КЛАССИФИКАЦИЯ ТЕРНАРНЫХ КВАЗИКАНОНИЧЕСКИХ СИСТЕМ СЧИСЛЕНИЯ В МНИМЫХ КВАДРАТИЧНЫХ ПОЛЯХ И ИХ ПРИЛОЖЕНИЕ

Богданов П.С., Чернов В.М.
Институт систем обработки изображений РАН

Аннотация

В работе рассматриваются все возможные тернарные квазиканонические системы счисления в мнимых квадратичных полях. Для представления целых алгебраических чисел мнимых квадратичных полей в указанных системах счисления используется алгоритм, основанный на делении с остатком. Кроме того, синтезируются алгоритмы реализации основных арифметических операций над числами в тернарных системах счисления кольца целых чисел Эйзенштейна. Рассматривается метод быстрого безошибочного вычисления дискретной циклической свёртки.

Ключевые слова: каноническая система счисления, деление с остатком по норме, квазиканоническая система счисления, мнимые квадратичные поля.

Введение

Целью настоящей работы является классификация одного класса троичных систем счисления в мнимых квадратичных полях. Актуальность работы определяется двумя факторами.

Во-первых, троичные системы счисления не часто, но всё же использовались в приложениях, например, в докомпьютерную эру Д.И. Менделеев интересовался тернарной уравновешенной системой счисления и на её основе разработал цифровой ряд значений весов разновеса для взвешивания на лабораторных весах, который используется по сей день [1, 2]. Позднее Джоном Фон Нейманом [3] было показано, что именно троичная система счисления наиболее экономична. В данном случае под экономичностью понимается возможность представления как можно большего диапазона чисел с использованием как можно меньшего общего количества состояний триггеров, составляющих регистры, которые и описывают представления чисел в некоторой системе счисления. Развитие же «экономичной» троичной вычислительной техники тормозилось в основном технологическими причинами.

В наше время, несмотря на скептическое высказывание Д. Кнута [4] относительно перспектив применения так называемой троичной уравновешенной системы счисления (то есть позиционной системы счисления с основанием 3 и цифрами $\{-1, 0, 1\}$), эта система всё же применяется, например, при создании электронных устройств, что объясняется тем, что умножение в такой системе счисления производится без переносов, а в таблице сложения переносы в старшие разряды присутствуют лишь в двух случаях.

Во-вторых, в работах И. Катаи и Б. Ковача [5, 6] введено понятие канонических систем счисления, экстраполирующее теорию систем счисления на случай квадратичных полей. Следует отметить, что И. Катаи, Б. Ковач и их последователи рассматривают только тот случай, когда конечное множество цифр состоит из целых рациональных чисел. В работах [5, 6, 7] ими получены классификационные теоремы для канонических систем счисления во всех квадратичных полях. Кроме того, Ковачем [8] найдены эффективные рекуррентные алгоритмы вычисления цифр представления элементов в канонических системах счисления.

В данной работе мы классифицируем тернарные системы счисления в мнимых квадратичных расширениях, предполагая, что цифрами в них являются целые квадратичные элементы. Такие системы счисления в статье называются квазиканоническими. В отличие от цитируемой работы [8] для нахождения цифр представления элементов в квазиканонических системах счисления синтезируются алгоритмы, основанные на алгоритме деления с остатком в некоторых квадратичных кольцах.

Основные определения

Определение 1. Пусть $Q(\sqrt{d})$ есть квадратичное поле [9]:

$$Q(\sqrt{d}) = \left\{ z = a + b\sqrt{d};\ a, b \in Q \right\},$$

где d – целое число, свободное от квадратов. При $d > 0$ квадратичное поле называется вещественным, а при $d < 0$ – мнимым.

Если норма $Norm(z) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$ элемента $z = a + b\sqrt{d} \in Q(\sqrt{d})$ и его след $Tr(z) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$ есть целые числа, то этот элемент называется целым алгебраическим числом поля $Q(\sqrt{d})$ [10].

Хорошо известно [9], что целые алгебраические числа мнимого поля $Q\left(i\sqrt{\Delta}\right)$, где $d < 0$, $\Delta = |d|$, имеют вид

$$z = \begin{cases} a + bi\sqrt{\Delta}; & a, b \in Z \text{ при } \Delta \equiv -2, -3 \pmod 4; \\ \dfrac{a + bi\sqrt{\Delta}}{2}; & a, b \in Z,\ a \equiv b \pmod 2 \text{ при} \\ & \Delta \equiv -1 \pmod 4. \end{cases}$$

Кольцо целых элементов поля $Q\left(\sqrt{d}\right)$ будем обозначать $S\left(\sqrt{d}\right)$.

Определение 2. Целое алгебраическое число $\alpha = A \pm \sqrt{d}$ (при $d \equiv 2, 3 \pmod 4$) или $\alpha = \frac{1}{2}\left(B \pm \sqrt{d}\right)$ (при $d \equiv 1 \pmod 4$) называется основанием канонической системы счисления (КСС) в кольце $S\left(\sqrt{d}\right)$ целых

элементов поля $Q(\sqrt{d})$, если любой целый элемент этого поля однозначно представим в форме конечной суммы

$$z=\sum_{j=0}^{k(z)} a_j\alpha^j,$$

$$a_j\in I=\{0,1,...,|Norm(\alpha)|-1\}.$$

Пара $\{\alpha;I\}$ называется канонической системой счисления (КСС) в кольце $S(\sqrt{d})$, а I – алфавитом этой системы [10].

В работах [8] для представления целого алгебраического числа в таких системах применяется рекуррентный алгоритм. Однако с той же целью можно использовать и деление с остатком, реализуемое лишь в некоторых кольцах [11]. В настоящей работе рассматриваются только мнимые кольца.

Определение 3. Говорят, что в кольце D имеет место алгоритм деления с остатком, если на отличных от нуля элементах $\beta\in D$ определена функция $\|\beta\|$, принимающая целые неотрицательные значения, так, что выполняются следующие условия:

1) если $\beta\neq 0$ делится на α, то $\|\beta\|\geq\|\alpha\|$;

2) для любых элементов β и $\alpha\neq 0$ в D существуют такие γ и r, что $\beta=\alpha\gamma+r$, причём либо $r=0$, либо $\|r\|<\|\alpha\|$.

Утверждение. Среди колец $S(\sqrt{d})$ целых элементов мнимых квадратичных полей $Q(\sqrt{d})$ алгоритмом деления с остатком по норме обладают те и только те, для которых d равно одному из следующих пяти значений: $\{-1,\ -2,\ -3,\ -7,\ -11\}$ [9].

Стоит отметить, что числа γ и r в равенстве $\beta=\alpha\gamma+r$ определяются неоднозначно, поскольку существует несколько различных остатков r, имеющих одну и ту же норму. Это позволяет рассматривать различные системы счисления с одним и тем же основанием α, но разными алфавитами (множествами цифр).

Если в качестве элементов множества I рассматривать не целые рациональные (обычные целые), а целые алгебраические числа, то можно получить целый класс систем счисления. Например, в поле $Q(i\sqrt{3})$ в качестве цифр можно рассматривать числа $0,\frac{1+i\sqrt{3}}{2},\frac{-1+i\sqrt{3}}{2}$, а в качестве основания – $\frac{-3+i\sqrt{3}}{2}$.

Определение 4. Целое алгебраическое число α называется основанием квазиканонической системы счисления в кольце $S(\sqrt{d})$ целых элементов поля $Q(\sqrt{d})$, если любой целый элемент этого поля представим в форме конечной суммы

$$z=\sum_{j=0}^{k(z)} a_j\alpha^j,\ a_j\in I,$$

где множество I состоит из целых алгебраических чисел, по норме меньших нормы основания α.

Пара $\{\alpha;I\}$ называется квазиканонической системой счисления в кольце $S(\sqrt{d})$, а I – алфавитом этой системы.

Тернарные квазиканонические системы счисления

Определение 5. Квазиканоническая система счисления с основанием α и алфавитом I называется тернарной системой счисления в поле $Q(\sqrt{d})$, если $Norm(\alpha)=3$ и алфавит I состоит из трёх цифр.

В табл. 1 указаны числа z, имеющие нормы 1, 2 и 3 в мнимых квадратичных полях, для которых существует алгоритм деления с остатком.

Таблица 1. Числа с нормами 1, 2 и 3 в полях $Q(i),Q(i\sqrt{2}),Q(i\sqrt{3}),Q(i\sqrt{7}),Q(i\sqrt{11})$

$\|z\|$ / d	1	2	3
-1	$\pm1;\pm i$	$\pm1\pm i$	нет
-2	±1	$\pm i\sqrt{2}$	$\pm1\pm i\sqrt{2}$
-3	$\pm1;\ \frac{\pm1\pm i\sqrt{3}}{2}$	нет	$\pm i\sqrt{3};\ \frac{\pm3\pm i\sqrt{3}}{2}$
-7	±1	$\frac{\pm1\pm i\sqrt{7}}{2}$	нет
-11	±1	нет	$\frac{\pm1\pm i\sqrt{11}}{2}$

Из этой таблицы следует, что тернарные квазиканонические системы счисления могут существовать только при $d=-2,-3,-11$.

Используя табл. 1, можно легко получить возможные комбинации оснований систем счисления и множества остатков.

Сформулируем в виде лемм ряд свойств, справедливых для любых тернарных квазиканонических систем счисления.

Лемма 1. Если $Norm(\alpha)=3$, то равенство $\beta=\alpha\gamma+r$ равносильно равенству

$$\gamma=\frac{(\beta-r)\bar{\alpha}}{3},\qquad(1)$$

где $\bar{\alpha}$ – число, сопряжённое α.

Лемма 2. Если для пары $\{\alpha;I\}$ доказано, что представление произвольного целого алгебраическо-

го числа γ_0 в форме $\gamma_0 = \gamma_1\alpha + r_0$ единственно, где $r_0 \in I$, то для того, чтобы пара $\{\alpha; I\}$ образовывала систему счисления, достаточно, чтобы представление числа γ_0 являлось конечным, то есть процесс деления с остатком:

$$\begin{aligned} &\gamma_0 = \gamma_1 \cdot \alpha + r_0, \\ &\gamma_1 = \gamma_2 \cdot \alpha + r_1, \\ &\ldots\ldots\ldots\ldots\ldots, \\ &\gamma_l = \gamma_{l+1} \cdot \alpha + r_l, \end{aligned} \qquad (2)$$

где $r_0, r_1, \ldots, r_l \in I$, был конечен. Другими словами, существует такое l, что $\gamma_{l+1} = 0$, а для этого, в свою очередь, достаточно, чтобы $Norm(\gamma_{m+1}) < Norm(\gamma_m)$ $\forall m = 0, 1, ..., l$.

Определение 6. Системы счисления $\{\alpha; I\}$ и $\{\alpha'; I'\}$ в кольце $S(\sqrt{d})$ называются эквивалентными, если существует взаимно однозначное отображение $f : S(\sqrt{d}) \to S(\sqrt{d})$, причём $f(I) = I'$, такое, что для любого числа $\gamma \in S(\sqrt{d})$, представимого в системе счисления $\{\alpha; I\}$ в виде $\gamma = \sum_{p=0}^{N} a_p \alpha^p$, где $a_p \in I$, число $f(\gamma)$ в системе счисления $\{\alpha'; I'\}$ записывается в виде $f(\gamma) = \sum_{p=0}^{N} f(a_p)(\alpha')^p$. Стоит отметить, что α' не обязательно равно $f(\alpha)$.

Лемма 3. Если r – первообразный корень из единицы степени, равной количеству чисел с единичной нормой (единиц поля) в кольце $S(\sqrt{d})$, то системы счисления $\{\alpha; I\}$ и $\{\alpha; I \cdot r^k\}$ эквивалентны, где $k = 0, 1, 2, \ldots$.

Доказательство. Действительно, если для γ_0, представимого в системе счисления $\{\alpha; I\}$, справедливо равенство $\gamma_0 = \gamma_1\alpha + r_0$, то, умножая это равенство на r^k, получим, что число $\gamma_0 r^k$ имеет такую же запись в системе счисления $\{\alpha; I \cdot r^k\}$, как и γ_0 в системе счисления $\{\alpha, I\}$, то есть если $\gamma_0 = \sum_{p=0}^{N} a_p \alpha^p$, то $\gamma_0 r^k = \sum_{p=0}^{N} (a_p r^k)\alpha^p$. Это означает, что системы счисления $\{\alpha; I\}$ и $\{\alpha; I \cdot r^k\}$ эквивалентны.

Лемма 4. Если $\bar{\alpha}$ – число комплексно-сопряжённое числу α, а $\bar{I}$ состоит из чисел комплексно-сопряжённых числам из I, то системы счисления $\{\alpha; I\}$ и $\{\bar{\alpha}; \bar{I}\}$ эквивалентны.

Доказательство. Действительно, если взять сопряжение от обеих частей равенства $\gamma_0 = \gamma_1\alpha + r_0$, то получим $\overline{\gamma_0} = \overline{\gamma_1}\overline{\alpha} + \overline{r_0}$, то есть число $\overline{\gamma_0}$ имеет такую же запись в системе счисления $\{\bar{\alpha}; \bar{I}\}$, как и число γ_0 в системе счисления $\{\alpha; I\}$. Следовательно, системы счисления $\{\alpha; I\}$ и $\{\bar{\alpha}; \bar{I}\}$ эквивалентны.

Замечание 1. Очевидно, что если f – функция, переводящая систему счисления $\{\alpha; I\}$ в эквивалентную ей систему $\{\alpha'; I'\}$, то алгоритм сложения двух чисел $f(\gamma)$ и $f(\beta)$ в системе счисления $\{\alpha'; I'\}$ легко получается из алгоритма сложения чисел γ и β в системе счисления $\{\alpha; I\}$. То же самое можно сказать и об инверсии знака.

Замечание 2. Если функция f задаётся равенством $f(\gamma) = \bar{\gamma}$, где $\bar{\gamma}$ – число, сопряжённое γ, то алгоритм умножения двух чисел $\bar{\gamma}$ и $\bar{\beta}$ в системе счисления $\{\bar{\alpha}; \bar{I}\}$ также легко получается из алгоритма умножения чисел γ и β в системе счисления $\{\alpha; I\}$. Если же функция f отличается от указанной выше, то алгоритм умножения в системе счисления $\{\alpha'; I'\}$ если и может быть получен из алгоритма умножения в системе счисления $\{\alpha; I\}$, то только нетривиальным образом.

Тернарные квазиканонические системы счисления в $S(i\sqrt{3})$

Элементы кольца целых чисел Эйзенштейна, то есть кольца $S(i\sqrt{3})$, представимы в виде

$$z = \frac{a + bi\sqrt{3}}{2}; \quad a, b \in Z; a \equiv b (\mathrm{mod} 2).$$

Так как в кольце $S(i\sqrt{3})$ нет элементов, норма которых равна двум, то при делении с остатком по норме на α норма ненулевого остатка может равняться только единице. Таких остатков довольно много: $\{\frac{1}{2}(\pm 1 \pm i\sqrt{3}), \pm 1\}$, что в сочетании с вариантами выбора α: $\{\frac{1}{2}(\pm 3 \pm i\sqrt{3}), \pm\sqrt{3}\}$ даёт $1/2 \times 6 \times (6-1) \times 6 = 90$ потенциальных комбинаций возможных оснований α и множеств I, то есть тернарных квазиканонических систем счисления. Заметим, что в алгоритме деления с остатком по норме однозначно определяется не сам остаток, а только его норма. И, следовательно, при достаточно широком выборе элементов с одинаковой нормой возникает проблема выбора таких остатков, т. е. «цифр», при котором последовательное деление с ос-

татком на основание α приведёт к получению конечного представления элемента именно в тернарной системе. Требование конечности представления чисел в системах счисления существенно ограничивает выбор α и *I*, что описывается следующей основной теоремой.

Теорема 1. В кольце целых алгебраических чисел $S(i\sqrt{3})$ существуют ровно 24 тернарные квазиканонические системы счисления, а именно: системы счисления с основаниями $\alpha_k = (i\sqrt{3})\omega^{k-1}$ и множествами цифр

$\{0,1,\omega\}, \{0,\omega,\omega^2\}, \{0,\omega^2,\omega^3\},$

$\{0,\omega^3,\omega^4\}, \{0,\omega^4,\omega^5\}, \{0,\omega^5,\omega^6\};$

где $\omega = 1/2(1+i\sqrt{3})$ и $k = 1,2,3,4$.

Доказательству теоремы предпошлём ряд лемм.

Лемма 5. Пусть $\alpha \in S\left(i\sqrt{3}\right)$ является основанием тернарной системы счисления, для которой множество цифр I выбирается из чисел $r \in S\left(i\sqrt{3}\right)$, причём $\|r\| < \|\alpha\| = 3$. Тогда $I = \left\{0, \omega^a, \omega^b\right\}$, где $\omega = 1/2(1+i\sqrt{3})$, $a,b = 1,2,3,4,5,6$ и $b \equiv a+1 \pmod 6$ или $b \equiv a+3 \pmod 6$.

Доказательство. Пусть $\beta = \dfrac{a_0 + b_0 i\sqrt{3}}{2}$, $a_0 \equiv b_0 \pmod 2$; $r = \dfrac{r_1 + r_2 i\sqrt{3}}{2}$, $r_1 \equiv r_2 \pmod 2$ и $\alpha = \dfrac{c + di\sqrt{3}}{2}$, $c \equiv d \pmod 2$, $a_0, b_0, c, d, r_1, r_2 \in Z$. Подставляя выражения для β, α и *r* в формулу (1), имеем

$$\gamma = \frac{ca_0 - 3db_0 + 3dr_2 - cr_1}{6} + \frac{a_0 d - r_1 d + cb_0 - cr_2}{6} i\sqrt{3}. \quad (3)$$

Поскольку γ – целое алгебраическое число поля $Q(i)$, то $\mathrm{Re}\,\gamma$ и $\mathrm{Im}\,\gamma$ должны быть целыми рациональными числами. Учитывая, что $c \equiv 0 \pmod 3$, а также условия сравнимости $a_0 \equiv b_0 \pmod 2$; $r_1 \equiv r_2 \pmod 2$; $c \equiv d \pmod 2$, получаем, что $\mathrm{Re}\,\gamma \in Z$, а числитель $\mathrm{Im}\,\gamma$ делится на 2. Далее несложно заметить, что $cb_0 - cr_2$ делится на 3. Таким образом, получаем $\mathrm{Im}\,\gamma \in Z \Leftrightarrow a_0 \equiv r_1 \pmod 3$. При этом условии легко убедиться в том, что $\mathrm{Im}\,\gamma - \mathrm{Re}\,\gamma \equiv 0 \pmod 2$, то есть $\mathrm{Im}\,\gamma \equiv \mathrm{Re}\,\gamma \pmod 2$.

Поскольку a_0 – любое целое рациональное число, то из доказанного следует, что для однозначности представления (1) необходимо и достаточно, чтобы множество остатков состояло ровно из трёх чисел, для каждого из которых выполняется только одно из следующих условий: $r_1 \equiv 0 \pmod 3$; $r_1 \equiv 1 \pmod 3$; $r_1 \equiv 2 \pmod 3$. В этом случае для каждого целого алгебраического числа β однозначно определяется *r* и по формуле (3) однозначно вычисляется γ.

Так как остатки *r*, кроме *r*=0, являются числами единичной нормы, то они могут быть записаны в виде ω^a и ω^b. Найдём теперь соотношения между *a* и *b*. Для этого переберём все 6 чисел с нормой, равной 1, и выясним, у каких из них $r_1 \equiv 1 \pmod 3$, а у каких – $r_1 \equiv 2 \pmod 3$. Несложно убедиться, что $r_1 \equiv 1 \pmod 3$ для $\omega^1, \omega^3, \omega^5$, а $r_1 \equiv 2 \pmod 3$ – для всех остальных. Следовательно, все возможные системы остатков могут быть представлены в виде $I = \left\{0, \omega^a, \omega^b\right\}$, где $a,b = 1,2,3,4,5,6$ и $b \equiv a+1 \pmod 6$ или $b \equiv a+3 \pmod 6$.

Таким образом, показано, что в системах счисления $\{\alpha_n; I\}$ возможно однозначное представление произвольного целого алгебраического числа из поля $Q\left(i\sqrt{3}\right)$.

Рассмотрим теперь конечность представления чисел в таких системах счисления, опираясь на лемму 2.

Лемма 6. В равенствах (2) найдётся такой элемент *l*, при котором $Norm(\gamma_{l+1}) \le 1$.

Доказательство. Выясним, для каких систем остатков условие $Norm\left(\gamma_{m+1}\right) < Norm\left(\gamma_m\right)$ $\forall m = 0,1,...,l$ выполняется для каждого целого алгебраического числа γ_m.

Пусть $\gamma_m = \dfrac{a_m + b_m i\sqrt{3}}{2}$, $r_m = \dfrac{r_{m1} + r_{m2} i\sqrt{3}}{2}$, $a_m, b_m, r_{m1}, r_{m2} \in Z$. Согласно формулам (2)

$$Norm\left(\gamma_{m+1}\right) = \frac{(\gamma_m - r_m)\overline{\alpha}}{3} \cdot \frac{\overline{(\gamma_m - r_m)\overline{\alpha}}}{3} = \frac{Norm\left(\gamma_m - r_m\right)}{3}.$$

Подставляя последнее выражение в неравенство $Norm\left(\gamma_{m+1}\right) < \dfrac{a_m^2 + 3b_m^2}{4}$, после преобразований получаем

$$\frac{\left(a_m + \frac{r_{m1}}{2}\right)^2}{3} + \left(b_m + \frac{r_{m2}}{2}\right)^2 > \frac{r_{m1}^2 + 3r_{m2}^2}{4}, \quad (4)$$

где $\dfrac{r_{m1}^2 + 3r_{m2}^2}{4} = Norm\left(r_m\right)$.

Если $r_m = 0$, то очевидно, что (4) выполняется для любого $\gamma_m \ne 0$.

Если $r_m \ne 0$, то $Norm(r_m) = 1$ и неравенство (4) принимает вид

$$\frac{\left(a_m + \frac{r_{m1}}{2}\right)^2}{3} + \left(b_m + \frac{r_{m2}}{2}\right)^2 > 1. \quad (5)$$

Таким образом, условие $Norm(\gamma_{m+1}) < Norm(\gamma_m)$ выполняется для всех целых a_m и b_m ($a_m \equiv b_m \pmod 2$), за исключением тех, которые удовлетворяют неравенству

$$\frac{\left(a_m + \frac{r_{m1}}{2}\right)^2}{3} + \left(b_m + \frac{r_{m2}}{2}\right)^2 \le 1. \qquad (6)$$

Такие a_m и b_m будем называть исключительными и исследуем их отдельно.

Введём следующие обозначения

$(-A) = \omega = \frac{1+i\sqrt{3}}{2}$; $(-B) = \omega^2 = \frac{1-i\sqrt{3}}{2}$. Тогда

$A = \omega^4 = \frac{-1-i\sqrt{3}}{2}$; $B = \omega^5 = \frac{-1+i\sqrt{3}}{2}$.

Далее, учитывая леммы 3 и 4, легко получить, что достаточно исследовать вместо 54 лишь 6 систем счисления, а именно:

$$\left\{\frac{3+i\sqrt{3}}{2};\{0,-1,B\}\right\},\ \left\{\frac{-3+i\sqrt{3}}{2};\{0,-1,B\}\right\},$$

$$\left\{i\sqrt{3};\{0,-1,B\}\right\},\ \left\{\frac{3+i\sqrt{3}}{2};\{0,1,-1\}\right\},$$

$$\left\{\frac{-3+i\sqrt{3}}{2};\{0,1,-1\}\right\},\ \left\{i\sqrt{3};\{0,1,-1\}\right\}.$$

В этих системах счисления неравенство (4) выполняется для всех γ_m, кроме конечного числа исключительных случаев. Результаты исследования исключительных случаев для шести приведённых систем счисления представлены в табл. 2.

Таблица 2. Представление чисел, удовлетворяющих неравенству (6) в исследуемых системах счисления

алфавит / α	$\{0,-1,1\}$	$\{0,-1,B\}$
$\frac{3+i\sqrt{3}}{2}$	$B = B\alpha + 1$	$-B = -B\alpha - 1$
$\frac{-3+i\sqrt{3}}{2}$	$A = A\alpha^2 - \alpha + 1$	$1 = -\alpha + B$, $-B = -\alpha - 1$, $A = B\alpha + B$, $-A = B\alpha^2 + B\alpha - 1$
$-i\sqrt{3}$	$A = A\alpha^4 + \alpha^3 -$ $-\alpha^2 - \alpha + 1$	$1 = B\alpha^2 - \alpha + B$, $-B = B\alpha^2 - \alpha - 1$, $A = B\alpha^3 - \alpha^2 + B\alpha + B$, $-A = B\alpha - 1$

Числа, приведённые в табл. 2, удовлетворяют неравенству (6), но при этом норма каждого такого числа равна 1, что и доказывает справедливость леммы 6.

Итак, найдётся такое значение $l = q$, при котором $Norm(\gamma_{q+1}) = 0$, следовательно, $\gamma_{q+1} = 0$, либо $Norm(\gamma_{q+1}) = 1$, то есть $\gamma_{q+1} = \omega^k$, где $k = 1,2,3,4,5,6$. Для всех этих значений γ_{q+1} в системах счисления $\left\{\frac{-3+i\sqrt{3}}{2};\{0,-1,B\}\right\}$ и $\left\{i\sqrt{3};\{0,-1,B\}\right\}$, легко проверить, используя табл. 2, что через конечное число шагов процесса деления с остатком появится частное $\gamma_p = 0$. То же самое справедливо и для всех систем счисления, эквивалентных двум вышеназванным. В системах счисления $\left\{\frac{3+i\sqrt{3}}{2};\{0,-1,B\}\right\}$, $\left\{\frac{3+i\sqrt{3}}{2};\{0,1,-1\}\right\}$, $\left\{\frac{-3+i\sqrt{3}}{2};\{0,1,-1\}\right\}$, $\left\{i\sqrt{3};\{0,1,-1\}\right\}$ при последовательном применении алгоритма деления с остатком возможно зацикливание. Поэтому в последних четырёх системах счисления и всех эквивалентных им не любое целое алгебраическое число допускает конечное представление. Примеры чисел с бесконечным представлением приведены в табл. 2.

Таким образом, в поле $Q\left(i\sqrt{3}\right)$ существует лишь 24 системы счисления, в которых представление целых алгебраических чисел этого поля единственно и конечно.

Из доказанного легко получается алгоритм записи целого числа Эйзенштейна $\gamma_0 = \frac{a_0 + b_0 i\sqrt{3}}{2}$; $a_0, b_0 \in Z$, $a_0 \equiv b_0 \pmod 2$, в системе счисления с основанием $\alpha = i\sqrt{3}\omega^k$ и алфавитом $I_k = \left\{0, \omega^t, \omega^{t+1}\right\}$, где $k = 1,2,3,4$ и $t = 0,1,2,3,4,5$.

Алгоритм 1.

Шаг 1. Полагаем $p = 0$.

Шаг 2. Если для $\gamma_p = \frac{a_p + b_p i\sqrt{3}}{2}$ $a_p \equiv 0 \pmod 3$, то $r_p = 0$.

Если $a_p \equiv 1 \pmod 3$, то $r_p = \omega^t$, где $t = 1,3,5$.

Если $a_p \equiv 2 \pmod 3$, то $r_p = \omega^t$, где $t = 0,2,4$.

Шаг 3. Вычисляем γ_{p+1} по формуле $\gamma_{p+1} = \frac{(\gamma_p - r_p)\overline{\alpha}}{3}$.

Если $\gamma_{p+1} = 0$, то алгоритм закончен.

Если $\gamma_{p+1} \ne 0$, то $p = p+1$ и переходим к шагу 2.

Сходимость данного алгоритма следует из доказательства теоремы 1.

Тернарные квазиканонические системы счисления в $S\left(i\sqrt{2}\right)$ *и* $S\left(i\sqrt{11}\right)$

Приведённый выше метод исследования обобщается и на случай колец $S(i\sqrt{2})$ и $S(i\sqrt{11})$.

Заметим, что в $S(i\sqrt{2})$ и $S(i\sqrt{11})$, наряду с троичными каноническими системами счисления, существуют и тернарные квазиканонические системы счисления, которые описываются следующими теоремами.

Теорема 2. В кольце целых алгебраических чисел $S(i\sqrt{2})$ существуют ровно 4 тернарные квазиканонические системы счисления, а именно: системы счисления с основаниями $\alpha = \pm 1 \pm i\sqrt{2}$ и множеством цифр $I = \{0,1,-1\}$.

Теорема 3. В кольце целых алгебраических чисел $S(i\sqrt{11})$ существуют ровно 4 тернарные квазиканонические системы счисления, а именно: системы счисления с основаниями $\alpha = (\pm 1 \pm i\sqrt{11})/2$ и множеством цифр $I = \{0,1,-1\}$.

Реализация арифметических операций

Рассмотрим теперь арифметические операции в системах счисления, указанных в теореме 1. Сложность вычислений и основные отличия арифметики в этих системах счисления определяются в основном сложностью «правил переноса в старший разряд» при сложении/умножении цифр. Эти правила достаточно просты. Например, таблицы 3–16 являются таблицами Кэли для сложения и умножения при

$$\alpha_k = -i\sqrt{3} \text{ и } \alpha_k = \frac{-1+i\sqrt{3}}{2}.$$

Таблица 3. Таблица Кэли для сложения в системе счисления $\left\{-i\sqrt{3};\{0,1,\omega\}\right\}$

+	0	ω	1
0	0	ω	1
ω	ω	$2\omega = \alpha^3+\omega\alpha^2+\omega\alpha+1$	$1+\omega = \alpha^4+\omega\alpha^3+\alpha^2+\alpha$
1	1	$1+\omega = \alpha^4+\omega\alpha^3+\alpha^2+\alpha$	$2 = \omega\alpha+\omega$

Таблица 4. Таблица Кэли для сложения в системе счисления $\left\{\frac{-1+i\sqrt{3}}{2};\{0,1,\omega\}\right\}$

+	0	ω	1
0	0	ω	1
ω	ω	$2\omega = \alpha^3+\alpha^2+\omega\alpha+1$	$1+\omega = \omega\alpha^2+\alpha$
1	1	$1+\omega = \omega\alpha^2+\alpha$	$2 = \omega\alpha^2+\omega\alpha+\omega$

Алгоритм 2 (Сложение).

Шаг 1. Складываем по разрядам два данных числа. При этом в записи суммы могут присутствовать цифры $2\omega, 1+\omega, 2$, не входящие в алфавит системы счисления. Тогда переходим к шагу 2, иначе, если таковой цифры не встретилось, получаем искомую сумму.

Шаг 2. Используем формулы из табл. 3 (или 4) сложения для каждой «цифры» в записи числа, не входящей в алфавит (по одному разу для каждого разряда). При этом в записи могут появиться и другие «цифры», избавиться от которых можно применяя формулы из табл. 3 (или 4) к числам, в сумме дающим данные «цифры». После этого, двигаясь от нулевого разряда, находим первую «цифру» справа, большую единицы по норме. Эта «цифра» и все другие, стоящие слева от неё, определяют некоторый многочлен $P(x)$. Если $P(x)$ делится на x^2+3 без остатка, то считаем его «нулевым», если с остатком, то повторяем шаг 2.

Если в сумме не осталось цифр, не принадлежащих алфавиту $\{0,1,\omega\}$, то получаем искомый результат.

Умножение. Реализация операции умножения даже в эквивалентных системах счисления может отличаться. В силу особенностей алфавита, а именно того, что одна из цифр является нулём, таблицы умножения для таких систем счисления сильно упрощаются, и достаточно записать разложение лишь четырёх чисел для тернарной квазиканонической системы счисления. Согласно леммам 3 и 4, алгоритм умножения чисел в системе счисления $\left\{\overline{\alpha}; \overline{I}\right\}$ легко получается из алгоритма умножения чисел в системе счисления $\{\alpha; I\}$. Для примера рассмотрим алгоритм умножения в системе счисления $\left\{-i\sqrt{3};\{0,1,\omega\}\right\}$.

Таблица 5. Таблица Кэли для умножения в системе счисления $\left\{-i\sqrt{3};\{0,1,\omega\}\right\}$

×	ω	1
ω	$\omega^2 = \alpha^3+\omega\alpha^2+\alpha+1$	ω
1	ω	1

Таблица 6. Таблица Кэли для умножения в системе счисления $\left\{-i\sqrt{3};\{0,\omega,\omega^2\}\right\}$

×	ω	ω^2
ω	ω^2	$-1 = \omega\alpha^3+\omega^2\alpha^2+\omega\alpha+\omega$
ω^2	$-1 = \omega\alpha^3+\omega^2\alpha^2+\omega\alpha+\omega$	$\omega^4 = \omega\alpha^2+\omega^2\alpha+\omega^2$

Таблица 7. Таблица Кэли для умножения в системе счисления $\left\{-i\sqrt{3};\{0,-1,\omega^2\}\right\}$

×	−1	ω^2
−1	$1 = \omega^2\alpha^2+(-1)\alpha+\omega^2$	$\omega^5 = \omega^2\alpha^2+(-1)\alpha+(-1)$
ω^2	$\omega^5 = \omega^2\alpha^2+(-1)\alpha+(-1)$	$\omega^4 = \omega^2\alpha^3+(-1)\alpha^2+\omega^2\alpha+\omega^2$

Таблица 8. Таблица Кэли для умножения в системе счисления $\left\{-i\sqrt{3};\{0,-1,\omega^4\}\right\}$

×	-1	ω^4
-1	$1=(-1)\alpha^2+(-1)\alpha+\omega^4$	$\omega=$ $=(-1)\alpha^2+(-1)\alpha+(-1)$
ω^4	$\omega=$ $=(-1)\alpha^2+(-1)\alpha+(-1)$	$\omega^2=(-1)\alpha+\omega^4$

Таблица 9. Таблица Кэли для умножения в системе счисления $\left\{-i\sqrt{3};\{0,\omega^4,\omega^5\}\right\}$

×	ω^5	ω^4
ω^5	ω^4	$\omega^3=\omega^4\alpha+\omega^5$
ω^4	$\omega^3=\omega^4\alpha+\omega^5$	$\omega^2=\omega^4\alpha^2+\omega^5\alpha+\omega^4$

Таблица 10. Таблица Кэли для умножения в системе счисления $\left\{-i\sqrt{3};\{0,1,\omega^5\}\right\}$

×	ω^5	1
ω^5	$\omega^4=\omega^5\alpha+1$	ω^5
1	ω^5	1

Таблица 11. Таблица Кэли для умножения в системе счисления $\left\{\frac{-1+i\sqrt{3}}{2};\{0,1,\omega\}\right\}$

×	ω	1
ω	$\omega^2=\alpha+1$	ω
1	ω	1

Таблица 12. Таблица Кэли для умножения в системе счисления $\left\{\frac{-1+i\sqrt{3}}{2};\{0,\omega,\omega^2\}\right\}$

×	ω	ω^2
ω	ω^2	$-1=\omega\alpha+\omega$
ω^2	$-1=\omega\alpha+\omega$	$\omega^4=\omega^2\alpha+\omega^2$

Таблица 13. Таблица Кэли для умножения в системе счисления $\left\{\frac{-1+i\sqrt{3}}{2};\{0,-1,\omega^2\}\right\}$

×	-1	ω^2
-1	$1=(-1)\alpha+\omega^2$	$\omega^5=(-1)\alpha+(-1)$
ω^2	$\omega^5=(-1)\alpha+(-1)$	$\omega^4=\omega^2\alpha+\omega^2$

Таблица 14. Таблица Кэли для умножения в системе счисления $\left\{\frac{-1+i\sqrt{3}}{2};\{0,-1,\omega^4\}\right\}$

×	-1	ω^4
-1	$1=\omega^4\alpha+\omega^4$	$\omega=\omega^4\alpha+(-1)$
ω^4	$\omega=\omega^4\alpha+(-1)$	$\omega^2=(-1)\alpha^2+(-1)\alpha+\omega^4$

Таблица 15. Таблица Кэли для умножения в системе счисления $\left\{\frac{-1+i\sqrt{3}}{2};\{0,\omega^4,\omega^5\}\right\}$

×	ω^5	ω^4
ω^5	ω^4	$-1=\omega^4\alpha^2+\omega^4\alpha+\omega^5$
ω^4	$-1=\omega^4\alpha^2+\omega^4\alpha+\omega^5$	$\omega^2=\omega^5\alpha+\omega^4$

Таблица 16. Таблица Кэли для умножения в системе счисления $\left\{\frac{-1+i\sqrt{3}}{2};\{0,1,\omega^5\}\right\}$

×	ω^5	1
ω^5	$\omega^4=\omega^5\alpha^2+\omega^5\alpha+1$	ω^5
1	ω^5	1

Поскольку алфавит системы счисления $\left\{-i\sqrt{3};\{0,1,\omega\}\right\}$ состоит из цифр 0, 1 и ω, то умножение чисел a и c в этой системе счисления сводится к сложению m чисел, где m – количество цифр единичной нормы в записи числа c. Складываемые числа получаются из числа a следующим образом. При умножении числа на цифру ω или 1, стоящую в разряде, соответствующем α^p, к записи числа a справа добавляется p нулей, а цифры заменяются согласно формулам из табл. 5 (или 6–16). Далее происходит упрощение полученного числа путём последовательного применения второго шага алгоритма сложения. Далее получившееся число складывают с результатом предыдущей операции сложения согласно алгоритму сложения.

О параллельных алгоритмах вычисления свёртки в тернарных квазиканонических системах счисления

В настоящее время для быстрого умножения больших целых чисел в основном используется алгоритм Шёнхаге–Штрассена [12] или алгоритм Фюрера [13]. До появления последнего наиболее быстрым алгоритмом умножения считался алгоритм Шёнхаге–Штрассена, основная идея которого заключалась в сведении умножения целых чисел, представленных в той или иной позиционной системе счисления, к вычислению циклической свёртки спектральным методом (с помощью дискретного преобразования Фурье (ДПФ) или его модулярных аналогов (теоретико-числовых преобразований, ТЧП).

Развитием алгоритма Шёнхаге–Штрассена можно считать алгоритмы, приведённые в работах [14, 15], которые позволяют вычислять свёртку параллельно и без умножений. В настоящей работе исследуется обобщение метода этих работ на случай квазиканонических систем счисления. Приведём полученные результаты.

Пусть $\mathrm{Norm}(\alpha)=3$. Э–М числом (числом Эйзенштейна–Мерсенна) будем называть целое рациональное число вида

$$M_n = (\alpha^n - 1)(\bar{\alpha}^n - 1) = 3^n - (\alpha^n + \bar{\alpha}^n) + 1,$$

а Э–Ф числом (числом Эйзенштейна–Ферма) – целое рациональное число вида

$$F_n = (\alpha^n + 1)(\bar{\alpha}^n + 1) = 3^n + (\alpha^n + \bar{\alpha}^n) + 1.$$

Лемма 7. При $n \neq 0(\mathrm{mod}4)$ сомножители $(\alpha^n \pm 1)$ и $(\bar{\alpha}^n \pm 1)$ взаимно просты.

Лемма 7 даёт гарантии возможности параллельного вычисления циклической свёртки (или, согласно методу Шенхаге–Штрассена, умножения целых чисел) в кольцах по модулям $(\alpha^n \pm 1)$, $(\bar{\alpha}^n \pm 1)$ с последующей реконструкцией результата по модулям M_n или F_n с помощью китайской теоремы об остатках при достаточно мягких дополнительных ограничениях на арифметическую структуру M_n или F_n. Непосредственный анализ этих ограничений показал, что при $1 \le n \le 100$, $m = (\alpha^n \pm 1)(\bar{\alpha}^n \pm 1)$, и α, равному одному из чисел множества

$$\left\{ i\sqrt{3}, -i\sqrt{3}, \frac{-3+i\sqrt{3}}{2}, \frac{-3-i\sqrt{3}}{2} \right\},$$

вычисление свёртки длины n=1, 2, 3, 4, 5, 7, 8, 11, 13, 16, 17, 19, 23, 29, 31, 32, 37, 41, 43, 47, 53, 59, 61, 64, 67, 71, 73, 79, 83, 89, 97 можно реализовать без умножений.

Заключение

В работе подробно рассмотрен алгоритм представления чисел и реализации основных арифметических операций в кольце целых чисел Эйзенштейна. Приведена полная классификация тернарных квазиканонических систем счисления в мнимых квадратичных полях. Подробно рассмотрен случай поля $Q\left(i\sqrt{3}\right)$, для которого представлено доказательство классификационной теоремы для этого случая.

Предложенный подход достаточно легко обобщается на случай других квадратичных расширений, для элементов которых существуют алгоритмы деления с остатком по норме или их аналоги.

Кроме того, в работе рассмотрена возможность применения метода параллельного вычисления произведения больших чисел [10] для тернарных квазиканонических систем счисления. В результате получены длины свёрток, которые можно использовать для быстрого вычисления произведения.

Благодарности

Работа выполнена при финансовой поддержке РФФИ (гранты 13-01-97007-р_поволжье_а, 12-01-00822а, 12-01-31316 мол а).

Литература

1. **Давыдов, Е.С.** Наименьшие группы чисел для образования натуральных рядов / Е.С. Давыдов. – Питербург: Типо – литография В.В. Комарова, 1903. – 39 с.
2. **Слудский, Ф.А.** О свойствах степеней двух и трёх / Ф.А. Слудский // Математический сборник. – 1870. – Т. 4, Вып. 3. – С. 171-175.
3. **Кушнеров, А.** Троичная цифровая техника. Ретроспектива и современность / А. Кушнеров. – Израиль: Университет им. Бен-Гуриона Беэр-Шева, 2005. – 15 с.
4. **Кнут, Д.** Искусство программирования. Том 2. Получисленные алгоритмы / Д. Кнут. – М.: Мир, 1977. – 727 с.
5. **Katai, I.** Kanonische Zahlensysteme in der Theorie der Quadratischen Zahlen / I. Katai, B. Kovacs // Acta Sci. Math. (Szeged). – 1980. – Vol. 42 – P. 99-107.
6. **Katai, I.** Canonical number systems in imaginary quadratic fields / I. Katai, B. Kovacs // Acta Math. Hungar. – 1981. – Vol. 37 – P. 159-164.
7. **Kovacs, B.** Canonical number systems in algebraic number fields / B. Kovacs // Acta Math. Hungar. – 1981. – Vol. 37 – P. 405-407.
8. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Univ. Sci. Budapest, Sect. Comp. – 2001. – Vol. 20. – P. 195-206.
9. **Боревич, З.И.** Теория чисел / З.И. Боревич, И.Р. Шафаревич. – М.: Наука, 1985. – 504 с.
10. **Чернов, В.М**. Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов. – М.: Физматлит, 2007. – 264 с.
11. **Solomyak, B.** Dynamics of self-similar tilings / B. Solomyak // Ergodic Theory Dynam. Systems. – 1997. – Vol. 17, N 3. – P. 695-738.
12. **Schoenhage, A.** Schnelle Multiplikation grosser Zahlen / A. Schoenhage, V. Strassen // Computing. – 1971. – Vol. 7. – P. 281-292.
13. **Fuerer, M.** Faster integer multiplication / M. Fuerer // STOC Proceedings. – 2007. – P. 57-66.
14. **Чернов, В.М.** Синтез параллельных алгоритмов преобразований Фурье–Галуа в прямых суммах конечных колец / В.М. Чернов // Известия Самарского научного центра Российской академии наук. – 2000. – Вып. 1. – С. 128-134.
15. **Chernov, V.** «Error-free» calculation of the convolution using generalized Mersenne and Fermat transforms over algebraic fields / V. Chernov, M. Pershina // Computer Analysis of Image and Pattern (CAIP'97). Lectures Notes in Computer Science. – 1997. – N 1296 – P. 621–628.

References

1. **Davydov, E.S.** Minimal number groups for the formation of natural series / E.S. Davydov – Petersburg: Typolithography of V.V. Komarov, 1903. – 39 p. – (In Russian).
2. **Sludsky, F.A.** On the properties of degrees of two and three / F. Sludskii // Mathematical Collection. – 1870. – Vol. 4, Issue. 3. – P. 171-175. – (In Russian).
3. **Kushnerov, A.** Ternary digital equipment. Retrospective and modern age / A. Kushnerov – Israel Ben-Gurion University, Beersheba, 2005. – 15 p. – (In Russian).
4. **Knuth, D.E.** The Art of Computer Programming. Vol. 2 Semi-numerical Algorithms / D.E. Knuth – Moscow: "Mir" Publisher, 1977. – 727 p. – (In Russian).
5. **Katai, I.** Kanonische Zahlensysteme in der Theorie der Quadratischen Zahlen / I. Katai, B. Kovacs // Acta Sci. Math. (Szeged). – 1980. – Vol. 42 –P. 99-107.
6. **Katai, I.** Canonical number systems in imaginary quadratic fields / I. Katai, B. Kovacs // Acta Math. Hungar. – 1981. – Vol. 37 – P. 159-164.

7. **Kovacs, B.** Canonical number systems in algebraic number fields / B. Kovacs // Acta Math. Hungar. – 1981. – Vol. 37 – P. 405-407.
8. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Univ. Sci. Budapest, Sect. Comp. – 2001. – Vol. 20 – P. 195-206.
9. **Borevich, Z.I.** Number theory / Z.I. Borevich, I.R. Shafarevich – Academic Press, 1986. – 434 p.
10. **Chernov, V.M.** Arithmetical methods of synthesis of fast algorithms of Discrete orthogonal Transforms / V.M. Chernov – Moscow.: "Fizmatlit" Publisher, 2007. – 264 p. – (In Russian).
11. **Solomyak, B.** Dynamics of self-similar tilings / B. Solomyak // Ergodic Theory Dynam. Systems. – 1997. – Vol. 17, N 3. – P. 695-738.
12. **Schoenhage, A.** Schnelle Multiplikation grosser Zahlen / A. Schoenhage, V. Strassen // Computing. – 1971. – Vol. 7. – P. 281-292.
13. **Fuerer, M.** Faster integer multiplication / M. Fuerer // STOC Proceedings. – 2007. – P. 57-66.
14. **Chernov, V.** Synthesis of parallel algorithms of Fourier-Galois transforms in direct sums of finite rings / V. Chernov // Proceedings of the Samara Scientific Center of Russian Academy of Sciences. – 2000. – Issue 1. – P. 128-134. – (In Russian).
15. **Chernov, V.** «Error-free» calculation of the convolution using generalized Mersenne and Fermat transforms over algebraic fields / V. Chernov, M. Pershina // Computer Analysis of Image and Pattern (CAIP'97). Lectures Notes in Computer Science. – 1997. – N 1296 – P. 621-628.

CLASSIFICATION OF TERNARY QUASICANONICAL NUMBER SYSTEMS IN IMAGINARY QUADRATIC FIELDS AND THEIR APPLICATION

P. S. Bogdanov, V. M. Chernov
Image Processing Systems Institute of the Russian Academy of Sciences

Abstract

In this paper all possible ternary quasicanonical number system in imaginary quadratic fields are considered. For representation of algebraic integers of imaginary quadratic fields in the specified number systems an algorithm based on the division with remainder is used. In addition, the algorithms of the basic arithmetic operations in ternary number systems in the ring of Eisenstain integers are synthesized. Method of fast error-free cyclic convolution computation is considered.

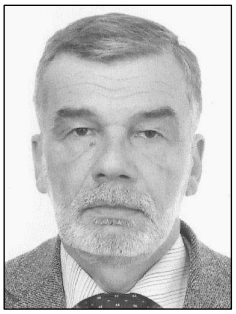
Key words: canonical numerical system, norm division with remainder, quasicanonical numerical system, imaginary quadratic fields.

Сведения об авторах

Богданов Павел Сергеевич, 1989 года рождения, аспирант Самарского государственного аэрокосмического университета имени академика С.П. Королёва. Стажёр-исследователь Института систем обработки изображений РАН. Область научных интересов: обработка изображений, программирование, прикладная математика.

E-mail: *poulsmb@rambler.ru* .

Pavel Sergeevich Bogdanov (b. 1989) postgraduate student of S. P. Korolyov Samara State Aerospace University *(SSAU)*. Trainee researcher of Image Processing Systems Institute of the RAS. Research interests are image processing, programming, applied mathematics.



Чернов Владимир Михайлович, 1949 года рождения, математик, доктор физико-математических наук. Главный научный сотрудник Института систем обработки изображений РАН. Профессор кафедры геоинформатики и информационной безопасности Самарского государственного аэрокосмического университета имени академика С.П. Королёва. Область научных интересов: алгебраические методы в цифровой обработке сигналов, криптография, машинная арифметика.

E-mail: *vche@smr.ru* .

Vladimir Michailovich Chernov (b. 1949) mathematician, Doctor of Physical and Mathematical Sciences. Chief researcher of Image Processing Systems Institute of the RAS. Professor of Geo-Information Science and Information Security department (S. P. Korolyov Samara State Aerospace University (SSAU)). Research interests are algebraic methods in digital signal processing, cryptography, computer arithmetic.

Поступила в редакцию 11 декабря 2013 г.