COMPOSITIO MATHEMATICA

JOHN MYRON MASLEY

Class numbers of real cyclic number fields with small conductor

Compositio Mathematica, tome 37, nº 3 (1978), p. 297-319

<http://www.numdam.org/item?id=CM_1978__37_3_297_0>

COMPOSITIO MATHEMATICA, Vol. 37, Fasc. 3, 1978, pag. 297–319
Sijthoff & Noordhoff International Publishers–Alphen aan den Rijn
Printed in the Netherlands

CLASS NUMBERS OF REAL CYCLIC NUMBER FIELDS WITH SMALL CONDUCTOR

JOHN MYRON MASLEY

By an algebraic number field F we shall mean a finite extension of $\mathbf{Q}$, the field of rational numbers. The class number $h(F)$ of F is the order of $C(F)$, the group of ideal classes (non-zero fractional ideals modulo principal ideals) of F. The discriminant of F will be denoted $d(F)$. The Kronecker–Weber Theorem says that the abelian extensions of $\mathbf{Q}$ are the subfields of all the full cyclotomic fields $\mathbf{C}(m) = \mathbf{Q}(\exp 2\pi i/m)$ where m is a positive integer. If K is an abelian extension of $\mathbf{Q}$, the least positive integer f with $\mathbf{C}(f) \supset K$ is called the conductor of K and is denoted $f(K)$. Since $\mathbf{C}(2f) = \mathbf{C}(f)$ for odd f, $f(K)$ is either odd or divisible by 4.

Hasse compiled many results about class numbers of abelian extensions of $\mathbf{Q}$ in his monograph [9]. In particular, for K an abelian extension of $\mathbf{Q}$, $h(K) = h^*(K)h(K')$ where K' is the maximal real subfield of K and the quotient $h(K)/h(K') = h^*(K)$, the relative class number of K, is an integer. When $K = \mathbf{C}(m)$ we shall abbreviate $h(\mathbf{C}(m))$ to $h(m) = h^*(m)h'(m)$ with $h'(m) = h(\mathbf{Q}(\cos 2\pi/m))$. Hasse shows that $h^*(K)$ is very easy to compute and he lists the relative class numbers of all imaginary abelian extensions of $\mathbf{Q}$ whose conductor does not exceed 100. In [8] Hasse calculated $h(K)$ for real cyclic $K/\mathbf{Q}$ of degree 3 and 4 where $f(K) \leq 100$.

Hasse's student Leopoldt took up the attack on the class number of real abelian extensions of $\mathbf{Q}$ in a series of papers [13–17]. In particular, he showed that, essentially, one need consider only the class numbers of the real cyclic extensions and some information on units. Bauer [1] used a computer to calculate the class numbers of most of the real cyclic extensions of $\mathbf{Q}$ of conductor ≤ 100 via methods derived from Leopoldt's results.

In previous work [18–21], we have determined explicitly all positive integers m with $h(m) \leq 10$. One ingredient needed in that work was various knowledge about the class numbers of real cyclic number fields with small conductor. Reference was made to [1] which covered most of the needed facts. Unfortunately Bauer's paper is merely a report and does not give any details of how he applied Leopoldt's results. A later computational paper of Bauer [2] does contain errors, so we wish to show that the results of [1] which we used are correct. We are able to verify the results of Bauer's computations for all but 5 fields. We are also able to compute the class numbers of 13 fields for which Bauer's computations were incomplete. In particular, we show that the class number of any real abelian field of prime power conductor less than 71 has class number one.

1. Root-discriminants and Odlyzko bounds

In this section we develop the theory of the root-discriminant and illustrate its application to class number problems.

DEFINITION: Let F be an extension of $\mathbf{Q}$ of finite degree n and discriminant $d(F)$. Then the root-discriminant of F, denoted $rd(F)$, is $|d(F)^{1/n}|$.

PROPOSITION 1.1: *Let $E \supset F$ both be algebraic number fields. Then $rd(E) \geq rd(F)$. Furthermore, equality holds if and only if no prime ideal of F ramifies in E.*

PROOF: Let $d(E/F)$ be the absolute norm from F of the relative discriminant ideal for E/F. By the relative discriminant formula for the tower $E \supset F \supset \mathbf{Q}$, we have $|d(E)| = d(E/F)|d(F)|^{|E:F|}$. Now $d(E/F) \geq 1$ with equality if and only if no prime ideal, i.e. no finite prime divisor, of F ramifies in E. The result follows upon taking $|E:\mathbf{Q}| = |E:F| \cdot |F:\mathbf{Q}|$-th roots.//

COROLLARY 1.2: *Let F be an algebraic number field and let E be any intermediate field between F and the narrow Hilbert class field of F. Then $rd(E) = rd(F)$. In particular, the Hilbert class field of F has the same root discriminant as F.*

PROOF: The narrow Hilbert class field of F, $N(F)$, is the maximal abelian extension of F unramified at all finite prime divisors of F. By (1.1) we have $rd(N(F)) \geq rd(E) \geq rd(F) = rd(N(F))$. In particular, $N(F)$ contains the Hilbert class field of F.//

EXAMPLE 1.3: All the fields in the infinite Hilbert class field tower of $Q(9699690^{1/2})$ have root discriminant 6228.9—.

EXAMPLE 1.4. We put $rd(m) = rd(\mathbf{C}(m))$ and $rd'(m) = rd(\mathbf{C}'(m))$. If at least two distinct primes, p and q say, are ramified in $\mathbf{C}(m)$, then $rd(m) = rd'(m)$. This follows from (1.1) since $\mathbf{C}(m) = \mathbf{C}'(m)\mathbf{C}(p) = \mathbf{C}'(m)\mathbf{C}(q)$ shows that, on the one hand, at most prime ideals above p are ramified in $\mathbf{C}(m)/\mathbf{C}'(m)$ and, on the other hand, at most prime ideals above q can be ramified. (If $p = 2$, use $\mathbf{C}(4)$ instead of $\mathbf{C}(2)$.)

PROPOSITION 1.5: *Let F and K be algebraic number fields with relatively prime discriminants and let E be the compositum of F and K. Then $rd(E) = rd(F)\, rd(K)$.*

PROOF: This follows from the relation

$$d(E) = d(F)^{|K:Q|}\, d(K)^{|F:Q|} \text{ (cf. [28]).//}$$

PROPOSITION 1.6: The root-discriminants $rd(m)$ of $\mathbf{C}(m)$ and $rd'(m)$ of $\mathbf{Q}(\cos 2\pi/m)$ are given by

$$rd(p^a) = p^{a-1/(p-1)},\ rd'(p^a) = p^{a-1/(p-1)-[p/p-1]/\varphi(p^a)}$$

for the prime power $p^a \neq 2$ where $[x]$ is the greatest integer in x, and $rd(m) = rd'(m) = \prod_{p^a \| m} rd(p^a)$ whenever at least two primes ramify in $\mathbf{C}(m)$.

PROOF: It is well-known that $d(\mathbf{C}(p^a)) = \pm p^{a\varphi(p^a)-\varphi(p^a)/(p-1)}$. Also (use the conductor-discriminant formula) we have that $[p/p-1] \cdot p \cdot d(\mathbf{C}'(p^a))^2 = \pm d(\mathbf{C}(p^a))$ so the root-discriminant values in the prime power case follow easily. For $m = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$ note that $\mathbf{C}(m) = \mathbf{C}(p_1^{a_1})\mathbf{C}(p_2^{a_2}) \dots \mathbf{C}(p_t^{a_t})$ and apply (1.5) and (1.4).//

To connect root-discriminants and class number bounds we need a new concept.

DEFINITION: **An increasing arithmetical arithmetical function $g{:}N \to \{x \in \mathbf{R} \mid x > 0\}$ is called a class number bound function (for totally real fields) if for all positive integers n we have $g(n) \leq \inf rd(F)$ where the infimum is taken over all totally real number fields of degree n.**

Since all the fields in the Hilbert class field tower of $\mathbf{Q}(9699690^{1/2})$ have the same root-discriminant (1.3), a class number bound function is necessarily bounded. The best bound is not known. Optimal values of a class number bound function are known only for n = 1,2, . . . ,7 [27]. The best known class number bound functions for class number problems have been constructed by Andrew Odlyzko in a recent series of articles [23–26] and preprints dealing with lower bounds for the absolute values of discriminants of number fields. We have indicated in [22] how the results of Odlyzko apply to number fields which are not totally real. For most of our purposes the following special case of Odlyzko's work will be sufficient.

THEOREM 1.7: *There are explicit ordered pairs of positive real numbers* (A,E) *for which* $g_{(A,E)}(x) = Ae^{-E/x}$ *is a class number bound function. The function* $G(x) = sup_{(A,E)}\, g_{(A,E)}(x)$ *is also a class number bound function.*

PROOF: The reader is referred to [23–26] and also to the survey article [27].//

We give a small table of values of $G(x)$ which we used in our work in the appendix. We can now give the main result of this section.

THEOREM 1.8: *(Class Number Bound) Let* F *be a totally real number field and let* $g(x)$ *be a class number bound function. Then* $g(x) > rd(F)$ *implies* $h(F) < x/|F{:}\mathbf{Q}|$.

PROOF: Let $H(F)$ be the Hilbert class field of F. We have $g(x) > rd(F) = rd(H(F)) \geq g(|H(F){:}Q|) = g(h(F) \cdot |F{:}\mathbf{Q}|)$ and g is increasing.//

Since $g(x)$ is necessarily bounded (Example 1.3), Theorem 1.8 is useful only for fields with small root discriminants. The best known upper bound for $g(x)$ is 1058.5+ and is due to Martinet [31].

2. Some general theorems.

In this section we give some general results about the class numbers and ideal class groups of extensions E/F of number fields. We shall illustrate the results with abelian number fields, especially those which are (totally) real. Of special interest will be $\mathbf{Q}(\cos 2\pi/m)$ which we shall denote by $\mathbf{C}'(m)$, the maximal real subfield of $\mathbf{C}(m)$. The discriminant and class number of $\mathbf{C}'(m)$ will be denoted by $d'(m)$ and $h'(m)$ respectively. We shall also use the notation $F(n,f)$ to denote an n-th degree cyclic extension of $\mathbf{Q}$ with conductor f. When n and f do not determine a unique field, we shall be considering all the fields with a given n and f at the same time. We will mention other ways to distinguish them when necessary.

For a number field F, the Hilbert class field $H(F)$ is the maximal unramified abelian extension of F. Since the Galois group of $H(F)/F$ is canonically isomorphic to $C(F)$, $|H(F):F| = h(F)$. The letter p shall always denote a prime number.

The following theorem enables one to characterize the relative class number $h^*(m)$.

THEOREM 2.1: *Let E/F be an extension of number fields. The following are equivalent*:

(*i*) *For any unramified abelian extension H of F, $E \cap H = F$.*

(*ii*) *The norm map $N{:}C(E) \longrightarrow C(F)$ is surjective.*

If (*i*) *and* (*ii*) *are satisfied for E/F, then $C(F)$ is isomorphic to a subgroup of $C(E)$. In particular, $h(F)$ divides $h(E)$ and the order of the kernel of N is $h(E)/h(F)$.*

PROOF: By class field theory, the unramified abelian extensions of F which are contained in E correspond in an inclusion-reversing manner to the subgroups of $C(F)$ which contain the image of the norm map $N{:}C(E) \longrightarrow C(F)$.

When (i) and (ii) are satisfied, $C(E)/\ker N$ is isomorphic to $C(F)$. Since a finite abelian group A is isomorphic to its dual, any factor group of A is isomorphic to some subgroup of A.//

If the equivalent conditions of Theorem 2.1 are satisfied for the extension E/F, then one sees directly that $h(F) = |H(F):F| = |EH(F):E|$ divides $|H(E):E| = h(E)$ since $EH(F) \subset H(E)$. We incorporate this weaker result in

COROLLARY 2.2 (*Pushing up*): *Let E/F be an extension of number fields. Then $|H(F):H(F) \cap E|$ divides $h(E)$ and $h(F)$ divides $|E:F|h(E)$. In particular, if for any unramified abelian extension H of F we have $E \cap H = F$, then $h(F)$ divides $h(E)$.*

PROOF: We have $|H(F):H(F) \cap E| = |EH(F):E|$ dividing $|H(E):E|$.//

We call an extension E/F totally ramified if no subextension of E/F except F itself is unramified over F.

COROLLARY 2.3: *Suppose E/F is totally ramified. Then $h(F)$ divides $h(E)$.*

PROOF: For any unramified abelian extension H of F, $E \cap H = F$ since any extension of F contained in E is totally ramified.//

EXAMPLE 2.4: Let $F \subset E \subset \mathbf{C}(p^a)$ Then $h(F)$ divides $h(E)$.

COROLLARY 2.5: *For the cyclotomic fields we have $h'(m)$ divides $h(m)$, $h'(m)$ divides $h'(km)$, and $h(m)$ divides $h(km)$ for any positive integer k.*

PROOF: The extensions $\mathbf{C}(m)/\mathbf{C}'(m)$, $\mathbf{C}'(km)/\mathbf{C}'(m)$, and $\mathbf{C}(km)/\mathbf{C}(m)$ are totally ramified.//

The preceding results give information on the class group of a number field which is "pushed up" from the class groups of certain subfields. We can also "push down" information. The following lemma is fundamental.

LEMMA 2.6: *Let E/F be a non-trivial p-extension which is unramified outside the (possibly empt) finite set S of prime divisors of F.*

If S is empty, F has an unramified cyclic extension of degree p.

If $v \in S$, put $S' = S - \{v\}$. If p divides $h(E)$, then F has a cyclic extension of degree p which is unramified outside S'.

PROOF: Any proper subgroup of a p-group is contained in a normal subgroup of index p.

Let S be empty. Then $\mathrm{Gal}(E/F)$ contains a normal subgroup A of index p and the subfield of E fixed by A satisfies our requirements.

Suppose $v \in S$. Since $p \mid h(E)$, $P(E)$, the maximal unramified abelian p-extension of E, is a proper extension of E. If s is any embedding of $P(E)$ into an algebraic closure of F which restricts to the identity on F, then $s(E) = E$ since E/F is normal and $s(P(E))/s(E)$ is an unramified abelian p-extension. By maximality, $s(P(E)) = P(E)$ so $P(E)/F$ is Galois. Let $G = \mathrm{Gal}(P(E)/F)$.

Now let T be an inertia group for a prime w of $P(E)$ lying above v. Since $P(E) \neq E$ and $P(E)/E$ is unramified, T is a proper subgroup of G. Let N be a normal subgroup of G containing T with $|G:N| = p$ and let K be the subfield of $P(E)$ fixed by N. The inertia group $T' \subset G$ of any prime of $P(E)$ lying above v is conjugate in G to T, hence is contained in N. It follows that K/F is unramified at v. Since $P(E)/F$ is unramified outside S, K/F is then unramifiid outside S'.//

We now have the following

THEOREM 2.7 (*Pushing down*): *Suppose E/F is a p-extension with at most one ramified prime divisor of F ramified in E. Then p divides $h(E)$ only if p divides $h(F)$. If E/F is totally ramified, then p divides $h(E)$ if and only if p divides $h(F)$.*

PROOF: By Lemma 2.6, $H(F)$, the Hilbert class field of F, contains a cyclic extension of degree p over F. Hence p divides $h(F) = |H(F):F|$.

If E/F is totally ramified, Corollary 2.3 shows that $h(F)$ divides $h(E)$ so p in $h(F)$ would push up to $h(E)$.//

EXAMPLE 2.8: If p divides $h(p^a)$, then p divides $h(p)$.

EXAMPLE 2.9. Let p, q be primes with $p \equiv 1 \bmod 2q$. Then $h(F(q,p))$ is prime to q. In particular, for $p \equiv 1 \bmod 4$, $\mathbf{Q}(p^{1/2})$ has odd class number.

THEOREM 2.10: *Suppose $f = 4p$, pq, or $2^a q$ with $a \geq 3$, p and q odd primes, and $q \equiv 3 \bmod 4$. Then the maximal real abelian 2-extension K of Q with conductor f has odd class number.*

PROOF: By our assumptions, there is a finite prime v of $\mathbf{Q}$ which is fully ramified in $K/\mathbf{Q}$. If $h(K)$ is even, Lemma 2.6 gives us a quadratic extension $L/\mathbf{Q}$, unramified at v, with L contained in $P(K)$, the Hilbert 2-class field of K. By looking at v we see that $K \cap L = \mathbf{Q}$ so that $K \underset{\neq}{\subset} LK \subset P(K)$. However, then LK is a real abelian 2-extension of conductor f properly containing K.//

EXAMPLE 2.11: The field $\mathbf{C}'(68)$ has odd class number.

EXAMPLE 2.12: The totally real fields $F(4, 87)$, $F(4, 91)$, and $F(4, 95)$ have odd class number since $7 \equiv 19 \equiv 3 \bmod 4$.

EXAMPLE 2.13: The maximal real abelian 2-extension K of conductor 65 has odd class number. Theorem 2.10 and this result are special cases of results of Frohlich [4]. We prove that K has odd class number directly. Since $\mathbf{Q}(5^{1/2})$ has a unique prime above 13, Lemma 2.6 can be used to produce a quadratic extension $L/\mathbf{Q}(5^{1/2})$ ramified only at the prime above 5 if $h(K)$ is even. Since the only non-abelian 2-group which is a subgroup of the symmetric group on 4 elements is

D, the dihedral group of order 8, N = the Galois closure of L over $\mathbf{Q}$ has Galois group D. However, then an inertia group for the rational prime 5 cannot be cyclic of order 4 or 8.

The following theorem gives information on the structure of ideal class groups. By the p-rank of a finite abelian group C we mean the dimension of the vector space $\mathbf{Z}/p\mathbf{Z}\otimes_{\mathbf{Z}}C \simeq C/\{c^p \mid c \in C\}$ over the field $\mathbf{Z}/p\mathbf{Z}$. The p-rank of C is thus the number of cyclic factors in an elementary divisor decomposition of the p-Sylow subgroup of C. Analogously, for $q = p^a$, a any positive integer, we define the q-rank of C to be the number of cyclic factors in an elementary divisor decomposition of the p-Sylow subgroup of C whose order is divisible by q. Then we have

Theorem 2.14 (*Structure*): *Let E/F be a cyclic extension of degree n and let p be a prime which divides neither n nor $h(\tilde{E})$ for $F \subset \tilde{E} \subsetneq E$. Let $q = p^a$ for some positive integer a. Then the q-rank of $C(E)$ is divisible by f, the order of p* modulo *n.*

Proof: Assume the q-rank of $C(E)$ is not zero. We identify $C(E)$ with $\mathrm{Gal}(H(E)/E)$ via the Artin reciprocity law and put L = the subfield of $H(E)$ fixed by $C_q = \{c^q \mid c \in C(E)\}$. The group $G = \mathrm{Gal}(E/F)$ acts naturally on $C(E)$ and, from properties of the Artin symbol, this action corresponds to group theoretic conjugation of $\mathrm{Gal}(H(E)/E)$ by G. Now C_q is G-invariant so it is a normal subgroup of $\mathrm{Gal}(H(E)/F)$, L/F is Galois, and G acts on $B = \mathrm{Gal}(L/E) \simeq C(E)/C_q$.

To prove our theorem, it suffices to show that the action of G on $B - \{1\}$ is faithful. For then the orbits of a generator of G will each have n elements so card $B \equiv 1 \bmod n$ and, consequently, the order of $B = B(q)$ is a power of p^f. The p-rank of $C(E)$ is just the exponent $r = r_1$ with p^r = card $B(p)$. For $a > 1$ and $q = p^a$, the q-rank of $C(E)$ is the exponent $r = r_a$ with p^r = card $B(p^a)$/card $B(p^{a-1})$. By induction on a we will have $f \mid r_a$ for any positive integer a. In particular, the p-Sylow subgroup of $C(E)$ is then the f-fold direct sum of an abelian p-group with itself.

To show G acts faithfully, take $g \in G$ and let S be the subgroup generated by g. For $b \in B$ let gb denote the result of the action of g on b and extending this action by additivity consider B as a $\mathbf{Z}[G]$-module. Assume now that $g \neq 1$. We will be done if we show that $(g-1)B = B$ for then $g-1$ acts surjectively on a finite set and thus injectively. The injectivity shows that G acts as desired.

Let $\tilde{E}$ be the subfield of E fixed by S. Now $(g-1)B$ is a subgroup of B on which S acts and hence is a normal subgroup of $\mathrm{Gal}(L/\tilde{E})$. Then $\tilde{L}$, the subfield of L fixed by $(g-1)B$ is a normal extension of $\tilde{\mathrm{E}}$. We put $A = \mathrm{Gal}(\tilde{L}/\tilde{E})$ and we have $\bar{B} = B/(g-1)B = \mathrm{Gal}(\tilde{L}/E)$. Now $A/\bar{B} \simeq S$ and S acts trivially B.

Since the order of S is prime to the order of B, the group extension $A/\bar{B}$ splits and we have the direct product $A \simeq \bar{B} \times D$ where $D \simeq S$. Let K be the fixed field of D so that $\mathrm{Gal}(\tilde{L}/K) = D$ and $\mathrm{Gal}(K/\tilde{E}) \simeq A/D \simeq B$. Suppose $\bar{B}$ is non-trivial. Let P be any prime divisor of $\tilde{L}$ with inertia group T for $\tilde{L}/\tilde{E}$. Since $\tilde{L}/E$ is unramified at all prime divisors, $T \cap \bar{B} = 1$. The groups $\bar{B}$ and D have relatively prime orders so it follows that T is contained in D. This shows that $K/\tilde{E}$ is unramified at all prime divisors. Hence $K \subset H(\tilde{E})$ and so $p \mid h(\tilde{E})$ contradicting our hypothesis. Thus $\bar{B} = 0$ and we are done.//

COROLLARY 2.15 (*Rank*): *Suppose E/F is a cyclic extension of degree n. Let p be a prime which does not divide $h(\tilde{E})$ for any field $\tilde{E}$ with $F \subset \tilde{E} \subsetneq E$ and which does not divide n. If $p \mid h(E)$ then the p-rank of $C(E)$ is a multiple of f, the order of p* modulo n, and $p^f \mid h(E)$.

EXAMPLE 2.16: If a prime $p \neq 29$ divides $h'(59)$, then p^f where f is the smallest positive integer with $p^f \equiv 1 \bmod 29$ also divides $h'(59)$. Since $h'(59)$ is prime to 29 by the Pushing Down Theorem (2.7), we see that $h'(59) = 1$ or $h'(59) \geq 59$. However, $d'(59) < 51.27$ so (1.8) and the class number bound function value (Table 1 in the Appendix) $G(340) = 51.328$ shows that $h'(59) < 340/29$. Hence $h'(59) = 1$.

EXAMPLE 2.17: From the Odlyzko class number bound function, it is easy to see that $h(F(3,67)) \leq 4$ and $h(F(11,67)) \leq 13$. The Pushing Down Theorem eliminates 3 and 11 respectively from these class numbers. The Rank Corollary (2.15) shows that $h(F(3,67)) = 1$ or 4 and also shows that if $11 \neq p \leq 13$ divides $h(F(11,67))$ then so does a power $p^f > 13$. Hence $h(F(11,67)) = 1$. Applying the Rank Corollary now to C′(67) shows that if $p \neq 2$, 3, 11 and $p \mid h'(67)$ we must have $p^f \geq 199$ and p^f a factor of $h'(67)$. (We have used here the fact that $67 \nmid h'(67)$, [30].) Since the Pushing Down Theorem eliminates 3 and 11 from $h'(67)$, we see that $h'(67)$ is a power of 2 (possibly 2^0) or a power of 2 times a number greater than 198.

We have seen in (2.5) that $h(m) = h^*(m)h'(m)$ for a natural number $h^*(m)$ called the relative class number. When $m = p$ there is a classical closed formula for $h^*(p)$,

$$h^*(p) = 2p \prod_{\chi} (-2f(\chi))^{-1} \sum_{a=1}^{f(\chi)} a\chi(a) \tag{2.18}$$

where the product runs over all primitive, odd (i.e. $\chi(-1) = -1$) Dirichlet characters χ of conductor $f(\chi)$ dividing p. This formula was known to Kummer and he called this the formula for the first factor $h_1(p)$ of the cyclotomic class number of p-th roots of unity. By replacing p by m in our definition, one obtains Kummer's general formula for the first factor $h_1(m)$ of the cyclotomic class number of m-th roots of unity, $m \not\equiv 2 \bmod 4$, m odd. For m divisible by 4, the 2 outside the product should be dropped also. Correspondingly the second factor $h_2(m)$ was for Kummer the quotient $h(m)/h_1(m)$, When m is a prime power p^a, then $h_1(p^a) = h^*(p^a)$ and so $h_2(p^a)$ is the class number of $\mathbf{C}'(p^a)$. However, when more than one rational prime ramifies in $\mathbf{C}(m)$, $h^*(m) = 2h_1(m)$ and, thus, $h_2(m)$ is twice the class number of $\mathbf{C}'(\mathrm{m})$. Kummer, however, considered the second factor to be the class number of $\mathbf{C}'(m)$ because his class group was ideals modulo ideals generated by an element of positive norm. For Kummer and some others then the first factor of the cyclotomic class number is not necessarily an integer but only a half-integer. In this paper we use exclusively the relative class number which is an integer.

The first factor $h_1(p) = h^*(p)$ enabled Kummer to tell whether a prime was regular (i.e. $p \nmid h(p)$) or irregular ($p \mid h(p)$), because he proved that p divided $h_2(p) = h'(p)$ only if p divided $h^*(p)$. This generalizes as follows;

THEOREM 2.19 (*Kummer Criterion*): *Let F be a totally real algebraic number field and let p be an odd prime. Suppose that adjoining a p-th root of a root of unity in $F\mathbf{C}(p)$ to $F\mathbf{C}(p)$ never gives an unramified extension of $F\mathbf{C}(p)$ of degree p. Then p divides $h(F)$ implies that p divides the quotient $h(F\mathbf{C}(p))/h(F\mathbf{C}'(p))$.*

PROOF: Let $K = F\mathbf{C}(p)$ and $K' = F\mathbf{C}'(p)$. If $p \mid h(F)$, then the Pushing Up Corollary (2.2) shows that $p \mid h(K')$ since $p \nmid |K':F|$ and so K' has a cyclic, unramified (totally real) extension L of degree p. Since L and K are both abelian extensions of $L \cap K = K'$, we see that LK/K' is a cyclic extension of degree 2p. If s generates $\mathrm{Gal}(LK/K)$ and J is the automorphism of LK induced by complex conjugation, then $sJ = Js$ is a generator of $\mathrm{Gal}(LK/K')$.

As a Kummer extension of K, $LK = K(a^{1/p})$ for some non-zero $a \in K$ which is not the p-th power of an element in K. Let $\alpha = a^{1/p}$ be a fixed p-th root of a and let $(Ja)^{1/p} = J\alpha$. Now $s\alpha = \zeta_1\alpha$ and $s(J\alpha) =$

$\zeta_2 J\alpha$ where ζ_1, ζ_2 are primitive p-th roots of unity. But $\zeta_2 J\alpha = s(J\alpha) = J(s\alpha) = \zeta_1^{-1} J\alpha$ so $s(\alpha J\alpha) = (s\alpha)(sJ\alpha) = \alpha J\alpha$. It follows that $a(Ja)$ is a p-th power in K. Since $b = a/Ja = a^2/aJa$ we get $LK = K(\alpha) = K(\alpha^2) = K(b^{1/p})$. Furthermore the ideal (b) generated by b in K must be $\mathbf{b}^p$ for some fractional ideal $\mathbf{b}$ of K (since LK/K is unramified) with $J\mathbf{b} = \mathbf{b}^{-1}$ because $bJb = 1$. The ideal class of $\mathbf{b}$ then is in the kernel of $N: C(K) \longrightarrow C(K')$ so by (2.1) we will be done if we prove that $\mathbf{b}$ is not a principal ideal.

If we had $\mathbf{b} = (d)$ with $d \in K$, then $\mathbf{b}^{2p} = \mathbf{b}^p/(J\mathbf{b})^p = (d/Jd)^p = (u)^p$ where $u = d/Jd$. Then $(b^2) = (u^p)$ so $v = u^p/b^2 = (d^p/a^2)/J(d^p/a^2)$ is a unit of K, all of whose conjugates have absolute value one. But then the unramified extension LK/K is just $K(v^{1/p})/K$ with v a root of unity in K contrary to hypothesis.//

COROLLARY 2.20: *Let M be the least common multiple of m and the odd prime p. Then p divides h′(m) only if p divides h*(M).*

PROOF: When $M = m$, the result follows immediately since $h(m) = h(M) = h^*(M)h'(M)$ and (2.19) shows that $p \mid h^*(M)$. When $m = p$ this is the case of Kummer's original criterion.

When $p \nmid m$, $p \mid h'(M)$ whenever $p \mid h'(m)$ by (2.5). We may argue then as above.//

We remark that $h^*(p) \mid h^*(M)$ (see [21]) so an irregular prime can never be eliminated from $h'(m)$ via (2.20).

There is a result analogous to (2.20) for the case $p = 2$.

THEOREM 2.21 (*Parity check*): *Let E/F be a ramified quadratic extension of number fields with no capitulation, that is no non-principal ideal of F becomes principal in E. Then h(F) is even only if h(E)/h(F) is even. In particular, h′(m) is even only if h*(m) is even.*

PROOF: Suppose $c \in C(F)$, $c^2 = 1$, $c \neq 1$. By hypothesis $C(F)$ injects into $C(E)$ so we may consider $c \in C(E)$, $c \neq 1$. Now by (2.1) the norm map $N: C(E) \longrightarrow C(F)$ is surjective and since $Nc = c^2 = 1$ the kernel of N has even order equal to $h(E)/h(F)$. In particular, $\mathbf{C}(m)/\mathbf{C}'(m)$ is ramified at the infinite primes and by a theorem of Kronecker [12] no non-principal ideal of $\mathbf{C}'(m)$ becomes principal in $\mathbf{C}(m)$.//

THEOREM 2.22 (*Cyclotomic spiegelungsatz*): *Let p be any prime number and let M be the least common multiple of m and p. Then p divides h′(m) only if p divides h*(M).*

PROOF: Since $C(M) = C(m)$ when $p = 2$, this is just a restatement of (2.20) and (2.21).//

EXAMPLE 2.23: For conductors $f \leq 100$, $h^*(f)$ is even ([9], [29]) only for $f = 29, 39, 55, 56, 65, 68, 77, 87, 91$, and 95. Consequently $h'(f)$ is odd for all other conductors $f \leq 100$. In particular $h'(p^a)$ is odd for $p^a < 100$ since (1.8) can be used to show $h'(29) = 1$.

EXAMPLE 2.24: The relative class number $h^*(3p)$ is prime to 3 for $p = 71, 79, 89$, and 97 (see [29]). Hence $h'(p)$ is prime to 3 for $p = 71$, 79, 89, 97, and by (2.4) the class number of any real abelian number field with conductor 71, 79, 89, or 97 is also prime to 3.

Besides eliminating possible class number divisors one can sometimes also find class number divisors. For abelian number fields there is a generalization of the theory of genera for quadratic fields. For K an abelian extension of $\mathbf{Q}$, the genus field of K, $G(K)$, is the maximal subfield of $C(f(K))$ such that $G(K)/K$ is unramified at all finite primes. For K of prime power conductor then $G(K) = K$. In that case or for K of odd degree or for K non-real, $G(K)$ is the maximal subfield of $H(K)$ which is still abelian over $\mathbf{Q}$. In these cases then non-trivial factors of $|G(K){:}K|$ are also factors of $h(K) = |H(K){:}K|$. In the remaining cases we may have K totally real and $G(K)$ totally imaginary so $G(K)/K$ is ramified at infinite primes. However, the maximal real subfield $G'(K)$ of $G(K)$ is contained in $H(K)$ so $|G(K){:}K| = |G(K){:}G'(K)| \cdot |G'(K){:}K|$ divides $2h(K)$.

Unlike the quadratic field theory, however, only a lower bound on the p-rank of $C(K)$ for K a cyclic extension of degree p is possible via genus theory. For example, the genus field of an $F(3, 79.97)$ has degree 3 over that cubic field but the 3-rank of $C(F(3, 7663))$ is 2 for both of those cubic fields ([6]). Bauer [1] mentions that in each field K for which he successfully determined the class number there is only one class per genus. What is meant by this is that $G'(K)$ is the same as $H(K)$ for those K.

The genus field of an abelian extension K is easily determined via the Dirichlet characters attached to K. Since $K \subset C(f(K))$, $\mathrm{Gal}(K/\mathbf{Q})$ may be viewed as a factor group of $(\mathbf{Z}/f(K)\mathbf{Z})^\times$, the multiplicative group of units mod $f(K)$. The dual of $\mathrm{Gal}(K/Q)$ is then a subgroup H of the group of characters of $(\mathbf{Z}/f(K)\mathbf{Z})^\times$. The characters in H may then be identified with a subgroup of the Dirichlet characters modulo $f(K)$. A Dirichlet character χ_f mod f is a product of (not necessarily primitive) Dirichlet characters χ_{p^a} modulo p^a, $p^a \| f$, where we call χ_{p^a}

the p-primary component of χ_f. One also gets a product decomposition of χ_f by replacing each p-primary component by the Dirichlet character modulo f which it induces. Now we can characterize $G(K)$.

THEOREM 2.25: *Let K be the abelian number field of conductor f corresponding to the subgroup H of the group D of Dirichlet characters* modulo *f. Let G be the subgroup of D which is generated by all the characters of D which are induced from a p-primary component of any character in H. Then the abelian field $G(K)$ of conductor f corresponding to G is the genus field of K, the maximal abelian extension of K unramified at all finite primes which is still abelian over* $\mathbf{Q}$.

PROOF: The reader is referred to [13].//

EXAMPLE 2.26: Let $p_i \equiv 1 \bmod q$, $i = 1, 2$ where p_1, p_2, and q are distinct primes. Any of the $q-1$ fields $F(q, p_1p_2)$ corresponds to a cyclic group H generated by a Dirichlet character $\chi_{p_1}\chi_{p_2}$ of order q where each component χ_{p_i} is non-trivial. The group G generated by the q-power characters mod p_i, 1, 2 is a (q, q) group corresponding to the field $G(F(q,p_1p_2)) = F(q, p_1)F(q, p_2)$. In particular $q \mid h(F(q, p_1p_2))$ if $G(F(q, p_1p_2))$ is real.

REMARKS: The Pushing Down Theorem (2.7) and the Rank Theorem (2.15) are generalizations of results of Iwasawa [10], [11]. Fröhlich derived 2.7 in [5]. Our proof is more direct. Fröhlich also proves a type of Structure Theorem in [3]. The proof of Kummer's Criterion (2.19) is Greenberg's [7] though he states the result in a less general form.

3. The prime-power conductor case.

In this section we apply the results of the preceding sections to calculate the class numbers of most of the real cyclic number fields of prime power conductor less than 100. Our results are compiled in Table 2 which we explain below. The class number was one for all the fields for which we were able to make a complete computation. This is not the general case as, for example, $h'(257)$ is divisible (2.4) by the class number of $\mathbf{Q}(257^{1/2})$ which is 3.

Given any prime power p^a, $\mathbf{C}'(p^a)/\mathbf{Q}$ is cyclic so the degree of a real abelian field of conductor p^a determines a unique field. In Table 2 we list for each field its conductor, its degree, and its root-discriminant rounded up. If b is the value listed in the rd column for $F(n,f)$ then $b - .01 \leq rd(F(n,f)) < b$. We ignore quadratic fields since methods of determining their class numbers are well-known. The values of the class number bound function $G(x)$ in Table 1 are truncated, so to reproduce our work one should find the minimal x with $G(x) \geq b$ in order to apply the Class Number Bound Theorem (1.8). The bound we obtained using that theorem is listed in the column headed "$h \leq$". We used a more complete table of values of $G(x)$ so for a few fields the value in the "$h \leq$" column will be less than that obtained by using Table 1. A blank in the "$h \leq$" column indicates that (1.8) does not apply since the root-discriminant exceeds all values of $G(x)$.

In the column marked "elimination" we indicate how possible prime divisors of $h(K)$ are eliminated for the field K. We saw (2.23), for example, that $h'(p^a)$ is odd. We have indicated this by $2PC$ since the Parity Check Theorem (2.21) was used. From (2.4) we see that all proper subfields of $\mathrm{C}'(p^a)$, $p^a < 100$, also have odd class number since a 2 "pushes up" to $\mathrm{C}'(p^a)$. We use PU to denote that the Pushing Up Corollary (2.2) was used. Because $F \subset E \subset \mathrm{C}'(p^a)$ implies that E/F has a unique ramified prime, the Pushing Down Theorem (2.7) can often be used. This is indicated by PD. The use of the Rank Corollary (2.15) is indicated by R. We do not, however, indicate which auxiliary fields are used when a prime is eliminated via PU, PD, or R. We also remark that there may be more than one way to eliminate a prime. One other method used in this section is the generalized Kummer Criterion (2.19) or its corollaries for which we use the notation K (see (2.24)). For diagrams of the fields involved in our considerations the reader is referred to the tables at the end of [9].

Example 3.1: In example 2.17 we saw that $F(11, 67)$ had class number one and that $F(3, 67)$ had class number 1 or 4. However, 2 in $h(F(3, 67))$ pushes up to $h'(67)$ which violates the Parity Check Theorem. We also saw that 3 and 11 in $h'(67)$ can be eliminated via the Pushing Down Theorem. From the Odlyzko Bound Theorem $h'(67) \leq 136$ and 67 is the only prime power less than 137 which is congruent to 1 mod 33. Since $67 \nmid h'(67)$, the Rank Corollary now shows that $h'(67) = 1$.

Our results give the following:

Theorem 3.2: *Any real abelian number field of prime power conductor less than* 70 *has class number one.*

We conjecture that 70 may be replaced by 100. If this conjecture is false, then we would have a zero of the Dedekind zeta function of a number field whose real part would be greater than $\frac{1}{2}$. This would occur because Odlyzko has produced a class number bound function $g(x)$ with lim $g(x) = 185+$as x goes to infinity by assuming that Dedekind zeta functions of totally real fields have no zeroes $\beta + i\gamma$ in a bounded region contained in $\frac{1}{2} < \beta < 1$. Using our techniques we can use this improved but conditional class number bound function to replace 70 by 100 in theorem 3.2.

A blank in the "$h =$" column of Table 2 indicates that Bauer [1] computed h, but we know of no independent verification. A question mark indicates that we are unaware of any computation of h. We need to refer to [8] to eliminate 5 for the fields $F(4, 89)$ and $F(4, 97)$.

4. The non-prime-power conductor case.

In this section we show how to calculate the class numbers of most of the real cyclic number fields whose conductor is not a prime power and does not exceed 100. Our results are compiled in Table 3. Table 3 is very similar to Table 2. In this case, however, there may be more than one field with a given degree and conductor. In some cases, the root-discriminants can distinguish the fields. When this is not the case, there is a double entry to indicate that there are two fields with the same conductor, degree, and root-discriminant. Although such fields can have different class numbers (for example, the two $F(3, 79 \cdot 97)$'s, see [6]), this does not occur for conductors less than 100 except possibly for $F(12, 91)$.

Another difference is the presence of genus factors. As we remarked in section 2, we must have $G(K) = K$ for $f(K) = p^a$. This is no longer the case when $f(K)$ is not a prime power. Hence the column between "$h \leq$" and "$h =$" is headed "divisors". A G indicates that the divisor is present from $|G'(K){:}K|$ (see 2.21). In all other cases a reason is indicated why a possible prime divisor of the class number h is eliminated. The notation is the same as in Table 2 with the addition of F to denote that Frøhlich's results were used (see 2.10–2.13).

The genus factors are always taken into account first. For example, knowing that $h(F(3, 91)) \leq 6$ does not allow us to eliminate 2 by the Rank Theorem. However, since $3 \mid h(F(3, 91))$ by (2.26), $4 \nmid h(F(3, 91))$. The following result was also used.

PROPOSITION 4.1: *Let E/F be an extension of number fields with*

$F \subset E \subset H(F)$ and $h(E)$ prime to p. Then $h(F)$ and $|E{:}F|$ are divisible by the same powers of p.

PROOF: Apply 2.2.//

EXAMPLE 4.2: Since $h^*(85) = 6205$, the Parity Check Theorem shows that $\mathrm{C}'(85)$ has odd class number. The extension $\mathrm{C}'(85)/\mathrm{C}'(5)F(4, 85)$ is totally ramified so by the Pushing Up Corollary the fields $\mathrm{C}'(5)F(4, 85)$ and $\mathrm{C}'(5)\mathrm{C}'(17)$ also have odd class number. Proposition 4.1 now shows that the class numbers of $F(16, 85)$ (both fields), $F(8, 85)$, and $F(4, 85)$ are divisible by 2 but not by 4.

EXAMPLE 4.3: We have $rd'(80) < 26.75$ so by (1.8) $h'(80) = 1$. By (2.2) then the maximal real subfields of the genus fields for all the $F(4, 80)$'s have class number one and so $4 \nmid h(F(4, 80))$.

EXAMPLE 4.4: The maximal real 2-extension of $\mathrm{C}(65)$ is $G'(F(4, 65))$. Its class number is odd by Example (2.13). The Rank Theorem applied to $\mathrm{C}'(65)/G'(F(4, 65))$ shows that $4 \mid h'(65)$ if $h'(65)$ is even. However, (1.8) yields that $h'(65) \leq 2$ so $h'(65) = 1$. Now $\mathrm{C}'(65) = G'(F(12, 65))$ so the class numbers of the two $F(12, 65)$'s and the two $F(4, 65)$'s are all twice an odd number. Since they are all less than 6 by (1.8), they are all equal to 2.

We summarize our results.

THEOREM 4.5: *Let K be a real, cyclic number field whose conductor does not exceed* 100 *and is not a prime power. Then $G'(K)$, the maximal real subfield of the genus field of K is the Hilbert class field of K except possibly for the following: the twelfth degree extensions of conductor* 91 *with root-discriminants greater than* 30, *the extensions of conductor* 95 *whose degrees are* 12 *and* 36.

Acknowledgements

The author wishes to thank Drs. Fröhlich, Greenberg, Iwasawa, Kisilevsky, Lenstra, and Odlyzko for their assistance, the Institute for Advanced Study for its hospitality, and the National Science Foundation for its support. Many helpful suggestions of the referee are also gratefully acknowledged.

Appendix

TABLE 1: Lower bounds for root-discriminants of totally real number fields of degree x ([26])

X	$G(x)$	x	$G(x)$	x	$G(x)$
		92	40.871	960	55.837
8	10.568	96	41.312	1000	55.966
9	11.787	100	41.728	1170	56.430
10	12.941	110	42.678	1183	56.461
11	14.034	120	43.513	1200	56.500
12	15.068	130	44.256	1332	56.780
14	16.971	140	44.921	1656	57.308
15	17.849	144	45.169	1800	57.493
16	18.684	150	45.522	2000	57.713
18	20.234	153	45.691	2200	57.899
20	21.642	154	45.746	2400	58.061
21	22.299	156	45.855	2800	58.324
22	22.929	160	46.067	3200	58.533
24	24.109	162	46.170	3600	58.704
27	25.709	165	46.322	4000	58.846
28	26.203	170	46.565	4500	58.993
30	27.138	180	47.021	4800	59.069
32	28.008	190	47.444	6000	59.310
35	29.208	192	47.524	7200	59.483
36	29.582	200	47.833	8100	59.584
40	30.971	208	48.124	9600	59.716
42	31.607	210	48.195	10000	59.746
44	32.209	220	48.530	31970	60.332
45	32.497	240	49.142		
46	32.778	260	49.680		
48	33.319	280	50.156		
50	33.832	300	50.588		
52	34.322	320	50.977		
54	34.789	324	51.051		
56	35.233	336	51.261		
60	36.067	340	51.328		
63	36.649	348	51.458		
64	36.834	360	51.652		
66	37.195	380	51.947		
69	37.708	400	52.221		
70	37.875	480	53.130		
72	38.197	492	53.246		
76	38.806	510	53.409		
77	38.951	576	53.952		
78	39.093	600	54.122		
80	39.373	696	54.717		
84	39.903	720	54.842		
88	40.402	750	54.997		
90	40.641	800	55.229		
91	40.757	840	55.396		

Any totally real field of degree greater than or equal to x has root-discriminant greater than or equal to $G(x)$.

TABLE 2: Real cyclic fields of prime power conductor < 100

f	n	rd	$h\leqslant$	Elimination	$h=$
8	2				1
16	4	6.73	1		1
32	8	14.68	1		1
64	16	30.65	2	$2PC$	1
9	3	4.33	1		1
27	9	14.67	1		1
81	27	45.83	5	$2PC/3PD/5R$	1
5	2				1
25	5	13.14	2	$2PU$	1
25	10	15.43	1		1
7	3	3.66	1		1
49	7	28.11	4	$2, 3PU$	1
49	21	33.83	2	$2PC$	1
11	5	6.81	1		1
13	2				1
13	3	5.53	1		1
13	6	8.48	1		1
17	2				1
17	4	8.38	1		1
17	8	11.94	1		1
19	3	7.13	1		1
19	9	13.70	1		1
23	11	17.30	1		1
29	2				1
29	7	17.93	2	$2PU$	1
29	14	22.81	1		1
31	3	9.87	2	$2PU$	1
31	5	15.60	2	$2PU$	1
31	15	24.66	1		1
37	2				1
37	3	11.11	2	$2PU$	1
37	6	20.27	3	$2, 3PU$	1
37	9	24.78	2	$2PU$	1
37	18	30.28	2	$2PC$	1
41	2				1
41	4	16.21	3	$2, 3PU$	1
41	5	19.51	3	$2, 3PU$	1
41	10	28.29	3	$2, 3PU$	1
41	20	34.06	2	$2PC$	1
43	3	12.28	3	$2, 3PU$	1
43	7	25.13	3	$2,3PU$	1
43	21	35.95	2	2PC	1
47	23	39.76	3	$2, 3R$	1
53	2				1
53	13	39.06	5	$2, 3, 5R$	1
53	26	45.50	5	$2, 3, 5R$	1
59	29	51.27	11	$2, 3, 5, 7, 11R$	1
61	2				1
61	3	15.50	4	$2PU/3PD$	1

TABLE 2: (continued)

f	n	rd	$h \leq$	Elimination	$h=$
61	5	26.81	5	2, 3R/5PD	1
61	6	30.75	6	2, 3PD/5R	1
61	10	40.44	8	2, 5PD/3, 7R	1
61	15	46.38	11	3, 5PD/2, 7, 11R	1
61	30	53.19	16	2PC/3, 5PD/7, 11, 13R	1
67	3	16.50	4	2PU/3PD	1
67	11	45.72	13	2PU/3, 5, 7, 13R/11PD	1
67	33	58.99	136	SEE (3.1)	1
71	5	30.27	7	2, 3, 7R/5PD	1
71	7	38.62	10	2PU/3, 5R/7PD	1
71	35	62.86		2PC/3K	?
73	2				1
73	3	17.47	4	2PU/3PD [8]	1
73	4	24.98	6	2PU/3R	1
73	6	35.71	9	2, 3PU/5R/	
73	9	45.32	16	2, 3PU/5, 7, 11, 13R	1
73	12	51.06	27	2,3PU	?
73	18	57.52	105	2, 3PU	?
73	36	64.80		2PC, 3PD	?
79	3	18.42	5	2PU/3PD/5R	1
79	13	56.45	90	2, 3PU	?
79	39	70.63		2PC, 3K	?
83	41	74.52		2PC	?
89	2				1
89	4	28.98	8	2PD/3, 7R/	1[8]
89	11	59.18	481	2, 3PU	?
89	22	72.58		2, 3PU	?
89	44	80.37		2PC/3K	?
97	2				1
97	3	21.12	6	2PU/3PD/5R	1
97	4	30.91	9	2, 3PU/7R/	1[8]
97	6	45.26	24	2, 3PU/5, 11, 17, 23R/	
97	8	54.76	87	2, 3PU/	
97	12	66.26		2, 3PU	?
97	16	72.88		2, 3PU/	?
97	24	80.17		2, 3PU/	?
97	48	88.19		2PC, 3K	?

f = conductor, n = degree, rd = root-discriminant, $h \leq$ = upper bound for class number using (1.8), $h =$ = the class number if computed; See section 3 for explanation of Elimination.

TABLE 3: Real cyclic fields of conductor ≤ 100 with more than one ramified prime

f	*n*	*rd*	*h*≤	Divisors	*h*=
12	2				1
15	4	5.80	1		1
20	4	6.69	1		1
21	2				1
21	6	8.77	1		1
24	2				1
28	2				1
28	6	10.13	1		1
33	2				1
33	10	15.00	1		1
35	4	8.85	1		1
35	6	8.19	1		1
35	12	16.93	1		1
36	6	10.40	1		1
39	4	11.86	2	2*PU*	1
39	12	18.19	1		1
40	2				2
40	4	9.46	1		1
44	2				1
44	10	17.31	1		1
45	6	9.68	1		1
45	12	17.38	1		1
48	4	11.66	2	2*PU*	1
51	16	24.67	1		1
52	4	13.70	2	2*PU*	1
52	12	21.00	1		1
55	4	11.09	2	2*PU*	1
55	10	15.23	1		1
55	20	28.94	1		1
56	2				1
56	6	10.36	1		1
56	6	14.32	1		1
57	2				1
57	6	20.15	2	2*PU*	1
57	18	27.95	1		1
60	2				2
63	3	15.84	4	3*G*	3
63	3	15.84	4	3*G*	3
63	6	13.75	1		1
63	6	26.30	4	3*G*	3
63	6	26.30	4	3*G*	3
65	2				2
65	4	22.90	5	2*G/SEE*(4.4)	2
65	4	22.90	5	2*G/SEE*(4.4)	2
65	6	12.37	1		1
65	6	18.96	2	2*G*	2
65	12	35.10	4	2*G/SEE*(4.4)	2
65	12	35.10	4	2*G/SEE*(4.4)	2
68	16	28.49	2	2*F*	1

TABLE 3 (*continued*)

f	*n*	*rd*	*h*≤	Divisors	*h*=
69	2				1
69	22	34.55	2	2*R*	1
72	6	12.24	1		1
72	6	14.70	1		1
75	20	28.96	1		1
76	2				1
76	6	23.27	3	2*R*/3*PD*	1
76	18	32.27	2	2*PC*	1
77	2				1
77	6	16.79	2	2*R*	1
77	10	22.90	2	2*R*	1
77	15	24.92	1		1
77	30	43.81	4	2*PC*/3*R*	1
80	4	15.05	2	2*G*	2
80	4	22.50	5	2*G*/*SEE*(4.3)	2
80	4	22.50	5	2*G*/*SEE*(4.3)	2
84	6	12.68	1		1
85	2				2
85	4	18.73	4	2*G*/*SEE*(4.2)	2
85	8	26.68	3	2*G*	2
85	16	47.62	12	2*G*/3, 5*R*/*SEE*(4.2)	2
85	16	47.62	12	2*G*/3,5*R*/*SEE*(4.2)	2
87	4	21.65	5	2*F*/3*R*/5*PU*	1
87	28	44.54	4	2, 3*R*	1
88	2				1
88	10	19.27	1		1
88	10	24.48	2	2*R*	1
91	3	20.24	6	3*G*/2*R*	3
91	3	20.24	6	3*G*/2*R*	3
91	4	18.12	3	2*F*/3*R*	1
91	6	13.20	1		1
91	6	31.03	6	3*G*/2*R*	3
91	6	31.03	6	3*G*/2*R*	3
91	12	27.78	2	2*R*	1
91	12	34.66	4	3*R*/	
91	12	53.14	40	3*G*/5, 7, 11*R*/	?
91	12	53.14	40	3*G*/5, 7, 11*R*/	?
92	2				1
92	22	39.89	3	2*PC*/3*R*	1
93	2				1
93	6	30.30	6	2*PU*/3*PD*/5*R*	1
93	10	38.09	7	2, 3, 7*R*/5*PD*	1
93	30	47.89	6	2*PC*/3, 5*PD*	1
95	4	14.58	2	2*F*	1
95	6	15.93	2	2*R*	1
95	12	38.90	6	3, 5*R*/	
95	18	30.64	2	2*R*	1

TABLE 3 (*continued*)

f	n	rd	$h \leq$	Divisors	$h =$
95	36	53.95	15	$5, 7, 11, 13R/$	?
96	8	25.42	3	$2PU/3R$	1
99	6	17.24	2	$2R$	1
99	15	29.47	2	$2R$	1
99	30	44.98	4	$2, 3R$	1
100	20	33.44	2	$2PC$	1

See Table 2 and section 4 for an explanation of the table.

REFERENCES

[1] H. BAUER: Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper. *J. of Number Theory* 1 (1969) 161–162.

[2] H. BAUER: Die 2-Klassenzahlen spezieller quadratischer Zahlkörper, *J. Reine Angew. Math.* 252 (1972), 79–81.

[3] A. FRÖHLICH: On the class group of relatively Abelian fields. *Quart. J. Math. Oxford Ser.* (2) 3 (1952) 98–106.

[4] A. FRÖHLICH: On the absolute class-group of Abelian fields II. *J. London Math. Soc.* 30 (1955) 72–80.

[5] A. FRÖHLICH: On a method for the determination of class number factors in number fields. *Mathematika* 4 (1957) 113–121.

[6] M. GRAS: Methodes et algorithmes pour le calcul numerique du nombre de classes et des unités des extensions cubiques cycliques de **Q**. *J. Reine Angew. Math.* 277 (1975), 89–116.

[7] R. GREENBERG: A generalization of Kummer's criterion. *Inventiones math.* 21 (1973) 247–254.

[8] H. HASSE: Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. *Abh. Deutsche Akad. Wiss.* 1948, Nr. 2 (1950).

[9] H. HASSE: *Über die Klassenzahl abelscher Zahlkörper.* Akademie Verlag, 1952.

[10] K. IWASAWA: A note on class numbers of algebraic number fields. *Abh. Math. Sem. Univ. Hamburg* 20 (1956) 257–258.

[11] K.IWASAWA: A note on ideal class groups. *Nagoya Math. J.* 27 (1966) 239–247.

[12] L. KRONECKER: Bemerkung über die Klassenanzahl der aus Einheitswurzeln gebildeten komplexen Zahlen. *Monatsber. Akad. d. Wiss.* Berlin 1863 = Werke 1, 123–131.

[13] H. LEOPOLDT: Zur Geschlechtertheorie in abelschen Zahlkörpern. *Math. Nachr.* 9(1953) 351–362.

[14] H. LEOPOLDT: Uber Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper. *Abh. Deutsche Akad. Wiss. Berlin Kl. Math. Nat.* 1953, Nr. 2 (1954).

[15] H. LEOPOLDT: Zür Struktur der l-Klassengruppe galoisscher Zahlkörper. *J. Reine Angew. Math.* 199 (1958) 165–174.

[16] H. LEOPOLDT: Über Klassenzahlprimteiler reeller abelscher Zahlkörper als Primteiler verallgemeinerter Bernoullischer Zahlen. *Abh. Math. Sem. Univ. Hamburg* 23 (1959) 36–47.

[17] H. Leopoldt: Über Fermatquotienten von Kreiseinheiten und Klassenzahlformeln modulo p. *Rend. Circ. Mat. Palermo* (2) 9 (1960) 39–50.

[18] J. Masley: *On the class number of cyclotomic fields.* Dissertation, Princeton Univ. 1972.

[19] J. Masley: Solution of the class number two problem for cyclotomic fields. *Inventiones math.* 28 (1975) 243–244.

[20] J. Masley:Solution of small class number problems for cyclotomic fields. *Compositio Math.* 33 (1976) 179–186.

[21] J. Masley and H.L. Montgomery: Unique factorization in cyclotomic fields. *J. Reine Angew. Math.* 286/287 (1976) 248–256.

[22] J. Masley: Odlyzko bounds and class number problems, *Algebraic Number fields* (edited by A. Fröhlich) Academic Press 1977, 465–474.

[23] A. Odlyzko: Some analytic estimates of class numbers and discriminants. *Inventiones Math.* 29 (1975) 275–286.

[24] A. Odlyzko: Lower bounds for discriminants of number fields. *Acta Arith.* 29 (1976) 275–297.

[25] A. Odlyzko: Lower bounds for discriminants of number fields II, *Tohoku Math. J.* 29 (1977) 209–216.

[26] A. Odlyzko: Unconditional lower bounds for discriminants of number fields (unpublished preprint, November 1976).

[27] G. Poitou: Minorations de discriminants (d'apres A.M. Odlyzko). *Sem Bourbaki,* Fev. 1976, no. 479.

[28] P. Ribenboim: *Algebraic Numbers.* Wiley-Interscience 1972, p. 218.

[29] G. Schrutka v. Rechtenstamm: Tabelle der (relativ-) Klassenzahlen von Kreiskorper. *Abh. Deutsche Akad. Wiss. Berlin,* 1964 Math Nat. Kl. Nr. 2.

[30] H.S. Vandiver: The relation of some data obtained from rapid computing machines to the theory of cyclotomic fields, *Proc. Nat. Acad. Sci.* 40 (1954), 474–480.

[31] J. Martinet: Tours de corps de classes et estimations de discriminants, Inventiones math. (to appear).

(Oblatum 7-IV-1977 & 12-VII-1977)

Mathematics Department
University of Illinois at
Chicago Circle
Box 4348
Chicago, IL 60680
USA