View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

ISSN 1064–5624, Doklady Mathematics, 2008, Vol. 78, No. 3, pp. 833–838. © Pleiades Publishing, Ltd., 2008.
Original Russian Text © V.V. Benyash-Krivets, V.P. Platonov, 2008, published in Doklady Akademii Nauk, 2008, Vol. 423, No. 2, pp. 155–160.

MATHEMATICS

Continued Fractions and *S*-Units in Function Fields

V. V. Benyash-Krivets[a] and Academician V. P. Platonov[b]

Received July 17, 2008

DOI: 10.1134/S1064562408060082

The purpose of this paper is two-fold: to present some results on continued fractions in function fields and show how continued fractions can be applied to find fundamental *S*-units in hyperelliptic fields.

Let k be an arbitrary field, and let $k(x)$ be the field of rational functions of one variable over k. For an irreducible polynomial $\nu \in k[x]$, $|\cdot| = |\cdot|_\nu$ denotes the corresponding valuation, $O_\nu = \{z \in k(x) | |z| \le 0\}$ denotes the corresponding valuation ring, and $p_\nu = \{z \in k(x) | |z| > 0\}$ is the ideal of the valuation $|\cdot|$. The residue field O_ν/p_ν coincides with $k[x]/(\nu)$ and is a finite extension of k. Let $k(x)_\nu$ be the completion of the field $k(x)$ in the valuation $|\cdot|$. We denote the extension of $|\cdot|$ to $k(x)$ by the same symbol $|\cdot|$. Let Σ be the system of coset representatives for the ideal (ν) in $k[x]$ consisting of all polynomials of degree less than $\deg\nu$. Then, each element $z \in k(x)_\nu$ has a unique representation in the form of a formal power series $z = \sum_{i=s}^{\infty} a_i \nu^i$, where $s \in \mathbf{Z}$ and $a_i \in \Sigma$. If $\deg\nu = 1$, then the field $k(x)_\nu$ can be identified with the field $k((\nu))$ of formal power series.

Continued fractions in function fields in the case of the valuation $|\cdot|_\infty$ were introduced by Artin [1]. We consider the general case of an arbitrary valuation $|\cdot| = |\cdot|_\nu$. Let $\beta \in k(x)_\nu$. We represent β as a formal power series $\beta = \sum_{i=s}^{\infty} d_i \nu^i$, where $d_i \in \Sigma$, and set $[\beta] = \sum_{i=s}^{0} d_i \nu^i$ if $s \le 0$ or $[\beta] = 0$ if $s > 0$. Let $a_0 = [\beta]$. If $\beta - a_0 \ne 0$, then we set $\beta_1 = \dfrac{1}{\beta - a_0} \in k(x)_\nu$ and $a_1 = [\beta_1]$. Then, by induction, we define elements a_i and β_i; namely, if $\beta_{i-1} - a_{i-1} \ne 0$, then we set $\beta_i = \dfrac{1}{\beta_{i-1} - a_{i-1}} \in k(x)_\nu$ and $a_i = [\beta_i]$. It is easy to show that the process terminates if and only if $\beta \in k(x)$. We use the standard shorthand notation $\beta = [a_0, a_1, a_2, \ldots]$ for continued fractions. By construction, $\beta_n = [a_n, a_{n+1}, \ldots]$.

Let us define elements $p_i, q_i \in k(x)$ by induction. We set $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$, and

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2} \tag{1}$$

for $n \ge 0$. We have $\dfrac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$ for $n \ge 0$. It can be shown in a standard way that, for $n \ge -1$,

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n, \tag{2}$$

$$q_n\beta - p_n = \frac{(-1)^n}{q_n\beta_{n+1} + q_{n-1}}, \tag{3}$$

$$\beta = \frac{p_n\beta_{n+1} + p_{n-1}}{q_n\beta_{n+1} + q_{n-1}}. \tag{4}$$

The fraction $\dfrac{p_n}{q_n}$ is called the nth convergent of β. By construction, $|a_n| = |\beta_n| < 0$ for $n \ge 1$. From (1) the following relation easily follows by induction:

$$|q_n| = |a_n| + |q_{n-1}| = \sum_{j=1}^{n} |a_j|, \tag{5}$$

and (3) implies

$$|q_n\beta - p_n| = -|q_{n+1}| = -|a_{n+1}| - |q_n| > -|q_n| \tag{6}$$

or, equivalently,

$$\left|\beta - \frac{p_n}{q_n}\right| > -2|q_n|. \tag{7}$$

Thus, $\lim\limits_{n\to\infty} \dfrac{p_n}{q_n} = \beta$. Let us introduce the notion of best approximation to β. If $\dfrac{a}{b} \in k(x)$, where $a, b \in k[x]$ are coprime polynomials, then we decompose a and b into

[a] *Belarussian State University, pr. Nezavisimosti 4, Minsk, 220030 Belarus*
e-mail: benyash@bsu.by

[b] *Research Institute for System Studies, Russian Academy of Sciences, Nakhimovskii pr. 36, korp. 1, Moscow, 117218 Russia*
e-mail: platonov@niisi.ras.ru

powers of ν as $a = a_0 + a_1\nu + \ldots + a_s\nu^s$ and $b = b_0 + b_1\nu + \ldots + b_t\nu^t$, where $a_i, b_i \in \Sigma$, $a_s \neq 0$, and $b_t \neq 0$. Dividing a and b by ν^r, where $r = \max\{s, t\}$, we represent the fraction $\frac{a}{b}$ in the form

$$\frac{a}{b} = \frac{c_{-p}\nu^{-p} + \ldots + c_0}{d_{-q}\nu^{-q} + \ldots + d_0}, \tag{8}$$

where $c_i, d_i \in \Sigma$; $c_{-p} \neq 0$; $d_{-q} \neq 0$; and c_0 and d_0 are not both zero. In what follows, we assume that all elements of $k(x)$ are written in the form (8).

Definition. An irreducible fraction $\frac{p}{q} \in k(x)$ is a best approximation to β if, for any other irreducible fraction $\frac{a}{b} \neq \frac{p}{q}$ such that $|b| \geq |q|$, $\left|\beta - \frac{p}{q}\right| > \left|\beta - \frac{a}{b}\right|$ (or, equivalently, $|q\beta - p| > |b\beta - a|$).

Proposition 1. *A fraction $\frac{p}{q}$ is a best approximation to β if and only if $\left|\beta - \frac{p}{q}\right| > -2|q|$ (or $|q\beta - p| > -|q|$).*

Proof. Let us write the elements p, q, β, and $q\beta$ as formal power series in ν:

$$p = \sum_{i=-r}^{0} a_i\nu^i, \quad q = \sum_{i=-s}^{0} b_i\nu^i, \quad \beta = \sum_{i=m}^{\infty} c_i\nu^i,$$

$$q\beta = \sum_{i=m-s}^{\infty} d_i\nu^i,$$

where $a_i, b_i, c_i, d_i \in \Sigma$, $a_{-r} \neq 0$, and $b_{-s} \neq 0$. Let $n = \deg\nu$. Then,

$$a_i = \sum_{j=0}^{n-1} a_{ij}x^j, \quad b_i = \sum_{j=0}^{n-1} b_{ij}x^j, \quad c_i = \sum_{j=0}^{n-1} c_{ij}x^j,$$

$$d_i = \sum_{j=0}^{n-1} d_{ij}x^j,$$

where $a_{ij}, b_{ij}, c_{ij}, d_{ij} \in k$. Moreover, $d_{ij} = L_{ij}(b_{00}, \ldots, b_{-s,n-1})$, where L_{ij} is a linear form in $n(s+1)$ variables with coefficients from the field k. Suppose that $|q\beta - p| = l \leq -|q| = s$. It follows from the definition of best approximation that $l > 0$. Thus, we have $|p| = |q| + |\beta|$, i.e., $r = s - m$. Since $q\beta - p = \sum_{i=-r}^{0}(d_i - a_i)\nu^i + \sum_{i=1}^{\infty} d_i\nu^i$, we have

$$a_i = d_i, \quad i = -r, \ldots, 0, \tag{9}$$

$$d_1 = d_2 = \ldots = d_{i-1} = 0. \tag{10}$$

It follows from (10) that

$$d_{ij} = L_{ij}(b_{00}, \ldots, b_{-s,n-1}) = 0, \quad i = 1, 2, \ldots, l-1, \quad j = 0, 1, \ldots, n-1. \tag{11}$$

Thus, the set $(b_{00}, \ldots, b_{-s,n-1})$ is a solution of the system of linear homogeneous equations

$$CY = 0, \tag{12}$$

where $Y = (y_{00}, \ldots, y_{-s,n-1})^t$ and C is a matrix with coefficients from the field k containing $n(s+1)$ columns and $n(l-1)$ rows. By assumption, $l \leq s$; therefore, $\operatorname{rank} C \leq n(l-1)$, and in solving (12), we obtain m free variables $z_1, z_2, \ldots, z_m$, where

$$m = n(s+1) - \operatorname{rank} C \geq n(s-l+2) \geq 2n.$$

The remaining variables y_{ij} are expressed in terms of the free ones as

$$y_{ij} = H_{ij}(z_1, z_2, \ldots, z_m) \tag{13}$$

for some linear form H_{ij}. Since $b_{-s} \neq 0$, it follows that (12) has a solution $(b_{00}, \ldots, b_{-s,n-1})$ in which not all of the $b_{-s,0}, \ldots, b_{-s,n-1}$ are zero. This means that not all linear forms H_{ij} identically vanish.

Consider the system of linear homogeneous equations

$$H_{-s,0}(z_1, z_2, \ldots, z_m)$$
$$\ldots = H_{-s,n-1}(z_1, z_2, \ldots, z_m) = 0, \tag{14}$$

which involves $m \geq 2n$ unknowns and n equations. System (14) has a nonzero solution $(z_1^0, z_2^0, \ldots, z_m^0)$. According to (13), we have $y_{ij}^0 = H_{ij}(z_1^0, z_2^0, \ldots, z_m^0)$, which yields the polynomials $b_i^0 = \sum_{j=0}^{n-1} y_{ij}^0 x^j$, where $i = -s, -s+1, \ldots, 0$. By construction, we have $b_{-s}^0 = 0$. As a result, we obtain $q_1 = \sum_{i=-s+1}^{0} b_i^0\nu^i$. Using (9), we find p_1. By construction, we have $|q_1| > |q|$ and $|q_1\beta - p_1| \geq l = |q\beta - p|$. Clearly, $\frac{p}{q} \neq \frac{p_1}{q_1}$, which contradicts $\frac{p}{q}$ being a best approximation. This completes the proof of Proposition 1.

Proposition 2. *If fractions $\frac{a}{b}$ and $\frac{c}{d}$ are best approximations to β and $|b| = |d|$, then there exists a constant $h \in k^*$ such that $a = hc$ and $b = hd$.*

Proof. If $\frac{a}{b} \neq \frac{c}{d}$ in $k(x)$, then, by the definition of best approximation, we have two opposite inequalities $\left|\beta - \frac{a}{b}\right| > \left|\beta - \frac{c}{d}\right|$ and $\left|\beta - \frac{a}{b}\right| < \left|\beta - \frac{c}{d}\right|$, which contradict each other. Therefore, $\frac{a}{b} = \frac{c}{d}$ in $k(x)$. The irreducibility of these fractions implies the required assertion.

Proposition 3. *If* $\deg\nu = 1$, *then the nth convergent* $\frac{p_n}{q_n}$ *of* β *is a best approximation to* β.

Proof. The elements p_n and q_n have the form

$$p_n = c_{-s}\nu^{-s} + \ldots + c_0, \quad q_n = d_{-r}\nu^{-r} + \ldots + d_0,$$

where $c_i, d_i \in k$. Therefore, $\frac{p_n}{q_n}$ is of the form (8). Now, Proposition 1 and relation (6) immediately imply that $\frac{p_n}{q_n}$ is a best approximation to β.

The following theorem shows that the converse is also true.

Theorem 1. *Let* $\deg\nu = 1$. *If a fraction* $\frac{a}{b}$ *is a best approximation to* β, *then there exists a convergent* $\frac{p_n}{q_n}$ *of* β *and a constant* $c \in k^*$ *such that* $a = cp_n$ *and* $b = cq_n$.

Proof. First, let us prove that $|b| = |q_n|$ for some convergent $\frac{p_n}{q_n}$. Assume the opposite. Since $|q_0| = |1| = 0$, $|q_n| < |q_{n-1}|$ (by of (5)), and $|b| \le 0$, it follows that there exists an n for which $|q_{n+1}| < |b| < |q_n|$. Since $\frac{p_{n+1}}{q_{n+1}}$ is a best approximation to β and $|b| > |q_{n+1}|$, it follows that $\left|\frac{p_{n+1}}{q_{n+1}} - \beta\right| > \left|\beta - \frac{a}{b}\right|$. Thus, we have

$$\left|\frac{1}{bq_{n+1}}\right| \ge \left|\frac{p_{n+1}}{q_{n+1}} - \frac{a}{b}\right| = \left|\frac{p_{n+1}}{q_{n+1}} - \beta + \beta - \frac{a}{b}\right| = \left|\beta - \frac{a}{b}\right|.$$

Therefore, $\left|\beta - \frac{a}{b}\right| \le \left|\frac{1}{bq_{n+1}}\right| = -|b| - |q_{n+1}|$. Using (6), we obtain $|b\beta - a| \le -|q_{n+1}| = |q_n\beta - p_n|$. Since $|q_n| > |b|$, this contradicts $\frac{a}{b}$ being a best approximation to β. Thus, for some n, we have $|q_n| = |b|$. Applying Proposition 2, we obtain the required assertion.

In the case of $\deg\nu > 1$, the convergent $\frac{p_n}{q_n}$ may not be a best approximation to β.

Example. Suppose that $k = F_3$, $\nu = x^2 + 1 \in k[x]$, and $d = x^3 + 2x^2 + x + 1 = (x + 2)\nu + 2 \in k[x]$ is an irreducible polynomial. Since 2 is a square in the residue field $k(x)/(\nu)$, it follows that $\sqrt{d} \in k(x)_\nu$, and the element $\sqrt{d}$ can be expanded as

$$\sqrt{d} = x + (x + 2)\nu + (x + 1)\nu^2 + x\nu^3 + x\nu^4 + 2x\nu^5 + (2x + 1)\nu^6 + \ldots.$$

Expanding $\sqrt{d}$ in a continued fraction, we obtain

$$a_0 = x, \quad a_1 = (x + 1)\nu^{-1} + 1, \quad a_2 = \nu^{-1} + x + 1,$$
$$a_3 = (2x + 1)\nu^{-1}, \ldots,$$

and the convergents of $\sqrt{d}$ have the form

$$\frac{p_1}{q_1} = \frac{(x-1)\nu^{-1} + x + 2}{(x + 1)\nu^{-1} + 1},$$

$$\frac{p_2}{q_2} = \frac{(x-1)\nu^{-2} + x\nu^{-1} + x + 2 + \nu}{(x + 1)\nu^{-2} + (2x + 1)\nu^{-1} + x}.$$

Let us show that $\frac{p_2}{q_2}$ is not a best approximation to $\sqrt{d}$. By virtue of (7), we have $\left|\sqrt{d} - \frac{p_2}{q_2}\right| = -|a_3| - 2|q_2| = 5$. On the other hand, to write the convergent $\frac{p_2}{q_2}$ in the form (8), we must divide the numerator and the denominator by ν: $\frac{p_2}{q_2} = \frac{\tilde{p}_2}{\tilde{q}_2} = \frac{(x-1)\nu^{-3} + x\nu^{-2} + (x + 2)\nu^{-1} + 1}{(x + 1)\nu^{-3} + (2x + 1)\nu^{-2} + x\nu^{-1}}$. We obtain $\left|\sqrt{d} - \frac{\tilde{p}_2}{\tilde{q}_2}\right| = \left|\sqrt{d} - \frac{p_2}{q_2}\right| = 5 < -2|\tilde{q}_2| = 6$. By Proposition 1, $\frac{p_2}{q_2}$ is not a best approximation to $\sqrt{d}$.

It can be shown in a standard way that if a continued fraction $[a_0, a_1, \ldots]$ for β is periodic, then β is a quadratic irrationality. In the case of an infinite field k and the valuation $|\cdot|_\infty$, the converse is not always true (see [2]). The following proposition is valid.

Proposition 4. *Suppose that* $k = F_q$ *is the field with* q *elements and* $\deg\nu = 1$. *Let us identify the completion* $k(x)_\nu$ *with the formal power series field* $k((\nu))$. *If* $\beta \in k((\nu))$ *is a quadratic irrationality, then the continued fraction for* β *is periodic.*

Proof. Let $\beta \in k((\nu))$ be a root of the quadratic polynomial $H(X) = rX^2 + sX + t$, where $r, s, t \in k[\nu]$, and let $\beta = [a_0, a_1, \ldots]$ be a decomposition of β into a continued fraction. We set $D = s^2 - 4rt \in k[\nu]\backslash k$ and $H(X, Y) = rX^2 + sXY + tY^2$. It follows from (3) that

$$\beta_{n+1} = \frac{B_n + r\beta}{A_n}, \tag{15}$$

where $A_n = (-1)^{n+1}H(p_n, q_n)$ and $B_n = (-1)^n(rp_{n-1}p_n + sp_{n-1}q_n + tq_{n-1}q_n)$. Clearly, for sufficiently large n, we have $\left|\frac{p_n}{q_n} - \beta\right| > |\beta - \bar{\beta}|$, where $\bar{\beta}$ is the second root of $H(X)$. Thus, $\left|\frac{p_n}{q_n} - \bar{\beta}\right| = \left|\frac{p_n}{q_n} - \beta + \beta - \bar{\beta}\right| = |\beta - \bar{\beta}|$. Since

$\beta - \bar{\beta} = \frac{2\sqrt{D}}{r}$, it follows that $|\beta - \bar{\beta}| = \frac{1}{2}|D| - |r|$. This implies $|p_n - \bar{\beta} q_n| = |q_n| + \frac{1}{2}|D| - |r|$. Since $H(X, Y) = r(X - \beta Y)(X - \bar{\beta} Y)$, we finally obtain

$$|A_n| = r(p_n - \beta q_n)(p_n - \bar{\beta} q_n) = \frac{1}{2}|D| - |a_{n+1}| > 0. \quad (16)$$

Let us find a lower bound for $|B_n|$. It follows from (15) that $B_n = A_n\beta_{n+1} - r\beta$. The equality $\beta(r\beta + s) = -t$ implies $|r\beta| \geq 0$. Taking into account (16), we obtain $|A_n\beta_{n+1}| = |A_n a_{n+1}| = \frac{1}{2}|D| \geq 0$. Therefore, $|B_n| \geq \min\{|A_n\beta_{n+1}|, |r\beta|\} \geq 0$.

Thus, A_n and B_n are polynomials from $k[x]$. Their degrees do not exceed $\max(\deg r, \deg s, \deg t)$. Since the field k is finite, there are only finitely many such polynomials. This means that, for some i and j, we have $A_i = A_{i+j}$ and $B_i = B_{i+j}$, whence $\beta_i = \beta_{i+j}$, and the continued fraction for β is periodic.

Note that the above argument does not apply if $\deg\nu > 1$. In this case, although A_n and B_n are still polynomials from $k[x]$, we cannot assert that their degrees are bounded above by $\max(\deg r, \deg s, \deg t)$. For $\beta = \sqrt{d}$ from the example considered above, we have $r = 1$, $s = 0$, $t = d$, $A_2 = p_2^2 - dq_2^2 = 2x(x^2 + 1)(x^2 + x + 2)$, and $\deg A_2 > \deg d$.

In what follows, we show how to use continued fractions for finding fundamental S-units in hyperelliptic fields in the case of $\deg\nu = 1$ and finite field k. Hereafter, we assume that $k = F_q$ is the finite field of characteristic $p > 2$, $d(x) = c_0x^{2n+1} + c_1x^{2n} + \ldots + c_{2n+1}$ is a square-free polynomial, and $c_0 \neq 0$. Suppose that $K = k(x)(\sqrt{d})$, $\nu = x - b$, and $\bar{x}$ is the image of x in the residue field O_ν/p_ν. We assume that $d(\bar{x}) = \beta^2$ for some $0 \neq \beta \in O_\nu/p_\nu$ (this means that the point $(\beta, \bar{x})$ is an O_ν/p_ν-point of the hyperelliptic curve $y^2 = d(x)$). The valuation $|\cdot|_\nu$ has two nonequivalent extensions to the field K. We denote these valuations by $|\cdot|_{\nu'}$ and $|\cdot|_{\nu''}$. The non-Archimedean valuation $|\cdot|_\infty$ admits a unique extension to K, and we denote it by the same symbol $|\cdot|_\infty$. Let $S = \{|\cdot|_\infty, |\cdot|_{\nu'}\}$, and let O_S be the ring of S-integer elements in K, i.e., of elements $z \in K$ such that $|z|_\nu \geq 0$ for all valuations $|\cdot|_\nu$ of the field K not belonging to S. The set U_S of invertible elements of the ring O_S is called the group of S-units of the field K. By virtue of the generalized Dirichlet theorem on units (see [3, Chapter IV, Theorem 9]), the group U_S is the direct product of the group k^* and the free Abelian group G of rank 1. The generator of the group G is called the fundamental S-unit.

In [5], an effective algorithm for calculating fundamental S-units was suggested. In the classical case of the quadratic extension $L = Q(\sqrt{d})$ of the field Q, the fundamental unit of the field L can be found by expanding $\sqrt{d}$ or $\frac{\sqrt{d} - 1}{2}$ into a continued fraction (see [4]). Our purpose is to show that, in the case of a hyperelliptic field K and the valuation $|\cdot|_\nu$ determined by a linear polynomial ν, the fundamental S-unit can also be found by the method of continued fractions. It was proved in [5] that calculating the fundamental S-unit requires finding the minimum positive integer m for which the valuation equation

$$f^2 - g^2 d = a\nu^m, \quad (17)$$

where $a \in k^*$, has a solution in polynomials $f, g \in k[\nu]$, where $g \neq 0$. Then either $f + g\sqrt{d}$ or $f - g\sqrt{d}$ is the fundamental S-unit. By the minimality of m, $(f, g) = 1$ and ν does not divide f and g. The following theorem (see also [6]) gives an algorithm for finding the fundamental S-unit by using continued fractions.

Theorem 2. *Let m be the minimum positive integer for which Eq.* (17) *has a solution in polynomials $f, g \in k[\nu]$, where $g \neq 0$.*

(1) *If $m = 2t + 1$ is odd, then $\frac{f}{g} = \frac{p_n}{q_n}$ for some convergent $\frac{p_n}{q_n}$ of $\sqrt{d}$.*

(2) *If $m = 2t$ is even, then there exists a divisor h of the polynomial d with the following properties*:

(i) $1 \leq \deg h \leq \frac{\deg d - 1}{2}$;

(ii) *the equation*

$$\frac{d}{h}g_1^2 - hf_1^2 = b\nu^t, \quad (18)$$

where $b \in k^*$, has a solution in polynomials $f_1, g_1 \in k[\nu]$, and $\frac{f_1}{g_1} = \frac{p_n}{q_n}$ for some convergent $\frac{p_n}{q_n}$ of $\frac{\sqrt{d}}{h}$. Conversely, if $f_1, g_1 \in k[\nu]$ are a solution of (18), *then the polynomials f and g defined by $f = \frac{1}{2}\left(hf_1^2 + \frac{d}{g}g_1^2\right)$ and $g = f_1g_1$ are a solution of Eq.* (17).

Proof. (1) Let us write (17) in the form $(f - g\sqrt{d})(f + g\sqrt{d}) = a\nu^{2t+1}$. Comparing the degrees of polynomials on the left- and right-hand sides of (17), we obtain $\deg f \leq t$ and $\deg g = \frac{2t + 1 - \deg d}{2} < t$. By virtue of Proposition 1 from [5], we can assume that $|f + g\sqrt{d}| = 0$

and $|f - g\sqrt{d}| = 2t + 1$. Suppose that $f = b_0 + b_1\nu + \ldots + b_r\nu^r$ and $g = c_0 + c_1\nu + \ldots + c_s\nu^s$, where $r, s \le t$; $b_i, c_i \in k$; $b_r \ne 0$; and $c_s \ne 0$. Let $h = \max\{r, s\}$. Consider the element $\bar{f} - \bar{g}\sqrt{d}$, where $\bar{f} = \dfrac{f}{\nu^h} = b_0\nu^{-h} + \ldots + b_r\nu^{r-h}$ and $\bar{g} = \dfrac{g}{\nu^h} = c_0\nu^{-h} + \ldots + c_s\nu^{s-h}$. Since $\dfrac{\bar{f}}{\bar{g}}$ has the form (8) and $|\bar{f} - \bar{g}\sqrt{d}| = 2t + 1 - t = t + 1 > -|\bar{g}| = t$, it follows from Proposition 1 that the fraction $\dfrac{\bar{f}}{\bar{g}} = \dfrac{f}{g}$ is a best approximation to $\sqrt{d}$. By Theorem 1, we have $\dfrac{f}{g} = \dfrac{p_n}{q_n}$ for some convergent $\dfrac{p_n}{q_n}$ of $\sqrt{d}$.

(2) Since a in (17) must be a square, we can divide both sides by a and assume without loss of generality that f, g is a solution of the valuation equation $f^2 - g^2 d = \nu^2$. This implies

$$(f - \nu^t)(f + \nu^t) = g^2 d. \tag{19}$$

Let $d = d_1 d_2 \ldots d_r$ be the irreducible decomposition of d. Then, each polynomial d_i divides precisely one of the factors $f - \nu^t$ or $f + \nu^t$ (otherwise, $d_i = c\nu^t$, $c \in k^*$ and, therefore, ν divides d, which is false).

Let h_1 be the product of those d_i which divide $f - \nu^t$, and let h_2 be the product of those d_i which divide $f + \nu^t$. Then, $h_1 h_2 = d$ and $(h_1, h_2) = 1$. Suppose for definiteness that $\deg h_1 < \deg h_2$, i.e., $\deg h_1 \le \dfrac{\deg d - 1}{2}$. Let us write

$$f - \nu^t = h_1 u_1, \quad f + \nu^t = h_2 u_2, \tag{20}$$

where $u_1, u_2 \in k[\nu]$. It follows from (20) that

$$f = \frac{1}{2}(h_1 u_1 + h_2 u_2), \quad \nu^t = \frac{1}{2}(h_2 u_2 - h_1 u_1). \tag{21}$$

Substituting (20) into (19), we obtain $u_1 u_2 = g^2$. Note that $(u_1, u_2) = 1$ (otherwise, f and g cannot be coprime). Thus, $u_1 = f_1^2$ and $u_2 = g_1^2$, whence

$$f = \frac{1}{2}(h_1 f_1^2 + h_2 g_1^2), \quad g = f_1 g_1. \tag{22}$$

It follows from (21) and (22) that

$$2\nu^t = \frac{d}{h_1} g_1^2 - h_1 f_1^2. \tag{23}$$

Thus, Eq. (17) has a solution in polynomials $f, g \in k[\nu]$ if and only if Eq. (23) has a solution in polynomials $f_1, g_1 \in k[\nu]$ for some divisor h_1 of d with $\deg h_1 \le \dfrac{\deg d - 1}{2}$. Consider Eq. (23) in more detail. Let us write it in the form

$$h_1\left(\frac{\sqrt{d}}{h_1} g_1 - f_1\right)\left(\frac{\sqrt{d}}{h_1} g_1 + f_1\right) = 2\nu^t. \tag{24}$$

Since $|h_1| = 0$ and $|\sqrt{d}| = 0$, it follows from Proposition 1 in [5] that we can assume that $\left|\dfrac{\sqrt{d}}{h_1} g_1 + f_1\right| = 0$ and $\left|\dfrac{\sqrt{d}}{h_1} g_1 - f_1\right| = t$. Comparing the degrees on the left- and right-hand sides of (23), we obtain $\deg g_1 \le \deg f_1 < \dfrac{t}{2}$. Suppose that $\deg f_1 = s$ and

$$f_1 = b_0 + b_1\nu + \ldots + b_s\nu^s,$$
$$g_1 = c_0 + c_1\nu + \ldots + c_r\nu^r,$$

where $r \le s < \dfrac{t}{2}$; $b_i, c_i \in k$; $b_s \ne 0$; and $c_r \ne 0$. Consider the element $\dfrac{\sqrt{d}}{h_1}\bar{g}_1 - \bar{f}_1$, where $\bar{f}_1 = \dfrac{f_1}{\nu^s}$ and $\bar{g}_1 = \dfrac{g_1}{\nu^s}$. Since $\dfrac{\bar{f}_1}{\bar{g}_1}$ has the form (8) and $\left|\dfrac{\sqrt{d}}{h_1}\bar{g}_1 - \bar{f}_1\right| = t - s > s = |\bar{g}_1|$, it follows from Proposition 1 that the fraction $\dfrac{\bar{f}_1}{\bar{g}_1} = \dfrac{f_1}{g_1}$ is a best approximation to $\dfrac{\sqrt{d}}{h_1}$. By Theorem 1, $\dfrac{f_1}{g_1} = \dfrac{p_n}{q_n}$ for some convergent $\dfrac{p_n}{q_n}$ of $\dfrac{\sqrt{d}}{h_1}$. Moreover, f and g are related to f_1 and g_1 by (22), as required.

The following proposition refines Theorem 2 in the case of an irreducible polynomial d.

Proposition 5. *Suppose that the polynomial d is irreducible and* $\deg\nu \ge 1$. *Then, the minimum positive integer m for which the valuation equation* (17) *has a solution in polynomials $f, g \in k[x]$, where $g \ne 0$, is odd. Thus, in calculating the fundamental S-unit in the case of* $\deg\nu = 1$, *assertion* (1) *of Theorem* 2 *holds.*

Proof. Suppose that $m = 2t$. Let us write Eq. (17) in the form (19). Since d is irreducible, it follows that it divides one of the factors on the left-hand side of (19). Suppose that, e.g., $f - \nu^t = df_1$. Then, $f = \nu^t + df_1$. Substituting this expression into (19), we obtain

$$f_1(2\nu^t + df_1) = g^2, \tag{25}$$

which implies that f_1 divides g^2. Therefore, the polynomials g and f_1 can be represented in the forms $g = f_2 h g_2$ and $f_1 = f_2^2 h$ for some $f_2, g_2, h \in k[x]$. Substituting g and f_1 into (25), we obtain

$$2\nu^t + d f_2^2 h = g_2^2 h. \quad (26)$$

It follows from (26) that h divides ν^t and, therefore, $h = b\nu^r$ for some $b \in k^*$. As a result, we conclude that the valuation equation $g_2^2 - f_2^2 d = 2b^{-1}\nu^{t-r}$ has a solution in polynomials $f_2, g_2 \in k[x]$ and $t - r < 2t$, which contradicts the minimality of m. This completes the proof of Proposition 5.

Note that Theorem 2 is invalid in the case of $\deg\nu > 1$. Consider again the above example. Using the method for calculating fundamental S-units developed in [5], we see that the minimum positive integer m for which the valuation equation (17) has a solution in polynomials $f, g \in k[\nu]$ equals 5, and

$$f = 1 - 2x\nu - x\nu^2, \quad g = x.$$

Moreover, $f^2 - g^2 d = \nu^5$. The polynomial d in the example under consideration is irreducible. It is easy to show that $\frac{f}{g} \neq \frac{p_1}{q_1}$ and $\frac{f}{g} \neq \frac{p_2}{q_2}$. Hence, $\frac{f}{g}$ cannot coincide with any convergent $\frac{p_n}{q_n}$ of $\sqrt{d}$ for $n > 2$, because the degree of the denominator is always higher than 1. Taking into account Proposition 5, we see that Theorem 2 in invalid in the case under consideration. Thus, in the general situation, the method for calculating S-units suggested in [5] is more effective than that of continued fractions.

Theorem 2 suggests an algorithm for calculating the fundamental S-unit in the case of $\deg\nu = 1$. Let d_1, d_2, …, d_r be all divisors of d of degree $\leq \frac{\deg d - 1}{2}$. We successively calculate the convergents of $\sqrt{d}$, $\frac{\sqrt{d}}{d_1}$, …, $\frac{\sqrt{d}}{d_r}$, and for each convergent $\frac{p_n}{q_n}$ verify equality (18). As soon as a convergent $\frac{p_n}{q_n}$ satisfying (18) is found, we obtain a solution f, g of the valuation equation (17) by formulas (22). Then either $f + g\sqrt{d}$ or $f - g\sqrt{d}$ is the fundamental S-unit.

REFERENCES

1. E. Artin, Math. Z. **19**, 153–246 (1924).
2. W. W. Adams and M. J. Razar, Proc. Math. Soc. London **41** (3), 481–498 (1980).
3. A. Weil, *Basic Number Theory* (Springer, Heidelberg, 1967; Mir, Moscow, 1972).
4. Z. I. Borevich and I. R. Shafarevich, *Number Theory* (Nauka, Moscow, 1964) [in Russian].
5. V. V. Benyash-Krivets and V. P. Platonov, Dokl. Math. **76**, 886–890 (2007) [Dokl. Akad. Nauk **417** (4), 446–450 (2007)].
6. V. V. Benyash-Krivets and V. P. Platonov, Usp. Mat. Nauk **63** (2), 159–160 (2008).