## Some generalizations of the $S_n$ sequence of Shanks

by

H. C. WILLIAMS (Winnipeg, Man.)

1. Introduction. The problem of detecting infinite parametric families  $\mathcal{N}$  of positive non-square integers such that if  $N \in \mathcal{N}$  a unit  $\eta$  of some order in  $\mathbb{Q}(\sqrt{N})$  can be easily predicted is a very old one. Several examples of such families are provided in Chapter XII of Dickson [4]. Perhaps the best known among these parametric families is that of the Richaud–Degert types. For these we have  $N = M^2 + r$  with  $r \mid 4M$ . This itself is a special case of the more general  $N = A^2X^2 + BX + C$ , where  $\Delta \mid 4 \operatorname{gcd}(2A^2, B)^2$  and  $\Delta = B^2 - 4A^2C$ , discovered by Schinzel [12]. Usually the units for these families are given by very simple expressions; for example, in the case of Schinzel's example above a unit  $\eta$  of the maximal order of  $\mathbb{Q}(\sqrt{N})$  is given by

 $\eta = \begin{cases} (2A^2X + B + 2A\sqrt{N})/\sqrt{|\varDelta|} & \text{if } |\varDelta| \text{ is a perfect integral square,} \\ (2A^2X + B + 2A\sqrt{N})^2/|\varDelta| & \text{otherwise.} \end{cases}$ 

Of particular interest, of course, is the question of when the predicted unit is the fundamental unit of the order in question. One way of approaching this question is to make use of continued fractions. In this paper we denote the simple continued fraction expansion of  $\theta$ ,

$$\theta = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\cdots + \frac{1}{q_{n-1} + \frac{1}{\theta_n}}}}}}$$

 $(q_0, q_1, \ldots, q_{n-1} \in \mathbb{Z})$  by  $\theta = \langle q_0, q_1, q_2, \ldots, q_{n-1}, \theta_n \rangle$ . We will concern ourselves with the problem of detecting the fundamental unit  $\varepsilon$  in the order

Research supported by NSERC of Canada Research Grant #A7649.

[199]

 $\mathbb{Z}[\nu]$ , where

and

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

$$\sigma = \begin{cases} 1 & \text{if } N \not\equiv 1 \pmod{4}, \\ 2 & \text{if } N \equiv 1 \pmod{4}. \end{cases}$$

Thus, if N is square-free, we see that  $\varepsilon$  is the fundamental unit of  $\mathbb{Q}(\sqrt{N})$ . It is well known that the continued fraction expansion of  $\nu$  is periodic with period length  $\pi = \pi(N)$  and

$$\nu = \langle q_0, \overline{q_1, q_2, \dots, q_\pi} \rangle.$$

In this case we have  $\theta_0 = \nu$ ,  $\theta_k = (P_k + \sqrt{N})/Q_k$ ,  $q_k = \lfloor \theta_k \rfloor$ ,  $P_{k+1} = q_k Q_k - P_k$ ,  $Q_{k+1} = (N - P_{k+1}^2)/Q_k$  (k = 0, 1, 2, ...). Also,

(1.1) 
$$\varepsilon = \prod_{i=1}^{\pi} \frac{P_i + \sqrt{N}}{Q_i}.$$

In fact, if  $P_j = P_{j+1}$   $(j \le \pi)$ , then  $\pi = 2j$  and

(1.2) 
$$\varepsilon = (Q_j/\sigma) \prod_{i=1}^j \left(\frac{P_i + \sqrt{N}}{Q_i}\right)^2.$$

Thus, if we can find a parametric family of N values such that  $\pi(N)$  is bounded by a small integer, it is a relatively simple matter to predict  $\varepsilon$ . For example, in the case of the Richaud–Degert types we always have  $\pi(N) \leq 6$ .

Let h(d) denote the class number of  $\mathbb{Q}(\sqrt{d})$ . In 1969 Shanks [13] tabulated h(d) for all  $d = n^2 - 8$  such that 0 < d < 10000 and d is a prime or prime power. He discovered that h(d) = 1 except for  $d = 4481 = 67^2 - 8 = (2^6 + 3)^2 - 8$ . This discovery led Shanks to give consideration to numbers of the form

$$S_n = (2^n + 3)^2 - 8 = (2^n + 1)^2 + 4 \cdot 2^n.$$

He was able to give reasons for why one would expect that as n increased one would have  $h(S_n)$  exceeding any given bound. Later in [14] he pointed out without proof that for  $N = S_n$  one would have  $\log \varepsilon = 2n^2 \log 2 + O(n2^{-n})$ . In [17] Yamamoto gave results concerning  $S_n$  which, essentially, are  $P_0 = 1$ ,  $Q_0 = 2$ ,  $q_0 = 2^{n-1} + 1$ ,  $P_{2i-1} = 2^n + 1$ ,  $Q_{2i-1} = 2^{n+2-i}$ ,  $q_{2i-1} = 2^{i+1}$ ,  $P_{2i} = 2^n - 1$ ,  $Q_{2i} = 2^{i+1}$ ,  $q_{2i} = 2^{n-i}$ . Thus,  $\varepsilon = \alpha \gamma^n / 2^n$ , where  $\alpha = (2^n + 1 + \sqrt{S_n})/2$ ,  $\gamma = (2^n + 3 + \sqrt{S_n})/2$ . This seems to be the first example ever found of a parametric family in which a fundamental unit can be easily predicted even though the period length of the continued fraction becomes arbitrarily large.

200

2. Generalizations of Shanks' sequence. Since 1969 a number of generalizations of Shanks' sequence have been described. Hendy [7] considered values of N given by

$$N = (\sigma(qa^n + (a-1)/q)/2)^2 + \sigma^2 a^n, \quad \sigma \in \{1, 2\}$$

with  $q \mid a - 1$ . Here we have  $\pi(N) = 2n + 1$  for  $\nu(N)$  and  $\varepsilon = \alpha \gamma^n / a^n$  with  $\alpha = (qa^n + (a - 1)/q + \sqrt{N})/2$ ,  $\gamma = (q^2a^n + a + 1 + q\sqrt{N})/2$ . Later Bernstein [2], [3] considered

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

 $\mu, \lambda \in \{-1, 1\}$ , and Williams [15] extended this to

$$N = (\sigma(qa^n + \mu(a + \lambda)/q)/2)^2 - \sigma^2 \mu \lambda a^n$$

where  $q\,|\,a+\lambda,\,\mu,\lambda\in\{-1,1\}.$  Leves que and Rhin [9] and Levesque [8] discussed

$$N = (\sigma(ra^{n} + \mu(a+1))/2)^{2} - \sigma^{2}\mu ra$$

with  $\mu = 1$  and  $r \mid a + 1$ . Azuhata [1] examined

$$N = (a^n + \mu(a^k + \lambda))^2 - 4\lambda\mu a^n$$

with  $n > k \ge 1$ , gcd(n, k) = 1.

In [5] Halter-Koch combined all of these forms except that of Azuhata into

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

with  $rq \mid a + \lambda$  and

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

For these values of N he found that  $\pi(N) = cn + b$  where  $c \in \{2, 3, 4, 6, 8\}$ ,  $b \in \{-4, -3, -2, 0, 1, 2, 4\}$ . Also,

$$\varepsilon = \begin{cases} \alpha \gamma^n / a^n & (r=1), \\ \alpha^2 \gamma^{2n} / (ra^{2n}) & (r>1), \end{cases}$$

where

$$\alpha = (\sigma(qra^n + \mu(a+\lambda)/q) + 2\sqrt{N})/(2\sigma),$$
  
$$\gamma = (\sigma(q^2ra^n + \mu(a-\lambda)) + 2q\sqrt{N})/(2\sigma).$$

If we combine the Halter-Koch form with that of Azuhata, we get

(2.1) 
$$N = (\sigma(qra^n + \mu(a^k + \lambda)/q)/2)^2 - \sigma^2 \mu \lambda a^n r$$

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

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

Predicting the value of  $\pi(N)$  for these values of N is much more difficult than for the Halter-Koch cases. For example, if  $r = \mu = -\lambda = 1$ , we get the form considered at some length by Mollin and Williams [10].

**3. Period lengths.** In order to discuss the simple continued fraction period length for  $\nu(N)$  for N given by (2.1) we must define some symbols. Consider positive integers r, s with r > 1. We can find the simple continued fraction expansion of

$$s/r = \langle q_0, q_1, q_2, \dots, q_m \rangle$$

with  $q_m > 1$ . Define  $M(r, s) = 2\lfloor (m+1)/2 \rfloor$ ,  $\overline{M}(r, s) = 2\lfloor m/2 \rfloor + 1$ . Since  $q_m > 1$ , there is no ambiguity in the definition of M(r, s) or  $\overline{M}(r, s)$ . If, for a fixed Q such that gcd(a, Q) = 1, we denote by  $s_i$  that integer satisfying

$$s_i \equiv a^i \pmod{Q}$$

where  $1 \leq s_i < Q$ , then we define

$$W(a,Q) = \sum_{i=1}^{\omega} M(s_i,Q), \quad W'(a,Q) = \sum_{i=1}^{\omega} M(Q-s_i,Q).$$

Here we use  $\omega = \omega(a, Q)$  to represent the multiplicative order of a modulo Q. The functions W(a, Q) and W'(a, Q) have a number of curious properties. We refer the reader to Mollin and Williams [11] for a discussion of W(a, Q). Undoubtedly, a more extensive investigation would reveal many more properties of these interesting number theoretic functions.

In [10] it was shown that for  $r = \mu = -\lambda = 1$  in (2.1) we get

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

In order to obtain the complete story on the period lengths for  $\nu(N)$  with N given by (2.1), we need now to give special attention to the case of  $\lambda = 1$ . If Q > 2, we see that  $2 | \omega(a, Q)$  when  $Q | a^k + 1$ . In this case we get

$$W(a,Q) = W'(a,Q)$$

Also, if we define

$$\chi(s,Q) = \begin{cases} -1 & \text{if } s < Q/2, \ 2 \nmid M(s,Q), \\ 1 & \text{if } s > Q/2, \ 2 \mid M(s,Q), \\ 0 & \text{otherwise} \end{cases}$$

and

$$A(a,Q) = \sum_{i=1}^{\omega/2} \chi(s_i,Q) \quad (\omega = \omega(a,Q)),$$

it is easy to show that

$$2W_1(a,Q) = W(a,Q) + 2A(a,Q), \quad 2W_2(a,Q) = W(a,Q) - 2A(a,Q),$$

where

$$W_1(a,Q) = \sum_{i=1}^{\omega/2} \overline{M}(s_i,Q), \quad W_2(a,Q) = \sum_{i=1}^{\omega/2} \overline{M}(Q-s_i,Q).$$

We now have the following values of  $\pi(N)$  for N given by (2.1). We must partition the problem into several cases.

$$\begin{array}{l} \text{Case A: } \lambda = -1, \ \mu = 1. \\ 1) \ \textit{If } r > 1 \ \textit{and } q > 2, \ \textit{then} \\ \pi(N) = \begin{cases} 2n + k + kW(a^2,q)/(2\omega(a^2,q)) \\ -kW(a^2,qr)/(2\omega(a,qr)) \\ +kW(a,qr)/\omega(a,qr) & \textit{if } 2 \, | \, k, \\ 4n + 2k + kW(a,q)/\omega(a,q) + kW(a,qr)/\omega(a,qr) & \textit{if } 2 \, | \, k. \end{cases}$$

2) If 
$$r > 1$$
 and  $q = 2$ , then

$$\pi(N) = \begin{cases} 2n + k + kW(a, 2r)/\omega(a, 2r) - kW(a^2, 2r)/(2\omega(a^2, 2r)) & \text{if } 2 \mid k, \\ 4n + 2k + kW(a, 2r)/\omega(a, 2r) & \text{if } 2 \nmid k. \end{cases}$$

3) If 
$$r > 2$$
 and  $q = 1$ , then

$$\pi(N) = \begin{cases} 2n + k + kW(a, r)/\omega(a, r) - kW(a^2, r)/(2\omega(a^2, r)) & \text{if } 2 \mid k, \\ 4n + 2k + kW(a, r)/\omega(a, r) & \text{if } 2 \nmid k. \end{cases}$$

4) If r = 2 and q = 1, then

$$\pi(N) = \begin{cases} 2n+k & \text{if } 2 \mid k, \\ 4n+2k & \text{if } 2 \nmid k. \end{cases}$$

5) If r = 1 and q > 2, then  $\pi(N) = 2n + k + kW(a,q)/\omega(a,q)$ . 6) If r = 1 and q = 1, 2, then  $\pi(N) = 2n + k$ .

Case B:  $\lambda = 1, \mu = 1.$ 

$$\begin{aligned} 1) \ & \textit{If} \ r > 1 \ \textit{and} \ q > 2, \ \textit{then} \\ \pi(N) = \begin{cases} 3n + 3k/2 + kW(a^2,q)/(2\omega(a^2,q)) \\ +kW(a,qr)/\omega(a,qr) - kW(a^2,qr)/(2\omega(a^2,qr)) \\ +A(a^2,q) + A(a,qr) - A(a^2,qr) & \textit{if} \ 2 \mid k, \\ 6n + 2k + kW(a,q)/\omega(a,q) + kW(a,qr)/\omega(a,qr) \\ +A(a,q) + A(a,qr) & \textit{if} \ 2 \nmid k. \end{cases} \end{aligned}$$

2) If 
$$r > 1$$
 and  $q = 2$ , then

$$\pi(N) = \begin{cases} 3n + 3k/2 + kW(a, 2r)/\omega(a, 2r) \\ -kW(a^2, 2r)/(2\omega(a^2, 2r)) + A(a, 2r) - A(a^2, 2r) & \text{if } 2 \mid k, \\ 6n + 3k + kW(a, 2r)/\omega(a, 2r) + A(a, 2r) & \text{if } 2 \nmid k. \end{cases}$$

2) If 
$$r > 1$$
 and  $q = 2$ , then  

$$\pi(N) = \begin{cases} 4n - 2 + kW'(a, 2r)/\omega(a, 2r) \\ -kW'(a^2, 2r)/(2\omega(a^2, 2r)) & \text{if } 2 \mid k, \\ 8n - 2 + kW'(a, 2r)/\omega(a, 2r) & \text{if } 2 \nmid k. \end{cases}$$
3) If  $r > 2$  and  $q = 1$ , then  

$$\int \frac{4n - 2 + kW'(a, r)/\omega(a, r)}{kW'(a^2 - r)/(2\omega(a^2 - r)))} dr = \frac{1}{2} |k|$$

$$\pi(N) = \begin{cases} -kW'(a^2, r)/(2\omega(a^2, r)) & \text{if } 2 \mid k, \\ 8n - 2 + kW'(a, r)/\omega(a, r) & \text{if } 2 \nmid k, a > 2, \\ 8n - 6 + kW'(a, r)/\omega(a, r) & \text{if } 2 \nmid k, a = 2. \end{cases}$$

4) If r = 2 and q = 1, then

$$\pi(N) = \begin{cases} 4n - 2 & \text{if } 2 \mid k \\ 8n - 4 & \text{if } 2 \nmid k \end{cases}$$

 $5) If r = 1 and q > 2, then \pi(N) = 4n + kW'(a,q)/\omega(a,q).$   $6) If r = 1 and q = 2, then \pi(N) = 4n - 2.$  7) If q = r = 1, then  $\pi(N) = \begin{cases} 4n - 2 & \text{if } a \neq 2 \text{ and } n > k + 1, \\ 4n - 6 & \text{if } a = 2 \text{ and } n > k + 1, \\ 4n - 6 & \text{if } a = 3 \text{ and } n = k + 1, \\ 4n - 6 & \text{if } a = 3 \text{ and } n = k + 1, \\ 4n - 10 & \text{if } a = 2 \text{ and } n = k + 1, \\ n > 4. \end{cases}$ 

4. Preliminary results. As there are many cases to be considered in Section 3, it is not our intention to give a complete proof of each of them. Rather, we will indicate the proof techniques used for the more difficult cases, particularly where they may differ from those used in [10].

The symbols  $\lambda_j$ ,  $\varepsilon_j$  will have the same meanings as those assigned on p. 236 of [10]. We also put  $\varrho_j = k - n + \lambda_j$  and  $\sigma_j = n - \lambda_j$ . Now let  $Q \in \{q, qr\}$  and put

$$t_{-2,j} = Q, \quad t_{-1,j} \equiv \mu a^{\varrho_j} \pmod{Q},$$

where  $0 < t_{-1,j} < Q$ . Put

$$t_{-2,j}/t_{-1,j} = \langle \mu_{0,j}, \mu_{1,j}, \dots, \mu_{m,j} \rangle,$$

where

$$m = \begin{cases} M(t_{-1,j}, t_{-2,j}) & \text{if } \lambda = -1, \\ \overline{M}(t_{-1,j}, t_{-2,j}) & \text{if } \lambda = 1. \end{cases}$$

Note that  $\lambda = (-1)^{m-1}$ . If we put  $A_{-2,j} = 0$ ,  $A_{-1,j} = 1$  and define

$$t_{n+1,j} = \mu_{n+1,j} t_{n,j} - t_{n-1,j},$$
  
$$A_{n+1,j} = \mu_{n+1,j} A_{n,j} + A_{n-1,j} \quad (-1 \le n \le m-1),$$

we get

$$(4.1) t_{i,j}A_{i+1,j} + t_{i+1,j}A_{i,j} = Q (-2 \le i \le m-1)$$

and

$$A_{m,j} = Q, \quad A_{m-1,j} \equiv \mu a^{\sigma_j} \pmod{Q}.$$

Putting

$$C_{i,j} = a^{\sigma_j} t_{i,j} - \mu \lambda (-1)^i A_{i,j}, \quad D_{i,j} = a^{\varrho_j} A_{i,j} + \mu (-1)^i t_{i,j},$$

we get

(4.2) 
$$C_{i,j}t_{i+1,j} - t_{i,j}C_{i+1,j} = (-1)^{i+1}\mu\lambda Q_{j}$$

(4.3) 
$$D_{i,j}A_{i+1,j} - D_{i+1,j}A_{i,j} = (-1)^i \mu Q$$

(4.4) 
$$D_{i,j}C_{i+1,j} + C_{i,j}D_{i+1,j} = (a^k + \lambda)Q,$$

(4.5) 
$$D_{i+1,j} = \mu_{i+1,j} D_{i,j} + D_{i-1,j},$$

(4.6) 
$$C_{i-1,j} = \mu_{i+1,j}C_{i,j} + C_{i+1,j} \quad (-1 \le i \le m-1).$$

Now it is easy to show by induction, using (4.5) and (4.6), that  $Q | C_{i,j}$ and  $Q | D_{i,j}$  for  $-2 \le i \le m$ . Also,  $D_{-2,j} = C_{m,j} = \mu Q$ ;  $D_{i,j} \ge 0$  for  $-1 \le i \le m$ , and  $C_{i,j} \ge 0$  for  $-2 \le i \le m - 1$ . Furthermore, if  $D_{i,j} = 0$ , then  $\mu = 1$ ,  $Q > a^{\varrho_j}$ , i = -1; or  $\mu = -1$ ,  $t_{0,j} = a^{\varrho_j}$ ,  $\mu_{0,j} = 1$ , i = 0,  $Q > a^{\varrho_j}$ . If  $C_{i,j} = 0$ , then  $\mu = 1$ ,  $Q > a^{\sigma_j}$ , i = m - 1; or  $\mu = -1$ ,  $t_{m-2,j} = 1$ ,  $A_{m-2,j} = Q - a^{\sigma_j}$ , i = m - 2,  $Q > a^{\sigma_j}$ .

Let  $T = (\sigma/2)(qra^n + \mu(a^k + \lambda)/q)$ . In most cases we have

$$\lfloor \sqrt{N} \rfloor = \begin{cases} T & \text{if } \mu \lambda < 0, \\ T - 1 & \text{if } \mu \lambda > 0. \end{cases}$$

If, as in [10], we put  $R_h = (P_h + \lfloor \sqrt{N} \rfloor)/\sigma$  and  $S_h = Q_h/\sigma$  (h = 0, 1, 2, ...), we have the following results.

THEOREM 4.1. If j < n-1 and

$$\begin{split} R_h &= (qr/Q) a^n t_{i-1,j} A_{i,j} + \mu C_{i-1,j} D_{i,j}/(qQ), \\ S_h &= (qr/Q) a^n t_{i,j} A_{i,j} + \mu C_{i,j} D_{i,j}/(qQ) \quad (-1 \leq i \leq m-1), \end{split}$$

then  $q_h = \mu_{i+1,j}$ .

In order to prove Theorem 4.1 we require two lemmas.

LEMMA 4.2. If  $-1 \le i \le m - 1$ , then  $S_h > D_{i,j}/q$ .

Proof. Suppose that  $i \ge 0$  and  $C_{i+1,j} > 0$ . In this case  $D_{i+1,j} > D_{i,j} \ge 0$ and  $C_{i+1,j} \ge Q$ . By (4.4) we have

$$(a^k + \lambda)Q \ge D_{i,j}Q + C_{i,j}D_{i,j}.$$

Hence

$$S_h \ge a^n - C_{i,j} D_{i,j} / (qQ) \ge a^n - (a^k + \lambda) / q + D_{i,j} / q > D_{i,j} / q$$

The particular cases of i = -1,  $C_{i+1,j} < 0$  (i = m - 1) or  $C_{i+1,j} = 0$  (i = m - 2, m - 3) can be dealt with separately. In each case it can be shown that  $S_h > D_{i,j}/q$ .

LEMMA 4.3. If  $r, s \in \mathbb{Z}$ ,  $s \nmid r$  and either  $|\alpha - r/s| < 1/s$  or  $-1/s \le \alpha - r/s \le 0$ , then  $|\alpha| = |r/s|$ .

Proof of Theorem 4.1. We first note that

$$q_h = \begin{cases} \lfloor (\sigma R_h - 1) / (\sigma S_h) \rfloor & \text{if } \mu \lambda > 0, \\ \lfloor R_h / S_h \rfloor & \text{if } \mu \lambda < 0. \end{cases}$$

Also, from (4.2) we get

$$t_{i,j}R_h - t_{i-1,j}S_h = D_{i,j}(-1)^i \lambda/q.$$

If  $S_h | R_h$ , then  $S_h | D_{i,j}/q$ . Since, by Lemma 4.2,  $S_h > D_{i,j}/q$ , we can only have  $D_{i,j}/q = 0$ .

If  $S_h \nmid R_h$ , then  $q_h = \lfloor R_h / S_h \rfloor$  by Lemma 4.3. Thus, if  $S_h \nmid R_h$ , we get

$$\left|\frac{R_h}{S_h} - \frac{t_{i-1,j}}{t_{i,j}}\right| = \frac{D_{i,j}}{qS_h t_{i,j}} < \frac{1}{t_{i,j}}.$$

If  $S_h | R_h$ , we get  $R_h = ct_{i-1,j}$ ,  $S_h = ct_{i,j}$  with c > 1. Hence,

$$\left|\frac{\sigma R_h - 1}{\sigma S_h} - \frac{t_{i-1,j}}{t_{i,j}}\right| = \frac{1}{\sigma S_h} < \frac{1}{t_{i,j}}$$

Thus, if  $t_{i,j} \nmid t_{i-1,j}$ , we get  $q_h = \mu_{i+1,j}$  by Lemma 4.3.

If  $t_{i,j} | t_{i-1,j}$ , then  $t_{i,j} = 1$  and i = m-1 or m-2. In these cases it is easy to show that  $D_{i,j} \neq 0$ , as  $\sigma_i \neq 0$  and  $\varrho_j \neq 0$  (j < n-1). If i = m-2, then  $t_{m-3,j} = \mu_{m-1,j} + 1$  and  $R_h - t_{m-3,j}S_h < 0$ . Hence

$$\lfloor R_h/S_h \rfloor = t_{m-3,j} - 1 = \mu_{m-1,j}.$$

If i = m - 1, then

$$\lfloor R_h/S_h \rfloor = t_{m-2,j} = \mu_{m,j}. \blacksquare$$

The following result can be proved in the same manner as Lemma 5.2 of [10] except that we use (4.1)-(4.3).

THEOREM 4.4. If  $R_h$  and  $S_h$  are given by the formulas of Theorem 4.1, then

$$R_{h+1} = q_h S_h - R_h + 2T/\sigma = (qr/Q)a^n t_{i,j}A_{i+1,j} + \mu C_{i,j}D_{i+1,j}/(qQ)$$
  

$$S_{h+1} = (2T/\sigma)R_{h+1} - R_{h+1}^2 - \mu\lambda ra^n$$
  

$$= (qr/Q)a^n A_{i+1,j}t_{i+1,j} + \mu C_{i+1,j}D_{i+1,j}/(qQ). \blacksquare$$

**5.** An example. In this section we will develop the continued fraction expansion of  $\nu(N)$  for certain N with  $\lambda = 1$ ,  $\mu = -1$ , r > 1. We do this to exemplify the techniques that were used to obtain all the results of Section 3.

However, in the interest of brevity, we will concentrate our efforts here on a few particular cases.

We define

$$\begin{split} \gamma_j^* &\equiv a^{\varrho_j} \pmod{qr}, \quad \gamma_j \equiv a^{\varrho_j} \pmod{q}, \\ \delta_j^* &\equiv a^{\varrho_j} \pmod{qr}, \quad \delta_j \equiv a^{\varrho_j} \pmod{q}, \end{split}$$

where  $0 < \gamma_j^*, \delta_j^* < qr, 0 \le \gamma_j, \delta_j < q$ . Put  $t_{i,j}^* = t_{i,j}, A_{i,j}^* = A_{i,j}, C_{i,j}^* = C_{i,j}, D_{i,j}^* = D_{i,j}$ , where the  $t_{i,j}, A_{i,j}, C_{i,j}, D_{i,j}$  are those defined in Section 4 with Q = qr. Put  $t_{i,j}, A_{i,j}, C_{i,j}, D_{i,j}$  to be those defined in Section 4 with Q = q.

We also define

$$\eta(i) = 3 + \varepsilon_i w_i \quad (0 \le i \le n - 1)$$

where  $w_i = 0$  when  $\varepsilon_i = 0$ . Since

$$\sum_{i=0}^{n-2} \varepsilon_i = \lfloor k(n-1)/n \rfloor = k-1,$$

we see that there are exactly k - 1 values of  $i \in \{1, \ldots, n - 2\}$  such that  $\varepsilon_i = 1$ . Let  $i_1, \ldots, i_{k-1}$  be those values of i. Then

$$\sum_{j=0}^{i_h-1} \varepsilon_j = h-1 \quad \text{and} \quad \sum_{j=0}^{i_h} \varepsilon_j = h;$$

thus,  $i_h$  is the least value of j such that  $\lfloor (j+1)k/n \rfloor = h$ . It follows that  $j \geq \lfloor hn/k \rfloor$ . Since for  $j = \lfloor hn/k \rfloor$  we get  $\lfloor (j+1)k/n \rfloor = h$ , we have  $j = i_h = \lfloor hn/k \rfloor$ . If  $\varepsilon_j = 1$ , where  $j = i_h$ , we put

$$w_j = \begin{cases} \overline{M}(qr - \gamma_j^*, qr) & \text{if } 2 \nmid h, \\ \overline{M}(q - \gamma_j, q) & \text{if } 2 \mid h. \end{cases}$$

Define

$$\psi(j) = 1 + \sum_{i=0}^{j-1} \eta(i) \quad (1 \le j \le n-1).$$

We will now deal with the case of q > 2. In this case we get  $\lfloor \sqrt{N} \rfloor = T$ and

$$\begin{split} R_0 &= 1 + (T-1)/\sigma, \quad S_0 = 1, \quad q_0 = 1 + (T-1)/\gamma; \\ R_1 &= 2T/\sigma, \quad S_1 = ra^n, \quad q_1 = q-1; \\ R_2 &= (q-1)ra^n, \quad S_2 = qra^n + (a^k+1)/q - ra^n - a^k, \quad q_2 = 1; \\ R_3 &= qra^n - a^k, \quad S_3 = a^k, \quad q_3 = qra^{n-k} - 1. \end{split}$$

By making use of Theorem 4.4 and the techniques of [10] we can now develop the continued fraction expansion of  $\nu(N)$ . For  $1 \leq h \leq k-1, \, \lfloor hn/k \rfloor \leq j < \lfloor (h+1)n/k \rfloor, \, j < n-1, \, 2 \nmid h, \, s = \psi(j),$  we get

$$R_s = 2T/\sigma, \quad S_s = ra^{n-\lambda_j},$$
$$q_s = \begin{cases} qa^{\lambda_j} - 1 & \text{if } \varepsilon_j = 0, \\ qa^{\lambda_j} - 1 - (a^{k+\lambda_j - n} - \gamma_j^*)/(qr) & \text{if } \varepsilon_j = 1. \end{cases}$$

If, in this case  $\varepsilon_j = 0$ , then  $\psi(j+1) = \psi(j) + 3$  and

$$\begin{aligned} R_{s+1} &= qra^n - ra^{n-\lambda_j}, \\ S_{s+1} &= qra^n + (a^k + 1)/q - ra^{n-\lambda_j} - a^{\lambda_j + k}, \quad q_{s+1} = 1; \\ R_{s+2} &= qra^n - a^{\lambda_j + k}, \quad S_{s+2} = a^{\lambda_j + k}, \quad q_{s+2} = qra^{n-\lambda_j - k} - 1. \end{aligned}$$

If  $\varepsilon_i = 1$ , then let  $m = \overline{M}(qr - \gamma_j^*, qr)$ . We get  $\psi(j+1) = \psi(j) + m + 3$ and for  $-1 \le i \le m$ ,

$$R_{s+i+2} = a^n t^*_{i-1,j} A^*_{i,j} - C^*_{i-1,j} D^*_{i,j} / (q^2 r),$$
  

$$S_{s+i+2} = a^n t^*_{i,j} A^*_{i,j} - C^*_{i,j} D^*_{i,j} / (q^2 r),$$
  

$$q_{s+i+2} = \begin{cases} \mu_{i+1,j} & \text{if } i < m, \\ q a^{n-\lambda_{j+1}} - 1 - (a^{k-\lambda_{j+1}} - \delta^*_j) / (qr) & \text{if } i = m. \end{cases}$$

For  $1 \leq h \leq k-1, \, \lfloor hn/k \rfloor \leq j < \lfloor (h+1)n/k \rfloor, \, j < n-1, \, 2 \, | \, h, \, s = \psi(j),$  we get

$$R_s = 2T/\sigma, \quad S_s = a^{n-\lambda_j},$$
$$q_s = \begin{cases} qra^{\lambda_j} - 1 & \text{if } \varepsilon_j = 0, \\ qra^{\lambda_j} - 1 - (a^{k+\lambda_j - n} - \gamma_j)/(qr) & \text{if } \varepsilon_j = 1. \end{cases}$$

If, in this case,  $\varepsilon_j = 0$ , then  $\psi(j+1) = \psi(j) + 3$  and

$$\begin{aligned} R_{s+1} &= qra^n - a^{n-\lambda_j}, \\ S_{s+1} &= qra^n + (a^k + 1)/q - ra^{\lambda_j + k} - a^{n-\lambda_j}, \quad q_{s+1} = 1; \\ R_{s+2} &= qra^n - ra^{\lambda_j + k}, \quad S_{s+2} = ra^{\lambda_j + k}, \quad q_{s+2} = qa^{n-\lambda_j - k} - 1. \end{aligned}$$

If  $\varepsilon_i = 1$ , then let  $m = \overline{M}(q - \gamma_j, q)$ . We get  $\psi(j+1) = \psi(j) + m + 3$  and for  $-1 \le i \le m$ 

$$\begin{aligned} R_{s+i+2} &= ra^n t_{i-1,j} A_{i,j} - C_{i-1,j} D_{i,j}/q^2, \\ S_{s+i+2} &= ra^n t_{i,j} A_{i,j} - C_{i,j} D_{i,j}/q^2, \\ q_{s+i+2} &= \begin{cases} \mu_{i+1,j} & \text{if } i < m, \\ qra^{n-\lambda_{j+1}} - 1 - (a^{k-\lambda_{j+1}} - \delta_j)/q & \text{if } i = m. \end{cases} \end{aligned}$$

If we put j = n - 1,  $\theta = \psi(n - 1) - 1$ , we get  $\varepsilon_{n-1} = 1$ ,  $\lambda_{n-1} = n - k$ . If

 $2 \mid k - 1$ , then

$$\begin{split} R_{\theta+1} &= 2T/\sigma, \quad S_{\theta+1} = ra^k, \quad q_{\theta+1} = qa^{n-k} - 1; \\ R_{\theta+2} &= qra^n - ra^k, \quad S_{\theta+2} = qra^n + (a^k + 1)/q - ra^k - a^n, \quad q_{\theta+2} = 1; \\ R_{\theta+3} &= qra^n - a^k, \quad S_{\theta+3} = a^n, \quad q_{\theta+3} = qr - 1; \\ R_{\theta+4} &= 2T/\sigma, \quad S_{\theta+4} = r, \quad q_{\theta+4} = qa^n - (a^k + 1)/(rq). \end{split}$$

Also,  $R_{\theta+5} = 2T/\sigma = R_{\theta+4}$ . Since  $R_i = R_{i+1}$  can occur at most once in the period of the continued fraction expansion of  $\nu(N)$  and since no value of  $S_i = 1$  for  $i \leq \theta + 5$  (see Lemma 4.2), we must have  $\pi(N) = 2(\theta + 4)$ .

If  $2 \nmid k - 1$ , then we find that

$$\begin{aligned} R_{\theta+1} &= 2T/\sigma, \quad S_{\theta+1} = a^k, \quad q_{\theta+1} = qra^{n-k} - 1; \\ R_{\theta+2} &= qra^n - a^k, \quad S_{\theta+2} = qra^n + (a^k + 1)/q - a^k - ra^n, \quad q_{\theta+2} = 1; \\ R_{\theta+3} &= qra^n - ra^n, \quad S_{\theta+3} = ra^n, \quad q_{\theta+3} = q - 1; \\ R_{\theta+4} &= 2T/\sigma, \quad S_{\theta+4} = 1; \end{aligned}$$

hence,  $\pi(N) = \theta + 4$ .

It remains to evaluate  $\psi(n-1)$ . Clearly

$$\psi(n-1) = 3n - 3 + \sum_{h=1}^{k-1} w_{i_h}$$

Putting  $t_h = q - \gamma_{i_h}, t_h^* = qr - \gamma_{i_h}^*$ , we get

$$t_h \equiv (-1)^{\lfloor hn/k \rfloor} a^{-nk} \pmod{q}, \quad t_h^* \equiv (-1)^{\lfloor hn/k \rfloor} a^{-nh} \pmod{qr}.$$

If we put

$$\Omega = \sum_{2|h, h=1}^{k-1} \overline{M}(t_h, q) + \sum_{2 \nmid h, h=1}^{k-1} \overline{M}(t_h^*, qr),$$

then  $\psi(n-1) = 3n - 3 + \Omega$ .

If k is odd, then

$$\Omega = \sum_{i=1}^{(k-1)/2} \overline{M}(t_{2i}, q) + \sum_{i=1}^{(k-1)/2} \overline{M}(t_{2i-1}^*, qr).$$

Also, if  $h \neq k$ , then  $t_{k-h} \equiv -t_h^{-1} \pmod{q}$  from which it is easy to show that

$$\overline{M}(t_{k-h},q) = \overline{M}(t_h,q).$$

Similarly

$$\overline{M}(t_{k-h}^*, q) = \overline{M}(t_h^*, q) \quad (k \neq h).$$

Since k - h and h have opposite parity, it follows that we can write

$$2\Omega = \sum_{i=1}^{k-1} \overline{M}(t_i, q) + \sum_{i=1}^{k-1} \overline{M}(t_i^*, qr).$$

Now Q > 2 means that  $\omega(a, Q) = 2\mu$  where  $\mu$  is odd and  $\mu \mid k$ . Hence, by the remarks at the beginning of Section 3 we have

$$\sum_{j=1}^{k} \overline{M}(Q - S_j, Q) = \lfloor k/\omega(a, Q) \rfloor W'(a, Q) + W_2(a, Q)$$
$$= kW(a, Q)/\omega(a, Q) - A(a, Q).$$

If we consider the sum  $\sum_{i=1}^{k-1} \overline{M}(t_i, q)$  and sum this over  $j \equiv -in \pmod{k}$ , we get

$$\sum_{i=1}^{k-1} \overline{M}(t_i, q) = \sum_{j=1}^{k-1} \overline{M}(q - s_j, q).$$

Also,

$$\sum_{i=1}^{k-1} \overline{M}(t_i^*, qr) = \sum_{j=1}^{k-1} \overline{M}(qr - s_j^*, qr),$$

where  $s_i \equiv a^i \pmod{q}$ ,  $s_i^* \equiv a^i \pmod{qr}$ ,  $0 < s_i \le q$ ,  $0 < s_i^* < qr$ . Thus, we get

$$\pi(N) = 6n + kW(a,qr)/\omega(a,qr) + kW(a,q)/\omega(a,q) - A(a,qr) - A(a,q).$$

To obtain the result when  $2 \mid k$ , we note that

$$\sum_{2 \nmid h, h=1}^{k} \overline{M}(t_h^*, qr) = \sum_{2 \nmid j, j=1}^{k} \overline{M}(q - s_j^*, qr)$$

and

$$\sum_{2|h,h=1}^{k} \overline{M}(t_h,q) = \sum_{2|j,j=1}^{k} \overline{M}(q-s_j,q).$$

Also,

$$\sum_{\substack{2|j, j=1}}^{k} \overline{M}(q - s_j, q) = \sum_{i=1}^{k/2} \overline{M}(q - s_{2i}, q)$$
$$= \lfloor k/(2\omega(a^2, q)) \rfloor W'(a^2, q) + W_2(a^2, q)$$

and

$$\sum_{2 \nmid j, j=1}^{k} \overline{M}(qr - s_{j}^{*}, qr) = \sum_{i=1}^{k} \overline{M}(qr - s_{i}^{*}, qr) - \sum_{i=1}^{k/2} \overline{M}(qr - s_{2i}^{*}, qr).$$

6. The fundamental units. The method of [10] can be extended to determine the values of  $P_i, Q_i$   $(i = 1, 2, ..., \pi(N))$  for any N given by (2.1). We can then use (1.1) to produce the value of  $\varepsilon$ . Curiously, although the formulas for  $\pi(N)$  given above are quite complicated, the values for  $\varepsilon$  are very simple and are given below.

Define

$$\alpha = (\sigma(qra^n + \mu(a^k + \lambda)/q) + 2\sqrt{N})/(2\sigma),$$
  
$$\gamma = (\sigma(q^2ra^n + \mu(a^k - \lambda)) + 2q\sqrt{N})/(2\sigma).$$

If r = 1, then

$$\varepsilon = \alpha^k \gamma^n / a^{kn}$$
 and  $N(\varepsilon) = (\mu \lambda)^k (-\lambda)^n$ .

If r > 1, then

$$\varepsilon = \begin{cases} \alpha^k \gamma^n / (r^{k/2} a^{kn}) & \text{if } 2 \mid k, \\ \alpha^{2k} \gamma^{2n} / (r^k a^{2kn}) & \text{if } 2 \nmid k. \end{cases}$$

In each of these cases  $N(\varepsilon) = 1$ .

We indicate how these results can be proved by once again discussing one case only. The proofs for the remaining cases are similar or simpler.

We first note that by making use of the identities given in Section 1 we can easily show that if  $\varphi_i = (P_i + \sqrt{N})/Q_i$ , then

$$\varphi_i \varphi_{i+1} = (P_{i+1}q_i + Q_{i+1} + q_i \sqrt{N})/Q_{i+1}.$$

Also, if we put

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

we get  $\alpha\beta = ra^n\gamma$ .

We consider the example of N with  $\mu = -1$ ,  $\lambda = 1$ , r > 1, q > 2discussed in Section 5. Let s, j and h have the meanings assigned to them in the continued fraction development of  $\nu(N)$  given in Section 5. If  $\varepsilon_j = 0$ , we get

$$\varphi_{s+1}\varphi_{s+2} = \begin{cases} \beta/a^{\lambda_j+k} & (2 \nmid h), \\ \beta/(ra^{\lambda_j+k}) & (2 \mid h). \end{cases}$$

Also,

$$\varphi_s = \begin{cases} \alpha/(ra^{n-\lambda_j}) & (2 \nmid h), \\ \alpha/a^{n-\lambda_j} & (2 \mid h). \end{cases}$$

Thus, if  $\varepsilon_j = 0$ , then

$$\varphi_s \varphi_{s+1} \varphi_{s+2} = \alpha \beta / (ra^{n+k}) = \gamma / a^k.$$

If  $\varepsilon_j = 1$ , set

$$\chi_j = \prod_{i=1}^{m+2} \varphi_{s+i}.$$

If we put

$$\varphi'_0 = (P_s + \sqrt{N})/Q_s = \langle q'_0, q'_1, q'_2, \ldots \rangle,$$
  
and  $A'_i/B'_i = \langle q'_0, q'_1, \ldots, q'_i \rangle$  with  $gcd(A'_i, B'_i) = 1$  and  $B'_i > 0$ , then we get  
 $\chi_j = Q_s(A'_{m+1} - B'_{m+1}\overline{\varphi}'_0)/Q_{s+m+2}.$ 

(See, for example, Williams and Wunderlich [16]).

If  $2 \nmid h$ , then

$$\varphi'_0 = \alpha/(ra^{n-\lambda_j}), \quad q'_0 = qa^{\lambda_j} - 1 - (a^{k-n+\lambda_j} - \gamma_j^*)/(qr), q'_i = \mu_{i-1,j} \quad (i = 1, 2, \dots, m+1).$$

Since

$$\langle \mu_{0,j}, \mu_{1,j}, \dots, \mu_{m,j} \rangle = qr/(qr - \gamma_j^*)$$

we get

$$\langle q'_0, q'_1, \dots, q'_{m+1} \rangle = q'_0 + (qr - \gamma_j^*)/(qr) = (q^2 r a^{\lambda_j} - a^{k-n+\lambda_j})/(qr).$$

Hence,

$$A'_{m+1} = q^2 r a^{\lambda_j} - a^{k-n+\lambda_j}, \quad B'_{m+1} = qr$$

Now,  $Q_s = \sigma r a^{n-\lambda_j}$  and  $Q_{s+m+2} = \sigma r a^{\lambda_{j+1}}$ ; therefore  $\chi_j = \gamma/a^{\lambda_{j+1}} = \gamma/a^{k-n+\lambda_{j+1}}$ . Furthermore,

$$\varphi_s \chi_j = \gamma/(ra^k) \quad (2 \nmid h).$$

By similar reasoning it can be shown that

$$\varphi_s \chi_j = \gamma/a^k \quad (2 \mid h).$$

We also note that

$$\varphi_{\theta+1}\varphi_{\theta+2}\varphi_{\theta+3} = \gamma/a^k$$
 and  $\varphi_{\theta+4} = \begin{cases} \alpha & \text{if } 2 \nmid k, \\ \alpha/r & \text{if } 2 \mid k. \end{cases}$ 

We are now ready to evaluate  $\zeta = \prod_{i=1}^{\theta+4} \varphi_i$ . We note that there are k-1 values of  $j = \lfloor hn/k \rfloor (h = 1, \dots, k-1)$  such that  $\varepsilon_j = 1$  and  $j \leq n-2$ . Of these exactly (k-1)/2 are such that h is odd when k is odd and exactly k/2 of these are such that h is odd when k is even. Thus, if  $2 \nmid k$ , then

$$\begin{split} \zeta &= r^{(k-1)/2} \Big( \prod_{\substack{0 \le j \le n-2 \\ \varepsilon_j = 0}} (\gamma/a^k) \prod_{\substack{0 \le j \le n-2 \\ \varepsilon_j = 1}} \gamma \alpha/(ra^k) \Big) (\gamma/a^k) \alpha \\ &= r^{(k-1)/2} (\gamma/a^k)^{n-1-(k-1)} (\gamma a/(ra^k))^{k-1} (\alpha \gamma/a^k) \\ &= a^k \gamma^n / (r^{(k-1)/2} a^{nk}). \end{split}$$

Since in this case we have  $P_{\theta+4} = P_{\theta+5}$ , we see by (1.2) that

$$\varepsilon = (Q_{\theta+4}/\sigma)\zeta^2 = \gamma^{2n}\alpha^{2k}/(r^ka^{2nk})$$

when  $2 \nmid h$ . If  $2 \mid k$ , then

$$\varepsilon = \zeta = r^{k/2} (\gamma/a^k)^{n-k} (\gamma \alpha/(ra^k))^{k-1} (\gamma \alpha)/(ra^k) = \gamma^n \alpha^k/(r^{k/2}a^{nk}).$$

It would be of some considerable interest to produce a simpler proof of the fundamentality of these units than that afforded by producing the very intricate continued fraction period of  $\nu(N)$ ; however, no such technique is known to the author. Also, from the above formulas for  $\varepsilon$ , we see that the regulator R of  $\mathbb{Q}(\sqrt{N})$  is  $O((\log N)^2)$ . It would be of very great interest if an infinite parametric family of N values could be produced such that for each N the complete continued fraction period could be predicted but  $R \gg (\log N)^3$ . No such family is known, although the family given by Yamamoto [17] (see also Halter-Koch [6]):

$$N = (a^n r + a - 1)^2 + 4ra^n,$$

where a, r are primes and a < r, is such that  $R \gg (\log N)^3$  infinitely often. Nevertheless, no one knows (beyond a certain point) how to predict its period. For example, if a = 3, r = 5 we get

n	$\pi(N)$
2	29
3	81
4	217
5	652
6	1801
7	2216
8	22206
9	44776
10	20968
11	61748
12	566474

## References

- T. Azuhata, On the fundamental units and the class numbers of real quadratic fields II, Tokyo J. Math. 10 (1987), 259–270.
- [2] L. Bernstein, Fundamental units and cycles, J. Number Theory 8 (1976), 446-491.
- [3] —, Fundamental units and cycles in the period of real quadratic fields, Part II, Pacific J. Math. 63 (1976), 63–78.
- [4] L. E. Dickson, History of the Theory of Numbers, Vol. II, Chelsea, 1971.
- [5] F. Halter-Koch, Einige periodische Kettenbruchentwicklungen und Grundeinheiten quadratischer Ordnung, Abh. Math. Sem. Univ. Hamburg 59 (1989), 157–169.
- [6] —, Reell-quadratische Zahlkörper mit grosser Grundeinheit, ibid., 171–181.
- M. D. Hendy, Applications of a continued fraction algorithm to some class number problems, Math. Comp. 28 (1974), 267–277.

- C. Levesque, Continued fraction expansions and fundamental units, J. Math. Phys. Sci. 22 (1988), 11–14.
- C. Levesque and G. Rhin, A few classes of periodic continued fractions, Utilitas Math. 30 (1986), 79–107.
- [10] R. A. Mollin and H. C. Williams, Consecutive powers in continued fractions, Acta Arith. 61 (1992), 233–264.
- [11] —, —, On the period length of some special continued fractions, Sém. Théorie des Nombres de Bordeaux 4 (1992), 19–42.
- [12] A. Schinzel, On some problems of the arithmetical theory of continued fractions, Acta Arith. 6 (1961), 393–413.
- [13] D. Shanks, On Gauss's class number problems, Math. Comp. 23 (1969), 151-163.
- [14] —, Class number, a theory of factorization and genera, in: Proc. Sympos. Pure Math. 20, Amer. Math. Soc., Providence, R.I., 1971, 415–440.
- [15] H. C. Williams, A note on the period length of the continued fraction expansion of certain  $\sqrt{D}$ , Utilitas Math. 28 (1985), 201–209.
- [16] H. C. Williams and M. C. Wunderlich, On the parallel generation of the residues for the continued fraction factoring algorithm, Math. Comp. 48 (1987), 405–423.
- [17] Y. Yamamoto, Real quadratic fields with large fundamental units, Osaka J. Math. 8 (1971), 261–270.

DEPARTMENT OF COMPUTER SCIENCE UNIVERSITY OF MANITOBA WINNIPEG, MANITOBA CANADA R3T 2NT

Received on 22.2.1993

(2383)