A NUMBER THEORETIC FUNCTION ARISING FROM CONTINUED FRACTIONS

H. C. Williams
University of Manitoba, Department of Computer Science
Winnipeg, Manitoba R3T 2N2 Canada

(*Submitted June 1998*)

1. INTRODUCTION

Let a, b be integers with $b > 0$. If we perform the Euclidean algorithm to find (a, b), the greatest common divisor of a and b, we get

$$\begin{array}{rcll} a &=& q_0 b + r_0 & (0 \le r_0 < b) \\ b &=& q_1 r_0 + r_1 & (0 \le r_1 < r_0) \\ r_0 &=& q_2 r_1 + r_2 & (0 \le r_2 < r_1) \\ \cdots && \cdots & \quad \cdots \end{array}$$

until we finally find the least $n \ge 0$ such that $r_n = 0$. Note that for this value of n we get $q_n > 1$. We will define $E(a, b)$ to be this value n. We now let a, q be any pair of coprime integers with $q > 0$ and set $\omega = \omega(a, q)$ to be the multiplicative order of a modulo q; that is, ω is the least positive value of m such that $a^m \equiv 1 \pmod{q}$. We define the number theoretic function $W(a, q)$ by

$$W(a, q) = 2\sum_{i=1}^{\omega} \lfloor E(a^i, q)/2 \rfloor. \tag{1.1}$$

We next let N be any positive non-square integer and define

$$\nu(N) = (\sigma - 1 + \sqrt{N})/\sigma,$$

where

$$\sigma = \begin{cases} 2 & \text{when } N \equiv 1 \pmod{4}, \\ 1 & \text{otherwise.} \end{cases}$$

Now consider

$$N = (\sigma(qra^n + \mu(a^k + \lambda)/q)/2)^2 - \sigma^2 \mu\lambda a^n r,$$

where $\mu, \lambda \in \{1, -1\}$, $qr \mid a^k + \lambda$, $(n, k) = 1$, $n > k \ge 1$, and

$$\sigma = \begin{cases} 1 & \text{if } 2 \mid qra^n + \mu(a^k + \lambda)/q, \\ 2 & \text{if } 2 \nmid qra^n + \mu(a^k + \lambda)/q. \end{cases}$$

It was shown in Williams [16] that $W(a, q)$ is a very important function for determining *a priori* the period length $p(N)$ of the simple continued fraction expansion of $\nu(N)$. For example, in the simple case of $r = \mu = -\lambda = 1$, we get

$$p(N) = 2n + k + kW(a, q)/\omega(a, q).$$

Indeed, as shown in Mollin and Williams [6], we get the simple continued fraction expansion for $\nu(N)$ as

$$\nu(N) = \langle q_0, \overline{q_1, q_2, \ldots, q_p} \rangle,$$

where we can actually provide formulas for q_i $(i = 0, 1, 2, \dots, p = p(N))$ in terms of q, a, n, k. In order to do this, we first need to define for $1 \le j \le n-1$ the symbols:

$$\lambda_j = jk - \lfloor kj/n \rfloor n,$$
$$\varepsilon_j = \lfloor (j+1)k/n \rfloor - \lfloor jk/n \rfloor,$$
$$\rho_j = k - n + \lambda_j,$$
$$m_j = \begin{cases} 2\lfloor E(a^i, q)/2 \rfloor + 1 & \text{when } \varepsilon_j = 1, \\ 1 & \text{when } \varepsilon_j = 0, \end{cases}$$

and $\psi(i)$, where $\psi(1) = 3$ and $\psi(j+1) = \psi(j) + \varepsilon_j m_j + 2$. With these in mind we get

$$q_0 = (qa^n + (a^k - 1)/q)/2 + (\sigma - 1)/\sigma,$$
$$q_1 = q,\ q_2 = qa^{n-k},$$
$$q_{\psi(j)} = \begin{cases} qa^{\lambda_j} & \text{when } \varepsilon_j = 0, \\ qa^{\lambda_j} + (a^{\rho_j} - \gamma_j)/q & \text{when } \varepsilon_j = 1. \end{cases}$$

Also, if $\varepsilon_j = 0$, then $q_{\psi(j)+1} = qa^{n-k-\lambda_j}$, and if $\varepsilon_j = 1$, then

$$q_{\psi(j)+i} = \begin{cases} b_{i,j} & \text{for } 1 \le i \le m_j, \\ qa^{2n-k-\lambda_j} + (a^{n-\lambda_j} - \delta_i)/q & \text{for } i = m_j + 1. \end{cases}$$

Here,

$$a^{\rho_j}/q = \langle b_{0,j}, b_{1,j}, \dots, b_{m_j,j} \rangle,$$
$$\gamma_j \equiv a^{\rho_j} (\operatorname{mod} q),\ \ \delta_j \equiv a^{n-\lambda_j} (\operatorname{mod} q), \text{ and } 0 < \gamma_j,\ \delta_j < q.$$

We have $p(N) = 2 + \psi(n-1) = 2n + k + kW(a, q)/\omega(a, q)$.

Some properties of $W(a, q)$ were developed by Mollin and Williams [7]; for example,

$$W(a, q) = 4 \sum_{i=1}^{(\omega-1)/2} \lfloor E(a^i, q)/2 \rfloor \quad \text{when } 2 \nmid \omega \tag{1.2}$$

and

$$W(a, q) = 4 \sum_{i=1}^{\omega/2-1} \lfloor E(a^i, q)/2 \rfloor + 2\lfloor E(a^{\omega/2}, q)/2 \rfloor \quad \text{when } 2 \mid \omega. \tag{1.3}$$

Thus, if ω is odd, we always have $4 \mid W(a, q)$, but if ω is even, the value of $W(a, q)$ is always even, of course, but its value modulo 4 is determined by $2\lfloor E(a^{\omega/2}, q)/2 \rfloor$. In the simple case of $a^{\omega/2} \equiv -1$ (mod q), we have $E(a^{\omega/2}, q) = 2$, but we see that $\omega(29, 35) = 2$ and $E(29, 35) = 4$. Thus, it appears that $W(a, q) \equiv 2, 0$ (mod 4) when $2 \mid \omega$. This raises the question of exactly what values can be assumed by $W(a, q)$. In this paper we will find values that can be assumed by $W(a, q)$ when $\omega = 1, 2, 3, 4, 6$. In particular, we show that if $\omega = 2$ or $\omega = 3$ then $W(a, q)$ can assume all possible positive values that are allowable under the above conditions, i.e., $W(a, q)/2$ or $W(a, q)/4$ can be any given positive integer when $\omega = 2$ or $\omega = 3$, respectively. We will then apply our results to the problem of determining values of N such that the period of the continued fraction expansion of $v(N)$ has a cyclic structure.

Bernstein [1], [2] seems to have been the first individual to examine the cycle structure of periodic continued fractions to any great extent. He developed a rather complicated definition of a cycle, which resulted from his investigation of the continued fraction expansion of $\sqrt{N}$ for certain parametric families of values of N. However, Nyberg [9], Shanks [11], [12], Yamomoto [18], and Hendy [4] had essentially discovered cycle structures for certain $\sqrt{N}$ or $\nu(N)$ earlier. For example, a result of Hendy is that if $N = (qa^n + (a-1)/q)^2 + 4a^n$, where $a \equiv 1 \pmod{q}$ and $2 \nmid qa^n + (a-1)/q$, then

$$\nu(N) = \langle q_0, \overline{q_1, q_2, \dots, q_p} \rangle,$$

where

$$q_0 = (qa^n + (a-1)/q + 1)/2, \ q_{2i+1} = qa^i, \ q_{2i+2} = qa^{n-i-1}$$

for $i = 0, 1, 2, \dots, n-1$, $q_p = 2q_0 - 1$, $p = p(N) = 2n+1$. Bernstein considered pairs like $\{qa^i, aq^{n-i-1}\}$ $(i = 0, 1, 2, \dots, n-1)$ to be cycles in the period $q_1, q_2, \dots, q_p$ of the continued fraction expansion of $\nu(N)$. For the purpose of this paper we will provide a somewhat more restrictive definition of cycles than that of Bernstein.

Let $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_k \subseteq \mathbb{Z}$ and $\mathcal{P} = \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_k$ be infinite. Let F be some function defined on $\mathcal{P}$ such that $F : \mathcal{P} \to \mathbb{Z}$ and let

$$\begin{aligned} \mathcal{N} = \{\nu(N) \mid N = F(p_1, p_2, \dots, p_k), \\ (p_1, p_2, \dots, p_k) \in \mathcal{P}, \ N > 0, \\ N \text{ not a perfect square}\}. \end{aligned}$$

We say that the simple continued fraction expansions of the values of $\nu(N)$ in the family $\mathcal{N}$ have *the structure of cycles of length c* if the periodic part $q_1, q_2, \dots, q_p$ $(p = p(N))$ of these continued fractions can, for some fixed value of $b \geq 0$, be given by

$$q_{ic+j+b} = f_j(i, p_1, p_2, \dots, p_k) \ \ (i = 0, 1, 2, \dots, t-1),$$

where $p(N) \equiv b \pmod{c}$, $t \geq 2$, and f_j $(j = 0, 1, 2, \dots, c-1)$ are c fixed functions such that

$$f_j : \{0, 1, 2, \dots, t-1\} \times \mathcal{P} \to \mathbb{Z}.$$

A *cycle* in the period of the continued fraction of $\nu(N) \in \mathcal{N}$ is any set

$$\{f_j(i, p_1, p_2, \dots, p_k) \mid j = 0, 1, 2, \dots, c-1\}.$$

The restriction that $t \geq 2$ ensures that there are at least two cycles in the period; otherwise, all continued fractions could be considered to have a cycle structure. In the case of Hendy's example, we get $b = 1$, $c = 2$, $f_0(i, a, q, n) = qa^i$, $f_1(i, a, q, n) = qa^{n-i-1}$.

In the families considered by Nyberg, Shanks, Yamomoto, and Hendy, the values of c are either 2 or 6, but Bernstein discovered families for which $c = 4, 5, 6, 8, 10, 11, 12$. Later, his results were extended by Williams [15] and Halter-Koch [3], but no new values of c were found except for $c = 3$. Bernstein expressed surprise that cycles with c as large as 12 exist, but we will show here that even under our more restrictive definition of cycle structure there always exist infinite families $\mathcal{N}$ such that any $\nu(N) \in \mathcal{N}$ has the structure of cycles of length c for any preselected value of $c > 0$.

2. SOME PRELIMINARY RESULTS

In order to determine values for $W(a,q)$, we must find values of a, q such that $a^{\omega}=1$ (mod q) for a given ω and such that we can predict the values of $E(a^i,q)$. We will do this by making use of some elementary properties of the continued fraction expansion of quadratic irrationals. In developing the material in this action, it is assumed that the reader is familiar with basic results concerning continued fractions which can be found in Perron [10] and Mollin [5] or Stephens and Williams [13], [14], and Williams and Wunderlich [17].

Consider the continued fraction $\langle q_0, q_1, \ldots, q_n, \ldots\rangle$. For a fixed i and j, define $A_{j,i}$ and $B_{j,i}$ by

$$A_{j+1,i}=q_{j+i+1}A_{j,i}+A_{j-1,i},$$
$$B_{j+1,i}=q_{j+i+1}B_{j,i}+B_{j-1,i},$$

where $A_{-2,i}=0$, $A_{-1,i}=1$, $B_{-2,i}=1$, $B_{-1,i}=0$. Then

$$\frac{A_{j,i}}{B_{j,i}}=\langle q_i, q_{i+1}, \ldots, q_{i+j}\rangle, \tag{2.1}$$

$$\frac{B_{j,i}}{B_{j,i-1}}=\langle q_{i+j}, q_{i+j-1}, \ldots, q_{i+1}\rangle, \tag{2.2}$$

and

$$A_{j,i}B_{j-1,i}-A_{j-1,i}B_{j,i}=(-1)^{j+1}. \tag{2.3}$$

Put $A_j=A_{j,0}$, $B_j=B_{j,0}$. If P, Q, $D\in\mathbb{Z}$, $\phi=(P+\sqrt{D})/Q$, where D is any positive non-square integer and $Q\mid D-P^2$, we put $P_0=P$, $Q_0=Q$, $\phi_0=\phi$, $q_0=\lfloor\phi_0\rfloor$. Compute P_n, Q_n, ϕ_n, q_n recursively by $P_n=q_{n-1}Q_{n-1}-P_{n-1}$, $Q_n=(D-P_n^2)/Q_{n-1}$, $\phi_n=(P_n+\sqrt{D})/Q_n$, $q_n=\lfloor\phi_n\rfloor$, and define

$$\begin{aligned} G_{j,i}&=Q_iA_{j,i}-P_iB_{j,i},\\ G_j&=G_{j,0.}\end{aligned} \tag{2.4}$$

Then ϕ_0 can be written in a continued fraction as $\phi_0=\langle q_0, q_1, \ldots, q_{n-1}, \phi_n\rangle$ and, in general, ϕ_i can be written as $\phi_i=\langle q_i, q_{i+1}, \ldots, q_{n-1}, \phi_n\rangle$. If we define $\theta_k=\prod_{i=1}^{k-1}\phi_i^{-1}$, then

$$\theta_k=(-1)^{k-1}(A_{k-2}-\phi B_{k-2})=(-1)^{k-1}(G_{k-2}-\sqrt{D}B_{k-2})/Q_0. \tag{2.5}$$

Denote by $N(\alpha)$ the norm of α. Since

$$N(\theta_k)=(-1)^{k-1}Q_{k-1}/Q_0, \tag{2.6}$$

we can show that

$$\begin{aligned}\frac{G_{j,i}+\sqrt{D}B_{j,i}}{Q_{j+i+1}}&=\prod_{k=i+1}^{j+i+1}(P_k+\sqrt{D})/Q_k\\ &=(-1)^i(G_{i-1}-\sqrt{D}B_{i-1})(G_{i+j}+\sqrt{D}B_{i+j})/(Q_0Q_{i+j+1});\end{aligned}$$

hence,

$$G_{j,i}+\sqrt{D}B_{j,i}=(-1)^i(G_{i-1}-\sqrt{D}B_{i-1})(G_{i+j}+\sqrt{D}B_{i+j})/Q_0. \tag{2.7}$$

Since $\phi_i=\langle q_i, q_{i+1}, \ldots, q_{i+j}, \phi_{i+j+1}\rangle$, we get

$$\phi_i = \frac{\phi_{i+j+1}A_{j,i} + A_{j-1,i}}{\phi_{i+j+1}B_{j,i} + B_{j-1,i}};$$

on equating rational and irrational parts, we find that

$$\begin{aligned} G_{j,i} &= P_{i+j+1}B_{j,i} + Q_{i+j+1}B_{j-1,i}, \\ DB_{j,i} &= P_{i+j+1}G_{j,i} + Q_{i+j+1}G_{j-1,i}. \end{aligned} \tag{2.8}$$

Let Q_0 be selected such that $Q_0 \mid 2D$. Since $G_i \equiv -P_0B_i \pmod{Q_0}$ for any $i \geq -2$, we get

$$(G_n - \sqrt{D}B_n)(G_m - \sqrt{D}B_m) = G_nG_m + DB_nB_m - (G_nB_m + G_mB_n)\sqrt{D} \equiv 0 \pmod{Q_0};$$

therefore, $(G_n - \sqrt{D}B_n)(G_m - \sqrt{D}B_m)/Q_0 \in \mathbb{Z}[\sqrt{D}]$ for $n, m \geq -2$. Now let $X, Y \in \mathbb{Z}$ and put $m = N(X + \sqrt{D}Y)$. We have the following theorem.

Theorem 2.1: Let $U, T \in \mathbb{Z}$ such that $U + \sqrt{D}T = (G_{i-1} - \sqrt{D}B_{i-1})^2(X + \sqrt{D}Y)/Q_0$ $(i \geq 0)$; then $S = (U + P_iT)/Q_i \in \mathbb{Z}$ and $S^2 \equiv m \pmod{T}$.

Proof: Put

$$\begin{aligned} R + \sqrt{D}S &= -(G_{i-2} - \sqrt{D}B_{i-2})(G_{i-1} - \sqrt{D}B_{i-1})(X + \sqrt{D}Y)/Q_0, \\ R' + \sqrt{D}S' &= (G_{i-2} - \sqrt{D}B_{i-2})^2(X + \sqrt{D}Y)/Q_0, \end{aligned}$$

where $R, S, R', S' \in \mathbb{Z}$. We get

$$\frac{R + \sqrt{D}S}{U + \sqrt{D}T} = -\frac{G_{i-2} - \sqrt{D}B_{i-2}}{G_{i-1} - \sqrt{D}B_{i-1}} = \frac{R' + \sqrt{D}S'}{R + \sqrt{D}S}. \tag{2.9}$$

Now, by (2.5),

$$-\frac{G_{i-2} - \sqrt{D}B_{i-2}}{G_{i-1} - \sqrt{D}B_{i-1}} = \frac{P_i + \sqrt{D}}{Q_i};$$

hence, by equating rational and irrational parts in (2.9), we get $U + P_iT = Q_iS$, $UP_i + TD = Q_iR$, $R + P_iS = Q_iS'$. It follows that

$$Q_i^2S' = UP_i + TD + P_i(U + P_iT) = 2P_iQ_iS + Q_iQ_{i-1}T$$

and

$$S' = (2P_iS + Q_{i-1}T)/Q_i.$$

By (2.6), we have $U^2 - DT^2 = Q_i^2m$; therefore, $(Q_iS - P_iT)^2 - DT^2 = Q_i^2m$, which can be written as $S^2 - TS' = m$. □

We next consider the special cases of $m = 1, -1, -3$. As before, we let P_0, Q_0 be selected such that $Q_0 \mid 2D$ and $Q_0 \mid D - P_0^2$. Denote by π the period length of the continued fraction expansion of $\phi_0 = (P_0 + \sqrt{D})/Q_0$. We know (see, e.g., [13]) that there must exist some minimal $h > 0$ such that either $P_h = P_{h+1}$ or $Q_h = Q_{h+1}$; in the former case, we get $\pi = 2h$ and in the latter, $\pi = 2h + 1$. If $n \equiv h \pmod{\pi}$, put

$$X + Y\sqrt{D} = (G_{n-1} + \sqrt{D}B_{n-1})^2/(Q_0Q_h) \tag{2.10}$$

when $\pi = 2h$, and put

$$X + Y\sqrt{D} = (P_{h+1} + \sqrt{D})(G_{n-1} + \sqrt{D}B_{n-1})^2/(Q_0Q_hQ_{h+1}) \tag{2.11}$$

when $\pi = 2h+1$. It is well known (see, e.g., [10]) that

$$N(X+Y\sqrt{D}) = (-1)^{\pi}. \tag{2.12}$$

From results in Mollin, van der Poorten, and Williams [8], we know that if the Diophantine equation $x^2 - Dy^2 = -3$ is solvable for $x, y \in \mathbb{Z}$, then we must get $Q_{h+1} = P_{h+1} + Q_h$ for some choice of Q_0, where $Q_0 \mid 2D$. We will assume that Q_0 has been so selected. Let $n \equiv h \pmod{\pi}$, then if

$$X + Y\sqrt{D} = (2Q_h - Q_{h+1} + 2\sqrt{D})(G_n + \sqrt{D}B_n)^2 / (Q_0 Q_{h+1}^2), \tag{2.13}$$

we have $X, Y \in \mathbb{Z}$ and

$$N(X+Y\sqrt{D}) = -3. \tag{2.14}$$

If, for example, we have X, Y given by (2.13), we get

$$\begin{aligned} U + \sqrt{D}T &= (G_{i-1} - \sqrt{D}B_{i-1})^2(X+Y\sqrt{D})/Q_0 \\ &= ((G_{n-i,i} + \sqrt{D}B_{n-i,i})/Q_{h+1})^2(2Q_h - Q_{h+1} + 2\sqrt{D}) \end{aligned}$$

by (2.7). It can be verified after some manipulation involving the identities in (2.8) and the condition $Q_{h+1} = P_{h+1} + Q_h$ that

$$\begin{aligned} U &= 2G_{n-i,i}B_{n-i,i} + G_{n-i,i}B_{n-i-1,i} + G_{n-i-1,i}B_{n-i,i} + 2G_{n-i-1,i}B_{n-i-1,i}, \\ T &= 2(B_{n-i,i}^2 + B_{n-i,i}B_{n-i-1,i} + B_{n-i-1,i}^2). \end{aligned} \tag{2.15}$$

On using (2.4) and (2.3), we get

$$\begin{aligned} S &= (U + P_iT)/Q_i \\ &= 2A_{n-i,i}B_{n-i,i} + A_{n-i,i}B_{n-i-1,i} + A_{n-i-1,i}B_{n-i,i} + 2A_{n-i-1,i}B_{n-i-1,i} \\ &= 2(A_{n-i,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i-1,i}) + (-1)^{n-i+1}. \end{aligned} \tag{2.16}$$

Similarly, we get

$$\begin{aligned} T &= B_{n-i-1,i}B_{n-i,i} + B_{n-i-2,i}B_{n-i-1,i}, \\ S &= B_{n-i-1,i}A_{n-i,i} + B_{n-i-2,i}A_{n-i-1,i}, \end{aligned} \tag{2.17}$$

when X, Y are given by (2.10), and

$$\begin{aligned} T &= B_{n-i,i}^2 + B_{n-i-1,i}^2, \\ S &= A_{n-i,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i-1,i}, \end{aligned} \tag{2.18}$$

when X, Y are given by (2.11).

3. VALUES ASSUMED BY $W(a, q)$

We now need to find a, q such that we can easily compute $E(a^i, q)$ for $i = 1, 2, \ldots, \lfloor \omega/2 \rfloor$. We first note that $E(a, q) = 1$ if and only if $q \mid a$, and $E(a, q) = 1$ if and only if $a \equiv 1 \pmod{q}$; thus, $W(a, q) = 0$ whenever $\omega = 1$ and $W(a, q) \neq 0$ whenever $\omega > 1$. Indeed, the story concerning the values that $W(a, q)$ can assume when $\omega = 2$ is very different from that when $\omega = 1$. For let T and S be given by (2.17). We have $S^2 \equiv 1 \pmod{T}$ by Theorem 2.1, and

$$\frac{S}{T} = \frac{(B_{n-i-1,i}/B_{n-i-2,i})A_{n-i,i} + A_{n-i-1,i}}{(B_{n-i-1,i}/B_{n-i-2,i})B_{n-i,i} + B_{n-i-1,i}}$$

$$= \langle q_i, q_{i+1}, \ldots, q_n, B_{n-i-1,i} / B_{n-i-2,i} \rangle$$
$$= \langle q_i, q_{i+1}, \ldots, q_n, q_{n-1}, q_{n-2}, \ldots, q_{i+1} \rangle$$

by (2.1) and (2.2). Thus, $E(S, t) = 2n - 2i - 1 - \chi_{i+1}$, where χ_j is defined by

$$\chi_j = \begin{cases} 0 & \text{when } q_j > 1, \\ 1 & \text{when } q_j = 1. \end{cases}$$

Thus, if $q = T$ and $a \equiv S \pmod{q}$, then

$$W(a, q) = 2\lfloor E(a, q)/2 \rfloor = 2(n - i - 1).$$

It is evident that if we put $n = k\pi + h$ then, for any given positive integer x, we can find k, i such that $W(a, q) = 2x$ when $\omega = 2$. Hence, $W(a, q)$ can assume all possible even positive values when $\omega = 2$.

We next consider the case of $\omega = 4$. We let T and S be given by (2.18); we have $S^2 \equiv -1$ (mod T) and

$$\frac{S}{T} = \frac{(B_{n-i,i} / B_{n-i-1,i})A_{n-i,i} + A_{n-i-1,i}}{(B_{n-i,i} / B_{n-i-1,i})B_{n-i,i} + B_{n-i-1,i}}$$
$$= \langle q_1, q_{i+1}, \ldots, q_n, q_n, q_{n-1}, \ldots, q_{i+1} \rangle.$$

Hence, $E(S, T) = 2n - 2i - \chi_{i+1}$. On putting $q = T$ and $a \equiv S \pmod{q}$, we get

$$W(a, q) = 4\lfloor E(S, T)/2 \rfloor + 2 = 4(n - i - \chi_{i+1}) + 2.$$

For $D = (4fc^2 + c + f)^2 + 4fc + 1$, we get $\sqrt{D} = \langle b, \overline{2c, 2c, 2b} \rangle$ with $b = 4fc^2 + c + f$. In this case, we have $h = 1, \pi = 3, n = 3r + 1, \chi_j = 0$ for all j; hence, $W(a, q) = 4(3r + 1 - i) + 2$. Thus, given any positive $x \equiv 2 \pmod{4}$, we can find values of a, q such that $\omega(a, q) = 4$ and $W(a, q) = x$.

The case of $\omega = 3$ is a little more difficult. We let T and S be given by (2.15) and (2.16) and note that $S^2 \equiv -3$ (mod T). Thus, since $2 \| T$, we have $S \equiv 1 \pmod{2}$ and

$$((S-1)/2)^2 + (S-1)/2 + 1 \equiv 0 \pmod{T/2};$$

it follows that

$$((S-1)/2)^3 \equiv 1 \pmod{T/2}$$

and $\omega((S-1)/2, T) = 3$. Let $n \equiv h \pmod{\pi}$ and put $q_n' = q_n + 1 - \eta$, $q_n'' = q_n + \eta$, where $\eta \in \{0, 1\}$. Then

$$\langle q_i, q_{i+1}, \ldots, q_{n-1}, q_n' \rangle = \frac{A_{n-i,i} + (1-\eta)A_{n-i-1,i}}{B_{n-i,i} + (1-\eta)B_{n-i-1,i}},$$
$$\langle q_n'', q_{n-1}, q_{n-2}, \ldots, q_{i+1} \rangle = q_n'' + \frac{B_{n-i-2,i}}{B_{n-i-1,i}} = \frac{B_{n-i,i}}{B_{n-i-1,i}} + \eta;$$

hence

$$(T/2)\langle q_i, q_{i+1}, \ldots, q_{n-1}, q_n', q_n'', q_{n-1}, \ldots, q_{i+1} \rangle$$
$$= A_{n-i,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i,i} + A_{n-i-1,i}B_{n-i-1,i} + \eta(-1)^{n-i+1}$$
$$= (S + (-1)^{n-i+1}(2\eta - 1))/2$$

by (2.3) and (2.16). Putting $2\eta - 1 = (-1)^{n-i}$, we get

$$\frac{(S-1)/2}{T/2}=\langle q_i, q_{i+1}, \dots, q_{n-1}, q_n', q_n'', q_{n-1}, \dots, q_{i+1}\rangle$$

and $E((S-1)/2, T/2)=2n-2i-\chi_{i+1}$. If we put $q=T/2$ and $a\equiv(S-1)/2 \pmod q$, we see by (1.2) that

$$W(a,q)=4\lfloor E(a,q)/2\rfloor=4(n-i-\chi_{i+1}).$$

We should also observe that, since $Q_{h+1}=Q_h+P_{h+1}$, we have $D=P_{h+1}^2+P_{h+1}Q_h+Q_h^2$ and $\sqrt{D}<P_{h+1}+Q_h$. It follows that $q_{h+1}=1$, $P_{h+2}=Q_{h+1}-P_{h+1}=Q_h$, and $Q_{h+2}=P_{h+1}$; hence, $Q_{h+1}=Q_{h+2}+P_{h+2}$. By the symmetry rules $Q_{\pi-i}=Q_i$ and $P_{\pi-i}=P_{i+1}$, we get $Q_{\pi-h-1}=P_{\pi-h-1}+Q_{\pi-h-2}$. Thus, we can replace h by $\pi-h-2$ and still have $Q_{h+1}=Q_h+P_{h+1}$. It follows that $n-i-\chi_{i+1}$ can be $\equiv h-i-\chi_{i+1}$ or $\equiv -h-2-i-\chi_{i+1} \pmod{\pi}$. For example, in the simple case of $D=21$, $P_0=0$, $Q_0=1$, we get

$$\sqrt{21}=\langle 4, \overline{1, 1, 2, 1, 1, 8}\rangle$$

with $Q_1=Q_0+P_1$ and $Q_5=Q_4+P_5$. We have $\pi=6$ and $n=6m$ or $n=6m+4$, $\chi_1=1$, $\chi_2=1$, $\chi_3=0$, $\chi_4=1$, $\chi_5=1$, $\chi_6=0$. The values of $n-i-\chi_{i+1}$ can be $6m-1$, $6m-2$, $6m-4$, $6m-5$, $6m-3$, $6m-6$, where in the last case $m>1$; that is, $n-i-\chi_{i+1}$ can take on any positive integral value and therefore $W(a,q)/4$ can take on any positive integral value.

For T, S given by (2.15), (2.16), we also have

$$((S+1)/2)^2-(S+1)/2+1\equiv 0 \pmod{T/2};$$

hence, $((S+1)/2)^6\equiv 1 \pmod{T/2}$ and $((S+1)/2)^3\equiv -1$, $((S+1)/2)^2\not\equiv 1$, $(S+1)/2\not\equiv 1$ (mod $T/2$). We get $\omega((S+1)/2, T/2)=6$ and

$$W(a,q)=4\lfloor E(a,q)/2\rfloor+4\lfloor E(a^2,q)/2\rfloor+2$$

by (1.3) when $q=T/2$ and $a\equiv(S+1)/2 \pmod{T/2}$. Since $a^2\equiv(S-1)/2 \pmod{T/2}$, the continued fraction expansion for a/q and a^2/q are identical except that the values of q_n' and q_n'' are interchanged. We get

$$W(a,q)=8(n-i-\chi_{i+1})+2$$

and $W(a,q)$ can therefore assume any positive value which is 2 (mod 8), but these need not be the only values that $W(a,q)$ is capable of assuming when $\omega=6$.

4. CYCLE STRUCTURES

We will now use our earlier results to establish the existence of cycle structures of arbitrary length in the continued fraction period of $\nu(N)$ for $N=(\sigma(qa^n+(a^k-1)/q))^2+\sigma^2a^n$ with certain values of a, q, n, k. We put $n=sk+1$ $(s\geq 1)$, $k=\omega t$, where $\omega=\omega(a,q)$. Then

$$p(N)=2(sk+1)+\omega t+tW=tc+2,$$

where $W=W(a,q)$ and $c=(2s+1)\omega+W$.

Let j be any nonnegative integer $\leq n-1=sk=\omega st$, and suppose $j=us+r$ $(1\leq r\leq s)$. We get $kj=un+\omega tr-u$ and $0<\omega tr-u<\omega st+1=n$; thus, $\lambda_j=\omega tr-u<(s-1)\omega t+1$ when $r<s$. It follows that $\lambda_j<n-k$ if $r<s$; hence, by Lemma 4.5 of [6], $\varepsilon_j=0$ if $r<s$ or, equivalently, $\varepsilon_j=0$ if $s\nmid j$. If $s\mid j$, then $r=s$ and $u=j/s-1\leq k-1$. In this case,

$$\lambda_j = \omega rt - u \geq \omega st - (k-1) = (s-1)\omega t + 1 = n - k;$$

thus, $\varepsilon_j = 1$ if and only if $s \mid j$.

We next assume that $j + gs\omega \leq n-1$. We get $k(j+gs\omega) = n(u+\omega g) - u - \omega g + \omega rt$. Now, $\omega rt \leq \omega st = n-1$ and $\omega st \geq j + gs\omega$ or $\omega t \geq u + g\omega + r/s$; hence, $u + g\omega < \omega tr < n$ and

$$\lfloor k(j+gs\omega)/n \rfloor = u + \omega g.$$

It follows that

$$\lambda_{j+gs\omega} = \lambda_j - g\omega.$$

If $j = gs\omega + is$, then $\lambda_j \equiv \lambda_{is} \equiv -i + 1 \pmod{\omega}$ and $\rho_j \equiv -i \pmod{\omega}$.

Consider

$$\begin{aligned}\Psi(g) &= \psi((g+1)s\omega + 1) - \psi(gs\omega + 1)\\ &= \sum_{j=gs\omega+1}^{(g+1)s\omega} \psi(j+1) - \psi(j) = \sum_{j=gs\omega+1}^{(g+1)s\omega} (\varepsilon_j m_j + 2)\\ &= 2s\omega + \sum_{i=1}^{\omega} m_{gs\omega+is} = 2s\omega + \omega + W = c,\end{aligned}$$

a value independent of the value of g as long as $(g+1)s\omega \leq n-1 = st\omega$ or $g+1 \leq t$. From this, we can easily establish by induction that $\psi(gs\omega+1) = gc+3$, and since $\varepsilon_j = \varepsilon_{gs\omega+j}$, $m_j = m_{gs\omega+j}$, we can use induction to show that $\psi(gs\omega+j) = gc + \psi(j)$ whenever $g+1 \leq t$ and $j \leq \omega s$.

We now see that the continued fraction expansion of $v(N)$ given in Section 1 with $n = sk+1$ $(s \geq 1)$ has

$$q_0 = (qa^n + (a^k - 1)/q)/2 + (\sigma - 1)/\sigma,$$
$$q_1 = q_1,\ q_2 = qa^{n-k}.$$

If $0 \leq g \leq t-1$, $1 \leq h \leq s\omega$, then

$$q_{\psi(h)+gc} = \begin{cases} qa^{\lambda_h - g\omega} & \text{when } s \nmid h,\\ qa^{\lambda_h - g\omega} + (a^{k-n+\lambda_h - g\omega} - \delta_h)/q & \text{when } s \mid h;\end{cases}$$

furthermore, when $s \nmid h$,

$$q_{\psi(h)+gc+1} = qa^{n-k-\lambda_h+g\omega},$$

and when $s \mid h$,

$$g_{\psi(h)+gc+i} = \begin{cases} b_{i,h} & \text{when } 1 \leq i \leq m_h,\\ qa^{2n-k-\lambda_h+g\omega} + (a^{n-g\omega-\lambda_h} - \delta_h)/q & \text{when } i = m_k + 1,\end{cases}$$

where

$$a^{\rho_h}/q = \left\langle b_{0,h}, b_{1,h}, \ldots, b_{m_h,h} \right\rangle.$$

That is, there are c functions $f_j(g,a,q,n,k)$ $(j = 0, 1, 2, \ldots, c-1)$ such that

$$q_{gc+j+3} = f_j(g,a,q,n,k)$$

for $g = 0, 1, \ldots, t-1$. This means that the period of $v(N)$ has t cycles of length $c = (2s+1)\omega + W(a,q)$ whenever $n = sk+1 > 1$.

We next show that, given any positive integer c, we can find s, a, q such that

$$c = (2s+1)\omega(a,q) + W(a,q).$$

When c is odd, this is very easy because $W = 0$ whenever $\omega = 1$; thus, we need only put $s = (c-1)/2$, $a = mq+1$. For example, if we have $c = 7$ (a cycle length not previously known), we can put $s = 3, k = t, n = 3k+1, a \equiv 1 \pmod{q}$ and

$$\begin{aligned}
&f_0(g,a,q,k) = qa^{k-g}, \quad f_1(g,a,q,k) = qa^{k+g+1},\\
&f_2(g,a,q,k) = qa^{2k-g}, \quad f_3(g,a,q,k) = qa^{g+1},\\
&f_4(g,a,q,k) = aq^{3k-g} + (a^{k-g-1}-1)/q,\\
&f_5(g,a,q,k) = q, \quad f_6(g,a,q,k) = qa^{2k+g+2} + (a^{g+1}-1)/q.
\end{aligned}$$

We get for $N = (qa^{3k+1} + (a^k - 1)/q)^2 + 4a^{3k+1}$ $(2\,|\,a)$ that the periodic part of the continued fraction expansion of $\nu(N)$ is given by $q_{7g+j+3} = f_j(g,a,q,k)$ for $g = 0,1,2,\ldots,k-1$.

It is also easy to handle this problem when c is even. Since $2\,|\,W(a,q)$, we must have $2\,|\,W$. If we put $\omega = 2$, we get $c = 2(2s+1) + W(a,q)$, but we can find a, q such that $W(a,q) = c - 2(2s+1)$ for any $s \ge 1$ such that $c - 2(2s+1) > 0$. Thus, if $c \ge 8$, we can always produce by this technique cycles of length c. We have already seen that examples exist of cycles of length 2, 4, 6.

When, in the case of odd c, we put $\omega = 1$, we are compelled to make s large in order to produce a large cycle length. We can also do this in another way by using $\omega = 3$. In this case, we have $c = 3(2s+1) + W$. Thus, we can keep s small and try to find $W = c - 3(2s+1)$. For example, consider the case of $c = 13$; we put $s = 1$ and must find a, q such that $W(a,q) = 4$. If we use $D = 21, i = 5, n = 6$, we get $n - i - \chi_{i+1} = 1$ and $(S-1)/T = \langle 1,9,8\rangle$. Hence, $(S-1)/2 = 81$ and $T/2 = 73$; and if $a \equiv 8 \pmod{73}$, $q = 73$, we get $\omega(a,q) = 4$. It follows that if $2\,|\,a$ and $a \equiv 8$ (mod 73), then $\nu(N)$, where

$$N = (73a^{3t+1} + (a^{3t}-1)/73)^2 + 4a^{3t+1}$$

has a cycle length of 13. This cycle is given by $q_{13g+j+3} = f_j(g,a,t)$, where

$$\begin{aligned}
&f_0(g,a,t) = 73a^{3t-3g} + (a^{3t-1-3g} - 64)/73,\\
&f_1(g,a,t) = 1, \quad f_2(g,a,t) = 7, \quad f_3(g,a,t) = 9,\\
&f_4(g,a,t) = 73a^{3g+2} + (a^{3g+1} - 8)/73,\\
&f_5(g,a,t) = 73a^{3t-3g-1} + (a^{3t-3g-2} - 8)/73,\\
&f_6(g,a,t) = 9, \quad f_7(g,a,t) = 7, \quad f_8(g,a,t) = 1,\\
&f_9(g,a,t) = 73a^{3g+3} + (a^{3g+2} - 64)/73,\\
&f_{10}(g,a,t) = 73a^{3t-3g-2} + (a^{3t-3g-3} - 1)/73,\\
&f_{11}(g,a,t) = 73, \quad f_{12}(g,a,t) = 73a^{3g+4} + (a^{3g+3} - 1)/73.
\end{aligned}$$

A more extreme example is provided by putting $i = 0$, $n = 12$. We get $n - i - \chi_{i+1} = 11$, $\eta = 1$,

$$\begin{aligned}
(S-1)/T &= \langle 4,1,1,2,1,1,8,1,1,2,1,1,8,9,1,1,2,1,1,8,1,1,2,2\rangle\\
&= 664670164/1450042921.
\end{aligned}$$

Thus, if

$$N = (1450042921a^{6t+1} + (a^{3t} - 1) / 1450042921)^2 + 4a^{6t+1},$$

where $a \equiv 84498480 \pmod{1450042921}$ and $2 \mid a$, then $\nu(N)$ has a cycle structure with cycle length

$$c = W + (2s+1)\omega = 44 + 15 = 59.$$

REFERENCES

1. L. Bernstein. "Fundamental Units and Cycles." *J. Number Theory* **8** (1976):446-91.
2. L. Bernstein. "Fundamental Units and Cycles in the Period of Real Quadratic Fields, Part II." *Pacific J. Math.* **63** (1976):63-78.
3. F. Halter-Koch. "Einige periodische Kettenbruchentwicklungen und Grundeinheiten quadratischer Ordnung." *Abh. Math. Sem. Univ. Hamburg* **59** (1989):157-69.
4. M. D. Hendy. "Applications of a Continued Fraction Algorithm to Some Class Number Problems." *Math. Comp.* **28** (1974):267-77.
5. R. A. Mollin. *Quadratics*. Boca Raton: CRC Press, 1996.
6. R. A. Mollin & H. C. Williams. "Consecutive Powers in Continued Fractions." *Acta Arith.* **61** (1992):233-64.
7. R. A. Mollin & H. C. Williams. "On the Period Length of Some Special Continued Fractions." *Sém. Théorie des Nombres de Bordeaux* **4** (1992):19-42.
8. R. A. Mollin, A. J. van der Poorten, & H. C. Williams. "Halfway to a Solution of $x^2 - Dy^2 = -3^n$." *J. de Théorie des Nombres* **6** (1994):421-59.
9. M. Nyberg. "Culminating and Almost Culminating Continued Fractions." *Norsk. Mat. Tidsskr.* **31** (1949):95-99.
10. O. Perron. *Die Lehre von der Kettenbrüchen*. Stuttgart: Teubner, 1977.
11. D. Shanks. "On Gauss's Class Number Problems." *Math. Comp.* **23** (1969):151-63.
12. D. Shanks. "Class Number: A Theory of Factorization and Genera." In *Proc. Sympos Pure Math 20*, pp. 415-40. Providence, RI: American Mathematical Society, 1971.
13. A. J. Stephens & H. C. Williams. "Some Computational Results on a Problem Concerning Powerful Numbers." *Math. Comp.* **50** (1988):619-32.
14. A. J. Stephens & H. C. Williams. "Computation of Real Quadratic Fields with Class Number One." *Math. Comp.* **51** (1988):809-24.
15. H. C. Williams. "A Note on the Period Length of the Continued Fraction Expansion of Certain $\sqrt{D}$." *Utilitas Math.* **28** (1985):201-09.
16. H. C. Williams. Some Generalizations of the S_n Sequence of Shanks." *Acta. Arith.* **69** (1995):199-215.
17. H. C. Williams & M. C. Wunderlich. "On the Parallel Generation of the Residues for the Continued Fraction Factoring Algorithm." *Math. Comp.* **177** (1987):405-23.
18. Y. Yamomoto. "Real Quadratic Fields with Large Fundamental Units." *Osaka J. Math.* **8** (1971):261-70.

AMS Classification Number: 11A55