КЛАССИФИКАЦИЯ БИНАРНЫХ КВАЗИКАНОНИЧЕСКИХ СИСТЕМ СЧИСЛЕНИЯ В МНИМЫХ КВАДРАТИЧНЫХ ПОЛЯХ

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

Аннотация

В работе рассматриваются все возможные бинарные 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 рассматриваемых системах счисления.

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

Введение

В основе представления и обработки информации в современных компьютерах лежит бинарная система счисления поля действительных чисел. Среди других систем счисления, которые используют всего две цифры для представления каждого элемента рассматриваемой алгебраической структуры, наиболее исследованы канонические системы счисления (КСС) квадратичных полей. Они являются естественным обобщением степенного представления обычных целых чисел [1] на случай алгебраических целых чисел. Такие системы счисления рассматривались ещё в монографии Кнута [2], но систематическая разработка теории КСС началась в работах И. Катаи и Я. Сабо [3], Б. Ковача [4], И. Катаи и Б. Ковача ([5], [6]), У. Дж. Джилберта [7] и других исследователей.

Понятие КСС впервые появилось в работах Катаи и Сабо [3], где были указаны все целые гауссовы числа, являющиеся основаниями КСС. Этот результат был обобщён на случай квадратичных целых чисел в работах Катаи и Ковача [5], [6], а также независимо от них в работе Джилберта [7].

Среди приложений КСС следует отметить работы, касающиеся связи фракталов и КСС [8 11]. Эта связь рассматривалась и в других работах [12–16]. Некоторые авторы исследовали фрактальную структуру границ [17–20] и динамические свойства [21] фундаментальных областей КСС. Более того, в работах [11], [22], [23] рассматривалась связь мозаик, а следовательно, и КСС с вейвлетами.

Системы счисления, в которых вместо целых рациональных чисел, образующих множество цифр КСС, рассматриваются целые квадратичные числа, изучены в меньшей степени. Такие системы счисления будем называть квазиканоническими.

В настоящей работе исследуются все бинарные квазиканонические системы счисления в кольцах целых чисел мнимых квадратичных полей. Для каждой из этих систем счисления рассматриваются алгоритмы реализации основных арифметических операций.

Канонические и квазиканонические системы счисления. Основные определения

Пусть $Q(\sqrt{d})$ есть квадратичное поле [24]:

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

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

Определение. 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 $Q(\sqrt{d})$ [25].

Сформулируем ряд известных утверждений о целых алгебраических числах.

Утверждение. Пусть $d < 0$, $\Delta = |d|$. Тогда целыми алгебраическими числами мнимого поля $Q\left(i\sqrt{\Delta}\right)$ являются числа

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

Кольцо целых элементов поля $Q\left(\sqrt{d}\right)$ будем обозначать $S\left(\sqrt{d}\right)$, а $Z\left(\sqrt{d}\right)$ – множество

$$Z\left(\sqrt{d}\right) = \left\{ z = a + b\sqrt{d} : a, b \in Z \right\} \subseteq S\left(\sqrt{d}\right) \subset Q\left(\sqrt{d}\right).$$

Определение. 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 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

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

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

Пара $\{\alpha; I\}$ называется канонической системой счисления в кольце $S\left(\sqrt{d}\right)$, а I – алфавитом этой системы [25].

В исследованиях различных авторов, рассматривающих КСС, для представления целого алгебраического числа применяется рекуррентный алгоритм [26]. Однако с той же целью можно использовать и деление с остатком, реализуемое лишь в некоторых кольцах [21]. В настоящей работе рассматриваются только мнимые кольца.

Определение. 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 $S\left(\sqrt{d}\right)$ целых элементов мнимых квадратичных полей $Q\left(\sqrt{d}\right)$ алгоритмом деления с остатком по норме обладают те и только те, для которых d равно одному из следующих пяти значений: $\{-1,\ -2,\ -3,\ -7,\ -11\}$ [24].

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).

Бинарные квазиканонические системы счисления

Рассмотрим все возможные бинарные системы счисления в кольцах целых алгебраических чисел мнимых квадратичных полей.

Определение. Квазиканоническая система счисления с основанием α и алфавитом I называется бинарной системой счисления, если $Norm(\alpha) = 2$ и алфавит I состоит из двух цифр.

Отметим легко проверяемые свойства, которые справедливы для всех бинарных квазиканонических систем счисления.

Свойство 1. Согласно определению деления с остатком по норме и учитывая, что $Norm(\alpha) = 2$, получаем

$$\gamma = \frac{(\beta - r)\overline{\alpha}}{2}, \tag{1}$$

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

Соотношение (1) следует из формулы $\beta = \alpha\gamma + r$, которая встречается в определении деления с остатком.

Свойство 2. Если для пары $\{\alpha; I\}$ доказано, что 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, достаточно показать, что представление числа γ_0 является конечным, то есть процесс деления с остатком:

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

где $r_0, r_1, \ldots, r_l \in I$, 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. Системы счисления $\{\alpha; I\}$ и $\{\alpha'; I'\}$ в кольце $S\left(\sqrt{d}\right)$ называются эквивалентными, если существует взаимно однозначное отображение $f : S\left(\sqrt{d}\right) \to S\left(\sqrt{d}\right)$, причём $f(I) = I'$, такое, что для любого числа $\gamma \in S\left(\sqrt{d}\right)$, 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 алфавите $\{\alpha'; I'\}$ записывается в виде $f(\gamma) = \sum_{p=0}^{N} f(a_p)(\alpha')^p$. Стоит отметить, что α' необязательно равно $f(\alpha)$.

Свойство 3. 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, где r – первообразный корень из единицы степени, равной количеству единиц поля в кольце $S\left(\sqrt{d}\right)$, 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.

Аналогично, 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 $\{\overline{\alpha}; \overline{I}\}$, как и число γ_0 в системе счисления $\{\alpha; I\}$. Следовательно, системы счисления $\{\alpha; I\}$ и $\{\overline{\alpha}; \overline{I}\}$ также эквивалентны.

Замечание. Очевидно, что если f – функция, переводящая систему счисления $\{\alpha; I\}$ в $\{\alpha'; I'\}$, 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.

Если функция f задаётся следующим равенством $f(\gamma)=\overline{\gamma}$, где $\overline{\gamma}$ – число, сопряжённое γ, то алгоритм умножения двух чисел $\overline{\gamma}$ и $\overline{\beta}$ в системе счисления $\{\overline{\alpha};\overline{I}\}$ также легко получается из алгоритма умножения чисел γ и β в системе счисления $\{\alpha; I\}$.

Квазиканонические системы счисления в S(i)

Кольцо $S(i)$ целых элементов (целых гауссовых чисел) поля $Q(i)$ состоит из элементов

$z=a+bi;\quad a,b\in Z.$

При делении с остатком по норме на α, $Norm(\alpha)=2$, норма ненулевого остатка может равняться только единице. Таких остатков ровно четыре: $\{\pm 1,\pm i\}$, что в сочетании с вариантами выбора α: $\{\pm 1\pm i\}$ даёт 16 потенциальных комбинаций возможных оснований α и множества I, то есть 16 бинарных квазиканонических систем счисления. Однако, учитывая свойство 3, получаем, что в кольце $S(i)$ достаточно исследовать лишь две системы счисления, а именно: $\{-1+i;\{0,i\}\}$ и $\{1+i;\{0,i\}\}$.

Следующая теорема описывает все возможные квазиканонические системы счисления в кольце $S(i)$.

Теорема 1. В кольце целых алгебраических чисел $S(i)$ существуют ровно 8 бинарных квазиканонических систем счисления, а именно: системы счисления с основаниями $\alpha=-1\pm i$ и множествами цифр $\{0,1\},\{0,i\},\{0,-1\},\{0,-i\}$.

Доказательство. Заметим, что остатки от деления на число α, имеющие норму 1, можно представить в виде i^k, где $k=1;2;3;4$, а основания систем счисления запишем как $\alpha_n=(1+i)\cdot i^{n-1}$, $n=1;2;3;4$. Покажем, что справедлива следующая лемма.

Лемма 1. Пусть $\alpha\in S(i)$ является основанием бинарной системы счисления, для которой множество цифр I выбирается из чисел $r\in S(i)$, причём $\|r\|<\|\alpha\|=2$. Тогда $I=\{0,\ i^k\}$, где $k=1,2,3,4$.

Доказательство. Пусть $r=r_1+r_2\cdot i$, $\alpha=\alpha_1+\alpha_2 i$, $\beta=a+bi$. Подставляя выражения для β, α и r в формулу (1), имеем

$$\gamma=\frac{a\alpha_1+b\alpha_2-r_1\alpha_1-r_2\alpha_2}{2}+\frac{b\alpha_1-a\alpha_2+r_1\alpha_2-r_2\alpha_1}{2}i. \quad (3)$$

Поскольку γ – целое алгебраическое число поля $Q(i)$, то $\mathrm{Re}\,\gamma$ и $\mathrm{Im}\,\gamma$ должны быть целыми рациональными числами, откуда при условии, что сумма $a+b$ чётная, получаем чётность r_1+r_2, значит, $r=0$, а в случае, когда $a+b$ нечётная, получаем нечётность r_1+r_2, следовательно, в качестве остатка выбираем $r=i^k$. Тогда γ однозначно определяется из формулы (1). ■

Таким образом, показано, что в системах счисления $\{\alpha_n; I=\{0,\ i^k\}\}$ возможно однозначное представление произвольного целого гауссова числа. Рассмотрим теперь конечность представления чисел в таких системах счисления, опираясь на свойство 2.

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

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

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

$$Norm(\gamma_{m+1})=\frac{(\gamma_m-r_m)\overline{\alpha}}{2}\cdot\frac{\overline{(\gamma_m-r_m)\overline{\alpha}}}{2}=\frac{Norm(\gamma_m-r_m)}{2}.$$

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

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

которое при $r_m=0$ справедливо для всех $\gamma_m\ne 0$.

Если $r_m=i^k$, то есть $r_{m1}^2+r_{m2}^2=1$, то неравенство (4) принимает вид $(a_m+r_{m1})^2+(b_m+r_{m2})^2>2$. Оно верно для всех $\gamma_m\in Z(i),\ Norm(\gamma_m)\ge 2,\ r_m\in\{0,i^k\}$, кроме $\gamma_m=(\pm 1-2i)\cdot i^{k-1}$, $\gamma_m=-2i\cdot i^{k-1}$, $\gamma_m=(\pm 1-i)\cdot i^{k-1}$.

Рассмотрим теперь системы счисления $\{-1+i;\{0,i\}\}$ и $\{1+i;\{0,i\}\}$. В этих системах счисления неравенство (4) выполняется для всех γ_m, кроме $\gamma_m=\pm 1-2i$, $\gamma_m=-2i$, $\gamma_m=\pm 1-i$, $\gamma_m=-i$, $\gamma_m=\pm 1$. Представления для этих чисел получим, применив к ним формулы (2).

Так, в системе счисления $\{-1+i;\{0,i\}\}$:

для $\gamma_m=1-2i$ $\gamma_{m+1}=-2+i$, $\gamma_{m+2}=1+i$, $\gamma_{m+3}=-i$, $Norm(\gamma_{m+3})=1$;

для $\gamma_m=-1-2i$ $\gamma_{m+1}=-1+2i$, $\gamma_{m+2}=1$, $Norm(\gamma_{m+2})=1$;

для $\gamma_m=-2i$ $\gamma_{m+1}=-1+i$, $\gamma_{m+2}=1$, $Norm(\gamma_{m+2})=1$;

для $\gamma_m=1-i$ $\gamma_{m+1}=-1$, $Norm(\gamma_{m+1})=1$;

для $\gamma_m=-1-i$ $\gamma_{m+1}=i$, $Norm(\gamma_{m+1})=1$.

В системе счисления $\{1+i;\{0,i\}\}$:

для $\gamma_m = 1-2i$ $\gamma_{m+1} = -1-2i$, $\gamma_{m+2} = -2-i$, $\gamma_{m+3} = -2$, $\gamma_{m+4} = -1+i$, $\gamma_{m+5} = i$, $Norm(\gamma_{m+5}) = 1$;

для $\gamma_m = -1-2i$ $\gamma_{m+1} = -2-i$, $\gamma_{m+2} = -2$, $\gamma_{m+3} = -1+i$, $\gamma_{m+4} = i$, $Norm(\gamma_{m+4}) = 1$;

для $\gamma_m = -2i$ $\gamma_{m+1} = -1-i$, $\gamma_{m+2} = -1$, $\mathrm{Norm}(\gamma_{m+2}) = 1$;

для $\gamma_m = 1-i$ $\gamma_{m+1} = -i$, $Norm(\gamma_{m+1}) = 1$;

для $\gamma_m = -1-i$ $\gamma_{m+1} = -1$, $Norm(\gamma_{m+1}) = 1$.

Таким образом, доказано, что норма частного всегда меньше нормы делимого, за исключением конечного числа случаев, и, следовательно, через конечное число шагов она станет меньше либо равна 1. Во всех исключительных случаях показано, что через конечное число шагов норма частного также станет меньше либо равна 1. ■

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 $\gamma_{q+1} = \pm 1; \pm i$. Для всех этих значений γ_{q+1} легко проверить, что через конечное число шагов появится частное $\gamma_p = 0$ в системе счисления $\left\{-1+i; \{0, i\}\right\}$. Поэтому из равенств (2) вытекает однозначное разложение числа γ_0 по степеням числа $\alpha = i-1$:

- для $\gamma_{q+1} = 0$

$$\gamma_0 = r_q\alpha^q + r_{q-1}\alpha^{q-1} + \ldots + r_1\alpha + r_0;$$

- для $\gamma_{q+1} = i$

$$\gamma_0 = i\cdot\alpha^{q+1} + r_q\alpha^q + r_{q-1}\alpha^{q-1} + \ldots + r_1\alpha + r_0;$$

- для $\gamma_{q+1} = -1$

$$\gamma_0 = i\cdot\alpha^{q+2} + i\cdot\alpha^{q+1} + r_q\alpha^q + r_{q-1}\alpha^{q-1} + \ldots + r_1\alpha + r_0;$$

- для $\gamma_{q+1} = -i$

$$\gamma_0 = i\alpha^{q+5} + i\alpha^{q+4} + i\alpha^{q+3} + 0\alpha^{q+2} + i\alpha^{q+1} + r_q\alpha^q + \ldots + r_0;$$ -

для $\gamma_{q+1} = 1$

$$\gamma_0 = i\cdot\alpha^{q+3} + i\cdot\alpha^{q+2} + i\cdot\alpha^{q+1} + r_q\alpha^q + \ldots + r_0,$$

где $r_t \in \{0; i\}; \quad t = 0; 1; \ldots; q.$

Если рассмотреть систему счисления $\left\{1+i; \{0, i\}\right\}$, то при последовательном применении алгоритма деления с остатком возможно зацикливание:

- для $\gamma_{q+1} = -1$

$$\gamma_0 = -1\cdot\alpha^{q+2} + i\cdot\alpha^{q+1} + r_q\alpha^q + \ldots + r_0;$$

где $r_t \in \{0, i\}; \quad t = 0; 1; \ldots; q.$

Таким образом, в системе $\left\{1+i; \{0, i\}\right\}$ и всех эквивалентных ей системах не любое целое гауссово число допускает конечное представление. ■

Из доказанного легко получается алгоритм записи целого гауссова числа $\gamma_0 = a_0 + b_0 i;\ a_0, b_0 \in Z$ в системе счисления с основанием $\alpha = \pm i - 1$ и алфавитом $I_k = \left\{0, i^k\right\}$.

Алгоритм 1.

Шаг 1. Полагаем $p = 0$.

Шаг 2. Если для $\gamma_p = a_p + b_p i$, сумма $a_p + b_p$ чётная, то $r_p = 0$.

Если $a_p + b_p$ нечётная, то $r_p = i^k$.

Шаг 3. Вычисляем γ_{p+1} по формуле $\gamma_{p+1} = \dfrac{\left(\gamma_p - r_p\right)\overline{\alpha}}{2}$.

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

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

Сходимость данного алгоритма следует из доказательства теоремы 1.

Рассмотрим теперь арифметические операции в системах счисления, указанных в теореме. Согласно свойству 3 и доказанной теореме, достаточно рассмотреть сложение лишь для одной системы счисления, например $\left\{-1+i; \{0,1\}\right\}$. Алгоритм сложения чисел в такой системе счисления рассмотрен в работе [27].

Умножение. Реализация операции умножения даже в некоторых эквивалентных системах счисления отличается. В силу особенностей алфавита (одна из цифр является нулём), таблицы умножения для таких систем счисления сильно упрощаются, и достаточно записать разложение лишь одного числа для каждой системы счисления. Согласно свойству 3, алгоритм умножения чисел в системе счисления $\left\{\overline{\alpha}; \overline{I}\right\}$ легко получается из алгоритма умножения чисел в системе счисления $\left\{\alpha; I\right\}$, поэтому достаточно рассмотреть лишь 4 системы из 8.

Для $\left\{i-1; \{0, i\}\right\}$ $i^2 = -1 = i\alpha + i$;

для $\left\{i-1; \{0, -1\}\right\}$

$$(-1)^2 = 1 = (-1)\alpha^4 + (-1)\alpha^3 + (-1)\alpha^2 + (-1);$$

для $\left\{i-1; \{0, -i\}\right\}$

$$(-i)^2 = -1 = (-i)\alpha^2 + (-i)\alpha + (-i);$$

для $\left\{i-1; \{0,1\}\right\}$ $1^2 = 1$.

Поскольку алфавит системы счисления $\left\{\alpha; \{0, i^k\}\right\}$ состоит из цифр 0 и i^k, 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 i^k, стоящую в разряде, соответствующем α^p, к записи числа a справа добавляется p нулей. Числа, полученные при умножении на цифры единичной нормы неко-

торых разрядов, складываются последовательно по два числа в соответствии с алгоритмом сложения.

Инверсия знака. Следует отметить, что инверсия знака будет одинаковой в различных системах счисления. Поэтому достаточно рассмотреть алгоритм лишь для одной системы счисления.

Пусть представление исходного числа β в системе счисления $\{-1+i;\{0,i\}\}$ имеет вид $\beta=\sum_{k=0}^{N}a_k\alpha^k$. Тогда, учитывая формулу $-i=i\alpha^4+i\alpha^3+i\alpha^2+i$, получаем следующий алгоритм инверсии знака.

Алгоритм 2.

Шаг 1. Полагаем $k=0$.

Шаг 2. Если $-a_k=0$ или $-a_k=i$, то переходим к шагу 3.

Если $-a_k=-i$, то в текущий разряд записываем i и прибавляем i к разрядам $k+2$, $k+3$, $k+4$.

Если $-a_k=2i, 3i, \ldots,$ то раскладываем его в данной системе счисления и добавляем его к текущему представлению, начиная с разряда k, то есть действуем, как в алгоритме сложения. Переходим к шагу 3.

Шаг 3. $k=k+1$.

Если k больше длины исходного числа β и $-a_k=-a_{k+1}=-a_{k+2}=-a_{k+3}=0,$ то алгоритм закончен.

Иначе переходим к шагу 2. ■

Сходимость данного алгоритма обусловлена сходимостью алгоритма сложения, а также алгоритма представления чисел в системе счисления с основанием $\alpha=\pm i-1$ и алфавитом $I_k=\{0,i^k\}$

Квазиканонические системы счисления в $S\left(i\sqrt{2}\right)$

Кольцо $S\left(i\sqrt{2}\right)$ целых элементов поля $Q\left(i\sqrt{2}\right)$ состоит из элементов

$$z=a+bi\sqrt{2};\quad a,b\in Z.$$

При делении с остатком по норме на α, $Norm(\alpha)=2$, норма ненулевого остатка может равняться только единице. Таких остатков ровно два: $\{\pm1\}$, что в сочетании с вариантами выбора α: $\left\{\pm i\sqrt{2}\right\}$ даёт 4 потенциальных комбинации возможных оснований α и множества I, то есть 4 бинарных квазиканонических системы счисления. Учитывая свойство 3, получаем, что в кольце $S\left(i\sqrt{2}\right)$ достаточно исследовать лишь одну систему счисления, а именно: $\left\{i\sqrt{2};\{0,-1\}\right\}$.

Следующая теорема описывает все возможные квазиканонические системы счисления в кольце $S\left(i\sqrt{2}\right)$.

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

Доказательство проводится по схеме доказательства теоремы 1.

Из доказательства теоремы 2 легко получается алгоритм записи целого алгебраического числа $\gamma_0=a_0+b_0i\sqrt{2};\ a_0,b_0\in Z$ в системе счисления с основанием $\alpha=\pm i\sqrt{2}$ и алфавитом $I_n=\left\{0,(-1)^n\right\}$.

Алгоритм 3.

Шаг 1. Полагаем $p=0$.

Шаг 2. Если для $\gamma_p=a_p+b_pi\sqrt{2}$ a_p – чётное, то $r_p=0$.

Если a_p – нечётное, то $r_p=(-1)^k$.

Шаг 3. Вычисляем γ_{p+1} по формуле $\gamma_{p+1}=\dfrac{(\gamma_p-r_p)\overline{\alpha}}{2}$.

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

Если $\gamma_{p+1}\neq0$, то $p=p+1$ и переходим к шагу 2. ■

Рассмотрим теперь арифметические операции в системах счисления, указанных в теореме. Согласно свойству 3 и доказанной теореме, достаточно рассмотреть сложение лишь для одной системы счисления, например, $\left\{i\sqrt{2};\{0,-1\}\right\}$.

Сложение. При сложении двух чисел в системе счисления $\left\{i\sqrt{2};\{0,-1\}\right\}$, иначе говоря, двух многочленов, получаем новый многочлен с коэффициентами 0, -1 или -2. При этом, поскольку $-2=(-1)\alpha^4+(-1)\alpha^2$, слагаемое вида $-2\alpha^t$ преобразуется по формуле

$$-2\alpha^t=\left((-1)\alpha^4+(-1)\alpha^2\right)\alpha^t=(-1)\alpha^{t+4}+(-1)\alpha^{t+2}.$$

В некоторых случаях преобразование суммы двух чисел с использованием последней формулы приводит к многочлену бесконечно большой степени с повторяющимся блоком коэффициентов (зацикливанию).

Очевидно, что любой многочлен от α, корнем которого является $\alpha=i\sqrt{2}$, также будет обращаться в нуль.

Таким образом, любой «нулевой» многочлен должен делиться на выражение

$$\left(\alpha-i\sqrt{2}\right)\left(\alpha+i\sqrt{2}\right)=\alpha^2+2.$$

Из сказанного выше следует алгоритм сложения двух чисел, записанных в системы счисления с основанием $i\sqrt{2}$.

Алгоритм 4.

Шаг 1. Складываем по разрядам два данных числа. При этом в записи суммы может присутствовать цифра -2, не входящая в алфавит системы счисления. Тогда переходим к шагу 2. Если таковой цифры не встретилось, то получаем искомую сумму.

Шаг 2. Используем формулу из таблицы сложения для каждой –2 в записи числа (по одному разу для каждого разряда), при этом в записи может появиться и цифра -3. После этого, двигаясь от нулевого разряда, находим первую цифру справа, большую единицы. Эта цифра и все другие, стоящие слева от неё, определяют некоторый многочлен $P(x)$. Если $P(x)$ делится на $(-1)x^2+(-2)$ без остатка, то считаем его «нулевым», если с остатком, то повторяем шаг 2, учитывая, что

$$-3=(-1)\alpha^4+(-1)\alpha^2+(-1)=(-1)0(-1)0(-1)_\alpha.$$

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

Умножение. Согласно свойству 3, алгоритм умножения чисел в системе счисления $\{\overline{\alpha};\overline{I}\}$ легко получается из алгоритма умножения чисел в системе счисления $\{\alpha;I\}$, поэтому достаточно рассмотреть лишь 2 системы из 4.

Для $\left\{i\sqrt{2};\{0,-1\}\right\}$ $(-1)^2=1=(-1)\alpha^2+(-1)$;

для $\left\{i\sqrt{2};\{0,1\}\right\}$ $(1)^2=1$.

Поскольку «алфавит» системы счисления $\left\{\alpha;\left\{0,(-1)^k\right\}\right\}$ состоит из цифр 0 и $(-1)^k$, 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 $(-1)^k$, стоящую в разряде, соответствующем α^p, к записи числа a справа добавляется p нулей. Числа, полученные при умножении на цифры единичной нормы некоторых разрядов, складываются последовательно по два числа в соответствии с алгоритмом сложения.

Инверсия знака. Следует отметить, что инверсия знака будет одинаковой в различных системах счисления. Поэтому достаточно рассмотреть алгоритм лишь для одной системы счисления.

Пусть представление исходного числа β в системе счисления $\left\{i\sqrt{2};\{0,-1\}\right\}$ имеет вид $\beta=\sum_{k=0}^{N}a_k\alpha^k$, то есть $-\beta=\sum_{k=0}^{N}(-a_k)\alpha^k$. Тогда, учитывая формулу $1=(-1)\alpha^2+(-1)$, получаем следующий алгоритм инверсии знака.

Алгоритм 5.

Шаг 1. Полагаем $k=0$.

Шаг 2. Если $-a_k=0$ или $-a_k=-1$, то переход к шагу 3.

Если $-a_k=1$, то в текущий разряд записываем -1 и прибавляем -1 к разряду $k+2$. Переходим к шагу 3.

Шаг 3. $k=k+1$.

Если k больше длины исходного числа β, то алгоритм закончен.

Иначе переходим к шагу 2. ■

Сходимость всех алгоритмов для кольца $S\left(i\sqrt{2}\right)$ обосновывается аналогично сходимости алгоритмов для кольца $S(i)$.

Квазиканонические системы счисления в $S\left(i\sqrt{7}\right)$

Кольцо $S\left(i\sqrt{7}\right)$ целых элементов поля $Q\left(i\sqrt{7}\right)$ состоит из элементов

$$z=\frac{a+bi\sqrt{7}}{2};\quad a\equiv b\,(\mathrm{mod}\,2),\ a,b\in Z.$$

При делении с остатком по норме на α, $Norm(\alpha)=2$, норма ненулевого остатка может равняться только единице. Таких остатков ровно два: $\{\pm1\}$, что в сочетании с вариантами выбора α: $\left\{\frac{\pm1\pm i\sqrt{7}}{2}\right\}$ даёт 8 потенциальных комбинаций возможных оснований α и множества I, то есть, 8 бинарных квазиканонических систем счисления. Учитывая свойство 3, получаем, что в кольце $S(i)$ достаточно исследовать лишь две системы счисления, а именно:

$$\left\{\frac{1+i\sqrt{7}}{2};\{0,-1\}\right\}\ \text{и}\ \left\{\frac{-1+i\sqrt{7}}{2};\{0,-1\}\right\}.$$

Следующая теорема описывает все возможные квазиканонические системы счисления в кольце $S\left(i\sqrt{7}\right)$.

Теорема 3. В кольце целых алгебраических чисел $S\left(i\sqrt{7}\right)$ существуют ровно 8 бинарных квазиканонических систем счисления, а именно: системы счисления с основаниями $\alpha=\frac{\pm1\pm i\sqrt{7}}{2}$ и множествами цифр $\{0,1\},\{0,-1\}$.

Доказательство проводится по схеме доказательства теоремы 1.

Из доказательства теоремы 3 легко получается алгоритм записи целого алгебраического числа $\gamma_0=\frac{a_0+b_0i\sqrt{7}}{2};\ a_0,b_0\in Z$, в системе счисления с основанием $\alpha=\frac{\pm1\pm i\sqrt{7}}{2}$ и алфавитом $I_n=\left\{0;(-1)^k\right\}$.

Алгоритм 6.

Шаг 1. Полагаем $p=0$.

Шаг 2. Если для

$$\gamma_p=\frac{a_p+b_pi\sqrt{7}}{2}\quad \alpha_1a_p-\alpha_2b_p\equiv0\,(\mathrm{mod}\,4),$$

то $r_p = 0$.

Если $\alpha_1 a_p - \alpha_2 b_p \equiv 2 \pmod 4$, то $r_p = (-1)^k$.

Переходим к шагу 3.

Шаг 3. Вычисляем γ_{p+1} по формуле $\gamma_{p+1} = \dfrac{(\gamma_p - r_p)\bar{\alpha}}{2}$.

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

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

Рассмотрим теперь арифметические операции в таких системах счисления. Согласно свойству 3 и доказанной теореме, достаточно рассмотреть сложение лишь для двух систем счисления, например:

$$\left\{\frac{-1+i\sqrt{7}}{2};\{0,-1\}\right\} \text{ и } \left\{\frac{1+i\sqrt{7}}{2};\{0,-1\}\right\}.$$

Сложение. При сложении двух чисел в системе счисления $\left\{\dfrac{-1+i\sqrt{7}}{2};\{0,-1\}\right\}$, иначе говоря, двух многочленов, получаем новый многочлен с коэффициентами 0, -1 или -2. При этом, поскольку $-2 = (-1)\alpha^3 + (-1)\alpha$, то слагаемое вида $-2\alpha^t$ преобразуется по формуле

$$-2\alpha^t = \left((-1)\alpha^3 + (-1)\alpha\right)\alpha^t = (-1)\alpha^{t+3} + (-1)\alpha^{t+1}.$$

Замечание. В некоторых случаях преобразование суммы двух чисел с использованием последней формулы приводит к тому, что алгоритм не сходится за конечное число шагов. Но данный недостаток можно компенсировать следующим образом.

Очевидно, что любой многочлен от α, корнем которого является $\alpha = \dfrac{-1+i\sqrt{7}}{2}$, также будет обращаться в нуль.

Таким образом, любой «нулевой» многочлен должен делиться на выражение

$$\left(\alpha - \frac{-1+i\sqrt{7}}{2}\right)\left(\alpha - \frac{-1-i\sqrt{7}}{2}\right) = \alpha^2 + \alpha + 2.$$

При сложении двух чисел в системе счисления $\left\{\dfrac{1+i\sqrt{7}}{2};\{0,-1\}\right\}$ получаем новый многочлен с коэффициентами 0, -1 или -2. В этом случае любой «нулевой» многочлен должен делиться на выражение

$$\left(\alpha - \frac{1+i\sqrt{7}}{2}\right)\left(\alpha - \frac{1-i\sqrt{7}}{2}\right) = \alpha^2 - \alpha + 2.$$

Из сказанного выше следует алгоритм сложения двух чисел, записанных в системе счисления с основанием $\dfrac{\pm 1 + i\sqrt{7}}{2}$.

Алгоритм 7.

Шаг 1. Складываем по разрядам два данных числа. При этом в записи суммы может присутствовать цифра -2, не входящая в алфавит систем счисления. Тогда переходим к шагу 2. Если таковой цифры не встретилось, то получаем искомую сумму.

Шаг 2. Используем формулу из таблицы сложения для каждой -2 в записи числа (по одному разу для каждого разряда), при этом в записи может появиться и цифра -3. После этого, двигаясь от нулевого разряда, находим первую цифру справа, большую единицы. Эта цифра и все другие, стоящие слева от неё, определяют некоторый многочлен $P(x)$. Если $P(x)$ делится без остатка на $(-1)x^2 + (-1)x + (-2)$ для системы счисления $\left\{\dfrac{-1+i\sqrt{7}}{2};\{0,-1\}\right\}$ или на $(-1)x^2 + x + (-2)$ для системы счисления $\left\{\dfrac{1+i\sqrt{7}}{2};\{0,-1\}\right\}$, то считаем его «нулевым». Если с остатком, то повторяем шаг 2.

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

Умножение. Согласно свойству 3, алгоритм умножения чисел в системе счисления $\{\bar{\alpha}, \bar{I}\}$ легко получается из алгоритма умножения чисел в системе счисления $\{\alpha, I\}$, поэтому достаточно рассмотреть лишь 4 системы из 8.

Для $\left\{\dfrac{-1+i\sqrt{7}}{2};\{0,-1\}\right\}$

$(-1)^2 = 1 = (-1)\alpha^2 + (-1)\alpha + (-1)$;

для $\left\{\dfrac{-1+i\sqrt{7}}{2};\{0,1\}\right\}$ $(1)^2 = 1$;

для $\left\{\dfrac{1+i\sqrt{7}}{2};\{0,-1\}\right\}$

$(-1)^2 = 1 = (-1)\alpha^3 + (-1)\alpha + (-1)$;

для $\left\{\dfrac{1+i\sqrt{7}}{2};\{0,1\}\right\}$ $(1)^2 = 1$.

Поскольку алфавит системы счисления $\left\{\alpha;\left\{0,(-1)^k\right\}\right\}$ состоит из цифр 0 и $(-1)^k$, 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 $(-1)^k$, стоящую в разряде, соответствующем α^p, к записи числа *a* справа добавляется *p* нулей. Числа, полученные при умножении на цифры единичной нормы некоторых разрядов, складываются последовательно по два числа в соответствии с алгоритмом сложения.

Инверсия знака. Следует отметить, что инверсия знака будет одинаковой в различных системах счисления. Поэтому достаточно рассмотреть алгоритм лишь для одной системы счисления.

Пусть представление исходного числа β в системе счисления $\{\alpha;\{0,-1\}\}$ имеет вид $\beta=\sum_{k=0}^{N}a_k\alpha^k$, то есть $-\beta=\sum_{k=0}^{N}(-a_k)\alpha^k$. Тогда, учитывая формулу $1=(-1)\alpha^2+(-1)$, получаем следующий алгоритм инверсии знака.

Алгоритм 8.

Шаг 1. Полагаем k=0.

Шаг 2. Если $-a_k=0$ или $-a_k=-1$, то переход к шагу 3.

Если $-a_k=1$, то в текущий разряд записываем -1 и прибавляем -1 к разрядам k+1 и k+2 для системы счисления $\left\{\frac{-1+i\sqrt{7}}{2};\{0,-1\}\right\}$ (прибавляем -1 к разрядам $k+1$ и $k+3$ для системы счисления $\left\{\frac{1+i\sqrt{7}}{2};\{0,-1\}\right\}$).

Если $-a_k$= –2,–3,…, то раскладываем его в данной системе счисления и добавляем его к текущему представлению, начиная с разряда k, то есть действуем, как в алгоритме сложения. Переходим к шагу 3.

Шаг 3. k=k+1.

Если k больше длины исходного числа β и $a_{k+1}=0,\quad a_{k+2}=0$, то алгоритм закончен.

Иначе переходим к шагу 2. ■

Сходимость всех алгоритмов для кольца $S\left(i\sqrt{7}\right)$ обосновывается аналогично сходимости алгоритмов для кольца $S(i)$**.**

Заключение

В работе подробно рассмотрены алгоритмы представления целых элементов (в том числе и обычных целых чисел) и реализации основных арифметических операций в кольцах целых алгебраических чисел мнимых квадратичных полей.

В отличие от метода работы [26], для представления чисел в системах счисления с основаниями в виде целого алгебраического числа используется факт наличия в кольцах целых алгебраических чисел квадратичных полей алгоритма деления с остатком по норме.

Предложенный подход достаточно легко обобщается на случай других квадратичных расширений, для элементов которых есть алгоритмы деления с остатком по норме и на случай небинарных систем счисления.

Рассмотренный подход обеспечивает дополнительную криптостойкость системы кодирования по методу работы [28] или новые алгоритмы параллельного вычисления произведения больших целых чисел методом, описанным в монографии [25].

Благодарности

Работа выполнена при финансовой поддержке РФФИ (гранты 09-01-0511а, 12-01-00822а, 12-01-31316 мол а).

Литература

1. **Grunwald, V.** Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale) / V. Grunvald // Giornale di matematiche di Battaglini. – 1885 – N 23 – P. 203-221.
2. **Knuth, D. E.** The Art of Computer Programming. Vol. 2 Semi-numerical Algorithms / D.E. Knuth. – 3rd edition. – London: Addison Wesley, 1998.
3. **Katai, I.** Canonical number systems for complex integers / I. Katai, J. Szabo // Acta Sci. Math. (Szeged). – 1975. – Vol. 37 – P. 255-260.
4. **Kovacs, B.** Canonical number systems in algebraic number fields / B. Kovacs // Acta Math. Hungar. – 1981. – Vol. 37. – P. 405-407.
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. **Gilbert, W.J.** Radix representations of quadratic fields / W.J. Gilbert // J. Math. Anal. Appl. – 1981. – Vol. 83 – P. 264-274.
8. **Akiyama, S.** Topological properties of two-dimensional number systems / S. Akiyama, J.M. Thuswaldner // J. Th´eor. Nombres Bordeaux. – 2000. – Vol. 12. – P. 69-79.
9. **Akiyama, S.** On the topological structure of fractal tilings generated by quadratic number systems / S. Akiyama, J.M. Thuswaldner // Comput. Math. Appl. – 2005. – Vol. 49, N 9-10 – P. 1439-1485.
10. **Katai, I.** Number systems and fractal geometry / I. Katai – Jannus Pannonius University Pecs, 1995.
11. **Grochenig, K.** Multiresolution analysis, Haar bases, and self-similar tilings of Rn. / K. Grochenig, W. R. Madych // IEEE Trans. Inform. Theory – 1992 – Vol. 38 – P. 556-568.
12. **Gilbert, W. J.** Complex numbers with three radix representations / W. J. Gilbert // Canadian J. Math. – 1982. – Vol. 34 – P. 1335-1348.
13. **Indlekofer, K.-H.** Some remarks on generalized number systems / K.-H. Indlekofer, I. Katai, P. Racsko // Acta Sci. Math. (Szeged) – 1993. – Vol. 57 – P. 543-553.
14. **Katai, I.** On number systems in algebraic number fields / I. Katai, I. Kornyei // Publ. Math. Debrecen – 1992. – Vol. 41. – P. 289-294.
15. **Praggastis, B.** Numeration systems and Markov partitions from self-similar tilings / B. Praggastis // Trans. Amer. Math. Soc. – 1999. – Vol. 351, N 8. – P. 3315-3349.
16. **Duvall, P.** The Hausdorff dimension of the boundary of a self-similar tile / P. Duvall, J. Keesling, A. Vince // J. London Math. Soc. – 2000. – Vol. 61. – P. 748-760.
17. **Gilbert, W.J.** Complex bases and fractal similarity / W.J. Gilbert // Ann. sc. math. Quebec. – 1987. – Vol. 11, N 1 – P. 65-77.
18. **Scheicher, K.** Canonical number systems, counting automata and fractals / K. Scheicher, J.M. Thuswaldner // Math. Proc. Cambridge Philos. Soc. – 2002. – Vol. 133, N 1. – P. 163-182.
19. **Veerman, J.J.P.** Hausdorff dimension of boundaries of self-affine tiles in Rn. / J.J.P. Veerman // Bol. Mex. Mat. – 1998. – Vol. 3, N. 4. – P. 1-24.

20. **Wang, Y.** Self-affine tiles / Y. Wang // Advances in Wavelet, Springer. – 1998. – P. 261-285.
21. **Solomyak, B.** Dynamics of self-similar tilings / B. Solomyak // Ergodic Theory Dynam. Systems. – 1997. – Vol 17, N 3. – P. 695-738.
22. **Bratteli, O.** Iterated function systems and permutation representations of the Cuntz algebra / O. Bratteli, P.E.T. Jorgensen // Mem. Amer. Math. Soc. – 1999. – Vol. 139, N 663.
23. **Wang, Y.** Wavelets, tiling, and spectral sets / Y. Wang // Duke Math. J. – 2002. – Vol. 114, N 1 – P. 43-57.
24. **Боревич, З.И.** Теория чисел / З.И. Боревич, И.Р. Шафаревич – М.: Наука, 1985. – 504 с.
25. **Чернов, В.М**. Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов – М.: ФИЗМАТЛИТ, 2007 – 264 с.
26. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Univ. Sci. Budapest, Sect. Comp. – 2001. – Vol. 20 – P. 195-206.
27. **Богданов П.С.** О представлении целых гауссовых чисел в системе счисления Пенни / П.С. Богданов // Компьютерная оптика. – 2010. – Т. 34, № 4. – С. 561-566.
28. **Fedoseev, V.** Cryptography and Canonical Number Systems in Quadratic Fields / V. Fedoseev, V. Chernov // Machine Graphic & Vision. – 2006. – Vol. 15, N ¾. – P. 363-372.

References

1. **Grunwald, V.** Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale) / V. Grunvald // Giornale di matematiche di Battaglini. – 1885. – N 23. – P. 203-221.
2. **Knuth, D. E.** The Art of Computer Programming. Vol. 2 Semi-numerical Algorithms / D. E. Knuth. – 3rd edition – London: Addison Wesley, 1998.
3. **Katai, I.** Canonical number systems for complex integers / I. Katai, J. Szabo // Acta Sci. Math. (Szeged) – 1975. – Vol. 37. – P. 255-260.
4. **Kovacs, B.** Canonical number systems in algebraic number fields / B. Kovacs // Acta Math. Hungar. – 1981. – Vol. 37. – P. 405-407.
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. **Gilbert, W.J.** Radix representations of quadratic fields / W.J. Gilbert // J. Math. Anal. Appl. – 1981. – Vol. 83 – P. 264-274.
8. **Akiyama, S.** Topological properties of two-dimensional number systems / S. Akiyama, J.M. Thuswaldner // J. Th´eor. Nombres Bordeaux – 2000. – Vol. 12. – P. 69-79.
9. **Akiyama, S.** On the topological structure of fractal tilings generated by quadratic number systems / S. Akiyama, J.M. Thuswaldner // Comput. Math. Appl. – 2005. – Vol. 49, N 9-10. – P. 1439-1485.
10. **Katai, I.** Number systems and fractal geometry / I. Katai – Jannus Pannonius University Pecs, 1995.
11. **Grochenig, K.** Multiresolution analysis, Haar bases, and self-similar tilings of Rn. / K. Grochenig, W. R. Madych // IEEE Trans. Inform. Theory. – 1992. – Vol. 38 – P. 556-568.
12. **Gilbert, W. J.** Complex numbers with three radix representations / W. J. Gilbert // Canadian J. Math. – 1982. – Vol. 34. – P. 1335-1348.
13. **Indlekofer, K.-H.** Some remarks on generalized number systems / K.-H. Indlekofer, I. Katai, P. Racsko // Acta Sci. Math. (Szeged). – 1993. – Vol. 57. – P. 543-553.
14. **Katai, I.** On number systems in algebraic number fields / I. Katai, I. Kornyei // Publ. Math. Debrecen. – 1992. – Vol. 41 – P. 289-294.
15. **Praggastis, B.** Numeration systems and Markov partitions from self-similar tilings / B. Praggastis // Trans. Amer. Math. Soc. – 1999. – Vol. 351, N 8. – P. 3315-3349.
16. **Duvall, P.** The Hausdorff dimension of the boundary of a self-similar tile / P. Duvall, J. Keesling, A. Vince // J. London Math. Soc. – 2000. – Vol. 61 – P. 748-760.
17. **Gilbert, W. J.** Complex bases and fractal similarity / W.J. Gilbert // Ann. sc. math. Quebec. – 1987. – Vol. 11, N 1 – P. 65-77.
18. **Scheicher, K.** Canonical number systems, counting automata and fractals / K. Scheicher, J. M. Thuswaldner // Math. Proc. Cambridge Philos. Soc. – 2002 – Vol. 133, N 1 – P. 163-182.
19. **Veerman, J. J. P.** Hausdorff dimension of boundaries of self-affine tiles in Rn. / J.J.P. Veerman // Bol. Mex. Mat. – 1998. – Vol. 3, N. 4. – P. 1-24.
20. **Wang, Y.** Self-affine tiles / Y. Wang // Advances in Wavelet, Springer. – 1998. – P. 261-285.
21. **Solomyak, B.** Dynamics of self-similar tilings / B. Solomyak // Ergodic Theory Dynam. Systems. – 1997. – Vol 17, N 3. – P. 695-738.
22. **Bratteli, O.** Iterated function systems and permutation representations of the Cuntz algebra / O. Bratteli, P.E.T. Jorgensen // Mem. Amer. Math. Soc. – 1999. – Vol. 139, N 663.
23. **Wang, Y.** Wavelets, tiling, and spectral sets / Y. Wang // Duke Math. J. – 2002. – Vol. 114, N 1. – P. 43-57.
24. **Borevich, Z.I.** Number theory / Z.I. Borevich, I.R. Shafarevich – Moscow.: “Nauka” Publisher, 1985. – 504 p. – (in Russian).
25. **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).
26. **Kovacs, A.** Generalized binary number system / A. Kovacs // Annales Univ. Sci. Budapest, Sect. Comp. – 2001. – Vol. 20. – P. 195-206.
27. **Bogdanov, P.S.** Gaussian integers representation in Pitti’s number system / P.S. Bogdanov // Computer Optics. – 2010. – Vol. 34, N 4. – P. 561-566.
28. **Fedoseev, V.** Cryptography and Canonical Number Systems in Quadratic Fields / V. Fedoseev, V. Chernov // Machine Graphic & Vision. – 2006. – Vol. 15, N ¾. – P. 363-372.

CLASSIFICATION OF BINARY QUASICANONICAL NUMBER SYSTEMS IN IMAGINARY QUADRATIC FIELDS

P. S. Bogdanov, V. M. Chernov
Image Processing Systems Institute of the RAS

Abstract

In this paper all possible binary 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 these number systems are synthesized.

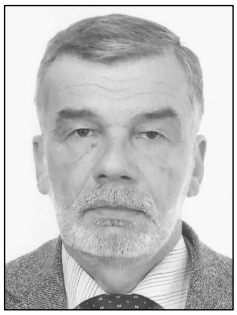
Key words: canonical numerical system, norm division with remainder, quasicanonical numerical system, imaginary quadratic fields.

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) is 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 Mikhailovich Chernov (b. 1949) is mathematician, doctor of physical and mathematical sciences. Chief researcher of Image Processing Systems Institute of the RAS. Professor of department of Geo-Information Science and Information Security of S. P. Korolyov Samara State Aerospace University (SSAU). Research interests are algebraic methods in digital signal processing, cryptography, computer arithmetic.

Поступила в редакцию 18 октября 2012 г.