

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 $w_a = (\sigma - 1 + \sqrt{d})/\sigma$ 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 $w_a = \langle a, a_1, a_2, \dots, a_k \rangle$ be the continued fraction expansion of w_a . Here $a_0 = a = \lfloor w_a \rfloor$, (where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x); and $a_i = \lfloor (P_i + \sqrt{d})/Q_i \rfloor$ 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 residue of 127 if $d = (2^n + 1)^2 + 2^{n+2}$, (observe: $127 = 2^7 - 1$).

Let $n \equiv m_0 \pmod{7}$ where $0 \leq m_0 \leq 6$.

$$\text{If } m_0 = 0 \text{ then } d \equiv 32^2 \pmod{127};$$

$$\text{If } m_0 = 1 \text{ then } d \equiv 25^2 \pmod{127};$$

*) Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, Canada, T2N 1N4.

***) Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada, R3T 2N2.