ЧИСЛЕННЫЕ МЕТОДЫ И АНАЛИЗ ДАННЫХ

«ЭКЗОТИЧЕСКИЕ» БИНАРНЫЕ СИСТЕМЫ СЧИСЛЕНИЯ ДЛЯ КОЛЕЦ ЦЕЛЫХ ЧИСЕЛ ГАУССА И ЭЙЗЕНШТЕЙНА

В.М. Чернов[1, 2]

[1] *ИСОИ РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН, 443001, Россия, г. Самара, ул. Молодогвардейская, д. 151,*

[2] *Самарский национальный исследовательский университет имени академика С.П. Королёва, 443086, Россия, г. Самара, Московское шоссе, д 34*

Аннотация

В работе рассматриваются нестандартные бинарные системы счисления для колец целых чисел Гаусса и Эйзенштейна. Принципиальным отличием («экзотичностью») таких систем счисления от канонических систем счисления И. Катаи для квадратичных полей является использование в качестве бинарного «цифрового алфавита» двухэлементного множества, не содержащего числового нуля.

В работе синтезируются также алгоритмы представления чисел в рассматриваемой системе счисления и характеризуются возможности эффективной реализации арифметических операций.

Ключевые слова: системы счисления в квадратичных кольцах, кольца целых чисел Гаусса и Эйзенштейна, машинная арифметика.

Цитирование: **Чернов, В.М.** «Экзотические» бинарные системы счисления для колец целых чисел Гаусса и Эйзенштейна / В.М. Чернов // Компьютерная оптика. – 2018. – Т. 42, № 6. – С. 1068-1073. – DOI: 10.18287/2412-6179-2018-42-6-1068-1073.

Введение

Системы счисления с базисом, порожденным последовательностью иррациональных чисел, как математический объект рассматривались, по всей видимости, впервые в работе [1] Дж. Бергмана (1957). По крайней мере именно на эту работу как приоритетную ссылаются чаще всего.

Фактически в цитированной работе неявно рассматривались более общая задача представления элементов кольца целых элементов $\mathbf{Z}\left(\sqrt{5}\right)$ квадратичного поля $\mathbf{Q}\left(\sqrt{5}\right)$, то есть подмножества элементов

$$\left\{z = x + y\sqrt{5} \in \mathbf{Q}\left(\sqrt{5}\right) : Norm\, z = x^2 - 5y^2, Tr\, z = 2x \in \mathbf{Z}\right\},$$

в форме

$$z = \sum_{k=u(z)}^{v(z)} \xi_k \omega^k, \qquad (1)$$

где $\omega = \phi$ («фи») – так называемое «золотое сечение»: а «цифры» $\xi_k \in \Lambda = \{0, 1\}$.

Такая система счисления с основанием ϕ получила в англоязычной литературе название «Phi number system» или «Golden ratio number system», а в русскоязычной литературе числовые последовательности «цифр» ξ_k, ассоциированные с (1), часто называют «кодами золотого сечения» [2]. Первоначально эти системы использовались в приложениях, в частности, для синтеза *отказоустойчивых* арифметических устройств. С развитием аппаратных возможностей вычислительной математики такие системы счисления [3 – 5] стали применяться и в криптографии, цифровой обработке сигналов и изображений [6 – 8].

Напомним некоторые теоретические сведения.

Пусть целое число d *свободно от квадратов.* Пусть далее $\mathbf{Z}(\sqrt{d})$ – кольцо целых квадратичных чисел поля $\mathbf{Q}(\sqrt{d})$, то есть чисел $z = a + b\sqrt{d}$ с условиями:

$$Norm(z) = a^2 - b^2 d \in \mathbf{Z}, Tr(z) = 2a \in \mathbf{Z}.$$

Как известно,

$$\mathbf{Z}(\sqrt{d}) = \\ = \begin{cases} z : z = a + b\sqrt{d}; a, b \in \mathbf{Z} \text{ при } d \neq 1 (\mathrm{mod}\, 4), \\ z : z = {a + b\sqrt{d}}\big/{2}; a \equiv b (\mathrm{mod}\, 2) \text{ при } d \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

Систематическое исследование позиционных систем счисления в общем случае колец целых элементов $\mathbf{Z}\left(\sqrt{d}\right)$ квадратичных полей $\mathbf{Q}\left(\sqrt{d}\right)$ началось с работ И. Катаи, Й. Сабо и Б. Ковача (в частности, [10]), опубликованных в малочитаемых венгерских журналах, где было введено понятие *канонической системы счисления* в $\mathbf{Z}\left(\sqrt{d}\right)$ и получена их классификация в зависимости от связи d, α и *алфавита цифр* $\Lambda \subset \mathbf{Z}$. В работе [11] автором было обобщено понятие канонической системы *счисления до квазиканонической системы счисления* путем расширения допустимого множества цифр до множества $\Lambda \subset \mathbf{Z}\left(\sqrt{d}\right)$. Другими словами, в качестве цифрового множества Λ рассматривались не только *целые рациональные* числа (т.е. «обычные» целые), но и целые элементы квадратичного поля $\mathbf{Q}\left(\sqrt{d}\right)$.

Цифры ξ_k представления (1) определяются в общем случае либо посредством нелинейного рекуррентного процесса [12], либо, что возможно далеко не во всех квадратичных кольцах, с помощью алгоритма

деления с остатком [11]. Заметим, что и для канонических, и для квазиканонических систем счисления цифры ξ_k подчиняются условию $0 \le \xi_k < Norm\,\omega$.
Иными словами, для построения, например, *бинарных* систем счисления требовалось существование в $\mathbf{Z}\left(\sqrt{d}\right)$ элемента α с условием $Norm\,\omega = 2$.

В связи с этим «экзотичность» рассматриваемых бинарных систем счисления, вынесенная в заголовок статьи, определяется следующими факторами.

- В полях $\mathbf{Q}\left(\sqrt{-1}\right)$, $\mathbf{Q}\left(\sqrt{-3}\right)$ нормы оснований ω систем счисления равны (+1).
- Алфавитами «цифр» в обоих случаях является множество $\Lambda = \{-1, +1\}$ и $0 \notin \Lambda$.
- Рассматриваемые системы счисления являются, как и Phi-система, *избыточными* (то есть представление элемента соответствующего кольца квадратичных целых в форме (1) не является однозначным).

Заметим, что последнее свойство для Phi-системы счисления рассматривалось как аргумент, обеспечивающий *отказоустойчивость* ассоциированных кодов машинной арифметики (отказы одного или нескольких триггеров возможно компенсировать переходом к эквивалентному кодовому представлению числа). Поэтому вводимые ниже «экзотические» бинарные системы счисления (далее – ЭСЧ) для целых чисел Гаусса и Эйзенштейна могут также, в известной мере, решить проблему отказоустойчивости, причем с помощью более простых программных средств.

1. Некоторые теоретические сведения

Определение 1.1. Говорят, что в кольце $\mathfrak{A}$ имеет место алгоритм деления с остатком, если на отличных от нуля элементах z кольца определена целочисленная неотрицательная функция $v(z)$ так, что выполняются следующие условия:

1) если z делится на w, то $v(z) \ge v(w)$;
2) для любых элементов z и $w \ne 0$ кольца $\mathfrak{A}$ существуют такие $\gamma, \rho \in \mathfrak{A}$, что $z = w\gamma + \rho$, причем либо $\rho = 0$, либо $v(\rho) < v(w)$.

Кольцо $\mathfrak{A}$ называется в этом случае *евклидовым.*

Если в кольце $\mathbf{Z}\left(\sqrt{d}\right)$ имеет место алгоритм деления с остатком, то метод определения цифр в представлении (1) элемента $z \in \mathbf{Z}\left(\sqrt{d}\right)$ в системе счисления с основанием ω полностью аналогичен методу определения цифр в g-ичной позиционной системе счисления для обычных целых чисел.

При $d < 0$ (т.е. для *мнимых* квадратичных колец целых $\mathbf{Z}\left(\sqrt{d}\right)$) алгоритм деления с остатком (относительно $\nu(z) = Norm\,z$) имеет место [13] только при $d = -1, -2, -3, -7, -11$.

При $d = -1, -2, -7$ в кольцах $\mathbf{Z}\left(\sqrt{d}\right)$ существуют элементы с условием $Norm\,\omega = 2$ и, как следствие, *бинарные* канонические системы счисления И. Катаи.

В частности, для $\mathbf{Z}(i) = \mathbf{Z}\left(\sqrt{-1}\right)$ существует «каноническая» система счисления [10] с множеством цифр $\Lambda = \{0, 1\}$ и основанием

$$\omega = -1 + i,\ Norm\,\omega = 2.$$

Поэтому вводимая ниже бинарная система счисления для $\mathbf{Z}(i)$ может рассматриваться как альтернатива канонической системе счисления Пенни [3].

В кольце $\mathbf{Z}\left(\sqrt{-3}\right)$ нет элементов ω таких, что $Norm\,\omega = 2$. Поэтому ни канонических бинарных, ни квазиканонических бинарных систем счисления в этом кольце нет (хотя есть тернарные [14]). В силу этого вводимая ниже бинарная система счисления представляется новой или малоизученной.

В кольце $\mathbf{Z}\left(\sqrt{-11}\right)$ нет элементов

$$\omega \in \mathbf{Z}\left(\sqrt{-11}\right) \setminus \mathbf{Z};\ Norm\,\omega \in \{1, 2\}.$$

Поэтому в этом кольце нет ни *бинарных* канонических, ни квазиканонических систем счисления, хотя есть тернарные системы счисления [14].

2. «Экзотическая» бинарная система счисления в кольце целых Гауссовых чисел

Введем обозначения. Пусть $\mathbf{Z}(i)$ – кольцо целых Гауссовых чисел:

$$\mathbf{Z}(i) = \left\{z = x + y\omega;\ x, y \in \mathbf{Z};\ \omega \doteq i,\ i^2 = -1\right\};$$

$$\Lambda = \{-1, +1\},$$

$$\nu(z) = Norm\,z = Norm(x + y\omega) = x^2 + y^2.$$

<u>*2.1.Представление целых Гауссовых чисел в ЭСЧ*</u>

Утверждение 2.1. Для $z \in \mathbf{Z}(i)$, или $\mathrm{Re}(z) \ne 0$ справедливо неравенство

$$\nu(z) > \begin{cases} \nu(z-1) \text{ при } \mathrm{Re}(z) > \dfrac{1}{2}, \\ \nu(z+1) \text{ при } \mathrm{Re}\ (z) < -\left(\dfrac{1}{2}\right). \end{cases}$$

А при $\mathrm{Re}(z) = 0$ справедливо равенство

$$\nu(z \pm 1) = \nu(z).$$

Доказательство. Непосредственная проверка.

Следствие 2.1. Для элементов $z \in \mathbf{Z}(i)$ справедливы представления (1) в форме

$$z = \sum_{k=0}^{\nu(z)} \xi_k \omega^k, \tag{2}$$

где $\omega = i$, $\xi_k \in \Lambda = \{-1, +1\}$.

Доказательство. Метод построения представления (2), допуская известную терминологическую вольность, будем называть алгоритмом.

(а) Пусть $\mathrm{Re}(z) \ne 0$. Положим $z_0 = z \in \mathbf{Z}(i)$. Выберем $\xi_0 \in \Lambda$ таким образом, чтобы согласно Утверждению 2.1 выполнялось неравенство

$\nu\left(z-\xi_0\right)<\nu\left(z\right)$.

Далее,

$z=\left(z-\xi_0\right)+\xi_0=\left(\left(z-\xi_0\right)\omega^{-1}\right)\omega+\xi_0$.

И так как

$z=\left(z-\xi_0\right)+\xi_0$, а $\nu\left(\omega\right)=\nu\left(\omega^{-1}\right)=1$,

то, полагая $z_1\doteq((z-\xi_0)\omega^{-1})$, получаем $\nu(z_1)<\nu(z)$.

(б) Пусть $\mathrm{Re}(z)=0$, $z\neq 0$. Положим

$z_0^*=z_0\omega^{-1}$ и уже $\mathrm{Re}\left(z_0^*\right)\neq 0$.

И так как $z_0=z_0^*\omega$, то для элемента z_0^* уже возможно корректное применение части (а) алгоритма.

Далее последовательными итерациями части (а) алгоритма и, если потребуется, части (б) получаем цепочку элементов z_k с убывающими до нуля нормами, что и доказывает сформулированную возможность представления элементов $z\in\mathbf{Z}(i)$ кольца в форме (2).

2.2. Особенности реализации базовых арифметических операций в ЭСЧ для целых Гауссовых чисел

При сложении элементов $z\in\mathbf{Z}(i)$ в форме (2) может возникнуть необходимость использования «правил переноса в старшие разряды»:

$$1\bullet\omega^k+1\bullet\omega^k="2\bullet\omega^k"=1\bullet\omega^k+1\bullet\omega^{k+4},$$

$$\left(-1\right)\bullet\omega^k+\left(-1\right)\bullet\omega^k="\left(-2\right)\bullet\omega^k"=\left(-1\right)\bullet\omega^k+\left(-1\right)\bullet\omega^{k+4},$$

$$1\bullet\omega^k+\left(-1\right)\bullet\omega^k="0\bullet\omega^k"=1\bullet\omega^k+1\bullet\omega^{k+2}$$

(в этих равенствах кавычками отмечены слагаемые, «недопустимые» для формата представления (2)).

Заметим, что представление (2) элемента $z\in\mathbf{Z}(i)$ не является однозначным. Более того, например, для четных целых рациональных чисел $0<2n\in\mathbf{Z}\subset\mathbf{Z}(i)$ тривиальным образом справедливо представление

$$2n=\sum_{m=0}^{n-1}(1\cdot\omega^{4m}+1\cdot\omega^{4m+1}+(-1)\cdot\omega^{4m+2}+1\cdot\omega^{4m+3}).$$

Аналогичным образом находятся также одно или несколько «очевидных» представлений для элементов $z\in\mathbf{Z}(i)$ кольца целых Гауссовых чисел, расположенных на комплексной плоскости в узлах квадратной целочисленной решетки.

3. «Экзотическая» бинарная система счисления в кольце целых чисел Эйзенштейна

Определение 3.1. Кольцом целых чисел Эйзенштейна называется подкольцо $\mathbf{E}(\omega)\subset\mathbf{C}$ комплексного поля, определённое как

$$\mathbf{E}\left(\omega\right)=\left\{z=x+y\omega;x,y\in\mathbf{Z};\omega=\frac{-1+i\sqrt{3}}{2}\right\}.$$

Нормой элемента $z=x+y\omega\in\mathbf{E}(\omega)$ является целое число

$$\varepsilon\left(z\right)=z\bar{z}=\left(x+y\omega\right)\left(x+y\bar{\omega}\right)=x^2-xy+y^2.$$

Замечание. Разумеется, кольцо $\mathbf{E}(\omega)$ можно определить и в «изоморфной терминологии» как кольцо $\mathbf{Z}\left(\sqrt{-3}\right)$ целых элементов квадратичного поля $\mathbf{Q}\left(\sqrt{-3}\right)\subset\mathbf{C}$, а именно:

$$\mathbf{E}\left(\omega\right)\cong\mathbf{Z}\left(\sqrt{-3}\right)=\left\{\frac{u+v\sqrt{-3}}{2};u,v\in\mathbf{Z};u\equiv v\left(\mathrm{mod}\,2\right)\right\}$$

и с обычной нормой, принятой в теории квадратичных полей

$$\nu\left(\frac{u+v\sqrt{-3}}{2}\right)=Norm\left(\frac{u+v\sqrt{-3}}{2}\right)=\frac{\left(u^2+3v^2\right)}{4}.$$

В настоящей работе мы будем использовать обе эквивалентные терминологии, руководствуясь, в первую очередь, технической простотой доказательств соответствующих утверждений.

3.1. Представление целых чисел Эйзенштейна в ЭСЧ

Как и для целых Гауссовых чисел, для целых чисел Эйзенштейна справедлив аналог Утверждения 2.1 в форме:

Утверждение 3.1. Для $z\in\mathbf{Z}\left(i\sqrt{3}\right)$ при $\mathrm{Re}(z)\neq 0$ справедливо неравенство

$$\nu\left(z\right)>\begin{cases}\nu\left(z-1\right)\text{ при }\mathrm{Re}\left(z\right)>1/2,\\ \nu\left(z+1\right)\text{ при }\mathrm{Re}\left(z\right)<-\left(1/2\right);\end{cases}$$

при $\mathrm{Re}(z)=0$ справедливо равенство $\nu(z\pm1)=\nu(z)$.

Доказательство почти дословно повторяет доказательство Утверждения 2.1, то есть непосредственную проверку с минимальными формальными изменениями.

В «эйзенштейновской терминологии» для кольца $\mathbf{E}(\omega)$ и нормы $\varepsilon(z)=\varepsilon(x+y\omega)=x^2-xy+y^2$ аналогом Утверждения 2.1 является

Утверждение 3.2. Пусть $z=x+y\omega\in\mathbf{E}(\omega)$. Тогда:

- при $|y-2x|>1$ справедливо неравенство $\varepsilon(z-1)<\varepsilon(z)$;
- при $2x-y+1=0$ справедливо равенство $\varepsilon(z-1)<\varepsilon(z)$.

Доказательство. Пусть $\xi=\pm1$, $z=x+y\omega\in\mathbf{E}(\omega)$. Имеем:

$$\varepsilon\left(z-\xi\right)=\left(x\pm1\right)^2-\left(x\pm1\right)y+y^2=\varepsilon\left(z\right)+\left(\mp y\pm 2x+1\right).$$

Отсюда следует, что неравенство $\varepsilon(z-1)<\varepsilon(z)$ выполняется при $(\mp y\pm 2x+1)<0$, то есть при выполнении одного из неравенств

$2x+1<y,\ 2x-1>y,$

что равносильно выполнению неравенства

$\left|y-2x\right|>1.$

Так как $x,y\in\mathbf{Z}$, то последнее неравенство выполняется для всех $x,y\in\mathbf{Z}$ за исключением целочисленных решений уравнения $2x-y+1=0$. Очевидно, что в этом случае для норм элементов имеет место равенство $\varepsilon(z-1)=\varepsilon(z)$.

Следствие 3.1. Для элементов $z\in\mathbf{Z}(\omega)$ справедливы представления, аналогичные (1), в форме

$$z=\sum_{k=0}^{\nu(z)}\xi_k\omega^k,\ \omega=\frac{-1+i\sqrt{3}}{2},\ \xi_k\in\Lambda=\{-1,+1\}. \qquad (3)$$

Доказательство. Как и при доказательстве Следствия 2.1, метод построения представления (3), допуская известную вольность речи, будем называть алгоритмом.

(а) Пусть $z=x+y\omega\in\mathbf{Z}(\omega)$, $2x-y+1\neq 0$.

Выберем $\xi_0\in\Lambda$ таким образом, чтобы согласно Утверждению 3.2 выполнялось неравенство

$$\varepsilon(z-\xi_0)<\varepsilon(z).$$

Далее

$$z=(z-\xi_0)+\xi_0=\left((z-\xi_0)\omega^{-1}\right)\omega+\xi_0.$$

И так как

$$z=(z-\xi_0)+\xi_0,\ \text{а}\ \varepsilon(\omega)=\varepsilon(\omega^{-1})=1,$$

то, полагая $z_1=((z-\xi_0)\omega^{-1})$, получаем $\varepsilon(z_1)<\varepsilon(z)$.

(б) Пусть $z_0=z=x+y\omega$, $2x-y+1=0$.

Полагая $z_0^*=z_0\omega^{-1}$, имеем

$$z_0^*=x_0(-\omega-1)+y_0=(y_0-x_0)+(-1)x_0=x_0^*+y_0^*\omega.$$

Так как уже $2x_0^*-y_0^*+1\neq 0$ при целых x,y и так как $z_0=z_0^*\omega$, то для элемента z_0^* корректно применение части (а) алгоритма.

Далее последовательными итерациями части (а) алгоритма и, если потребуется, части (б) получаем цепочку элементов z_k с убывающими до нуля нормами, что и доказывает сформулированную возможность представления элементов кольца $\mathbf{E}(\omega)$ в форме (3).

3.2. Особенности реализации базовых арифметических операций в ЭСЧ для целых чисел Эйзенштейна

При сложении элементов $z\in\mathbf{E}(\omega)$ в форме (2) может возникнуть необходимость использования «правил переноса в старшие разряды»:

$$1\bullet\omega^k+1\bullet\omega^k="2\bullet\omega^k"=1\bullet\omega^k+1\bullet\omega^{k+3},$$

$$(-1)\bullet\omega^k+(-1)\bullet\omega^k="(-2)\bullet\omega^k"=(-1)\bullet\omega^k+(-1)\bullet\omega^{k+3},$$

$$1\bullet\omega^k+(-1)\bullet\omega^k="0\bullet\omega^k"=1\bullet\omega^k+1\bullet\omega^{k+1}+1\bullet\omega^{k+2}$$

(в этих равенствах кавычками отмечены слагаемые, «недопустимые» для формата представления (3)).

Заметим, что представление (3) элемента $z\in\mathbf{E}(\omega)$ не является однозначным. Более того, например, для целых чисел $0<n\in\mathbf{Z}\subset\mathbf{E}(\omega)$ тривиальным образом справедливо представление

$$n=\sum_{m=0}^{n-1}\left((-1)\cdot\omega^{3m+1}+(-1)\cdot\omega^{3m+2}\right).$$

Аналогичным образом находятся также одно или несколько «очевидных» представлений для элементов $z\in\mathbf{E}(\omega)$ кольца целых чисел Эйзенштейна, расположенных на комплексной плоскости в узлах треугольной решетки.

Неоднозначность представления целых элементов колец в рассмотренных системах счисления лишний раз подтверждает тезис, что с точки зрения синтеза отказоустойчивых арифметических устройств Phi-системы счисления с дробным основанием ϕ не являются уникальными. Относительным недостатком, на первый взгляд, является целочисленность рассматриваемых решеток комплексных чисел. Претензии, указывающие на этот недостаток, легко парируются тем аргументом, что в *практических* задачах исследователь имеет дело исключительно с рациональными аппроксимациями «виртуально» действительных чисел, то есть с масштабированными элементами многомерных целочисленных решёток.

Заключение

В работе рассмотрены системы счисления для квадратичных колец, ассоциированных с двумя целочисленными решетками на комплексной плоскости. Введенные «экзотические» системы счисления связаны с двумя задачами, имеющими скорее методологическую, нежели прикладную значимость.

Во-первых, введенные системы счисления обладают в некотором смысле уникальным свойством: норма каждой из возможных цифр равна норме основания (ср. с традиционными позиционными системами счисления для целых чисел). Кроме того, как показано автором [21], представление элементов алгебры комплексных чисел в «базисе Эйзенштейна» $\{1,\omega\}$ позволяет, в частности, тривиализировать часть умножений в быстрых алгоритмах дискретного преобразования Фурье.

Во-вторых, введенные системы счисления представляют некоторую альтернативу Phi-системам именно с точки зрения проектирования отказоустойчивых арифметических устройств, для которых Phi-системам счисления придавалась чуть ли не монопольная значимость.

Автор статьи полностью отдает себе отчет, что проблемы синтеза отказоустойчивых кодов именно как «кодов золотого сечения» может вызвать негативную реакцию у скептического настроенного читателя: «Опять кролики Фибоначчи!». Поэтому автор считает необходимым прояснить свою позицию в отношении «фибоначчиведения». Действительно, несмотря на давнее и эффективное использование чисел Фибоначчи, «золотого сечения» и т. п. в прикладных задачах (сортировка данных, построение квадратурных формул для численного интегрирования, моделирование «хаотических» и фрактальных процессов или объектов и т. д.), основная масса публикаций связана фактически с нумерологией, к «научному жанру» не относящейся. Несмотря на то, что автор использовал числа Фибоначчи, Люка и т.п. для решения локальных задач обработки сигналов [16 – 19], он никогда не разделял энтузиазма в поисках «Всеобщей гармонии» и/или построения «Общей теории всего» на основе анализа тех или иных числовых феноменов.

Тем не менее, вполне серьёзные профессиональные исследования в тематике, связанной, в частности, с теорией и приложениями последовательности чисел Фибоначчи, проводятся под эгидой *Fibonacci Association*. Регулярно проводятся конференции, издаются книги и журнал *Fibonacci Quarterly*. К сожалению, большинство из этих изданий практически недоступно российскому читателю. Приоритет в области применения теории чисел Фибоначчи к задачам информатики в СССР принадлежит А.П. Стахову (например, [2], [15] и др.), рассматривавшему представления данных в системе счисления Фибоначчи как средство построения отказоустойчивых машинных кодов. Разумеется, вопрос о *целесообразности* широкого использования «процессоров Фибоначчи» остается открытым с неоднозначным к нему отношением, хотя, скорее всего, в настоящее время создание таких процессоров не представляет принципиальной *технологической* трудности.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования в рамках выполнения работ по Государственному заданию ФНИЦ «Кристаллография и фотоника» РАН в части «Системы счисления» и Российского фонда фундаментальных исследований (проекты РФФИ №16-41-630676 р а, № 18-29-03135_ мк) в части «Машинная арифметика».

Литература

1. **Bergman, G.** A number system with an irrational base / G. Bergman // Mathematics Magazine. – 1957. – Vol. 31, No. 2. – P. 98-110.
2. **Стахов, А.П.** Коды золотой пропорции / А.П. Стахов. – М.: Радио и связь, 1984. – 152 с.
3. **Кнут, Д.** Искусство программирования для ЭВМ. Том 2. Получисленные алгоритмы / Д. Кнут. – М.: Мир, 1977. – 728 с.
4. **Fraenkel, A.S.** Systems of numeration /A.S. Fraenkel // The American Mathematical Monthly. – 1985. – Vol. 92, Issue 2. – P. 105-114. – DOI: 10.2307/2322638.
5. **Fraenkel, A.S.** The use and usefulness of numeration systems / A.S. Fraenkel // Information and Computation. – 1989. – Vol. 81, Issue 1. – P. 46-61. – DOI: 10.1016/0890-5401(89)90028-X.
6. **Joo, I.** Expansion with respect to non-integer bases/ I. Joo, F. Snitzer // Grazer Mathematische Berichte. – 1996. – Vol. 329. – P. 1-35.
7. Fibonacci ratios with pattern recognition / ed. by L. Pesavento, S. Shapiro. – Greenville: Trader Press Inc., 1997. – 184 p. – ISBN: 978-0-934380-36-2.
8. **Peters, J.M.H**. A ten point FFT calculation which features the golden ratio / J.M.H. Peters // The Fibonacci Quarterly. – 1996. – Vol. 34, Issue 4. – P. 323-325.
9. **Agaian, S.S.** Fast orthogonal Fibonacci transforms / S.S. Agaian, S.B. Alaverdian // Proc. Int. Coll. On Coding Theory. – 1998. – P. 335-352.
10. **Kátai, I.** Canonical number systems in imaginary quadratic fields / I. Kátai, J. Szabo // Acta Scientiarum Mathematicarum. – 1975. – Vol. 37. – P. 255-260.
11. **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.
12. **Thuswardner, J.** Elementary properties of canonical number systems in quadratic fields / J. Thuswaldner. – In: Application of Fibonacci numbers / ed. by G.E. Bergum, A.N. Philippou, A.F. Horadam. – Dordrecht: Springer Science+Business Media, 1998. – P. 405-414. – DOI: 10.1007/978-94-011-5020-0_45.
13. **Боревич, З.И.** Теория чисел / З.И. Боревич, И.Р. Шафаревич. – 3-е изд. – М.: Наука, 1985. – 504 с.
14. **Чернов, В.М.** Тернарные системы счисления в конечных полях / В.М. Чернов // Компьютерная оптика. – 2018. – Т. 42, № 4. – С. 704-711. – DOI: 10.18287/2412-6179-2018-42-4-704-711.
15. **Стахов, А.П.** Помехоустойчивые коды (Компьютер Фибоначчи) / А.П. Стахов. – М.: Знание, 1989. – 64 с. – ISBN: 5-07-000867-6.
16. **Чернов, В.М**. Реализация теоретико-числовых преобразований в кодах, порождённых избыточными системами счисления / В.М. Чернов // Электронное моделирование. – 1992. – Т. 15, № 4. – С. 33-37.
17. **Chernov, V.M.** Fast algorithms of discrete orthogonal transforms realized in the number system with an irrational base / V.M. Chernov, D.V. Sobolev // Optical Memory & Neural Networks. – 2000. – Vol. 9, Issue 2. – P. 91-100.
18. **Chernov, V.M.** Fibonacci-Mersenne and Fibonacci-Fermat discrete transforms / V.M. Chernov, M.V. Pershina // The Golden Section: Theory and Applications. Boletim de Informatica. – 1999. – No. 9/10. – P. 25-31.
19. **Chernov, V.M.** Fast algorithm for «error-free» convolution computation using Mersenne-Lucas codes / V.M. Chernov // Chaos, Solitons and Fractals. – 2006. –Vol. 29, Issue 2. – P. 372-380. – DOI: 10.1016/j.chaos.2005.08.081.
20. **Чернов, В.М.** Квазипараллельный алгоритм безошибочного вычисления свёртки в редуцированных кодах Мерсенна–Люка / В.М. Чернов // Компьютерная оптика. – 2015. – Т. 39, № 2. – С. 241-248. – DOI: 10.18287/0134-2452-2015-39-2-241-248.
21. **Чернов, В.М.** Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов. – М.: Физматлит, 2007. – 261 с. – ISBN: 5-9221-0940-6.

Сведения об авторе

Чернов Владимир Михайлович, 1949 г.р., математик, доктор физико-математических наук. Главный научный сотрудник лаборатории математических методов обработки изображений Института систем обработки изображений РАН (филиал ФНИЦ «Кристаллография и фотоника» РАН); профессор кафедры геоинформатики и информационной безопасности Самарского национального исследовательского университета имени академика С.П. Королева. Область научных интересов: алгебраические методы в цифровой обработке сигналов, криптография, машинная арифметика. E-mail: vche@smr.ru .

ГРНТИ:27.41.41 .

Поступила в редакцию 28 октября 2018 г. Окончательный вариант – 11 ноября 2018 г.

"EXOTIC" BINARY NUMBER SYSTEMS FOR RINGS OF GAUSS AND EISENSTEIN INTEGERS

V.M. Chernov[1,2]

[1]*IPSI RAS - Branch of the FSRC "Crystallography and Photonics" RAS, Russia, Samara, 443001, Molodogvardeyskaya 151,*

[2]*Samara National Research University, 443086, Russia, Samara, Moskovskoye Shosse 34*

Abstract

The paper considers nonstandard binary number systems for rings of Gauss and Eisenstein integers. The principal difference ("exoticism") of such number systems from the canonical number systems introduced by I. Katai for quadratic fields is that as a binary "digital alphabet", it uses a two-element set that does not contain a numeric zero. The paper also synthesizes algorithms for the representation of numbers in the considered number system and characterizes the possibility of an efficient implementation of arithmetic operations.

Keywords: number systems in quadratic rings, rings of Gauss and Eisenstein integers, machine arithmetic.

Citation: Chernov VM. "Exotic" binary number systems for rings of Gauss and Eisenstein integers. Computer Optics 2018; 42(6): 1068-1073. DOI: 10.18287/2412-6179-2018-42-6-1068-1073.

Acknowledgements: This work was partly funded by the RF Ministry of Science and Higher Education under FSRC "Crystallography and Photonics" RAS' state project ("Number systems") and the Russian Foundation for Basic Research under grants 16-41-630676_р_а and 18-29-03135_ мк ("Machine arithmetic").

References

[1] Bergman G. A number system with an irrational base. Math Magaz 1957; 31(2): 98-110.
[2] Stahov AP. Golden ratio codes [In Russian]. Moscow: "Radio & Sviaz" Publisher, 1984.
[3] Knuth DE. The art of computer programming. Volume 2: Seminumerical algorithms. 3rd ed. Reading, MA: Addison-Wesley; 1997. ISBN: 978-0-201-89684-8.
[4] Fraenkel AS. Systems of numeration. Amer Math Monthly 1985; 92(2): 105-114. DOI: 10.2307/2322638.
[5] Fraenkel AS. The use and usefulness of numeration systems. Information and Computation 1989; 81(1): 46-61. DOI: 10.1016/0890-5401(89)90028-X.
[6] Joo I, Snitzer F. Expansion with respect to non-integer bases. Graz Math Bericht 1996; 329: 1-35.
[7] Pesavento L, Shapiro S, eds. Fibonacci ratios with pattern recognition. Greenville: Trader Press Inc; 1997. ISBN: 978-0-934380-36-2.
[8] Peters JMH. A ten point FFT claculation which features the golden ratio. The Fibonacci Quarterly 1996; 34(4): 323-325.
[9] Agaian SS, Alaverdian SB. Fast orthogonal Fibonacci transforms. Proc Int Coll on Coding Theory, Osaka, Japan, 1998: 335-352.
[10] Katai I, Szabo J. Canonical number systems in imaginary quadratic fields. Acta Sci Math 1975; 37: 255-260.
[11] Bogdanov PS, Chernov VM. Classification of binary quasi-canonical number systems in imaginary quadratic fields [In Russian]. Computer Optics 2013; 37(3): 391-400.
[12] Thuswardner J. Elementary properties of canonical number systems in quadratic fields. In Book: Bergum GE, Philippou AN, Horadam AF, eds. Applications of Fibonacci numbers. 405-414. Dordrecht: Springer Science+Business Media; 1998: 405-414. DOI: 10.1007/978-94-011-5020-0_45.
[13] Borevich ZI, Shafarevich IR. Number theory. New York, London: Academic Press; 1966.
[14] Chernov VM. Ternary number systems in finite fields. Computer Optics 2018; 42(4): 704-711. DOI: 10.18287/2412-6179-2018-42-4-704-711.
[15] Stahov AP. Error-correcting codes (Fibonacci computer) [In Russian]. Moscow: "Znanie" Publisher, 1989. ISBN: 5-07-000867-6.
[16] Chernov VM. The implementation of number-theoretic transforms in the code generated by the redundant number systems [In Russian]. Electronic Simulation 1992; 15(4): 33-37.
[17] Chernov VM, Sobolev DV. Fast algorithms of discrete orthogonal transforms realized in the number system with an irrational base. Optical Memory & Neural Networks 2000; 9(2): 91-100.
[18] Chernov VM, Pershina MV. Fibonacci-Mersenne and Fibonacci-Fermat discrete transforms. Boletim de Informatica, 1999; 9/10: 25-31.
[19] Chernov VM. Fast algorithm for «error-free» convolution computation using Mersenne-Lucas codes // Chaos, Solitons and Fractals 2006; 29(2): 372-380. DOI: 10.1016/j.chaos.2005.08.081.
[20] Chernov VM. Quasi-parallel algorithm for error-free convolution computation using reduced Mersenne–Lucas codes [In Russian]. Computer Optics 2015; 39(2): 241-248. DOI: 10.18287/0134-2452-2015-39-2-241-248.
[21] Chernov V.M Arithmetic methods of fast algorithm of discrete orthogonal transforms synthesis [In Russian]. Moscow: "Fizmathlit" Publisher; 2007. ISBN: 5-9221-0940-6.

Author's information

Vladimir Mikhailovich Chernov (b. 1949) is mathematician, Doctor of Physical and Mathematical Sciences. Chief researcher of the Image Processing Systems Institute of the RAS (Branch of the FSRC "Crystallography and Photonics" RAS) and a professor of Geo-Information Science and Information Security department at Samara National Research University (SSAU). Research interests are algebraic methods in digital signal processing, cryptography, computer arithmetic.

Received October 28, 2018. The final version – November 11, 2018.