

**Necessary and Sufficient Conditions for the Class Number of a Real Quadratic Field to be One, and a Conjecture of S. Chowla**



R. A. Mollin

*Proceedings of the American Mathematical Society*, Vol. 102, No. 1 (Jan., 1988), 17-21.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9939%28198801%29102%3A1%3C17%3ANASCFT%3E2.0.CO%3B2-V>

*Proceedings of the American Mathematical Society* is currently published by American Mathematical Society.

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/ams.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

---

JSTOR is an independent not-for-profit organization dedicated to creating and preserving a digital archive of scholarly journals. For more information regarding JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).

NECESSARY AND SUFFICIENT CONDITIONS  
FOR THE CLASS NUMBER OF A REAL QUADRATIC FIELD  
TO BE ONE, AND A CONJECTURE OF S. CHOWLA

R. A. MOLLIN

(Communicated by Larry J. Goldstein)

ABSTRACT. Based on the fundamental unit of  $Q(\sqrt{n})$ , an arbitrary real quadratic field, we provide a necessary condition for the class number  $h(n)$  to be 1. For  $n = 4m^2 + 1$  we prove the equivalence of three necessary and sufficient conditions for  $h(n)$  to be 1. One of these conditions is that  $-x^2 + x + m^2$  is prime for all integers  $x$  such that  $1 < x < m$ . This is the exact analogue of the complex quadratic field case. We discuss the connection with a conjecture of S. Chowla as well as with other related topics.

**1. Introduction.** In [3] S. Chowla conjectured that if  $p = m^2 + 1$  is prime with  $m > 26$  then  $h(p) > 1$ . First we note that there are only finitely many such fields with  $h(p) = 1$ . To see this we observe that the fundamental unit of  $Q(\sqrt{p})$  is  $m + \sqrt{p}$  (see [5 and 14]). Thus the Brauer-Siegel Theorem yields

$$\frac{\log(h(p) \cdot \log(m + \sqrt{p}))}{\log \sqrt{p}} \rightarrow 1 \quad \text{as } p \rightarrow \infty.$$

However  $\log(m + \sqrt{p}) < (\log 2\sqrt{p})$  from which it follows that  $h(p) \rightarrow \infty$  as  $p \rightarrow \infty$ . Thus we are concerned with effectively determining such  $p$  with  $h(p) = 1$ .

It follows from general results proved in Mollin [9] that if  $n = m^2 + 1 > 17$  is square-free and  $m \neq 2q$  for an odd prime  $q$  then  $h(n) > 1$ , (see also [10 and 11]). In this paper the equivalent conditions for class number 1 which we provide allow us to reduce to the case where  $4q^2 + 1$  is prime and  $q$  is an odd prime. The reduction to the  $n = \text{prime}$  case was known to Gauss via genus theory. However in this paper we use only the most *elementary* techniques to establish the result, (Corollary 2). The reduction to the case where  $m = 2q$ ,  $q > 2$  prime, is also known, (see [2, p. 48] for example). However we again use only elementary techniques in the proof, (Corollary 1). For primes of the form  $m^2 + 1 = p$ , S. Chowla and J. Friedlander [3] also reduced to the  $m = 2q$  case; and in [4] they proved that, under a suitable hypothesis for  $L$ -functions,  $h(p) > 1$  for large enough  $p$ . Also F. Callialp [2] used analytic techniques to prove that for  $m \equiv 0 \pmod{4}$ ,  $h(n) = 1$  for only finitely many  $n = m^2 + 1$ . However, as noted above the results in Mollin [9] say more specifically that there is *exactly one* such square-free  $n$  for which  $h(n) = 1$ , namely  $n = 17$ . Moreover the algebraic techniques of proof used in Mollin [9] are far more straightforward. We show herein that the Callialp result is an immediate

---

Received by the editors April 15, 1986 and, in revised form, September 2, 1986.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 12A50, 12A25; Secondary 10B05.

*Key words and phrases.* Class number 1, real quadratic field, prime valued polynomial.

consequence of the criteria for class number 1 which we provide by elementary techniques. In any case the Chowla conjecture remains open for the  $m = 2q$  case. We provide strong evidence for the validity of the Chowla conjecture by showing that the remaining case is tantamount to  $-x^2 + x + q^2$  being prime for all integers  $x$  with  $1 < x < q$ . This provides a real quadratic field version of the complex quadratic field case proved by G. Rabinovitch [13]. Finally we submit several related conjectures.

**2. Criteria for class number 1.** In [7] M. Kutsuna proved that class number 1 for an arbitrary real quadratic field is tantamount to the nonexistence of so-called störend fractions. However it is virtually impossible to verify this condition for a given real quadratic field. For the case under consideration herein, the criteria in Theorem 1 are more elementary and we are able to improve upon Kutsuna's results to a certain extent. For example, Kutsuna [7, Corollary 1°, p. 127] shows that if  $n = 1 + 4m$  is square-free and  $-x^2 + x + m$  is prime for all integers  $x$  such that  $1 \leq x < \sqrt{m}$  then  $h(n) = 1$ . For the case  $m = q^2$ , Kutsuna's result does not, therefore, apply. Moreover, Kutsuna [7, Corollary 2°, p. 127] shows that if  $n = 1 + 4m$  where  $m$  is odd and the Legendre symbol  $(n/p) = -1$  for every prime  $p$  such that  $2 < p \leq \sqrt{m}$  then  $h(n) = 1$ . Again for our case  $m = q^2$ , Kutsuna's result does not apply. Theorem 1 herein eliminates these problems. Furthermore the result gives us the analogue of:  $x^2 + x + (p+1)/4$  is prime for  $0 \leq x \leq (p-7)/4$  with  $p \equiv 1 \pmod{4}$  and  $p > 5$  if and only if  $h(-p) = 1$ , (see H. Stark [15], D. Lehmer [8], and G. Rabinovitch [13]; as well as R. Ayoub and S. Chowla [1] for an elegant proof of the necessity).

We begin now by providing a necessary condition to achieve class number 1 for an arbitrary real quadratic field, and then use it to prove the main result.

**LEMMA 1.** *Let  $n$  be a square-free positive integer,  $\sigma = 2$  if  $n \equiv 1 \pmod{4}$  and  $\sigma = 1$  otherwise. Suppose that  $(A + B\sqrt{n})/\sigma$  is the fundamental unit of  $K = \mathbb{Q}(\sqrt{n})$  and  $N((A + B\sqrt{n})/\sigma) = \delta$  where  $N$  is the norm from  $K$  to  $\mathbb{Q}$ . If  $h(n) = 1$  then  $p$  is inert in  $K$  for all primes  $p < ((2A/\sigma) - \delta - 1)/B^2$ .*

**PROOF.** Let  $p < ((2A/\sigma) - \delta - 1)/B^2$  be a prime which is not inert in  $K$ . If  $h(n) = 1$  then there are integers  $x$  and  $y$  such that  $x^2 - ny^2 = \pm\sigma^2p$ . By Mollin [9, Lemma 1.1, p. 40] this equation implies  $p \geq ((2A/\sigma) - \delta - 1)/B^2$ , a contradiction. Q.E.D.

**THEOREM 1.** *Let  $n = 4m^2 + 1$  be square-free where  $m$  is a positive integer. Then the following are equivalent.*

- (1)  $h(n) = 1$ .
- (2)  $p$  is inert in  $K = \mathbb{Q}(\sqrt{n})$  for all primes  $p < m$ .
- (3)  $f(x) = -x^2 + x + m^2 \not\equiv 0 \pmod{p}$  for all integers  $x$  and primes  $p$  satisfying  $0 < x < p < m$ .
- (4)  $f(x)$  is equal to a prime for all integers  $x$  satisfying  $1 < x < m$ .

**PROOF.** That (1) implies (2) is a special case of Lemma 1 with  $A = 4m$ ,  $B = 2$ ,  $\delta = -1$  and  $\sigma = 2$ , (see C. Richaud [14] and G. Degert [5]).

Suppose that  $f(x) \equiv 0 \pmod{p}$  for some integer  $x$  and some prime  $p$  satisfying  $0 < x < p < m$ . Thus,  $n \equiv (2x - 1)^2 \pmod{4p}$ , whence  $p$  is either ramified or split in  $K$ . Hence (2) implies (3).

Assume (3) holds. Suppose  $m$  is composite and  $q$  is a prime dividing  $m$ . If  $x = 1$  then  $f(x) \equiv 0 \pmod{q}$  with  $0 < x < q < m$ , a contradiction. Therefore we assume that  $m$  is prime.

Suppose that  $f(x)$  is composite for some integer  $x$  with  $1 < x < m$ . Therefore there are primes  $p_1$  and  $p_2$  (not necessarily distinct) such that  $f(x) \equiv 0 \pmod{p_1 p_2}$ . If  $p_i$  divides  $x$  for  $i \in \{1, 2\}$  then  $p_i$  divides  $m$ , whence  $m = p_i$ , a contradiction to  $1 < x < m$ . Therefore there exists an integer  $x_i$  with  $0 < x_i < p_i$  such that  $x \equiv x_i \pmod{p_i}$  and  $f(x) \equiv 0 \pmod{p_i}$ . Now, if  $p_1 p_2 > m^2$  then  $-x^2 + x + m^2 > m_2$  forcing  $x < 1$  a contradiction. Thus, without loss of generality we may assume that  $p_1 < m$ . Hence we have that  $f(x) \equiv -x_1^2 + x_1 + m^2 \equiv 0 \pmod{p_1}$  for  $0 < x_1 < p_1 < m$ , which violates (3). Hence (3) implies (4).

Finally assume (4) holds. If  $h(n) > 1$  then by Kutsuna [7, Propositions 3 and 4, p. 126] there exist an integer  $x$  and a prime  $p$  with  $0 \leq x < p \leq m$  such that both:

(a)  $N((2x - 1 - \sqrt{n})/2) \equiv 0 \pmod{p}$ , and

(b) there does not exist an integer  $k$  such that  $|N((2x + 2kp - 1 - \sqrt{n})/2)| < p^2$ .

Now, (a) implies that  $-x^2 + x + m^2 \equiv 0 \pmod{p}$ . If  $1 < x < m$  then (4) implies  $-x^2 + x + m^2 = p$ . However  $x < m$  implies that  $x(1 - x) > m(1 - m)$ ; i.e.,  $-x^2 + x + m^2 > m$ , whence  $p > m$ , a contradiction. Hence  $x \in \{0, 1\}$ , whence  $p$  divides  $m$ . Therefore  $f(p) = p(-p + 1 + m^2/p)$ . By (4)  $m = p$  is forced. Now let  $k = 1$  in (b) to get

$$p^2 \leq |N((2p \pm 1 - \sqrt{n})/2)| = |(4p^2 \pm 4p + 1 - n)/4| = p$$

a contradiction. Hence (4) implies (1). Q.E.D.

**COROLLARY 1.** *If  $n = 4m^2 + 1$  is square-free where  $m$  is composite then  $h(n) > 1$ .*

**PROOF.** Let  $p$  divide  $m$  which is composite. If  $x = 1$  in (3) then the result follows. Q.E.D.

**COROLLARY 2.** *If  $n = 4m^2 + 1$  is a square-free composite number then  $h(n) > 1$ .*

**PROOF.** If  $n$  is divisible by more than two primes then clearly at least one of these primes is less than  $m$ , say  $p$ . Let  $x = (p + 1)/2$  in (3) and the result follows. Therefore we may assume that  $n = rs$  where  $r$  and  $s$  are primes. We claim that one of  $r$  or  $s$  is less than  $2m - 1$ . If both  $r$  and  $s$  are bigger than or equal to  $2m - 1$  then they must both be larger than  $2m$ . Otherwise one of them,  $r$  say, equals  $2m - 1$ . Therefore  $(2m - 1)s = 4m^2 + 1 = (2m - 1)(2m + 1) + 2$ , whence  $m = 1$  a contradiction. Now, since both  $r$  and  $s$  are larger than or equal to  $2m + 1$  we have  $n = rs \geq 4m^2 + 4m + 1$  a contradiction, and the claim is secured. Hence, without loss of generality we may assume that  $r < 2m - 1$ . Let  $x = (r + 1)/2$ , then  $4f(x) = n - r^2 = r(s - r)$ . By (4), if  $h(n) = 1$ , then  $f(x) = r$  and  $s - r = 4$ . However  $rs = 4m^2 + 1$  so  $r(4 + r) = 4m^2 + 1$ ; i.e.,  $r^2 + 4r - 4m^2 - 1 = 0$ . Therefore  $r = -2 + \sqrt{4m^2 + 5}$  by the quadratic formula. Hence  $4m^2 + 5$  is a square which forces  $m = 1$ , a contradiction. Q.E.D.

Callalp's result [2] that  $h(n) = 1$  for at most finitely many  $n$  when  $m \equiv 0 \pmod{2}$  is immediate (and more specific) from the above in that only  $h(17) = 1$ . In view of Corollaries 1 and 2 we have reduced to the situation where  $4q^2 + 1$  is prime and  $q$  is prime. The case  $q = 2$  yields  $h(17) = 1$  which follows vacuously from Theorem 1.

In view of the above and Chowla's conjecture we make the following conjectures. First we preface the conjectures by

ASSUMPTION.  $p = 4q^2 + 1$  is prime and  $q$  is an odd prime.

CONJECTURE 1.  $-x^2 + x + q^2$  is prime for all integers  $x$  satisfying  $1 < x < q$  if and only if  $q \leq 13$ .

CONJECTURE 2. All odd primes  $r < q$  are inert in  $Q(\sqrt{p})$  if and only if  $q \leq 13$ .

CONJECTURE 3.  $-x^2 + x + q^2 \not\equiv 0 \pmod{r}$  for all integers  $x$  and primes  $r$  satisfying  $0 < x < r < q$  if and only if  $q \leq 13$ .

It is easy to verify one direction of Conjectures (1)–(3). The results are tabulated in the following:

TABLE 1			
$q$	$p$	$(-x^2 + x + q^2, x)$	inert $r < q$
3	37	(7, 2)	2
5	101	(23, 2), (19, 3), (13, 4)	2, 3
7	197	(47, 2), (43, 3), (37, 4), (29, 5), (19, 6)	2, 3, 5
13	677	(167, 2), (163, 3), (157, 4), (149, 5), (139, 6), (127, 7), (113, 8), (97, 9), (79, 10), (59, 11), (37, 12)	2, 3, 5, 7, 11

In [6], Hongwen has given a criteria for class number 1 in terms of the zeta function  $\zeta_F$  of a field  $F$ . In view of this result we have for  $F = Q(\sqrt{p})$ .

CONJECTURE 4.

$$2\zeta_F(-1) = q(2q^2 + 7)/45$$

if and only if  $q \leq 13$ .

Finally we conclude with the observation that in view of the equivalence of (1) and (2) in Theorem 1 it would be valuable to have an effective bound for the least prime quadratic residue. However the known bounds in the literature are ineffective (for example see J. Pintz [12]).

ACKNOWLEDGEMENT. The author wishes to thank the referee for suggestions.

NOTE ADDED IN PROOF. Since the writing of this paper substantial progress has been made. The author and H. C. Williams, in another paper to appear in the Proceedings of the American Mathematical Society, have used a suitable Riemann hypothesis to verify the Chowla conjecture under consideration in this paper. Moreover, in subsequent work, the author and H. C. Williams have invoked a suitable Riemann hypothesis to determine *all* real quadratic fields of *Richaud-Degert* type which have *class number one*. Moreover they established a strong connection between the class number one problem and certain prime-producing polynomials.

#### REFERENCES

1. R. G. Ayoub and S. Chowla, *On Euler's polynomial*, J. Number Theory **13** (1981), 443–445.
2. F. Callialp, *Non-nullité des fonctions zeta des corps quadratiques réels pour  $0 < s < 1$* , C. R. Acad. Sci. Paris Sér. A-B **291** (1980), A623–A625.
3. S. Chowla and J. Friedlander, *Class numbers and quadratic residues*, Glasgow Math. J. **17** (1976), 47–52.
4. ———, *Some remarks on L-functions and class numbers*, Acta Arith. **28** (1975/76), 413–417.

5. G. Degert, *Über die Bestimmung der Grundeinheit gewisser reellquadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97.
6. L. Hongwen, *On the real quadratic fields of class number one*, Sci. Sinica **24** (1981), 1352–1357.
7. M. Kutsuna, *On a criterion for the class number of a quadratic number field to be one*, Nagoya Math. J. **79** (1980), 123–129.
8. D. H. Lehmer, *On the function  $x^2 + x + A$* , Sphinx **6** (1936), 212–214.
9. R. A. Mollin, *On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud-Degert type*, Nagoya Math. J. **105** (1987), 39–47.
10. ———, *Diophantine equations and class numbers*, J. Number Theory **24** (1986), 7–19.
11. R. A. Mollin, *Lower bounds for class numbers of real quadratic fields*, Proc. Amer. Math. Soc. **96** (1986), 545–550.
12. J. Pintz, *Elementary methods in the theory of L-functions*, VI. *On the least prime quadratic residue (mod p)*, Acta Arith. **32** (1977), 173–178.
13. G. Rabinovitch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in Quadratischen Zahlkörpern*, J. Reine Angew. Math. **142** (1913), 153–164.
14. C. Richaud, *Sur la résolution des équations  $x^2 - Ay^2 = \pm 1$* , Atti Accad. Pontif. Nuovi Lincei (1866), 177–182.
15. H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), 1–27.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALGARY, CALGARY, ALBERTA  
CANADA, T2N 1N4