*ДОКЛАДЫ АКАДЕМИИ НАУК, 2008, том 423, № 2, с. 155–160*

**МАТЕМАТИКА**

*УДК 511.24*

# НЕПРЕРЫВНЫЕ ДРОБИ И *S*-ЕДИНИЦЫ В ФУНКЦИОНАЛЬНЫХ ПОЛЯХ

**© 2008 г. В. В. Беняш-Кривец, академик В. П. Платонов**

Поступило 17.07.2008 г.

В настоящей статье мы преследуем двойную цель: изложить некоторые результаты исследования непрерывных дробей в функциональных полях и показать, как непрерывные дроби могут быть использованы для нахождения фундаментальных *S*-единиц в гиперэллиптических полях.

Пусть $k$ – произвольное поле, $k(x)$ – поле рациональных функций от одной переменной над $k$. Для неприводимого многочлена $\nu \in k[x]$ через $|\cdot| = |\cdot|_\nu$ будем обозначать нормирование, соответствующее $\nu$, через $O_\nu = \{z \in k(x) | |z| \geq 0\}$ – соответствующее кольцо нормирования, через $p_\nu = \{z \in k(x) | |z| > 0\}$ – идеал нормирования $|\cdot|$. Тогда поле вычетов $O_\nu/p_\nu$ совпадает с $k[x]/(\nu)$ и является конечным расширением $k$. Пусть $k(x)_\nu$ – пополнение поля $k(x)$ относительно нормирования $|\cdot|$. Продолжение нормирования $|\cdot|$ на $k(x)_\nu$ по-прежнему будем обозначать через $|\cdot|$. Выберем в $k[x]$ фиксированную систему $\Sigma$ представителей смежных классов по идеалу $(\nu)$, состоящую из всех многочленов степени меньше $\deg\nu$. Тогда каждый элемент $z \in k(x)_\nu$ единственным образом можно представить в виде формального степенного ряда $z = \sum_{i=s}^{\infty} a_i \nu^i$, где $s \in \mathbf{Z}$, а $a_i \in \Sigma$. Если $\deg\nu = 1$, то поле $k(x)_\nu$ можно отождествить с полем формальных степенных рядов $k((\nu))$.

Непрерывные дроби в функциональных полях в случае нормирования $|\cdot|_\infty$ были впервые введены Э. Артином [1]. Мы рассматриваем общий случай произвольного нормирования $|\cdot| = |\cdot|_\nu$. Пусть $\beta \in k(x)_\nu$. Представим $\beta$ в виде формального степенного ряда $\beta = \sum_{i=s}^{\infty} d_i \nu^i$, где $d_i \in \Sigma$, и положим $[\beta] = \sum_{i=s}^{0} d_i \nu^i$, если $s \leq 0$, и $[\beta] = 0$ в случае $s > 0$. Пусть $a_0 = [\beta]$. Если $\beta - a_0 \neq 0$, то положим $\beta_1 = \frac{1}{\beta - a_0} \in k(x)_\nu$, $a_1 = [\beta_1]$. Далее по индукции определяем элементы $a_i$, $\beta_i$: если $\beta_{i-1} - a_{i-1} \neq 0$, то $\beta_i = \frac{1}{\beta_{i-1} - a_{i-1}} \in k(x)_\nu$, $a_i = [\beta_i]$. Нетрудно показать, что этот процесс оборвется тогда и только тогда, когда $\beta \in k(x)$. Будем использовать стандартную сокращенную запись для непрерывной дроби $\beta = [a_0, a_1, a_2, \ldots]$. По построению, $\beta_n = [a_n, a_{n+1}, \ldots]$.

Определим по индукции элементы $p_i, q_i \in k(x)$. Положим $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$ и если $n \geq 0$, то

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

Тогда $\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$ при $n \geq 0$. Стандартным образом можно показать, что для $n \geq -1$ справедливы соотношения

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

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

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

Дробь $\frac{p_n}{q_n}$ назовем $n$-й подходящей дробью к $\beta$. По построению, $|a_n| = |\beta_n| < 0$ для $n \geq 1$. Из (1) по индукции легко получить соотношение

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

а из (3) получаем

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

или, что эквивалентно,

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

*Белорусский государственный университет, Минск*

*Научно-исследовательский институт системных исследований Российской Академии наук, Москва*

Значит, $\lim\limits_{n\to\infty}\frac{p_n}{q_n} = \beta$. Введем понятие наилучшего приближения к $\beta$. Если $\frac{a}{b} \in k(x)$, где $a, b \in k[x]$ – взаимно простые многочлены, то разложим $a$ и $b$ по степеням $\nu$: $a = a_0 + a_1\nu + \ldots + a_s\nu^s$, $b = b_0 + b_1\nu + \ldots + b_t\nu^t$, где $a_i, b_i \in \Sigma$, $a_s \neq 0$, $b_t \neq 0$. Тогда, разделив $a$ и $b$ на $\nu^r$, где $r = \max\{s, t\}$, представим дробь $\frac{a}{b}$ в виде

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

где $c_i, d_i \in \Sigma$, $c_{-p} \neq 0$, $d_{-q} \neq 0$, $c_0$ и $d_0$ одновременно не равны нулю. Будем в дальнейшем предполагать, что все элементы из $k(x)$ записаны в виде (8).

Определение. Несократимая дробь $\frac{p}{q} \in k(x)$ является наилучшим приближением к $\beta$, если для любой другой несократимой дроби $\frac{a}{b} \neq \frac{p}{q}$, такой, что $|b| \geq |q|$, справедливо неравенство $\left|\beta - \frac{p}{q}\right| > \left|\beta - \frac{a}{b}\right|$ (или, что эквивалентно, $|q\beta - p| > |b\beta - a|$).

Предложение 1. *Дробь $\frac{p}{q}$ является наилучшим приближением к $\beta$ тогда и только тогда, когда $\left|\beta - \frac{p}{q}\right| > -2|q|$ (или $|q\beta - p| > -|q|$).*

Доказательство. Запишем элементы $p$, $q$, $\beta$, $q\beta$ в виде формальных степенных рядов от $\nu$

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

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

где $a_i, b_i, c_i, d_i \in \Sigma$, $a_{-r} \neq 0$, $b_{-s} \neq 0$. Пусть $n = \deg\nu$. Тогда

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

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

где $a_{ij}, b_{ij}, c_{ij}, d_{ij} \in k$. При этом $d_{ij} = L_{ij}(b_{00}, \ldots, b_{-s,n-1})$, где $L_{ij}$ – линейная форма от $n(s+1)$ переменной с коэффициентами из поля $k$. Допустим, что $|q\beta - p| = l \leq -|q| = s$. Из определения наилучшего приближения следует, что $l > 0$. Тогда мы должны иметь $|p| = |q| + |\beta|$, т.е. $r = s - m$. Поскольку $q\beta - p = \sum\limits_{i=-r}^{0}(d_i - a_i)\nu^i + \sum\limits_{i=1}^{\infty} d_i\nu^i$, получаем

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

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

Из (10) следует, что

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

Таким образом, набор элементов $(b_{00}, \ldots, b_{-s,n-1})$ является решением системы линейных однородных уравнений

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

где $Y = (y_{00}, \ldots, y_{-s,n-1})^t$, $C$ – матрица с коэффициентами из поля $k$, содержащая $n(s+1)$ столбцов и $n(l-1)$ строк. Поскольку по нашему предположению $l \leq s$, то $\operatorname{rank} C \leq n(l-1)$ и при решении (12) получаем $m$ свободных переменных $z_1, z_2, \ldots, z_m$, где

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

При этом остальные переменные $y_{ij}$ выражаются через свободные в виде

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

для некоторой линейной формы $H_{ij}$. Поскольку $b_{-s} \neq 0$, то (12) имеет такое решение $(b_{00}, \ldots, b_{-s,n-1})$, что не все из чисел $b_{-s,0}, \ldots, b_{-s,n-1}$ равны нулю. Это означает, что не все линейные формы $H_{ij}$ тождественно равны нулю.

Рассмотрим систему линейных однородных уравнений

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

которая имеет $m \geq 2n$ неизвестных и $n$ уравнений. В силу этого (14) имеет ненулевое решение $(z_1^0, z_2^0, \ldots, z_m^0)$. Теперь по формулам (13) находим $y_{ij}^0 = H_{ij}(z_1^0, z_2^0, \ldots, z_m^0)$ и получаем многочлены $b_i^0 = \sum\limits_{j=0}^{n-1} y_{ij}^0 x^j$, $i = -s, -s+1, \ldots, 0$. При этом $b_{-s}^0 = 0$ по построению. В результате получаем элемент $q_1 = \sum\limits_{i=-s+1}^{0} b_i^0\nu^i$. Затем с помощью (9) находим $p_1$. По построению имеем $|q_1| > |q|$ и $|q_1\beta - p_1| \geq l = |q\beta - p|$. Ясно, что $\frac{p}{q} \neq \frac{p_1}{q_1}$, и мы получили проти-

воречие с тем, что $\frac{p}{q}$ – наилучшее приближение. Предложение 1 доказано.

Предложение 2. *Если дроби* $\frac{a}{b}$ *и* $\frac{c}{d}$ *– такие наилучшие приближения к* $\beta$, *что* $|b| = |d|$, *то найдется константа* $h \in k^*$, *такая, что* $a = hc$, $b = hd$.

Доказательство. Если $\frac{a}{b} \neq \frac{c}{d}$ в $k(x)$, то имеем по определению наилучшего приближения два противоположных неравенства $\left|\beta - \frac{a}{b}\right| > \left|\beta - \frac{c}{d}\right|$ и $\left|\beta - \frac{a}{b}\right| < \left|\beta - \frac{c}{d}\right|$ – противоречие. Значит, $\frac{a}{b} = \frac{c}{d}$ в $k(x)$. Учитывая несократимость этих дробей, получаем требуемое утверждение.

Предложение 3. *Пусть* $\deg\nu = 1$. *Тогда n-я подходящая дробь* $\frac{p_n}{q_n}$ *к* $\beta$ *является наилучшим приближением к* $\beta$.

Доказательство. Элементы $p_n$, $q_n$ имеют вид

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

где $c_i, d_i \in k$. Следовательно, $\frac{p_n}{q_n}$ имеет вид (8). Теперь предложение 1 и выражение (6) немедленно влекут, что $\frac{p_n}{q_n}$ является наилучшим приближением к $\beta$.

Следующая теорема показывает, что справедливо и обратное утверждение.

Теорема 1. *Пусть* $\deg\nu = 1$. *Если дробь* $\frac{a}{b}$ *является наилучшим приближением к* $\beta$, *то найдется такая подходящая дробь* $\frac{p_n}{q_n}$ *к* $\beta$ *и такая константа* $c \in k^*$, *что* $a = cp_n$, $b = cq_n$.

Доказательство. Вначале докажем, что $|b| = |q_n|$ для некоторой подходящей дроби $\frac{p_n}{q_n}$. Допустим противное. Поскольку $|q_0| = |1| = 0$, $|q_n| < |q_{n-1}|$ в силу (5) и $|b| \le 0$, то найдется такое $n$, что $|q_{n+1}| < |b| < |q_n|$. Поскольку $\frac{p_{n+1}}{q_{n+1}}$ – наилучшее приближение к $\beta$ и $|b| > |q_{n+1}|$, то $\left|\frac{p_{n+1}}{q_{n+1}} - \beta\right| > \left|\beta - \frac{a}{b}\right|$. Тогда имеем

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

Следовательно, $\left|\beta - \frac{a}{b}\right| \le \left|\frac{1}{bq_{n+1}}\right| = -|b| - |q_{n+1}|$. Используя (6), получаем $|b\beta - a| \le -|q_{n+1}| = |q_n\beta - p_n|$. Поскольку $|q_n| > |b|$, то мы получили противоречие с тем, что $\frac{a}{b}$ – наилучшее приближение к $\beta$. Итак, для некоторого $n$ мы имеем $|q_n| = |b|$. Применяя предложение 2, завершаем доказательство теоремы.

В случае $\deg\nu > 1$ подходящая дробь $\frac{p_n}{q_n}$ не обязательно является наилучшим приближением к $\beta$.

Пример. Пусть $k = F_3$, $\nu = x^2 + 1 \in k[x]$ и $d = x^3 + 2x^2 + x + 1 = (x + 2)\nu + 2 \in k[x]$ – неприводимый многочлен. Поскольку 2 является квадратом в поле вычетов $k(x)/(\nu)$, то $\sqrt{d} \in k(x)_\nu$ и элемент $\sqrt{d}$ можно представить в виде ряда

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

Разлагая $\sqrt{d}$ в непрерывную дробь, получаем

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

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

Тогда подходящие дроби к $\sqrt{d}$ имеют вид

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

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

Покажем, что $\frac{p_2}{q_2}$ не является наилучшим приближением к $\sqrt{d}$. В силу (7) $\left|\sqrt{d} - \frac{p_2}{q_2}\right| = -|a_3| - 2|q_2| = 5$. С другой стороны, для того чтобы записать подходящую дробь $\frac{p_2}{q_2}$ в виде (8), нужно числитель и знаменатель разделить на $\nu$: $\frac{p_2}{q_2} = \frac{\tilde{p}_2}{\tilde{q}_2} = \frac{(x - 1)\nu^{-3} + x\nu^{-2} + (x + 2)\nu^{-1} + 1}{(x + 1)\nu^{-3} + (2x + 1)\nu^{-2} + x\nu^{-1}}$. Тогда мы имеем $\left|\sqrt{d} - \frac{\tilde{p}_2}{\tilde{q}_2}\right| = \left|\sqrt{d} - \frac{p_2}{q_2}\right| = 5 < -2|\tilde{q}_2| = 6$. В силу

предложения 1 дробь $\frac{p_2}{q_2}$ не является наилучшим приближением к $\sqrt{d}$.

Стандартным образом можно показать, что если непрерывная дробь $[a_0, a_1, \ldots]$ для $\beta$ является периодической, то $\beta$ – квадратичная иррациональность. В случае бесконечного поля $k$ и нормирования $|\cdot|_\infty$ обратное утверждение верно не всегда (см. [2]). Справедливо

Предложение 4. *Пусть $k = F_q$ – поле из $q$ элементов и $\deg\nu = 1$. Отождествим пополнение $k(x)_\nu$ с полем формальных степенных рядов $k((\nu))$. Если $\beta \in k((\nu))$ – квадратичная иррациональность, то непрерывная дробь для $\beta$ периодична.*

Доказательство. Пусть $\beta \in k((\nu))$ является корнем квадратного многочлена $H(X) = rX^2 + sX + t$, где $r, s, t \in k[\nu]$, и $\beta = [a_0, a_1, \ldots]$ – разложение $\beta$ в непрерывную дробь. Положим $D = s^2 - 4rt \in k[\nu]\setminus k$, $H(X, Y) = rX^2 + sXY + tY^2$. Тогда из (3) получаем

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

где $A_n = (-1)^{n+1}H(p_n, q_n)$, $B_n = (-1)^n(rp_{n-1}p_n + sp_{n-1}q_n + tq_{n-1}q_n)$. Ясно, что для достаточно большого $n$ имеем $\left|\frac{p_n}{q_n} - \beta\right| > |\beta - \bar{\beta}|$, где $\bar{\beta}$ – второй корень $H(X)$. Тогда $\left|\frac{p_n}{q_n} - \bar{\beta}\right| = \left|\frac{p_n}{q_n} - \beta + \beta - \bar{\beta}\right| = |\beta - \bar{\beta}|$. Так как $\beta - \bar{\beta} = \frac{2\sqrt{D}}{r}$, то $|\beta - \bar{\beta}| = \frac{1}{2}|D| - |r|$. Отсюда получаем $|p_n - \bar{\beta}\, q_n| = |q_n| + \frac{1}{2}|D| - |r|$. Поскольку $H(X, Y) = r(X - \beta Y)(X - \bar{\beta}\, Y)$, то в итоге имеем

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

Найдем нижнюю оценку для $|B_n|$. Из (15) находим $B_n = A_n\beta_{n+1} - r\beta$. Из равенства $\beta(r\beta + s) = -t$ следует, что $|r\beta| \geq 0$. Учитывая (16), находим $|A_n\beta_{n+1}| = |A_n a_{n+1}| = \frac{1}{2}|D| \geq 0$. Значит, $|B_n| \geq \geq \min\{|A_n\beta_{n+1}|, |r\beta|\} \geq 0$.

Таким образом, $A_n$, $B_n$ являются многочленами из $k[x]$. Их степени не превосходят $\max(\deg r, \deg s, \deg t)$. Поскольку поле $k$ конечно, таких многочленов конечное число. Это означает, что для некоторых $i$ и $j$ мы должны иметь $A_i = A_{i+j}$, $B_i = B_{i+j}$. Тогда $\beta_i = \beta_{i+j}$ и непрерывная дробь для $\beta$ периодична.

Отметим, что в случае $\deg\nu > 1$ приведенное выше рассуждение перестает быть справедливым. Хотя $A_n$, $B_n$ по-прежнему будут многочленами из $k[x]$, мы не можем утверждать, что их степени ограничены сверху числом $\max(\deg r, \deg s, \deg t)$. Если взять $\beta = \sqrt{d}$ из рассмотренного выше примера, то тогда $r = 1$, $s = 0$, $t = d$, $A_2 = p_2^2 - dq_2^2 = = 2x(x^2 + 1)(x^2 + x + 2)$ и $\deg A_2 > \deg d$.

Далее мы покажем, как непрерывные дроби в случае $\deg\nu = 1$ и конечного поля $k$ могут быть использованы для нахождения фундаментальных $S$-единиц в гиперэллиптических полях. В дальнейшем будем предполагать, что $k = F_q$ – конечное поле характеристики $p > 2$ и $d(x) = c_0x^{2n+1} + + c_1x^{2n} + \ldots + c_{2n+1}$ – свободный от квадратов многочлен, $c_0 \neq 0$. Пусть $K = k(x)(\sqrt{d})$, $\nu = x - b$, $\bar{x}$ – образ $x$ в поле вычетов $O_\nu/p_\nu$. Будем предполагать, что $d(\bar{x}) = \beta^2$ для некоторого $0 \neq \beta \in O_\nu/p_\nu$ (это означает, что точка $(\beta, \bar{x})$ является $O_\nu/p_\nu$-точкой гиперэллиптической кривой $y^2 = d(x)$). Тогда нормирование $|\cdot|_\nu$ имеет два неэквивалентных продолжения на поле $K$. Эти нормирования будем обозначать $|\cdot|_{\nu'}$ и $|\cdot|_{\nu''}$. Неархимедово нормирование $|\cdot|_\infty$ имеет единственное продолжение на $K$ и мы также будем обозначать его через $|\cdot|_\infty$. Пусть $S = \{|\cdot|_\infty, |\cdot|_{\nu'}\}$, $O_S$ – кольцо $S$-целых элементов в $K$, т.е. таких элементов $z \in K$, что $|z|_\nu \geq 0$ для всех нормирований $|\cdot|_\nu$ поля $K$, не принадлежащих $S$. Множество обратимых элементов $U_S$ кольца $O_S$ называется группой $S$-единиц поля $K$. В силу обобщенной теоремы Дирихле о единицах (см. [3, гл. IV, теорема 9]) группа $U_S$ является прямым произведением группы $k^*$ и свободной абелевой группы $G$ ранга 1. Образующая группы $G$ называется фундаментальной $S$-единицей.

В [5] найден эффективный алгоритм для вычисления фундаментальной $S$-единицы. В классическом случае квадратичного расширения $L = Q(\sqrt{d})$ поля $Q$ фундаментальную единицу поля $L$ можно найти, используя разложение $\sqrt{d}$ либо $\frac{\sqrt{d} - 1}{2}$ в непрерывную дробь (см. [4]). Наша цель – показать, что и в случае гиперэллиптического поля $K$ и нормирования $|\cdot|_\nu$, определяемого линейным многочленом $\nu$, фундаментальную $S$-единицу можно найти, используя метод непрерывных дробей. В [5] доказано, что для вычисления фундаментальной $S$-единицы нужно найти минимальное натуральное $m$, такое, что норменное уравнение

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

где $a \in k^*$, имеет решение в многочленах $f, g \in \in k[\nu]$, $g \neq 0$. Тогда либо $f + g\sqrt{d}$, либо $f - g\sqrt{d}$ является фундаментальной $S$-единицей. В силу минимальности $m$ имеем, что $(f, g) = 1$ и $\nu$ не делит $f$ и $g$. Следующая теорема (см. также [6]) дает алго-

ритм для нахождения фундаментальной $S$-единицы с помощью непрерывных дробей.

Т е о р е м а 2. *Пусть $m$ – такое минимальное натуральное число, что уравнение* (17) *имеет решение в многочленах $f, g \in k[\nu]$, $g \neq 0$.*

1. *Если $m = 2t + 1$ нечетно, то $\frac{f}{g} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\sqrt{d}$.*

2. *Если $m = 2t$ четно, то найдется делитель $h$ многочлена $d$, обладающий следующими свойствами*:

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

(ii) *уравнение*

$$\frac{d}{h} g_1^2 - h f_1^2 = b\nu^t, \tag{18}$$

*где $b \in k^*$, имеет решение в многочленах $f_1, g_1 \in k[\nu]$, при этом $\frac{f_1}{g_1} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\frac{\sqrt{d}}{h}$. Наоборот, если $f_1, g_1 \in k[\nu]$ – решение* (18), *то многочлены $f$ и $g$, определяемые по формулам $f = \frac{1}{2}\left( h f_1^2 + \frac{d}{g} g_1^2 \right)$, $g = f_1 g_1$, являются решением уравнения* (17).

Д о к а з а т е л ь с т в о. 1. Запишем (17) в виде $(f - g\sqrt{d})(f + g\sqrt{d}) = a\nu^{2t+1}$. Сравнивая степени многочленов в левой и правой части (17), находим $\deg f \le t$, $\deg g = \frac{2t + 1 - \deg d}{2} < t$. В силу предложения 1 из [5] можно считать, что $|f + g\sqrt{d}| = 0$, $|f - g\sqrt{d}| = 2t + 1$. Пусть $f = b_0 + b_1\nu + \ldots + b_r\nu^r$, $g = c_0 + c_1\nu + \ldots + c_s\nu^s$, где $r, s \le t$, $b_i, c_i \in k$, $b_r \neq 0$, $c_s \neq 0$. Пусть $h = \max\{r, s\}$. Рассмотрим элемент $\bar{f} - \bar{g}\sqrt{d}$, где $\bar{f} = \frac{f}{\nu^h} = b_0\nu^{-h} + \ldots + b_r\nu^{r-h}$, $\bar{g} = \frac{g}{\nu^h} = c_0\nu^{-h} + \ldots + c_s\nu^{s-h}$. Поскольку $\frac{\bar{f}}{\bar{g}}$ имеет вид (8) и $|\bar{f} - \bar{g}\sqrt{d}| = 2t + 1 - t = t + 1 > -|\bar{g}| = t$, то по предложению 1 дробь $\frac{\bar{f}}{\bar{g}} = \frac{f}{g}$ является наилучшим приближением к $\sqrt{d}$. По теореме 1 $\frac{f}{g} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\sqrt{d}$.

2. Поскольку $a$ в (17) должно быть квадратом, то, разделив обе части на $a$, без ограничения общности можно считать, что $f$, $g$ – решения норменного уравнения $f^2 - g^2 d = \nu^2$. Отсюда получаем

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

Пусть $d = d_1 d_2 \ldots d_r$ – разложение $d$ на неприводимые множители. Тогда каждый многочлен $d_i$ делит ровно один из множителей $f - \nu^t$ или $f + \nu^t$ (в противном случае $d_i = c\nu^t$, $c \in k^*$ и, следовательно, $\nu$ делит $d$, а это не так).

Пусть $h_1$ – произведение тех $d_i$, которые делят $f - \nu^t$, а $h_2$ – произведение тех $d_i$, которые делят $f + \nu^t$. Тогда $h_1 h_2 = d$, $(h_1, h_2) = 1$. Пусть для определенности $\deg h_1 < \deg h_2$, т.е. $\deg h_1 \le \frac{\deg d - 1}{2}$. Запишем

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

где $u_1, u_2 \in k[\nu]$. Из (20) получаем

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

Подставляя (20) в (19), получаем $u_1 u_2 = g^2$. Заметим, что $(u_1, u_2) = 1$ (в противном случае $f$ и $g$ не были бы взаимно простыми). Тогда $u_1 = f_1^2$, $u_2 = g_1^2$. Таким образом,

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

Из (21), (22) получаем

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

Таким образом, уравнение (17) имеет решение в многочленах $f, g \in k[\nu]$ тогда и только тогда, когда уравнение (23) имеет решение в многочленах $f_1, g_1 \in k[\nu]$ для некоторого делителя $h_1$ многочлена $d$, такого, что $\deg h_1 \le \frac{\det d - 1}{2}$. Рассмотрим подробнее уравнение (23). Запишем его в виде

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

Поскольку $|h_1| = 0$, $|\sqrt{d}| = 0$, то в силу предложения 1 из [5] можно считать, что $\left|\frac{\sqrt{d}}{h_1} g_1 + f_1\right| = 0$, $\left|\frac{\sqrt{d}}{h_1} g_1 - f_1\right| = t$. Сравнивая степени в левой и правой частях (23), получаем $\deg g_1 \le \deg f_1 < \frac{t}{2}$. Пусть $\deg f_1 = s$

$$f_1 = b_0 + b_1\nu + \ldots + b_s\nu^s,$$

$$g_1 = c_0 + c_1\nu + \ldots + c_r\nu^r,$$

где $r \le s < \frac{t}{2}$, $b_i, c_i \in k$, $b_s \ne 0$, $c_r \ne 0$. Рассмотрим элемент $\frac{\sqrt{d}}{h_1}\bar{g}_1 - \bar{f}_1$, где $\bar{f}_1 = \frac{f_1}{\nu^s}$, $\bar{g}_1 = \frac{g_1}{\nu^s}$. Поскольку $\frac{\bar{f}_1}{\bar{g}_1}$ имеет вид (8) и $\left|\frac{\sqrt{d}}{h_1}\bar{g}_1 - \bar{f}_1\right| = t - s > s = |\bar{g}_1|$, то по предложению 1 дробь $\frac{\bar{f}_1}{\bar{g}_1} = \frac{f_1}{g_1}$ является наилучшим приближением к $\frac{\sqrt{d}}{h_1}$. В силу теоремы 1 $\frac{f_1}{g_1} = \frac{p_n}{q_n}$ для некоторой подходящей дроби $\frac{p_n}{q_n}$ к $\frac{\sqrt{d}}{h_1}$. При этом $f, g$ связаны с $f_1, g_1$ формулами (22), что и требовалось доказать.

Следующее предложение уточняет теорему 2 для случая неприводимого многочлена $d$.

Предложение 5. *Предположим, что многочлен $d$ неприводим*, $\deg\nu \ge 1$. *Тогда наименьшее натуральное $m$, для которого норменное уравнение* (17) *имеет решение в многочленах $f, g \in k[x]$, $g \ne 0$, является числом нечетным. Таким образом, при вычислении фундаментальной $S$-единицы в случае* $\deg\nu = 1$ *справедлив пункт* 1 *теоремы* 2.

Доказательство. Предположим, что $m = 2t$. Запишем уравнение (17) в виде (19). Поскольку $d$ неприводим, то он делит один из множителей в левой части (19). Пусть, например, $f - \nu^t = df_1$. Тогда $f = \nu^t + df_1$. Подставляя это выражение в (19), получаем

$$f_1(2\nu^t + df_1) = g^2, \qquad (25)$$

откуда следует, что $f_1$ делит $g^2$. Следовательно, многочлены $g$ и $f_1$ можно представить в виде $g = f_2 h g_2, f_1 = f_2^2 h$ для некоторых $f_2, g_2, h \in k[x]$. Подставляя $g$ и $f_1$ в (25), получаем

$$2\nu^t + df_2^2 h = g_2^2 h. \qquad (26)$$

Из (26) следует, что $h$ делит $\nu^t$ и поэтому $h = b\nu^r$ для некоторого $b \in k^*$. В результате получаем, что норменное уравнение $g_2^2 - f_2^2 d = 2b^{-1}\nu^{t-r}$ имеет решение в многочленах $f_2, g_2 \in k[x]$ и $t - r < 2t$, что противоречит минимальности $m$. Предложение 5 доказано.

Отметим, что теорема 2 становится неверной в случае $\deg\nu > 1$. Вернемся к рассмотренному выше примеру. Используя разработанный в [5] метод вычисления фундаментальных $S$-единиц, находим, что наименьшее натуральное $m$, для которого норменное уравнение (17) имеет решение в многочленах $f, g \in k[\nu]$, равно 5 и

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

При этом $f^2 - g^2 d = \nu^5$. Многочлен $d$ в нашем примере неприводим. Легко проверить, что $\frac{f}{g} \ne \frac{p_1}{q_1}$ и $\frac{f}{g} \ne \frac{p_2}{q_2}$. Тем более $\frac{f}{g}$ не совпадает ни с одной подходящей дробью $\frac{p_n}{q_n}$ к $\sqrt{d}$ для $n > 2$, поскольку степень знаменателя всегда будет больше 1. Учитывая предложение 5, мы видим, что теорема 2 неприменима в рассматриваемом случае. Таким образом, предложенный в [5] метод вычисления $S$-единиц в общей ситуации является более эффективным, нежели метод непрерывных дробей.

Теорема 2 дает алгоритм для вычисления фундаментальной $S$-единицы в случае $\deg\nu = 1$. Пусть $d_1, d_2, \ldots, d_r$ – все делители $d$ степени $\le \frac{\deg d - 1}{2}$. Будем последовательно вычислять подходящие дроби к $\sqrt{d}$, $\frac{\sqrt{d}}{d_1}, \ldots, \frac{\sqrt{d}}{d_r}$ и для каждой подходящей дроби $\frac{p_n}{q_n}$ проверять, выполняется ли равенство (18). Как только найдем подходящую дробь $\frac{p_n}{q_n}$, удовлетворяющую (18), по формулам (22) находим решение $f, g$ норменного уравнения (17). Тогда либо $f + g\sqrt{d}$, либо $f - g\sqrt{d}$ будет фундаментальной $S$-единицей.

## СПИСОК ЛИТЕРАТУРЫ


1. *Artin E.* // Math. Z. 1924. V. 19. P. 153–246.
2. *Adams W.W., Razar M.J.* // Proc. London Math. Soc. 1980. V. 41. № 3. P. 481–498.
3. *Вейль А.* Основы теории чисел. М.: Мир, 1972. 408 с.
4. *Боревич З.И., Шафаревич И.Р.* Теория чисел. М.: Наука, 1964. 566 с.
5. *Беняш-Кривец В.В., Платонов В.П.* // ДАН. 2007. Т. 417. № 4. С. 446–450.
6. *Беняш-Кривец В.В., Платонов В.П.* // УМН. 2008. Т. 63. № 2. С. 159–160.