COMPOSITIO MATHEMATICA

JOHN MYRON MASLEY

Solution of small class number problems for cyclotomic fields

Compositio Mathematica, tome 33, n° 2 (1976), p. 179-186

<http://www.numdam.org/item?id=CM_1976__33_2_179_0>

COMPOSITIO MATHEMATICA, Vol. 33, Fasc. 2, 1976, pag. 179–186
Noordhoff International Publishing
Printed in the Netherlands

SOLUTION OF SMALL CLASS NUMBER PROBLEMS FOR CYCLOTOMIC FIELDS

John Myron Masley

By an algebraic number field F we shall mean a finite extension of $\mathbb{Q}$, the field of rational numbers. The class number h_F of F is the order of C_F, the group of ideal classes of F. In previous work ([5], [6], [7]) we have determined all F of the form $F = \mathbb{C}_m = \mathbb{Q}(\exp 2\pi i/m)$ such that $h_m = h_{\mathbb{C}_m} \leq 2$. In this paper we extend our results and give a complete list of cyclotomic fields whose class number is less than 11. Since for m an odd integer we have $\mathbb{C}_m = \mathbb{C}_{2m}$, we assume throughout this paper that $m \not\equiv 2 \bmod 4$ and our result is

MAIN THEOREM: *Let m be an integer greater than 2, $m \not\equiv 2 \bmod 4$. Then all the values of m for which the cyclotomic field $\mathbb{C}_m$ has class number h_m with $2 \leq h_m \leq 10$ are listed in the table:*

h_m	2	3	4	5	6	7	8	9	10
m	39	23	120	51	*none*	63	29	31	55
	56	52		80			68	57	
		72						96	

Furthermore, all the other values of m with $\varphi(m) = |\mathbb{C}_m : \mathbb{Q}| \leq 24$ give the twenty-nine values of m for which $h_m = 1$.

In §1 we use group actions on the ideal class group to prove a general lemma which is of interest in itself. Essentially it says that for non-cyclic abelian extensions L/K all the possible prime divisors of h_L can be found by looking at $|L:K|$ and the class numbers of proper subfields of L. In §2 we show how the problem of finding all m with

$h_m \leq 10$ is reduced to a finite amount of calculation. In §3 we indicate an easy way to carry out that computation. Here the lemma of §1 proves useful.

1. The (p, p)-lemma

In the sequel we shall refer to the following lemma as the (p, p)-lemma.

LEMMA 1: *Let p and q be distinct primes and let L/K be a Galois extension of type (p, p). Then q divides h_L if and only if q divides the class number of at least one of the proper intermediate fields between K and L.*

PROOF: Let G_0 be the Galois group of L/K and let $G_1, \ldots, G_{p+1}$ be the distinct subgroups of G_0 which have order p. Denote the fixed field of G_i by K_i (so $K = K_0$), put $C_i = C_{K_i}$, and let S_i be the q-Sylow Subgroup of C_i, $0 \leq i \leq p+1$. Let S be the q-Sylow subgroup of C_L.

Now if $L \supset E \supset K_i$ with $|E : K_i| = p$, then $q | h_E$ whenever $q | h_{K_i}$. One sees this as follows. A non-trivial ideal class c of order q in S_i may be viewed as an element of C_E by extending any ideal representative $\mathfrak{a}$ of c to an ideal $\mathfrak{A}$ of E in the natural manner. Suppose c is trivial in C_E, i.e. $\mathfrak{A}$ is a principal ideal of E. Applying the norm map shows that $\mathfrak{a}^p$ is principal and hence $c^p = 1$ in S_i, a q-group. This contradicts the non-triviality of c. Thus, $q | h_{K_i}$ implies a non-trivial class c exists in S_i and this class extends to a non-trivial class of C_E whence $q | h_E$. This proves the "if" part of the lemma. Moreover, it shows that $q | h_{K_i}$, $1 \leq i \leq p+1$ whenever $q | h_K$ so we may assume for the "only if" part of the lemma that $q \nmid h_K$.

The group G_0 operates on S and since every element of S has a unique p-th root we may extend the action of G_0 on S to an action of $R = (\mathbb{Z}[G_0])[p^{-1}]$ on S where $\mathbb{Z}$ denotes the ring of rational integers. We denote this action exponentially so that for $r \in R$, $s \in S$, s^r is the result of the action of r on s.

We now decompose $1 \in R$ into a sum of orthogonal idempotents and use the resulting decomposition of S to achieve our result. For a subgroup H of G_0 let $H^+ \in R$ be the sum of the elements of H and put $d_i^+ = p^{-1} G_i^+$, $d_i = 1 - d_i^+$ for $1 \leq i \leq p+1$. Let $e_0 = p^{-2} G_0^+$ and $e_i = d_1 \cdots d_{i-1} d_i^+ d_{i+1} \cdots d_{p+1} = d_i^+ - e_0$, $1 \leq i \leq p+1$. Then $1 = e_0 + \cdots + e_{p+1}$ and $e_i e_j = \delta_{ij} e_i$ for $0 \leq i, j \leq p+1$ where δ_{ij} is the Kronecker delta.

Define $S^{e_i} = \{s^{e_i} | s \in S\}$ for $0 \le i \le p+1$. Then $S^{e_i} = \{s \in S | s^{e_i} = s\}$ and since $S^{e_0} = 1$ (we assumed $q \not| h_K$), $S = S^{e_1} \times \cdots \times S^{e_{p+1}}$, an internal direct product. We claim the norm map N_i from S to S_i induces an embedding of S^{e_i} into S_i for $1 \le i \le p+1$. To see this, note that $N_i(s) = 1 \in S_i$ for $s \in S^{e_i}$ implies $s^p = s^{e_i p} = s^{pd_i^+ - pe_0} = s^{G_i^+} = 1 \in S^{e_i}$, a q-group. Consequently, $q | h_L$ implies that S and hence at least one S^{e_j} is non-trivial so that via the embedding of S^{e_j} into S_j we see that $q | h_{K_j}$.

2. The relative class number

Let $\mathbb{C}_m^+$ be the maximal real subfield of $\mathbb{C}_m$ and put $h_m^+ = h_{\mathbb{C}_m^+}$. Then $h_m^+ | h_m$ so $h_m = h_m^* h_m^+$ where the positive integer h_m^* is called the relative class number of $\mathbb{C}_m$. In this section we will determine all m with $h_m^* \le 10$. We shall call such a value of m admissible. We obtain a finite list of admissible m so that to determine when $h_m \le 10$ we need only to find h_m^+ for each admissible value of m. In the next section we will see that $h_m^+ = 1$ whenever $h_m^* \le 10$.

We require a formula for h_m^* which may be described as follows (cf. [3], pp. 78–79). Let Δ be the group of Dirichlet characters modulo m. For each cyclic subgroup of Δ choose a generator χ, let $\psi \pmod{f_\psi}$ be the primitive character which induces χ (so that f_ψ is the conductor of both χ and ψ), and let n_ψ be the order of ψ. Denote by $\Psi = \Psi(m)$ the set of such ψ with $\psi(-1) = -1$. Let N_ψ be the norm map $N_\psi : \mathbb{C}_{n_\psi} \to \mathbb{Q}$ and put $\Theta_\psi = -(2f_\psi)^{-1} \sum_{a=1}^{f_\psi} a\psi(a)$. Then

$$h_m^* = Qw \prod_{\psi \in \Psi(m)} N_\psi(\Theta_\psi) \tag{2.1}$$

where $Q = 1$ if m is a prime power and $Q = 2$ otherwise, and w is the number of distinct roots of unity in $\mathbb{C}_m$. We use the following properties of the $N_\psi(\Theta_\psi)$.

LEMMA 2: *Let ψ be a primitive Dirichlet character* mod f_ψ *with $\psi(-1) = -1$ and let n_ψ be the order of ψ.*

(A) *If f_ψ is divisible by more than one prime, then $N_\psi(\Theta_\psi) \in \mathbb{Z}$.*

(B) *Suppose n_ψ is a power of 2.*

(i) *If at least three distinct primes divide f_ψ, then $N_\psi(\Theta_\psi) \in 2\mathbb{Z}$.*

(ii) *If exactly two primes $p > q$ divide f_ψ, then $N_\psi(\Theta_\psi)$ is an even or an odd integer according as the quadratic residue symbol $\left(\frac{q}{p}\right) = 1$ or -1.*

(C) *If $f_\psi = p^\alpha$ for p a prime, then $N_\psi(\Theta_\psi) \in (2p)^{-1}\mathbb{Z}$ and, more precisely, the absolute value of the denominator (in lowest terms)*

(i) *may be divisible by* p *for* p *odd and* $n_\psi = \varphi(p^\alpha)$.
(ii) *is divisible by* 2 *if* p *is odd and* $n_\psi = 2^u$ *(since* $\psi(-1) = -1$, *this occurs only for* $2^u \| p-1$).
(iii) *is* 4 *for* $f_\psi = 4$ *and is* 2 *for* $f_\psi = 2^\alpha$, $\alpha \geq 3$.
(iv) *is* 1, *i.e.* $N_\psi(\Theta_\psi) \in \mathbb{Z}$, *in all other cases.*

PROOF: This is the content of Sätze 30–33 in [3].

From the properties of the $N_\psi(\Theta_\psi)$ recorded in Lemma 2 we have proved in [7], Lemma 5 that

LEMMA 3: *If* $m|n$, *then* $h_m^*|h_n^*$.

By virtue of Lemma 3 we limit the admissible values of m to those m whose prime power factors are admissible. That there are only finitely many admissible m follows then from

LEMMA 4: *If* $p^\alpha > 32$ *for a prime* p, *then* $h_{p^\alpha}^* > 10$.

PROOF: It is known ([7], Cor. 1) that $h_p^* > 10^{20}$ for $p > 131$. Now the numbers h_p^*, $3 \leq p < 200$ have been calculated independently by Schrutka [10] and M. Newman [9] and one sees then that the prime p is admissible if and only if $p < 32$. With regard to prime powers one knows ([8]) that $h_{p^\alpha}^* > e^3 h_{p^{\alpha-1}}^*$ for $\alpha \geq 2$ and $p^\alpha > 100$. Hence, $h_{p^\alpha}^* > e^3 > 10$ for $p^\alpha = 5^3, 11^2, 13^2, 17^2, 19^2, 23^2, 29^2, 31^2$. We have ([3] or [10]) $h_{p^\alpha}^* > 10$ for $p^\alpha = 2^6, 3^4, 7^2$ so by Lemma 3 we are done.

The following two lemmas are useful for showing that values of m are inadmissible.

LEMMA 5: *If* $p \neq q$ *are odd primes, then* $h_{pq}^*/(h_p^* h_q^*) = \Pi_{\psi \in \Psi(pq)} f_\psi = pq N_\psi(\Theta_\psi) \in \mathbb{Z}$. *In particular, if there exists* $\psi \in \Psi(pq)$ *of conductor* pq *with* $N_\psi(\Theta_\psi) > 10/(h_p^* h_q^*)$ *then* pq *is inadmissible.*

PROOF: Use (2.1) for $m = p$, q, and pq to get the expression for $h_{pq}^*/(h_p^* h_q^*)$ as a product of norms. Lemma 2A says that each norm in the product $\in \mathbb{Z}$.

LEMMA 6: *If* p *and* q *are odd primes,* $p \not\equiv q \bmod 4$, *then for* $K = \mathbb{Q}((-pq)^{1/2})$ *we have* $h_K h_p^* h_q^* | 2h_{pq}^*$.

PROOF: Use Lemma 5, Lemma 2A, and the fact that the quadratic character ψ mod pq satisfies $h_K = 2N_\psi(\Theta_\psi)$.

It is now easy to find all admissible m. The result is as follows:

PROPOSITION 1: *Let* $m \not\equiv 2 \bmod 4$ *be an integer greater than* 1. *Then the relative class number* h_m^* *of the cyclotomic field* $\mathbb{C}_m$ *is less than* 11 *precisely for* $m = 51, 55, 57, 63, 68, 80, 96, 120$ *and all* m *with* $|\mathbb{C}_m : \mathbb{Q}| = \varphi(m) < 32$.

REMARK: A more exact breakdown of this list is provided in the statement of the Main Theorem because we shall show in the next section that $h_m^+ = 1$ and hence $h_m^* = h_m$ for all admissible m.

PROOF of Proposition 1: An admissible $m = p_1^{q_1} \cdots p_t^{q_t}$ with $p_1, \ldots, p_t$ distinct primes must have $p_i^{q_i} \leq 32$ for $1 \leq i \leq t$ by Lemmas 3 and 4. We use Lemmas 2, 5, and 6 to cut down the possibilities even further. For example, $h_{221}^* = h_{221}^*/(h_{13}^* h_{17}^*)$ is a product of the integers $N_\psi(\Theta_\psi)$ with $\psi \in \Psi(221)$, $f_\psi = 221$ (cf. Lemma 5). There are six such ψ with n_ψ a power of 2 so by Lemma 2B(ii) we have $2^6 | h_{221}^*$, and, by Lemma 3, $2^6 | h_{13 \cdot 17 \cdot k}^*$ for any positive integer k. Lemma 3 also shows that $h_{23}^* h_{29}^* = 24$ divides $h_{23 \cdot 29 \cdot k}^*$.

The values of h_m^* for $\varphi(m) \leq 256$ which are given in the tables of Schrutka [10] show that most values of m are inadmissible. For example, $h_{75}^* = h_{132}^* = 11$ so $m = 3 \cdot 5^2 \cdot k$ and $m = 3 \cdot 4 \cdot 11 \cdot k$, k any positive integer, are inadmissible. For values not covered in available tables one can check that m is inadmissible by computing enough $N_\psi(\Theta_\psi)$-type factors, $\psi \in \Psi(m)$ keeping Lemma 2 in mind. A remarkably simple scheme for computing $N_\psi(\Theta_\psi)$ when more than one prime divides f_ψ is given in §§28,33 of [3]. We used these methods and Lemma 5 to show that $m = 31 \cdot 19$, $31 \cdot 13$, $31 \cdot 11$, $29 \cdot 17$, $29 \cdot 13$, $19 \cdot 17$ and their multiples are inadmissible. We used Lemma 6 to see that $m = 31 \cdot 29$, $31 \cdot 17$, $29 \cdot 19$, $29 \cdot 11$, $23 \cdot 17$, $23 \cdot 13$ and their multiples are inadmissible. From all these considerations the only m with $h_m^* \leq 10$ are found to be the 44 values mentioned in the proposition and the Main Theorem.

3. Class numbers of maximal real subfields

In this section we show that $h_m^+ = 1$ whenever $h_m^* < 11$. Hence, the admissible m determined in §2 all give cyclotomic fields with class

numbers < 11 and these are all the full cyclotomic fields with such low class numbers.

We have already shown ([5], [6], [7]) that $h_m^+ = 1$ when $h_m^* \leq 2$. The m with $3 \leq h_m^* \leq 10$ are $m = 23, 29, 31, 51, 52, 55, 57, 63, 68, 72, 80, 96$, and 120. For $m = 23, 29, 31, 51, 52, 55, 57$, and 68 we have $\mathbb{C}_m^+$ cyclic over $\mathbb{Q}$ and then $h_m^+ = 1$ from computations of Bauer [1]. For $m = 63$, 72, 80, 96, and 120 we will use other methods to determine h_m^+. We will need

LEMMA 7: *Let L/K be a cyclic extension with $|L:K| = p^\alpha$ for p a prime. Suppose only one prime divisor of K ramifies in L. Then $p|h_L$ only if $p|h_K$.*

PROOF: This lemma was first proved by Iwasawa [4]. The result is true under the weaker assumption that L/K is a p-extension (cf. Yokoyama [11]).

DEFINITION: Let L/K be a cyclic extension of algebraic number fields and let p be a rational prime. We say L/K pushes p away if $|L:K| = p^\alpha$, $p \nmid h_K$, and if there is a unique prime P of K above p and P is the only prime divisor of K ramified in L.

We note that $\mathbb{C}_{63}^+/\mathbb{C}_{21}^+$ pushes 3 away so $3 \nmid h_{63}^+$ by Lemma 7. We claim also that $\mathbb{C}_{72}^+/\mathbb{C}_9^+(6^{1/2})$, $\mathbb{C}_{80}^+/\mathbb{C}_{40}^+$, $\mathbb{C}_{120}^+/\mathbb{C}_{60}^+$, $\mathbb{C}_{60}^+/\mathbb{C}_{15}^+$, and $\mathbb{C}_{96}^+/F_{96}$ push 2 away where F_{96} is the cyclic subfield of $\mathbb{C}_{96}^+$ of degree 8 and conductor 96. All the conditions are easy to check except that $h_{60}^+ = h_{40}^+ = 1$ which is done in [7] and that $h_{F_{96}} = h_{\mathbb{C}_9+(6^{1/2})} = 1$ which is covered in Bauer's computations [1]. Hence h_{72}^+, h_{80}^+, h_{120}^+, and h_{96}^+ are odd by Lemma 7.

We are now ready to prove the

MAIN THEOREM: *Let m be an integer greater than one, $m \not\equiv 2 \bmod 4$ and let h_m be the class number of $\mathbb{Q}(\exp 2\pi i/m)$. Then all the m with $2 \leq h_m \leq 10$ are listed in the table:*

h_m	2	3	4	5	6	7	8	9	10
m	39	23	120	51	*none*	63	29	31	55
	56	52		80			68	57	
		72						96	

Furthermore, the twenty-nine other values of m with $\varphi(m) \leq 24$ are all the m with $h_m = 1$.

PROOF: All that remains is to show that no odd prime divides h_{72}^+, h_{80}^+, h_{96}^+, or h_{120}^+ and that no prime other than 3 divides h_{63}^+. We have used the (p, p)-lemma to verify this. To illustrate the procedure we will show that $h_{120}^+ = h_{63}^+ = 1$.

Suppose the odd prime q divides h_{120}^+. Now $\mathbb{C}_{120}^+/\mathbb{C}_{20}^+$ is a $(2, 2)$-extension with intermediate fields $\mathbb{C}_{20}^+(6^{1/2})$, $\mathbb{C}_{60}^+$, $\mathbb{C}_{40}^+$. Since $h_{60}^+ = h_{40}^+ = 1$ (see [7]), the $(2, 2)$-lemma implies that q must divide the class number of $\mathbb{C}_{20}^+(6^{1/2})$. Now $\mathbb{C}_{20}^+(6^{1/2})/\mathbb{C}_5^+$ is again a $(2, 2)$-extension so then q must divide the class number of at least one of $\mathbb{C}_{20}^+$, $\mathbb{C}_5^+(6^{1/2})$, or F_{120} where F_{120} is a cyclic extension of degree 4 over $\mathbb{Q}$, has conductor 120, and contains $\mathbb{C}_5^+ = \mathbb{Q}(5^{1/2})$ as unique quadratic subfield. The field $\mathbb{C}_{20}^+$ has class number one ([7]) and the $(2, 2)$-lemma shows that the class number of $\mathbb{C}_5^+(6^{1/2})$ is prime to q so it suffices to show that q does not divide $h_{F_{120}}$ to obtain a contradiction. A defining equation for F_{120} is $f(x) = x^4 - 30x^2 + 180$ (cf. [2]). It is easy to verify that the ideals generated by 2 and 3 are each the square of a prime ideal, that the ideal generated by 5 is the fourth power of a prime ideal ($f(x)$ is Eisenstein for 5), and that all other prime ideals of norm less than the Minkowski bound are in the ideal classes generated by the prime ideals above 2, 3, and 5. Therefore, no class has odd order in $C_{F_{120}}$ and q does not divide $h_{F_{120}}$.

Similarly, assume the prime $q \neq 3$ divides h_{63}^+. Now $\mathbb{C}_{63}^+/\mathbb{Q}(21^{1/2})$ is a $(3, 3)$-extension with four proper intermediate fields (cf. [3], p. 169) each of which is a cyclic extension of $\mathbb{Q}$ of degree 6. The tables of Bauer [1] show that two of these fields have class number three and the other two have class number one. However, the $(3, 3)$-lemma implies that q divides the class number of one of these four fields. This contradiction proves that $q \nmid h_{63}^+$ and since we have already seen that $3 \nmid h_{63}^+$ we obtain $h_{63}^+ = 1$ and $h_{63} = 7$.

REMARKS:

1. There are 189 real cyclic fields with conductor not exceeding 100. For those fields of degree 8 or higher we can improve the Minkowski bound for minimal norms of integral ideals in an ideal class. If the field has degree n, we multiply the usual Minkowski bound by

$$e^{3/2}(1 + n \log n)(2.5 \log n)^{3/2 \log n}\left(\frac{\pi}{4\sqrt{e}}\right)^n.$$

This formula can be found in [H]. Bauer's paper [1] lists those of the 189 fields which have improved Minkowski bound of more than 50,000.

2. The bound of 10 was chosen because $h_{132}^* = 11$ and $\mathbb{C}_{132}^+$ contains a cyclic field of degree 10 not covered by Bauer's computations.

3. New methods have developed which have allowed us to check all of Bauer's computations which were needed in [5–7] and this paper. Refinements of the new methods will probably allow us to verify all the results of [1].

4. It would be useful to have divisors of h_m^* computed for $m = pq$ with p and q distinct primes < 70. It seems likely that then we could determine all m with $h_m < 1{,}000{,}000$.

5. The structure of the class groups of $\mathbb{C}_m$ for $m = 120, 68, 57$, and 96 is unknown. For the other m with $h_m < 11$, the class group is cyclic except for that of $\mathbb{C}_{29}$ which is of exponent 2.

REFERENCES

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

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

[3] H. HASSE: *Uber die Klassenzahl abelscher Zahlkorper.* Akademie Verlag, 1952.

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

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

[6] J. MASLEY: Solution of the class number two problem for cyclotomic fields. *Inventiones Math. 25* (1975).

[7] J. MASLEY and H. L. MONTGOMERY: Unique factorization in cyclotomic fields. To appear in Crelle's Journal.

[8] T. METSANKYLA: On the growth of the first factor of the cyclotomic class number. *Ann. Univ. Turku, Ser. AI 155* (1972).

[9] M. NEWMAN: A table of the first factor for prime cyclotomic fields. *Math. Comp. 24* (1970) 215–219.

[10] G. SCHRUTKA V. RECHTENSTAMM: Tabelle der (relativ-)Klassenzahlen von Kreiskorper. Abh. Deutsche Akad. Wiss. Berlin, 1964 Math Nat. Kl. Nr. 2.

[11] A. YOKOYAMA: On class numbers of finite algebraic number fields. *Tohoku Math J., 17* (1965) 349–357.

[H] H. HASSE: *Zahlentheorie.* Akademie Verlag, Berlin, 3rd edition, 1969, p. 591.

(Oblatum 0–VII–1975 & 4–II–1976)

Mathematics Department
University of Illinois at Chicago Circle
Box 4348
Chicago, Illinois 60680
U.S.A.