CONTINUED FRACTIONS OF GIVEN SYMMETRIC PERIOD

Franz Halter-Koch
Karl-Franzens-Universität, Halbärthgasse 1/I, A-8010 Graz, Österreich
(Submitted October 1989)

1. If $D > 1$ is a rational number, not a square, then $\sqrt{D}$ has a (simple) continued fraction expansion of the form

$$\sqrt{D} = [b_0, \overline{b_1, \ldots, b_{k-1}, 2b_0}]$$

with $k \geq 1$ and positive integers b_i such that the sequence $(b_1, \ldots, b_{k-1})$ is *symmetric*, i.e., $b_i = b_{k-i}$ for all $i \in \{1, \ldots, k-1\}$. Necessary and sufficient conditions on $b_0, \ldots, b_{k-1}$ which guarantee that D is an integer are stated in [3; §26]. Recently, C. Friesen [1] gave a fresh proof of these conditions. He deduced, moreover, that for a given symmetric sequence $(b_1, \ldots, b_{k-1})$ there is either no integral D such that the continued fraction expansion of $\sqrt{D}$ has the given sequence as its symmetric part or there are infinitely many squarefree such D.

In this paper, I shall prove a more precise statement. Starting with the conditions as in [3; §26] I will show that, given a symmetric sequence which meets these conditions, there are infinitely many D with prescribed p-adic exponent $v_p(D)$ for finitely many p and $p^2 \nmid D$ for all other p, such that $\sqrt{D}$ has the given sequence as the symmetric part of its continued fraction expansion. Moreover, I will show that about 2/3 (resp. 5/6) of all symmetric sequences of the given even (resp. odd) length are symmetric parts of the continued fraction expansion of $\sqrt{D}$ for some integral D. Finally, I consider the corresponding questions for the continued fraction expansion of $(1 + \sqrt{D})/2$ for an integral $D \equiv 1 \pmod 4$.

2. I begin by citing Satz [3; 3.17] in an appropriate form.

Theorem 1: Let $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ be a symmetric sequence in $\mathbb{N}_+$ and let $b_0 \in \mathbb{N}_+$. Then the following assertions are equivalent:

a) $[b_0, \overline{b_1, \ldots, b_{k-1}, 2b_0}] = \sqrt{D}$ with $D \in \mathbb{N}_+$;

b) $b_0 = \frac{1}{2} \cdot [me - (-1)^k fg]$ for some $m \in \mathbb{Z}$, where e, f, and g are defined by the matrix equation

$$\begin{pmatrix} e & f \\ f & g \end{pmatrix} = \prod_{i=1}^{k-1} \begin{pmatrix} b_i & 1 \\ 1 & 0 \end{pmatrix}. \tag{1}$$

If this condition is fulfilled, then

$$D = b_0^2 + mf - (-1)^k g^2. \tag{2}$$

In order to state more precise results, I introduce the following notation.

Definition: For a symmetric sequence of positive integers $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ let

$$\mathscr{D}(b_1, \ldots, b_{k-1})$$

be the set of all $D \in \mathbb{N}_+$ with $\sqrt{D} = [b_0, \overline{b_1, \ldots, b_{k-1}, 2b_0}]$ for some $b_0 \in \mathbb{N}_+$.

Corollary 1: Let $(b_1, \ldots, b_{k-1})$ be a symmetric sequence in $\mathbb{N}_+$ and define e, f, g by (1). Then the following assertions are equivalent:

a) $\mathcal{D}(b_1, \ldots, b_{k-1}) \neq \emptyset$.

b) Either $e \equiv 1 \pmod 2$ or $e \equiv fg \equiv 0 \pmod 2$.

If b) is fulfilled, then $\mathcal{D}(b_1, \ldots, b_{k-1})$ consists of all $D \in \mathbb{N}_+$ which are of the form

$$D = \frac{e^2m^2}{4} + \left[f - (-1)^k \frac{efg}{2}\right] \cdot m + \left[\frac{f^2g^2}{4} - (-1)^k g^2\right] \tag{3}$$

with $m \in \mathbb{Z}$ satisfying $me - (-1)^k fg > 0$.

Proof: The conditions stated in b) are necessary and sufficient for the existence of $m \in \mathbb{Z}$ such that

$$b_0 = \frac{1}{2} \cdot [me - (-1)^k fg]$$

is a positive integer. Inserting this expression for b_0 in (2) yields (3). □

Applying Corollary 1 to the special sequence $(b_1, \ldots, b_{k-1}) = (1, \ldots, 1)$ gives

$$\begin{pmatrix} e & f \\ f & g \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{pmatrix},$$

where $(F_n)_{n \geq -1}$ is the ordinary Fibonacci sequence defined by

$$F_{-1} = 1,\ F_0 = 0,\ F_{n+1} = F_n + F_{n-1}.$$

Taking into account that $F_k \equiv 0 \pmod 2$ if and only if $k \equiv 0 \pmod 3$, I obtain

Corollary 2: $\mathcal{D}(\underbrace{1, \ldots, 1}_{(k-1)}) \neq \emptyset$ if and only if $k \not\equiv 0 \pmod 3$.

3. Now I investigate the possible prime powers dividing $D \in \mathcal{D}(b_1, \ldots, b_{k-1})$ for a given symmetric sequence $(b_1, \ldots, b_{k-1})$.

For $n \in \mathbb{Z}$, $n \neq 0$, and a prime p, set

$$v_p(n) = w \text{ if } p^w | n,\ p^{w+1} \nmid n\ (w \geq 0).$$

The following result is an immediate consequence of the arguments given in [2; §2].

Lemma: Let $F(X) = AX^2 + BX + C \in \mathbb{Z}[X]$ be a quadratic polynomial. For a prime p, set

$$E_p(F) = \{w \in \mathbb{N} \mid v_p(F(x)) = w \text{ for some } x \in \mathbb{Z}\}.$$

Let P be a finite set of primes, $w_p \in E_p(F)$ for $p \in P$, and suppose that, for every prime $p \notin P$, the congruence $F(x) \equiv 0 \pmod{p^2}$ has at most two solutions $x \pmod{p^2}$. Then there exist infinitely many $x \in \mathbb{N}$, such that

$$v_p(F(x)) = w_p \text{ for all } p \in P$$

and

$$v_p(F(x)) \leq 1 \text{ for all primes } p \notin P.$$

Now let $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ be a symmetric sequence of positive integers. Define e, f, and g by (1) and, depending on these numbers, for every prime p, a set $E_p = E_p(e, f, g, k) \subset \mathbb{N}$ of possible exponents as follows:

a) $p \neq 2$.

$$E_p = \begin{cases} \{0\}, & \text{if } e \equiv 1 \pmod 2,\ p \nmid e, \text{ and } \left(\frac{(-1)^k}{p}\right) = -1; \\ \mathbb{N}, & \text{otherwise.} \end{cases}$$

b) $p = 2$, $e \equiv 1 \pmod 2$:

$$E_2 = \begin{cases} \{0, 1\}, & \text{if } k \equiv 1 \pmod 2; \\ \mathbf{N}\backslash\{1, 2\}, & \text{if } k \equiv 0 \pmod 2. \end{cases}$$

c) $p = 2$, $e \equiv fg \equiv 0 \pmod 2$:

$$E_2 = \begin{cases} \mathbf{N}_+, & \text{if } e \equiv 2,\ g \equiv 0 \pmod 4; \\ \mathbf{N}, & \text{otherwise}. \end{cases}$$

With these definitions, it is possible to state Theorem 2, which generalizes the results of [1]:

Theorem 2: Let $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ be a symmetric sequence of positive integers, define e, f, and g by (1), and suppose that either $e \equiv 1 \pmod 2$ or $e \equiv fg \equiv 0 \pmod 2$. For a prime p, let $E_p = E\ (e, f, g, k)$ be defined as above.

i) If $D \in \mathscr{D}(b_1, \ldots, b_{p-1})$, then $v_p(D) \in E_p$ for all primes p.

ii) Let P be a finite set of primes and $w_p \in E_p$ for $p \in P$. Then there are infinitely many $D \in \mathscr{D}(b_1, \ldots, b_{k-1})$ such that $v_p(D) = w_p$ for all $p \in P$ and $v_p(D) \leq 1$ for all primes $p \notin P$.

Proof:

Case 1. $e \equiv 1 \pmod 2$. By (1), $eg - f^2 = (-1)^{k+1}$ and thus $f + g \equiv 1 \pmod 2$. It follows from (3) that $D \in \mathbf{N}$ if and only if m is even. Set $m = 2n$; then, by (3),

$$D = D(n) = e^2n^2 + [2f - (-1)^k efg] \cdot n + \left[\frac{f^2g^2}{4} - (-1)^k g^2\right]. \tag{4}$$

By the above Lemma, it is enough to show that for every prime p the following two assertions are true:

1. $E_p = \{v_p(D(x))\,|\,x \in \mathbf{Z}\}$.
2. The congruence $D(x) \equiv 0 \pmod{p^2}$ has at most two solutions $x \pmod{p^2}$.

From (4) I obtain, by an easy calculation,

$$e^2 \cdot D(n) = \left[e^2n + f - (-1)^k \frac{efg}{2}\right]^2 - (-1)^k,$$

$$D'(n) = 2e^2n + 2f - (-1)^k efg.$$

If $p|e$, $p \neq 2$, the congruence $D(x) \equiv 0 \pmod{p^w}$ has exactly one solution $x \pmod{p^w}$ for every $w \geq 1$ and thus there are $x \in \mathbf{Z}$ with $v_p(D(x)) = w$ for every $w \geq 0$. If $p\nmid e$, $p \neq 2$, and $[(-1)^k/p] = -1$, the congruence $D(x) \equiv 0 \pmod p$ has no solution. If $p\nmid e$, $p \neq 2$, and $[(-1)^k/p] = 1$, the congruence $D(x) \equiv 0 \pmod p$ has two different solutions; these satisfy $D'(x) \not\equiv 0 \pmod p$ and, therefore, for every $w \geq 0$, there are $x \in \mathbf{Z}$ with $v_p(D(x)) = w$, and the congruence $D(x) \equiv 0 \pmod{p^2}$ also has exactly two solutions modulo p^2.

If $k \equiv 1 \pmod 2$, the congruence $D(x) \equiv 0 \pmod 4$ is unsolvable, but since $D(0) \not\equiv D(1) \pmod 2$, there are $x \in \mathbf{Z}$ with $v_2(D(x)) = w$ for $w = 0$ and $w = 1$.

If $k \equiv 0 \pmod 2$, then

$$D(n) \equiv \left(n + f + \frac{efg}{2}\right)^2 - 1 \pmod 8;$$

thus $D(x) \equiv 0 \pmod 2$ already implies $D(x) \equiv 0 \pmod 8$, the congruence $D(x) \equiv 0 \pmod 4$ has exactly two solutions $x \pmod 4$, and for every $w \geq 3$ there are $x \in \mathbf{Z}$ with $v_2(D(x)) = w$.

Case 2: $e \equiv fg \equiv 0 \pmod 2$. By (1), $eg - f^2 = (-1)^{k+1}$; thus, $k \equiv 0 \pmod 2$, $f \equiv 1 \pmod 2$, and $eg \equiv 0 \pmod 8$. It follows from (3) that $D \in \mathbf{Z}$ for all $m \in \mathbf{Z}$; therefore, I have to consider the polynomial

$$D = D(m) = \frac{e^2}{4}\cdot m^2 + \left(f - \frac{efg}{2}\right)\cdot m + \left(\frac{f^2g^2}{4} - g^2\right).$$

Again it is enough to show that for every prime p the following two assertions are true:

1. $E_p = \{v_p(D(x)) \mid x \in \mathbf{Z}\}$.
2. The congruence $D(x) \equiv 0 \pmod{p^2}$ has at most two solutions $x \pmod{p^2}$.

First, observe that

$$e^2D(m) = \left(\frac{e^2}{2}\cdot m + f - \frac{efg}{2}\right)^2 - 1.$$

If $p \neq 2$, the congruence $D(x) \equiv 0 \pmod{p}$ has at least one and at most two solutions $x \pmod{p}$, and these satisfy $D'(x) \not\equiv 0 \pmod{p}$. Therefore, for every $w \in \mathbf{N}$, there are $x \in \mathbf{Z}$ with $v_p(D(x)) = w$, and the congruence $D(x) \equiv 0 \pmod{p^2}$ has at most two solutions $x \pmod{p^2}$.

Suppose now that $e \equiv 2 \pmod 4$ and $g \equiv 0 \pmod 4$. Then $D(m) \equiv m^2 + fm \pmod 4$, and it follows that $D(m) \equiv 0 \pmod 2$ for all m, $D'(m) \equiv 1 \pmod 2$ for all m, the congruence $D(x) \equiv 0 \pmod 4$ has exactly two solutions $x \pmod 4$, and for every $w \in \mathbf{N}$ there are $x \in \mathbf{Z}$ with $v_p(D(x)) = w$.

If $e \equiv 0 \pmod 4$ or $g \equiv 2 \pmod 4$, then the congruence $D(x) \equiv 0 \pmod 2$ is soluble, and from $D'(x) \equiv 1 \pmod 2$ for all x, it follows that the congruence $D(x) \equiv 0 \pmod 4$ has at most two solutions $x \pmod 4$ and that, for every $w \in \mathbf{N}$, there are $x \in \mathbf{Z}$ with $v_p(D(x)) = w$. □

4. In this section it will be shown that about 2/3 (resp. 5/6) of all symmetric integer sequences $(b_1, \ldots, b_{k-1})$ satisfy $\mathscr{D}(b_1, \ldots, b_{k-1}) \neq \emptyset$. To do this, define $\theta : \mathbf{Z} \to GL_2(\mathbf{F}_2)$ by

$$\theta(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \pmod 2;$$

for a finite sequence $(b_1, \ldots, b_m)$ define

$$\theta(b_1, \ldots, b_m) = \prod_{j=1}^{m} \theta(b_j) \in GL_2(\mathbf{F}_2).$$

Obviously, $\theta(b_1, \ldots, b_m)$ depends only on $b_1, \ldots, b_m \pmod 2$. Put

$$\sigma = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbf{F}_2)$$

and find $\sigma^3 = \tau^2 = 1$, $\sigma\tau = \tau\sigma^2$ [as $GL_2(\mathbf{F}_2) \simeq \mathscr{S}_3$]. With these definitions, the following holds.

Theorem 3: Let $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ be a symmetric sequence of positive integers.

i) $(b_1, \ldots, b_{k-1}) \neq \emptyset$ if and only if $\theta(b_1, \ldots, b_{k-1}) \neq \sigma^2$.

ii) If k is even, $k = 2\ell$, then $\theta(b_1, \ldots, b_{k-1}) = \sigma^2$ if and only if

$$\theta(b_1, \ldots, b_{\ell-1}) \in \{\tau, \sigma^2\} \text{ and } b_\ell \equiv 1 \pmod 2.$$

Furthermore, if N_ℓ denotes the number of all

$$(b_1, \ldots, b_{\ell-1}) \in \{0, 1\}^{\ell-1} \text{ with } \theta(b_1, \ldots, b_{\ell-1}) \in \{\tau, \sigma^2\},$$

then

$$N_\ell = \frac{2^{\ell-1} + (-1)^\ell}{3}.$$

iii) If k is odd, $k = 2\ell + 1$, then $\theta(b_1, \ldots, b_{k-1}) = \sigma^2$ if and only if

$$\theta(b_1, \ldots, b_\ell) \in \{\sigma, \sigma\tau\}.$$

Furthermore, if N'_ℓ denotes the number of all

$$\theta(b_1, \ldots, b_\ell) \in \{0, 1\}^\ell \text{ with } \theta(b_1, \ldots, b_\ell) \in \{\sigma, \sigma\tau\},$$

then

$$N'_\ell = N_{\ell+1}.$$

Proof: i) is an immediate consequence of Corollary 1. If $k = 2\ell$ and

$$\theta(b_1, \ldots, b_{\ell-1}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_2),$$

then

$$\theta(b_1, \ldots, b_{k-1}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} b_\ell & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} ab_\ell & ab_\ell c + 1 \\ ab_\ell c + 1 & cb_\ell \end{pmatrix}$$

and thus

$$\theta(b_1, \ldots, b_{k-1}) = \sigma^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

if and only if $a = 0$, $c = b_\ell = 1$. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_2),$$

this implies also $b = 1$. Therefore, $\theta(b_1, \ldots, b_{k-1}) = \sigma^2$ if and only if

$$\theta(b_1, \ldots, b_{\ell-1}) = \begin{pmatrix} 0 & 1 \\ 1 & d \end{pmatrix} \in \{\tau, \sigma^2\}.$$

If $k = 2\ell + 1$ and

$$\theta(b_1, \ldots, b_\ell) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{F}_2),$$

then

$$\theta(b_1, \ldots, b_{k-1}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a + b & ac + bd \\ ac + bd & c + d \end{pmatrix} = \sigma^2$$

if and only if $a = b = 1$ and $d = c + 1$, i.e.,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \{\sigma, \sigma\tau\}.$$

To obtain the formulas for N_ℓ and N'_ℓ, consider the number

$$A_n(\xi) = \# (b_1, \ldots, b_n) \in \{0, 1\}^n \,|\, \theta(b_1, \ldots, b_n) = \xi\}$$

for any $n \in \mathbf{N}_+$ and $\xi \in GL_2(\mathbf{F}_2)$. These quantities satisfy the recursion formulas

$$A_1(\sigma) = A_1(\tau) = 1,$$
$$A_1(\xi) = 0 \text{ for all } \xi \in GL_2(\mathbf{F}_2)\backslash\{\sigma, \tau\},$$
$$A_{n+1}(\xi) = A_n(\xi\sigma^2) + A_n(\xi\tau) \text{ for all } \xi \in GL_2(\mathbf{F}_2),$$

which have the solution

$$A_n(\sigma) = A_n(\tau) = \frac{2^{n-1} + 2(-1)^{n-1}}{3},$$

$$A_n(\xi) = \frac{2^{n-1} + (-1)^n}{3} \text{ for } \xi \in GL_2(\mathbf{F}_2)\backslash\{\sigma, \tau\}.$$

Therefore, for $\ell \geq 2$,

$$N_\ell = A_{\ell-1}(\tau) + A_{\ell-1}(\sigma^2) = \frac{2^{\ell-1} + (-1)^\ell}{3},$$

$$N'_\ell = A_\ell(\sigma) + A_\ell(\sigma\tau) = \frac{2^\ell + (-1)^{\ell+1}}{3} = N_{\ell+1},$$

and these formulas remain true for $\ell = 1$. □

5. In this final section I formulate the corresponding results for the continued fraction expansion of $(1 + \sqrt{D})/2$ for $D \equiv 1 \pmod 4$; as the proofs are very similar to those for $\sqrt{D}$, I leave them to the reader. (For Theorem IA, see Satz [3; 3.34].)

Theorem 1A: Let $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ be a symmetric sequence in $\mathbf{N}_+$ and let $b_0 \in \mathbf{N}_+$. Then the following assertions are equivalent:

a) $[b_0, \overline{b_1, \ldots, b_{k-1}, 2b_0 - 1}] = \dfrac{1 + \sqrt{D}}{2}$ with $D \in \mathbf{N}_+$, $D \equiv 1 \pmod 4$.

b) $b_0 = \dfrac{1}{2} \cdot [1 + me - (-1)^k fg]$ for some $m \in \mathbf{Z}$, where e, f, and g are defined by (1).

If this condition is fulfilled, then

$$D = (2b_0 - 1)^2 + 4mf - 4 \cdot (-1)^k g^2.$$

Definition: For a symmetric sequence of positive integers $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ let $\mathscr{D}'(b_1, \ldots, b_{k-1})$ be the set of all $D \in \mathbf{N}_+$ with $D \equiv 1 \pmod 4$ and

$$\frac{1 + \sqrt{D}}{2} = [b_0, \overline{b_1, \ldots, b_{k-1}, 2b_0 - 1}] \quad \text{for some } b_0 \in \mathbf{N}_+.$$

Corollary 1A: Let $(b_1, \ldots, b_{k-1})$ be a symmetric sequence in $\mathbf{N}_+$ and define e, f, g by (1). Then the following assertions are equivalent:

a) $\mathscr{D}'(b_1, \ldots, b_{k-1}) \neq \emptyset$.

b) Either $e \equiv 1 \pmod 2$ or $e \equiv fg + 1 \equiv 0 \pmod 2$.

If b) is fulfilled, then $\mathscr{D}'(b_1, \ldots, b_{k-1})$ consists of all $D \in \mathbf{N}_+$, $D \equiv 1 \pmod 4$, which are of the form

$$D = e^2m^2 + [4f - 2 \cdot (-1)^k efg] \cdot m + [f^2g^2 - 4 \cdot (-1)^k g^2]$$

with $m \in \mathbf{Z}$ satisfying $1 + me - (-1)^k fg > 0$.

Corollary 2A: $\mathscr{D}'(1, \ldots, 1) \neq \emptyset$ (always).

Theorem 2A: Let $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ be a symmetric sequence of positive integers, define e, f, g by (1), and suppose that either $e \equiv 1 \pmod 2$ or $e \equiv fg + 1 \equiv 0 \pmod 2$. Let P' be the set of all odd primes p with $p \nmid e$ and

$$\left(\frac{(-1)^k}{p}\right) = -1.$$

i) If $D \in \mathscr{D}'(b_1, \ldots, b_{k-1})$ and $p \in P'$, then $p \nmid D$.

ii) Let P be a finite set of odd primes, $P \cap P' = \emptyset$ and $(w_p)_{p \in P}$ a sequence in $\mathbf{N}$. Then there are infinitely many $D \in \mathscr{D}'(b_1, \ldots, b_{k-1})$ such that $v_p(D) = w_p$ for all $p \in P$ and $v_p(D) \leq 1$ for all primes $p \notin P$.

Theorem 3A: Let $(b_1, \ldots, b_{k-1})$ $(k \geq 1)$ be a symmetric sequence of positive integers. Then $\mathscr{D}'(b_1, \ldots, b_{k-1}) = \emptyset$ if and only if k is even, $k = 2\ell$, and $b_\ell \equiv 0 \pmod 2$.

References

1. C. Friesen. "On Continued Fractions of Given Period." *Proc. AMS* *103* (1988): 9-14.
2. T. Nagell. "Zur Arithmetik der Polynome." *Abh. Math. Sem. Univ. Hamburg 1* (1922):184-88.
3. O. Perron. *Die Lehre von den Kettenbrüchen*. Bd. 1. Teubner, 1954.

*****