О СХОДИМОСТИ НЕКОТОРЫХ АЛГОРИТМОВ БИНАРНОЙ И ТЕРНАРНОЙ МАШИННОЙ АРИФМЕТИКИ ДЛЯ ВЫЧИСЛЕНИЙ В МНИМЫХ КВАДРАТИЧНЫХ ПОЛЯХ

Богданов П.С.

Институт систем обработки изображений РАН,

Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет) (СГАУ)

Аннотация

В работе доказывается ряд утверждений, позволяющих существенно уменьшить сложность доказательств классификационных теорем для квазиканонических систем счисления в мнимых квадратичных полях. Доказываются теоремы сходимости алгоритмов, реализующих сложение целых алгебраических чисел в квазиканонических системах счисления.

Ключевые слова: каноническая система счисления, квазиканоническая система счисления, деление с остатком по норме, эквивалентные системы счисления.

Введение

Наметившаяся в последние годы тенденция к расширению возможностей машинной (компьютерной) арифметики определяется в основном двумя факторами.

Во-первых, это возможность создания надёжных аппаратных средств, позволяющих обрабатывать вещественные и комплексные цифровые данные, представленные в системах счисления, отличных от ставшей уже классической двоичной системы.

Во-вторых, это теоретические результаты, касающиеся собственно систем счисления, имеющих «дружественную» структуру по отношению к упомянутым выше аппаратным средствам.

В частности, в работах И. Катаи и Б. Ковача [1, 2] введено понятие канонических систем счисления, экстраполирующее теорию систем счисления на случай квадратичных алгебраических полей и дискретных решёток в них. 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 [1 – 3] ими получены классификационные теоремы для канонических систем счисления во всех квадратичных полях. Кроме того, Ковачем [4] найдены эффективные нелинейные рекуррентные алгоритмы вычисления цифр представления элементов в канонических системах счисления.

Системы счисления, в которых вместо целых рациональных чисел, образующих допустимое множества цифр (алфавит) канонических систем счисления, рассматриваются целые квадратичные числа, изучены в меньшей степени. В частности, в работах [5 – 8] было введено понятие квазиканонических систем счисления, которые являются одним из естественных обобщений систем счисления в поле комплексных или действительных чисел, в частности, на случай дискретных решёток квадратичных полей. В этих работах приведена классификация всех бинарных и тернарных квазиканонических систем счисления в мнимых квадратичных полях, а также рассмотрены некоторые приложения таких систем счисления.

В отличие от рекуррентных нелинейных алгоритмов работы [1] в работах [5 – 7] для нахождения представления элементов в квазиканонических системах счисления используется алгоритм деления с остатком, который имеет место не во всех квадратичных кольцах, а только в кольцах целых элементов мнимых полей $Q(\sqrt{d})$.

Такой подход сталкивается со значительной вычислительной трудностью, связанной с тем, что при делении с остатком вычисляется не остаток, а только его норма. Нахождение же из конечного множества элементов с одинаковой нормой необходимого остатка (то есть «цифры» разложения) требует дополнительного исследования, которое может включать в себя достаточно громоздкий перебор, а именно: выбор такого остатка, при котором неполное частное имеет норму, меньшую, чем делимое (в частности, для кольца $S(i\sqrt{3})$ целых элементов поля $Q(i\sqrt{3})$ существует 6 элементов с нормой 1 и 6 элементов с нормой 3, что приводит к исследованию 90 вариантов пар «основание системы счисления – цифровое множество»). В настоящей работе получены и систематизированы аналитические соотношения, позволяющие оптимизировать такой перебор.

Кроме того, в работе формулируются условия сходимости алгоритмов сложения целых алгебраических чисел в произвольных квазиканонических системах счисления.

1. Основные определения

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. Если $d < 0$, то квадратичное поле называется мнимым, если $d > 0$ – действительным.

Определение 1. Если у элемента $z = a + b\sqrt{d} \in Q(\sqrt{d})$ его норма $Norm(z)$ и след $Tr(z)$ есть целые числа:

$$Norm(z) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in Z,$$

$$Tr(z) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in Z,$$

то этот элемент называется целым алгебраическим числом поля $Q(\sqrt{d})$ [10].

Известен следующий критерий целостности алгебраических чисел для мнимых квадратичных полей [9].

Утверждение. Если $d \in Z$, $d \equiv 1, 2, 3 \pmod 4$, то целыми алгебраическими числами мнимого квадратичного поля $Q(\sqrt{d})$ являются числа $a+b\sqrt{d}; a,b\in Z$ при $d\equiv 2,3(\mathrm{mod}\ 4)$ и числа $(a+b\sqrt{d})/2; a,b\in Z$, $a\equiv b(\mathrm{mod}\ 2)$ при $d\equiv 1(\mathrm{mod}\ 4)$.

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

Определение 2. Целое алгебраическое число α называется основанием квазиканонической системы счисления в мнимом кольце $S(\sqrt{d})$ целых элементов поля $Q(\sqrt{d})$, если любой целый элемент этого поля однозначно представим в виде конечной суммы $z=\sum_{j=0}^{k(z)} a_j\alpha^j$, $a_j\in I$, $k(z)\in N\cup\{0\}$, где множество I состоит из целых алгебраических чисел кольца $S(\sqrt{d})$, абсолютная величина нормы которых меньше модуля нормы основания α.

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

Определение 3. Если множество I состоит из всех целых неотрицательных рациональных чисел, меньших нормы основания, то есть $I=\{0,1,...,|Norm(\alpha)|-1\}$, то пара $\{\alpha;I\}$ называется канонической системой счисления в мнимом кольце $S(\sqrt{d})$ [10].

Определение 4. Квазиканоническая система счисления с основанием α и алфавитом I называется бинарной системой счисления в мнимом кольце $S(\sqrt{d})$, если $|Norm(\alpha)|=2$ и алфавит I состоит из двух цифр.

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

2. Представление чисел в квазиканонических системах счисления

В работах [6, 7] рассматривались классификационные теоремы для всех бинарных и тернарных квазиканонических систем счисления в мнимых квадратичных полях. Доказательство таких теорем можно оптимизировать, если опираться на некоторые утверждения, справедливые для всех мнимых квадратичных полей. Эти утверждения необходимы для обоснования единственности и конечности представления каждого целого элемента поля $Q(\sqrt{d})$ в рассматриваемых квазиканонических системах счисления.

Лемма 1. Если $Norm(\alpha)\neq 0$, то равенство $\beta=\alpha\gamma+r$ равносильно равенству

$$\gamma=(\beta-r)\bar{\alpha}/Norm(\alpha). \tag{1}$$

Лемма 2. Если для пары $\{\alpha;I\}$ представление произвольного целого алгебраического 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 в кольце $S(\sqrt{d})$, необходимо и достаточно, чтобы процесс деления с остатком [9]:

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

где $r_0, r_1, \ldots, r_l\in I$, был конечен.

Лемма 3. Если $|Norm(\gamma_{m+1})|<|Norm(\gamma_m)|$ $\forall m=0,1,\ldots$, то процесс деления с остатком (2) конечен.

Лемма 4. Если, γ_{m+1} и γ_m – целые алгебраические числа мнимого кольца $S(i\sqrt{\Delta})$ ($\Delta=-d$) на m шаге процесса деления с остатком (2), то для выполнения неравенства $Norm(\gamma_{m+1})\geq Norm(\gamma_m)$ необходимо и достаточно, чтобы

$$Norm\left(\gamma_m+\frac{r_m}{Norm(\alpha)-1}\right)\leq\frac{Norm(r_m)\cdot Norm(\alpha)}{(Norm(\alpha)-1)^2}.$$

Определение 6. Пару $\{\alpha; I\}$, где α – целое алгебраическое число мнимого кольца $S(\sqrt{d})$, а множество I состоит из целых алгебраических чисел кольца $S(\sqrt{d})$, абсолютная величина нормы которых меньше модуля нормы α, назовём α-системой в кольце $S(\sqrt{d})$.

Очевидно, что любая квазиканоническая система счисления является α-системой, обратное утверждение неверно.

Теорема 1. Если для каждого $\gamma\in S(i\sqrt{\Delta})$, удовлетворяющего условию

$$Norm\left(\gamma+\frac{r_j}{Norm(\alpha)-1}\right)\leq\frac{Norm(r_j)\cdot Norm(\alpha)}{(Norm(\alpha)-1)^2},$$

хотя бы при одном элементе r_j множества I существует конечное представление γ в α-системе $\{\alpha, I\}$, то любое целое алгебраическое число также конечным образом представимо в α-системе $\{\alpha, I\}$.

Если представление произвольного целого алгебраического числа γ_0 единственно и конечно, то α-система $\{\alpha, I\}$ будет являться квазиканонической системой счисления. Стоит отметить, что для остатка $r_m=0$ последнее неравенство записывается в виде $Norm(\gamma_m)\leq 0$. Это означает, что для остатка $r_m=0$ существует лишь одно число $\gamma_m=0$, удовлетворяющее неравенству $Norm(\gamma_{m+1})\geq Norm(\gamma_m)$, появление которого свидетельствует об окончании процесса деления с остатком (2).

Лемма 5. Если (α, I) – квазиканоническая система счисления в мнимом кольце $S(\sqrt{d})$, то множество I содержит один и только один остаток с нулевой нормой, а именно, $r_0 = 0$.

Определение 7. Пусть $\{\alpha; I\}$ и $\{\alpha'; I'\}$ – две α-системы в мнимом кольце $S(\sqrt{d})$, где

$$\left|Norm(\alpha)\right| = \left|Norm(\alpha')\right|,$$

и существует взаимно однозначное отображение

$$f : S\left(\sqrt{d}\right) \to S\left(\sqrt{d}\right),$$

причём $f(I) = I'$, а для любого числа $\gamma \in S\left(\sqrt{d}\right)$

$$\left|Norm(\gamma)\right| = \left|Norm\left(f(\gamma)\right)\right|.$$

Тогда если из представления числа γ в α-системе $\{\alpha; I\}$ в виде $\gamma = \gamma_1\alpha + r$, где

$$\left|Norm(r)\right| < \left|Norm(\alpha)\right|,$$

следует справедливость представления $f(\gamma) = f(\gamma_1)\alpha' + f(r)$ в α-системе $\{\alpha'; I'\}$, то α-система $\{\alpha; I\}$ называется эквивалентной α-системе $\{\alpha'; I'\}$.

Из определения 7 следует, что если α-система $\{\alpha; I\}$ является квазиканонической системой счисления в мнимом кольце $S(\sqrt{d})$, то и все эквивалентные ей α-системы тоже будут квазиканоническими системами счисления в кольце $S(\sqrt{d})$. Если же α-система $\{\alpha; I\}$ не является квазиканонической системой счисления в кольце $S(\sqrt{d})$, то и все эквивалентные ей α-системы также не являются квазиканоническими системами счисления в кольце $S(\sqrt{d})$.

Рассмотрим некоторые примеры эквивалентности α-систем.

Лемма 6. Пусть n – количество чисел единичной нормы в кольце $S(\sqrt{d})$. Если r – первообразный корень из единицы степени n, то α-системы $\{\alpha; I\}$ и $\{\alpha; I \cdot r^k\}$ в кольце $S(\sqrt{d})$ эквивалентны, где $k = 0, 1, 2, \ldots$.

Лемма 7. Если $\bar{\alpha}$ – число комплексно-сопряжённое числу α, а $\bar{I}$ состоит из чисел комплексно-сопряжённых числам из I, то α-системы $\{\alpha; I\}$ и $\{\bar{\alpha}; \bar{I}\}$ эквивалентны.

Лемма 8. Пусть $f : (\alpha, I) \to (\alpha, I \cdot r^k)$ – эквивалентность α-систем (α, I) и $(\alpha, I \cdot r^k)$. Тогда для любых γ и $\beta \in S(\sqrt{d})$ справедливы равенства:

1) $f(\gamma + \beta) = f(\gamma) + f(\beta)$,

2) $f(-\gamma) = -f(\gamma)$.

Лемма 9. Пусть $f : (\alpha, I) \to (\bar{\alpha}, \bar{I})$ – эквивалентность α-систем (α, I) и $(\bar{\alpha}, \bar{I})$. Тогда для любых γ и $\beta \in S(\sqrt{d})$ справедливы равенства:

1) $f(\gamma + \beta) = f(\gamma) + f(\beta)$,

2) $f(-\gamma) = -f(\gamma)$,

3) $f(\gamma \cdot \beta) = f(\gamma) \cdot f(\beta)$.

Из леммы 8 следует, что алгоритмы сложения и инверсии знака в системах счисления (α, I) и $(\alpha, I \cdot r^k)$ имеют одинаковый вид.

Из леммы 9 следует, что алгоритмы сложения, инверсии знака и умножения в системах счисления (α, I) и $(\bar{\alpha}, \bar{I})$ имеют одинаковый вид.

3. Сходимость алгоритмов арифметических операций в квазиканонических системах счисления

В работах [6, 7] была рассмотрена реализация арифметических операций в бинарных и тернарных квазиканонических системах счисления. Приведённые ниже утверждения позволяют получить алгоритмы арифметических операций в произвольных квазиканонических системах счисления.

Пусть представления чисел β_1, β_2 и $\beta_1 + \beta_2$ в квазиканонической системе счисления (α, *I*) имеют вид

$$\beta_1 = \sum_{i=0}^{M_1} r_{1i}\alpha^i, \quad \beta_2 = \sum_{i=0}^{M_2} r_{2i}\alpha^i \quad \text{и} \quad \beta_1 + \beta_2 = \sum_{i=0}^{M_3} r_{3i}\alpha^i.$$

Тогда

$$\beta_1 + \beta_2 = \sum_{i=0}^{M_3} r_{3i}\alpha^i = \sum_{j=0}^{\max(M_1, M_2)} \left(r_{1j} + r_{2j}\right)\alpha^j,$$

а следовательно,

$$\sum_{j=0}^{\max(M_1, M_2)} \left(r_{1j} + r_{2j}\right)\alpha^j - \sum_{i=0}^{M_3} r_{3i}\alpha^i = 0$$

$$\text{или} \quad \sum_{j=0}^{\max(M_1, M_2, M_3)} \left(r_{1j} + r_{2j} - r_{3j}\right)\alpha^j = 0.$$

Последнее равенство можно переписать в виде $\sum_{j=0}^{M} c_j\alpha^j = 0$, где $M = \max(M_1, M_2, M_3)$ и $c_j = r_{1j} + r_{2j} - r_{3j}$. Таким образом, если выделить в сумме

$$\beta_1 + \beta_2 = \sum_{j=0}^{\max(M_1, M_2)} \left(r_{1j} + r_{2j}\right)\alpha^j$$

выражение $\sum_{j=0}^{M} c_j\alpha^j = 0$ и заменить его нулём, то результат сложения $\beta_1 + \beta_2$ будет совпадать с результатом представления $\beta_1 + \beta_2$. Введём следующее обозначение $P_2(\alpha) = \alpha^2 - Tr(\alpha) \cdot \alpha + Norm(\alpha)$.

Лемма 10. Если $\sum_{i=0}^{M} c_i\alpha^i = 0$, где $c_i \in C$, $M \geq 2$, $\alpha = const$, $\mathrm{Im}(\alpha) \neq 0$, то это равенство может быть представлено в виде $c_M \cdot P_2(\alpha)\cdot\left(\sum_{i=0}^{M-2} c_i'\alpha^i\right) = 0$, где $c_i' \in C$.

Замечание. Если все условия леммы выполнены, но $M = 1$, то равенство $\sum_{i=0}^{1} c_i\alpha^i = 0$ может быть представлено в виде $\sum_{i=0}^{M} c_i'\alpha^i = 0$, где $c_0' = r_j$ и $c_1' = r_s$, $r_j, r_s \in I$, $M \geq 2$. Действительно, из равенства $\sum_{i=0}^{1} c_i\alpha^i = 0$ следует $Norm(-c_0) = Norm(c_1\alpha)$ или $Norm(c_0) = Norm(\alpha)\cdot Norm(c_1) \geq Norm(\alpha)$, тогда c_0 может быть представлено в системе счисления $\{\alpha, I\}$. Подставим его в выражение $\sum_{i=0}^{1} c_i\alpha^i = 0$. Тогда значение c_1 изменится, и, подставив его представление, получим, что $\sum_{i=0}^{1} c_i\alpha^i = \sum_{i=0}^{M} c_i'\alpha^i = 0$, где $c_0' = r_j$ и $c_1' = r_s$, $r_j, r_s \in I$.

Лемма 11. Если числа β_1, β_2 и $\beta_1 + \beta_2$ в системе счисления (α, I) имеют представления $\beta_1 = \sum_{i=0}^{M_1} r_{1i}\alpha^i$, $\beta_2 = \sum_{i=0}^{M_2} r_{2i}\alpha^i$ и $\beta_1 + \beta_2 = \sum_{i=0}^{M_3} r_{3i}\alpha^i$ соответственно, то выражение

$$\sum_{j=0}^{\max(M_1, M_2, M_3)} \left(r_{1j} + r_{2j} - r_{3j}\right)\alpha^j = \sum_{j=0}^{M} c_j\alpha^j,\ M \geq 2,$$

может быть представлено в виде

$$P_2(\alpha)\cdot\left(\sum_{i=0}^{Norm(\alpha)-1}\left(r_i \cdot \sum_{j=0}^{M'} c_{ij}'\alpha^j\right)\right),$$

где $c_{ij}' \in Z$, $c_{ij}' \geq 0$, $r_i \in I$.

Выражение из леммы 11 может быть записано следующим образом

$$P_2(\alpha)\cdot\left(\sum_{i=0}^{Norm(\alpha)-1}\left(r_i \cdot \sum_{j=0}^{M'} c_{ij}'\alpha^j\right)\right) =$$
$$= \sum_{i=0}^{Norm(\alpha)-1}\left(r_i \cdot P_2(\alpha)\cdot \sum_{j=0}^{M'} c_{ij}'\alpha^j\right).$$

Так как $r_i \cdot P_2(\alpha) = r_i \cdot P_2(\alpha)\cdot\alpha^j$, то обнулять $r_i \cdot P_2(\alpha)$ в сумме $\beta_1 + \beta_2$ можно на любой позиции. Это означает, что, обнуляя в сумме $\beta_1 + \beta_2$ выражения $r_i \cdot P_2(\alpha)$ конечное число раз, равное $\sum_{j=0}^{M'} c_{ij}$ для каждого r_i, получаем результат, совпадающий с записью числа $\beta_1 + \beta_2$ в системе счисления $\{\alpha, I\}$.

Теорема 2. Если в произвольной квазиканонической системе счисления $\{\alpha, I\}$ для любых двух элементов r_{j_1} и r_{j_2} множества I выполняется условие $k_1 \cdot r_{j_1} \neq k_2 \cdot r_{j_2}$, $j_1 \neq j_2$, $k_1, k_2 \in Z$, $k_1 \cdot k_2 < 0$ и в этой системе счисления существует алгоритм сложения произвольных чисел β_1 и β_2, обнуляющий все выражения вида $r_i \cdot P_2(\alpha)$, то такой алгоритм сложения будет конечен и его результат будет совпадать с результатом представления числа $\beta_1 + \beta_2$ в системе счисления $\{\alpha, I\}$.

Теорема 3. Если в произвольной квазиканонической системе счисления $\{\alpha, I\}$ существуют хотя бы два элемента r_{j_1} и r_{j_2} множества I, для которых выполняется условие $k_1 \cdot r_{j_1} = k_2 \cdot r_{j_2}$, $j_1 \neq j_2$, $k_1, k_2 \in Z$, $k_1 \cdot k_2 < 0$, и в этой системе счисления существует алгоритм сложения произвольных чисел β_1 и β_2, обнуляющий все выражения вида $r_i \cdot P_2(\alpha)$, причём для этого алгоритма все c_i ограничены, где

$$c_i = \sum_{j=0}^{M'} c_{ij}',\ \text{и}\ c_{ij}'$$

берутся из формулы в лемме 11, то такой алгоритм сложения будет конечен и его результат будет совпадать с результатом представления числа $\beta_1 + \beta_2$ в системе счисления $\{\alpha, I\}$.

Теорема 2 означает, что при выполнении условия $k_1 \cdot r_{j_1} \neq k_2 \cdot r_{j_2}$, $j_1 \neq j_2$, $k_1, k_2 \in Z$, $k_1 \cdot k_2 < 0$ для произвольных r_{j_1} и r_{j_2} из множества I алгоритм сложения, обнуляющий все выражения вида $r_i \cdot P_2(\alpha)$, будет сходиться, причём сходиться он будет независимо от способа обнуления этих выражений.

В теореме 3 говорится, что при выполнении условий $k_1 \cdot r_{j_1} = k_2 \cdot r_{j_2}$, $j_1 \neq j_2$, $k_1, k_2 \in Z$, $k_1 \cdot k_2 < 0$ сходиться будет лишь та вариация алгоритма, для которой выполняется условие, и все c_i ограничены. Несложно убедиться в том, что если какие либо c_i не ограничены, то их можно сделать ограниченными за счёт формулы $k_1 \cdot r_{j_1} = k_2 \cdot r_{j_2}$, то есть для этого случая всегда найдётся такая вариация алгоритма сложения, которая будет сходиться.

Всё сказанное выше применимо не только к сложению чисел, но и к другим операциям. Учитывая эти требования, можно составлять различные алгоритмы арифметических операций. Так, альтернативной версией описанного в работе [5] алгоритма сложения чисел в бинарных системах счисления кольца $S(i)$ является алгоритм сложения, начинающий свою работу со старшего разряда. Сходимость этих алгоритмов гарантируется теоремой 2.

Введём следующие обозначения. Количество разрядов в записи суммы обозначим l. Значение в разряде с номером $j \in \{0, 1, \ldots, l-1\}$ обозначим как x_j, $x_j \in \{0, r, 2r, \ldots\}$.

Алгоритм 1.

Шаг 1. Складываем по разрядам два данных числа. При этом в записи суммы может присутствовать цифра $2r$, не входящая в алфавит системы счисления. Если есть такие $j_s \in \{0, 1, \ldots, l-1\}$, что $x_{j_s} = 2r$, то $k = \max(J_s)$ и переходим к шагу 2, иначе алгоритм закончен.

Шаг 2. Если $k < 0$, то алгоритм закончен. Иначе, если $x_k \in \{r, 2r\}$, то переходим к шагу 3, если $x_k = 0$, то переходим к шагу 2, при $k = k-1$.

Шаг 3. Если $k-2 \geq 0$, то

– если $x_k = r$, $x_{k-1} = r$, $x_{k-2} = 0$ или $x_k = r$, $x_{k-1} = 0$, $x_{k-2} = 0$, то переходим к шагу 2, при $k = k-3$;

– если $x_k = r$, $x_{k-1} = r$, $x_{k-2} = r$ или $x_k = r$, $x_{k-1} = 0$, $x_{k-2} = r$, то переходим к шагу 2, при $k = k-2$;

– если $x_k = r$, $x_{k-1} = 2r$, $x_{k-2} = 2r$, то $x_k = 0 = x_{k-1} = x_{k-2}$ и переходим к шагу 2, при $k = k-3$. Если при этом $l = k$, то присваиваем l значение $l-3$;

– если $x_k = r$, $x_{k-1} = 2r$, $x_{k-2} = r$ или $x_k = r$, $x_{k-1} = 2r$, $x_{k-2} = 0$, то $x_{k+2} = x_{k+2} + r$, $x_{k+1} = x_{k+1} + r$, $x_{k-1} = 0$ и переходим к шагу 2, при $k = k+3$. Если при этом $l < k+3$, то присваиваем l значение $k+3$;

– если $x_k = r$, $x_{k-1} = r$, $x_{k-2} = 2r$ или $x_k = r$, $x_{k-1} = 0$, $x_{k-2} = 2r$, то $x_{k+1} = x_{k+1} + r$, $x_k = x_k + r$, $x_{k-2} = 0$ и переходим к шагу 2, при $k = k+2$. Если при этом $l < k+2$, то присваиваем l значение $k+2$;

– если $x_k = 2r$, $x_{k-1} = 2r$, $x_{k-2} = 2r$, то $x_k = r$, $x_{k-1} = 0$, $x_{k-2} = 0$ и переходим к шагу 2, при $k = k-3$.

Заключение

В работе приведены утверждения, позволяющие упростить доказательство классификационных теорем для квазиканонических систем счисления в мнимых квадратичных полях. Большая часть из этих утверждений справедлива и для действительных квадратичных полей, за исключением леммы 4 и, соответственно, теоремы 1, что позволяет исследовать квазиканонические системы счисления и в этих полях. Кроме того, в работе сформулированы леммы, позволяющие реализовать арифметические операции в произвольных квазиканонических системах счисления.

Основные результаты работы представлены в теоремах 1, 2 и 3. Теорема 1 является критерием сходимости алгоритма представления целого алгебраического числа в квазиканонической системе счисления, а теоремы 2 и 3 – критериями сходимости алгоритма сложения в такой системе счисления.

Благодарности

Работа выполнена при финансовой поддержке РФФИ (гранты 15-07-05576, 13-01-97007-р_поволжье_а).

Литература

1. **Katai, I.** Kanonische Zahlensysteme in der Theorie der Quadratischen Zahlen / I. Katai, B. Kovacs // Acta Scientiarum Mathematicarum (Szeged). – 1980. – Vol. 42. – P. 99-107.
2. **Katai, I.** Canonical number systems in imaginary quadratic fields / I. Katai, B. Kovacs // Acta Mathematica Hungarica. – 1981. – Vol. 37. – P. 159-164.
3. **Kovacs, B.** Canonical number systems in algebraic number fields / B. Kovacs // Acta Mathematica Hungarica. – 1981. – Vol. 37. – P. 405-407.
4. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Universitatis Scientiarum Budapest, Sectio Computatorica. – 2001. – Vol. 20. – P. 195-206.
5. **Богданов, П.С.** О представлении целых гауссовых чисел в системе счисления Пенни // Компьютерная оптика. – 2010. – Т. 34, № 4. – С. 561-566. – ISSN 0134-2452.
6. **Богданов, П.С.** Классификация бинарных квазиканонических систем счисления в мнимых квадратичных полях / П.С. Богданов, В.М. Чернов // Компьютерная оптика. – 2013. – Т. 37, № 3. – С. 391-400. – ISSN 0134-2452.
7. **Богданов, П.С.** Классификация тернарных квазиканонических систем счисления в мнимых квадратичных полях и их приложение / П.С. Богданов, В.М. Чернов // Компьютерная оптика. – 2014. – Т. 38, № 1. – С. 139-147. – ISSN 0134-2452.
8. **Богданов, П.С.** О размерности границ некоторых фрактальных множеств на гексагональных решётках / П.С. Богданов, В.М. Чернов // Компьютерная оптика. – 2014. – Т. 38, № 2. – С. 330-334. – ISSN 0134-2452.
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.

References

1. **Katai, I.** Kanonische Zahlensysteme in der Theorie der Quadratischen Zahlen / I. Katai, B. Kovacs // Acta Scientiarum Mathematicarum (Szeged). – 1980. – Vol. 42. – P. 99-107.
2. **Katai, I.** Canonical number systems in imaginary quadratic fields / I. Katai, B. Kovacs // Acta Mathematica Hungarica. – 1981. – Vol. 37. – P. 159-164.
3. **Kovacs, B.** Canonical number systems in algebraic number fields / B. Kovacs // Acta Mathematica Hungarica. – 1981. – Vol. 37. – P. 405-407.
4. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Universitatis Scientiarum Budapest, Sectio Computatorica. – 2001. – Vol. 20. – P. 195-206.
5. **Bogdanov, P.S.** Gaussian integers representation in pitti's number system // Computer Optics. – 2010. – Vol. 34(4). – P. 561-566. – ISSN 0134-2452. – (In Russian).
6. **Bogdanov, P.S.** Classification of binary quasicanonical number systems in imaginary quadratic fields / P.S. Bogdanov, V.M. Chernov // Computer Optics. – 2013. – Vol. 37(3). – P. 391-400. – ISSN 0134-2452.
7. **Bogdanov, P.S.** Classification of ternary quasicanonical number systems in imaginary quadratic fields and their application / P.S. Bogdanov, V.M. Chernov // Computer Optics. – 2014. – Vol. 38(1). – P. 139-147. – ISSN 0134-2452.

8. **Bogdanov, P.S.** Dimension of Some fractal sets on hexagonal lattices / P.S. Bogdanov, V.M. Chernov // Computer Optics. – 2014. – Vol. 38(2). – P. 330-334. – ISSN 0134-2452.
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).

ON THE CONVERGENCE OF SOME ALGORITHMS OF BINARY OR TERNARY MACHINE ARITHMETIC FOR CALCULATIONS IN IMAGINARY QUADRATIC FIELDS

P.S. Bogdanov
Image Processing Systems Institute,
Russian Academy of Sciences,
Samara State Aerospace University

Abstract

The paper proves a number of statements that significantly reduce the complexity of proofs of the classification theorems for quasicanonical number systems in imaginary quadratic fields. Theorems on convergence of algorithms that implement the addition of algebraic integers in quasicanonical number systems are proved.

Keywords: canonical numerical system, quasicanonical numerical system, norm division with remainder, equivalent numerical systems.

Сведения об авторе

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 the Image Processing Systems Institute of the RAS. Research interests are image processing, programming, applied mathematics.

Поступила в редакцию 24 февраля 2015 г.
Окончательный вариант – 8 апреля 2015 г.