h(K_{36})$ are 2, 3, 5, 13, and 37. Now we can use Corollary 12 (Pushing Down) to get $3 \nmid h(K_{12})$ and $3 \nmid h(K_{36})$.

The extension K_{12}/L_3 is only ramified at the prime $\mathfrak{p}$ over 37 and the prime $\mathfrak{q}$ over 3. If $2 \mid h(K_{12})$, we can use Theorem 11 to show that there is a quadratic extension M/L_3 in which only $\mathfrak{q}$ ramifies. This must be a tame ramification, so $\mathfrak{f}_{M/L_3} = \mathfrak{q}$. By

class field theory this implies $2 \mid \text{Index}[(\mathcal{O}(L_3)/\mathfrak{q})^* : \mathcal{O}(L_3)^* \bmod \mathfrak{q}]$. But $N\mathfrak{q} = 27 \equiv 3 \bmod 4$, and $-1 \in \mathcal{O}(L_3)^*$. So this index is odd, and $2 \nmid h(K_{12})$. Now we can use Theorem 13 (Pushing Up) and Theorem 8 (Rank) to find that $2 \nmid h(K_4)$ and $2 \nmid h(K_{36})$.

We use step 5 to get $37 \nmid h(K_{36})$ as follows. Let σ be the automorphism of $\mathbf{Q}(\zeta_{222})$ defined by $\zeta_{222}^{\sigma} = \zeta_{222}^{5}$. We denote the restriction of σ to K_{36} again by σ. This is a generator of $\text{Gal}(K_{36}/\mathbf{Q})$.

We use Theorem 16. The group $C = C'_{K_{36}}$ is generated as a $\mathbf{Z}[G]$-module by

$$\alpha = (\zeta - \zeta^{-1})/(\zeta^5 - \zeta^{-5}) \quad \text{and} \quad \beta = (\xi - \xi^{-1})/(\xi^5 - \xi^{-5}),$$
$$\text{with } \zeta = \zeta_{222} \text{ and } \xi = \zeta_{74} = \zeta^3.$$

We have $\alpha^{1+\sigma^{18}} = \beta^{1-\sigma^2}$.

There is a $\mathbf{Z}[G]$-module isomorphism between C/C^{37} and $\mathbf{F}_{37}[G]/\mathbf{F}_{37} \cdot \text{Tr}$, with $\text{Tr} = \sum_{i=0}^{35} \sigma^i$. Let $F_i \in \mathbf{Z}[G]$ be defined by

$$F_i = \prod_{\substack{j=2 \\ j \neq i}}^{36} (\sigma - j) \quad \text{for } j = 2, \ldots, 36.$$

We can calculate $F_i \pmod{37}$ by a "polynomial"-division $\text{Tr}/(\sigma - i)$. Put

$$C_i = C^{F_i} \cdot C^{37} \qquad (2 \leqslant i \leqslant 36).$$

Then the minimal submodules of C/C^{37} are precisely the modules

$$C_i/C^{37} \qquad (2 \leqslant i \leqslant 36).$$

The submodule B of C generated by β is equal to the group C_L for $L = L_{18}$. Since $h(L) = 1$, we know that $\mathcal{O}(L)^{*37} \cap B = B^{37}$ from Theorem 15. Using that $K_{36}^{*37} \cap L^* = L^{*37}$, we deduce that

$$(*) \qquad E^{37} \cap (B \cdot C^{37}) = C^{37}.$$

To prove that $37 \nmid h(K_{36})$, we must show that $E^{37} \cap C_i = C^{37}$ for $2 \leqslant i \leqslant 36$. If $(i/37) = 1$, then $1 + \sigma^{18} \mid F_i$ so $C_i \subset B \cdot C^{37}$, and we can apply $(*)$. If $(i/37) = -1$, then $1 - \sigma^{18} \mid F_i$, and $C_i = \langle \alpha^{F_i} \rangle \cdot C^{37}$. For these i we can show that α^{F_i} is not a 37th power in the following way. Let $\mathfrak{p}$ be a prime over 223. It is easy to compute $\alpha^{\sigma^i} \bmod \mathfrak{p}$ using that, for example, 5 is a primitive 222th root of unity mod 223. Now we can compute $\alpha^{F_i} \bmod \mathfrak{p}$. We know that α^{F_i} is a 37th power mod $\mathfrak{p}$ if and only if $\alpha^{6F_i} \equiv 1 \bmod \mathfrak{p}$. It turns out that $\alpha^{6F_i} \not\equiv 1 \bmod \mathfrak{p}$ for $(i/37) = -1$, $2 \leqslant i \leqslant 36$. This proves that $37 \nmid h(K_{36})$.

For the primes 5 and 13 we can proceed in an analogous way: for 5 we work with cyclotomic units in K_4, and we reduce modulo a prime lying over 2221; for 13 we work with cyclotomic units in K_{12}, reducing modulo a prime lying over 2887.

Appendix. In this appendix we give an abstract from the tables of Odlyzko [14], which we use when we compute class number bounds.

Table 1. Let K be a totally real field. For the discriminant we then have $\Delta_K > A^n e^{-E}$ for the following pairs:

A	E	A	E
18.916	5.3334	54.333	26.667
21.512	6.0001	55.335	29.334
24.016	6.6667	56.129	32.001
26.406	7.3334	56.767	34.667
28.668	8.0001	57.286	37.334
32.780	9.3334	57.714	40.001
36.347	10.667	58.070	42.667
39.407	12.001	58.370	45.334
42.018	13.334	58.624	48.001
46.138	16.001	59.028	53.334
49.145	18.667	59.456	61.334
51.371	21.334	59.896	74.667
53.047	24.001	60.704	200.01

Recently Diaz y Diaz [21] published a table of discriminant lower bounds, not assuming GRH. He computed this table with techniques analogous to those of Odlyzko. In all cases where we derived upper bounds from Table 1, we can also get this upper bound or a slightly better one using the tables of Diaz y Diaz, except for $K = \mathbf{Q}(\zeta_{111})^+$. In the latter case we derive $h(K) \leqslant 62$ from formula (1) of [21].

For the class field H of $\mathbf{Q}(\zeta_{128})^+$ of degree $[H:\mathbf{Q}] = 32h$, we derive from the paper of Poitou [22] the following formula (not assuming GRH).

$$\frac{191}{32}\log 2 \geqslant \gamma + \log 4\pi + 1 - \frac{7\zeta(3) + 4\zeta(2)}{8b} - \frac{b\sqrt{\pi}}{8h} + \frac{1}{16h}\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\frac{\log N\mathfrak{p}}{(N\mathfrak{p})^{m/2}}F(\log N\mathfrak{p}^m) \quad \text{for all } b > 0,$$

where the outer summation is over all primes $\mathfrak{p}$ of H, and

$$F(x) = \frac{e^{-x^2/4b}}{\cosh(x/2)}.$$

If we sum only over the primes over 2 and only for $1 \leqslant m \leqslant 8$, we obtain $h \leqslant 112$, where we use the fact that the prime over 2 splits completely in $H/\mathbf{Q}(\zeta_{128})^+$, because it is principal. Using Theorem 8 and Corollary 12, we derive $h = 1$ or $h = 97$. If, however, we use the formula of Odlyzko, we could derive $h \leqslant 37$, which implies $h = 1$.

Table 2. Let K be a totally real field, for which GRH is true for the ζ-function of K. Then $\Delta_K > A^n e^{-E}$ for the following pairs:

A	E	A	E
29.298	7.8187	84.656	36.044
31.386	8.3664	94.761	48.840
33.511	8.9400	104.174	66.559
35.667	9.5414	112.863	91.287
37.853	10.173	120.834	126.05
40.063	10.837	128.112	175.22
42.295	11.535	133.464	229.13
44.543	12.270	138.423	300.88
46.806	13.045	143.015	396.69
49.079	13.863	147.266	525.04
51.359	14.726	151.201	697.52
55.928	16.603	154.845	929.98
60.490	18.706	158.220	1244.2
65.024	21.066	162.826	1937.1
69.513	23.723	213.626	5.7672×10^{26}
73.940	26.719		

We can also obtain upper bounds, assuming GRH, by using formula (10) of [23].

Mathematisch Instituut
Universiteit van Amsterdam
Roetersstraat 15
1018 WB Amsterdam, The Netherlands

1. S. I. Borewicz & I. R. Šafarevič, *Zahlentheorie*, Birkhäuser-Verlag, Basel-Stuttgart, 1966.
2. J. W. S. Cassels & A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, New York, 1967.
3. A. Fröhlich, "On the class group of relatively abelian fields," *Quart. J. Math. Oxford Ser.* (2), v. 3, 1952, pp. 98–106.
4. G. Gras & M. N. Gras, "Signature des unités cyclotomiques et parité du nombre de classes des extensions cycliques de **Q** de degré premier impair," *Ann. Inst. Fourier (Grenoble)*, v. 25, 1975, pp. 1–22.
5. M. N. Gras, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de **Q**," *J. Reine Angew. Math.*, v. 277, 1975, pp. 89–116.
6. M. N. Gras, "Table numérique de nombre de classes et des unités des extensions cycliques réelles de degré 4 de **Q**," *Publ. Math. Fac. Sci. Besançon*, 1978.
7. H. Hasse, *Ueber die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
8. S. Iyanaga (ed.), *The Theory of Numbers*, North-Holland, Amsterdam and American Elsevier, New York, 1975.
9. S. Lang, *Cyclotomic Fields*, Springer-Verlag, Berlin and New York, 1979.
10. H. W. Leopoldt, *Ueber Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Akademic-Verlag, Berlin, 1954.
11. S. Mäki, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math., vol. 797, Springer-Verlag, Berlin and New York, 1980.
12. J. Martinet, "Tours de corps de classes et estimations de discriminants," *Invent. Math.*, v. 44, 1978, pp. 65–73.
13. J. M. Masley, "Class numbers of real cyclic number fields with small conductor," *Compositio Math.*, v. 37, 1978, pp. 297–319.
14. A. M. Odlyzko, *Discriminant Bounds*, Unpublished tables (Nov. 1976).
15. G. Schrutka von Rechtenstamm, *Tabelle der (Relativ)-Klassenzahlen der Kreiskörper*, Akademic-Verlag, Berlin, 1964.

16. J.-P. SERRE, *Représentations Linéaries des Groups Finis*, Hermann, Paris, 1967.

17. W. SINNOTT, "On the Stickelberger ideal and the circular units of a cyclotomic field," *Ann. of Math.* (2), v. 108, 1978, pp. 107–134.

18. W. SINNOTT, "On the Stickelberger ideal and the circular units of an abelian field," *Invent. Math.*, v. 62, 1980, pp. 181–234.

19. S. WAGSTAFF, JR., "The irregular primes to 125000," *Math. Comp.*, v. 32, 1978, pp. 583–591.

20. N. G. DE BRUIJN, "On the factorization of cyclic groups," *Indag. Math.*, v. 15, 1953, pp. 370–377.

21. F. DIAZ Y DIAZ, "Tables minorant la racine n-ième du discriminant d'un corps de degré n," *Publ. Math. Orsay* 80, 1980.

22. G. POITOU, "Minorations de discriminants," *Séminaire Bourbaki*, Vol. 1975/76, 28ème année, Exp. No. 479, pp. 136–153.

23. G. POITOU, "Sur les petits discriminants," *Séminaire Delange-Pisot-Poitou*, v. 18, no. 6, 1976/77, pp. 1–21.