

# Class Numbers and a Generalized Fermat Theorem

R. A. MOLLIN\*

*Department of Mathematics and Statistics,  
University of Calgary, Calgary, Alberta, Canada*

*Communicated by D. J. Lewis*

Received July 1, 1981

Conditions for divisibility of class numbers of algebraic number fields by prime powers are explored and linked to the existence of integer solutions of certain cyclotomic polynomials modulo a given rational integer. Several applications are provided, including a generalization of the Fermat "two-square theorem."

## INTRODUCTION

The purpose of this paper is twofold. In the first section we provide sufficient conditions for the divisibility of the class number of certain algebraic number fields by prime powers and applications thereof. We were initially inspired in this regard by Watabe [11], wherein some of the results are false thereby leading to the above.

In the second section we generalize Fermat's well-known "two-square theorem." We then apply the results of the first section to the latter result to obtain a connection between the existence of an integer solution to the  $2$   $p$ th cyclotomic polynomial modulo  $n$  and the divisibility of the class number of  $\mathbf{Q}(\varepsilon_{pq})$  (for all primes  $q$  dividing  $n$ ) by  $p$ -powers and the divisibility of the class number of  $\mathbf{Q}(\varepsilon_p, \sqrt{q^*})$  by  $2$ , where  $q^* = (-1)^{(q-1)/2} q$ .

## 1. CLASS NUMBERS OF ALGEBRAIC NUMBER FIELDS

We let  $K$  denote an algebraic number field, and let  $h(K)$  denote its class number. Suppose that  $q$  is a prime and  $\varepsilon_q$ , a primitive  $q$ th root of unity, is in  $K$ . Let  $L$  be a cyclic Kummer extension of degree  $q$  over  $K$ , with Galois group  $G(L/K) = \langle \sigma \rangle$ . An element  $C$  of the ideal class group of  $L$  is called *ambiguous* over  $K$  if  $C = C^\sigma$ . Now set  $\eta^* = N_{L/K}(L) \cap U_K$ , where  $U_K$

\* The author's research is supported by N.S.E.R.C. Canada.

denotes the unit group of the ring of integers of  $K$ , and  $N_{L/K}$  is the norm map for  $L$  over  $K$ . Let  $|\eta^* : U_K^q| = q^e$ ;  $g$  = the number of  $K$ -primes ramified in  $L$ ;  $f$  = the number of fundamental units in  $K$ ; and let  $A$  = the number of ambiguous classes for  $L$  over  $K$ .

A tool which we shall use in this section is the following lemma for which the above notation is in force.

LEMMA 1.1. (1)  $A = h(K)q^{e+g-f-2}$ ; (2)  $A|h(L)$ ; (3)  $q|A$  if and only if  $q|h(L)$ .

*Proof.* (1) is proved in Hasse [5, p. 98]. (2) and (3) are proved in Moriya [9].

The above notation is in force for the following result.

THEOREM 1.1. *Let  $K$  be an algebraic number field with  $c$  complex primes and  $\iota$  real primes.*

*Suppose that*

(1)  $\varepsilon_{q^m}$  is in  $K$  but  $\varepsilon_{q^{m+1}}$  is not in  $K$ , where  $q$  is a prime and  $m$  is a positive integer;

(2)  $F$  is a finite Galois extension of  $K \cap F$  in which some finite  $K \cap F$ -prime is totally ramified;

(3)  $F$  has a subfield  $F_1$  of degree  $q$  over  $K \cap F$ ; and

(4) all finite  $K \cap F$ -primes which ramify in  $F_1$  are completely split in  $K(\varepsilon_{q^{m+a}})$  where  $a \geq 0$ . Let  $d$  denote the number of finite  $K \cap F$ -primes which ramify in  $F_1$ .

If  $d \leq |K \cap F : \mathbf{Q}|$  then we require  $|K : K \cap F| \geq c + \iota + 1$ . Then:

(i) For  $a = 0$ :  $q^\ell |h(KF_1)$  and  $q^\ell |h(KF)$ , where  $\ell = d|K : K \cap F| - c - \iota - 1$ ; and

(ii) For  $a > 0$ : if either  $\iota = 0$  or  $\iota$  is odd then  $q^{\ell+1} |h(KF_1)$  and  $q^{\ell+1} |h(KF)$ .

*Proof.* From (1) and (3) we get that  $KF_1$  is a Kummer extension of  $K$  of degree  $q$ , so  $KF_1 = K(\sqrt[q]{\alpha})$  for some non-zero  $\alpha$  in  $K$  but not in  $K^q$ . From (4) it follows that  $g \geq d|K : K \cap F|$ . Moreover, we have  $f = c + \iota - 1$  by Dirichlet's unit theorem. Therefore  $e + g - f - 2 \geq e + d|K : K \cap F| - c - \iota - 1 = e + \ell$ .

(i) For  $a = 0$ :  $e \geq 0$  and since either  $d > |K \cap F : \mathbf{Q}|$  or  $|K : K \cap F| \geq c + \iota + 1$  by (4) then  $\ell \geq 0$ . Thus  $e + g - f - 2 \geq \ell \geq 0$ , and so by Lemma 1.1  $q^\ell |h(KF_1)$ . Furthermore from (2) and (4) it follows that some finite  $K$ -prime is totally ramified in  $KF_1$ . Thus by Iwasawa [7, I] we get that  $q^\ell |h(KF)$ .

(ii) For  $\alpha > 0$ : we first show that  $\varepsilon_{qm}$  is in  $\eta^* = N_{L/K}(L) \cap U_K$  where  $L = KF_1$ . Let  $(\alpha, \varepsilon_{qm})_q$  denote the norm residue symbol at the  $K$ -prime  $q$  (see [3, pp. 351–355]). Since  $\varepsilon_{qm}$  is a unit then  $(\alpha, \varepsilon_{qm})_q = 1$  whenever  $q$  is unramified in  $L$  by [3, Corollary, p. 142]. Now by [3, 2.6, p. 352] we have  $(\alpha, \varepsilon_{qm})_q^{-1} = (\varepsilon_{qm}, \alpha)_q$ . But by (4) all finite  $K \cap F$  primes which ramify in  $F_1$  are completely split in  $K(\varepsilon_{qm+a})$ . Since  $a > 0$ , then by [3, 2.4, p. 351] we have  $(\varepsilon_{qm}, \alpha)_q = 1$  at all finite  $K$ -primes  $q$  which ramify in  $L$ . Therefore  $(\alpha, \varepsilon_{qm})_q = 1$  for all finite  $K$ -primes  $q$ ; and so it remains to check for the infinite  $K$ -primes. Since  $\iota = 0$ , or  $\iota$  is odd then by [3, 2.9, p. 352] we have  $(\alpha, \varepsilon_{qm}) = 1$  for all infinite  $K$ -primes  $q$ . Hence  $(\alpha, \varepsilon_{qm})_q = 1$  for all  $K$ -primes  $q$ ; i.e.,  $\varepsilon_{qm}$  is in  $\eta^*$ . But  $\varepsilon_{qm+1}$  is not in  $K$ , so  $e \geq 1$ . Thus we have  $e + g - f - 2 \geq \ell + 1 \geq 1$ . Thus by the same reasoning as in (i) we get  $q^{\ell+1} | h(KF_1)$ , and  $q^{\ell+1} | h(KF)$ .

We note that Theorem 1.1 generalizes Watebe [11, Theorem 1]. To see this we isolate as a corollary a special case of Theorem 1.1. The above notation is in force.

**COROLLARY 1.2.** *Let  $K$  be a non-real algebraic number field containing  $\varepsilon_{qm}$  but not  $\varepsilon_{qm+1}$  for  $m \geq 1$  and let  $p$  be an odd prime completely split in  $K(\varepsilon_{qm+a})$  for  $a \geq 0$ . Then:*

(i) *For  $a = 0$ : if  $q = 2$  then  $q^{e-1} | h(K(\sqrt{p^*}))$  where  $p^* = (-1)^{(p-1)/2} p$ . If  $q \geq 2$  then  $q^{e-1} | h(K(\varepsilon_p))$ .*

(ii) *For  $a > 0$ : if  $\iota = 0$  or  $\iota$  is odd then if  $q = 2$  we have  $q^e | h(K(\sqrt{p^*}))$  and if  $q \geq 2$  then  $q^e | h(K(\varepsilon_p))$ .*

*Applications of Corollary 1.2.* (A) If  $q \geq 5$ ,  $p \equiv 1 \pmod{q}$  and  $K = \mathbf{Q}(\varepsilon_q)$  then  $q^{(q-3)/2} | h(\mathbf{Q}(\varepsilon_{pq}))$ . (This is [11, Theorem 1(A)].)

(B) If  $p \equiv 1 \pmod{9}$ , and  $K = \mathbf{Q}(\varepsilon_3)$  then  $3 | h(\mathbf{Q}(\varepsilon_{3p}))$ . (This is [11, Theorem 1(B)].)

(C) If  $r \geq 5$ ,  $p \equiv 1 \pmod{r}$  and  $K = \mathbf{Q}(\varepsilon_r)$  then  $2^{(r-3)/2} | h(\mathbf{Q}(\sqrt{p^*}, \varepsilon_r))$  and  $2^{(r-3)/2} | h(\mathbf{Q}(\varepsilon_{pr}))$ . (This is [11, Theorem 1(C)(I)].)

(D) If  $p \equiv 1 \pmod{8}$  and  $K = \mathbf{Q}(\sqrt{-1})$  then  $2 | h(\mathbf{Q}(\sqrt{p}, \sqrt{-1}))$  and  $2 | h(\mathbf{Q}(\varepsilon_{4p}))$ . (This is [11, Theorem 1(C)(II)].)

(E) If  $p \equiv 1 \pmod{12}$  and  $K = \mathbf{Q}(\varepsilon_3)$  then  $2 | h(\mathbf{Q}(\sqrt{p}, \varepsilon_3))$  and  $2 | h(\mathbf{Q}(\varepsilon_{3p}))$ . (This is [11, Theorem 1C(III)].)

Now we provide applications of Theorem 1.1 which cannot be obtained from the corollary.

*More applications.* (A) Let  $K = \mathbf{Q}$  and let  $F = F_1 = \mathbf{Q}(\sqrt{n})$  where  $n$  is a square-free integer. Assume that  $d$  finite primes ramify in  $F$  where  $d > 1$ . By Theorem 1.1(i) we have  $2^{d-2} | h(F)$ . Moreover, if we restrict all finite primes which ramify in  $F$  to being only primes congruent to 1 modulo 4 then we may apply Theorem 1.1(ii) to get  $2^{d-1} | h(F)$ .

These results are fundamental for quadratic fields (e.g., see [6, Section 3, p. V11-12]).

(B) Let  $K = \mathbf{Q}(\sqrt{m})$  where  $m < -1$  is a square-free integer, and let  $F = \mathbf{Q}(\sqrt{n})$  where  $n$  is a square free integer. Assume that all  $d$  finite primes which ramify in  $F$  are completely split in  $K$ . By Theorem 1.1(i) we have  $2^{2^{d-2}} | h(KF)$ . If we place a further restriction on the primes which ramify in  $F$ , viz., that they are all congruent to 1 modulo 4, then by Theorem 1.1(ii) we have  $2^{2^{d-1}} | h(KF)$ .

It is interesting to compare the results of (B) with those of (A).

(C) Let  $K$  be an algebraic number field containing  $\epsilon_q$  where  $q$  is a prime, and suppose that  $m$  is a  $q$ -power free integer divisible by at least two primes all of which are completely split in  $K$ . Let  $F = K(\sqrt[q]{m})$  then we may apply Theorem 1.1(i) to get  $q^{d-c-\iota-1} | h(F)$ .

In particular if  $K = \mathbf{Q}(\epsilon_q)$  then  $q^{d-(q-3)/2} | h(F)$ . We note that C. Parry and C. Walter [10, Theorem 8] have provided necessary and sufficient conditions for  $h(F)$  to be relatively prime to  $q$  for  $q > 2$ . Some of the conditions are that  $m$  is divisible by no more than two primes, and that the order of any  $p|m$ ,  $p \neq q$ , must be non-trivial modulo  $q$ . We note that in our case if  $m$  is divisible by exactly two primes then the orders of these primes are trivial modulo  $q$ .

**THEOREM 1.2.** *Let  $K$  be a cyclic extension of  $k$  of  $p$ -power degree where  $p$  is a prime and assume that if  $k \neq K$  then exactly one  $k$ -prime ramifies in  $K$  and that this prime is in fact totally ramified in  $K$ . Suppose that  $q = 1 + 2p^t$ ,  $t \geq 0$  is a prime, and assume that  $q$  has only one  $K$ -prime above it. Then the following are equivalent (i)  $p | h(k)$ , (ii)  $p | h(K)$ , and (iii)  $p | h(K(\epsilon_q + \epsilon_q^{-1}))$ . Moreover, if  $p = 2$  and  $K$  is totally non-real, i.e.,  $\iota = 0$ , then the following are equivalent: (i)  $2 | h(k)$ , (ii)  $2 | h(K)$ , and (iii)  $2 | h(K(\epsilon_q))$ .*

*Proof.* (a) If  $p | h(K(\epsilon_q + \epsilon_q^{-1}))$  then, since  $|K(\epsilon_q + \epsilon_q^{-1}) : K|$  is a  $p$ -power and only the  $K$ -prime above  $q$  ramifies in  $K(\epsilon_q + \epsilon_q^{-1})$ , we get  $p | h(K)$  from [7, II]. Since exactly one  $k$ -prime ramifies in  $K$  then we use [7, II] again to get  $p | h(k)$ . Conversely, if  $p | h(k)$  then  $p | h(K)$  by [7, I]; and  $p | h(K)$  implies  $p | h(K(\epsilon_q + \epsilon_q^{-1}))$  by [7, I] again. (b) If  $2 | h(K(\epsilon_q))$  then since  $K$  is non-real and  $q$  is a Fermat prime above which there is only one prime in  $K$  then  $2 | h(k)$  by [7, II], as in (i)  $2 | h(k)$ .

Conversely  $2 | h(k)$  implies  $2 | h(K(\epsilon_q))$  as in (i).

We note that one direction of Theorem 1.2 for  $p = 2$  is similar to [11, Theorem 2]. However, the latter is false. Here is a counterexample. Let  $K = \mathbf{Q}(\epsilon_{29})$ ,  $k = \mathbf{Q}(\epsilon_{29} + \epsilon_{29}^{-1})$ , and  $q = 3$  in [11, Theorem 2]. By Bauer [1],  $h(k) = 1$ , and since 3 is inert in  $K$  then by Watabe's theorem we get  $2 \nmid h(K(\epsilon_3))$ . However,  $2 | h(\mathbf{Q}(\epsilon_{29}))$ . In fact  $h(\mathbf{Q}(\epsilon_{29})) = 8$  (see [2, p. 429]).

Since the  $K$ -prime above 3 is totally ramified in  $K(\varepsilon_3)$  then by Theorem 1.2,  $2|h(K(\varepsilon_3))$ , contradicting Watabe. The error in Watabe's proof [11, p. 215] stems from ignoring the possibility of having an infinite prime ramify *as well as* a finite prime, thus invalidating Watabe's use of Iwasawa [7, II]. The theorem, however, will hold if  $k$  is restricted to being non-real. Moreover, we note that as a result of the above then [11, Example II] is false as well. (Take  $K$  to be the subfield of  $\mathbf{Q}(\varepsilon_{29})$  of degree 4 over  $\mathbf{Q}$ , and take  $q = 5$ . Then by [7, I],  $2|h(K)$  implies  $2|h(K(\varepsilon_5))$ .)

*Applications of Theorem 1.2.* (I) Let  $q = 1 + 2p^t$ ;  $t \geq 0$  be a prime where  $p$  is a prime then by Theorem 1.2,  $p \nmid h(\mathbf{Q}(\varepsilon_q + \varepsilon_q^{-1}))$ . (Take  $K = \mathbf{Q}(\varepsilon_q + \varepsilon_q^{-1})$  and  $k = \mathbf{Q}$ .)

In particular if  $p = 2$ , i.e.,  $q$  is a Fermat prime, then  $2 \nmid h(\mathbf{Q}(\varepsilon_q + \varepsilon_q^{-1}))$ .

(II) Now we use Theorem 1.2 to show that  $2 \nmid h(\mathbf{Q}(\varepsilon_q))$  for  $q = 1 + 2^t$ . When  $t = 1$  the result is well known. We assume  $t > 1$ . Let  $p$  be a prime such that  $p \equiv 3 \pmod{4}$  and  $p \equiv g \pmod{q}$  where  $g$  is a primitive root modulo  $q$ . Such a prime exists by the Chinese remainder theorem and Dirichlet's theorem on primes in arithmetic progression. Since  $p \equiv 3 \pmod{4}$  then  $2 \nmid h(\mathbf{Q}(\sqrt{-p}))$  (see [2, Theorem 4, p. 346]). Since  $p$  is a primitive root modulo  $q > 3$  then  $q$  is inert in  $\mathbf{Q}(\sqrt{-p})$ . Thus the  $\mathbf{Q}(\sqrt{-p})$ -prime above  $q$  is the only such prime ramified in  $\mathbf{Q}(\varepsilon_q, \sqrt{-p})$ . By Theorem 1.2 we have  $2 \nmid h(\mathbf{Q}(\varepsilon_q, \sqrt{-p}))$ . Since  $p$  is a primitive root modulo  $q$  then only the  $\mathbf{Q}(\varepsilon_q)$ -prime above  $p$  ramifies in  $\mathbf{Q}(\varepsilon_q, \sqrt{-p})$ . Thus by Theorem 1.2,  $2 \nmid h(\mathbf{Q}(\varepsilon_q))$ .

(III) Let  $K = \mathbf{Q}(\varepsilon_4(\varepsilon_2 s + 3 + \varepsilon_2^{-1} s + 3))$  where  $s \geq 0$ . Then  $K$  is a non-real subfield of  $\mathbf{Q}(\varepsilon_2 s + 3)$ . We claim  $2 \nmid h(K)$ . Suppose  $2 \mid h(K)$ . Then by Theorem 1.2,  $2 \mid h(\mathbf{Q}(\varepsilon_2 s + 3))$ . However, this is known to be false (see Weber [10]). Thus  $2 \nmid h(K)$ . Let  $q$  be any Fermat prime inert in  $K$ . Then by Theorem 1.2,  $2 \mid h(K(\varepsilon_q))$ .

(IV) We conclude by noting that the following result is immediate from Theorem 1.2.

Let  $K_n = \mathbf{Q}(\varepsilon_p n + 1)$  where  $p$  is an odd prime, and  $n \geq 0$ . Then  $p \mid h(K_0)$  if and only if  $p \mid h(K_n)$ .

This result was first proved by Furtwangler in 1911 as an extension of Weber's theorem (*ibid.*) for the odd prime case.

## 2. A GENERALIZED FERMAT THEOREM

Fermat's "two-square theorem" says that a prime  $q$  is expressible as the sum of two squares if and only if  $-1$  is a quadratic residue modulo  $q$  (see

[4]). It can be shown that for an arbitrary positive integer  $n$  this extends to the following, which we will have occasion to prove later.

(2.1) If  $(x^2 + 1) \equiv 0 \pmod{n}$  is solvable for some integer then  $n = a^2 + b^2$  for some integers  $a$  and  $b$ .

(2.2) Conversely, if  $n = a^2 + b^2$  with  $a$  and  $b$  being relatively prime then  $x^2 + 1 \equiv 0 \pmod{n}$  is solvable for some integer.

We wish to generalize (2.1) from the  $p - 2$  case to the case of an arbitrary prime  $p$ . In proving (2.1) the following fact may be used.

(2.3)  $x^2 + 1 \equiv 0 \pmod{n}$  is solvable for some integer if and only if  $n \not\equiv 0 \pmod{4}$  and all primes  $q$  dividing  $n$  satisfy either  $q \equiv 1 \pmod{4}$  or  $q = 2$ .

It is natural therefore to generalize (2.3) first. We isolate this result since it is of independent interest and we are able to apply the results of Section 1 to obtain a corollary which yields additional information.

In what follows  $\phi_k(x)$  shall denote the  $k$ th cyclotomic polynomial. In particular we shall be interested in case  $k = 2p$ ; i.e.,  $\phi_{2p}(x) = x^{p-1} - x^{p-2} + x^{p-3} - \dots - x + 1$  for  $p > 2$ , and  $\phi_{2p}(x) = x^2 + 1$  for  $p = 2$ .

**THEOREM 2.4.** *Let  $n$  be a fixed positive integer and let  $p$  be a prime: then the following are equivalent:*

- (1)  $\phi_{2p}(x) \equiv 0 \pmod{n}$  is solvable for some integer.
- (2) All primes  $q$  dividing  $n$  are such that  $q \equiv 1 \pmod{2p}$  or  $q = p$ . If  $p = q$  then  $p^2 \nmid n$ .
- (3) All finite primes which ramify in  $\mathbf{Q}(\epsilon_n)$  are either completely split or ramified in  $\mathbf{Q}(\epsilon_{2p})$ .

*Proof.* The equivalence of (2) and (3) is well known (e.g., see [8, pp. 39–48]), so we prove only the equivalence of (1) and (2). The equivalence of (1) and (2) is also known but we include a proof for lack of a convenient reference.

First assume (1). Then  $m^{2p} \equiv 1 \pmod{n}$  since  $m^{2p} - 1 = \phi_{2p}(m) \cdot \phi_p(m) \cdot (m^2 - 1)$ . Thus  $m^{2p} \equiv 1 \pmod{q}$  for all primes  $q$  dividing  $n$ . Therefore the order,  $d$ , of  $m$  modulo  $q$  is a divisor of  $2p$ . By (1),  $d \neq 1$  unless possibly  $p = 2$  in which case  $q = p$ . If  $d = 2$  then by (1)  $q = p$ . If  $d = p$  then  $q \equiv 1 \pmod{p}$  and so  $q \equiv 1 \pmod{2p}$  for  $p > 2$ , whereas if  $p = 2$  then by (1)  $q = p = 2$ . If  $d = 2p$  then  $q \equiv 1 \pmod{2p}$ . If  $p = q$  then if  $\phi_2(m)$  is exactly divisible by  $p^a$  it follows that  $\phi_2(m^p)$  is exactly divisible by  $p^{a+1}$ . However,  $\phi_{2p}(m) = \phi_2(m^p)/\phi_2(m)$  so  $p^2 \nmid n$ .

Conversely, assume (2); i.e.,  $n = p^{a_0} q_1^{a_1} \dots q_r^{a_r}$  where  $q_i \equiv 1 \pmod{2p}$  for all  $i = 1, 2, \dots, r$  and  $a_i \geq 1$  for  $i = 1, \dots, r$ ; and  $a_0 \leq 1$ . From the Chinese remainder theorem it follows that it suffices to find an integer solution to  $\phi_{2p}(x) \equiv 0 \pmod{q_i^{a_i}}$  for  $i = 1, 2, \dots, r$ . Let  $m_i$  be an integer of order  $2p$

modulo  $q_i^{a_i}$ . Then  $m_i^{2p} \equiv 1 \pmod{q_i^{a_i}}$ . By the choice of  $m_i$  we have that  $q_i$  and  $\phi_p(m_i) \cdot (m_i^2 - 1)$  are relatively prime. Thus

$$\frac{m_i^{2p} - 1}{\phi_p(m_i)(m_i^2 - 1)} = \phi_{2p}(m_i) \equiv 0 \pmod{q_i^{a_i}}.$$

Now if  $q = p$  then by hypothesis  $a_0 = 1$  and so we choose an integer  $m_0$  such that  $m_0 \equiv -1 \pmod{p}$ . Therefore we have  $\phi_{2p}(m_0) \equiv 0 \pmod{p}$ .

The following result links the results of Section 1 with the above known result.

**COROLLARY 2.5.** *If  $\phi_{2p}(x) \equiv 0 \pmod{n}$  has an integer solution then for all primes  $q \neq p$  dividing  $n$  we have  $p^{(p-3)/2} | h(\mathbf{Q}(\varepsilon_{pq}))$  for  $p > 2$  (respectively,  $p | h(\mathbf{Q}(\varepsilon_{p^2q}))$  for  $p = 2$ ).*

*Proof.* By the equivalence of (1) and (3) in Theorem 2.4 we have that the hypothesis of Corollary 1.2 is satisfied. The result follows.

The following theorem generalizes Fermat’s “two-square theorem.”

**THEOREM 2.6.** *Suppose  $\phi_{2p}(x) \equiv 0 \pmod{n}$  has an integer solution and  $h(\mathbf{Q}(\sqrt{p^*})) = 1$  where  $p = p^*$  for  $p > 2$  and  $p^* = -1$  for  $p = 2$ . Moreover, if  $p > 2$  and  $q$  is a prime dividing  $n$  with  $q \equiv 3 \pmod{4}$  then  $q$  appears to an even exponent in  $n$ , then we have  $n = a^2 - p^*b^2$  where  $a$  and  $b$  are integers.*

*Proof.* It suffices to show that  $q = a^2 - p^*b^2$  for each prime  $q$  dividing  $n$  since we have that

$$(c^2 - p^*d^2)(e^2 - p^*f^2) = (ce - p^*df)^2 - p^*(de - cf)^2.$$

However, since  $\phi_{2p}(x) \equiv 0 \pmod{n}$  is solvable for some integer then by Theorem 2.4 we have that all primes dividing  $n$  are congruent to 1 modulo  $2p$  or equal to  $p$ . If  $q | n$  such that  $q \equiv 1 \pmod{2p}$  and  $q \equiv 1 \pmod{4}$  then  $n(q) = N(a + \sqrt{p^*}b) = a^2 - p^*b^2 = q$  where  $q$  is a  $\mathbf{Q}(\sqrt{p^*})$ -prime above  $q$ , and  $q = (a + \sqrt{p^*}b)$  since  $h(\mathbf{Q}(\sqrt{p^*})) = 1$ , with  $a + \sqrt{p^*}b$  an element of the ring of integers of  $\mathbf{Q}(\sqrt{p^*})$ . If  $p \equiv 3 \pmod{4}$  then  $a$  and  $b$  are integers. If  $p \equiv 1 \pmod{4}$  then  $2a$  and  $2b$  are integers. Assume in this case that  $a = c/2$  and  $b = d/2$ . Then  $4 \equiv 4q \equiv c^2 \pmod{4p}$  which implies that  $c$  is even; and so  $d$  is even. This completes the case  $q \equiv 1 \pmod{2p}$  and  $q \equiv 1 \pmod{4}$ .

By hypothesis, if  $q \equiv 3 \pmod{4}$ ,  $q \equiv 1 \pmod{2p}$  and  $p > 2$ , then  $q$  appears to exponent  $2a$ , say. Thus in this case  $q^{2a} = (q^a)^2 - p^*0^2$ .

Finally, if  $q = p$  then for  $p > 2$  we have by Theorem 2.4 that  $q \equiv 1 \pmod{4}$ . Then  $p = (pa)^2 - pb^2$  where  $b^2 - pa^2 = -1$  for integers  $a$  and  $b$ . If  $p = 2$  then  $p = 1^2 + 1^2$ .

We note that the converse of Theorem 2.6 fails. Here are counterexamples:

Let  $p$  be a prime with  $h(\mathbf{Q}(\sqrt{p})) = 1$ , and let  $n = a^2 - pb^2$  where  $p > 3$

and  $a^2 \not\equiv 1 \pmod{2p}$ . For  $p = 3$  take  $n = 54 = 9^2 - 3 \cdot 3^2$ . Clearly  $q \not\equiv 1 \pmod{2p}$  for each prime  $q$  dividing  $n$  where  $p > 3$ , and  $2 \not\equiv 1 \pmod{3}$  where  $2|n$  for  $p = 3$ . Therefore by Theorem 2.4 we have that  $\phi_{2p}(x) \equiv 0 \pmod{n}$  does not have an integer solution. This means that we cannot generalize (2.2) to the  $p > 2$  case. The reason for this becomes clear when we examine Theorem 2.4. The only primes  $p$  for which the converse of Theorem 2.6 could hold would be those primes  $p$  such that  $q \equiv 1 \pmod{2p}$  for all primes  $q \neq p$  dividing a given  $n$ .

There are only two primes for which all quadratic residues are congruent to 1 modulo  $2p$ , namely,  $p = 2, 3$ . The  $p = 2$  case is (2.2). The  $p = 3$  case requires a slight restriction. We combine the two cases in the following result which provides a form of the converse of Theorem 2.6 which holds, and provides a short straightforward proof of (2.2) as well.

**LEMMA 2.7.** *If  $n = a^2 + b^2$  (respectively, if  $n = a^2 + 3b^2$  with  $2|a$ ) such that  $(a, b) = 1$  then  $\phi_{2p}(x) \equiv 0 \pmod{n}$  has an integer solution, for  $p = 2$  (respectively,  $p = 3$ ).*

*Proof.* We have  $p^* \equiv a^2/b^2 \pmod{q}$  for all primes  $q$  dividing  $n$ , where  $p^* = -1$  for  $p = 2$  and  $p^* = -3$  for  $p = 3$ .  $(b, 2) = 1$  can be assumed in either case and since  $(a, b) = 1$  then  $(b, q) = 1$  so we may invoke [3, 1.5, p. 349] to get that  $p^*$  is a square in  $\mathbf{Q}_q$ , the completion of  $\mathbf{Q}$  at  $q$ , for all primes  $p \neq 2, p$ . Thus  $\mathbf{Q}_q = \mathbf{Q}_q(\sqrt{p^*})$  for all  $q \neq 2, p$  dividing  $n$ . Since  $n$  must be odd for  $p = 2$  or 3 then we have shown that all  $q$  dividing  $n$  are congruent to 1 modulo  $2p$ , or  $q = p$ . We may invoke Theorem 2.4 to secure the result.

Although Lemma 2.7 gives us conditions for an integer solution to  $\phi_4(x) \equiv 0 \pmod{n}$  and  $\phi_6(x) \equiv 0 \pmod{n}$  it does not explicitly give us the solution. We conclude therefore with a method of determining such explicit solutions. We shall provide the details for the determination of solutions to  $\phi_3(x) \equiv 0 \pmod{n}$ , under minor restrictions. The calculation for  $\phi_4(x) \equiv 0 \pmod{n}$  and  $\phi_6(x) \equiv 0 \pmod{n}$  is similar. We leave this as an exercise for the reader.

**THEOREM 2.8.** *Let  $n = a^2 + 3b^2$  where  $(a, b) = 1$ . If 2 does not divide  $cd$  where  $bd - ac = 1$  and  $2|ab$  then  $m = (1 + 3bc + ad)/2$  is an integer solution to  $\phi_3(x) \equiv 0 \pmod{n}$ .*

*Proof.* Consider the following matrix product:

$$\begin{pmatrix} 2b & b-a \\ -c & \frac{d-c}{2} \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{d-c}{2} & a-b \\ c & 2b \end{pmatrix}$$

$$= \begin{pmatrix} \frac{ac - bd - 3bc - ad}{2} & -a^2 - 3b^2 \\ \frac{d^2 + 3c^2}{4} & \frac{ac - bd + 3bc + ad}{2} \end{pmatrix}$$

$$\begin{pmatrix} \frac{-1 - 3bc - ad}{2} & -n \\ \frac{d^2 + 3c^2}{4} & \frac{-1 + 3bc + ad}{2} \end{pmatrix}$$

since  $bd - ac = 1$ .

By hypothesis  $m = (1 + 3bc + ad)/2$  and  $k = (d^2 + 3c^2)/4$  are integers. Thus the matrix product equals  $\begin{pmatrix} -m & n \\ k & m+1 \end{pmatrix}$ . Clearly the determinants of  $\begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} -m & n \\ k & m+1 \end{pmatrix}$  are equal so  $1 = -m(m+1) + kn$ ; i.e.,  $\phi_3(m) = m^2 + m + 1 \equiv 0 \pmod{n}$ .

EXAMPLE. Let  $p$  be any prime congruent to 3 modulo 4. Then if  $n = p^2 + 3 \cdot 2^2$  we have  $((1-p)/2) \cdot 2 - (-1)p = 1$  so  $a = p$ ,  $b = 2$ ,  $c = -1$ , and  $d = (1-p)/2$ . Thus  $m = -((p^2 - p + 10)/4)$  by Theorem 2.8 and  $m$  is an integer solution to  $\phi_3(x) \equiv 0 \pmod{n}$ .

#### REFERENCES

1. H. BAUER, Numerische Bestimmung von Klassenzahlen reeler zyklischen Zahlkörper, *J. Number Theory* 1 (1969), 161-162.
2. Z. I. BOREVICH AND I. R. SHAFAREVICH, "Number Theory," Academic Press, New York, 1966.
3. J. W. S. CASSELS AND A. FRÖHLICH, "Algebraic Number Theory," Proceedings of an Instructional Conference (Brighton 1965), Academic Press, New York, 1967.
4. G. H. HARDY AND E. M. WRIGHT, "Introduction to the Theory of Numbers," Oxford Univ. Press (Clarendon), London, 1960.
5. H. HASSE, "Bericht über Neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper," Physica-Verlag, Wurzburg/Wien, 1970.
6. C. S. HERTZ, "Seminar on Complex Multiplication," Lecture Notes in Mathematics, No. 21, Springer-Verlag, Berlin, 1966.
7. K. IWASAWA, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* 20 (1956), 257-258.
8. G. J. JANUSZ, "Algebraic Number Fields," Academic Press, New York, 1973.
9. M. MORIYA, Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrad, *Proc. Imper. Acad. Japan* 6 (1930), 245-247.

10. C. PARRY AND C. WALTER, The class number of pure fields of prime degree, *Mathematika* **23** (1976), 220–226.
11. M. WATABE, On class numbers of some cyclotomic fields, *J. Reine Angew. Math* **301** (1978), 212–215.
12. H. WEBER, “Lehrbuch der Algebra,” Vol. II, 2nd ed. Braunschweig, 1899. Reprinted, Chelsea, New York, 1966.