Тернарная машинная арифметика в квадратичных полях

В.М. Чернов[1,2]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086
[2]Институт систем обработки изображений РАН - филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001

Аннотация. Как известно, наиболее экономичной является троичная система счисления (используемая в троичных ЭВМ), следом за которой идут двоичная система счисления (традиционно используемая в большинстве распространённых ЭВМ). Этот широко известный факт стимулировал в свое время исследования по разработке троичных вычислительных средств. Тем не менее, тернарные системы счисления в компьютерных науках являются все же относительной экзотикой, несмотря на ясные теоретические преимущества и наличие довольно почтенной истории. В настоящее время исследования теоретических вопросов и приложений тернарных систем счисления ограничиваются, в основном, работами по приложениям очень частного случая т.н. «уравновешенных» троичных систем счисления для (приближенных) вычислений в поле действительных (а точнее, рациональных) чисел. В докладе приводятся систематизированные авторские результаты по синтезу тернарных систем счисления для мнимых квадратичных полей. В работе также рассматриваются системы счисления и алгоритмы арифметических операций при представлении элементов конечных полей в так называемых редуцированных системах счисления, то есть в редукциях канонических систем счисления при отображении соответствующего кольца целых квадратичного поля в поле классов вычетов по простому модулю – то есть, обобщения модулярной машинной арифметики.

Не могу представить себе, чтобы кому-нибудь потребовалось выполнять умножения со скоростью 40000 или даже 4000 операций в час; такое радикальное изменение (как переход к восьмеричной системе) не следует навязывать всему человечеству ради нескольких личностей
Fillips E. U. «Binary calculations» (1936),

Реальный мир полон отвратительных чисел типа 0,79134989..., мир же компьютеров имеет дело с милыми числами типа 0 и 1.
Дж. Конвей, Н. Слоэн. «Упаковки шаров, решетки и группы» (1988).

1. Введение

Вынесенная в эпиграф первая цитата из работы почти вековой давности как нельзя лучше характеризует, на взгляд автора статьи, бытующее до сих пор снисходительно-высокомерное отношение к тематике, связанной с исследованиями в области систем счисления «ортодоксальных» математиков, а вторая - не менее «ортодоксальных компьютерщиков». И первые, и вторые считают эту тематику слишком элементарной, «школьной». Однако именно в связи с бурным развитием вычислительной техники и появлением программно-аппаратных средств, позволяющих *в принципе* решать задачи недоступной ранее сложности, стали предъявляться и повышенные требования к теоретической поддержке методов представления цифровых данных в задачах «безошибочных» вычислений, криптографии, дискретного спектрального анализа, цифровой обработке сигналов, теории кодирования, комбинаторике и т.д. Одним из направлений теоретических исследований является разработка методов представления данных в алгебраических структурах, свойства которых согласованы как со структурой применяемых алгоритмов, так и с архитектурой используемых вычислительных средств.

Тернарные системы счисления в компьютерных науках являются все же относительной экзотикой, несмотря на ясные теоретические преимущества и наличие довольно почтенной истории, восходящей к следующей аргументации.

Как известно, в цифровой технике система счисления с основанием b реализуется регистрами, состоящими из наборов триггеров, каждый из которых может принимать b различных состояний, кодирующих цифры числа. При этом особое значение приобретает *экономичность системы счисления* — возможность представления как можно большего количества чисел с использованием как можно меньшего общего количества знаков. Если количество триггеров равно r, то общее количество знаков равно $m = rb$, а количество представимых ими чисел соответственно $b^r = b^{m/b}$. Как функция от b, это выражение достигает максимума при $b = e = 2,718281828\ldots$.

При целых значениях b максимум достигается при $b = 3$. Следовательно, наиболее экономичной является троичная система счисления (используемая в троичных ЭВМ), следом за которой идут двоичная система счисления (традиционно используемая в большинстве распространённых ЭВМ). Этот широко известный факт стимулировал исследования по разработке троичных вычислительных средств. Так еще в 1840 г. Томас Фоулер (Великобритания) построил механическую троичную вычислительную машину - одну из самых ранних механических вычислительных машин [1]. Эпоха тернарных электронных вычислительных машин общепризнанно ведет отсчет с 1958 г., когда в ВЦ МГУ Н. П. Брусенцов построил первую опытную электронную троичную ЭВМ (компьютер) «Сетунь» [2]. В США примерно в то же время тоже рассматривали преимущества и недостатки троичного компьютера [3], но после проведённых теоретических исследований строить троичный компьютер не стали. Скорее всего, в те годы развитие троичных вычислительных средств тормозило отсутствие надежных и дешевых «триггеров» с тремя устойчивыми состояниями. В настоящее время многие технологические проблемы успешно решены [4]-[6], [7]-[9]. Более того, обоснована и экспериментально подтверждена эффективность новых применений троичных арифметических устройств в задачах обработки цветных изображений [10], в криптографии [6]. Автор полагает, что если сейчас что-то и тормозит более широкое внедрение троичной вычислительной техники, то это, в основном, коммерческие, но не технологические причины.

В настоящей работе мы рассматриваем некоторые новые тернарные системы счисления в специальных алгебраических структурах, имея в виду перспективные приложения.

2. Некоторые теоретические сведения

2.1. Системы счисления

В не самой общей постановке исследуемая проблема выглядит следующим образом:

- для данного кольца Ω определить такие параметры*: основание системы счисления* $g \in \Omega$ и *алфавит цифр* $\Lambda \subset \Omega$, что любой элемент $\xi \in \Omega$ был бы представим в виде линейной комбинации

$$\xi = \sum_{k=0}^{k(z))} \xi_k g^k, \xi_k \in \Lambda, \quad (1)$$

то есть, определить *позиционную систему (системы) счисления* для данного кольца;

- синтезировать алгоритм определения цифр ξ_k в представлении (1);
- синтезировать алгоритмы реализации базовых арифметических операций в определенной выше системе счисления.

2.2. Кольца целых элементов квадратичных полей

Пусть $\mathbf{Z}(\sqrt{d})$ - кольцо целых квадратичных чисел, то есть, чисел $z = a + b\sqrt{d}; a, b \in \mathbf{Q}$ с условиями:

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

Как известно,

$$\mathbf{Z}(\sqrt{d}) = \left\{ z = a + b\sqrt{d} \right\} =$$

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

Согласно [11], элемент $g \square \alpha \in \mathbf{Z}(\sqrt{d})$ называется основанием *канонической системы счисления* в $\mathbf{Z}(\sqrt{d})$ если любой элемент z этого кольца представим в виде (1), а $\Lambda = \{0, 1, ..., |Norm(\alpha)| - 1\}$.

Числа z_k, допуская некоторую методологическую вольность, будем называть *цифрами*, множество Λ - *цифровым алфавитом,* а пару (α, Λ) - *системой счисления* в кольце $\mathbf{Z}(\sqrt{d})$.

Исчерпывающее описание канонических систем счисления для мнимых квадратичных полей получено в [11]. В работе [12] было предложено обобщение понятия канонической системы счисления: допускался цифровой алфавит Λ, являющийся конечным подмножеством множества $\mathbf{Z}(\sqrt{d})$. Иными словами, «цифрами» при таком обобщении могут быть не только целые рациональные («обычные» целые), но и целые квадратичные элементы. Такие системы счисления будем называть *квазиканоническими системами счисления.* Классификация бинарных и тернарных квазиканонических систем счисления приведена в [12].

2.3. Евклидовы кольца

Определение 2.1. Говорят, что в кольце Ω имеет место алгоритм деления с остатком, если на отличных от нуля элементах z кольца определена целочисленная неотрицательная функция $\nu(z)$ так, что выполняются следующие условия:

1. если z делится на w, то $\nu(z) \geq \nu(w)$;
2. для любых элементов z и $w \neq 0$ кольца Ω существуют такие $\gamma, \rho \in \mathbf{A}$, что $z = w\gamma + \rho$, причем либо $\rho = 0$, либо $\nu(\rho) < \nu(w)$.

Кольцо Ω называется в этом случае *евклидовым.* Евклидовых целых квадратичных колец не очень много: пять *мнимых* колец - $d \in \{-1, -2, -3, -7, -11\}$ и шестнадцать *вещественных* - $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$. В данной работе рассматриваются только тернарные системы счисления в мнимых евклидовых квадратичных кольцах, а в последнем разделе в кольцах, являющихся редукциями $(\mathrm{mod}\, p)$ таких колец.

Алгоритм определения цифр в представлении (1) в общем случае *канонических* систем счисления сводится к достаточно простому нелинейному рекуррентному соотношению [13].

Если в кольце $\mathbf{Z}\left(\sqrt{d}\right)$ имеет место алгоритм деления с остатком, то метод определения цифр в представлении (1) элемента $\xi \in \mathbf{Z}\left(\sqrt{d}\right)$ Ω как в канонических, так и в квазиканонических системах счисления с основанием g ω полностью аналогичен методу определения цифр в обычной g – ичной позиционной системе счисления для целых чисел.

Свяжем с представлением (1) элемента его *код* – вектор цифр $\xi = \xi_0 g^0 + \xi_1 g^1 + ... \leftrightarrow (\xi_0, \xi_1, \xi_2, ...)$.

Операции над представлениями элементов кольца в форме (1) индуцируют соответствующие им правила преобразований кодов.

Замечание 2.1. Отметим, что в такой интерпретации цифры ξ_k (компоненты кода) при реализации операций играют не только роль чисел, но и являются "идентификаторами состояния соответствующего триггера". Чтобы подчеркнуть этот факт, далее для обозначения умножения элемента цифрового алфавита на элемент конечного поля в работе используется знак $(\bullet)$, а знак (+), в зависимости от контекста, интерпретируется и как знак, обозначающий сложение и как разделительный знак между состояниями триггеров.

3. Тернарные системы счисления в мнимых квадратичных полях

Как следует из ограничений классификационных теорем работы [11], тернарные *канонические* системы счисления существуют при $d < 0$ только в кольцах $\mathbf{Z}(\sqrt{-2})$, $\mathbf{Z}(\sqrt{-3})$, $\mathbf{Z}(\sqrt{-11})$. В [12] показано, что при $d < 0$ в этих кольцах существуют также и квазиканонические тернарные системы счисления, то есть, такой элемент $\omega \in \mathbf{Z}\left(\sqrt{d}\right)$ и такое конечное подмножество $\Lambda \subset \mathbf{Z}\left(\sqrt{d}\right)$, что любое целое квадратичное число данного кольца может быть представлено в форме (1).

В кольце $\mathbf{Z}(\sqrt{-2})$ существует восемь тернарных квазиканонических систем счисления: четыре уравновешенные с цифровым алфавитом $\Lambda = \{-1, 0, +1\}$ и с основаниями $\alpha = \pm 1 \pm i\sqrt{2}$, а также четыре неуравновешенные системы счисления с параметрами:

$$\alpha_1 = -1 + i\sqrt{2},\ \Lambda_1 = \left\{0, 1, -i\sqrt{2}\right\}; \alpha_2 = -1 + i\sqrt{2},\ \Lambda_3 = \left\{0, -1, i\sqrt{2}\right\};$$

$$\alpha_3 = -1 - i\sqrt{2},\ \Lambda_3 = \left\{0, 1, i\sqrt{2}\right\}; \alpha_4 = -1 - i\sqrt{2},\ \Lambda_4 = \left\{0, -1, -i\sqrt{2}\right\}.$$

Пример 3.1. Обозначим $\alpha = -1 + i\sqrt{2}, (+1) \triangleq \mathrm{I}, (-1) \triangleq \Upsilon, 0 \triangleq \Theta$. Тогда справедливы равенства («правила переноса в старшие разряды»):

$$\mathrm{I} + \mathrm{I} = \mathrm{I} \bullet \alpha^3 + \mathrm{I} \bullet \alpha^2 + \mathrm{I} \bullet \alpha^1 - \Upsilon \bullet \alpha^0,\ \mathrm{I} + \Upsilon = \Theta,\ \Upsilon + \Upsilon = \Upsilon \bullet \alpha^3 + \Upsilon \bullet \alpha^2 + \Upsilon \bullet \alpha^1 - \mathrm{I} \bullet \alpha^0.$$

В кольце $\mathbf{Z}\left(i\sqrt{11}\right)$ существуют четыре тернарные квазиканонические системы счисления с уравновешенным цифровым алфавитом $\Lambda = \{-1, 0, +1\}$ и с основаниями

$$\alpha_1 = \left(+1 + i\sqrt{11}\right)\Big/_2,\quad \alpha_2 = \left(+1 - i\sqrt{11}\right)\Big/_2,\ \alpha_3 = \left(-1 + i\sqrt{11}\right)\Big/_2,\quad \alpha_4 = \left(-1 - i\sqrt{11}\right)\Big/_2.$$

Заметим также, что два последних из приведенных значений оснований могут служить и основаниями канонических тернарных систем счисления [11] в рассматриваемом кольце, но с цифровым алфавитом $\{0,1,2\}$

Пусть, как и ранее, $\mathrm{I} = 1, \Upsilon = -1$. Тогда "правила переноса в старший разряд(ы)" - имеют вид:

$$2 = \begin{cases} \Upsilon \bullet \alpha^2 + \mathrm{I} \bullet \alpha + \Upsilon \bullet \alpha^0 \text{ при } \alpha = \alpha_1, \\ \Upsilon \bullet \alpha^2 + \mathrm{I} \bullet \alpha \text{ при } \alpha = \alpha_2 = \overline{\alpha_1}, \\ \Upsilon \bullet \alpha^2 + \Upsilon \bullet \alpha \text{ при } \alpha = \alpha_3 = -\overline{\alpha_1}, \\ \Upsilon \bullet \alpha^2 + \Upsilon \bullet \alpha + \Upsilon \bullet \alpha^0 \text{ при } \alpha = \alpha_4 = -\alpha_1. \end{cases}$$

В квадратичном кольце $\mathbf{Z}(i\sqrt{3})$ существуют 24 тернарные квазиканонические системы счисления, а именно системы счисления с основаниями $\alpha_k = (i\sqrt{3})\omega^{k-1}$ и с алфавитами цифр

$$\{0,1,\omega\},\{0,\omega,\omega^2\},\{0,\omega^2,\omega^3\},\{0,\omega^3,\omega^4\},\{0,\omega^4,\omega^5\},\{0,\omega^5,\omega^6\},$$

где $\omega = 2^{-1}\left(1+i\sqrt{3}\right)$ и $k = 1,2,3,4.$ Легко убедиться, что во всех них цифровой алфавит Λ не является уравновешенным.

Пример 3.2. Пусть $\alpha = \left(i\sqrt{3}\right)\omega = 2^{-1}\left(-3+i\sqrt{3}\right), \Lambda = \left\{0,1,\omega^5\right\}.$ Тогда базовые арифметические правила имеют вид: $(-1) = \alpha + \omega^5,\ 2 = \alpha^3 + \alpha^2 + \alpha^1 + \omega^5,\ 1+\omega^5 = \frac{1}{2}\left(3-i\sqrt{3}\right) = -\alpha = \left(\alpha+\omega^5\right)\alpha.$

4. «Экзотические» тернарные системы в кольцах целых Гаусса и Эйзенштейна

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 $\mathbf{Z}\left(\sqrt{5}\right)$ вещественного 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 (1), где g = φ («фи») - так называемое «золотое сечение», $\phi = 2^{-1}\left(1+\sqrt{5}\right)$, 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) при $g = \phi$, часто называют «кодами золотого сечения» [15].

Первоначально эти системы использовались в приложениях, в частности, для синтеза *отказоустойчивых* арифметических устройств. С развитием аппаратных возможностей вычислительной математики такие системы счисления с разным успехом стали применяться и в криптографии, цифровой обработке сигналов и изображений.

Как уже отмечалось выше, цифры ξ_k представления (1) определяются в общем случае либо посредством нелинейного рекуррентного процесса [13], либо, что возможно далеко не во всех квадратичных кольцах, с помощью алгоритма деления с остатком [12]. Заметим, что для указанных алгоритмов 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 тернарных систем счисления, вынесенная в заголовок раздела, определяется следующими факторами.

- В кольцах целых элементов полей $\mathbf{Q}\left(\sqrt{-1}\right)$, $\mathbf{Q}\left(\sqrt{-3}\right)$ нормы оснований систем счисления равны $(+1)$.
- Алфавитами «цифр» в обоих случаях является множество $0 \notin \Lambda = \{-1,+1\}.$
- 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-систем счисления рассматривалась как аргумент, обеспечивающий *отказоустойчивость* ассоциированных кодов машинной арифметики (отказы одного или нескольких триггеров возможно компенсировать переходом к эквивалентному

кодовому представлению числа) и в некоторой степени оправдывало их прикладную значимость. 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.

Рассмотрим $\mathbf{Z}(i)$ - кольцо целых гауссовых чисел:

$$\mathbf{Z}(i)=\{z=x+y\omega;\ x,y\in\mathbf{Z};\ \omega\ i,i^2=-1\};\quad \Lambda=\{-1,+1\},\nu(z)=Norm\ z=Norm(x+y\omega)=x^2+y^2$$

Утверждение 4.1. Для $z\in\mathbf{Z}(i)$, при $\mathrm{Re}(z)\neq 0$ справедливо неравенство

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

А при $\mathrm{Re}(z)=0$ справедливо равенство $\nu(z\pm 1)=\nu(z)$.

Следствие 4.1. Для элементов $z\in\mathbf{Z}(i)$ справедливы представления (1) где $g=i,\xi_k\in\Lambda=\{-1,+1\}$.

Доказательство. (а) Пусть $\mathrm{Re}(z)\neq 0$. Положим $z_0=z\in\mathbf{Z}(i)$. Выберем $\xi_0\in\Lambda$ таким образом, чтобы согласно Утверждению 4.1, выполнялось бы неравенство $\nu(z-\xi_0)<\nu(z)$.

Далее, $z=(z-\xi_0)+\xi_0=((z-\xi_0)\omega^{-1})\omega+\xi_0$. И, так как $z=(z-\xi_0)+\xi_0$, а $\nu(\omega)=\nu(\omega^{-1})=1$, 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 тогда уже $\mathrm{Re}(z_0^*)\neq 0$. 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 (1).

При сложении элементов $z\in\mathbf{Z}(i)$ в форме (1) может возникнуть необходимость использования «правил переноса в старшие разряды»:

$$1\bullet\omega^k+1\bullet\omega^k="2\bullet\omega^k"=1\bullet\omega^k+1\bullet\omega^{k+4},$$
$$(-1)\bullet\omega^k+(-1)\bullet\omega^k="(-2)\bullet\omega^k"=(-1)\bullet\omega^k+(-1)\bullet\omega^{k+4},$$
$$1\bullet\omega^k+(-1)\bullet\omega^k="0\bullet\omega^k"=1\bullet\omega^k+1\bullet\omega^{k+2}$$

(в этих равенствах кавычками отмечены слагаемые, «недопустимые» для формата представления (1) с алфавитом $0\notin\Lambda=\{-1,+1\}$.).

Заметим, что представление (1) 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.

Определение 4.1. Кольцом целых чисел Эйзенштейна называется подкольцо $\mathbf{E}(\omega)\subset\mathbf{C}$ комплексного поля, определённое как

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

Нормой элемента $z=x+y\omega\in\mathbf{E}(\omega)$ является целое число $\varepsilon(z)=z\bar{z}=(x+y\omega)(x+y\bar{\omega})=x^2-xy+y^2$.

Замечание 4.1. 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:

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

и с обычной нормой, принятой в теории квадратичных полей

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

Как и для целых гауссовых чисел, для целых чисел Эйзенштейна справедлив аналог Утверждения 4.1.

Утверждение 4.2. Для $z\in\mathbf{Z}\left(i\sqrt{3}\right)$ при $\mathrm{Re}(z)\neq 0$ справедливо неравенство

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

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

В «эйзенштейновской терминологии» для кольца $\mathbf{E}(\omega)$ и нормы $\varepsilon(z)=\varepsilon(x+y\omega)=x^2-xy+y^2$ аналогом Утверждения 4.1 является следующее утверждение.

Утверждение 4.3. 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 $\xi=\pm1$, $z=x+y\omega\in\mathbf{E}(\omega)$, тогда справедливо равенство:

$$\varepsilon(z-\xi)=(x\pm1)^2-(x\pm1)y+y^2=\varepsilon(z)+(\mp y\pm2x+1).$$

Отсюда следует, что неравенство $\varepsilon(z-1)<\varepsilon(z)$ выполняется при $(\mp y\pm2x+1)<0$, то есть, при выполнении одного из неравенств $2x+1<y$ или $2x-1>y$, что равносильно неравенству $|y-2x|>1$.

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 4.2. Для элементов $z\in\mathbf{Z}(\omega)$ справедливы представления (1) с параметрами

$$g=\omega=\left(-1+i\sqrt{3}\right)\big/2\,,\ \xi_k\in\Lambda=\{-1,+1\}.$$

Доказательство. (а) Пусть $z=x+y\omega\in\mathbf{Z}(\omega),\ 2x-y+1\neq0$. Выберем $\xi_0\in\Lambda$ таким образом, чтобы согласно Утверждению 4.2 выполнялось бы 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 $z=(z-\xi_0)+\xi_0$, а $\varepsilon(\omega)=\varepsilon\left(\omega^{-1}\right)=1$, то, полагая $z_1\square\left((z-\xi_0)\omega^{-1}\right)$, 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 теперь уже $2x_0^*-y_0^*+1\neq0$ 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 (1).

При сложении элементов $z \in \mathbf{E}(\omega)$ в форме (1) 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 (1) при с алфавите $0 \notin \Lambda = \{-1, +1\}$.).

Заметим, что представление (1) 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

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

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.

5. Тернарная модулярная машинная арифметика в редуцированных кольцах

Автор вполне отдает себе отчет о том, что тематика этого раздела не кажется связанной напрямую с вычислительными задачами по тематике конференции «Информационные технологии и нанотехнологии». Поэтому естественно возникает вопрос: «*Зачем «эта модулярность» нужна?»*

Дело в том, что реальные вычисления при численном решении любой прикладной задачи производятся не с элементами полей действительных или комплексных чисел, а с некоторым множеством их рациональных аппроксимаций, причем происхождение обрабатываемых данных и возможности используемых вычислительных средств выделяют во множестве рациональных чисел *конечное* подмножество - некую “рабочую зону”. После соответствующего масштабирования, элементы этого конечного множества можно считать целыми числами и, более того, вычетами по некоторому достаточно большому модулю p. Таким образом, “экзотические” системы счисления – модулярные бинарные и тернарные *редуцированные* $(\mathrm{mod}\, p)$ системы счисления в определенной мере представляют альтернативу традиционным “битовым” системам счисления.

Кроме того, постановка некоторых задач (например, в криптографии) *принципиально* не допускает в качестве ответа результат приближенных вычислений – «или ответ точный, или это не ответ». Стремление же получить результат с нулевой (или легко компенсируемой) погрешностью простыми «универсальными» средствами часто приводит к возникновению известных эффектов «разбухания промежуточных вычислений», «проклятия размерностей», которые могут иметь место даже, на первый взгляд, и во вполне безобидных задачах.

Пример 5.1. При вычислении НОД двух многочленов

$$f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x + 5, \text{ и } g = 3x^6 + 5x^4 - 4x^2 - 9x + 2$$

для выяснения вопроса об их взаимной простоте (то есть, для получения *битового* ответа “ДА-НЕТ”), стандартное применение алгоритма Евклида даёт в качестве последнего ненулевого остатка число

$$r = 125933387955007431009311519921875 00,$$

что и указывает на взаимную простоту многочленов f и g.

Основная идея. Пусть для данного простого p число d является квадратичным вычетом $(\mathrm{mod}\, p)$, то есть, существуют решения сравнения $y^2 \equiv d \ (\mathrm{mod}\, p)$. Пусть ξ - одно из решения этого сравнения. Рассмотрим отображение (гомоморфизм) $\varphi : z = a + b\sqrt{d} \mapsto a + \eta b \equiv \gamma \ (\mathrm{mod}\, p)$ и, если d - квадратичный вычет $(\mathrm{mod}\, p)$, то элемент γ принадлежит конечному полю $\mathbf{F}_p$, то есть, φ отображает $\mathbf{Z}(\sqrt{d})$ в поле $\mathbf{F}_p$. А так как в поле $\mathbf{F}_p$ нет нетривиальных подколец, то $\mathrm{Im}\,\varphi \cong \mathbf{F}_p$.

Отображение φ, *редукция* $(\mathrm{mod}\, p)$, очевидным образом индуцирует преобразование представления (1) для элемента $\varphi(z) = \gamma$ с новыми параметрами: цифрами $\varphi(z_k)$ и основанием $\varphi(\alpha) = \mathrm{g}$. Такие представления будем называть представлениями в *редуцированных системах счисления.* Как и ранее, свяжем с элементом γ редуцированного поля $\mathbf{F}_p$ его код – вектор цифр

$$\gamma = \gamma_0 g^0 + \gamma_1 g^1 + \ldots \leftrightarrow (\gamma_0, \gamma_1, \gamma_2, \ldots).$$

Операции над представлениями элементов (1) индуцируют соответствующие им правила преобразований кодов.

В данном разделе работы рассматриваются только те из мнимых колец целых квадратичных чисел $\mathbf{Z}(\sqrt{d})$, для которых выполняются условия:

(a) число (d) является квадратичным вычетом $(\mathrm{mod}\, p)$,

(b) в кольце $\mathbf{Z}(\sqrt{d})$ существуют тернарные квазиканонические системы счисления.

Таких колец $\mathbf{Z}(\sqrt{d})$, с условием (b) немного: $\mathbf{Z}(i\sqrt{2})$, $\mathbf{Z}(i\sqrt{3})$, $\mathbf{Z}(i\sqrt{11})$. Исследуя каждое из них, получаем следующее утверждение.

Утверждение 5.1. Чтобы при $d \in \{-2, -3, -11\}$ в кольце $\mathbf{Z}_p\left(\sqrt{d}\right)$ существовали редуцированные $(\mathrm{mod}\, p)$ тернарные системы счисления необходимо, выполнение одного из следующих условий:

- $p \equiv 1 (\mathrm{mod}\, 3)$ для $\mathbf{Z}_p\left(i\sqrt{3}\right)$;
- $p \equiv 1$ или $p \equiv 3 (\mathrm{mod}\, 8)$ для $\mathbf{Z}_p\left(i\sqrt{2}\right)$;
- $p \equiv a \in \{1, 3, 4, 5, 9\} (\mathrm{mod}\, 11)$ для $\mathbf{Z}_p\left(i\sqrt{11}\right)$.

Пример 5.2. Рассмотрим поле $\mathbf{Z}_p\left(i\sqrt{2}\right) \cong \mathbf{F}_p$. Как отмечено выше, кольце $\mathbf{Z}\left(i\sqrt{2}\right)$ существует восемь тернарных квазиканонических систем счисления, из которых четыре являются уравновешенными с цифровым алфавитом $\Lambda = \{-1, 0, +1\}$ и с основаниями $\alpha = \pm 1 \pm i\sqrt{2}$, а также неуравновешенные системы счисления например с параметрами: $\alpha_1 = -1 + i\sqrt{2}$, $\Lambda_1 = \left\{0, 1, -i\sqrt{2}\right\}$; $\alpha_2 = -1 + i\sqrt{2}$, $\Lambda_3 = \left\{0, -1, i\sqrt{2}\right\}$.

При вычислениях в кодах желательно иметь простые правила действия над цифрами («правило переноса в старший(е) разряд(ы)» и т.п.)

Обозначим $\alpha = -1 + i\sqrt{2}, (+1) \triangleq \mathrm{I}, (-1) \triangleq \Upsilon, 0 \triangleq \Theta$. Тогда справедливы равенства:

$$\mathrm{I} + \mathrm{I} = \mathrm{I} \bullet \alpha^3 + \mathrm{I} \bullet \alpha^2 + \mathrm{I} \bullet \alpha^1 - \Upsilon \bullet \alpha^0,$$

$$\mathrm{I} + \Upsilon = \Theta,$$

$$\Upsilon + \Upsilon = \Upsilon \bullet \alpha^3 + \Upsilon \bullet \alpha^2 + \Upsilon \bullet \alpha^1 - \mathrm{I} \bullet \alpha^0.$$

Суммируя результаты исследований колец $\mathbf{Z}(i\sqrt{2})$, $\mathbf{Z}(i\sqrt{3})$, $\mathbf{Z}(i\sqrt{11})$, получаем *основное утверждение.*

Утверждение 5.2. Во всех конечных полях $\mathbf{F}_p$ кроме девяти случаев, а именно:

$$p \equiv s \in \Omega, \quad \Omega = \{29, 95, 101, 149, 167, 173, 215, 239, 263\} \pmod{264}$$

существуют тернарные редуцированные системы счисления.
(Иными словами, доля «плохих» простых чисел составляет менее 4%. Но всё не так уж и плохо: в этих полях существуют *бинарные* редуцированные системы счисления).

6. Заключение

В работе рассмотрены полученные автором теоретические результаты в области тернарных систем машинной арифметики способствующие развитию известных и созданию новых методов и алгоритмов решения прикладных задач информатики, в частности:

- обработки изображений, в том числе цветных;
- криптографии;
- безошибочных вычислений, в том числе параллельных;
- быстрому умножению больших целых чисел;
- разработки отказоустойчивых машинных кодов.

7. Литература

[1] Glusker, M. The ternary calculating machine of Thomas Fowler / M. Glusker, D.M. Hogan, P. Vass// IEEE Ann. Hist. Comput. – 2005. – Vol. 27. – P. 4-22.
[2] Brousentov, N.P. Development of Ternary Computers at Moscow State University / N.P. Brousentov, S.P. Maslov, J.R. Alvarez, E.A. Zhogolev // Russian Virtual Computer Museum: Moscow, Russia, 2002.
[3] Frieder, G. Ternary Computers, part 1: Motivation for ternary computers // Proc. of the 5th Annual Workshop on Microprogramming, Urbana, IL, USA, 1972.
[4] Srivastava, A. Design and implementation of a low power ternary full adder / A. Srivastava, K. Venkatapathy // VLSI Design. – 1996. – Vol. 4(1). – P. 75-81.
[5] Gundersen, H. Aspect of Balanced Ternary Arithmetic Implemented Using CMOS Recharged Semi-Floating Gate Device // Ph.D. Thesis, Oslo University, Oslo, Norway, 2008.
[6] Adikari, J. Hybrid Binary-Ternary Number System for Elliptic Curve Crypto System / J. Adikari, V. S. Dimitrov, L. Imbert // IEEE Transactions on Computers. – 2010. – Vol. 60(2). – P. 254-265. DOI:10.1109/TC.2010.138.
[7] Ahmad, S. Balanced Ternary Logic For Improving Computing/ S. Ahmad, M. Alam // Int. J. Comput. Sci. Inf. Technol. – 2014. – Vol. 5. – P. 51-57.
[8] Wu, X.W. CMOS Ternary Logic Circuits // IEE Proc. – 1990. – Vol. 137. – P. 21-27.
[9] Nagaraju, P. Ternary Logic Gates and Ternary SRAM Implementation in VLSI / P. Nagaraju, N. Vishnuvardhan // Int. J. Sci. Res. – 2014. – Vol. 3. – P. 245-250.
[10] Obiniyi, A.A. Arithmetic Logic Design with Color Coded Ternary for Ternary Computing / A.A. Obiniyi, E.E. Absalom, K. Adako // Int. J. Comput. Appl. – 2011. – Vol. 26. – P. 31-37.
[11] Katai, I. Canonical number systems in imaginary quadratic fields / I. Katai, B. Kovacs // Acta Mathematica Hungarica. – 1981. – Vol. 37. – P. 159-164.
[12] Богданов, П.С. Классификация бинарных квазиканонических систем счисления в мнимых квадратичных полях /П.С. Богданов, В.М. Чернов // Компьютерная оптика. – 2013. – № 37. – С. 391-400.
[13] Thuswardner, J. Elementary properties of canonical numder systems in quadratic fields // Application of Fibonacci Numbers. – 1996. – Vol. 7. – P. 405-414.
[14] Bergman, G. A number system with an irrational base / G. Bergman // Math.Magaz. – 1957. – Vol. 31. – P. 98-119.
[15] Стахов, А.П. Коды золотой пропорции. – М.: Радио и связь, 1984. – 152 с.

Благодарности
Работы выполнены при финансовой поддержке Российского фонда фундаментальных исследований (Проекты 15-07-05576,16-41-630676, 18-29-03135, 19-07-00357).

Ternary machine arithmetic in quadratic fields

V.M. Chernov[1,2]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086
[2]Image Processing Systems Institute of RAS - Branch of the FSRC "Crystallography and Photonics" RAS, Molodogvardejskaya street 151, Samara, Russia, 443001

Abstract. As you know, the most economical is the ternary number system (used in ternary computers), followed by a binary number system (traditionally used in most common computers). This well-known fact stimulated research into the development of ternary computing. However, ternary number systems in computer science are still relatively exotic, despite the clear theoretical advantages and the presence of a fairly respectable history.
Currently, the research of theoretical issues and applications of ternary number systems is limited mainly to the applications of a very special case of the so-called "balanced" ternary number systems for (approximate) calculations in the field of real (or rather, rational) numbers.
The report presents the systematized author's results on the synthesis of ternary number systems for both real and imaginary quadratic fields. The paper also considers the number systems and algorithms of arithmetic operations in the representation of finite field elements in the so – called reduced number systems, that is, in the reduction of canonical number systems when displaying the corresponding ring of an integer quadratic field in the field of residue classes by a simple module-that is, generalization of modular machine arithmetic.