

## 18. Affirmative Solution of a Conjecture Related to a Sequence of Shanks

By R. A. MOLLIN\*) and H. C. WILLIAMS\*\*)

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1991)

**Abstract:** In [6] the authors conjectured that if  $d \equiv 1 \pmod{8}$  is positive, square-free and all  $Q_i$ 's (see below) are powers of 2 in the continued fraction expansion of  $(1 + \sqrt{d})/2$  then the class number  $h(d)$  of  $Q(\sqrt{d})$  is equal to 1 if and only if  $d \in \{17, 41, 113, 353, 1217\}$ . The purpose of this note is to prove this conjecture and show how it relates to results in the literature including work of Shanks [7] concerning certain special forms. Moreover we solve the class number 2, 3, and 4 problems for these forms. Finally, we leave a conjecture for other forms at the end.

§1. Notations and preliminaries. Let  $d$  be a positive square-free integer and let  $w_d = (\sigma - 1 + \sqrt{d})/\sigma$  where  $\sigma = \begin{cases} 1 & \text{if } d \equiv 2, 3 \pmod{4} \\ 2 & \text{if } d \equiv 1 \pmod{4} \end{cases}$ . The discriminant of  $K = Q(\sqrt{d})$  is  $\Delta = (2/\sigma)^2 d$ , and the maximal order in  $K$  is denoted  $\mathcal{O}_K$ . Let  $w_d = \langle a, a_1, a_2, \dots, a_k \rangle$  be the continued fraction expansion of  $w_d$ . Here  $a_0 = a = [w_d]$ , (where  $[x]$  denotes the greatest integer less than or equal to  $x$ ); and  $a_i = [(P_i + \sqrt{d})/Q_i]$  for  $i \geq 1$  where:  $(P_0, Q_0) = (\sigma, \sigma - 1)$  and  $P_{i+1} = a_i Q_i - P_i$ ;  $Q_{i+1} Q_i = d - P_{i+1}^2$  for  $i \geq 0$ .

The Legendre symbol will be denoted by  $(/)$ . Finally for the theory of reduced ideals used herein the reader is referred to [5] or [8].

§2.  $Q_i$ 's as powers of 2. The conjecture posed in [6] is that any square-free  $d \equiv 1 \pmod{8}$  with all  $Q_i$ 's as powers of 2 and  $h(d) = 1$  can only hold for  $d \in \{17, 41, 113, 252, 1217\}$ . In [1] we classified for a general square-free  $d$  all those forms for which all the  $Q_i/Q_0$ 's are powers of a given integer  $c > 1$ . In particular for the case where  $d \equiv 1 \pmod{8}$  and all the  $\mathcal{O}_K$ -primes above 2 are principal then all  $Q_i$ 's are powers of 2 if and only if  $d = (2^s + 1)^2 + 2^{s+2}$ , where  $s > 0$  and  $k = 1 + 2s$ .

**Theorem 2.1.** *If  $d \equiv 1 \pmod{8}$  and all  $Q_i$ 's are powers of 2 then  $h(d) = 1$  if and only if  $d \in \{17, 41, 113, 353, 1217\}$ .*

*Proof.* We will now show the remarkable fact that  $d$  is a quadratic

- If  $m_0=2$  then  $d \equiv 26^2 \pmod{127}$ ;  
 If  $m_0=3$  then  $d \equiv 42^2 \pmod{127}$ ;  
 If  $m_0=4$  then  $d \equiv 37^2 \pmod{127}$ ;  
 If  $m_0=5$  then  $d \equiv 57^2 \pmod{127}$ ;  
 If  $m_0=6$  then  $d \equiv 6^2 \pmod{127}$ .

Now since  $(d/127)=1$ , we have that 127 splits in  $Q(\sqrt{d})$ . Since  $N(\mathcal{P})=127$  for  $\mathcal{P}$  an  $\mathcal{O}_K$ -prime above 127 when  $h(d)=1$  then  $127 < \sqrt{d}/2$  implies that  $\mathcal{P}$  is reduced (by [2], [5] or [8]), so  $127=Q_i/2$  for some  $i$ , a contradiction. If  $127 \geq \sqrt{d}/2$  then  $d \leq 64, 516$ . A computer check up to that bound reveals only those on the list.

**Remark 2.1.** Observe that  $d=(2^n+1)^2+2^{n+2}=(2^n+3)^2-8$ , the forms studied by Shanks in [7]. Thus we have not only affirmatively settled the conjecture in [6] but also some queries raised by Shanks therein.

**Remark 2.2.** It can be easily shown using the results of [5] that if  $h=h((2^n+3)^2-8)$  then  $n < 7h+1$ . Thus a computer check has allowed us to determine the following.

**Theorem 2.2.** Let  $d=(2^n+3)^2-8$ . Then:

- (I)  $h(d)=2$  if and only if  $d=17153$   
 (II)  $h(d)=3$  if and only if  $d \in \{4481, 67073\}$   
 (III)  $h(d) \neq 4$  for any  $n$ .

Thus to solve the class number problem for  $d$  in general is limited now only by computational considerations.

In [1] we showed that if  $d \not\equiv 1 \pmod{4}$  has all  $Q_i$ 's as powers of a prime  $p > 2$  then  $h(d) > 1$ . Moreover if  $d \not\equiv 1 \pmod{4}$  and all  $Q_i$ 's are powers of 2 we leave the reader with:

**Conjecture 2.1.** If  $d \not\equiv 1 \pmod{4}$  and all  $Q_i$ 's are powers of 2 then  $h(d)=1$  if and only if  $d \in \{2, 3, 6, 11, 38, 83, 227\}$ .

In [1] we showed that if  $d \not\equiv 1 \pmod{4}$  and all  $Q_i$ 's are powers of 2 then  $h(d)=1$  implies  $d=l^2+2$ . Thus, in consideration of our solution of the class number one problem for ERD-types (with one possible exception) in [4], then Conjecture 2.1 has been shown to hold with possibly only one more value remaining. It seems to the authors to be virtually intractable to remove this exceptional value.

## References

- [1] R. A. Mollin: Powers in continued fractions and class numbers of real quadratic fields (to appear).  
 [2] —: Class numbers and the divisor function (to appear).  
 [3] R. A. Mollin and H. C. Williams: Class number problems for real quadratic fields. Number Theory and Cryptography (ed. J. H. Loxton). London Math. Soc. Lecture Note Series, 154, 175–195 (1990).  
 [4] —: Solutions of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception). Number Theory (ed. R. A. Mollin). Walter de Gruyter, Berlin, pp. 417–425 (1990).

- [5] —: Computation of the class number of a real quadratic field (to appear: *Advances in the Theory of Computation and Computational Mathematics*).
- [6] —: Powers of 2, continued fractions, and the class number one problem for real quadratic fields  $Q(\sqrt{d})$ , with  $d \equiv 1 \pmod{8}$  (to appear in the *Math. Heritage of C. F. Gauss* (ed. G. M. Rassias)).
- [7] D. Shanks: On Gauss's class number problems. *Math. Comp.*, **23**, 151-163 (1969).
- [8] H. C. Williams and M. C. Wonderlick: On the parallel generation of the residues for the continued fraction factoring algorithm. *Math. Comp.*, **177**, 405-423 (1987).