ЧИСЛЕННЫЕ МЕТОДЫ И АНАЛИЗ ДАННЫХ

ТЕРНАРНЫЕ СИСТЕМЫ СЧИСЛЕНИЯ В КОНЕЧНЫХ ПОЛЯХ

В.М. Чернов [1, 2]

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

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

Аннотация

Работа продолжает авторские исследования позиционных систем счисления в конечных полях. В работе рассматриваются тернарные системы счисления и алгоритмы арифметических операций при представлении элементов конечного поля в так называемых тернарных редуцированных системах счисления, являющихся редукциями канонических систем счисления при отображении соответствующего кольца целых квадратичного поля в поле классов вычетов по простому модулю. Приводится классификация конечных полей, в которых существуют такие системы счисления. Доказывается, что тернарные редуцированные системы счисления существуют для большинства простых конечных полей.

Ключевые слова: преобразования Фурье–Галуа, конечные поля, тернарные редуцированные системы счисления.

Цитирование: **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.

Введение

Работа посвящена исследованию тернарных систем счисления специального вида в конечных алгебраических полях и продолжает исследования автора [1, 2].

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

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.

В 1840 г. Томас Фоулер (Великобритания) построил механическую троичную вычислительную машину – одну из самых ранних механических вычислительных машин [3].

Эпоха троичных электронных вычислительных машин общепризнанно ведет отсчет с 1958 г., когда в ВЦ МГУ Н.П. Брусенцов построил первую опытную электронную троичную ЭВМ (компьютер) «Сетунь» на ячейках из ферритдиодных магнитных усилителей переменного тока, работавших в двухбитном троичном коде (четвёртое состояние двух битов не использовалось) [4]. В США примерно в то же время рассматривали преимущества и недостатки троичного компьютера [5], 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 [6, 8], [15 – 17]. Более того, обоснована и экспериментально подтверждена эффективность новых применений троичных арифметических устройств в задачах обработки цветных изображений [11], в криптографии [8]. Автор полагает, что если сейчас что-то и тормозит более широкое внедрение троичной вычислительной техники, то это в основном коммерческие, но не технологические причины.

Следует также отметить, что, наряду с работами, относящимися к троичной компьютерной арифметике, проводятся многочисленные исследования по тернарной логике, продолжающие основополагающие работы польского математика Я. Лукасевича [12], но относящиеся, на наш взгляд, к пограничной области между математикой и философией [14]. (*«Есть три вида людей: живые, мертвые и те, что плавают по морям».* – Анахарсис (Ανάχαρσις), античный философ.)

В данной работе исследовались так называемые «уравновешенные» тернарные системы счисления в

конечных полях ($\mathrm{mod}\, p$), то есть троичные системы счисления с алфавитом «цифр» $\Lambda = \{-1, 0, 1\ (\mathrm{mod}\, p)\}$. Именно подобная система счисления для действительных чисел «машинного диапазона» была реализована в ЭВМ «Сетунь» [4], и именно такие системы счисления чаще всего рассматривались в позднейших публикациях разных авторов [7, 15]. Но, как выяснилось в процессе исследований автора, не в каждом конечном поле, в котором существуют тернарные системы счисления, они являются именно уравновешенными. В работе рассматриваются также и конечные поля с неуравновешенными тернарными системами счисления.

1. Теоретические сведения и обозначения

Автор вынужден далее воспроизвести достаточно объемную цитату из работы [1] с целью достижения замкнутости изложения и возможности независимого использования далее обозначений этой работы.

Пусть $\mathbf{Z}(\sqrt{d})$ – 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 [20],

$$\mathbf{Z}(\sqrt{d}) = \left\{ z = a + b\sqrt{d}\,; a, b \in \mathbf{Z} \text{ при } d \neq 1(\mathrm{mod}\, 4) \right\},$$

$$\mathbf{Z}(\sqrt{d}) = \tag{1}$$

$$= \left\{ z = a + b\sqrt{d}\,/_2\,; a \equiv b\,(\mathrm{mod}\, 2) \text{ при } d \equiv 1(\mathrm{mod}\, 4) \right\}.$$

Согласно [21] элемент $\alpha \in \mathbf{Z}\left(\sqrt{d}\right)$ называется основанием канонической системы счисления в кольце $\mathbf{Z}\left(\sqrt{d}\right)$, если любой элемент z этого кольца представим в виде

$$z = \sum_{k=0}^{k(z)} z_k \alpha^k,\ z_k \in \Lambda. \tag{2}$$

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

$$\Lambda = \left\{0, 1, ..., \left|Norm(\alpha)\right| - 1\right\}, \tag{3}$$

то система счисления называется *канонической системой счисления.* Исчерпывающее описание канонических систем счисления для мнимых квадратичных полей получено в [21].

В работе [2] было предложено обобщение понятия канонической системы счисления: допускался цифровой алфавит Λ, являющийся конечным подмножеством множества $\mathbf{Z}(\sqrt{d})$. Такие системы счисления, следуя [2], будем называть *квазиканоническими системами счисления.*

Замечание 1. Отметим некоторую терминологическую особенность: канонические в «привычном смысле» системы счисления – троичная с цифрами $\{0, 1, 2\}$ и даже обычная $(0-1)$-битовая системы счисления не являются каноническими в смысле базового определения работы [21]. Действительно, алгебраические нормы целых чисел 2 и 3 равны 4 и 9 соответственно, поэтому указанные системы счисления не удовлетворяют (3).

Как легко следует из ограничений классификационных теорем работы [21], например, *бинарные* канонические системы счисления существуют только в кольцах

$$\mathbf{Z}(i),\ \mathbf{Z}(i\sqrt{2}),\ \mathbf{Z}(i\sqrt{7}). \tag{4}$$

В [2] показано, что в этих кольцах существуют и бинарные квазиканонические системы счисления.

Определить цифры z_k, разложения (2) можно с помощью рекуррентного процесса [21, 22], но для рассматриваемых колец $\mathbf{Z}(\sqrt{d})$ лучше воспользоваться алгоритмом деления по норме на элемент α [2]. Такой алгоритм существует лишь для пяти значений $d \leq 0$ [20], а именно:

$$d = -1, -2, -3, -7, -11,$$

то есть, в частности, и для рассматриваемых колец (4).

В настоящей работе объектом рассмотрения являются уже *тернарные* (троичные) редуцированные системы счисления.

2. Основные идеи

Пусть далее для данного простого p число d является квадратичным вычетом ($\mathrm{mod}\, p$) [19], то есть существуют решения сравнения

$$y^2 \equiv d\ (\mathrm{mod}\, p). \tag{5}$$

Пусть ξ – одно из решений сравнения (5), рассмотрим гомоморфизм

$$\varphi : z = a + b\sqrt{d} \mapsto a + \xi b \equiv \gamma\ (\mathrm{mod}\, p), \tag{6}$$

и так как d – квадратичный вычет ($\mathrm{mod}\, p$), то элемент в правой части (6) принадлежит конечному полю $\mathbf{F}_p$, то есть φ отображает $\mathbf{Z}(\sqrt{d})$ в поле $\mathbf{F}_p$. А так как в простом поле $\mathbf{F}_p$ нет нетривиальных подколец, то

$$\mathrm{Im}\,\varphi \cong \mathbf{F}_p.$$

Образ кольца $\mathbf{Z}(\sqrt{d})$ относительно гомоморфизма φ также будем обозначать $\mathbf{Z}_p(\sqrt{d})$. Отображение φ, *редукция* ($\mathrm{mod}\, p$), очевидным образом индуцирует преобразование представления (2) для элемента $\varphi(z) = \gamma$ с новыми параметрами: цифрами $\varphi(z_k)$ и основанием $\varphi(\alpha) = g$. Такие представления будем называть представлениями в *редуцированных системах счисления.*

Свяжем с элементом γ редуцированного поля $\mathbf{F}_p$ его код – вектор цифр:

$$\gamma = \gamma_0 g^0 + \gamma_1 g^1 + ... \leftrightarrow \left(\gamma_0, \gamma_1, \gamma_2, ...\right). \tag{7}$$

Операции над представлениями элементов (2) индуцируют соответствующие им правила преобразований кодов.

Замечание 2. Отметим, что в такой интерпретации цифры γ_k 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 (●), а знак (+), в зависимости от контекста, интерпретируется и как знак, обозначающий сложение, и как разделительный знак между состояниями триггеров.

3. Конечные поля с тернарными уравновешенными редуцированными системами счисления

Рассмотрим подробнее те из 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,

(c) эта квазиканоническая система счисления является уравновешенной с цифровым алфавитом $\Lambda = \{-1, 0, +1\}$.

Колец $\mathbf{Z}(\sqrt{d})$ с условием (b) немного [2, 21]:

$\mathbf{Z}(i\sqrt{2})$, $\mathbf{Z}(i\sqrt{3})$, $\mathbf{Z}(i\sqrt{11})$.

Исследуем, при каких простых p каждое из перечисленных колец удовлетворяет условию (a).

3.1. Случай поля $\mathbf{Z}_p\left(i\sqrt{2}\right) \cong \mathbf{F}_p$.

Как следует из работы [21] о канонических системах счисления в мнимых квадратичных полях и ее обобщения [2], в 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

$$\alpha = \pm 1 \pm i\sqrt{2}, \tag{8}$$

а также неуравновешенные системы счисления с параметрами:

$$\begin{aligned}
&\alpha_1 = -1 + i\sqrt{2},\ \Lambda_1 = \left\{0, 1, -i\sqrt{2}\right\};\\
&\alpha_2 = -1 + i\sqrt{2},\ \Lambda_3 = \left\{0, -1, i\sqrt{2}\right\};\\
&\alpha_3 = -1 - i\sqrt{2},\ \Lambda_3 = \left\{0, 1, i\sqrt{2}\right\};\\
&\alpha_4 = -1 - i\sqrt{2},\ \Lambda_4 = \left\{0, -1, -i\sqrt{2}\right\}.
\end{aligned} \tag{9}$$

В данном разделе работы мы рассматриваем только редуцированные уравновешенные тернарные системы счисления, а именно редукции $(\mathrm{mod}\, p)$ систем счисления (8) в кольце $\mathbf{Z}_p\left(i\sqrt{2}\right)$.

Так как требуется, чтобы в редуцированном $(\mathrm{mod}\, p)$ кольце элемент (–2) был квадратичным вычетом $(\mathrm{mod}\, p)$, то, вычисляя символ Лежандра [19], имеем:

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{p-1/2} \cdot (-1)^{p^2-1/8}.$$

Нетрудно убедиться, правая часть последнего равенства равна (+1) при всех простых p с условием

$$p^2 + 4p - 5 \equiv 0 \left(\mathrm{mod} 16\right),$$

что очевидно выполняется для простых вида $p = 8k + 1$ или $p = 8k + 3$, $k \in \mathbf{Z}$, то есть для простых чисел – членов последовательности A004625 и членов последовательности A007520 по классификации «Онлайновой энциклопедии целочисленных последовательностей» [23].

При вычислениях в кодах (7) желательно иметь простые правила действия над цифрами («правило переноса в старший(е) разряд(ы)» и т.п.).

С учетом Замечания 2 обозначим

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

Тогда справедливы равенства:

$$\begin{aligned}
&\mathrm{I} + \mathrm{I} = \mathrm{I} \bullet \alpha^3 + \mathrm{I} \bullet \alpha^2 + \mathrm{I} \bullet \alpha^1 - \Upsilon \bullet \alpha^0,\\
&\mathrm{I} + \Upsilon = \Theta,\\
&\Upsilon + \Upsilon = \Upsilon \bullet \alpha^3 + \Upsilon \bullet \alpha^2 + \Upsilon \bullet \alpha^1 - \mathrm{I} \bullet \alpha^0.
\end{aligned} \tag{10}$$

Замечание 3. Из соотношений (10) следует, что «житейская простота» уравновешенной тернарной системы счисления становится иллюзорной при переходе к рассматриваемым редуцированным системам счисления. Например, в «обычной» тернарной уравновешенной системе счисления аналогом первого равенства соотношений (10) является очевидное равенство

$$2 = (+1) \cdot 3^1 + (-1) \cdot 3^0.$$

Именно с желанием автора добиться возможной относительной простоты базовых арифметических правил отчасти и связано рассмотрение также и неуравновешенных систем счисления.

Пример 1. Пусть $p = 11$, ξ – решение сравнения

$$\xi^2 \equiv -2 \equiv p - 2 \left(\mathrm{mod}\, p\right).$$

В рассматриваемом случае указанное сравнение имеет два решения $\xi_+ \equiv 3$, $\xi_- \equiv 8 (\mathrm{mod}\ 11)$.

Далее, при

$$\begin{aligned}
&\xi \equiv 8 \left(\mathrm{mod} 11\right),\\
&\Lambda = \left\{-1, 0, 1\right\} \triangleq \left\{\Upsilon, \Theta, \mathrm{I}\right\},\\
&\alpha = -1 + i\sqrt{2} \equiv 7 \left(\mathrm{mod} 11\right)
\end{aligned}$$

первое из соотношений равенств (10) примет вид:

$$2 \equiv 1 \cdot 7^3 + 1 \cdot 7^2 + 1 \cdot 7^1 + (-1) \cdot 7^0 \ \left(\mathrm{mod}\ 11\right).$$

3.2. Случай поля $\mathbf{Z}_p\left(i\sqrt{11}\right) \cong \mathbf{F}_p$.

В кольце $\mathbf{Z}\left(i\sqrt{11}\right)$ существуют четыре тернарные квазиканонические системы счисления с уравновешенным цифровым алфавитом и с основаниями

$$\alpha_1 = \left(+1+i\sqrt{11}\right)\Big/2, \quad \alpha_2 = \left(+1-i\sqrt{11}\right)\Big/2,$$
$$\alpha_3 = \left(-1+i\sqrt{11}\right)\Big/2, \quad \alpha_4 = \left(-1-i\sqrt{11}\right)\Big/2. \qquad (11)$$

Заметим также, что два последних из приведенных значений оснований могут служить и основаниями канонических тернарных систем счисления работы [21] в рассматриваемом кольце, но с цифровым алфавитом $\{0, 1, 2\}$ (См. Замечание 1).

Так как требуется, чтобы в редуцированном $(\mathrm{mod}\, p)$ кольце элемент (-11) был квадратичным вычетом $(\mathrm{mod}\, p)$, то, вычисляя символ Лежандра (Якоби) [19], получаем:

$$\left(\frac{-11}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{11}{p}\right)=$$
$$=(-1)^{p-1/2}\cdot(-1)^{(11-1/2)\left(p-1/2\right)}\left(\frac{p}{11}\right)=\left(\frac{p}{11}\right).$$

Нетрудно убедиться, что правая часть последнего равенства равна $(+1)$ при простых $p \equiv 1, 3, 4, 5, 9 (\mathrm{mod}\ 11)$.

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

$$2=\begin{cases}\Upsilon\bullet\alpha^2+\mathrm{I}\bullet\alpha+\Upsilon\bullet\alpha^0 \text{ при } \alpha=\alpha_1,\\ \Upsilon\bullet\alpha^2+\mathrm{I}\bullet\alpha \text{ при } \alpha=\alpha_2=\overline{\alpha_1},\\ \Upsilon\bullet\alpha^2+\Upsilon\bullet\alpha \text{ при } \alpha=\alpha_3=\overline{-\alpha_1},\\ \Upsilon\bullet\alpha^2+\Upsilon\bullet\alpha+\Upsilon\bullet\alpha^0 \text{ при } \alpha=\alpha_4=-\alpha_1.\end{cases} \qquad (12)$$

Пример 2. Пусть $p=23$, ξ – решение сравнения

$$\xi^2 \equiv -11 \equiv 12 (\mathrm{mod} 23).$$

В рассматриваемом случае указанное сравнение имеет два решения $\xi_+ \equiv 9$, $\xi_- \equiv -9 \equiv 14 \mathrm{mod}(23)$.

Далее, при

$$\xi \equiv 14 (\mathrm{mod} 23), \Lambda = \{-1, 0, 1\} \triangleq \{\Upsilon, \Theta, \mathrm{I}\},$$
$$\alpha = +1 + i\sqrt{2} \equiv 15 (\mathrm{mod}\, 23)$$

первое из соотношений равенств (12) примет вид:

$$2 \equiv (-1)\bullet 15^2 + (+1)\bullet 15^1 + (-1)\bullet 15^0 \ (\mathrm{mod}\ 23).$$

4. Конечные поля с тернарными неуравновешенными системами счисления

4.1.Случай поля $\mathbf{Z}_p\left(i\sqrt{2}\right) \cong \mathbf{F}_p$.

Как уже отмечалось выше, в кольце $\mathbf{Z}\left(i\sqrt{2}\right)$, кроме уравновешенных квазиканонических систем счисления, существуют и неуравновешенные системы счисления (9).

С учётом Замечания 2 введём обозначения:

$$\alpha = -1 + i\sqrt{2}, \Lambda = \left\{0, -1, i\sqrt{2}\right\},$$
$$0 \triangleq \Theta, (-1) \triangleq \Upsilon, i\sqrt{2} \triangleq \Psi, 1 \triangleq \mathrm{I}.$$

Сформулируем непосредственно проверяемые правила «переноса в старший разряд», то есть правила преобразования сумм и произведений цифр, возникающих при арифметических действиях над кодами (7).

$$\Upsilon + \Upsilon = \Psi \bullet \alpha + \Psi, \mathrm{I} + \Upsilon = \Theta, \Psi + \Upsilon = \alpha,$$
$$\mathrm{I} = \Upsilon \bullet \alpha + \Psi, \Psi + \Psi = \Upsilon \bullet \alpha^2 + \Upsilon.$$

Пример 3. Пусть по-прежнему $p=11$, ξ – решение сравнения

$$\xi^2 \equiv -2 \equiv p - 2 (\mathrm{mod}\, p).$$

Как и в Примере 1, указанное сравнение имеет два решения $\xi_+ \equiv 3$, $\xi_- \equiv 8 \mathrm{mod}(11)$.

Пусть далее:

$$\alpha = -1 + \xi_- \equiv 7 (\mathrm{mod} 11), \Lambda = \left\{0, -1, i\sqrt{2}\right\},$$
$$0 \triangleq \Theta, (-1) \triangleq \Upsilon, i\sqrt{2} = \xi_- \triangleq \Psi, 1 \triangleq \mathrm{I}.$$

Тогда, например, справедливо равенство

$$-2 \equiv 8 \cdot 7^1 + 8 \cdot 7^0 \ (\mathrm{mod} 11),$$

существенно более простое, чем соответствующее равенство Примера 1.

4.2. Случай поля $\mathbf{Z}_p\left(i\sqrt{3}\right) \equiv \mathbf{F}_p$.

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

Пример 4. Пусть

$$\alpha = \left(i\sqrt{3}\right)\omega = \frac{1}{2}\left(-3 + i\sqrt{3}\right), \Lambda = \left\{0, 1, \omega^5\right\}.$$

Тогда базовые арифметические правила, выраженные через цифры и основание системы счисления, выглядят следующим образом:

$$(-1) = \alpha + \omega^5,$$
$$2 = \alpha^3 + \alpha^2 + \alpha^1 + \omega^5, \qquad (13)$$
$$1 + \omega^5 = \frac{1}{2}\left(3 - i\sqrt{3}\right) = -\alpha = \left(\alpha + \omega^5\right)\alpha.$$

Пусть, к примеру, $p=13$, обозначим ξ – решение сравнения

$$\xi^2 \equiv -3 \equiv p - 3 \equiv 13 - 3 \equiv 10 (\mathrm{mod} 13),$$

то есть $i\sqrt{3} \triangleq \xi$ и $\Lambda = \{0, 1, \omega\} \triangleq \{\Theta, \mathrm{I}, \Psi\}$.

В рассматриваемом случае указанное сравнение имеет два решения $\xi_+ \equiv 4$, $\xi_- \equiv 9 \mathrm{mod}(13)$.

И далее для $p=13$ выбранных основания системы счисления $\alpha=\xi\omega$, и алфавита цифр

$$\Lambda=\left\{0,1,\omega^5=2^{-1}\left(1-i\sqrt{3}\right)\right\}$$

имеем:

$$\xi=i\sqrt{3}\equiv 4\left(\mathrm{mod}13\right),$$

$$\omega^5=2^{-1}\left(1-i\sqrt{3}\right)\equiv 7\cdot(1-4)\equiv 8\left(\mathrm{mod}13\right),$$

$$\alpha=\xi\omega\equiv 36\equiv 10\left(\mathrm{mod}13\right).$$

5. О количестве простых полей, в которых существуют тернарные редуцированные системы счисления

Как показано выше, чтобы в кольце $\mathbf{Z}_p(\sqrt{d})$ 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 $\mathbf{Z}_p\left(i\sqrt{11}\right)$.

Суммируя сформулированные выше условия и результаты рассмотрений колец

$$\mathbf{Z}(i\sqrt{2}),\ \mathbf{Z}(i\sqrt{3}),\ \mathbf{Z}(i\sqrt{11}),$$

учитывая, что $3\times 8\times 11=264$, получаем основное утверждение работы.

Утверждение. Во всех конечных полях $\mathbf{F}_p$, кроме случаев, когда:

$$p\equiv s\left(\mathrm{mod}\,264\right),\ \text{где}$$

$$s\in\left\{29,95,101,149,167,173,215,239,263\right\},$$

существуют тернарные редуцированные системы счисления.

Иными словами, доля «плохих» простых чисел составляет менее 4 %.

Но всё не так уж плохо: как показано в [1], в этих полях существуют *бинарные* редуцированные системы счисления.

Заключение

Автор отдает себе отчёт в том, что тематика статьи не кажется связанной напрямую с вычислительными задачами дифракционной оптики или обработки изображений. Поэтому естественно возникают два вопроса.

Во-первых, 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, рассмотренные «экзотические» системы счисления – бинарные и тернарные *редуцированные* ($\mathrm{mod}\,p$) системы счисления в определенной мере представляют альтернативу традиционной «битовой» системе счисления [10].

Кроме того, постановка некоторых задач (например, в криптографии) *принципиально* не допускает в качестве ответа результат приближённых 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, во вполне безобидных задачах.

Пример 5. См. [26]. При вычислении НОД двух многочленов

$$f=x^8+x^6-3x^4-3x^3+8x^2+2x+5,$$

$$g=3x^6+5x^4-4x^2-9x+2$$

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.

Во-вторых, «бинарные, тернарные…что дальше?»

Автор вполне допускает бесконечность ряда натуральных чисел и уникальную специфику конкретных представителей этого ряда, но всё же склонен считать, что в многопараметрических задачах основные теоретические трудности возникают при возрастании (скачке) принципиального параметра (например, размерности пространства или, как в данной задаче, «арности» системы счисления) именно от двух до трёх. Уровень развития современной электроники и оптоэлектроники снимает многие проблемы, актуальные 30 лет назад и обсуждаемые, например, в [26, глава 8].

Следует также отметить, что и в [1], и в данной работе рассматривались редуцированные системы счисления, индуцированные квазиканоническими системами счисления в кольцах целых элементов *мнимых* квадратичных полей алгебраических чисел. Представляется перспективным исследование возможности перенесения методов и результатов данной работы на *вещественные* квадратичные расширения и, в качестве первого этапа, на кольца целых квадратичных с возможностью деления с остатком, то есть на квадратичные кольца целых $\mathbf{Z}(\sqrt{d})$ при

$$d=3,5,6,7,11,13,17,19,21,29,33,37,41,57,73.$$

В случае вещественных расширений алгебраическая норма основания системы счисления может быть и отрицательной, что порождает, в частности, интересные, но малоизученные (или забытые) системы счисления с отрицательным основанием – т.н. «нега-позиционные» системы счисления.

Нега-позиционные системы счисления были впервые предложены Витторио Грюнвальдом в его работе «*Giornale di Matematiche di Battaglini*», опубликованной в 1885 году. Грюнвальд описал алгоритмы сложения, вычитания, умножения, деления, извлечения корня, признаков делимости и преобразования систем счисления. Тем из читателей, кто затруднится в поисках и прочтении оригинальной «антикварной» работы В. Грюнвальда, можно порекомендовать более позднюю работу [27] или раздел, посвященный системам счисления известного многотомника Д. Кнута. Отметим также относительно недавнюю работу [28] с оригинальными приложениями.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования в рамках выполнения работ по Государственному заданию ФНИЦ «Кристаллография и фотоника» РАН (соглашение № 007-ГЗ/Ч3363/26) в части «компьютерные системы счисления» и Российского фонда фундаментальных исследований (проекты РФФИ № 16-41-630676_р_а, № 18-29-03135_ мк) в части «Исследования тернарной машинной арифметики».

Литература

1. **Чернов, В.М.** Вычисление преобразований Фурье–Галуа в редуцированных бинарных системах счисления / В.М. Чернов // Компьютерная оптика. – 2018. – Т. 42, № 3. – С. 495-500. – DOI: 10.18287/2412-6179-2018-42-3-495-500.
2. **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.
3. **Glusker, M**. The ternary calculating machine of Thomas Fowler / M. Glusker, D.M. Hogan, P. Vass // IEEE Annals of the History of Computing. – 2005. – Vol. 27, Issue 3. – P. 4-22. – DOI: 10.1109/MAHC.2005.49.
4. **Brousentov, N.P.** Development of ternary computers at Moscow State University [Electronical Resource] / N.P. Brousentov, S.P. Maslov, J.R. Alvarez, E.A. Zhogolev. – Russian Virtual Computer Museum. – URL: http://www.computer-museum.ru/english/setun.htm (request date 23.07.2018).
5. **Frieder, G.** Ternary computers: Part 1: Motivation for ternary computers / G. Frieder // Proceedings of the 5th Annual Workshop on Microprogramming. – 1972. – P. 83-86. – DOI: 10.1145/776378.776392.
6. **Srivastava, A.** Design and implementation of a low power ternary full adder / A. Srivastava, K. Venkatapathy // VLSI Design. – 1996. – Vol. 4, Issue 1. – P. 75-81. – DOI: 10.1155/1996/94696.
7. **Gundersen, H**. Aspect of balanced ternary arithmetic implemented using CMOS recharged semi-floating gate device / H. Gundersen // Ph.D. Thesis. Oslo, Norway: Oslo University, 2008.
8. **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, Issue 2. – P. 254-265. – DOI: 10.1109/TC.2010.138.
9. **Porat, D.I.** Three valued digital systems / D.I. Porat // Proceedings of the Institution of Electrical Engineers. – 1969. – Vol. 116, Issue 6. – P. 947-954. – DOI: 10.1049/piee.1969.0177.
10. **Vasundara, P.K.S.** Multi-valued logic addition and multiplication in Galois field / P.K.S. Vasundara, K.S. Gurumurthy // Proceedings of the International Conference on Advances in Computing, Control and Telecommunication Technologies. – 2009. – DOI: 10.1109/ACT.2009.190.
11. **Obiniyi, A.A**. Arithmetic logic design with color coded ternary for ternary computing / A.A. Obiniyi, E.E. Absalom, K. Adako // International Journal of Computer Applications. – 2011. – Vol. 26, Issue 11. – P. 31-37. – DOI: 10.5120/3162-2929.
12. **Лукасевич, Я**. Аристотелевская силлогистика с точки зрения современной формальной логики / Я. Лукасевич – М.: Издательство иностранной литературы, 1959. – 312 с.
13. **Profeanu, I.** A ternary arithmetic and logic / I. Profeanu // Proceedings of the World Congress on Engineering. – 2010. – Vol. 1.
14. **Карпенко, А.С.** Логики Лукасевича и простые числа / А.С. Карпенко. – М.: Наука, 2000. – 318 с. – ISBN: 5-02-013048-6.
15. **Ahmad, S.** Balanced-ternary logic for improved and advanced computing / S. Ahmad, M. Alam // International Journal of Computer Science and Information Technologies. – 2014. – Vol. 5, Issue 4. – P. 5157-5160.
16. **Wu, X.W.** CMOS ternary logic circuits / X.W. Wu // IEE Proceedings G – Circuits, Devices and Systems. – 1990. – Vol. 137, Issue 1. – P. 21-27. – DOI: 10.1049/ip-g-2.1990.0005.
17. **Nagaraju, P.** Ternary logic gates and ternary SRAM cell implementation in VLSI / P. Nagaraju, N. Vishnuvardhan // International Journal of Science and Research. – 2014. – Vol. 3, Issue 11. – P. 1920-1924.
18. **Lin, S.** CNTFET-Based design of ternary logic gates and arithmetic circuits / S. Lin, Y.-B. Kim, F. Lombardi // IEEE Transactions on Nanotechnology. – 2011. – Vol. 10, Issue 2. – P. 217-225. – DOI: 10.1109/TNANO.2009.2036845.
19. **Айерлэнд, К.** Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен; пер. с англ. – М.: Мир, 1987. – 415 с.
20. **Боревич, З.И.** Теория чисел / З.И. Боревич, И.Р. Шафаревич. – 3-е изд. – М.: Наука, 1985. – 504 с.
21. **Katai, I.** Canonical number systems in imaginary quadratic fields / I. Katai, B. Kovacs // Acta Mathematica Academiae Scientarium Hungarica. – 1981. – Tomus 37(1-3). – P. 159-164.
22. **Thuswardner, J.** Elementary properties of canonical numder systems in quadratic fields / J. Thuswaldner. – In: Application of Fibonacci numbers / ed. by G.E. Bergum, A.N. Philippou, A.F. Horadam. – Dordrecht: Springer, 1998. – P. 405-414. – DOI: 10.1007/978-94-011-5020-0_45.
23. The On-Line encyclopedia of integer sequences® (OEIS®) [Electronical Resource]. – URL: https://oeis.org (request date 02.06.2018).
24. **Вариченко, Л.В.** Абстрактные алгебраические системы и цифровая обработка сигналов / Л.В. Вариченко, В.Г. Лабунец, М.А. Раков. – Киев: Наукова думка, 1986. – 247 с.
25. **Грегори, Р.** Безошибочные вычисления. Методы и приложения / Р. Грегори, Е. Кришнамурти; пер. с англ. – М.: Мир, 1988. – 207 с. – ISBN: 5-03-001145-5.
26. **Дэвенпорт, Дж.** Компьютерная алгебра / Дж. Дэвенпорт, И. Сирэ, Э. Турнье // М.: Мир, 1991. – 352 с.

27. **Pawlak, Z.** An electronic digital computer based on the (–2) system / Z. Pawlak // International Journal of Computer and Information Science. – 1959. – Vol. 7. – P. 713-721.

28. **Masáková, Z.** Arithmetics in number systems with a negative base / Z. Masáková, E. Pelantová, T. Vávra // Theoretical Computer Science. – 2011. – Vol. 412, Issue 8-10. – P. 835-845. – DOI: 10.1016/j.tcs.2010.11.033.

Сведения об авторе

Чернов Владимир Михайлович, 1949 года рождения, 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. Королёва. Область научных интересов: алгебраические методы в цифровой обработке сигналов, криптография, машинная арифметика. E-mail: vche@smr.ru .

ГРНТИ: 27.41.41.
Поступило в редакцию 20 июня 2018 г. Окончательный вариант – 27 июля 2018 г.

TERNARY NUMBER SYSTEMS IN FINITE FIELDS

V.M. Chernov[1, 2]
[1]*IPSI RAS - Branch of the FSRC "Crystallography and Photonics" RAS, 443001, Samara, Russia, Molodogvardeyskaya 151,*
[2]*Samara National Research University, 443086, Russia, Samara, Moskovskoye Shosse 34*

Abstract

The work continues the author's previous study of positional number systems in finite fields. The paper considers ternary number systems and arithmetic operations algorithms for the representation of elements of finite fields in the so-called ternary reduced number systems, which are reductions of the canonical number systems when mapping the corresponding ring of integers of a quadratic field into some prime field. A classification of finite fields in which such number systems exist is given. It is proved that the reduced ternary number systems exist for most finite prime fields.

Keywords: canonical and reduced number systems, finite fields, machine arithmetic.

Citation: Chernov V.M. Ternary number systems in finite fields. Computer Optics 2018; 42(4): 704-711. DOI: 10.18287/2412-6179-2018-42-4-704-711.

Acknowledgements: This work was supported by the Ministry of Science and Higher Education with in the State assignment FSRC «Crystallography and Photonics» RAS (No 007-ГЗ/Ч3363/26) in part of «Number systems for computers» and by Russian Foundation for Basic Research (Grants 16-41-630676_p_a and 18-29-03135_ мк) in part of «Ternary machine arithmetics».

References

[1] Chernov VM. Calculation of Fourier–Galois transforms in reduced binary number systems [In Russian]. Computer Optics 2018; 42(3): 495-500. DOI: 10.18287/2412-6179-2018-42-3-495-500.

[2] Bogdanov PS, Chernov VM. Classification of binary quasi-canonical number systems in imaginary quadratic fields [In Russian]. Computer Optics 2013; 37(3): 391-400.

[3] Glusker M, Hogan DM, Vass P. The ternary calculating machine of Thomas Fowler. IEEE Ann Hist Comput 2005; 27(3): 4-22. DOI: 10.1109/MAHC.2005.49.

[4] Brousentov NP, Maslov SP, Alvarez JR, Zhogolev EA. Development of ternary computers at moscow state university. Source: ⟨http://www.computer-museum.ru/english/setun.htm⟩.

[5] Frieder G. Ternary computers; Part 1: Motivation for ternary computers. Proceedings of the 5th Annual Workshop on Microprogramming 1972: 83-86. DOI: 10.1145/776378.776392.

[6] Srivastava A, Venkatapathy K. Design and implementation of a low power ternary full adder. VLSI Design 1996; 4(1), 75-81. DOI: 10.1155/1996/94696.

[7] Gundersen H. Aspect of balanced ternary arithmetic implemented using CMOS recharged semi-floating gate device. Oslo: Oslo University; 2008.

[8] Adikar J, Dimitrov VS, Imbert L. Hybrid binary-ternary number system for elliptic curve crypto system. IEEE Transactions on Computers 2010; 60(2): 254-265. DOI: 10.1109/TC.2010.138.

[9] Porat D.I. Three valued digital systems. Proc IEE 1969; 116(6): 947-954. DOI: 10.1049/piee.1969.0177.

[10] Vasundara PKS, Gurumurthy KS. Multi-valued logic addition and multiplication in Galois fields. Proc. ACT' 09 2009. DOI: 10.1109/ACT.2009.190.

[11] Obiniyi AA, Absalom EE, Adako K. Arithmetic logic design with color coded ternary for ternary computing. Int J Comput Appl 2011; 26(11): 31-37. DOI: 10.5120/3162-2929.

[12] Łukasiewicz J. Aristotile's sillogistic from the standpoint of modern formal logic. Oxford: Clarendon Press; 1957.

[13] Profeanu I. A ternary arithmetic and logic. Proc WCE 2010; 1.

[14] Karpenko AS. Łukasiewicz's logics and prime numbers [In Russian]. Moscow: "Nauka" Publisher; 2000. ISBN: 5-02-013048-6.

[15] Ahmad S, Alam M. Balanced-ternary logic for improved and advanced computing. Int J Comput Sci Inf Technol 2014; 5(4): 5157-5160.

[16] Wu X.W. CMOS ternary logic circuits. IEE Proceedings G – Circuits, Devices and Systems 1990; 137(1): 21-27. DOI: 10.1049/ip-g-2.1990.0005.

[17] Nagaraju P, Vishnuvardhan N. Ternary logic gates and ternary SRAM cell implementation in VLSI. Int J Sci Res 2014; 3(11): 1920-1924.
[18] Lin S, Kim Y-B, Lombardi F. CNTFET-Based design of ternary logic gates and arithmetic circuits. IEEE Trans Nanotechnol 2011; 10(2): 217-225. DOI: 10.1109/TNANO.2009.2036845.
[19] Ireland K, Rosen M. A classical introduction to modern number theory. New York: Springer Verlag; 1982. ISBN: 978-0-387-97329-6.
[20] Borevich ZI, Shafarevich IR. Number theory. New York, London: Academic Press; 1966.
[21] Katai I, Kovacs B. Canonical number systems in imaginary quadratic fields. Acta Mathematica Academiae Scientarium Hungarica 1981; 37(1-3): 159-164.
[22] Thuswardner J. Elementary properties of canonical numder systems in quadratic fields. In book: Bergum GE, Philippou AN, Horadam AF, eds. Application of Fibonacci numbers. Dordrecht: Springer; 1998: 405-414. DOI: 10.1007/978-94-011-5020-0_45.
[23] The On-Line Encyclopedia of Integer Sequences® (OEIS®). Source: ⟨https://oeis.org⟩.
[24] Varichenko LV, Labunetc VG, Rakov MA. Abstract algebraic systems and digital signal processing [In Russian]. Kiev, "Naukova dumka" Publisher; 1986.
[25] Gregory RT, Krishnamurty EV. Methods and applications of error-free computation. New York: Springer-Verlag; 1984. ISBN: 978-1-4612-9754-3.
[26] Davenport J, Siret Y, Tournier É. Calcul formel: systèmes et algorithmes de manipulations algébriques. Paris, New York: Masson; 1987. ISBN: 2-225-80990-9.
[27] Pawlak Z. An electronic digital computer based on the (–2) system. International Journal of Computer and Information Science 1959; 7, 713-721.
[28] Masáková Z, Pelantová E, Vávra T. Arithmetics in number systems with a negative base. Theoretical Computer Science 2011; 412(8-10): 835-845. DOI: 10.1016/j.tcs.2010.11.033.

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

Received June 20, 2018. The final version – July 27, 2018.