# Continued fractions and $S$-units in hyperelliptic fields



2008 Russ. Math. Surv. 63 357

(http://iopscience.iop.org/0036-0279/63/2/L06)

*Russian Math. Surveys* **63**:2 357–396 

*Uspekhi Mat. Nauk* **63**:2 157–184

COMMUNICATIONS OF THE MOSCOW MATHEMATICAL SOCIETY

# Continued fractions and $S$-units in hyperelliptic fields

V. V. Benyash-Krivets and V. P. Platonov

The aim of this note is twofold: to present some results about continued fractions in function fields and to show how continued fractions can be used 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 a polynomial $v = x - a$, denote by $|\cdot| = |\cdot|_v$ the valuation corresponding to $v$. The completion of $k(x)$ with respect to the valuation $v$ can be identified with the field $k((v))$ of formal power series. The extension of $|\cdot|$ to $k((v))$ is denoted by $|\cdot|$ as before.

Continued fractions in function fields for the case of the valuation $|\cdot|_\infty$ were first introduced by E. Artin [1]. Here we consider the case of the valuation $|\cdot|_v$. For an element $\beta = \sum_{i=-s}^{\infty} d_i v^i \in k((v))$ we define $[\beta] = \sum_{i=-s}^{0} d_i v^i \in k[v^{-1}]$. Let $a_0 = [\beta]$. If $\beta - a_0 \neq 0$, then let $\beta_1 = 1/(\beta - a_0) \in k((v))$ and $a_1 = [\beta_1]$. The elements $a_i$ and $\beta_i$ are defined inductively: if $\beta_{i-1} - a_{i-1} \neq 0$, then $\beta_i = 1/(\beta_{i-1} - a_{i-1})$ and $a_i = [\beta_i]$. This process terminates if and only if $\beta \in k(v)$. We use the standard abbreviated notation $\beta = [a_0; a_1, a_2, \dots]$ for the continued fraction.

We define elements $p_i, q_i \in k[v^{-1}]$ by induction. Let $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, and $q_{-1} = 0$; for $n \geqslant 0$ let $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$. Then $p_n, q_n \in k[v^{-1}]$ and $p_n/q_n = [a_0; a_1, \dots, a_n]$ for $n \geqslant 0$. For $n \geqslant -1$, the following relations hold:

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

The fraction $p_n/q_n$ is called the $n$th convergent of $\beta$. It is not difficult to show that

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \beta.$$

By construction, $|a_n| = |\beta_n| < 0$. The following relations are easily derived from (1) by induction:

$$|q_n| = \sum_{j=1}^{n} |a_j|, \qquad |q_n\beta - p_n| = -|q_{n+1}| > -|q_n|. \tag{2}$$

Let us introduce a notion of best approximation. A fraction $p/q$ with $p, q \in k[v^{-1}]$ and $q \neq 0$ is a *best approximation* of $\beta$ if $|\beta - p/q| > |\beta - a/b|$ for any other fraction $a/b$ with $a, b \in k[v^{-1}]$ and $b \neq 0$ such that $a/b \neq p/q$ in $k(v)$ and $|b| \geqslant |q|$.

**Proposition 1.** *A reduced rational fraction $p/q$ with $p, q \in k[v^{-1}]$ and $q \neq 0$ is a best approximation of $\beta$ if and only if $|\beta - p/q| > -2|q|$ (equivalently, $|q\beta - p| > -|q|$).*

Proposition 1 and the relations (2) immediately imply that the $n$th convergent $p_n/q_n$ of $\beta$ is a best approximation of $\beta$. The following theorem asserts that the converse is true as well.

---

*AMS* 2000 *Mathematics Subject Classification.* Primary 11A55; Secondary 12E20.

DOI 10.1070/RM2008v063n02ABEH004519.

**Theorem 1.** *If $a/b$ is a best approximation of $\beta$, then there exist a convergent $p_n/q_n$ of $\beta$ and a constant $c \in k^*$ such that $a = cp_n$ and $b = cq_n$.*

One can show in a standard way that if the continued fraction $[a_0; a_1, a_2, \dots]$ for $\beta$ is periodic, then $\beta$ is a quadratic irrationality. In the case of an infinite field $k$, the converse of this statement does not always hold [2]. In what follows we assume that $k = \mathbb{F}_q$ is a field with $q$ elements and that the characteristic of $k$ is not equal to 2. We have the following result.

**Proposition 2.** *If $\beta \in k((v))$ is a quadratic irrationality, then the continued fraction for $\beta$ is periodic.*

We show below how continued fractions can be used to find fundamental $S$-units in hyperelliptic fields. Let $d(x) = b_0x^{2n+1} + b_1x^{2n} + \dots + b_{2n+1} \in k[x]$, where $b_0 \neq 0$, be a square-free polynomial, and let $K = k(x)(\sqrt{d})$. Assume that our valuation $|\cdot| = |\cdot|_v$ has two extensions $|\cdot|_1$ and $|\cdot|_2$ to $K$. The valuation $|\cdot|_\infty$ has a unique extension to $K$. Let $S = \{|\cdot|_\infty, |\cdot|_1\}$, let $\mathcal{O}_S$ be the ring of $S$-integers in $K$, and let $U_S = \mathcal{O}_S^*$ be the group of $S$-units of the field $K$. It is known that the group $U_S$ is the direct product of the group $k^*$ and a free Abelian group $G$ of rank 1. A generator of the group $G$ is called a fundamental $S$-unit.

An effective algorithm for computing a fundamental $S$-unit was found in [3]. In the classical case of a quadratic extension $L = \mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, one can find a fundamental unit of $L$ using the continued fraction expansion of $\sqrt{d}$ or $(\sqrt{d}-1)/2$. Our aim is to show that also in the case of a hyperelliptic field $K$ one can find a fundamental $S$-unit using the continued fraction method. It is proved in [3] that to compute a fundamental $S$-unit it is necessary to find the minimal positive integer $m$ such that the norm equation

$$f^2 - g^2 d = av^m, \tag{3}$$

where $a \in k^*$, is soluble in polynomials $f, g \in k[v]$ with $g \neq 0$. Then either $f + g\sqrt{d}$ or $f - g\sqrt{d}$ is a fundamental $S$-unit. The following theorem provides an algorithm for determining a fundamental $S$-unit by means of continued fractions.

**Theorem 2.** *Let $m$ be the minimal positive integer such that the norm equation (3) is soluble in polynomials $f, g \in k[v]$ with $g \neq 0$.*

1. *If $m$ is odd, then $f/g = p_n/q_n$ for some convergent $p_n/q_n$ of $\sqrt{d}$.*

2. *If $m = 2t$ is even, then there exists a divisor $h$ of the polynomial $d$ with the following properties*: i) $1 \leqslant \deg h \leqslant (\deg d - 1)/2$; ii) *the equation*

$$hf_1^2 - \frac{d}{h}g_1^2 = bv^t, \tag{4}$$

*where $b \in k^*$, is soluble in polynomials $f_1, g_1 \in k[v]$, and $f_1/g_1 = p_n/q_n$ for some convergent $p_n/q_n$ of $\sqrt{d}/h$. Conversely, if $f_1, g_1 \in k[x]$ is a solution of (4), then the polynomials $f$ and $g$ defined by $f = hf_1^2 + (d/h)g_1^2$ and $g = 2f_1g_1$ are solutions of the norm equation (3).*

## Bibliography


[1] E. Artin, *Math. Z.* **19**:1 (1924), 153–206.

[2] W. W. Adams and M. J. Razar, *Proc. London Math. Soc.* (3) **41**:3 (1980), 481–498.

[3] В. В. Беняш-Кривец, В. П. Платонов, *Докл. РАН* **417**:4 (2007), 446–450; English transl., V. V. Benyash-Krivets and V. P. Platonov, *Dokl. Math.* **76**:3 (2007), 886–890.

**V. V. Benyash-Krivets**
Belarusian State University
*E-mail*: benyash@bsu.by

Presented by D. V. Anosov
Accepted 12/FEB/08
Translated by THE AUTHORS

**V. P. Platonov**
Scientific Research Institute for Systems Analysis,
Russian Academy of Sciences
*E-mail*: platonov@niisi.ras.ru