Journal of Number Theory **72**, 269–281 (1998)
Article No. NT982275

Cyclotomic Integers of Prescribed Absolute Value and the Class Group

Bernhard Schmidt

Department of Mathematics, California Institute of Technology, Mail Code 253-37, Pasadena, California 91125

Communicated by A. Granville

Received May 27, 1997; revised February 16, 1998

We obtain a new method for the study of class groups of cyclotomic fields by investigating cyclotomic integers of prescribed absolute value. Explicit subgroups [illegible] field K_m, where $m = p^a m'$, $(p, m') = 1$, and p is a prime, we determine the structure of C^+C_P/C^+C_Q up to a binary parameter; here C_P, C_Q are the subgroups of C generated by the classes $[P_i]$ respectively $[Q_i]$, where p factors in K_m as $\prod Q_i$, $Q_i = P_i^{\varphi(p^a)}$, and the P_i are prime ideals.

1. INTRODUCTION

A basic theorem of algebraic number theory asserts that all elements of a prescribed norm in an order $\mathcal{O}$ of an algebraic number field have the form εx for a unit $\varepsilon \in \mathcal{O}$ and $x \in X$, where X is a fixed finite subset of $\mathcal{O}$. Furthermore, X can be determined in a finite number of steps. The corresponding section of [2], for instance, ends with the sentence, "This gives a final solution to the problem..." [2, p. 123]. Statements like this are very frustrating for anyone who really wants to work with numbers of prescribed norm—because the actual computation of X is usually impossible within one's lifetime and theoretically almost nothing is known about X.

The first part of this paper is devoted to an instance of the norm problem of particular interest, namely cyclotomic integers with prescribed absolute value. That is, we investigate the problem of prescribed *relative* norm for cyclotomic fields K with respect to the maximal real subfield K^+. In the second part we will show that the absolute value problem is intimately connected with the structure of the class group of K modulo the class group of K^+, thereby demonstrating the significance of our approach. Our main result will concern the class group C of the mth cyclotomic field K_m where $m = p^a m'$ and p is a prime. Let C_P, C_Q be the subgroups of C

0022-314X/98 $25.00

generated by the classes $[P_i]$ respectively $[Q_i]$, where p factors in K_m as $\prod Q_i$, $Q_i = P_i^{\varphi(p^a)}$, and the P_i are prime ideals. We will determine the structure of the group C^+C_P/C^+C_Q almost completely. A further result of a different type will provide explicit bounds on the size of subgroups of C/C^+. Of course, the knowledge of C^+C_P/C^+C_Q also yields information on class number factors, a problem which has been studied intensively in the literature. Work related to our results in one way or another can be found in [4–8, 12, 13, 15, 16]. The underlying methods mainly rely on the class number formula or on class field theory and are completely different from our approach. I am not aware of any previous work utilizing the connection to the absolute value problem for the study of class groups.

Last but not least, cyclotomic integers of prescribed absolute value play an important role in combinatorics, see [1, 10, 11, 14, 17, 19]. For example, one of the most popular combinatorial problems related to the absolute value problem is circulant Hadamard matrices. A *circulant Hadamard matrix* is a $v \times v$-matrix H with entries ± 1 of the form

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_v \\ a_v & a_1 & \cdots & a_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

such that any two rows of H are orthogonal. The *Circulant Hadamard Matrix Conjecture* asserts that there is no circulant Hadamard matrix besides the trivial examples for $v = 1, 4$. The connection to cyclotomic integers of prescribed absolute value is the following. Set $b_i := (a_i + 1)/2$. One can show that $\sum_{i=1}^{v} b_i \xi^i$ has absolute value $u := \sqrt{v}/2$ for any vth root of unity $\xi \neq 1$ and that u must be a rational integer. Thus the investigation of elements of $\mathbf{Z}[\xi]$ of absolute value u is essential for the study of Circulant Hadamard matrices. Using this method, dramatic progress towards the Circulant Hadamard Matrix Conjecture was recently achieved in [18].

2. CYCLOTOMIC INTEGERS OF PRESCRIBED ABSOLUTE VALUE

We will prove several restrictions on the structure of cyclotomic integers satisfying the equation $x\bar{x} = n$ for an integer $n > 1$. Exploiting the decomposition groups of the prime ideals involved in the right way will be the key to these results.

Throughout the rest of the paper, we use the following notation. By $K_m = \mathbf{Q}(\xi_m)$, $\xi_m = e^{2\pi i/m}$, we denote the mth cyclotomic field and by $\mathcal{O}_m$ its ring of integers. For $\sigma \in G_m := \mathrm{Gal}(K_m/\mathbf{Q})$ we write $\mathrm{Fix}(\sigma)$ for the subfield of K_m fixed by $\langle \sigma \rangle$. For positive integers t and s we denote the order of t modulo s by $o_s(t)$.

A prime p will be called *self-conjugate modulo m* if there is an integer j such $p^j \equiv -1 \pmod{m'}$, where $m = p^a m'$, $(p, m') = 1$. Note that p is self-conjugate modulo m if and only if the primes above p in $\mathcal{O}_m$ are invariant under complex conjugation. Moreover, if $q \neq p$ is an odd prime then p is self-conjugate modulo $p^a q^b$, $a \geqslant 0$, $b \geqslant 1$, if and only if $o_q(p)$ is even.

The following preliminary results will be basic for the whole paper.

We first note the following consequence of Kronecker's result that an algebraic integer all of whose conjugates have absolute value 1 is a root of unity.

Lemma 2.1. *Let $x \in \mathcal{O}_m$ be a solution of $x\bar{x} = n$, where n is a positive integer. If $\sigma \in G_m$ fixes all primes above n then*

$$x^\sigma = \varepsilon(\sigma)\, \xi_m^{j(\sigma)} x,$$

where $\varepsilon(\sigma)$ and $j(\sigma)$ are integers with $\varepsilon(\sigma) = \pm 1$ and $\varepsilon(\sigma) = 1$ if m is even.

Proof. Since $(x) = (x^\sigma)$, we have $x^\sigma = ux$ for some unit u. As $|x^\sigma|^2 = (x\bar{x})^\sigma = n^\sigma = n = |x|^2$, u has absolute value 1. By Kronecker's result, u must be a root of unity, i.e., $u = \pm \xi_m^j$ for some j. If m is even then we can choose the positive sign. ▮

The next lemma shows that $\varepsilon(\sigma)$ and $j(\sigma)$ satisfy important restrictions.

Lemma 2.2. *In the situation of Lemma* 2.1, *write $m = q^a m'$, where q is a prime and $(q, m') = 1$. Let σ be defined by $\xi_m \to \xi_m^t$, $(t, m) = 1$, let $y = o_m(t)$ denote the order of σ, and write*

$$x^\sigma = \varepsilon(\sigma)\, \xi_{q^a}^{j_1} \xi_{m'}^{j_2(\sigma)} x$$

(*with $\varepsilon(\sigma) = 1$ if m is even*). *Then $q^a/(q^a, (t^y - 1)/(t-1))$ divides $j_1(\sigma)$. Furthermore, if both m and y are odd then $\varepsilon(\sigma) = 1$.*

Proof. Write $\eta := \xi_{q^a}^{j_1(\sigma)}$ and $\gamma := \xi_{m'}^{j_2(\sigma)}$. We have

$$\begin{aligned} x = x^{\sigma^y} &= (\varepsilon(\sigma)\, \eta\gamma x)^{\sigma^{y-1}} \\ &= (\varepsilon(\sigma)^2\, \eta^{1+t} \gamma^{t+1} x)^{\sigma^{y-2}} \\ &= \cdots \\ &= \varepsilon(\sigma)^y\, \eta^{(t^y-1)/(t-1)} \gamma^{(t^y-1)/(t-1)} x. \end{aligned}$$

Thus $\varepsilon(\sigma)^y\, \eta^{(t^y-1)/(t-1)} = 1$ (in any case!) implying the assertion. ▮

We need conditions guaranteeing that we can assume $j_1(\sigma)=0$. This will be achieved simply by replacing x by x times a suitable root of unity.

LEMMA 2.3. *Assume that q does not divide $t-1$ or that q^{a+1} does not divide t^y-1 in Lemma 2.2. Then there is an integer k such that*

$$(x\xi_{q^a}^k)^\sigma = \varepsilon(\sigma)\,\xi_{m'}^{j_2(\sigma)}(x\xi_{q^a}^k).$$

Proof. We have to find a solution k of $\xi_{q^a}^{tk+j_1(\sigma)}=\xi_{q^a}^k$, i.e., of $k(t-1)+j_1(\sigma)\equiv 0 \pmod{q^a}$. This is possible if and only if $(q^a, t-1)$ divides $j_1(\sigma)$. Thus the assertion is clear if $(q^a, t-1)=1$. Assume that q^{a+1} does not divide t^y-1. Then $(q^a, (t^y-1)/(t-1))=q^a/(q^a, t-1)$ and Lemma 2.2 implies that $(q^a, t-1)$ divides $j_1(\sigma)$. ▮

COROLLARY 2.4. *If m is even or both m and y are odd and the assumption of Lemma 2.3 is satisfied for every prime divisor q of m then there is an integer r such that $x\xi_m^r\in \mathrm{Fix}(\sigma)$.*

Proof. Note $\varepsilon(\sigma)=1$ and apply Lemma 2.3 repeatedly. ▮

Now we are ready to prove an important restriction on the structure of the solutions of $x\bar{x}=n$ in the case where $n=p^a$ for a rational prime p. In a sense this result will tell us that any "ramified" solution of $x\bar{x}=p^a$ is necessarily a Gauss sum times an "unramified" solution.

Let $p=ef+1$ $(e\neq 1)$ be an odd prime, let Γ be the set of all primitive eth roots of unity and let h be a fixed primitive root modulo p. The set of all Gauss sums $\sum_{i=0}^{p-2}\gamma^i\xi_p^{h^i}$, $\gamma\in\Gamma$, will be denoted by $G(p,e)$. For $p=2$ we define $G(2,2)=\{1+i\}$.

THEOREM 2.5. *Let $m=p^a m'$, where p is a prime, $(p,m')=1$, and $m\not\equiv 2 \pmod 4$. If $x\in\mathcal{O}_m$ is a solution of $x\bar{x}=p^b$, $b\geqslant 1$, then there is an integer j such that*

$$x\xi_m^j\in\mathcal{O}_{m'} \qquad \text{or} \qquad x=\xi_m^j yz,$$

where $z\in\mathcal{O}_{m'}$, $z\bar{z}=p^{b-1}$, and $y\in G(p,e)$ for some divisor $e\neq 1$ of w_0 with $w_0=2$ if $p=2$, $w_0=(p-1,m')$ if m' is even, and $w_0=(p-1,2m')$ if both p and m' are odd.

Remark. The special case $m'=4$, $p\equiv 1 \pmod 4$ and $a=1$ of Theorem 2.5(b) was obtained in [14, Lemma 5].

Proof. Let $\prod_{i=1}^s q_i^{a_i}$ be the prime power decomposition of m'.

(a) We first treat the case $p=2$. Let t be an integer satisfying $t\equiv 5 \pmod{2^{a+1}}$ and (for technical reasons only) $t\equiv q_i^{a_i}+1 \pmod{q_i^{a_i+1}}$, $i=1, ..., s$, and let $\sigma \in G_m$ be defined by $\xi_m \to \xi_m^t$. Since $t \equiv 1 \pmod{m'}$, σ fixes all primes above 2 in $\mathcal{O}_m$. We will show that the assumption of Lemma 2.3 is satisfied for every prime divisor of m. We have $y = 2^{a-2}$ and 2^{a+1} does not divide $t^y - 1$ since $o_{2^{a+1}}(5) = 2^{a-1}$. Similarly, we conclude that $t^y - 1$ is not divisible by $q_i^{a_i+1}$ for all i. Thus we can apply Corollary 2.4 to get $x_1 := x\xi_m^r \in \operatorname{Fix}(\sigma) \cap \mathcal{O}_m = \mathcal{O}_{4m'}$ for some r. Let σ_1 be defined by $i \to -i$, $\xi_{m'} \to \xi_{m'}$. By Lemma 2.3 there are integers r_1, r_2 such that $x_2^{\sigma_1} = i^{r_1} x_2$ where $x_2 := x_1 \xi_{m'}^{r_2}$. Write $x_2 = y_1 + y_2 i$ with $y_1, y_2 \in \mathcal{O}_{m'}$. If $r_1 = 0$ then $x_2 \in \operatorname{Fix}(\sigma_1)$ and we are finished. If $r_1 = 2$ then $x_2^{\sigma_1} = y_1 - y_2 i = -x_2 = -y_1 - y_2 i$. Hence $x_2 = y_2 i$ yielding the assertion. If $r_1 = 1$ then $x_2^{\sigma_1} = y_1 - y_2 i = i x_2 = -y_2 + y_1 i$. Thus $y_1 = -y_2$, i.e., $x_2 = (1-i)\, y_1 = -i(1+i)\, y_1$ again yielding the assertion. The case $r_1 = 3$ is similar. This completes the proof for $p = 2$.

(b) Let p be odd. We first show $x\xi_m^j \in \mathcal{O}_{pm'}$ for some j. Let t be an integer satisfying $t \equiv p+1$ (mod $p^{a+1)}$ and (for technical reasons) $t \equiv q^{a_i} + 1$ (mod $q_i^{a_i+1}$), $i = 1, ..., s$. Then $\sigma \in G_m$ defined by $\xi_m \to \xi_m^t$ fixes all primes above p. It is easy to see that Corollary 2.4 can be applied and yields $x_1 := x\xi_m^j \in \operatorname{Fix}(\sigma) \cap \mathcal{O}_m = \mathcal{O}_{pm'}$ for some j.

Now let t_1 satisfy the same conditions as t with the first one replaced by $t_1 \equiv h \pmod{p}$ and let $\sigma_1 \in G_{pm'}$ be defined by $\xi_{pm'} \to \xi_{pm'}^{t_1}$. Note that σ_1 fixes all primes above p. However, also note that we cannot apply Corollary 2.4—this is quite plausible since it would imply the nonexistence of Gauss sums. By Lemma 2.1 we have $x_1^{\sigma_1} = \varepsilon \xi_p^{j_0} \prod_{i=1}^s \xi_{q_i^{a_i}}^{j_i} x_1$ with $\varepsilon = \pm 1$ and for some integers j_i. Since $(p, t_1 - 1) = 1$, we can assume $j_0 = 0$ by Lemma 2.3. Let $q_i^{b_i}$ be the highest power of q_i dividing $p-1$. From Lemma 2.2 we infer that $q_i^{a_i}/(q_i^{a_i}, (t_1^{p-1} - 1)/(t_1 - 1))$ divides j_i for all i. Since $o_{q_i^{a_i+1}}(t_1) = q_i$, we have $o_{q_i^{a_i+b_i+1}}(t_1) = q_i^{b_i+1}$ and hence $q_i^{a_i+b_i+1}$ does not divide $t_1^{p-1} - 1$. As $q_i^{a_i}$ divides $t_1 - 1$, we get $(q_i^{a_i}, (t_1^{p-1} - 1)/(t_1 - 1)) \mid q_i^{b_i}$ and thus $q_i^{a_i - b_i} \mid j_i$. It follows that $x_1^{\sigma_1} = \eta x_1$ where η is a primitive eth root of unity for some divisor e of w_0. If $\eta = 1$ then $x_1 \in \operatorname{Fix}(\sigma_1) \cap \mathcal{O}_m = \mathcal{O}_{m'}$ yielding the assertion. Thus assume $\eta \neq 1$. We write $x_1 = \sum_{i=0}^{p-2} A_i \xi_p^{h^i}$ with $A_i \in \mathcal{O}_{m'}$. Then

$$
\begin{aligned}
x_1^{\sigma_1} &= \eta \sum_{i=0}^{p-2} A_i \xi_p^{h^i} \\
&= \sum_{i=0}^{p-2} A_i \xi_p^{h^{i+1}} \\
&= A_{p-2} \xi_p^{h^0} + \sum_{i=1}^{p-2} A_{i-1} \xi_p^{h^i}.
\end{aligned}
$$

Hence $A_0 \eta = A_{p-2}$ and $A_i \eta = A_{i-1}$ for $i = 1, ..., p-2$. Thus $A_i = A_0 \eta^{-i}$, $i = 1, ..., p-2$. This gives $x_1 = A_0 \sum_{i=0}^{p-2} \eta^{-i} \xi_p^{h^i}$ completing the proof. ▌

The following theorem gives a restriction on the solutions of $x\bar{x}=n$ of a completely different type. A special case of this result was proved in [3].

THEOREM 2.6. *Let $x \in \mathcal{O}_m$ be a solution of $x\bar{x}=n$, where $(m, n)=1$, $m=p^a$, and p is an odd prime. Let $n=\prod_{i=1}^{s} r_i^{a_i}$ be the prime power decomposition of n. If $a \geqslant 2$, we assume $r_i^{p-1} \not\equiv 1 \pmod{p^2}$ for all i. Let f be any common divisor of $o_p(r_i)$, $i=1, ..., s$, and write $p=ef+1$. Then the following hold.*

(a) *If n is a square of a rational integer u and $f>2u(p-1)/p$ then $(x)=(u)$.*

(b) *If n is a nonsquare then f is odd and there is an integer y satisfying $y^2 \equiv e^2 n \pmod{p}$ and $1 \leqslant y \leqslant e\sqrt{n}$. In particular, $e^2 n>p$.*

Remarks. (i) Under additional assumptions, one can allow m to be the product of two prime powers in Theorem 2.6.

(ii) For $f=(p-1)/2$ the assumptions of Theorem 2.6 can slightly be weakened.

Proof. If f is even, the assertion is obvious since then all primes above n in $\mathcal{O}_m$ are invariant under complex conjugation; see the beginning of this section or [19], for instance.

Thus assume that f is odd. Let t be an integer such that $o_{p^a}(t)=fp^{a-1}$ and define $\sigma \in G_m$ by $\xi_m \to \xi_m^t$. It is easy to see that the assumptions of the theorem imply that fp^{a-1} divides $o_{p^a}(r_i)$ for all i. We conclude that for every i there is an integer j_i such that $r_i^{j_i} \equiv t \pmod{p^a}$. Thus σ fixes all primes above n in $\mathcal{O}_m$. As $o_{p^a}(t)=fp^{a-1}$ is odd and since $(p, t-1)=1$, we can apply Corollary 2.4 which shows that we can assume $x \in K_{p,e}$, where $K_{p,e}$ is the subfield of dimension $e:=(p-1)/f$ of K_p. Let g be a primitive root modulo p. The Gaussian periods $\eta_i=\sum_{t=0}^{f-1} \xi_p^{g^{et+i}}$, $i=0, ..., e-1$, form an integral basis of $K_{p,e}$ over $\mathbf{Q}$. Hence we can write $x=\sum_{i=0}^{e-1} b_i \eta_i$ with $b_i \in \mathbf{Z}$. It is shown in [3, Lemma 2.3] that this implies

$$en=p\sum b_i^2-f\left(\sum b_i\right)^2 \tag{1}$$

and $|\sum b_i| \leqslant e\sqrt{n}$. Considering (1) modulo p and multiplying by e we conclude $y^2 \equiv e^2 n \pmod{p}$ where $y=|\sum b_i|$. This already proves part (b). Furthermore, if $n=u^2$ for a positive integer u then $y \equiv \pm eu \pmod{p}$. Since $y \leqslant eu$ and $p>2u(p-1)/f=2ue$, we infer $y=ue$. Now (1) gives $\sum b_i^2=eu^2$ and this together with $|\sum b_i|=eu$ implies that $b_i=u$ or $b_i=-u$ for all i completing the proof of (a). ▌

Remark. Under appropriate assumptions one can combine Theorem 2.5 and Theorem 2.6 to show that under these assumptions $(x)=(p^a)$ if $x\bar{x}=p^{2a}$, $x\in\mathcal{O}_{p^bq^c}$, where p and q are primes and q is odd. We omit the explicit statement and proof which are tedious but straightforward.

3. SUBGROUPS OF THE CLASS GROUPS OF CYCLOTOMIC FIELDS

In this section, we use our results on cyclotomic integers of prescribed absolute value to study subgroups of ideal class groups of cyclotomic fields generated by prime ideals above fixed rational integers. The both most obvious and most important connection between the class group and solutions of $x\bar{x}=n$ in cyclotomic integers is described in the following proposition. For the sake of clarity, we state it in a way slightly differing from the version needed in the proofs of Theorems 3.3 and 3.7.

PROPOSITION 3.1. *Let m and n be any positive integers and assume that there is a principal ideal $A=(y)$ of $\mathcal{O}_m$ solving the ideal equation $A\bar{A}=(n)$. Then the following hold.*

(a) *There is a solution $x\in\mathcal{O}_m$ of $x\bar{x}=n$ with $(x)=A$ if and only if $n/y\bar{y}$ is a square of a real unit ε in $\mathcal{O}_m$.*

(b) *There is* always *a solution $z\in\mathcal{O}_m$ of $z\bar{z}=n^2$ with $(z)=A^2$.*

Proof. (a) If $n/y\bar{y}=\varepsilon^2$ then $x:=\varepsilon y$ solves $x\bar{x}=n$.
Conversely, if $x\bar{x}=n$ and $(x)=A$ then $x=\delta y$ for some unit δ and $n/y\bar{y}=\delta\bar{\delta}$ which is a square of a real unit since any unit in $\mathcal{O}_m$ is a product of a real unit and a root of unity.

(b) This follows from (a) since $n^2/y^2\bar{y}^2$ surely is a square of a real unit. ▮

Our strategy will be the following. Theorems 2.5 and 2.6 provide necessary conditions on the ideals (x) generated by solutions of $x\bar{x}=n$. Combined with Proposition 3.1 this shows that usually a lot of solutions of the ideal equation $A\bar{A}=(n)$ must be *nonprincipal*. Thus we get a grip on the subgroup of the classgroup generated by the classes of the prime ideals above n.

We are now going to utilize Theorem 2.5 for the study of class groups. We will need some notation. We fix a positive integer $m\not\equiv 2 \pmod 4$ and work in the mth cyclotomic field $K=K_m$. Let K^+ be the maximal real subfield of K. By I, H, C, respectively I^+, H^+, C^+, we denote the group of all (fractional) ideals, the group of all principal ideals, and the class group of K, respectively K^+. We view I^+, H^+, C^+ as imbedded in I, H,

C in the natural way. Note that the imbedding of C^+ in C makes sense, since the natural homomorphism $C^+ \to C$ is an injection, see [20, Theorem 4.14].

Let $m = p^a m'$, where p is a prime relatively prime to m'. Recall that p factors in K as $\prod Q_i$, where $Q_i = P_i^{(p-1)\,p^{a-1}}$ and the P_i are distinct prime ideals. We write I_P, I_Q for the subgroups of I generated by the P_i, respectively the Q_i. The groups H_P, H_Q, C_P, C_Q are defined similarly. Thus, for instance, $C_P = I_P H/H$ and $C_Q = I_Q H/H$.

We define the "Gauss sum group" as the subgroup $G(p)$ of H generated by all $J \in H$ which are generated by an element of $G(p, e)$ for some divisor $e \neq 1$ of w_0, where $w_0 = 2$ if $p = 2$, $w_0 = (p-1, m')$ if m' is even, and $w_0 = (p-1, 2m')$ if both p and m' are odd.

Finally, φ denotes the Euler φ function.

Lemma 3.2. (a) *The ideal group*

$$I_P^- := \{J \in I_P \colon J/\bar{J} \in G(p)\, I_Q\}$$

contains $I_P \cap I^+ I_Q H$.

(b) *Assume that p is not self-conjugate modulo $m = p^a m'$. Then*

$$I_P/I_P^- \cong (\mathbf{Z}/w\mathbf{Z}) \times (\mathbf{Z}/u\mathbf{Z})^{e/2-1},$$

where $u = \varphi(p^a)$, $e = \varphi(m')/o_{m'}(p)$, $w = u/w_0$, *and* w_0 *is defined above.*

Proof. (a) Since $I_Q \leqslant I_P^-$ by definition, it suffices to show $I_P \cap I^+ H \leqslant I_P^-$. Thus let $J \in I_P \cap I^+ H$ be arbitrary and write $J = J^+(h)$ with $J^+ \in I^+$ and $h \in K$. Since J^+ is invariant under complex conjugation, we have $J/\bar{J} = (h/\bar{h})$. As $J/\bar{J} \in I_P$, there is a positive integer b such that $y := p^b h/\bar{h} \in \mathcal{O}_m$. Because of $y\bar{y} = p^{2b}$ we conclude $(y) \in G(p)\, I_Q$ by Theorem 2.5. Hence $J/\bar{J} = (y)/(p^b) \in G(p)\, I_Q$, too, since $(p^b) \in I_Q$. This shows $I_P \cap I^+ I_Q H \leqslant I_P^-$.

(b) Let $P_1, \overline{P_1}, ..., P_{e/2}, \overline{P_{e/2}}$ denote the primes above p in $\mathcal{O}_m$ and define

$$T := \left\{ \prod_{i=1}^{e/2} P_i^{c_i} \colon 0 \leqslant c_1 \leqslant w-1,\ 0 \leqslant c_i \leqslant u-1 \text{ for } i = 2, ..., e/2 \right\}.$$

We first show that the elements of T represent distinct cosets of I_P^- in I_P. Thus assume $S := \prod_{i=1}^{e/2} P_i^{c_i - c'_i} \in I_P^-$ with $0 \leqslant c_1,\ c'_1 \leqslant w-1$ and $0 \leqslant c_i,\ c'_i \leqslant u-1$ for $i = 2, ..., e/2$. Then $S/\bar{S} \in G(p)\, I_Q$ by the definition of I_P^-. Theorem 2.5 implies that every element of $G(p)\, I_Q$ can be written in the form $G^\delta J$ with $\delta \in \{0, 1\}$, $G \in G(p, r)$ for some divisor $r \neq 1$ of w_0, and $J \in I_Q$. Thus we can write $S/\bar{S}$ in this form, say $S/\bar{S} = G_S^{\delta_S} J_S$. If $\delta_S = 1$ then by Stickelberger's relation (see [9, p. 209, Theorem 2; 20, p. 98, 1.19]) P_1 occurs in $S/\bar{S} = G_S^{\delta_S} J_S$ to a power $xu/r + yu$, where x, y are integers with

$(x, r) = 1$. This implies $|c_1 - c_1'| = |xu/r + yu| \geqslant u/r \geqslant w$ which is impossible. Hence $\delta_S = 0$, i.e., $S/\overline{S} \in I_Q$. We conclude $c_i = c_i'$ for all i showing that the elements of T indeed represent distinct cosets of I_P^-.

Our next goal is to show $I_P^- T = I_P$. For that let $J \in I_P$ be arbitrary, say $J = \prod_{i=1}^{e/2} P_i^{a_i} \overline{P_i}^{b_i}$. Because of $P_i \overline{P_i} \in I_P^-$ we may assume $b_i = 0$ for all i. Write $a_1 = z_1 w + z_2$, where z_1, z_2 are integers with $0 \leqslant z_2 < w$. By Stickelberger's relation there is $G \in G(p)$ such that $G = P_1^w \overline{P_1}^{u-w} \prod_{i=2}^{e/2} P_i^{f_i} \overline{P_i}^{u-f_i}$ for some integers f_i. Then $J_1 := P_1^w \prod_{i=2}^{e/2} P_i^{f_i} \in I_P^-$, since $I_Q J_1 \overline{J_1}^{-1} = I_Q G$. Note that $P_1^{z_2} \prod_{i=2}^{e/2} P_i^{a_i - z_1 f_i}$ can be written as $L_1 L_2$ with $L_1 \in T$ and $L_2 \in I_Q$. Thus $J = P_1^{z_2} J_1^{z_1} \prod_{i=2}^{e/2} P_i^{a_i - z_1 f_i} = (J_1^{z_1} L_2)\, L_1 \in I_P^- T$. This shows $I_P^- T = I_P$.

We conclude $[I_P : I_P^-] = wu^{e/2-1}$. Let U be the subgroup of I_P generated by $P_2, \overline{P_2}, ..., P_{e/2}, \overline{P}_{e/2}$. Then $I_P^- U/I_P^- \cong (\mathbf{Z}/u\mathbf{Z})^{e/2-1}$, since by what we have shown $I_P^- P_2, ..., I_P^- P_{e/2}$ is a basis of $I_P^- U/I_P^-$. Now assertion (b) follows from the theorem on subgroups of free abelian groups of finite rank since the exponent of I_P/I_P^- divides u. ▮

THEOREM 3.3. *Assume that p is not self-conjugate modulo $m = p^a m'$. Then*

$$C_P C^+/C_Q C^+ \cong (\mathbf{Z}/2^\delta w\mathbf{Z}) \times (\mathbf{Z}/u\mathbf{Z})^{e/2-1},$$

where $\delta \in \{0, 1\}$, $u = \varphi(p^a)$, $e = \varphi(m')/o_{m'}(p)$, $w = u/w_0$, $w_0 = 2$ if $p = 2$, $w_0 = (p-1, m')$ if m' is even, and $w_0 = (p-1, 2m')$ if both p and m' are odd. In particular, the relative class number h_m^- of K_m is divisible by $wu^{e/2-1}$.

Remarks. (a) If p is self-conjugate modulo $m = p^a m'$ then $C_P C^+/C_Q C^+ = \{1\}$ trivially.

(b) The reason for the binary uncertainty δ in the structure of $C_P C^+/C_Q C^+$ is the loss of information by squaring in Proposition 3.1(b). The determination of δ is an interesting problem; in particular, it would yield new information on cyclotomic integers of prescribed absolute value.

Proof. We first note

$$\begin{aligned} C^+ C_P/C^+ C_Q &\cong (I^+ I_P H/H)/(I^+ I_Q H/H) \\ &\cong I^+ I_P H/I^+ I_Q H \\ &\cong I_P/I_P \cap I^+ I_Q H. \end{aligned}$$

Write $A = I_P/I_P \cap I^+ I_Q H$. The exponent of A divides u and its rank is at most $e/2$. We know from Lemma 3.2(a) that I_P/I_P^- is isomorphic to a factor group of A. Putting these facts together and using Lemma 3.2(b) we see that $A \cong (\mathbf{Z}/v\mathbf{Z}) \times (\mathbf{Z}/u\mathbf{Z})^{e/2-1}$ for some divisor v of u with $v \equiv 0 \pmod{w}$ by the theorem on subgroups of free abelian groups of finite rank.

Our next claim is that $B := I_P^- / I_P \cap I^+ I_Q H$ is either trivial or an elementary abelian 2-group. For that let $J \in I_P^-$ be arbitrary. Then $J/\bar{J} \in I_P \cap I_Q H$ and hence $J^2 = (J/\bar{J})(J\bar{J}) \in I_P \cap I^+ I_Q H$, as $J\bar{J} \in I_P \cap I^+$. This proves the claim.

Finally, since $A/B \cong I_P/I_P^- \cong (\mathbf{Z}/w\mathbf{Z}) \times (\mathbf{Z}/u\mathbf{Z})^{e/2-1}$, we must have $v = w$ or $v = 2w$. ▌

It is interesting to compare Theorem 3.3 with previously known results which were obtained by completely different methods. We first consider some results of Metsänkylä [15, 16] who proved congruences for relative class numbers by manipulations of the class number formula. In parts (a) and (b) of the following corollary we essentially recover Satz 10 of [15] and in part (c) we obtain new congruences which are somewhat related to Satz 8 and Satz 9 of [15].

Corollary 3.4. *Let p and q be odd primes and let h_m^- denote the relative class number of K_m. Then the following hold.*

(a) $h_{3p^a}^- \equiv 0 \pmod{\varphi(p^a)/6}$ *for* $p \equiv 1 \pmod 3$,

(b) $h_{4p^a}^- \equiv 0 \pmod{\varphi(p^a)/4}$ *for* $p \equiv 1 \pmod 4$,

(c) $h_{p^a q^b}^- \equiv 0 \pmod{\varphi(p^a)^{(q-1)\,q^{c-1}/2}/2q^c}$ *if* q^c, $1 \leqslant c \leqslant b$, *is the highest power of* q *dividing* $p-1$.

Proof. (a) We put $m' = 3$ in Theorem 3.3. Then the assumptions are satisfied and we have $u = \varphi(p^a)$, $e = 2$, $w_0 = 6$, and $w = \varphi(p^a)/6$ implying the assertion.

(b) We put $m' = 4$ in Theorem 3.3 and get the assertion.

(c) Put $m' = q^b$ in Theorem 3.3. Then $u = \varphi(p^a)$, $w_0 = 2q^c$, and $e = (q-1)\,q^{c-1}$ since $o_{q^b}(p) = q^{b-c}$. ▌

Example 3.5. We choose an example which can be compared with the table of relative class numbers in [20]. By Corollary 3.4(c) we have $h_{23 \cdot 11}^- \equiv 0 \pmod{2^4 \cdot 11^4}$. The table shows that 2^4, 11^4 are actually the highest powers of 2 respectively 11 dividing $h_{23 \cdot 11}^-$.

Another approach to class number factors can be found in [4, 6]; the method is to use Abhyankar's lemma to construct unramified abelian extensions which yield class number factors by class field theory. For instance, it is shown in [4] that the class group of K_{4p}, where $p \equiv 1 \pmod 4$ is a prime, contains a cyclic group of order $(p-1)/4$. Note that this result is contained in our Theorem 3.3. A further result from [6] is that the class number of K_{pq} is divisible by $(p-1)/2$ or $(q-1)/2$ if p and q are distinct primes $\equiv 3 \pmod 4$. This is a consequence of the following.

Corollary 3.6. *Let p and q be primes $\equiv 3 \pmod 4$. By quadratic reciprocity we may w.l.o.g. assume that p is a square modulo q, i.e., that $o_q(p)$ is odd. Then*

$$h_{pq}^- \equiv 0 \qquad (\mathrm{mod}(p-1)^{(q-1)/(2o_q(p))}/2)$$

if $(p-1, q) = 1$ and

$$h_{pq}^- \equiv 0 \qquad (\mathrm{mod}(p-1)^{(q-1)/2}/(2q))$$

if q divides $p-1$.

Proof. Put $m' = q$ in Theorem 3.3. ▌

We need some notation for the formulation of our next result. Let m and t be positive, relatively prime integers, where $m = p^a$ for an odd prime p. Furthermore, let $t = \prod_{i=1}^{s} r_i^{d_i}$ be the prime power decomposition of t. We are only interested in the case where $f_i := o_p(r_i)$ is odd for every i. Then the prime ideals above r_i in $\mathcal{O}_m$ are *not* invariant under complex conjugation. Hence each r_i factors in $\mathcal{O}_m$ as

$$(r_i) = \prod_{j=1}^{u_i} P_{ij}\overline{P_{ij}},$$

where $u_i = \varphi(p^a)/(2o_{p^a}(r_i))$ and the P_{ij} are distinct prime ideals. We also keep the notation introduced before Lemma 3.2.

Theorem 3.7. *Assume that f is a common divisor of $f_1, ..., f_s$ and that $r_i^{p-1} \not\equiv 1 \pmod{p^2}$ if $m = p^a > p$. If the f_i are odd and if*

$$t = \prod_{i=1}^{s} r_i^{d_i} < \frac{fp}{2(p-1)},$$

where the d_i are any nonnegative integers, then the ideal classes

$$\left[\prod_{i=1}^{s} \prod_{j=1}^{u_i} P_{ij}^{c_{ij}}\right], \qquad 0 \leqslant c_{ij} \leqslant d_i,$$

$i = 1, ..., s$, $j = 1, ..., u_i$, represent distinct cosets of C^+ in C. Here we have $u_i = (p-1)/2f_i$.

In particular, the order of the subgroup of C/C^+ generated by the cosets $C^+[P_{ij}]$, $i = 1, ..., s$, $j = 1, ..., u_i$, is at least $\prod_{i=1}^{s} (d_i + 1)^{u_i}$.

Proof. Assume $C^+[\prod_{i=1}^{s}\prod_{j=1}^{u_i} P_{ij}^{c_{ij}}] = C^+[\prod_{i=1}^{s}\prod_{j=1}^{u_i} P_{ij}^{c'_{ij}}]$. Then there are $h \in K$ and $J^+ \in I^+$ such that $J := \prod_{i=1}^{s}\prod_{j=1}^{u_i} P_{ij}^{c_{ij}-c'_{ij}} = (h)\, J^+$. Since $(h/\bar{h}) = J/\bar{J}$ and $|c_{ij} - c'_{ij}| \leqslant d_i$ for all i, j, we know that $y := th/\bar{h}$ lies in $\mathcal{O}_m$. As $y\bar{y} = t^2$ and $f > 2t(p-1)/p$ by the assumption, we can apply Theorem 2.6(a) and get $(y) = (t)$. Thus $(h) = (\bar{h})$ and $J = \bar{J}$, i.e., $c_{ij} = c'_{ij}$ for all i, j. ∎

Corollary 3.8. *Let $m = p^a$ for an odd prime p. Assume that q is a prime such that $o_p(q)$ is odd and that $q^{p-1} \not\equiv 1 \pmod{p^2}$ if $a \geqslant 2$.*

Then the size of the subgroup of C/C^+ generated by the classes of the primes Q_i above q in $\mathcal{O}_m$ is at least

$$\left(\left\lfloor \ln \frac{o_p(q)\, p}{2(p-1)} \Big/ \ln q \right\rfloor + 1\right)^{(p-1)/2o_p(q)}.$$

Furthermore, each Q_i has order at least $\lfloor \ln((o_p(q)\, p)/2(p-1))/\ln q \rfloor + 1$ in C.

Proof. We put $s = 1$, $r_1 = q$, $f = o_p(q)$, and $d_1 = \lfloor \ln((o_p(q)\, p)/2(p-1))/\ln q \rfloor$ in Theorem 3.7. Then the assumptions are satisfied, for $t = q^{d_1} < fp/(2(p-1))$. Thus Theorem 3.7 gives the assertion. ∎

Example 3.9. We consider the classical example $p = 23$, $q = 2$. Corollary 3.8 shows that the order of a prime above 2 in the class group of K_{23} is at least $\lfloor \ln((11 \cdot 23)/(2 \cdot 22))/\ln 2 \rfloor + 1 = 3$. Since the class number of K_{23} is 3, such a prime generates the full class group.

It is straightforward to combine Corollary 3.8 with reciprocity laws to show that certain prime ideals are always nonprincipal. We only mention the following case containing the classical $p = 23$.

Corollary 3.10. *Let $p \geqslant 23$ be a prime* $\equiv 7 \pmod 8$. *Then the prime ideals above 2 in $\mathcal{O}_p$ are nonprincipal.*

Proof. Since $p \geqslant 23$ and $o_{23}(2) = 11$, we have $o_p(2) \geqslant 5$. By quadratic reciprocity $o_p(2)$ is odd. Thus Corollary 3.8 shows that the order of a prime above 2 in the class group of K_p is at least $\lfloor (\ln 5/2)/\ln 2 \rfloor + 1 = 2$. ∎

ACKNOWLEDGMENTS

I am grateful to S. Jakubec for drawing my attention to the work of T. Metsänkylä, to T. Metsänkylä for sending me his work [15, 16], and to L. C. Washington for pointing out Refs. [4, 6]. I also thank the referee for his careful reading of the manuscript.

REFERENCES

1. T. Beth, D. Jungnickel, and H. Lenz, "Design Theory," Cambridge Univ. Press, Cambridge, 1986.
2. Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York/San Francisco/London, 1966.
3. W. K. Chan, Necessary conditions for Menon difference sets, *Designs Codes Cryptography* **3** (1993), 147–154.
4. G. Cornell, Abhyankar's lemma and the class group, *in* "Number Theory" (M. Nathanson, Ed.), Lecture Notes in Math., Vol. 751, pp. 82–88, Springer-Verlag, Berlin/New York/Heidelberg, 1979.
5. G. Cornell and M. Rosen, Group-theoretic constraints on the structure of the class group, *J. Number Theory* **13** (1981), 1–11.
6. G. Cornell and L. C. Washington, Class numbers of cyclotomic fields, *J. Number Theory* **21** (1985), 260–274.
7. F. Gerth, The ideal class group of two cyclotomic fields, *Proc. Amer. Math. Soc.* **78** (1980), 321–322.
8. H. Hasse, "Über die Klassenzahl Abelscher Zahlkörper," Springer-Verlag, Berlin/Heidelberg/New York/Tokyo, 1985.
9. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," Graduate Texts in Math., Vol. 84, Springer-Verlag, Berlin/New York/Heidelberg, 1990.
10. D. Jungnickel, Difference sets, *in* "Contemporary Design Theory, a Collection of Surveys" (J. H. Dinitz and D. R. Stinson, Eds.), pp. 241–324, Wiley, New York, 1992.
11. D. Jungnickel and B. Schmidt, Difference sets: An update, *in* "Geometry, Combinatorial Designs and related Structures," Proceedings of the First Pythagorean Conference (J. W. P. Hirschfeld, S. S. Magliveras, and M. J. de Resmini, Eds.), pp. 89–112, Cambridge University Press, 1997.
12. D. Kubert, The 2-divisibility of the class number of cyclotomic fields and the Stickelberger ideal, *J. Reine Angew. Math.* **369** (1986), 192–218.
13. J. Masley, "On the Class Number of Cyclotomic Fields," Ph.D. thesis, Princeton University, 1972.
14. R. L. McFarland, Difference sets in abelian groups of order $4p^2$, *Mitt. Math. Sem. Giessen* **192** (1989), 1–70.
15. T. Metsänkylä, Über den ersten Faktor der Klassenzahl des Kreiskörpers, *Ann. Acad. Sci. Fenn. Ser. A I* **416** (1967).
16. T. Metsänkylä, Über die Teilbarkeit des ersten Faktors der Klassenzahl des Kreiskörpers, *Ann. Univ. Turku. Ser. A I* **124** (1968).
17. A. Pott, "Finite geometry and Character Theory," Lecture Notes in Math., Vol. 1601, Springer-Verlag, Berlin/New York/Heidelberg, 1995.
18. B. Schmidt, Cyclotomic integers and finite geometry, *J. Amer. Math. Society*, to appear.
19. R. J. Turyn, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.
20. L. C. Washington, "Introduction to Cyclotomic Fields," Graduate Texts in Math., Vol. 83, Springer-Verlag, Berlin/New York/Heidelberg, 1997.