ACTA ARITHMETICA
LXI.3 (1992)

Consecutive powers in continued fractions

by

R. A. Mollin (Calgary, Alta.) and H. C. Williams (Winnipeg, Man.)

1. Introduction. Let $N > 0$ be a square-free integer throughout and let $\sigma = 2$ (respectively $\sigma = 1$) if $N \equiv 1 \pmod 4$ (respectively $N \equiv 2, 3 \pmod 4$). Set $\omega = (\sigma - 1 + \sqrt{N})/\sigma$. The main purpose herein is to give a complete description of all the reduced ideals which are in the principal class of $\mathbb{Q}(\sqrt{N})$ whenever N is such that the norms of three or more consecutive (as determined by the continued fraction expansion of ω (see [13])) principal reduced ideals are powers of a single given integer $a > 1$. This assumption allows us to give a remarkable explicit formula for the period length of the continued fraction expansion of ω in terms of this phenomenon. Moreover, we are also able to give an upper bound on the regulator of $\mathbb{Q}(\sqrt{N})$ in this instance. Examples are also provided.

Shanks [11] has shown that the ordering of the reduced principal ideals in a real quadratic field K (as determined by the continued fraction algorithm) conforms to a certain structure within the principal ideal class. He called this structure the "infrastructure" of the class. Because of the importance of this continued fraction ordering scheme, we will employ it here and, throughout the paper, use terms like "consecutive" or "in a row" with reference to this particular ordering. We point out that the assumption that the norms of *less than three consecutive reduced principal ideals* be powers of a single integer $a > 1$, provides us with very little information concerning the set of reduced principal ideals. It is therefore rather remarkable how the simple assumption that 3 consecutive norms in a row are powers of $a > 1$ allows us to determine so completely the principal period of reduced ideals of $K = \mathbb{Q}(\sqrt{N})$ including a simple formula for the period length.

There are two cases, one of which we show will allow for at most 4 consecutive norms in a row being powers of a. The complete description is given in Section 3. We are also able in both cases to give a remarkable explicit formula for the period length of the continued fraction expansion of ω. Examples to illustrate the major theorems are also presented.

In Section 6 we give an upper bound on the regulator of $\mathbb{Q}(\sqrt{N})$, when

the aforementioned phenomenon of at least 3 norms in a row occur as powers of a. Section 7 contains only the proofs of the 10 lemmas in Sections 3–5, acting therefore as an appendix.

This continues work in [7]–[9] as well as related work by Levesque *et al.* in [5], [6], Bernstein [1], [2] and Hendy [4].

2. Continued fractions. We will need some basic facts concerning continued fractions given below. For a more detailed presentation of this material the reader is referred to [3] or [10]. Let $N > 0$ be a positive square-free integer and let

$$\sigma = \begin{cases} 2 & \text{if } N \equiv 1 \pmod 4, \\ 1 & \text{if } N \equiv 2, 3 \pmod 4. \end{cases}$$

Set $\omega = (\sigma - 1 + \sqrt{N})/\sigma$. Then $\omega = \langle q_0, \overline{q_1, \ldots, q_\pi} \rangle$ is the continued fraction expansion of ω with period length π. Here $q_0 = \lfloor \omega \rfloor$ and $q_i = \lfloor (P_i + \sqrt{N})/Q_i \rfloor$ for $i \geq 1$ where $\lfloor\ \rfloor$ denotes the greatest integer function; and $(P_0, Q_0) = (\sigma - 1, \sigma)$ with $P_{i+1} = q_i Q_i - P_i$ for $i \geq 0$ and $Q_{i+1} Q_i = N - P_{i+1}^2$ for $i \geq 0$.

It can be shown that $q_i < q_0$ for $\pi > i \geq 1$; while $P_i < \sqrt{N}$, $Q_i < 2\sqrt{N}$, and $-1 < (P_i - \sqrt{N})/Q_i < 0$ for $i \geq 1$. Moreover, if $N \equiv 1 \pmod 4$ then

$$\omega = \langle q_0, \overline{q_1, q_2, \ldots, q_{\pi-1}, 2q_0 - 1} \rangle .$$

If $N \equiv 2, 3 \pmod 4$ then

$$\omega = \langle q_0, \overline{q_1, q_2, \ldots, q_{\pi-1}, 2q_0} \rangle .$$

Also, we note the symmetry properties of the continued fraction expansion of ω, viz.

$$\begin{aligned} P_{i+1} &= P_{\pi-i} && \text{for } i \geq 1 , \\ Q_i &= Q_{\pi-i}, && \text{for } i \geq 0 \text{ and for } i \geq 1 , \\ q_i &= q_{\pi-i} . \end{aligned}$$

3. Consecutive powers of the Q_i/Q_0's. In what follows we wish to investigate the conditions for the existence of at least three consecutive Q_i/Q_0's in a row being the power of a single integer $a > 1$ in the continued fraction expansion of ω. We will (see below) have an overriding hypothesis throughout (unless specified otherwise).

Also, the sequence of reduced ideals which belong to the principal class is given by $I_1, I_2, \ldots, I_k, \ldots$ where

$$I_j = (Q_j/\sigma)\mathbb{Z} + ((P_j + \sqrt{N})/\sigma)\mathbb{Z} \quad \text{where } j = 1, 2, \ldots$$

We have $I_k = I_{\pi+k}$ and the norm of I_k, denoted by $N(I_k)$, is $Q_k/\sigma = Q_k/Q_0$. Thus if $N(I_i)$, $N(I_{i+1})$, $N(I_{i+2})$ are powers of a then Q_i/Q_0, Q_{i+1}/Q_0,

Q_{i+2}/Q_0 are powers of a. From this we also see that π is the least positive value of i for which $Q_i/Q_0 = 1$.

ASSUMPTION. We assume that $\pi > 3$, that a is an integer greater than 1, and that $Q_i/Q_0 = a^r$, $Q_{i+1}/Q_0 = a^s$ and $Q_{i+2}/Q_0 = a^t$ for positive integers r, s and t, where $i \geq 1$ and $i + 2 \leq \pi$.

Remark 3.1. We may assume without loss of generality that $r \leq t$, for if $r > t$ then by putting $j = \pi - i$ we get $Q_j/Q_0 = a^r$, $Q_{j-1}/Q_0 = a^s$ and $Q_{j-2}/Q_0 = a^t$, by the symmetry properties of the continued fraction expansion.

Remark 3.2. We need several lemmas, mostly of a technical nature. Therefore, in order to improve the flow and readability of the paper we have put the proofs of all the lemmas from this section into Section 7.

The notation from above will remain in force.

LEMMA 3.1. $\gcd(a, N) = 1$.

LEMMA 3.2. $q_{i+1} \equiv 0 \pmod{a^r}$, *and if* $q_{i+1} = m = a^r q$ *then* $qa^n > a^k > 1$ *where* $n = r + s$ *and* $k = t - r > 0$.

Remark 3.3. In [7] and [8] we classified completely those forms for which all Q_i/Q_0's are powers of a single integer (including the case where $\pi \leq 3$). Therein we found that this will occur if and only if $n \equiv 0 \pmod{k}$. We have $\pi = 1 + 2n/k$ if $k > 0$, while $\pi = 1$ if $k = 0$. Thus, for $\pi > 3$ the results of [7] and [8] can be considered as special cases of the results given here.

Remark 3.4. Now we wish to detail the form of the continued fraction expansion of ω so that we may specify where, when, and how blocks of consecutive powers of a (3 or more) occur as Q_i/Q_0's. First we observe that if $n = k$ then $Q_3 = \sigma$ so $\pi = 3$, contradicting our assumption. Thus we assume in the sequel that $n \neq k$. Moreover, since $\gcd(a, N) = 1$, by Lemma 3.1 we have $k \neq 0$. Furthermore, if $n = 0$ then $Q_1 = \sigma$, which implies that $\pi = 1$, contradicting our assumption. Thus, we may also assume in the sequel that $k \neq 0$ and $n > 0$.

Moreover, from Lemmas 3.1 and 3.2 we see that in order to have at least three Q_i/σ's in a row as powers of a single integer we must have

$$N = (\sigma(qa^n + (a^k - 1)/q)/2)^2 + \sigma^2 a^n \,. \tag{3.1}$$

4. Preliminary results. Before proceeding with our classification we need some definitions and technical data as machinery for the task. The first concept we need is:

Definition 4.1 (The Euclidean Algorithm). Set $t_{-2} = q$ and $t_{-1} = x > 0$. Then

$$\begin{aligned}
t_{-2} &= \mu_0 t_{-1} + t_0 && \text{for } 0 < t_0 < t_{-1}\,,\\
t_{-1} &= \mu_1 t_0 + t_1 && \text{for } 0 < t_1 < t_0\,,\\
t_0 &= \mu_2 t_1 + t_2 && \text{for } 0 < t_2 < t_1\,,\\
&\vdots && \vdots\\
t_{i-2} &= \mu_i t_{i-1} + t_i && \text{for } 0 < t_i < t_{i-1}\,,\\
&\vdots && \vdots\\
t_{m-2} &= \mu_m t_{m-1} + t_m && \text{with } t_m = 0\,.
\end{aligned}$$

We now modify this algorithm slightly when m is odd only. In this case we replace the value of m by that of $m+1$ which is now even. Having done this we set μ_{m-1} equal to the former μ_m less 1, and put $\mu_m = 1$. If $\gcd(q, x) = 1$ we have $t_{m-1} = 1$, so in the case under discussion we have $t_{m-1} = t_{m-2} = 1$. For a fixed q we denote by $p(x)$ this value of m.

Definition 4.2. Let $A_{-2} = 0 = B_{-1}$; $B_{-2} = 1 = A_{-1}$ and $A_{n+1} = \mu_{n+1}A_n + A_{n-1}$; $B_{n+1} = \mu_{n+1}B_n + B_{n-1}$.

Remark 4.1. It is easily shown that $(-1)^{k+1}t_k = A_kB_m - A_mB_k$. If we assume that $x > 0$ and $\gcd(q, x) = 1$, then $A_m = q$ and $B_m = x$. Also,

$$t_{j-3}A_{j-2} + A_{j-3}t_{j-2} = t_{-2} = A_m = q$$

and

$$t_{j-3}B_{j-2} + B_{j-3}t_{j-2} = t_{-1} = x\,.$$

These results are needed in the sequel.

Definition 4.3.

$$\begin{aligned}
\lambda_j &= jk - \lfloor kj/n \rfloor n, \quad & \varepsilon_j &= \lfloor (j+1)k/n \rfloor - \lfloor jk/n \rfloor\,,\\
\nu_j &= jn - \lfloor nj/k \rfloor k, \quad & \eta_j &= \lfloor (j+1)n/k \rfloor - \lfloor nj/k \rfloor\,,\\
& & d &= \gcd(n,\, k)\,.
\end{aligned}$$

Observe that ν_j and η_j are respectively the same as λ_j and ε_j with the values of k and n reversed.

Now we need some technical lemmas related to Definition 4.3.

Lemma 4.1. $0 \le \lambda_j < n$ *and* $0 \le \nu_j < k$.

Lemma 4.2. (1) $\lambda_j = 0$ *if and only if* $j \equiv 0 \pmod{n/d}$.
(2) $\nu_j = 0$ *if and only if* $j \equiv 0 \pmod{k/d}$.

Lemma 4.3. (1) $\lambda_{j+1} = \lambda_j + k - \varepsilon_j n$.
(2) $\nu_{j+1} = \nu_j + n - \eta_j k$.

LEMMA 4.4. (1) *If $n > k > 0$ then $\varepsilon_j \in \{0, 1\}$.*
(2) *If $k > n > 0$ then $\eta_j \in \{0, 1\}$.*

LEMMA 4.5. (1) *If $n > k > 0$ then*

$$\varepsilon_j = \begin{cases} 1 & \text{if and only if } \lambda_j \geq n - k, \\ 0 & \text{if and only if } \lambda_j < n - k. \end{cases}$$

(2) *If $k > n > 0$ then*

$$\eta_j = \begin{cases} 1 & \text{if and only if } \nu_j \geq k - n, \\ 0 & \text{if and only if } \nu_j < k - n. \end{cases}$$

DEFINITION 4.4. When $n > k$ set

$$\varrho_j = k - n + \lambda_j = \lambda_{j+1},$$
$$\sigma_j = n - \lambda_j = k - \lambda_{j+1} \quad \text{when } \varepsilon_j = 1\,.$$

When $n < k$ set

$$\varrho_j = 2k - n - \nu_j = k - \nu_{j+1}\,,$$
$$\sigma_j = n - k + \nu_j = \nu_{j+1} \quad \text{when } \eta_j = 1\,.$$

If $\eta_j = 0$, then put

$$\varrho_j = k - n - \nu_j = k - \nu_{j+1},$$
$$\sigma_j = k + \nu_j = \nu_{j+1}\,.$$

DEFINITION 4.5. With notation as above

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

where $t_{-1,j} \equiv a^{\varrho_j} \equiv a^{-\sigma_j} \pmod q$ and $0 < t_{-1,j} < q$. The $A_{i,j}$ and $t_{i,j}$ are then computed as described in Definition 4.1 with $x = t_{-1,j}, A_{i,j} = A_i, t_{i,j} = t_i$ and $\mu_{i,j} = \mu_i$.

Remark 4.2. If $m = p(t_{-1,j})$ we get $B_{m,j} = t_{-1,j}, t_{m,j} = 0$, $A_{m,j} = q$, $t_{m-1,j} = 1$ (since $\gcd(q, a) = 1$). (Henceforth $\gcd(\,,\,) = (\,,\,)$ will be used.) Since $B_{m,j}A_{m-1,j} - A_{m,j}B_{m-1,j} = 1$, we get

$$A_{m-1,j} \equiv a^{\sigma_j} \pmod q\,.$$

Furthermore,

$$D_{i+1,j} = \mu_{i+1,j} D_{i,j} + D_{i-1,j}, \qquad C_{i-1,j} = \mu_{i+1,j} C_{i,j} + C_{i+1,j}\,.$$

Now

$$D_{-2,j} = t_{-2,j} = q > 0\,,$$
$$D_{-1,j} = a^{\varrho_j} - t_{-1,j} \geq 0\,,$$
$$D_{0,j} = a^{\varrho_j} A_{0,j} + t_{0,j} > 0\,.$$

Hence $D_{i+1,j} \geq \mu_{i+1,j} D_{i,j}$ $(i \geq -1)$. Thus, $D_{i,j} > 0$ unless $i = -1$ when it is possible for $D_{i,j} = 0$. This can occur only when $a^{\varrho_j} < q$.

Since

$$\begin{aligned} C_{m-2,j} &= a^{\sigma_j} t_{m-2,j} + A_{m-2,j} > 0\,, \\ C_{m-1,j} &= a^{\sigma_j} t_{m-1,j} - A_{m-1,j} = a^{\sigma_j} - A_{m-1,j} \geq 0\,, \\ C_{m,j} &= q\,, \end{aligned}$$

we get $C_{i-1,j} \geq \mu_{i+1,j} C_{i,j}$ $(i \leq m-1)$. Thus, $C_{i,j} > 0$ unless $i = m-1$ when it is possible for $C_{i,j} = 0$. This can only occur when $a^{\sigma_j} < q$. We also note that $C_{i,j} \equiv D_{i,j} \equiv 0 \pmod q$ for $i = -2, -1, \ldots, m$.

5. The continued fraction expansions

Definition 5.1. Let u be the order of a modulo q when $q > 1$, and $u = 1$ when $q = 1$. Set $s_i \equiv (a^{-n})^i \pmod q$ with $0 < s_i < q$. (Observe $k \equiv 0 \pmod u$ and $s_i \neq 0$ since $(a, q) = 1$.) Set $w_i = p(s_i) + 1$.

There are exactly $\kappa = u/\gcd(n, u)$ distinct s_i values. Thus, there are at most κ distinct w_i values. Note that $s_\kappa \equiv 1 \pmod q$ implies $p(s_\kappa) = 0$; whence $w_\kappa = 1$. With all the above in force we have

Definition 5.2. For given $n > k$ and q let

$$\begin{aligned} W(n, q) = W &= \sum_{i=1}^{\kappa} w_i\,, \\ \sigma(r, n, q) = \sigma_r &= \begin{cases} \sum_{i=1}^{r} w_i & \text{if } 0 < r \leq \kappa, \\ 0 & \text{if } r = 0, \end{cases} \\ \psi(k, n, q, j) = \psi(j) &= 1 + 2j + W\lfloor jk/(\kappa n)\rfloor + \sigma_{r_j} \end{aligned}$$

where $r_j = \lfloor jk/n\rfloor - \kappa\lfloor jk/(\kappa n)\rfloor$.

Lemma 5.1. *If $\varepsilon_j = 0$ then $\psi(j+1) = \psi(j) + 2$.*
If $\varepsilon_j = 1$ then $\psi(j+1) = \psi(j) + 2 + w_{r_j+1}$.

Definition 5.3. For the continued fraction expansion of ω with N given by (3.1), put $R_h = (P_h + \lfloor\sqrt{N}\rfloor)/\sigma$ and $S_h = Q_h/\sigma$.

Lemma 5.2. *If $R_h = a^n t_{i-1,j} A_{i,j} + C_{i-1,j} D_{i,j}/q^2$ and $S_h = a^n t_{i,j} A_{i,j} + C_{i,j} D_{i,j}/q^2$ then*

$$\begin{aligned} R_{h+1} &= q_h S_h - R_h + q a^n + (a^k - 1)/q \\ &= a^n t_{i,j} A_{i+1,j} + C_{i,j} D_{i+1,j}/q^2\,, \\ S_{h+1} &= (a^n + R_{h+1}(q a^n + (a^k - 1)/q - R_{h+1}))/S_h \\ &= a^n t_{i+1,j} A_{i+1,j} + C_{i+1,j} D_{i+1,j}/q^2\,. \end{aligned}$$

Now we are in a position to prove our classification for the first case.

THEOREM 5.1. *Assume that $n > k > 0$ and either $\sigma \neq 2$ or $q \neq 1$. Then in the continued fraction expansion of $\omega = (\sigma - 1 + \sqrt{N})/\sigma$ we have*

$$\begin{aligned}
R_0 &= (qa^n + (a^k - 1)/q)/2 + (\sigma - 1)/\sigma\,,\\
S_0 &= 1\,,\\
q_0 &= (qa^n + (a^k - 1)/q)/2 + (\sigma - 1)/\sigma\,,\\
R_1 &= (qa^n + (a^k - 1)/q)\,, \qquad R_2 = qa^n\,,\\
S_1 &= a^n\,, \qquad S_2 = a^k\,,\\
q_1 &= q\,, \qquad q_2 = qa^{n-k}\,,
\end{aligned}$$

and for $1 \le j < n/d - 1$ we have

$$\begin{aligned}
R_{\psi(j)} &= qa^n + (a^k - 1)/q\,,\\
S_{\psi(j)} &= a^{n-\lambda_j}\,,\\
q_{\psi(j)} &= \begin{cases} qa^{\lambda_j} & \text{if } \varepsilon_j = 0,\\ qa^{\lambda_j} + (a^{k-n+\lambda_j} - \gamma_j)/q & \text{if } \varepsilon_j = 1,\end{cases}
\end{aligned}$$

where $\gamma_j \equiv a^{k-n+\lambda_j} \equiv a^{\varrho_j} \equiv t_{-1,j} \equiv a^{-n(\lfloor jk/n \rfloor + 1)} \pmod q$ with $0 < \gamma_j < q$.

Moreover, if $\varepsilon_j = 0$ then

$$\begin{aligned}
R_{\psi(j)+1} &= qa^n\,,\\
S_{\psi(j)+1} &= a^{k+\lambda_j} = a^{\lambda_{j+1}}\,,\\
q_{\psi(j)+1} &= qa^{n-k-\lambda_j} = qa^{n-\lambda_{j+1}}\,.
\end{aligned}$$

If $\varepsilon_j = 1$ and $m = p(\gamma_j)$ then for $1 \le i \le m + 2$

$$\begin{aligned}
R_{\psi(j)+i} &= a^n t_{i-3,j} A_{i-2,j} + C_{i-3,j} D_{i-2,j}/q^2\,,\\
S_{\psi(j)+i} &= a^n t_{i-2,j} A_{i-2,j} + C_{i-2,j} D_{i-2,j}/q^2\,,\\
q_{\psi(j)+i} &= \begin{cases} \mu_{i-1,j} & \text{if } 1 \le i \le m+1,\\ qa^{2n-k-\lambda_j} + (a^{n-\lambda_j} - \delta_j)/q & \text{if } i = m+2,\end{cases}
\end{aligned}$$

where $\delta_j \equiv a^{n-\lambda_j} \equiv a^{\sigma_j} \pmod q$, with $0 < \delta_j < q$ and $\delta_j = 1$ when $q = 1$.

If $j = n/d - 1$ put $\theta = \psi(n/d - 1) - 1$; then $\lambda_j = n - k$ and

$$\begin{aligned}
R_{\theta+1} &= qa^n + (a^k - 1)/q\,,\\
S_{\theta+1} &= a^k = a^{n-\lambda_j}\,,\\
q_{\theta+1} &= qa^{n-k} = qa^{\lambda_j}\,, \qquad q_{\theta+2} = q\,,\\
R_{\theta+2} &= qa^n\,, \qquad R_{\theta+3} = qa^n + (a^k - 1)/q\,,\\
S_{\theta+2} &= a^n\,, \qquad S_{\theta+3} = 1\,.
\end{aligned}$$

Also $\pi = \theta + 3 = \psi(n/d - 1) + 2 = 2n/d + kW/(\kappa d)$.

Proof. We proceed by induction on j. For $j = 1$ we have $\psi(1) = 3$,

$R_3 = qa^n + (a^k - 1)/q$, $S_3 = a^{n-k} = a^{n-\lambda_1}$ and

$$q_3 = \begin{cases} qa^k & \text{if } \varepsilon_1 = 0, \text{ i.e.,} \lfloor 2k/n \rfloor = 0 \text{ so } n > 2k, \\ qa^k + (a^{2k-n} - \gamma_1)/q & \text{if } \varepsilon_1 = 1, \text{ i.e., } n \le 2k, \end{cases}$$

and $\gamma_1 \equiv a^{-n} \pmod q$. Thus, the result holds when $j = 1$.

Case 1. $\varepsilon_j = 0$. Given $R_{\psi(j)}$, $S_{\psi(j)}$ and $q_{\psi(j)}$ as in the hypothesis, we have from Lemma 5.2

$$R_{\psi(j)+1} = q_{\psi(j)}S_{\psi(j)} - R_{\psi(j)} + qa^n + (a^k - 1)/q = qa^n\,,$$
$$S_{\psi(j)+1} = [a^n + R_{\psi(j)+1}(qa^n + (a^k - 1)/q - R_{\psi(j)+1})]/S_{\psi(j)} = a^{\lambda_{j+1}}\,,$$
$$q_{\psi(j)+1} = \lfloor R_{\psi(j)+1}/S_{\psi(j)+1} \rfloor = qa^{n-\lambda_{j+1}}\,.$$

Claim 1.1. $R_{\psi(j+1)} = qa^n + (a^k - 1)/q$.

From Lemmas 5.1 and 5.2 we have

$$\begin{aligned} R_{\psi(j+1)} = R_{\psi(j)+2} &= q_{\psi(j)+1}S_{\psi(j)+1} - R_{\psi(j)+1} + qa^n + (a^k - 1)/q \\ &= qa^n + (a^k - 1)/q\,. \end{aligned}$$

Claim 1.2. $S_{\psi(j+1)} = a^{n-\lambda_{j+1}}$.

Again from Lemmas 5.1 and 5.2,

$$\begin{aligned} S_{\psi(j+1)} &= S_{\psi(j)+2} \\ &= [a^n + R_{\psi(j)+2}(qa^n + (a^k - 1)/q - R_{\psi(j)+2})]/S_{\psi(j)+1} = a^{n-\lambda_{j+1}}\,. \end{aligned}$$

Finally, it is clear from Claims 1.1 and 1.2 that

$$q_{\psi(j+1)} = \begin{cases} qa^{\lambda_{j+1}} & \text{if } \varepsilon_{j+1} = 0, \\ qa^{\lambda_{j+1}} + (a^{k-n+\lambda_{j+1}} - \gamma_{j+1})/q & \text{if } \varepsilon_{j+1} = 1. \end{cases}$$

Hence, we have proved the result in the case where $\varepsilon_j = 0$.

Case 2. $\varepsilon_j = 1$. By Lemma 5.2,

$$\begin{aligned} R_{\psi(j)+1} &= q_{\psi(j)}S_{\psi(j)} - R_{\psi(j)} + qa^n + (a^k - 1)/q \\ &= (qa^{\lambda_j} + (a^{k-n+\lambda_j} - \gamma_j)/q)a^{n-\lambda_j} \\ &\quad - (qa^n + (a^k - 1)/q) + qa^n + (a^k - 1)/q \\ &= qa^n + (a^k - \gamma_j a^{n-\lambda_j})/q = t_{-2,j}A_{-1,j}a^n + C_{-2,j}D_{-1,j}/q^2\,. \end{aligned}$$

Also,

$$\begin{aligned} S_{\psi(j)+1}S_{\psi(j)} &= a^n + R_{\psi(j)+1}(qa^n + (a^k - 1)/q - R_{\psi(j)+1}) \\ &= a^n + (a^n q + (a^k - a^{n-\lambda_j}\gamma_j)/q)(qa^n + (a^k - 1)/q \\ &\qquad\qquad -qa^n - (a^k - \gamma_j a^{n-\lambda_j})/q) \\ &= a^n + ((\gamma_j a^{n-\lambda_j} - 1)/q)(a^n q + (a^k - a^{n-\lambda_j}\gamma_j)/q) \\ &= \gamma_j a^{2n-\lambda_j} + (a^{n-\lambda_j}\gamma_j - 1)(a^k - a^{n-\lambda_j}\gamma_j)/q^2\,. \end{aligned}$$

Therefore,

$$S_{\psi(j)+1} = a^n\gamma_j + (a^{\sigma_j}\gamma_j - 1)(a^{\varrho_j} - \gamma_j)/q^2 = a^n t_{-1,j}A_{-1,j} + C_{-1,j}D_{-1,j}/q^2\,.$$

Thus, by Lemma 5.2,

$$\begin{aligned} S_{\psi(j)+i} &= a^n t_{i-2,j}A_{i-2,j} + C_{i-2,j}D_{i-2,j}/q^2\,,\\ R_{\psi(j)+i} &= t_{i-3,j}A_{i-2,j}a^n + C_{i-3,j}D_{i-2,j}/q^2\,. \end{aligned}$$

Now we show that if the results hold for j then they hold for $j+1$. First we prove

Claim 2.1. $\psi(j+1) = \psi(j) + m + 3$.

Since $r_j \equiv \lfloor jk/n \rfloor \pmod{\kappa}$ and $a^\kappa \equiv 1 \pmod q$ therefore $a^{-n(r_j+1)} \equiv \gamma_j \pmod q$ implies $s_{r_j+1} = \gamma_j$ since both are less than q. Hence,

$$w_{r_j+1} = p(\gamma_j) + 1 = m + 1\,.$$

By Lemma 5.1 we get

$$\psi(j+1) = \psi(j) + w_{r_j+1} + 2 = \psi(j) + p(\gamma_j) + 3 = \psi(j) + m + 3\,,$$

which secures the claim.

Now, from the above we get

$$\begin{aligned} R_{\psi(j)+m+2} &= a^n t_{m-1,j}A_{m,j}a^n + C_{m-1,j}D_{m,j}/q^2\,,\\ S_{\psi(j)+m+2} &= a^n t_{m,j}A_{m,j} + C_{m,j}D_{m,j}/q^2\,. \end{aligned}$$

Thus,

$$\begin{aligned} R_{\psi(j)+m+2} &= qa^n + (a^{\sigma_j} - A_{m-1,j})qa^{\varrho_j}/q^2 = qa^n + (a^k - a^{\varrho_j}A_{m-1,j})/q\,,\\ S_{\psi(j)+m+2} &= q^2a^{\varrho_j}/q^2 = a^{\varrho_j} = a^{\lambda_{j+1}} = a^{k-n+\lambda_j}\,. \end{aligned}$$

Since $A_{m-1,j} \equiv a^{\sigma_j} \equiv a^{n-\lambda_j} \equiv \delta_j \pmod q$ we have $A_{m-1,j} = \delta_j$. Thus,

$$q_{\psi(j)+m+2} = qa^{2n-k-\lambda_j} + (a^{n-\lambda_j} - \delta_j)/q\,.$$

Hence, by Lemma 5.2,

$$\begin{aligned} R_{\psi(j+1)} = R_{\psi(j)+m+3} &= (qa^{2n-k-\lambda_j} + (a^{n-\lambda_j} - \delta_j)/q)a^{k-n+\lambda_j}\\ &\quad - (qa^n + (a^k - \delta_j a^{k-n+\lambda_j})/q) + qa^n + (a^k - 1)/q\\ &= qa^n + (a^k - 1)/q\,,\\ S_{\psi(j+1)} = S_{\psi(j)+m+3} &= a^n/a^{k-n+\lambda_j} = a^{2n-k-\lambda_j} = a^{n-\lambda_{j+1}}\,. \end{aligned}$$

Finally,

$$q_{\psi(j+1)} = q_{\psi(j)+m+3} = \begin{cases} qa^{\lambda_{j+1}} & \text{if } \varepsilon_{j+1} = 0,\\ qa^{\lambda_{j+1}} + (a^{k-n+\lambda_{j+1}} - \gamma_{j+1})/q & \text{if } \varepsilon_{j+1} = 1. \end{cases}$$

This completes the induction for all $j < n/d - 1$.

Now we deal with the period π. Put $\theta = \psi(n/d-1)-1$. We find that $\lambda_j = n-k$ if and only if $j+1 \equiv 0 \pmod{n/d}$. Also,

$$\begin{aligned}
R_{\theta+1} &= qa^n + (a^k-1)/q\,, \\
S_{\theta+1} &= a^k = a^{n-\lambda_j}\,, \\
q_{\theta+1} &= qa^{n-k} = qa^{\lambda_j}\,, \qquad & q_{\theta+2} &= q\,, \\
R_{\theta+2} &= qa^n - (a^k-1)/q\,, & R_{\theta+3} &= qa^n + (a^k-1)/q\,, \\
S_{\theta+2} &= a^n\,, & S_{\theta+3} &= 1\,.
\end{aligned}$$

Thus, $S_k > 1$ for all k with $1 \le k \le \theta+2$ and $S_{\theta+3} = 1$. Therefore, $\pi = \theta+3 = \psi(n/d-1)+2$.

Now, if $j = n/d-1$ then

$$\begin{aligned}
r_j &= \lfloor (n/d-1)k/n \rfloor - \kappa \lfloor (n/d-1)k/(\kappa n) \rfloor \\
&= k/d - 1 - \kappa \lfloor k/(\kappa d) - k/(\kappa n) \rfloor\,.
\end{aligned}$$

Since $\kappa = u/(n,u)$, we have $k/(\kappa d) = k(n,u)/(ud)$. But $kn \equiv 0 \pmod{ud}$ and $uk \equiv 0 \pmod{ud}$, so $k/(\kappa d)$ is an integer. Thus, $\lfloor (k/(\kappa d)) - (k/(\kappa n)) \rfloor = k/(\kappa d) - 1$; whence $r_j = k/d - 1 - k/d + \kappa = \kappa - 1$. We have $\sigma_{r_j} = W - w_k = W-1$ and $\lfloor jk/\kappa n \rfloor = k/(\kappa d) - 1$. Therefore,

$$\psi(n/d-1) = 1 + 2(n/d-1) + W(k/(\kappa d)-1) + W - 1\,.$$

Hence, $\pi = 2n/d + kW/(\kappa d)$. ∎

Now we illustrate Theorem 5.1.

Example 5.1. Let $N = 561730 = (3^6+20)^2 + 3^6$. Thus we have: $a = 3, n = 6, k = 4,\ q = 2,\ d = 2,\ \kappa = 1,\ u = 2,\ w_1 = s_1 = W = 1,\ p(s_1) = 0 = r_1,\ \varepsilon_1 = \lambda_1 = 4,\ m = 0,\ \gamma_1 = 1,\ \sigma_1 = 2,\ \varrho_1 = 2,\ \psi(1) = 3,\ \psi(2) = 6,\ \pi = 8$ and $j = 1$ only for $1 \le j < n/d - 1$. Thus,

$$\begin{aligned}
R_0 &= (qa^n + (a^k-1)/q)/2 = 749 = P_0 + \lfloor \sqrt{N} \rfloor\,, \\
S_0 &= 1\,, \\
q_0 &= (qa^n + (a^k-1)/q)/2 = 749\,, \\
R_1 &= qa^n + (a^k-1)/q = 1498 = P_1 + \lfloor \sqrt{N} \rfloor\,, \\
R_2 &= qa^n = 1458 = P_2 + \lfloor \sqrt{N} \rfloor\,, \\
S_1 &= a^n = 729\,, \qquad S_2 = a^k = 81\,, \\
q_1 &= q = 2\,, \qquad q_2 = qa^{n-k} = 18\,, \\
R_{\psi(1)} &= R_3 = qa^n + (a^k-1)/q = 1498 = P_3 + \lfloor \sqrt{N} \rfloor\,, \\
S_{\psi(1)} &= S_3 = a^{n-\lambda_1} = 9\,, \\
q_{\psi(1)} &= q_3 = qa^{\lambda_1} + (a^{k-n+\lambda_1} - \gamma_1)/q = 166\,,
\end{aligned}$$

$$
\begin{aligned}
R_{\psi(1)+1} &= R_4 = a^n t_{-2,1} A_{-1,1} + C_{-2,1} D_{-1,1}/q^2 \\
&= 3^6 \cdot 2 \cdot 1 + (18 \cdot 8)/4 = 1494 = P_4 + \lfloor \sqrt{N} \rfloor \,, \\
S_{\psi(1)+1} &= S_4 = a^n t_{-1,1} A_{-1,1} + C_{-1,1} D_{-1,1}/q^2 = 3^6 \cdot 1 \cdot 1 + (8 \cdot 8)/4 = 745 \,, \\
q_{\psi(1)+1} &= q_4 = \mu_0 = 2 \,, \\
R_{\psi(1)+2} &= R_5 = a^n t_{-1,1} A_{0,1} + C_{-1,1} D_{0,1}/q^2 \\
&= 3^6 \cdot 1 \cdot 2 + (8 \cdot 18)/4 = 1494 = P_5 + \lfloor \sqrt{N} \rfloor \,, \\
S_{\psi(1)+2} &= S_5 = a^n t_{0,1} A_{0,1} + C_{0,1} D_{0,1}/q^2 = 3^6 \cdot 0 \cdot 2 + (2 \cdot 18)/4 = 9 \,, \\
q_{\psi(1)+2} &= q_5 = q a^{2n-k-\lambda_1} + (a^{n-\lambda_1} - \delta_1)/q = 2 \cdot 3^4 + (3^2 - 1)/2 = 166 \,.
\end{aligned}
$$

Since $\theta = \psi(2) - 1 = 5$ we have

$$
\begin{aligned}
R_{\theta+1} &= R_6 = q a^n + (a^k - 1)/q \\
&= 2 \cdot 3^6 + (3^4 - 1)/2 = 1498 = P_6 + \lfloor \sqrt{N} \rfloor \,, \\
S_6 &= a^k = 81 \,, \\
q_6 &= q a^n - (a^k - 1)/q = 18 \,, \qquad q_7 = q = 2 \,, \\
R_7 &= q a^n = 1458 = P_7 + \lfloor \sqrt{N} \rfloor \,, \\
R_8 &= q a^n + (a^k - 1)/q = 749 = P_8 + \lfloor \sqrt{N} \rfloor \,, \\
S_7 &= a^n = 729 \,, \qquad S_8 = 1 \,.
\end{aligned}
$$

Hence we have compiled the following table:

i	0	1	2	3	4	5	6	7	8
P_i	0	749	709	749	745	745	749	709	749
Q_i	1	729	81	9	745	9	81	729	1
a_i	749	2	18	166	2	166	18	2	1498

Thus, we see in this example that there is one run of 4 consecutive Q_i/σ's in a row as powers of 3, namely for $i = 5, 6, 7, 8$ (since i must be positive).

It is possible to have runs of arbitrary length in the case where $n > k$ (including the case where all Q_i/σ's are powers of a; see Remark 3.3). However, in our next case where $k > n$ we shall see that this is not possible; in fact, we have a considerable restriction.

First, however, we must finish the case where $n > k$. Theorem 5.1 fails for $q = 1$ and $\sigma = 2$, so we treat this case separately. The following can be proved in the same way as Theorem 5.1 so we do not include the proof here. Moreover, we exclude the initial and final sequence of values of $i \in \{0, 1, 2\}$ since they are clear in this case.

THEOREM 5.2. *If $n > k > 0$, $q = 1$ and $\sigma = 2$ then in the continued fraction expansion of $(1 + \sqrt{N})/2$ we have for $1 \le j < n/d - 1$:*

$$
R_{\psi(j)} = a^n + a^k - 1/2 \,, \qquad S_{\psi(j)} = a^{n-\lambda_j} \,,
$$

$$q_{\psi(j)} = \begin{cases} a^{\lambda_j} & \text{if } \varepsilon_j = 0, \\ a^{\lambda_j} + a^{k-n+\lambda_j} - 1 & \text{if } \varepsilon_j = 1. \end{cases}$$

Moreover, if $\varepsilon_j = 0$ *then*

$$\begin{aligned} R_{\psi(j)+1} &= a^n + 1/2\,, \\ S_{\psi(j)+1} &= a^{\lambda_j+k}\,, \\ q_{\psi(j)+1} &= a^{n-\lambda_j-k}\,. \end{aligned}$$

If $\varepsilon_j = 1$ *then* (*observe that* $q = 1$ *implies* $p(x) = 0$ *so* $\psi(j+1) = \psi(j) + 3$)

$$\begin{aligned} R_{\psi(j)+1} &= a^n + a^k - a^{n-\lambda_j} + 1/2\,, \\ S_{\psi(j)+1} &= a^n + a^k - a^{n-\lambda_j} - a^{k-n+\lambda_j} + 1\,, \\ q_{\psi(j)+1} &= 1\,, \\ R_{\psi(j)+2} &= a^n + a^k - a^{k-n+\lambda_j} + 1/2\,, \\ S_{\psi(j)+2} &= a^{k-n+\lambda_j}\,, \\ q_{\psi(j)+2} &= a^{2n-k-\lambda_j} + a^{n-\lambda_j} - 1\,, \\ R_{\psi(j)+3} &= R_{\psi(j+1)} = a^n + a^k - 1/2\,, \\ S_{\psi(j+1)} &= a^{2n-k-\lambda_j} = a^{n-\lambda_{j+1}}\,, \\ q_{\psi(j+1)} &= \begin{cases} a^{\lambda_{j+1}} & \text{if } \varepsilon_{j+1} = 0, \\ a^{\lambda_{j+1}} + a^{k-n+\lambda_{j+1}} - 1 & \text{if } \varepsilon_{j+1} = 1 \end{cases} \end{aligned}$$

and

$$\pi = \psi(n/d - 1) + 2 = 2n/d + kW/(\kappa d)\,.$$

Now we turn to the case where $k > n \geq 1$. First we need:

Definition 5.4. Let δ'_j be determined by $\delta'_j \equiv a^{\nu_j} \pmod q$ with $0 < \delta'_j < q$ and let $\theta_j = \lfloor q/\delta'_j \rfloor$.

Remark 5.1. We have $C_{m,j} = q$, $C_{m-1,j} = a^{\sigma_j} t_{m-1,j} - A_{m-1,j} = a^{\sigma_j} - A_{m-1,j}$, $A_{m-1,j} \equiv a^{\sigma_j} \equiv a^{\nu_{j+1}} \pmod q$, $t_{-1,j} \equiv a^{-n-\nu_j} \equiv a^{\varrho_j} \pmod q$, when $m = p(t_{-1,j})$, $C_{m-2,j} = C_{m,j} - \mu_{m,j} C_{m-1,j}$, which implies that $C_{m-2,j} = q - \mu_{m,j}(a^{\nu_{j+1}} - \delta'_{j+1})$. Also, $A_{m,j} = \mu_{m,j} A_{m-1,j} + A_{m-2,j}$ with $A_{m-2,j} < A_{m-1,j}\mu_{m,j} = \lfloor A_{m,j}/A_{m-1,j} \rfloor$ implies that $\mu_{m,j} = \theta_{j+1}$. Thus,

$$\begin{aligned} C_{m-2,j} &= q - \theta_{j+1}(a^{\nu_{j+1}} - \delta'_{j+1})\,, \\ C_{m-1,j} &= a^{\nu_{j+1}} - \delta'_{j+1}\,, \\ D_{m-1,j} &= a^{k-\nu_{j+1}}\delta'_{j+1} - 1\,, \quad & t_{m-1,j} &= 1\,, \\ A_{m-1,j} &= \delta'_{j+1}\,, & t_{m-2,j} &= \theta_{j+1}\,. \end{aligned}$$

Also, $a^n A_{-2,j} t_{-2,j} + C_{-2,j} D_{-2,j}/q^2 = a^{\sigma_j}$.

DEFINITION 5.5. When $k > n > 0$ define α by $a^\alpha < q < a^{\alpha+1}$ and set

$$\tau_j = \begin{cases} 1 & \text{when } \nu_j > \alpha \text{ and } k - \nu_j - n > \alpha, \\ 0 & \text{otherwise.} \end{cases}$$

DEFINITION 5.6. We note that if $\tau_j = 1$ we have $k - n > 2\alpha$, which implies that $a^{k-n} \geq a^{2\alpha+1} > q$; whence $qa^n < a^k$. Thus if $qa^n > a^k$ then $\tau_j = 0$. Also, if $k - n \leq 2\alpha$ then $\tau_j = 0$. We define

$$w'_j = p(\gamma_j) + 2\eta_{j-1} + 1 + 2\tau_{j-1}$$

where $\gamma_j \equiv a^{-n-\nu_j} \pmod q$ with $0 < \gamma_j < q$, and

$$\psi'(j) = 1 + \sum_{i=1}^{j} w'_i \,.$$

Thus $\psi'(j+1) = \psi'(j) + w'_{j+1}$ and

$$\psi'(j) = 1 + \sum_{i=1}^{j} w_i + 2\sum_{i=1}^{j} \eta_{i-1} + 2T_j \,, \qquad \text{where } T_j = \sum_{i=1}^{j} \tau_{i-1} \,.$$

Now

$$\sum_{i=1}^{j} \eta_{i-1} = \sum_{i=1}^{j} \lfloor in/k \rfloor - \lfloor (i-1)n/k \rfloor = \lfloor jn/k \rfloor \,.$$

Further,

$$\sum_{i=1}^{j} w_i = \lfloor j/k \rfloor W(n,q) + \sigma_{r'_j} \qquad \text{where } r'_j = j - \lfloor j/\kappa \rfloor \kappa \,.$$

Hence,

$$\psi'(j) = 1 + 2\lfloor jn/k \rfloor + \lfloor j/\kappa \rfloor W(n,q) + \sigma_{r'_j} + 2T_j \,.$$

Further, $\psi'(0) = 1$.

In the following theorem we do not make the assumption given at the outset of the section. Therefore, the following result is quite general (for the case $k > n$), including the possibility that $qa^n < a^k$, as we shall see as one of the possible conditions. We assume only that

$$N = (\sigma(qa^n + (a^k - 1)/q)/2)^2 + \sigma^2 a^n \,.$$

We now have the following

THEOREM 5.3. *If $k > n > 0$, then in the continued fraction expansion of $(\sigma - 1 + \sqrt{N})/\sigma$ we have for $0 \leq j < k/d - 1$:*

$$R_{\psi'(j)} = \theta_j \delta'_j a^n + (\delta'_j a^{k-\nu_j} - 1)(\theta_j a^{\nu_j} - \theta_j \delta'_j + q)/q^2 \,,$$

$$S_{\psi'(j)} = a^n \delta'_j + (a^{\nu_j} - \delta'_j)(a^{k-\nu_j}\delta'_j - 1)/q^2 \,,$$

$$q_{\psi'(j)} = \begin{cases} \theta_j + (a^{k-n-\nu_j} - \gamma_j)/q & \text{if } \eta_j = 0, \text{ and } k - n - \nu_j > \alpha \geq \nu_j, \\ \theta_j & \text{otherwise.} \end{cases}$$

If $\eta_j = 1$, *then*

$$\begin{aligned} R_{\psi'(j)+1} &= qa^n + (a^k - \delta'_j a^{k-\nu_j})/q\,, \\ S_{\psi'(j)+1} &= a^{k-\nu_j}\,, \\ q_{\psi'(j)+1} &= qa^{\nu_j+n-k} + (a^{\nu_j} - \delta'_j)/q\,, \end{aligned}$$

$$\begin{aligned} R_{\psi'(j)+2} &= qa^n + (a^k - 1)/q\,, \\ S_{\psi'(j)+2} &= a^{n-k-\nu_j} = t_{-2,j}A_{-2,j}a^n + C_{-2,j}D_{-2,j}/q^2\,, \\ q_{\psi'(j)+2} &= qa^{k-\nu_j} + (a^{2k-n-\nu_j} - \gamma_j)/q\,, \end{aligned}$$

$$\begin{aligned} R_{\psi'(j)+2+i} &= a^n t_{i-3,j}A_{i-2,j} + C_{i-3,j}D_{i-2,j}/q^2\,, \\ S_{\psi'(j)+2+i} &= a^n t_{i-2,j}A_{i-2,j} + C_{i-2,j}D_{i-2,j}/q^2\,, \\ q_{\psi'(j)+2+i} &= \mu_{i-1,j} \quad \textit{for } i = 1, 2, \ldots, m, \ \textit{where } m = p(\gamma_j)\,. \end{aligned}$$

If $\eta_j = 0$, $\nu_j > \alpha$, *and* $k - \nu_j - n > \alpha$, *then*

$$\begin{aligned} R_{\psi'(j)+1} &= qa^n + (a^k - \delta'_j a^{k-\nu_j})/q\,, \\ S_{\psi'(j)+1} &= a^{k-\nu_j}\,, \\ q_{\psi'(j)+1} &= (a^{\nu_j} - \delta'_j)/q\,, \end{aligned}$$

$$\begin{aligned} R_{\psi'(j)+2} &= (a^k - 1)/q\,, \\ S_{\psi'(j)+2} &= a^{n+\nu_j} = a^n A_{-2,j}t_{-2,j} + C_{-2,j}D_{-2,j}/q^2\,, \\ q_{\psi'(j)+2} &= (a^{k-n-\nu_j} - \gamma_j)/q\,, \end{aligned}$$

$$\begin{aligned} R_{\psi'(j)+2+i} &= a^n t_{i-3,j}A_{i-2,j} + C_{i-3,j}D_{i-2,j}/q^2\,, \\ S_{\psi'(j)+2+i} &= a^n t_{i-2,j}A_{i-2,j} + C_{i-2,j}D_{i-2,j}/q^2\,, \\ q_{\psi'(j)+2+i} &= \mu_{i-1,j} \quad \textit{for } i = 1, 2, \ldots, m. \end{aligned}$$

If $\eta_j = 0$ *and* $k - \nu_j - n \le \alpha$, *then*

$$\begin{aligned} R_{\psi'(j)+1} &= qa^n + (a^k - \delta'_j a^{k-\nu_j})/q\,, \\ S_{\psi'(j)+1} &= a^{k-\nu_j} = A_{-1,j}t_{-1,j}a^n + D_{-1,j}C_{-1,j}/q^2\,, \\ q_{\psi'(j)+1} &= \mu_{0,j} + (a^{\nu_j} - \delta'_j)/q\,, \end{aligned}$$

$$\begin{aligned} R_{\psi'(j)+i} &= a^n t_{i-3,j}A_{i-2,j} + C_{i-3,j}D_{i-2,j}/q^2\,, \\ S_{\psi'(j)+i} &= a^n t_{i-2,j}A_{i-2,j} + C_{i-2,j}D_{i-2,j}/q^2\,, \\ q_{\psi'(j)+i} &= \mu_{i-1,j} \quad \textit{for } i = 2, \ldots, m. \end{aligned}$$

If $\eta_j = 0$ *and* $k - n - \nu_j > \alpha \le \nu_j$ *then*

$$\begin{aligned} R_{\psi'(j)+i} &= a^n t_{i-3,j}A_{i-2,j} + C_{i-3,j}D_{i-2,j}/q^2\,, \\ S_{\psi'(j)+i} &= a^n t_{i-2,j}A_{i-2,j} + C_{i-2,j}D_{i-2,j}/q^2\,, \end{aligned}$$

$$q_{\psi'(j)+i} = \mu_{i-1,j} \quad \text{for } i = 1, 2, \dots, m.$$

Finally,

$$\pi = \psi'(k/d-1)+2 = \begin{cases} 2n/d + kW(n,q)/(d\kappa) & \text{if } k-n \le 2\alpha, \\ 2k/d + kW(n,q)/(d\kappa) - 4\lfloor \alpha/d \rfloor - 2 & \text{if } k > n+2\alpha. \end{cases}$$

P r o o f. The formulas for R, S, q are proved as in Theorem 5.1 by induction on j. We now look at the problem of determining π. Note that $\nu_j = k-n$ if and only if $j+1 \equiv 0 \pmod{k/d}$. Thus, if $j < k/d-1$ then $S_h > 1$ for all $h < \psi'(k/d-1)-1 = \lambda$. Put $j = k/d-1$. We get

$$\begin{aligned} R_{\lambda+1} &= \theta_j \delta'_j a^n + (\delta'_j a^{k-\nu_j} - 1)(a_j a^{\nu_j} - \theta_j \delta'_j + q)/q^2\,, \\ S_{\lambda+1} &= a^n \delta'_j + (a^{\nu_j} - \delta'_j)(a^{k-\nu_j}\delta'_j - 1)/q^2\,, \\ q_{\lambda+1} &= \theta_j \quad \text{(note that } j = k/d-1 \text{ forces } \eta_j = 1)\,. \end{aligned}$$

Thus,

$$R_{\lambda+2} = qa^n(a^k - \delta'_j a^{k-\nu_j})/q, \quad R_{\lambda+3} = qa^n + (a^k-1)/q\,,$$
$$S_{\lambda+2} = a^n\,, \quad S_{\lambda+3} = 1\,,$$
$$q_{\lambda+2} = q + (a^{k-n} + \delta_j)/q\,.$$

Thus for $j = k/d-1$ we get $\pi = \lambda+3 = \psi'(k/d-1)+2$. Now, $r'_j = k/d-1-\lfloor k/(d\kappa)-1/\kappa \rfloor \kappa = \kappa-1$ and $\lfloor jn/k \rfloor = \lfloor (k/d-1)n/k \rfloor = n/d-1$, $\psi'(j)+2 = 3 + 2(n/d-1) + (k/(d\kappa)-1)W(n,q) + \sigma_\kappa - 1 + 2T$ with $\sigma_\kappa - 1 = W(n,q) - w_\kappa = W(n,q)-1$, which implies that

$$\psi'(k/d-1)+2 = 2n/d + kW(n,q)/(d\kappa) + 2T$$

where $T = T_j$ with $j = k/d-1$.

It remains to evaluate T. If $k-n \le 2\alpha$ then $T_j = 0$ for all j. Assume $k-n > 2\alpha$. Since ν_j/d assumes each value in the set $\{0, 1, 2, \dots, k/d-1\}$ as $j = 0, 1, 2, \dots, k/d-1$, all of the values of ν_j/d in the interval $0 < \alpha/d < \nu_j/d < (k-n)/d - \alpha/d < k/d-1$ will be assumed as $j = 0, 1, 2, \dots, k/d-1$. Since there are exactly $(k-n)/d - 2\lfloor \alpha/d \rfloor - 1$ values of ν_j/d in this interval, we get $T = (k-n)/d - 2\lfloor \alpha/d \rfloor - 1$, which implies that $\pi = 2k/d + kW(n,q)/(d\kappa) - 4\lfloor \alpha/d \rfloor - 2$ whenever $k > n+2\alpha$. ∎

Now we illustrate Theorem 5.3.

Example 5.2. Let $N = 247073 = (31 \cdot 2^4 + 1)^2 + 4 \cdot 2^4$. Then $n = 4$, $k = 5$, $d = 1$, $q = 31$, $\nu_0 = 0$, $\nu_1 = 4$, $\nu_2 = 3$, $\nu_3 = 2$, $\delta_0 = 1$, $\delta_1 = 16$, $\delta_2 = 8$, $\delta_3 = 4$, $a^{k-\nu_0} = 32$, $a^{k-\nu_1} = 2$, $a^{k-\nu_2} = 4$, $a^{k-\nu_3} = 8$, $\theta_0 = 31$, $\theta_1 = 1$, $\theta_2 = 3$, $\theta_3 = 7$, $\kappa = u = 5$, $\gamma_0 = 2$, $\gamma_1 = 4$, $\gamma_2 = 8$, $\gamma_3 = 16$, $\gamma_4 = 2$, $w'_0 = 1$, $w'_1 = 3$, $w'_2 = 5 = w'_3 = w'_4$, $W = 15$, $p(\gamma_i) = 2$ for $i = 0, 1, 2, 3, 4$, $\eta_0 = 0$, $\eta_i = 1$ for $i = 1, 2, 3$, $\alpha = 4$, $\psi'(0) = 1$, $\psi'(1) = 4$, $\psi'(2) = 9$, $\psi'(3) = 14$, $\psi'(4) = 19$.

Thus we have

$$S_{\psi'(0)} = S_1 = 2^4,\ \ S_{\psi'(1)} = S_4 = 2^8,\ \ S_{\psi'(2)} = S_9 = 2^7,\ \ S_{\psi'(3)} = S_{14} = 2^6.$$

Since $\eta_j = 0$ if and only if $j = 0$ we have

$$S_{\psi'(0)+1} = S_2 = 2^5, \quad S_{\psi'(0)+2} = S_3 = 241, \quad S_{\psi'(1)+1} = S_5 = 2\,.$$

Since $\eta_j = 1$ for $j = 1, 2, 3$ we have

$$S_{\psi'(1)+2} = S_6 = 2^3, \quad S_{\psi'(1)+3} = S_7 = 2^6, \quad S_{\psi'(2)+1} = S_{10} = 2^2\,,$$
$$S_{\psi'(2)+2} = S_{11} = 2^2, \quad S_{\psi'(2)+3} = S_{12} = 2^7\,,$$
$$S_{\psi'(3)+1} = S_{15} = 2^3, \quad S_{\psi'(3)+2} = 2, \quad S_{\psi'(3)+3} = S_{17} = 2^8\,,$$
$$S_{\psi'(4)} = S_{19} = 2^5, \quad S_{\psi'(4)+1} = S_{20} = 2^4, \quad S_{\psi'(4)+2} = S_{21} = 1$$

and thus we get:

i	0	1	2	3	4	5	6
P_i	1	497	495	465	17	495	497
Q_i	2	32	64	482	512	4	16
q_i	249	31	15	1	1	248	62

i	7	8	9	10	11	12	13
P_i	495	401	273	495	497	495	273
Q_i	128	674	256	8	8	256	674
q_i	7	1	3	124	124	3	1

i	14	15	16	17	18	19	20	21
P_i	401	495	497	495	17	465	495	497
Q_i	128	16	4	512	482	64	32	2
q_i	7	62	248	1	1	15	31	497

We observe that there are 3 runs of four consecutive powers of 2, each beginning with Q_4, Q_9 and Q_{14}. There is always the final run of 3 consecutive powers of a. We conclude this section with an answer to the question concerning the possibility of longer runs when $k > n$.

LEMMA 5.3. *If $k > n$ then there are at most* 4 *successive Q_i/Q_0's in a row as powers of a.*

P r o o f: see Section 7.

6. An upper bound on the regulator. It is often very useful to have a good upper bound on the size of the regulator of any real quadratic field. We will now give an upper bound on the size of the regulator of $\mathbb{Q}(\sqrt{N})$. We need a preliminary result.

LEMMA 6.1. *If $p(\gamma_j) = m$ then for $1 \le i \le m-1$ we have*

$$A_{i,j}t_{i-2,j}C_{i-1,j}D_{i-1,j} \ge A_{i-1,j}t_{i-1,j}C_{i,j}D_{i,j}\,.$$

Proof. The result certainly holds for $C_{i,j} = 0$ ($i = m-1$).

Suppose now that $C_{i,j} \ne 0$. We can write

$$t_{i-2,j} = \mu_{i,j}t_{i-1,j} + t_{i,j}\,, \qquad C_{i-1,j} = \mu_{i+1,j}C_{i,j} + C_{i+1,j}\,,$$
$$A_{i,j} = \mu_{i,j}A_{i-1,j} + A_{i-2,j}\,, \qquad D_{i,j} = \mu_{i,j}D_{i-1,j} + D_{i-2,j}\,.$$

Thus,

$$A_{i,j}t_{i-2,j}C_{i-1,j}D_{i-1,j} - A_{i-1,j}t_{i-1,j}C_{i,j}D_{i,j} = A_{i-1,j}t_{i-1,j}C_{i,j}D_{i-1,j}E\,,$$

where

$$E = (\mu_{i,j} + A_{i-2,j}/A_{i-1,j})(\mu_{i,j} + t_{i,j}/t_{i-1,j})(\mu_{i+1,j} + C_{i+1,j}/C_{i,j}) - (\mu_{i,j} + D_{i-2,j}/D_{i-1,j})\,.$$

Since $D_{i-2,j}/D_{i-1,j} \le 1$, we get our result if either $\mu_{i,j}$ or $\mu_{i+1,j}$ is not 1. Also the result holds if $D_{i-2,j} = 0$ ($i = 1$). Suppose then that $\mu_{i,j} = \mu_{i+1,j} = 1$ and $D_{i-2,j} \ne 0$. Since $t_{i-1,j} = \mu_{i+1,j}t_{i,j} + t_{i+1,j}$ we get

$$t_{i-1,j}/t_{i,j} = 1 + t_{i+1,j}/t_{i,j} \le 2\,.$$

This implies that $t_{i,j}/t_{i-1,j} \ge 1/2$; thus $\mu_{i,j} + t_{i,j}/t_{i-1,j} \ge 3/2$. Also,

$$D_{i-1,j} = \mu_{i-1,j}D_{i-2,j} + D_{i-3,j}\,, \qquad A_{i-1,j} = \mu_{i-1,j}A_{i-2,j} + A_{i-3,j}\,.$$

Hence,

$$E > (3/2)(1 + (\mu_{i-1,j} + A_{i-3,j}/A_{i-2,j})^{-1})(1 + C_{i+1,j}/C_{i,j}) - (1 + (\mu_{i-1,j} + D_{i-3,j}/D_{i-2,j})^{-1})\,.$$

If $\mu_{i-1,j} \ge 2$ then $(\mu_{i-1,j} + D_{i-3,j}/D_{i-2,j})^{-1} < 1/2$, whence $E > 0$.

If $\mu_{i-1,j} = 1$ then $\mu_{i-1,j} + A_{i-3,j}/A_{i-2,j} \le 2$; therefore, $1 + (\mu_{i-1,j} + A_{i-3,j}/A_{i-2,j})^{-1} \ge 3/2$, whence $E > 9/4 - 2 > 0$. ∎

THEOREM 6.1. *If $n > k$ then $R < (k+n)\log(\sqrt{\Delta})/d$ where R is the regulator of $\mathbb{Q}(\sqrt{N})$ and $\Delta = (2/\sigma)^2 N$ is the discriminant of $\mathbb{Q}(\sqrt{N})$.*

Proof. If $R_h/S_h = t_{i-1,j}/t_{i,j} + (-1)^{i-1}D_{i,j}/(t_{i,j}qS_h)$, then

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

Therefore,

$$(P_h + \sqrt{N})/Q_h = t_{i-1,j}(1 + (-1)^{i-1}D_{i-j}/(t_{i-1,j}qS_h))/t_{i-1,j} + (\sqrt{N} - \lfloor\sqrt{N}\rfloor)/Q_h\,.$$

In the case where $q \ne 1$ when $\sigma = 2$ we get

$$\lfloor\sqrt{N}\rfloor = \sigma(qa^n + (a^k - 1)/q)/2\,.$$

Also,

$$\begin{aligned} N &= (\sigma(qa^n + (a^k - 1)/q)/2)^2 + \sigma^2 a^n \\ &= (\sigma(qa^n + (a^k - 1)/q)/2)^2(1 + \sigma^2 a^n/(\sigma(qa^n + (a^k - 1)/q)/2)^2) \\ &= (\sigma(qa^n + (a^k - 1)/q)/2)^2(1 + 4a^n/(qa^n + (a^k - 1)/q)^2)\,. \end{aligned}$$

Since $(1 + x)^{1/2} < 1 + x/2$ we get

$$\begin{aligned} (\sqrt{N} - \lfloor\sqrt{N}\rfloor)/Q_h &< [(\sigma(qa^n + (a^k - 1)/q)/2)(1 + 2a^n/(qa^n + (a^k - 1)/q)) \\ &\quad - (\sigma(qa^n + (a^k - 1)/q)/2)]/Q_h \\ &= \sigma a^n/(Q_h(qa^n + (a^k - 1)/q)) < 1/(qS_h)\,. \end{aligned}$$

Thus,

$$\begin{aligned} (P_h + \sqrt{N})/Q_h &< t_{i-1,j}(1 + (-1)^{i-1}D_{i,j}/(t_{i-1,j}qS_h))/t_{i,j} + 1/(qS_h) \\ &= t_{i-1,j}(1 + ((-1)^{i-1}D_{i,j} + t_{i,j})/(t_{i-1,j}qS_h))/t_{i,j}\,. \end{aligned}$$

Since

$$(-1)^{i-1}D_{i,j} + t_{i,j} = (-1)^{i-1}a^{\varrho_j}A_{i,j} - t_{i,j} + t_{i,j} = (-1)^{i-1}a^{\varrho_j}A_{i,j}\,,$$

we get

$$(P_h + \sqrt{N})/Q_h < t_{i-1,j}(1 + \zeta_{i,j})/t_{i,j}\,,$$

where

$$\zeta_{i,j} = (-1)^{i-1}a^{\varrho_j}A_{i,j}/(qt_{i-1,j}(A_{i,j}t_{i,j}a^n + C_{i,j}D_{i,j}/q^2))\,.$$

Now for $1 \le i \le m - 1$,

$$\begin{aligned} &|\zeta_{i,j}| - |\zeta_{i-1,j}| \\ &\quad = a^{\varrho_j}[A_{i,j}/(t_{i-1,j}(A_{i,j}t_{i,j}a^n + C_{i,j}D_{i,j}/q^2)) \\ &\qquad - A_{i-1,j}/(t_{i-2,j}(A_{i-1,j}t_{i-1,j}a^n + C_{i-1,j}D_{i-1,j}/q^2))]/q \\ &\quad = a^{\varrho_j}[A_{i,j}A_{i-1,j}t_{i-1,j}(t_{i-2,j} - t_{i,j})a^n + G/q^2] \\ &\qquad \times [q(A_{i,j}t_{i,j}a^n + C_{i,j}D_{i,j}/q^2) \\ &\qquad\qquad \times(A_{i-1,j}t_{i-1,j}a^n + C_{i-1,j}D_{i-1,j}/q^2)]^{-1}\,, \end{aligned}$$

where

$$G = A_{i,j}t_{i-2,j}C_{i-1,j}D_{i-1,j} - A_{i-1,j}t_{i-1,j}C_{i,j}D_{i,j} > 0\,.$$

Since $t_{i-2,j} - t_{i-1,j} > 0$, we get

$$|\zeta_{i,j}| - |\zeta_{i-1,j}| > 0 \quad \text{for } 1 \le i \le m - 1\,.$$

Now,

$$qA_{i,j}t_{i,j}a^n + C_{i,j}D_{i,j}/q \ge qA_{i,j}t_{i,j}a^n > a^kA_{i,j}t_{i,j} > a^{\varrho_j}A_{i,j}t_{i,j}\,.$$

Therefore, letting ζ_i stand for $\zeta_{i,j}$ for any fixed j, we get

$$|\zeta_i| < 1/(t_{i-1,j}t_{i,j}) \le 1\,.$$

Also,

$$\begin{aligned}\sum_{i=-1}^{m-1}\zeta_i &= |\zeta_{m-1}| - (|\zeta_{m-2}| - |\zeta_{m-3}|)\\ &\quad - (|\zeta_{m-4}| - |\zeta_{m-5}|) - \ldots - (|\zeta_0| - |\zeta_{-1}|)\\ &< |\zeta_{m-1}| - (|\zeta_0| - |\zeta_{-1}|) < |\zeta_{m-1}| + |\zeta_{-1}|\,.\end{aligned}$$

If we set $\phi_h = (P_h + \sqrt{N})/Q_h$ then it is well known that

$$\varepsilon_0 = \prod_{i=1}^{\pi}\phi_i\,.$$

If $n > k$ then

$$\begin{aligned}\phi_1 &= (qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/(2a^n)\,,\\ \phi_2 &= (qa^n - (a^k-1)/q + 2\sqrt{N}/\sigma)/(2a^k)\,.\end{aligned}$$

If we put $\theta = \psi(n/d-1)$, we have $\pi = \theta + 3$ and

$$\begin{aligned}\phi_{\theta+1} &= (qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/(2a^k)\,,\\ \phi_{\theta+2} &= (qa^n - (a^k-1)/q + 2\sqrt{N}/\sigma)/(2a^n)\,,\\ \phi_{\theta+3} &= (qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/2\,.\end{aligned}$$

Now if $\varepsilon_j = 1$ and $m = p(\gamma_j)$, then

$$\begin{aligned}\prod_{i=1}^{m+1}(P_{\psi(j)+i} + \sqrt{N})/Q_{\psi(j)+i} &< \prod_{i=1}^{m+1} t_{i-3,j}(1+\zeta_{i-2})/t_{i-2,j}\\ &< q\exp\Big(\sum_{i=-1}^{m-1}\zeta_i\Big) < q\exp(|\zeta_{m-1}| + |\zeta_{-1}|)\,,\end{aligned}$$

since $1 + \zeta_{i-2} < e^{\zeta_{i-2}}$. Also

$$\begin{aligned}&(P_{\psi(j)+m+2} + \sqrt{N})/Q_{\psi(j)+m+2}\\ &\quad = (qa^n + (a^k - 2A_{m-1,j}a^{k-n+\lambda_j} + 1)/q + 2\sqrt{N}/\sigma)/(2a^{k-n+\lambda_j})\\ &\quad = ((qa^n + (a^k-1)/q + 2\sqrt{N})/\sigma)(2a^{k-n+\lambda_j})^{-1}\\ &\qquad \times (1 - 2(A_{m-1,j}a^{k-n+\lambda_j} - 1)/(q(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)))\\ &\quad < (qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/(2a^{k-n+\lambda_j})\\ &\qquad \times \exp(-2(A_{m-1,j}a^{k-n+\lambda_j} - 1))/(q(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma))\,.\end{aligned}$$

If we put

$$T_j = |\zeta_{m-1}| + |\zeta_{-1}| - 2(A_{m-1,j}a^{k-n+\lambda_j} - 1)/(q(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma))\,,$$

then

$$\begin{aligned} T_j &= a^{\varrho_j} A_{m-1,j}/(q(A_{m-1,j}a^n + C_{m-1,j}D_{m-1,j}/q^2)) \\ &\quad + a^{\varrho_j}/(q(qa^n + C_{-1,j}D_{-1,j}/q^2)) \\ &\quad - 2(A_{m-1,j}a^{\varrho_j} - 1)/(q(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma))\,. \end{aligned}$$

Now, since $2\sqrt{N}/\sigma < 2qa^n$ we get

$$\begin{aligned} T_j &< a^{\varrho_j}/(qa^n) + a^{\varrho_j}/(q^2a^n) - (A_{m-1,j}a^{\varrho_j} - 1)/(2q^2a^n) \\ &= (2a^{\varrho_j}q + 2a^{\varrho_j} - A_{m-1,j}a^{\varrho_j} + 1)/(2q^2a^n) \\ &< (a^{\varrho_j}(2q+1) + 1)/(2q^2a^n) < 1\,. \end{aligned}$$

Since

$$\prod_{i=1}^{m+2} (P_{\psi(j)+i} + \sqrt{N})/Q_{\psi(j)+i} < qe^{T_j}$$

we get

$$\begin{aligned} \varepsilon_0 < \Bigg(&\prod_{\substack{\varepsilon_j=0 \\ 1\le j\le n/d-2}} \frac{qa^n - (a^k-1)/q + 2\sqrt{N}/\sigma}{2a^{\lambda_j+k}} \\ &\qquad \times \frac{qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma}{2a^{n-\lambda_j}} \Bigg) \\ \times \Bigg(&\prod_{\substack{\varepsilon_j=1 \\ 1\le j\le n/d-2}} \frac{qe^{T_j}(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)^2}{2a^{k-n+\lambda_j}} \\ &\qquad \times \frac{qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma}{2a^{n-\lambda_j}} \Bigg) \\ \times &\frac{(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)^2}{(2a^n)^2} \cdot \frac{(qa^n - (a^k-1)/q + 2\sqrt{N}/\sigma)^2}{(2a^k)^2} \\ \times &(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/2\,. \end{aligned}$$

Put $\nu = (\sqrt{N} - \lfloor\sqrt{N}\rfloor)/\sigma < 1/q$; we get

$$\begin{aligned} &(qa^n - (a^k-1)/q + 2\sqrt{N}/\sigma)/2 \\ &\qquad = (qa^n - (a^k-1)/q + 2\lfloor\sqrt{N}\rfloor/\sigma + 2\nu)/2 \\ &\qquad = (qa^n - (a^k-1)/q + qa^n + (a^k-1)/q)/2 + \nu \\ &\qquad = qa^n + \nu = qa^n(1 + \nu/(qa^n)) < qa^n \exp(\nu/(qa^n))\,. \end{aligned}$$

Also,

$$\begin{aligned}(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/2 \\ &= (2\lfloor\sqrt{N}\rfloor/\sigma + 2\sqrt{N}/\sigma)/2 = (2(\sqrt{N}/\sigma - \nu) + 2\sqrt{N}/\sigma)/2 \\ &= 2\sqrt{N}/\sigma - \nu < 2\sqrt{N}\exp(-\nu\sigma/(2\sqrt{N}))/\sigma\,.\end{aligned}$$

Since

$$\sum_{j=1}^{n/d-2} \varepsilon_j = k/d - 1$$

we see that

$$\begin{aligned}\varepsilon_0 &< (qa^n\exp(\nu/(qa^n)))^{n/d-k/d-1}(2\sqrt{N}\exp(-\nu\sigma/(2\sqrt{N}))/\sigma)^{n/d-k/d-1} \\ &\quad\times a^{-(n+k)(n/d-k/d-1)}q^{k/d-1}(2\sqrt{N}\exp(-\nu\sigma/(2\sqrt{N})/\sigma))^{2(k/d-1)} \\ &\quad\times a^{-k(k/d-1)}\Big(\exp\Big(\sum_{\substack{i=1\\ \varepsilon_j=1}}^{n/d-2} T_j\Big)\Big)(2\sqrt{N}\exp(-\nu\sigma/(2\sqrt{N}))/\sigma)^3 \\ &\quad\times (qa^n\exp(\nu/(qa^n)))^2 a^{-2(n+k)} \\ &= q^{n/d}(2\sqrt{N}/\sigma)^{n/d+k/d} \\ &\quad\times a^{-k(k/d-1)-(n+k)(n/d-k/d-1)+n(n/d-k/d-1)+2n-2(n+k)}E \\ &= q^{n/d}(2\sqrt{N}/\sigma)^{(n+k)/d}a^{-nk/d}E = (q/a^k)^{n/d}\sqrt{\Delta}^{(k+n)/d}E\,.\end{aligned}$$

Here

$$\begin{aligned}E = {}& \exp(-\nu\sigma/(2\sqrt{N}))((n/d-k/d-1)+2(k/d-1)+3) \\ &\times\exp(\nu/(qa^n))((n/d-k/d-1)+2)\exp\Big(\sum_{j=1}^{n/d-2} T_j\Big)\,.\end{aligned}$$

Put

$$\begin{aligned}\kappa = {}& -\nu\sigma(n/d+k/d)/(2\sqrt{N}) + \nu(n/d-k/d+1)/(qa^n) + \sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} T_j \\ < {}& -\nu(n/d+k/d)/(2qa^n) + \nu(n/d-k/d+1)/(qa^n) + \sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} T_j \\ < {}& (n/(2d) - 3k/(2d) + 1)/(q^2a^n) + \sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} T_j\,.\end{aligned}$$

Now,

$$\sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} T_j < \sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} (a^{\varrho_j}(2q+1)+1)/(2q^2a^n)$$
$$= (2q+1)\sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} a^{\varrho_j}/(2q^2a^n) + (k/d-1)/(2q^2a^n)\,.$$

Also,

$$\sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} a^{\varrho_j} \le a^{d(k/d-1)} + a^{d(k/d-2)} + \ldots + a^d$$
$$= a^d(a^{d(k/d-1)}-1)/(a^d-1) = (a^k-a^d)/(a^d-1)$$
$$< (a^k/(a^d-1)) - 1 \le a^n/(a(a^d-1)) - 1\,.$$

Hence,

$$\sum_{\substack{j=1\\ \varepsilon_j=1}}^{n/d-2} T_j < (2q+1)/(2q^2a(a^d-1)) - (2q+1)/(2q^2a^n)\,.$$

Thus,

$$\begin{aligned}\kappa &< (n/(2d) - 3k/(2d) + 1)/(q^2a^n) + (k/d-1)/(2q^2a^n)\\ &\quad + (2q+1)/(2q^2a(a^d-1)) - (2q+1)/(2q^2a^n)\\ &\le (n/(2d) - k/d - q)/(q^2a^n) + (2q+1)/(4q^2)\\ &< 1/(4q^2) + 1/(2q) + 1/(4q^2) < 1/q\end{aligned}$$

(since $a^n > 2n-8$ for $a \ge 2$). It follows that

$$(*) \qquad \varepsilon_0 < (q/a^k)^{n/d}(\sqrt{\Delta})^{(k+n)/d}e^{1/q}$$

and

$$R < 1/q + n\log(q/a^k)/d + (k+n)\log(\sqrt{\Delta})/d\,.$$

We now point out that $a^k - 1 \ge q$ implies that $a^{-k} \le (q+1)^{-1}$, whence $q/a^k \le q/(q+1)$. Furthermore,

$$\begin{aligned}\log(q/a^k) &\le \log q/(q+1) = -\log(q+1)/q\\ &= -\log(1+1/q) = -(1/q - 1/(2q^2) - 1(3q^3) - \ldots)\\ &< -1/q + 1/(2q^2)\end{aligned}$$

and so

$$\begin{aligned}1/q + n\log(q/a^k)/d &< 1/q + n(-1/q + 1/(2q^2))/d\\ &= (1-n/d)/q + n/(2dq^2) < 0 \quad \text{if } n/d \ge 2 \text{ and } q \ge 2\,.\end{aligned}$$

Hence $R < ((k+n)/d)\log\sqrt{\Delta}$.

Note that the result (∗) also holds for the case where $\sigma = 2$ and $q = 1$. In this case we have $\lfloor\sqrt{N}\rfloor = a^n + a^k$ and $\nu + 1/2 < a^n/(a^n + a^k - 1)$; thus,

$$(a^n - a^k + 1 + \sqrt{N})/2 < a^n \exp((\nu + 1/2)/a^n)$$

and $\phi_{\psi(j)+1} < 1 + a^{k-n+\lambda_j}/a^n$ when $\varepsilon_j = 1$. ∎

THEOREM 6.2. *If $qa^n > a^k$ and $k > n$ then $R < (k+n)\log(\sqrt{\Delta})/d + 1$.*

Proof. For a fixed j we have

$$\begin{aligned}|\zeta_0| - |\zeta_{-1}| &= a^{\varrho_j} A_{0,j}/(\gamma_j q(A_{0,j}t_{0,j}a^n + C_{0,j}D_{0,j}/q^2))\\ &\quad - a^{\varrho_j}/(q^2(\gamma_j a^n + C_{-1,j}D_{-1,j}/q^2))\\ &= a^{\varrho_j} G/(\gamma_j q^2(A_{0,j}t_{0,j}a^n + C_{0,j}D_{0,j}/q^2)\\ &\qquad \times(\gamma_j a^n + C_{-1,j}D_{-1,j}/q^2))\,,\end{aligned}$$

where

$$\begin{aligned}G &= qA_{0,j}(\gamma_j a^n + C_{-1,j}D_{-1,j}/q^2) - \gamma_j A_{0,j}t_{0,j}a^n - \gamma_j C_{0,j}D_{0,j}/q^2\\ &= A_{0,j}a^n\gamma_j(q - t_{0,j}) + qA_{0,j}D_{-1,j}C_{-1,j}/q^2 - \gamma_j C_{0,j}D_{0,j}/q^2\\ &= A_{0,j}a^n\gamma_j(\mu_{0,j}\gamma_j) - \gamma_j C_{0,j}D_{0,j}/q^2 + qA_{0,j}C_{-1,j}D_{-1,j}/q^2\\ &> A_{0,j}a^n\gamma_j^2\mu_{0,j} - \gamma_j a^n + qA_{0,j}C_{-1,j}D_{-1,j}/q^2 \ge 0\,.\end{aligned}$$

Therefore, $|\zeta_0| - |\zeta_{-1}| \ge 0$, and

$$\Big|\sum_{i=-1}^{m-1}\zeta_i\Big| < |\zeta_{m-1}| = \xi_j < a^{\varrho_j}/(qa^n)\,.$$

When $\eta_j = 1$, $m = p(\gamma_j)$ and $\xi_j := |\zeta_{m-1}|$. By using the above results we see that if $k - \nu_j - n \le \alpha$, then, as before,

$$\prod_{i=1}^{m+1}(P_{\psi(j)+2+i} + \sqrt{N})/Q_{\psi(j)+2+i} < qe^{\xi_j}\,.$$

When $\eta_j = 0$ we have $t_{-1,j} \equiv a^{2k-n-\nu_j} \equiv a^{k-n-\nu_j} \pmod q$. Also, $k - n - \nu_j < k - n$ so $a^{k-n-\nu_j} < a^{k-n} < q$, which implies that $t_{-1,j} = a^{k-n-\nu_j}$. In this case

$$\begin{aligned}&\prod_{i=2}^{m+1}(P_{\psi(j)+i} + \sqrt{N})/Q_{\psi(j)+i}\\ &\qquad < (t_{-1}/t_0)(t_0/t_1)\dots(t_{m-2}/t_{m-1})\exp\Big(\sum_{i=0}^{m-1}\zeta_i\Big)\\ &\qquad < a^{k-n-\nu_j}e^{\xi_j}\,.\end{aligned}$$

It follows that

$$\varepsilon_0 < \frac{qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma}{2a^n} \cdot \frac{qa^n - (a^k-1)/q + 2\sqrt{N}/\sigma}{2a^n} \times (qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/2$$
$$\times \prod_{\substack{j=0 \\ \eta_j=1}}^{k/d-2} qe^{\xi_j}\left(\frac{qa^n + (a^k - 2\delta'_j a^{k-\nu_{j+1}})/q + 2\sqrt{N}/\sigma}{2a^{k-\nu_j}}\right) \times \left(\frac{qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma}{2a^{n-k+\nu_j}}\right)$$
$$\times \prod_{\substack{j=0 \\ \eta_j=0}}^{k/d-2} e^{\xi_j}\left(\frac{qa^n + (a^k - 2\delta'_j a^{k-\nu_{j+1}})/q + 2\sqrt{N}/\sigma}{2a^{k-\nu_j}}\right) a^{k-n-\nu_j}\,.$$

As before,

$$(qa^n - (a^k-1)/q + 2\sqrt{N}/\sigma)/2 < qa^n \exp(\nu/(qa^n))\,,$$
$$(qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/2 < 2\sqrt{N}\exp(-\nu\sigma/(2\sqrt{N}))/\sigma\,,$$
$$\sum_{j=0}^{k/d-2} \eta_j = \lfloor (k/d-1)n/k \rfloor = n/d - 1\,.$$

Also,

$$(qa^n + (a^k - 2\delta'_j a^{k-\nu_j} + 1)/q + 2\sqrt{N}/\sigma)/2$$
$$< (qa^n + (a^k-1)/q + 2\sqrt{N}/\sigma)/2 < 2\sqrt{N}\exp(-\nu\sigma/(2\sqrt{N}))/\sigma\,.$$

Thus,

$$\varepsilon_0 < ((qa^n/a^n)2\sqrt{N}/(\sigma a^n))(2\sqrt{N}/\sigma)((2\sqrt{N}/\sigma)^2 q/a^n)^{n/d-1} \times (2\sqrt{N}/(\sigma a^n))^{k/d-1-(n/d-1)} E\,,$$

where

$$E = \exp\Big\{ \sum_{j=0}^{k/d-2} \xi_j + \nu/qa^n - \sigma\nu(n/d-1)/\sqrt{N} - \nu\sigma(k/d-1-(n/d-1))/(2\sqrt{N}) - \sigma\nu/\sqrt{N}\Big\}\,.$$

As in Theorem 6.1, we get

$$\varepsilon_0 < q^{n/d}(2\sqrt{N}/\sigma)^{2(n/d-1)+2+k/d-n/d} a^{-n-(n/d-1)n-(k/d-n/d)n} E$$
$$= q^{n/d}(2\sqrt{N}/\sigma)^{(k+n)/d} a^{-kn/d} E = (q/a^k)^{n/d}(\sqrt{\Delta})^{(k+n)/d} E\,.$$

Now,

$$\sum_{j=0}^{k/d-2} \xi_j \le \sum_{j=0}^{k/d-2} a^{\varrho_j}/(a^n q) = \Big(\sum_{j=0}^{k/d-2} a^{\varrho_j}\Big)\Big/(qa^n)\,,$$

and

$$\begin{aligned}\sum_{j=0}^{k/d-2} a^{\varrho_j} &= \sum_{j=0}^{k/d-1} a^{k-\nu_j} = \sum_{j=1}^{k/d-1} a^{d(k/d-\nu_j/d)} = \sum_{j=1}^{k/d-1} a^{dj} \\ &= a^d(a^{d(k/d-1)}-1)/(a^d-1) = (a^k-a^d)/(a^d-1) < a^k\,.\end{aligned}$$

Hence, $\sum_{j=0}^{k/d-2}\xi_j < a^k/(qa^n)$. Also, since $2\sqrt{N}/\sigma < 2qa^n$ we have

$$\nu/(qa^n) - \sigma\nu(n/d+k/d)/(2\sqrt{N}) < 0\,.$$

Thus $E < e$ and $\varepsilon_0 < (q/a^k)^{n/d}(\sqrt{\Delta})^{(k+n)/d}e$. ∎

7. Proofs of the lemmas. In this section we provide the proofs of the lemmas in Sections 3–5.

Proof of Lemma 3.1. Let p be a prime which divides both a and N. Since $Q_iQ_{i+1} = N - P_{i+1}^2$, we see that p divides P_{i+1}. Since $P_{i+2} = q_{i+1}Q_{i+1} - P_{i+1}$, p also divides P_{i+2}. Hence p divides Q_j for $j = i,\ i+1$, $i+2$ and p divides P_k for $k = i+1,\ i+2$. Therefore, p divides $P_{i+3} = q_{i+2}Q_{i+2} - P_{i+2}$ and p divides $Q_{i+3} = Q_{i+1} - q_{i+2}(P_{i+3} - P_{i+2})$. Thus, by induction, p divides $Q_\pi = Q_0$, whence $p = Q_0 = \sigma = 2$ is forced. However, $N \equiv 0 \pmod 2$ and $N \equiv 1 \pmod 4$ are contradictory. The result follows. ∎

Proof of Lemma 3.2. Since $P_{i+2} = q_{i+1}Q_{i+1} - P_{i+1}$, we have $P_{i+2} = q_{i+1}\sigma a^s - P_{i+1}$. Also, if we put $m = q_{i+1}$ then $\sigma^2 a^{r+s} = N - P_{i+1}^2$, so

$$\begin{aligned}\sigma^2 a^{s+t} &= N - P_{i+2}^2 = N - (\sigma m a^s - P_{i+1})^2 \\ &= N - P_{i+1}^2 - \sigma^2 m^2 a^{2s} + 2\sigma m a^s P_{i+1} \\ &= \sigma^2 a^{r+s} - \sigma^2 m^2 a^{2s} + 2\sigma m a^s P_{i+1}\,.\end{aligned}$$

Hence, $a^t = a^r - m^2 a^s + 2mP_{i+1}/\sigma$; whence m divides $a^t - a^r$. Also, a^r divides $m(2P_{i+1}/\sigma - ma^s)$.

If $a \equiv 0 \pmod p$ for some prime p and $ma^s \equiv 2P_{i+1}/\sigma \pmod p$ then $2P_{i+1}/\sigma \equiv 0 \pmod p$ so p divides $2/\sigma$ or P_{i+1}. If p divides P_{i+1} then since $\sigma^2 a^{r+s} = N - P_{i+1}^2$ we must have p dividing N, which contradicts Lemma 3.1. If p divides $2/\sigma$ but not P_{i+1} then $\sigma = 1$, $p = 2$, and P_{i+1} is odd. However, $N \not\equiv 1 \pmod 4$ whenever $\sigma = 1$, and since r and s are positive we get $N \equiv P_{i+1}^2 \pmod 4$, a contradiction. Thus, p does not divide $2P_{i+1}/\sigma - ma^s$ whenever p divides a. It follows that $m \equiv 0 \pmod{a^r}$. Set

$m = a^r q$; we get $2P_{i+1}/\sigma = qa^{r+s} + (a^{t-r} - 1)/q$. If we put $n = r + s$ and $k = t - r$ then $N = (\sigma(qa^n + (a^k - 1)/q)/2)^2 + \sigma^2 a^n$. If $k = 0$ we get $N = (\sigma q a^n/2)^2 + \sigma^2 a^n$. Thus either a divides N or $a = 1$. The former contradicts Lemma 3.1 and the latter contradicts our assumption. Hence we have $k > 0$.

If either $\sigma \neq 2$ or $q \neq 1$ then $\lfloor \sqrt{N} \rfloor = \sigma(qa^n + (a^k - 1)/q)/2$. If $\sigma = 2$ and $q = 1$ then $\lfloor \sqrt{N} \rfloor = a^n + a^k$. In the former case

$$\begin{aligned} 1 \leq q_{i+2} &= \lfloor (P_{i+2} + \sqrt{N})/Q_{i+2} \rfloor \\ &= \left\lfloor \frac{\sigma(qa^n - (a^k - 1)/q)/2 + \sigma(qa^n + (a^k - 1)/q)/2}{\sigma a^t} \right\rfloor \\ &= \lfloor qa^n/a^t \rfloor . \end{aligned}$$

Thus, $qa^n \geq a^t > a^{t-r}$ so $qa^n > a^k$.

In the latter case

$$\begin{aligned} (P_{i+2} + \lfloor \sqrt{N} \rfloor)/Q_{i+2} &= (a^{r+s} - a^{t-r} + 1 + a^{r+s} + a^{t-r})/(2a^t) \\ &= (2a^n + 1)/(2a^t) \geq 1 \end{aligned}$$

since $q_{i+2} \geq 1$. Hence $2a^n + 1 \geq 2a^t$, i.e., $a^n \geq a^t - 1/2$, which implies that $n \geq t > k$. Thus, we always have $qa^n > a^k$. ∎

Proof of Lemma 4.2. (1) If $jk - \lfloor kj/n \rfloor n = 0$ then $jk/d - \lfloor kj/n \rfloor n/d = 0$. Since $\gcd(k/d, n/d) = 1$ we must have $j \equiv 0 \pmod{n/d}$. If $j = rn/d$ then $jk - \lfloor kj/n \rfloor n = rnk/d - \lfloor krn/dn \rfloor n = 0$.

(2) is proved in a similar fashion. ∎

Proof of Lemma 4.3. (1) $\lambda_j = jk - \lfloor kj/n \rfloor n = (j + 1)k - (\lfloor k(j + 1)/k \rfloor - \varepsilon_j)n - k = \lambda_{j+1} + \varepsilon_j n - k$.

(2) is proved in a similar fashion. ∎

Proof of Lemma 4.4. (1) Clearly $\lfloor (j + 1)k/n \rfloor - \lfloor jk/n \rfloor \geq 0$. Also,

$$\begin{aligned} \lfloor (j + 1)k/n \rfloor &\leq (j + 1)k/n = jk/n + k/n \\ &\leq \lfloor jk/n \rfloor + 1 - 1/n + k/n \leq \lfloor jk/n \rfloor + 1 + (k - 1)/n . \end{aligned}$$

Since $\lfloor (j + 1)k/n \rfloor$ and $\lfloor jk/n \rfloor + 1$ are integers and $0 \leq (k - 1)/n < 1$ we get $\lfloor (j + 1)k/n \rfloor \leq \lfloor jk/n \rfloor + 1$.

(2) Similar. ∎

Proof of Lemma 4.5. (1) We first assume that $j + 1 \not\equiv 0 \pmod{n/d}$. In this case $0 < \lambda_{j+1} < n$ implies that $0 < \lambda_j + k - \varepsilon_j n < n$; whence $\lambda_j > \varepsilon_j n - k$ and $\lambda_j < (\varepsilon_j + 1)n - k$. Thus, if $\varepsilon_j = 1$ we get $\lambda_j > n - k$ and if $\varepsilon_j = 0$ we get $\lambda_j < n - k$.

If $\lambda_j > n - k$ then $\lambda_{j+1} > n - \varepsilon_j n$, so $\varepsilon_j = 1$. If $\lambda_j < n - k$ then $\lambda_{j+1} < n - \varepsilon_j n$, so $\varepsilon_j = 0$.

If $j+1 \equiv 0 \pmod{n/d}$ then $j = rn/d - 1$ and

$$\begin{aligned}\varepsilon_j &= \lfloor rnk/(dn) \rfloor - \lfloor (rn/d-1)k/n \rfloor = rk/d - \lfloor rk/d - k/n \rfloor \\ &= rk/d - (rk/d - 1) = 1\,.\end{aligned}$$

Also,

$$\begin{aligned}\lambda_j &= (rn/d-1)k - \lfloor (rn/d-1)k/n \rfloor n \\ &= rnk/d - k - (rk/d-1)n = n-k\,.\end{aligned}$$

Moreover, if $\lambda_j = n-k$ then $jk - \lfloor kj/n \rfloor n = n-k$ implies that $(j+1)k = n(\lfloor kj/n \rfloor + 1)$; whence $j+1 \equiv 0 \pmod{n/d}$.

(2) Similar. ∎

Proof of Lemma 5.1. If $\varepsilon_j = 0$ then $\lfloor jk/n \rfloor = \lfloor (j+1)k/n \rfloor$ and this implies that $\lfloor jk/(n\kappa) \rfloor = \lfloor (j+1)k/(n\kappa) \rfloor$. Also, $r_{j+1} = \lfloor (j+1)k/n \rfloor - \kappa \lfloor (j+1)k/(\kappa n) \rfloor = r_j$; hence, $\psi(j+1) = 2 + \psi(j)$.

If $\varepsilon_j = 1$ then $\lfloor jk/n \rfloor = \lfloor (j+1)k/n \rfloor - 1$, which implies that $\lfloor jk/(n\kappa) \rfloor = \lfloor (j+1)k/(n\kappa) \rfloor + \delta$ where $\delta \in \{0, -1\}$. Also, if $r' = r_{j+1}$ then $r' = r_j + 1 + \kappa\delta$.

If $\delta = 0$ then $r' = 1 + r_j$ and if $\delta = -1$ then $1 + r_j = \kappa + r'$ so $r' = 0$ and $r_j = \kappa - 1$. Thus, if $\delta = 0$ then

$$\psi(j+1) = 1 + 2(j+1) + W\lfloor (j+1)k/(\kappa n) \rfloor + \sigma_{r'} = 2 + \psi(j) + w_{r_j+1}\,.$$

If $\delta = -1$ then

$$\begin{aligned}\psi(j+1) &= 1 + 2(j+1) + W\lfloor (j+1)k/(\kappa n) \rfloor + \sigma'_r \\ &= 1 + 2(j+1) + W\lfloor jk/(\kappa n) \rfloor + W \\ &= 2 + \psi(j) + w_\kappa = 2 + \psi(j) + w_{r_j+1}\,.\end{aligned}$$ ∎

Proof of Lemma 5.2.

$$\begin{aligned}R_h - t_{i-1,j}S_h/t_{i,j} &= D_{i,j}(C_{i-1,j} - t_{i-1,j}C_{i,j}/t_{i,j})/q^2 \\ &= D_{i,j}(C_{i-1,j}t_{i,j} - t_{i-1,j}C_{i,j})/(t_{i,j}q^2)\,.\end{aligned}$$

Now by Definition 4.5

$$\begin{aligned}C_{i-1,j}t_{i,j} - t_{i-1,j}C_{i,j} &= (a^{\sigma_j}t_{i-1,j} + (-1)^{i-1}A_{i-1,j})t_{i,j} \\ &\quad - t_{i-1,j}(a^{\sigma_j}t_{i,j} + (-1)^i A_{i,j}) \\ &= (-1)^{i-1}(A_{i-1,j}t_{i,j} + t_{i-1,j}A_{i,j})\end{aligned}$$

and from Remark 4.1 it follows that the latter equals $(-1)^{i-1}q$. Hence,

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

Therefore,

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

For $i > -2$ we get $S_h > C_{i,j}D_{i,j}/q^2 \geq D_{i,j}/q$ when $C_{i,j} \neq 0$. Thus,

$$|R_h/S_h - t_{i-1,j}/t_j| < 1/t_{i,j}\,.$$

This implies that $q_h = \lfloor R_h/S_h \rfloor = \lfloor t_{i-1,j}/t_{i,j} \rfloor = \mu_{i+1,j}$ (as long as $i > -2$ and $C_{i,j} \neq 0$).

If $C_{i,j} = 0$ then $i = m-1$ and $q > a^{\sigma_j}$. In this case $C_{m-1,j} = 0$ and $D_{m-1,j} = a^{\varrho_j} A_{m-1,j} - 1$. Furthermore, $A_{m-1,j} = a^{\sigma_j}$ implies that $D_{m-1,j} = a^k - 1$. We also have

$$\begin{aligned} C_{m-2,j} &= \mu_{m,j} C_{m-1,j} + C_{m,j} = q\,, \qquad S_h = a^{n+\sigma_j}\,, \\ R_h &= a^{n+\sigma_j}\mu_{m,j} + (a^k - 1)/q\,, \\ q_h &= \lfloor R_h/S_h \rfloor = \mu_{m,j} + \lfloor (a^k - 1)/(q a^{n+\sigma_j}) \rfloor\,. \end{aligned}$$

Since $q_h = \mu_{i+1,j}$, we get

$$\begin{aligned} R_{h+1} &= \mu_{i+1,j} S_h - R_h + 2\lfloor \sqrt{N} \rfloor/\sigma \\ &= \mu_{i+1,j} a^n t_{i,j} A_{i,j} + \mu_{i+1,j} C_{i,j} D_{i,j}/q^2 - a^n t_{i-1,j} A_{i,j} \\ &\quad - C_{i-1,j} D_{i,j}/q^2 + 2\lfloor \sqrt{N} \rfloor/\sigma \\ &= a^n (t_{i,j}\mu_{i+1,j} A_{i,j} - t_{i-1,j} A_{i,j}) \\ &\quad + (\mu_{i+1,j} D_{i,j} C_{i,j} - C_{i-1,j} D_{i,j})/q^2 + q a^n + (a^k - 1)/q \\ &= a^n (t_{i,j}(A_{i+1,j} - A_{i-1,j}) - t_{i-1,j} A_{i,j}) \\ &\quad + (C_{i,j}(D_{i+1,j} - D_{i-1,j}) - C_{i-1,j} D_{i,j})/q^2 + q a^n + (a^k - 1)/q \\ &= a^n (t_{i,j} A_{i+1,j} - q) \\ &\quad + (C_{i,j} D_{i+1,j} - (C_{i,j} D_{i-1,j} + C_{i-1,j} D_{i,j}))/q^2 + q a^n + (a^k - 1)/q\,. \end{aligned}$$

Since (from Definition 4.5) we have $C_{i,j} D_{i-1,j} + C_{i-1,j} D_{i,j} = q(a^k - 1)$, we have shown that

$$R_{h+1} = a^n t_{i,j} A_{i+1,j} + C_{i,j} D_{i+1,j}/q^2\,.$$

Now we verify the formulas for S_{h+1}. If we make use of the easily verified identities

$$\begin{aligned} C_{i,j} t_{i+1,j} - C_{i+1,j} t_{i,j} &= (-1)^i q\,, \\ D_{i,j} A_{i+1,j} - D_{i+1,j} A_{i,j} &= (-1)^i q\,, \end{aligned}$$

we get

$$\begin{aligned} q^2 &= C_{i,j} t_{i+1,j} D_{i,j} A_{i+1,j} + D_{i+1,j} C_{i+1,j} t_{i,j} A_{i,j} \\ &\quad - C_{i+1,j} t_{i,j} D_{i,j} A_{i+1,j} - D_{i+1,j} A_{i,j} C_{i,j} t_{i+1,j}\,. \end{aligned}$$

Hence

$$\begin{aligned} q^2 - q C_{i,j} D_{i+1,j} &+ q(a^k - 1) t_{i,j} A_{i+1,j} - 2 t_{i,j} A_{i+1,j} C_{i,j} D_{i+1,j} \\ &= C_{i,j} t_{i+1,j} D_{i,j} A_{i+1,j} + D_{i+1,j} C_{i+1,j} t_{i,j} A_{i,j} - C_{i+1,j} t_{i,j} D_{i,j} A_{i+1,j} \\ &\quad - D_{i+1,j} A_{i,j} C_{i,j} t_{i+1,j} + (t_{i+1,j} A_{i,j} + A_{i+1,j} t_{i,j}) C_{i,j} D_{i+1,j} \\ &\quad + (D_{i,j} C_{i+1,j} + C_{i,j} D_{i+1,j}) t_{i,j} A_{i+1,j} - 2 t_{i,j} A_{i+1,j} C_{i,j} D_{i+1,j} \\ &= C_{i,j} t_{i+1,j} D_{i,j} A_{i+1,j} + D_{i+1,j} C_{i+1,j} t_{i,j} A_{i,j}\,. \end{aligned}$$

Since $S_{h+1} = (N - P_{h+1}^2)/(\sigma^2 S_h)$, we get

$$\begin{aligned}\sigma^2 S_h S_{h+1} &= N - \lfloor\sqrt{N}\rfloor^2 + \lfloor\sqrt{N}\rfloor^2 - P_{h+1}^2\\ &= \sigma^2 a^n + \sigma R_{h+1}(2\lfloor\sqrt{N}\rfloor - \sigma R_{h+1})\,.\end{aligned}$$

This implies that

$$\begin{aligned}&S_h S_{h+1}\\ &= a^n + R_{h+1}(2\lfloor\sqrt{N}\rfloor/\sigma - R_{h+1}) = a^n + 2\lfloor\sqrt{N}\rfloor R_{h+1}/\sigma - R_{h+1}^2\\ &= a^n + (qa^n + (a^k-1)/q)R_{h+1} - R_{h+1}^2\\ &= a^n + (qa^n + (a^k-1)/q)(a^n t_{i,j}A_{i+1,j} + C_{i,j}D_{i+1,j}/q^2)\\ &\quad - (a^n t_{i,j}A_{i+1,j} + C_{i,j}D_{i+1,j}/q^2)^2\\ &= a^{2n}t_{i,j}A_{i+1,j}(q - t_{i,j}A_{i+1,j}) + C_{i,j}D_{i+1,j}(q(a^k-1) - C_{i,j}D_{i+1,j})/q^4\\ &\quad + a^n(q^2 + qC_{i,j}D_{i+1,j} + q(a^k-1)t_{i,j}A_{i+1,j} - 2t_{i,j}A_{i+1,j}C_{i,j}D_{i+1,j})/q^2\\ &= a^{2n}t_{i,j}t_{i+1,j}A_{i,j}A_{i+1,j} + C_{i,j}D_{i+1,j}C_{i+1,j}D_{i,j}/q^4\\ &\quad + a^n(C_{i,j}t_{i+1,j}D_{i+1,j}A_{i+1,j} + t_{i,j}A_{i,j}C_{i+1,j}D_{i+1,j})/q^2\\ &= (a^n t_{i+1,j}A_{i+1,j} + C_{i+1,j}D_{i+1,j}/q^2)(a^n t_{i,j}A_{i,j} + C_{i,j}D_{i,j}/q^2)\,.\end{aligned}$$

Thus,

$$S_{h+1} = a^n t_{i+1,j}A_{i+1,j} + C_{i+1,j}D_{i+1,j}/q^2\,. \ \blacksquare$$

Proof of Lemma 5.3. Let

$$N = \left[\frac{\sigma}{2}\left(qa^n + \frac{a^k-1}{q}\right)\right]^2 + \sigma^2 a^n\,.$$

We get $Q_i/\sigma = a^r$, $Q_{i+1}/\sigma = a^s$ and $Q_{i+2}/\sigma = a^t$ with $n = r+s$, $k = t-r$ and $t \ge r$.

Claim 1. *Q_{i+3}/σ is a power of a if and only if $t \le r+s = n$.*

Suppose $t > n$, and let $q \equiv \gamma \pmod{a^{t-n}}$ with $0 < \gamma < a^{t-n}$. We have $q = \mu a^{t-n} + \gamma$ and $qa^n = \mu a^t + \gamma a^n$. Thus, $qa^n/a^t = \mu + \gamma a^n/a^t \le \mu + (a^{t-n}-1)a^n/a^t = \mu + (a^t - a^n)/a^t$. Since $(a^t - a^n)/a^t < 1$ we get $q_{i+2} = \lfloor qa^n/a^t\rfloor = \mu$. (Note that this is true when $q > 1$. Also note, however, that if $q = 1$, then $\lfloor(2a^n+1)/(2a^t)\rfloor = 0$ if $t > n$, a contradiction.) Thus,

$$\begin{aligned}P_{i+3} &= \mu Q_{i+2} - P_{i+2} = \mu\sigma a^t - \frac{\sigma}{2}(qa^n - (a^k-1)/q)\,,\\ Q_{i+3} &= Q_{i+1} - q_{i+2}(P_{i+3} - P_{i+2})\\ &= \sigma a^s - \mu\left(\sigma\mu a^t - \frac{\sigma}{2}(qa^n - (a^k-1)/q) - \frac{\sigma}{2}(qa^n - (a^k-1)/q)\right)\\ &= \sigma a^s - \sigma\mu(\mu a^t - qa^n + (a^k-1)/q) = \sigma a^s - \sigma\mu(-\gamma a^n + (a^k-1)/q)\,.\end{aligned}$$

Now, $q < a^k = a^{t-n+s} = \mu a^{t-n} + \gamma$ with $0 < \gamma < a^{t-n}$. Thus, if μ is exactly divisible by a^ν we must have $\nu < s$. Therefore,

$$Q_{i+3}/\sigma = a^s + a^\nu \mu'(a^n\gamma - (a^k - 1)/q)\,.$$

Now, $qa^n > a^k$ implies that $a^n\gamma - (a^k - 1)/q > 0$. Therefore, $Q_{i+3}/\sigma = a^s + a^\nu h$ where $h > 0$ and a does not divide h. If $Q_{i+3}/\sigma = a^\lambda$, then $a^\lambda = a^s + a^\nu h$ implies that $a^{\lambda-\nu} = a^{s-\nu} + h$ if $\lambda - \nu > 0$; whence a divides h, a contradiction. If $\lambda - \nu = 0$ then $a^{s-\nu} + h = 1$, a contradiction since $h > 0$, and $s - \nu > 0$. It follows that $Q_{i+3}/2$ cannot be a power of a if $t > n$.

Now we examine the conditions under which Q_{i-1}/σ can be a power of a.

Claim 2. *If $qa^r < a^k - 1$ then Q_{i-1}/σ cannot be a power of a.*

We have (for either $q \neq 1$ or $\sigma \neq 2$)

$$\begin{aligned} q_i &= \lfloor (P_{i+1} + \sqrt{N})/Q_i \rfloor = \lfloor ((2/\sigma)P_{i+1} + \sqrt{(2/\sigma)^2 N})/(2Q_i/\sigma) \rfloor \\ &= \lfloor ((a^k - 1)/q + a^n q + qa^n + (a^k - 1)/q)/(2a^r) \rfloor \\ &= a^s q + \lfloor (a^k - 1)/(qa^r) \rfloor\,. \end{aligned}$$

If $q = 1$ and $\sigma = 2$ then

$$\begin{aligned} q_i &= \lfloor ((a^k - 1) + a^n + a^n + a^k)/(2a^r) \rfloor \\ &= a^s q + \lfloor (2a^k - 1)/(2a^r) \rfloor = a^s q + \lfloor (a^k - 1)/a^r \rfloor\,. \end{aligned}$$

If $qa^r < a^k - 1$ put $\nu = \lfloor (a^k - 1)/(qa^r) \rfloor$. Now put $\mu = q_i = a^s q + \nu$. Thus, $P_{i+1} = \sigma\mu a^r - P_i$ and $P_{i+1}/(2\sigma) = (\mu a^r/2) - P_i/(2\sigma)$. Also,

$$P_{i+1}/\sigma = (a^n q + (a^k - 1)/q)/2\,,$$

which implies that

$$P_{i+1}/(2\sigma) - P_i/(2\sigma) = (a^n q + (a^k - 1)/q - a^r\mu)/2\,.$$

Therefore,

$$(P_{i+1} - P_i)/\sigma = a^n q + (a^k - 1)/q - a^r\mu$$

and we get

$$\begin{aligned} Q_{i-1}/\sigma &= Q_{i+1}/\sigma + \mu(P_{i+1} - P_i)/\sigma \\ &= a^s + \mu(a^n q + (a^k - 1)/q - a^r\mu) \\ &= a^s + \mu(a^n q + (a^k - 1)/q - a^r a^s q - a^r\nu) \\ &= a^s + \mu((a^k - 1)/q - a^r\nu)\,. \end{aligned}$$

Put $(a^k - 1)/q - a^r\nu = m$. We have $\gcd(a, m) = 1$, and $Q_{i-1}/\sigma = a^s + \mu m$. Let a^λ exactly divide μ. Since $qa^n > a^k$ we have $\nu < a^k/qa^r < a^s$. Hence $\mu = qa^s + \nu$ where $\nu < a^s$ and $\lambda < s$. Thus, $Q_{i-1}/\sigma = a^s + a^\lambda\mu' m$ with a not dividing $\mu' m$. Therefore, a^λ divides Q_{i-1}/σ. If $Q_{i-1}/\sigma = a^\kappa$, then

$a^{\kappa-\lambda} = a^{s-\lambda} + \mu' m$. Since $\mu' m > 0$ we have $\kappa - \lambda \neq 0$. However, if $\kappa - \lambda > 0$ then a divides $\mu' m$, a contradiction which secures Claim 2.

If $qa^r > a^k - 1$ (observing that we cannot have equality) then $\nu = 0$. Hence,

$$Q_{i-1}/\sigma = a^s + \mu(a^k - 1)/q = a^s + a^s(a^k - 1) = a^{s+k}\,.$$

Thus, Q_{i-1}/σ is a power of a if and only if $qa^r > a^k - 1$.

If $n < k$ then $n < t - r < t$ so Q_{i+3}/σ is not a power of a. If $qa^r > a^k - 1$, then Q_{i-1}/σ is a power of a and we have 4 consecutive ($Q_{i-1}/\sigma = a^{s+k}$, $Q_i/\sigma = a^r$, $Q_{i+1}/\sigma = a^s$, $Q_{i+2}/\sigma = a^t$) powers of a.

We will now show that Q_{i-2}/σ cannot be a power of a. We may assume that $q > a^{k-r} - a^{-r}$. Thus, $q \geq a^{k-r} > a^s > 1$. Therefore, $q > a^{k-r}$ and $k > n$ imply that $t - r > r + s$, so $t - 2r > s$. Now, $q_{i-1} = \lfloor (P_i + \lfloor \sqrt{N} \rfloor)/Q_{i-1} \rfloor$ and $2P_{i-1}/\sigma = qa^n - (a^k - 1)/q$. Thus, $q_{i-1} = \lfloor qa^n/a^{s+k} \rfloor = \lfloor q/a^{t-2r} \rfloor$. Put $\nu = q_{i-1}$ and let $q = a^{t-2r}\nu + m$ where $0 < m < a^{t-2r}$. Since $Q_{i-2}/\sigma = Q_i/\sigma + q_{i-1}(P_i - P_{i-1})/\sigma$, and $P_i - P_{i-1} = 2P_i - \nu Q_{i-1}$, we get

$$Q_{i-2}/\sigma = a^r + \nu(qa^n - (a^k - 1)/q - \nu a^{s+k}) = a^r + \nu(a^n m - (a^k - 1)/q)\,.$$

Note that $\gcd(a^n m - (a^k - 1)/q, a) = 1$, and let a^λ exactly divide ν.

We get $Q_{i-2}/\sigma = a^r + a^\lambda \mu$, where a does not divide μ. If a^r divides ν, then $q > a^{t-r} = a^k$, a contradiction. Thus, $\lambda < r$ and we get $Q_{i-2}/\sigma \equiv 0 \pmod{a^\lambda}$. If $Q_{i-2}/\sigma = a^\kappa$ then $a^{k-\lambda} = a^{r-\lambda} + \mu$. Since $qa^n > a^k$ we must have $\mu > 0$. Thus, $k - \lambda \neq 0$. It follows that $\mu \equiv 0 \pmod{a}$, a contradiction. ∎

Acknowledgements. The authors' research is supported by NSERC Canada (grants number A8484 and A7649 respectively). Moreover, the first author's current research is supported by a Killam research award held at the University of Calgary in 1990. Finally, the authors thank the referee for so carefully checking the manuscript.

References

[1] L. Bernstein, *Fundamental units and cycles*, J. Number Theory 8 (1976), 446–491.

[2] —, *Fundamental units and cycles in the period of real quadratic number fields*, Part II, Pacific J. Math. 63 (1976), 63–78.

[3] G. Chrystal, *Textbook of Algebra*, part 2, 2nd ed., Dover Reprints, N.Y., 1969, 423–490.

[4] M. D. Hendy, *Applications of a continued fraction algorithm to some class number problems*, Math. Comp. 28 (1974), 267–277.

[5] C. Levesque, *Continued fraction expansions and fundamental units*, J. Math. Phys. Sci. 22 (1988), 11–44.

[6] C. Levesque and G. Rhin, *A few classes of periodic continued fractions*, Utilitas Math. 30 (1986), 79–107.

[7] R. A. Mollin, *Prime powers in continued fractions related to the class number one problem for real quadratic fields*, C. R. Math. Rep. Acad. Sci. Canada 11 (1989), 209–213.

[8] —, *Powers in continued fractions and class numbers of real quadratic fields*, Utilitas Math., to appear.

[9] R. A. Mollin and H. C. Williams, *Powers of* 2*, continued fractions and the class number one problem for real quadratic fields* $\mathbb{Q}(\sqrt{d})$ *with* $d \equiv 1 \pmod 8$, in: The Mathematical Heritage of C. F. Gauss, G. M. Rassias (ed.), World Sci., 1991, 505–516.

[10] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner, Stuttgart 1977.

[11] D. Shanks, *The infrastructure of a real quadratic field and its applications*, in: Proc. 1972 Number Theory Conf., Univ. of Colorado, Boulder, Colo., 1973, 217–224.

[12] H. C. Williams, *A note on the period length of the continued fraction expansion of certain* $\sqrt{D}$, Utilitas Math. 28 (1985), 201–209.

[13] H. C. Williams and M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*, Math. Comp. 177 (1987), 405–423.

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

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF MANITOBA
WINNIPEG, MANITOBA R3T 2N2
CANADA

E-mail:
RAMOLLIN@ACS.UCALGARY.CA
Hugh_Williams@CSMAIL.CS.UMANITOBA.CA

Received on 7.9.1990
and in revised form on 24.10.1991 (2078)