Системы счисления в модулярных кольцах и их приложения к «безошибочным» вычислениям

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 статье вводятся и исследуются новые системы параллельной машинной арифметики, связанной с представлением данных в избыточной системе счисления с базисом, формируемым последовательностями степеней корней характеристического полинома рекуррентности второго порядка. Такие системы счисления являются модулярными редукциями обобщений системы счисления Дж. Бергмана с основанием, равным «золотому сечению». Описывается ассоциированная система остаточных классов. В качестве приложения к задачам цифровой обработки сигналов в работе предлагается, в частности, новый «безошибочный» алгоритм вычисления дискретной циклической свёртки. Алгоритм основан на применении нового класса дискретных ортогональных преобразований, для которых существуют эффективные реализации, не использующие умножений.

Ключевые слова: система счисления, модулярная арифметика, дискретная свертка, система остаточных классов.

Цитирование: **Чернов, В.М.** Системы счисления в модулярных кольцах и их приложения к «безошибочным» вычислениям / В.М. Чернов // Компьютерная оптика. – 2019. –Т. 43, № 5. – С. 901-911. – DOI: 10.18287/2412-6179-2019-43-5-901-911.

Введение

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

Фактически, в указанной работе неявно рассматривалась более общая задача представления элементов кольца целых элементов $\mathbf{Z}(\sqrt{5})$ квадратичного поля $\mathbf{Q}(\sqrt{5})$, то есть множества

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

в форме

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

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

$$\phi = 2^{-1}\left(1 + \sqrt{5}\right),$$

то есть один из корней характеристического уравнения

$$w^2 - w - 1 = 0 \qquad (2)$$

для рекуррентной последовательности Фибоначчи

$$\Psi(n+2) = \Psi(n+1) + \Psi(n),\ \Psi(0) = \Psi(1) = 1. \qquad (3)$$

Система счисления с основанием ϕ получила в англоязычной литературе название «Phi number system» или «golden ratio number system» [2], а в русскоязычной литературе числовые последовательности «цифр» ξ_k, ассоциированные с (1), часто называют «кодами золотого сечения» [3].

Замечание 1. Отметим, что введенные в [4] так называемые *канонические системы счисления* (также с иррациональными основаниями) в квадратичных полях являются безызбыточными (т.е. представление (1) элемента в таких системах однозначно), но предполагают выполнение жесткого требования к алфавиту цифр Λ:

$$\Lambda = \left\{0, 1, \ldots \left| Norm(\omega) \right| - 1\right\}.$$

Из этого требования следует, в частности, отсутствие в вещественных квадратичных полях бинарных и тернарных систем счисления, *канонических* в смысле работ [4–5], и «неканоничность» системы счисления Бергмана (так как $Norm(\phi) = (-1)$). ■

Целью настоящей работы являются исследования по двум взаимосвязанным проблемам цифровой обработки сигналов.

Во-первых, развитие теории систем счисления «бергмановского» типа с целью разработки машинной арифметики, адекватной по своим структурным характеристикам общей концепции распараллеливания вычислений в системе остаточных классов (СОК) [6–7].

Во-вторых, синтез быстрых алгоритмов «безошибочных» вычислений, в частности вычисления дискретных сверток с помощью новых теоретико-числовых преобразований, реализуемых без умножений для данных, представленных в кодах, ассоциированных с новыми системами счисления «бергмановского» типа.

В работе [8] автора предложены подобные алгоритмы «безошибочного» вычисления свертки при

представлении целочисленных данных в кодах, ассоциированных с последовательностью Люка:

$$\Psi(n+2)=\Psi(n+1)+\Psi(n);\ \Psi(0)=2,\Psi(1)=1 \qquad (4)$$

и применении модулярных версий дискретного преобразования Фурье (преобразований Фурье–Галуа, теоретико-числовых преобразований) в специфической форме.

К сожалению, ни сумма, ни произведение чисел Люка (или Фибоначчи) таковыми не являются, что требует при реализации дополнительно приведения сумм/произведений к кодовому представлению или использования специализированных гипотетических «процессоров Фибоначчи».

В работе [9] предложен параллельный алгоритм «безошибочного» вычисления целочисленной свертки с помощью преобразований Фурье–Галуа в модулярном кольце по специально сконструированному модулю и свободному, в отличие от алгоритмов работы [8] от проблем, связанных с приведением промежуточных результатов к «законному виду». Тем не менее объективным недостатком работы [9] является то, что число возможных модулей теоретико-числовых преобразований и длин свёртки, для которых возможна реализация предложенных в этой работе алгоритмов, как и у алгоритмов работы [8], относительно невелико.

Это и определяет конкретные задачи работы – перенесение идей и методов работ [8–9] на более общий случай рекуррентных соотношений

$$\Psi\left(n\right)=a\Psi\left(n-1\right)+b\Psi\left(n-2\right);\ a,b\in\mathbf{Z} \qquad (5)$$

с характеристическим уравнением

$$w^2-aw-b=0\,. \qquad (6)$$

1. Основные идеи

Вычисление дискретной циклической свёртки последовательностей с периодом N

$$z\left(k\right)=\left(x*h\right)\left(k\right)=\sum_{n=0}^{N-1}x\left(n\right)h\left(k-n\right),\quad k=0,1,...,N-1 \qquad (7)$$

является одной из наиболее типичных задач цифровой обработки сигналов.

Для вычисления массива $z(k)$ непосредственно с помощью соотношения (7) требуется $O(N^2)$ сложений и умножений членов последовательностей $x(n)$ и $h(n)$. Для многих длин свёрток N существуют эффективные «спектральные» методы вычисления $z(m)$, которые основаны на применении дискретного преобразования Фурье (ДПФ) [10–11].

Если члены последовательностей $x(n)$ и $h(n)$ являются целыми (неотрицательными) числами, то для «безошибочного» вычисления свёртки можно использовать преимущества модулярных аналогов комплексных ДПФ:

$$\hat{x}(m)=\sum_{n=0}^{N-1}x(n)\omega^{mn}\pmod p\,, \qquad (8)$$

где p – достаточно большое простое число, $\omega\in\mathbf{GF}(p)$ – корень степени N из единицы в конечном поле $\mathbf{GF}(p)$ (то есть $Ord(\omega)$ – такое минимальное число k, что $\omega^k=1\in\mathbf{GF}(p)$ – равен N).

Теоретико-числовое преобразование (8) (ТЧП, преобразование Фурье–Галуа) имеет ряд недостатков, в частности, существует ограничение на длину преобразования и модуль, а именно требование делимости: $N|(p-1)$. Кроме того, арифметические операции $(\mathrm{mod}\,p)$ не являются элементарными компьютерными операциями. Но для некоторых простых p арифметика конечного поля $\mathbf{GF}(p)$ может быть более «дружественной компьютеру» (например, если $p=2^q-1$ – простое число Мерсенна). Более того, если $\omega\equiv 2(\mathrm{mod}\,p)$, то умножения в (8) могут быть заменены циклическими сдвигами векторов цифр в представлении элементов соответствующего конечного поля в двоичной системе счисления.

К сожалению, для конечных полей $\mathbf{GF}(p)$ по модулю чисел Мерсенна для мультипликативного порядка элемента $\omega\equiv 2(\mathrm{mod}\,p)$ справедливо равенство $Ord(\omega)=q$. Поэтому возможно вычислить теоретико-числовое преобразование (8) с использованием арифметики по модулю чисел Мерсенна без умножений только при $N=q$, то есть для

$$q=3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ ...\ .$$

Ещё большие трудности возникают в случае вычисления (7), когда $N\neq q$ является «немерсенновским» показателем. Несмотря на известный метод Рейдера–Винограда [11] вычисления ДПФ (или ТЧП), существуют, как показано в [8], «плохие» простые числа, для которых применение метода Рейдера–Винограда приводит к «быстрым» алгоритмам, мультипликативная сложность которых даже больше тривиальной $O(N^2)$.

Использование в качестве модулей в преобразовании (8) составных чисел p добавляет к непосредственно вычислительным проблемам принципиальные теоретические трудности, связанные с существованием в модулярных кольцах по составным модулям делителей нуля и, как следствие, с возможной необратимостью элементов соответствующих колец или с неортогональностью базисных функций преобразования (8).

Действительно, доказательство ортогональности базисных функций дискретного преобразования Фурье длины N сводится к проверке равенства

$$\sum_{n=0}^{N-1}\omega^{(m-k)n}\equiv\begin{cases}\dfrac{1-\omega^{(m-k)N}}{1-\omega^{(m-k)}}=0,\ \text{при } m\neq k\left(\mathrm{mod}\,N\right);\\ N,\ \text{при } m\equiv k\left(\mathrm{mod}\,N\right).\end{cases} \qquad (9)$$

Доказательство последнего соотношения представляет собой тривиальное упражнение на суммирование геометрической прогрессии и остаётся справедливым и для случая конечного поля, в котором существует корень степени N из единицы.

Условие «быть полем», то есть простота модуля p при рассмотрении преобразования (8) в фактор-кольцах $\mathbf{Z}/p\mathbf{Z}$, существенно. При простом p в рассматриваемых фактор-кольцах только нулевой элемент является необратимым, что гарантирует возможность «деления» на элемент $(1-\omega^{m-k})$ в равенстве (9). При составном модуле элемент $(1-\omega^{m-k})$ может быть необратимым и при $m \neq k \pmod N$.

При (паллиативном) распараллеливании вычислений в СОК характерные преимущества «битовой» реализации арифметических операций в полях, например, по модулям чисел Мерсенна не наследуются для вычислений в полях по модулям простых целых *сомножителей* составных чисел Мерсенна, так как эти сомножители уже числами Мерсенна не являются.

Дискретные ортогональные преобразования работы [9] могут быть реализованы параллельно «без умножений», но применяются к данным, представленным не в традиционной позиционной бинарной системе счисления, а в «системе счисления Люка». Для этого альтернативного представления сохраняются достоинства «мерсенновской» машинной арифметики для более широкого спектра длин ТЧП. В частности, использование таких преобразований для данных, представленных в этой альтернативной системе счисления, позволило существенно уменьшить мультипликативную сложность алгоритмов вычисления свёртки.

В настоящей работе мы также сохраняем общую идею работы [9] вычисления свёртки в кодах, связанных с системами счисления, порожденными линейными рекуррентными последовательностями второго порядка. Именно, предлагается версия алгоритмов, свободных от недостатков, связанных, в частности, с «нефибоначчиевостью» произведений чисел Фибоначчи или Люка, как в [7], которая достаточно эффективна для систем счисления, порождаемых более общими рекуррентными последовательностями.

Более точно: в настоящей работе предлагается достаточно общая схема параллельного вычисления дискретной свёртки (7) с помощью новых ТЧП «по составному модулю M». Определяется такое, вообще говоря, составное число M, что справедливо представление кольца классов вычетов $\mathbf{Z}(\sqrt{d})(\mathrm{mod}\, M)$ в форме прямой суммы

$$\mathbf{Z}\left(\sqrt{d}\right)\Big/_{M\mathbf{Z}} \cong \mathbf{Z}\left(\sqrt{d}\right)\Big/_{\left[\omega^n \pm 1\right]} \oplus \mathbf{Z}\left(\sqrt{d}\right)\Big/_{\left[\overline{\omega^n} \pm 1\right]},$$

где $\mathbf{Z}(\sqrt{d})$, d свободно от квадратов, есть кольцо целых элементов некоторого квадратичного поля $\mathbf{Q}(\sqrt{d})$ – поля разложения характеристического многочлена (6) рекуррентного соотношения (5), ω – корень уравнения (6), $[\omega^n \pm 1]$ – главный идеал, порожденный элементом $(\omega^n \pm 1)$, знаки в обозначении идеалов $[\omega^n \pm 1]$, $[\overline{\omega}^n \pm 1]$ выбраны согласованным образом (либо оба (+), либо оба (–)), а здесь и далее черта над символом означает не комплексное сопряжение, а сопряжение относительно единственного нетождественного автоморфизма Галуа:

$$\sigma : \omega = \mu + \eta\sqrt{d} \to \overline{\omega} = \mu - \eta\sqrt{d}\,. \qquad (10)$$

При некоторых дополнительных условиях, обсуждаемых ниже, вычисление свёртки может быть произведено по обычной параллельной схеме с применением семейства дискретных преобразований (аналогов ТЧП) в фактор-кольцах, т.е. в прямых слагаемых с последующей реконструкцией значения свёртки $(\mathrm{mod}\, M)$ по китайской теореме об остатках. Базисные функции $H_m(n)$ семейства этих преобразований в кольцах

$$\mathbf{Z}\left(\sqrt{d}\right)\Big/_{\left[\omega^n \pm 1\right]} = \mathbf{W}_1, \quad \mathbf{Z}\left(\sqrt{d}\right)\Big/_{\left[\overline{\omega^n} \pm 1\right]} = \mathbf{W}_2$$

выбираются в форме $H_m(n) = \omega^{mn}$ или $\overline{H}_m(n) = \overline{\omega}^{mn}$ соответственно.

Эффективность предложенной схемы вычислений связана, естественно, с возможностью эффективной реализации арифметических операций при представлении данных в «нетрадиционных» системах счисления. В частности, если входные данные преобразований в фактор-кольцах $\mathbf{W}_1$, $\mathbf{W}_2$ представлены в кодах, связанных с системами счисления «с основаниями ω, $\overline{\omega}$», то умножение на степени ω при вычислении таких дискретных преобразований реализуется сдвигами этих кодов.

В данной работе рассматривается случай числа (модуля) M, являющегося произведением *двух целых квадратичных* чисел, причем их произведение может быть как *простым целым рациональным* (т.е. «обычным» целым) числом, так и *составным целым рациональным* числом при выполнении некоторых условий.

2. Обобщенные бинарные и тернарные Phi- системы счисления

Для системы счисления работы [1] с основанием ϕ и цифровым множеством $\Lambda = \{0, 1\}$ (Phi-системы счисления) представление (1) требует использования отрицательных степеней ϕ даже для представления «обычных» целых чисел, например:

$$2 = 1\cdot\phi^{-2} + 0\cdot\phi^{-1} + 0\cdot\phi^{0} + 1\cdot\phi^{1}$$
$$4 = 1\cdot\phi^{-2} + 0\cdot\phi^{-1} + 1\cdot\phi^{0} + 0\cdot\phi^{1} + 1\cdot\phi^{2}.$$

Или, если воспользоваться в этом случае записью соотношения (1) в виде *кода цифр*

$$z = \sum_{k=-u(z)}^{v(z)} \xi_k \phi^k \leftrightarrow \left\langle \xi_{v(z)}, \xi_{v(z)-1}, ..., \xi_0; \xi_{-1}, ..., \xi_{-u(z)} \right\rangle, \qquad (11)$$

то, например, $4 \leftrightarrow \langle 1,0,1;0,1\rangle$ и т.п.

Система счисления Бергмана (Phi-система счисления) тесно связана с рекуррентным соотношением Фибоначчи (3), порождающим при различных начальных условиях $\Psi(0)$, $\Psi(1)$ различные последовательности:

(a) при $\Psi(0)=1=\phi^0, \Psi(1)=\phi^1=2^{-1}(1+\sqrt{5})$ порождается последовательность степеней числа ϕ;
(b) при $\Psi(0)=1=\Psi(1)$ порождается последовательность чисел Фибоначчи F_n:

1, 1, 2, 3, 5, 8, 13, ...

c) при $\Psi(0)=2$, $\Psi(1)=1$ порождается последовательность чисел Люка L_n;

2, 1, 3, 4, 7, 11, 18, ...

Как известно (напр., [12]), общим решением рекуррентного соотношения (3) является функция

$$\Psi(n)=C_1\phi^n+C_2\overline{\phi^n}=C_1\phi^n+C_2(-\phi)^{-n} \qquad (12)$$

с константами C_1, C_2, взаимно-однозначно связанными с начальными значениями $\Psi(0)$, $\Psi(1)$. (Последнее (правое) равенство в (12) справедливо в силу того, в характеристическом уравнении

$$w^2-w-1=0$$

рекуррентного соотношения (3) произведение корней уравнения равно (–1)). Отметим также, что для последовательности Люка константы C_1, C_2 в (12) равны: $C_1=C_2=1$.

Рассмотрим решение общего линейного рекуррентного соотношения второго порядка

$$\Psi(n)=a\Psi(n-1)+b\Psi(n-2) \qquad (13)$$

с такими начальными значениями $\Psi(0)$, $\Psi(1)$, что

$$\Psi(n)=\omega^n+\overline{\omega}^n, \qquad (14)$$

где ω, $\overline{\omega}$ – корни характеристического уравнения

$$w^2-aw-b=0 \qquad (15)$$

для рекуррентности (13).

Корни ω, $\overline{\omega}$ характеристического уравнения (15) есть элементы кольца целых $\mathbf{Z}(\sqrt{d})$ некоторого квадратичного поля. Как и ранее, в обозначении $\overline{\omega}$ черта над символом означает не комплексное сопряжение, а сопряжение относительно единственного нетождественного автоморфизма Галуа:

$$\tau:\omega=\alpha+\beta\sqrt{d}\to\overline{\omega}=\alpha-\beta\sqrt{d}\ .$$

Замечание 2. В настоящей работе рассматриваются только частные случаи при $a>0$, $b=\pm1$. Такой выбор знака $b=\pm1$ не является принципиальным, но обеспечивает простое соотношение $\overline{\omega}=\mp\omega^{-1}$ между корнями ω, $\overline{\omega}$ характеристического уравнения (15), а неположительность коэффициента a может привести к необходимости рассмотрения последовательностей $\Psi(n)$ с также неположительными значениями и, как следствие, к исследованию интересных, но малоизученных теоретических и прикладных вопросов, связанных с системами счисления с отрицательными основаниями (см., например, [13]).

Замечание 3. Решения рекуррентного соотношения (13) при $a>2$, $b=\pm1$ обладают рядом особенностей.

Во-первых, при $b=-1$ характеристическое уравнение $w^2-2w+1=0$ рекуррентного соотношения (13) имеет кратный корень $\theta=1$. Поэтому общее решение для $\Psi(n)$ в этом случае имеет вид

$$\Psi(n)=C_1\theta^n+C_2n\theta^n=C_1\cdot1+C_2\cdot n\cdot1$$

с константами C_1, C_2, взаимно-однозначно связанными с начальными значениями $\Psi(0)$, $\Psi(1)$.

Во-вторых, при $a=2$, $b=1$ решением соотношения (13) с «люкаподобными» начальными значениями

$$\Psi(0)=(\omega_2)^0+\overline{(\omega_2)^0}=2=\Psi(1)=(\omega_2)^1+\overline{(\omega_2)^1}$$

является последовательность только *четных* чисел. В этом случае рассматриваемые далее алгоритмы реализуются для последовательности (13) с начальными значениями

$$\Psi^*(0)=2^{-1}\left((\omega_2)^0+\overline{(\omega_2)^0}\right)=1,$$

$$\Psi^*(1)=2^{-1}\left((\omega_2)^1+\overline{(\omega_2)^1}\right)=1. \qquad \blacksquare$$

Табл. 1. Примеры параметров систем счисления для некоторых колец $\mathbf{Z}(\sqrt{d})$

a	b	ω_a	$\mathbf{Z}(\sqrt{d})$
1	–1	Нет, так как тогда $\omega_1=1$	–
	+1	$2^{-1}(1\pm\sqrt{5})$	$\mathbf{Z}(\sqrt{5})$
2	–1	Нет, так как тогда характеристическое уравнение имеет кратный корень	
	+1	$1\pm\sqrt{2}$	$\mathbf{Z}(\sqrt{2})$
3	–1	$2^{-1}(3\pm\sqrt{5})$	$\mathbf{Z}(\sqrt{5})$
	+1	$2^{-1}(3\pm\sqrt{13})$	$\mathbf{Z}(\sqrt{13})$

Так как при увеличении коэффициента a увеличивается сложность реализации арифметических операций в «ω_a-кодах», то мы ограничиваемся только подробным рассмотрением случая $a=3$, для которого основные идеи работы представляются в рафинированном виде.

2.1. Случай a = 3, b = 1

Рассмотрим рекуррентное соотношение (13), соответствующее рассматриваемому случаю

$$\Psi_+(n)=3\Psi_+(n-1)+\Psi_+(n-2). \qquad (16)$$

Пусть ω, $\overline{\omega}$ – корни характеристического уравнения соотношения (16):

$$\omega=2^{-1}\left(3+\sqrt{13}\right),\ \overline{\omega}=2^{-1}\left(3-\sqrt{13}\right),$$

пусть далее $\Psi_+(0)=2$, $\Psi_+(1)=3$; при таких начальных значениях соответствующее частное решение имеет вид $\Psi_+(n)=\omega^n+\overline{\omega}^n$ и порождает в некотором смысле обобщение классической последовательности Люка.

Так как (асимптотически) справедливы соотношения

$$3^n<\Psi_+(n)<4^n;\ \Psi_+(0)=2,\ \Psi_+(1)=3,\ \Psi_+(2)=11,$$

то с помощью обычной процедуры последовательного деления с остатком можно найти представление целого числа z в форме

$$z=\sum_{k=2}^{v(z)}\beta_k\Psi_+(k)+\rho,\ \ \beta_k\in\{0,1,2,3\},\tag{17}$$

где $0\le\rho<11=\Psi_+(2)$. Нетрудно убедиться в справедливости равенств:

$$10=2\cdot3+2\cdot2=2\cdot\Psi_+(1)+2\cdot\Psi_+(0),$$
$$9=3\cdot3+0\cdot2=3\cdot\Psi_+(1)+0\cdot\Psi_+(0),$$
$$8=2\cdot3+1\cdot2=2\cdot\Psi_+(1)+1\cdot\Psi_+(0),$$
$$7=1\cdot3+2\cdot2=1\cdot\Psi_+(1)+2\cdot\Psi_+(0),$$
$$6=2\cdot3+0\cdot2=3\cdot\Psi_+(1)+0\cdot\Psi_+(0)=0\cdot3+3\cdot2,$$
$$5=1\cdot3+1\cdot2=1\cdot\Psi_+(1)+1\cdot\Psi_+(0),$$
$$4=0\cdot3+2\cdot2=0\cdot\Psi_+(1)+2\cdot\Psi_+(0),$$
$$3=1\cdot3+0\cdot2=1\cdot\Psi_+(1)+0\cdot\Psi_+(0),$$
$$2=0\cdot3+1\cdot2=0\cdot\Psi_+(1)+1\cdot\Psi_+(0).$$

Несколько особняком стоит равенство для выражения числа (+1) из-за того, что $\Psi_+(n)>1$ при $n>0$:

$$1=1\cdot3+(-1)\cdot2=1\cdot\Psi_+(1)+(-1)\cdot\Psi_+(0).$$

Далее, так как $\Psi_+(n)=\omega^n+\overline{\omega^n}$, то

$$z=\sum_{k=0}^{v(z)}\beta_k\omega^k+\sum_{k=0}^{v(z)}\beta_k\overline{\omega^k}\triangleq X(z)+Y(z),$$
$$\beta_k\in\begin{cases}\{0,1,2,3\}\ \text{при}\ k>0;\\ \{0,1,2,3;-1\}\ \text{при}\ k=0,\end{cases}\tag{18}$$

а так как в рассматриваемом случае $\omega=-\overline{\omega^{-1}}$, то соотношение (17) приводится к виду

$$z=\sum_{k=-v(z)}^{v(z)}\eta_k\omega^k,\ \ \eta_k\in\{0\pm1,\pm2,\pm3\}.\tag{19}$$

Далее, из уравнений $\omega^2-3\omega-1=0$, $\overline{\omega}^2-3\overline{\omega}-1=0$ следуют правила преобразования цифрового алфавитного η-множества:

$$3=\omega-\omega^{-1},\quad 2=\omega-\omega^{-1}-1,$$
$$3=\overline{\omega}-\overline{\omega}^{-1},\quad 2=\overline{\omega}-\overline{\omega}^{-1}-1,\tag{20}$$

что окончательно позволяет привести и представление (19) целого z

$$z=\sum_{k=-u(z)}^{v(z)}\varsigma_k\omega^k,\ \varsigma_k\in\{-1,0,1\},\tag{21}$$

и ω, $\overline{\omega}$-компонент

$$X(z)=\sum_{k=v(z)}^{v(z)}\varsigma_k\omega^k,\ Y(z)=\sum_{k=v(z)}^{v(z)}\varsigma_k\overline{\omega^k};$$
$$\varsigma_k\in\{-1,0,1\}\tag{22}$$

к *тернарному* цифровому алфавиту.

2.2. Случай a=3, b=–1

Рассмотрим рекуррентное соотношение (13), соответствующее случаю

$$\Psi_-(n)=3\Psi_-(n-1)-\Psi_-(n-2).\tag{23}$$

Пусть ω, $\overline{\omega}$ – корни характеристического полинома соотношения (23):

$$\omega=2^{-1}\left(3+\sqrt{5}\right),\ \overline{\omega}=2^{-1}\left(3-\sqrt{5}\right).$$

Аналогично предыдущему пункту 2.1, при начальных значениях $\Psi_-(0)=2$, $\Psi_-(1)=3$ соответствующее частное решение, как и в подпараграфе 2.1, имеет вид

$$\Psi_-(n)=\omega^n+\overline{\omega^n}$$

и также порождает в некотором смысле обобщение классической последовательности Люка.

Так как $\Psi_-(3)=7$ и (асимптотически) справедливо неравенство $2^n<\Psi_-(n)<3^n$, то с помощью обычной процедуры последовательного деления с остатком можно найти представление целого числа в форме

$$z=\sum_{k=2}^{v(z)}\beta_k\Psi_-(k)+\rho,\ \ \beta_k\in\{0,1,2\},\tag{24}$$

где $0\le\rho<7=\Psi_-(2)$.

Нетрудно убедиться в справедливости равенств:

$$6=2\cdot3+0\cdot2=2\cdot\Psi_-(1)+0\cdot\Psi_-(0),$$
$$5=1\cdot3+1\cdot2=1\cdot\Psi_-(1)+1\cdot\Psi_-(0),$$
$$4=0\cdot3+2\cdot2=0\cdot\Psi_-(1)+2\cdot\Psi_-(0),\tag{25}$$
$$3=1\cdot3+0\cdot2=1\cdot\Psi_-(1)+0\cdot\Psi_-(0),$$
$$2=0\cdot3+1\cdot2=0\cdot\Psi_-(1)+1\cdot\Psi_-(0).$$

Здесь, как и в подпараграфе 2.1, также приходится выделять равенство для выражения числа (+1), так как $\Psi_-(n)>1$ при $n>0$:

$$1=1\cdot3+(-1)\cdot2=1\cdot\Psi_-(1)+(-1)\cdot\Psi_-(0).$$

В рассматриваемом случае $\omega=\overline{\omega^{-1}}$ и аналогично случаю подпараграфа 2.1 равенство представления элемента z последовательно приводится к виду

$$z=\sum_{k=-v(z)}^{v(z)}\eta_k\omega^k+\sum_{k=-v(z)}^{v(z)}\eta_k\overline{\omega}^k=X(z)+Y(z),$$
$$\eta_k\in\{0,\ 1,\ 2\}.$$

Далее из уравнений $\omega^2-3\omega-1=0$, $\overline{\omega}^2-3\overline{\omega}-1=0$ следуют правила преобразования цифрового алфавитного η-множества:

$$2=\omega+\omega^{-1}-1,\quad 2=\overline{\omega}+\overline{\omega}^{-1}-1,$$

что, аналогично случаю 2.1, позволяет привести и представление целого z и компонент $X(z)$, $Y(z)$ к *тернарному* цифровому алфавиту $\{-1,0,1\}$.

3. Синтез специальных модулей для параллельных теоретико-числовых преобразований

Рассмотрим последовательности целых чисел:

$$M_{(+1)}^{-}(n)=-\left(\omega^n-1\right)\left(\overline{\omega^n}-1\right)=-1-(-1)^n+\Psi_+(n),$$
$$M_{(+1)}^{+}(n)=\left(\omega^n+1\right)\left(\overline{\omega^n}+1\right)=1+(-1)^n+\Psi_+(n),\tag{26}$$

где ω, $\overline{\omega}$ – корни характеристического уравнения соответствующего рекуррентного соотношения (16) или (23). Будем рассматривать далее последовательность

$$M^{\pm}_{(+1)}(n)=\left(\omega^n\pm1\right)\left(\overline{\omega^n}\pm1\right)=\pm\left(1+(-1)^n\right)+\Psi_+(n),$$

где, для краткости

$$\begin{aligned}&\Psi_+(n)\triangleq\Psi(n)=3\Psi(n-1)+\Psi(n-2);\\&\Psi(0)=2,\ \Psi(1)=3.\end{aligned}\qquad(27)$$

В рассматриваемом случае корни ω, $\overline{\omega}$ характеристического уравнения рекуррентного соотношения (27) равны

$$\omega=2^{-1}\left(3+\sqrt{13}\right),\ \overline{\omega}=2^{-1}\left(3-\sqrt{13}\right),$$

Зафиксируем некоторое натуральное n и рассмотрим канонические гомоморфизмы λ_1, λ_2 кольца $\mathbf{Z}(\sqrt{d})$ (в данном случае кольца $\mathbf{Z}(\sqrt{13})$):

$$\begin{aligned}&\lambda_1:\mathbf{Z}(\sqrt{13})\to\frac{\mathbf{Z}(\sqrt{13})}{\left[\omega^n+1\right]}\cong\mathbf{F}_1;\\&\lambda_2:\mathbf{Z}(\sqrt{13})\to\frac{\mathbf{Z}(\sqrt{13})}{\left[\overrightarrow{\omega}^n+1\right]}\cong\mathbf{F}_2.\end{aligned}\qquad(28)$$

При этих редуцирующих отображениях элементы

$$\begin{aligned}&X(\mathrm{z})=\sum_{k=v(z)}^{v(z)}\varsigma_k\omega^k,\mathrm{Y}(\mathrm{z})=\sum_{k=v(z)}^{v(z)}\varsigma_k\overline{\omega^k};\\&\varsigma_k\in\{-1,\,0,\,1\}\end{aligned}\qquad(29)$$

преобразуются в элементы конечных колец $\mathbf{F}_1$, $\mathbf{F}_2$ так, что

$$\begin{aligned}&\lambda_1:X(\mathrm{z})\to X_{red}(\mathrm{z})=\sum_{k=0}^{v(z)}\chi_k g_1^k,\\&\lambda_2:Y(\mathrm{z})\to\mathrm{Y}_{red}(\mathrm{z})=\sum_{k=0}^{v(z)}\chi_k g_2^k,\end{aligned}\qquad(30)$$

где $g_1=\lambda_1(\omega)$, $g_2=\lambda_2(\overline{\omega})$, $\chi_k\in\{-1,0,1\}$.

Замечание 4. Автор счел возможным опустить детальное описание рутинных выкладок, относящихся к преобразованию представлений элементов (29) в представления редуцированных элементов (30). ■

Следующее ниже утверждение подводит формальное обоснование возможности параллельной реализации вычислений в конечном кольце $\mathbf{Z}(\sqrt{d})(\mathrm{mod}\,M(n))$.

Утверждение 1. Пусть $M^{\pm}_{(+1)}$ – любое из чисел $M^{+}_{(+1)}(n)$, $M^{-}_{(+1)}(n)$, определенных равенствами (26). Пусть $z\in\mathbf{Z}(\sqrt{13})$; z_{red}, $X_{red}(z)$, $Y_{red}(z)$ – редукции z по модулям $M^{\pm}_{(+1)}$, $[\omega^n\pm1]$, $[\overline{\omega^n}\pm1]$ соответственно. Тогда, если $M^{\pm}_{(+1)}\neq0(\mathrm{mod}\,4)$, то справедливо равенство

$$z_{red}=\rho_1\cdot X_{red}(\mathrm{z})\cdot\left(\overline{\omega^n}\pm1\right)+\rho_2\cdot Y_{red}(\mathrm{z})\cdot\left(\omega^n\pm1\right),\qquad(31)$$

где для $M^{\pm}_{(+1)}=M^{\pm}_{(+1)}(n)$ с нечетными номерами n коэффициент $\rho_{1,2}=(\mp2)^{-1}(\mathrm{mod}\,M^{\pm}_{(+1)})$.

Доказательство. Проверка (31) сводится к несложным преобразованиям:

$$\begin{aligned}&z\left(\mathrm{mod}\left[\omega^n\pm1\right]\right)\equiv\\&\equiv\left\{\rho_1\cdot X_{red}(\mathrm{z})\cdot\left(\overline{\omega^n}\pm1\right)+\right.\\&\quad\left.+\left\{\rho_2\cdot Y_{red}(\mathrm{z})\cdot\left(\omega^n\pm1\right)\right\}\left(\mathrm{mod}\left[\omega^n\pm1\right]\right),\ 0\right.\\&\equiv\rho_1\cdot X_{red}(\mathrm{z})\cdot\left(\overline{\omega^n}\pm1\right)\left(\mathrm{mod}\left[\omega^n\pm1\right]\right)\equiv\\&\equiv X_{red}(\mathrm{z})\cdot\left(\rho_1\cdot\left(\overline{\omega^n}\pm1\right)\mathrm{mod}\left[\omega^n\pm1\right]\right)\equiv\\&\equiv X_{red}(\mathrm{z})\cdot\left(\rho_1\cdot\left((-\omega)^{-n}\pm1\right)\mathrm{mod}\left[\omega^n\pm1\right]\right)\equiv\\&\equiv X_{red}(\mathrm{z})\cdot\left(\rho_1\cdot\left((-1)^{-n}\pm(-1)^n\right)\times\right.\\&\quad\left.\times\left((-1)^{-n}\left(\mathrm{mod}\left[\omega^n\pm1\right]\right)\right)\equiv\right.\\&\equiv X_{red}(\mathrm{z})\cdot\left(\rho_1\cdot\left((-1)^{-n}\mp1\right)\times\right.\\&\quad\left.\times\left((\mp1)\cdot\left(\mathrm{mod}\left[\omega^n\pm1\right]\right)\right)\equiv\right.\\&\equiv X_{red}(\mathrm{z})\cdot\rho_1\times\\&\quad\times\begin{cases}0,\ \text{при чётном}\quad n;\\\pm2,\ \text{при нечётном}\ n.\end{cases}\left(\mathrm{mod}\left[\omega^n\pm1\right]\right).\end{aligned}\qquad(32)$$

Аналогично проверяется и равенство

$$\begin{aligned}&z\left(\mathrm{mod}\left[\overline{\omega}^n\pm1\right]\right)\equiv\mathrm{Y}_{red}(\mathrm{z})\times\\&\quad\times\rho_2\cdot\begin{cases}0,\ \text{при чётном}\quad n;\\\pm2,\ \text{при нечётном}\ n.\end{cases}\left(\mathrm{mod}\left[\overline{\omega}^n\pm1\right]\right).\end{aligned}$$

■

Замечание 5. Отметим, что хрестоматийный вариант равенства (31), являющийся формальным обоснованием возможности распараллеливания вычислений $(\mathrm{mod}\,M)=(\mathrm{mod}\,PQ)$ в СОК, предполагает взаимную простоту сомножителей $PQ=M$. Заметим, что в общем случае это требование «Китайской теоремы об остатках» является только достаточным. В Утверждении 1 рассматривается как раз случай «разумной достаточности» ограничений, гарантирующих обратимость элемента $2\in\mathbf{F}_1\mathbf{F}_2$, необходимую для корректности определения параметров $\rho_{1,2}$. Таким «гарантом» является условие $M^{\pm}_{(+1)}\neq0\left(\mathrm{mod}\,4\right)$. ■

Рассмотрим аналогично числа $M^{\pm}_{(+1)}(n)$:

$$\begin{aligned}&M^{-}_{(-1)}(n)=-\left(\omega^n-1\right)\left(\overline{\omega^n}-1\right)=-2+\Psi_-(n),\\&M^{+}_{(-1)}(n)=\left(\omega^n+1\right)\left(\overline{\omega^n}+1\right)=2+\Psi_-(n).\end{aligned}\qquad(33)$$

Утверждение 2. Пусть $M^{\pm}_{(-1)}$ – любое из чисел $M^{+}_{(-1)}(n)$, $M^{-}_{(-1)}(n)$, определенных равенствами (33). Пусть $z\in\mathbf{Z}(\sqrt{5})$; z_{red}, $X_{red}(z)$, $Y_{red}(z)$ – редукции z по

модулям $M^{\pm}_{(-1)}$, $[\omega^n \pm 1]$, $[\overline{\omega}^n \pm 1]$ соответственно. Тогда для $M^{+}_{(-1)}$ справедливо равенство

$$z_{red} = \rho \cdot X_{red}(\mathrm{z}) \cdot \left(\overline{\omega}^n \pm 1\right) + \rho \cdot Y_{red}(\mathrm{z}) \cdot \left(\omega^n \pm 1\right), \qquad (34)$$

где $\rho = 2^{-1} (\mathrm{mod}\, M^{+}_{(-1)})$.

Доказательство. Так как ω, $\overline{\omega}$ – корни характеристического уравнения соотношения (23), равны

$$\omega = 2^{-1}\left(3+\sqrt{5}\right),\ \overline{\omega} = 2^{-1}\left(3-\sqrt{5}\right),$$

и, кроме того, $\omega^{-1} = \overline{\omega}$, то:

$$z\left(\mathrm{mod}\left[\omega^n \pm 1\right]\right) \equiv \left\{\rho \cdot X_{red}(\mathrm{z}) \cdot \left(\overline{\omega^n} \pm 1\right) + \right.$$
$$\left. + \left\{\rho \cdot Y_{red}(\mathrm{z}) \cdot \left(\omega^n \pm 1\right)\right\}\left(\mathrm{mod}\left[\omega^n \pm 1\right]\right),\right.$$
$$\equiv \rho \cdot X_{red}(\mathrm{z}) \cdot \left(\overline{\omega^n} \pm 1\right)\left(\mathrm{mod}\left[\omega^n \pm 1\right]\right) \equiv$$
$$\equiv X_{red}(\mathrm{z})\left(\rho\left(\omega^{-n} \pm 1\right)\mathrm{mod}\left[\omega^n \pm 1\right]\right) \equiv$$
$$\equiv \rho X_{red}(\mathrm{z}) \begin{cases} 0 \text{ для } M^{-}_{(-1)}; \\ 2 \text{ для } M^{+}_{(-1)}. \end{cases}$$

Аналогично вычисляется коэффициент ρ для редукции $z(\mathrm{mod}[\overline{\omega}^n \pm 1])$. ■

4. Параллельное ТЧП в редуцированных кольцах

Пусть ω – корень характеристического полинома одного из рекуррентных соотношений (16), (23); пусть далее: $H_m(t) = \omega^{mt}$; $m, t \in \mathbf{Z}$. Пусть $M = M^{\pm}_{(\pm 1)}$ – одно из чисел, (26) или (33).

Определение 1. Число $M(n) = M^{\pm}_{(\pm 1)}(n)$ будем называть нормальным числом, если $M(s)$ и $M(n)$ взаимно простые для всех $0 < s < n$.

(Заметим, что если $M(n)$ – простое число, то оно нормальное, но не всякое нормальное число является простым).

Утверждение 3. Если $M = M(n)$ – нормальное число, то функции $H_m(n)$ ортогональны в форме:

$$\sum_{t=0}^{K-1} H_p(t) \cdot \sigma\left(H_q(t)\right) \equiv \delta(p,q) K \left(\mathrm{mod}\, M\right),$$

где δ – дельта Кронекера, σ – автоморфизм (10), и

$$K = \begin{cases} n, & \text{при } M = M^{\pm}_{(+1)}; \\ 2n, & \text{при } M = M^{\pm}_{(-1)}. \end{cases}$$

Доказательство. Если и $M = M^{\pm}_{(-1)}(n)$ – нормальное число, то доказательство тривиально:

$$\sum_{t=0}^{n-1} H_p(t) \cdot \sigma\left(H_q(t)\right) \equiv \sum_{t=0}^{n-1} \omega^{pt} \omega^{-qt} \equiv$$
$$\equiv \begin{cases} \dfrac{1-\omega^{(p-q)n}}{1-\omega^{(p-q)}} = 0, & \text{при } p \neq q \left(\mathrm{mod}\, K\right); \\ n = K, & \text{при } p \equiv q \left(\mathrm{mod}\, K\right), \end{cases}$$

так как в силу условия нормальности $M = M(n)$

$$Norm(1-\omega^s) = M(\mathrm{s}) \text{ и } \gcd(M(n), M(\mathrm{s})) = 1,$$

что обеспечивает обратимость $1-\omega^{(p-q)} (\mathrm{mod}\, M)$ при p, q из рассматриваемого диапазона.

При $M = M^{\pm}_{(+1)}(n)$ имеем:

$$\sum_{t=0}^{2n-1} H_p(t) \cdot \sigma\left(H_q(t)\right) \equiv \sum_{t=0}^{n-1} H_p(2t) \cdot \sigma\left(H_q(2t)\right) +$$
$$+ \sum_{t=0}^{n-1} H_p(2t+1) \cdot \sigma\left(H_q(2t+1)\right) \equiv$$
$$\equiv \sum_{t=0}^{n-1} \omega^{2pt} \cdot \omega^{-2qt} - \sum_{t=0}^{n-1} \omega^{p(2t+1)} \cdot \omega^{-(2t+1)q} \equiv$$
$$\equiv \frac{1-\omega^{2(p-q)n}}{1-\omega^{2(p-q)}} - \omega^{(p-q)} \frac{1-\omega^{2(p-q)n}}{1-\omega^{2(p-q)}} \equiv$$
$$\equiv \left(1-\omega^{(p-q)}\right) \frac{1-\omega^{2(p-q)n}}{1-\omega^{2(p-q)}} \left(\mathrm{mod}\, M\right) =$$
$$= \begin{cases} 0, \text{ при } p \neq q \left(\mathrm{mod}\, K\right); \\ 2n = K, \text{ при } p \equiv q \left(\mathrm{mod}\, K\right). \end{cases}$$

■

Определение 2. Вектор цифр $\chi_k \in \{-1,0,1\}$ в представлении элементов $X_{red}(z)$, $Y_{red}(z)$ в форме (30), где $K = n$ или $K = 2n$ (в зависимости от того $M = M^{-}_{(\pm 1)}(n)$ или $M = M^{+}_{(\pm 1)}(n)$), будем называть *редуцированным кодом компонент элемента z* и обозначать

$$X_{red}(z), Y_{red}(z) \sim \left\langle \chi_0, \chi_1, ..., \chi_{K-1} \right\rangle. \qquad (35)$$

Естественно, что арифметические операции в факторкольцах

$$\frac{\mathbf{Z}\left(\sqrt{d}\right)}{\left[\omega^n \pm 1\right]} = \mathbf{W}_1, \frac{\mathbf{Z}\left(\sqrt{d}\right)}{\left[\overline{\omega^n} \pm 1\right]} = \mathbf{W}_2$$

индуцируют правила действия над кодами.

Рассмотрим теперь преобразования в кольцах $\mathbf{W}_1, \mathbf{W}_2$ – аналоги канонических преобразований Фурье–Галуа:

$$\widehat{X}_{red}(m) = \sum_{t=0}^{K-1} X_{red}\left(z(t)\right) \omega^{mt} \left(\mathrm{mod}\left[\omega^n \pm 1\right]\right),$$
$$\widehat{Y}_{red}(m) = \sum_{t=0}^{K-1} Y_{red}\left(z(t)\right) \overline{\omega}^{mt} \left(\mathrm{mod}\left[\overline{\omega}^n \pm 1\right]\right), \qquad (36)$$
$$m \in \{0,1,...,K-1\}.$$

Пусть далее **J** – оператор циклического сдвига кода вправо

$$\mathbf{J}: \left\langle \chi_0, \chi_1, ..., \chi_{K-1} \right\rangle \to \left\langle \chi_{K-1}, \chi_0, \chi_1, ..., \chi_{K-2} \right\rangle.$$

Наряду с преобразованиями (36), будем рассматривать их выражения в «кодовом виде»:

$$\left\langle \widehat{X_{red}}(m) \right\rangle = \sum_{t=0}^{K-1} \mathbf{J}^{mt} \left\langle X_{red}\left(z(t)\right) \right\rangle,$$
$$\left\langle \widehat{Y_{red}}(m) \right\rangle = \sum_{t=0}^{K-1} \mathbf{J}^{-mt} \left\langle Y_{red}\left(z(t)\right) \right\rangle, \qquad (37)$$
$$m \in \{0,1,...,K-1\}.$$

Утверждение 4. Пусть преобразования компонент $X_{red}(z)$, $Y_{red}(z)$ заданы соотношениями (36).

Тогда преобразования

$$X_{red}\left(z(t)\right)=K^{-1}\sum_{t=0}^{K-1}\widehat{X_{red}}(m)\omega^{mt}\left(\mathrm{mod}\left[\omega^{n}\pm 1\right]\right),$$

$$Y_{red}\left(z(t)\right)=K^{-1}\sum_{t=0}^{K-1}\widehat{Y_{red}}(m)\overline{\omega}^{mt}\left(\mathrm{mod}\left[\overline{\omega}^{n}\pm 1\right]\right), \qquad (38)$$

$$t,m\in\{0,1,...,K-1\}$$

являются обратными к преобразованиям (36).

Доказательство. Непосредственная проверка. ■

5. Алгоритм безошибочного вычисления циклической свёртки

Вычисление дискретной циклической свертки является массовой задачей цифровой обработки сигналов. В ряде случаев (например, в криптографии) не допускается приближенное вычисление значений этой свертки. Именно это, начиная с работы [14] об умножении больших целых чисел («алгоритм Шёнхаге–Штрассена»), и послужило толчком к исследованию дискретного преобразования Фурье в модулярных кольцах, то есть ТЧП.

Ниже изложим кратко обычную схему «спектрального» вычисления дискретной циклической свертки двух n-периодических функций $a(k)$ и $h(k)$, адаптированную к особенностям рассматриваемого в работе подхода.

Шаг 1. Согласно Утверждениям 1 и 2 выбирается число $M=M_{(\pm 1)}^{\pm}$ такое, что

$$M>n\cdot\max\{a(k)\}\cdot\max\{h(k)\},$$

и находятся кодовые представления проекций значений $a(k)$ и $h(k)$ в соответствующих кольцах

$$\mathbf{Z}\left(\mathrm{mod}\left[\omega^{n}\pm 1\right]\right),\ \mathbf{Z}\left(\mathrm{mod}\left[\overline{\omega}^{n}\pm 1\right]\right),$$

то есть $\langle a_{\omega}(k)\rangle$, $\langle a_{\overline{\omega}}(k)\rangle$, $\langle h_{\omega}(k)\rangle$, $\langle h_{\overline{\omega}}(k)\rangle$.

Шаг 2. Вычисляются результаты преобразования (36) в форме (37): $\langle\widehat{a_{\omega}}(m)\rangle,\langle\widehat{a_{\overline{\omega}}}(m)\rangle,\langle\widehat{h_{\omega}}(m)\rangle,\langle\widehat{h_{\overline{\omega}}}(m)\rangle$; эти вычисления не требуют умножений.

Шаг 3. Вычисляются массивы кодов

$$\left\langle\widehat{a_{\omega}}(m)\cdot\widehat{h_{\omega}}(m)\right\rangle,\left\langle\widehat{a_{\overline{\omega}}}(m)\cdot\widehat{h_{\overline{\omega}}}(m)\right\rangle.$$

Эти вычисления также не требуют нетривиальных умножений.

Шаг 4. Выполняются обратные преобразования Утверждения 4, то есть коды компонентов свертки:

$$\left\langle\widehat{a_{\omega}}(m)\cdot\widehat{h_{\omega}}(m)\right\rangle\rightarrow\left\langle(a*h)_{\omega}(k)\right\rangle,$$

$$\left\langle\widehat{a_{\overline{\omega}}}(m)\cdot\widehat{h_{\overline{\omega}}}(m)\right\rangle\rightarrow\left\langle(a*h)_{\overline{\omega}}(k)\right\rangle.$$

Шаг 5. В соответствии с Утверждениями 1 и 2 проводится реконструкция значений $(a*h)(k)$.

6. Некоторые численные результаты

В этом параграфе, исключительно в качестве иллюстрации, приводятся численные результаты, касающиеся «непустоты» множеств чисел $M_{(-1)}^{\pm}=M_{(-1)}^{\pm}(n)$, для которых выполняются (или не выполняются (*)) Утверждения 1 и 2.

Табл. 2. Свойства чисел $M_{(+1)}^{-}$

n	$\Psi_{+}(n)$	$M_{(+1)}^{-}(n)$	Факторизация	Простота
1	3	3	3	**простое**
2	11	9	3^2	*
3	36	36	$2^2\cdot 3^2$	*
4	155	153	$3^2\cdot 17$	*
5	501	501	3^2	*
6	1658	1656	$2^3\cdot 3^2\cdot 23$	*
7	5475	5475	$3\cdot 5^2\cdot 73$	*
8	18083	18081	$3^2\cdot 7^2\cdot 41$	*
9	59724	59724	$2^2\cdot 3^3\cdot 7\cdot 79$	*
10	197255	197253	$3^2\cdot 7\cdot 31\cdot 101$	*

Табл. 3. Свойства чисел $M_{(+1)}^{+}$

n	$\Psi_{+}(n)$	$M_{(+1)}^{+}(n)$	Факторизация	Простота
1	3	3	3	**простое**
2	11	13	13	**простое**
3	36	36	$2^2\cdot 3^2$	*
4	155	157	157	**простое**
5	501	501	3^2	*
6	1658	1660	$2^2\cdot 5\cdot 83$	*
7	5475	5475	$3\cdot 5^2\cdot 73$	*
8	18083	18085	$5\cdot 3617$	**нормальное**
9	59724	59724	$2^2\cdot 3^3\cdot 7\cdot 79$	*
10	197255	197257	197257	**простое**

Табл. 4. Свойства чисел $M_{(-1)}^{-}$

n	$\Psi_{-}(n)$	$M_{(-1)}^{-}(n)$	Факторизация	Простота
1	3	1	1	
2	7	5	5	**простое**
3	18	16	2^4	*
4	47	45	$3^2\cdot 5$	*
5	123	121	11^2	**нормальное**
6	322	320	$2^6\cdot 5$	*
7	843	841	29^2	**нормальное**
8	2207	2205	$3^2\cdot 5\cdot 7^2$	*
9	5778	5776	$2^4\cdot 19^2$	*
10	15127	15125	$5^3\cdot 11^2$	*

Табл. 5. Свойства чисел $M_{(-1)}^{+}$

n		$M_{(-1)}^{+}(n)$	Факторизация	Простота
0	2	4	2^2	
1	3	5	5	**простое**
2	7	9	3^2	*
3	18	20	$2^2\cdot 5$	*
4	47	49	7^2	**нормальное**
5	123	125	5^3	*
6	322	324	$2^2\cdot 3^4$	*
7	843	845	$5\cdot 13^2$	*
8	2207	2209	47^2	**нормальное**
9	5778	5780	$2^2\cdot 5\cdot 17^2$	*
10	15127	15129	$3^2\cdot 41^2$	*

Заключительные замечания

1. Несмотря на давнее и локально-эффективное использование чисел Фибоначчи, «золотого сечения»

и т. п. в прикладных задачах (сортировка данных, построение квадратурных формул для численного интегрирования, криптография), значительная часть публикаций этой тематики связана фактически с нумерологией, к «научному жанру» не относящейся. Хотя автор настоящей работы и использовал числа Фибоначчи, Люка и т.п. для решения частных задач цифровой обработки сигналов [15–17], он никогда не разделял энтузиазма в поисках «Всеобщей Гармонии» и/или построения «Общей Теории Всего» на основе анализа тех или иных числовых феноменов [18].

Отметим также, что заверения многочисленных авторов в научной новизне использования ими СОК при решении тех или иных вычислительных задач зачастую базируются на малоубедительных аргументах.

Действительно, тезис, что «если алгебраическая структура **A** изоморфна прямой сумме структур той же категории $\mathbf{A} \cong \mathbf{A}_1 \oplus \mathbf{A}_2 \oplus \ldots \mathbf{A}_r$, то вычисления в **A** можно распараллелить и заменить «покоординатными» вычислениями в $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_r$, является давно известным, хрестоматийным фактом, частные случаи систематического использования которого восходят едва ли ни к методу координат Р. Декарта.

Основная масса работ по применению СОК, всё же претендующих на научную новизну, относится, по мнению автора, к двум основным категориям.

(А) Предлагается (*новое*) представление (*новой*) алгебраической структуры **A** в виде прямой суммы субструктур, операции в которых реализуются эффективно и «дружественно» по отношению к архитектуре используемых вычислительных средств, что и является основным *теоретическим* достижением таких работ. *Техническая* сторона в этом случае сводится к достаточно рутинной работе – к синтезу эффективных алгоритмов проектирования данных в слагаемые прямой суммы и алгоритма «склеивания» окончательного результата в структуре **A** из «частичных» результатов вычислений в $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_r$.

(Б) Используется хорошо известная версия СОК для решения задач в «новой» предметной области. *Научная новизна* решения, как задачи информатики, оправдывается важностью решения «народохозяйственной задачи» и её социальной значимостью.

Автор всё же надеется, что представленная работа относится к категории (А).

2. Рассмотренный подход экстраполируется и на случай неквадратичных алгебраических расширений.

В этом случае реализация метода сводится к нескольким задачам при определении такого числа M, что

$$\frac{\mathbf{Z}}{M\mathbf{Z}} \subseteq \mathbf{Z}(\mathbf{K}) \cong \sum_{\sigma \in \mathbf{H}}^{\oplus} \left(\frac{\mathbf{Z}(\mathbf{K})}{\left[\sigma(\alpha^r) \pm 1 \right]} \right), \tag{39}$$

где
– сумма в (39) прямая;
– суммирование ведется по автоморфизмам подгруппы **H** группы Галуа **G** характеристического полинома линейного рекуррентного соотношения

$$P(n) = \sum_{k=1}^{N} \beta_k P(n-k); \tag{40}$$

– **Z**(**K**) – кольцо целых поля **K** – поля разложения характеристического полинома

$$h(w) = w^N - \sum_{k=1}^{N} \beta_k w^{N-k} \tag{41}$$

рекуррентного соотношения (40) над **Q**;
– α – корень полинома (41);
– $[\alpha^r \pm 1]$ – главный идеал, порожденный элементом $(\alpha^r \pm 1)$;
– справедливо равенство

$$\beta_0 = \pm 1 = \pm \prod_{\sigma \in \mathbf{H}} \sigma(\alpha).$$

В этом случае основную теоретическую сложность представляет исследование систем счисления в кольцах целых неквадратичных расширений, определение параметров систем счисления и связанных с особенностями оснований этих систем счисления свойствами линейных рекуррентных соотношений высоких порядков. После нахождения требуемых параметров вычисление свёртки также может быть произведено по хрестоматийной параллельной схеме с применением семейства дискретных преобразований (аналогов ТЧП) в фактор-кольцах с последующей реконструкцией значения свёртки ($\mathrm{mod}\, M$) по китайской теореме об остатках. Базисные функции этих преобразований выбираются, как и ранее, в форме

$$h_m^{\sigma}(n) = \left(\sigma(\alpha) \right)^{mn}.$$

В частности, нетрудно показать возможность перенесения методов данной работы на случай простого M при

$$M = \left(\alpha^n + 1 \right) \left(\beta^n + 1 \right) \left(\gamma^n + 1 \right),$$

где α, β, γ – корни характеристического уравнения

$$w^3 - w^2 - w - 1 = 0$$

для рекуррентного соотношения («последовательность трибоначчи» [19])

$$T(n+3) = T(n+2) + T(n+1) + T(n)$$

с «неканоническими» в сравнении с [19] начальными значениями $T(0) = 3$, $T(1) = 1$, $T(2) = 3$.

Эффективность предложенной схемы вычислений определяется, как и ранее в данной работе, возможностью эффективной реализации арифметических операций при представлении данных в «нетрадиционных» системах счисления.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования РФ в рамках выполнения работ по Государственному заданию ФНИЦ «Кристаллография и фотоника» РАН (соглашение № 007-

ГЗ/Ч3363/26) в части исследования систем счисления и Российского фонда фундаментальных исследований (проекты РФФИ №19-07-00357 А № 18-29-03135_ мк) в части исследования машинной арифметики.

Литература

1. **Bergman, G.** A number system with an irrational base / G. Bergman // Mathematics Magazine. – 1957. – Vol. 31, Issue 2. – P. 98-110.
2. **Rousseau, C.** The Phi number system revisited. / G. Rousseau // Mathematics Magazine. – 1995. – Vol. 48, Issue 4. – P. 283-284.
3. **Стахов, А.П.** Коды золотой пропорции / А.П. Стахов // М.: Радио и связь, 1984. – 152 с.
4. **Katai, I.** Canonical number systems for complex integers / I. Katai, J. Szabo // Acta Scientiarum Mathematicarum. – 1975. – Vol. 37. – P. 255-260.
5. **Thuswardner, J.** Elementary properties of canonical number systems in quadratic fields / J. Thuswaldner. – In: Application of Fibonacci numbers / ed. by G.E. Bergum). – Dordrecht, Boston, London: Kluwer Academic Publishers, 1996. – Vol. 7. – P. 405-414.
6. **Ananda Mohan, P.V.** Residue number systems / P.V. Ananda Mohan. – Basel: Birkhäuser, 2016. – 351 p. – ISBN: 978-3-319-41383-9.
7. Embedded systems design with special arithmetic and number systems / ed. by A.S. Molahosseini, L.S. de Sousa, C.-H. Chang. – Springer International Publishing AG, 2017. – 389 p. – ISBN: 978-3-319-49741-9.
8. **Chernov, V.** Fast algorithm for “error-free” convolution computation using Mersenne-Lucas codes / V. Chernov // Chaos, Solitons and Fractals. – 2006. – Vol. 29. – P. 372-380.
9. **Чернов, В.М**. Квазипараллельный алгоритм для 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.
10. **Nussbaumer, H.J.** Fast Fourier transform and convolution algorithms / H.J. Nussbaumer. – Berlin, Heidelberg: Springer-Verlag, 1981.
11. **Блейхут, Р.** Быстрые алгоритмы цифровой обработки сигналов / Р. Блейхут; пер с англ. – М: Мир, 1989. – 448 с.
12. **Wimp, J.** Computations with recurrence relations / J. Wimp // Boston, MA: Pitman, 1984.
13. **Masáková, Z.** Arithmetics in number systems with a negative base / Z. Masáková, E. Pelantová, T. Vávra // Theoretical Computer Science. – 2011. – Vol. 412, Issues 8-10. – P. 835-845.
14. **Schönhage, A**. Schnelle Multiplikation großer Zahlen / A. Schönhage, V. Strassen // Computing. – 1971. – Vol. 7. – P. 281-292.
15. **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.
16. **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(1). – P. 91-100.
17. **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.
18. **Stakhov, A.P.** The mathematics of harmony: From Euclid to contemporary mathematics and computer science / A.P. Stakhov. – Singapore: World Scientific, 2009.
19. **Feinberg, M.** Fibonacci-Tribonacci / M. Feinberg // The Fibonacci Quarterly. – 1963. – Vol. 1(30). – P. 71-74.

Сведения об авторе

Чернов Владимир Михайлович, 1949 года рождения, 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
Поступило в редакцию 31 июля 2019 г. Окончательный вариант – 5 сентября 2019 г.

Number systems in modular rings and their applications to "error-free" computations

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

Abstract

The article introduces and explores new systems of parallel machine arithmetic associated with the representation of data in the redundant number system with the basis, the formative sequences of degrees of roots of the characteristic polynomial of the second order recurrence. Such number systems are modular reductions of generalizations of Bergman's number system with the base equal to the "Golden ratio". The associated Residue Number Systems is described. In particular, a new "error-free" algorithm for calculating discrete cyclic convolution is proposed as an application

to the problems of digital signal processing. The algorithm is based on the application of a new class of discrete orthogonal transformations, for which there are effective “multipication-free” implementations.

Keywords: number system, modular arithmetic, discrete convolution, residue number systems.

Citation: Chernov VM. Number systems in modular rings and their applications to "error-free" computations. Computer Optics 2019; 43(5): 901-911. DOI: 10.18287/2412-6179-2019-43-5-901-911.

Acknowledgements: The work was partly funded by the Russian Federation Ministry of Science and Higher Education within a state contract with the “Crystallography and Photonics” Research Center of the RAS under agreement 007-ГЗ/Ч3363/26 in part of “number systems” and by Russian Foundation for Basic Research (Grants 19-07-00357 A and 18-29-03135_ мк) in part of “machine arithmetic”.

References

[1] Bergman G. A number system with an irrational base. Mathematics Magazine 1957; 31(2): 98-110.

[2] Rousseau C. The Phi number system revisited. Mathematics Magazine 1995; 48(4): 283-284.

[3] Stakhov AP. Goden ratio codes [In Russian]. Moscow: “Radio i Svyas” Publisher; 1984.

[4] Katai I, Szabo J. Canonical number systems for complex integers. Acta Sci Math 1975; 37: 255-260.

[5] Thuswaldner J. Elementary properties of canonical number systems in quadratic fields. In Book: Bergum GE, ed. Application of Fibonacci numbers. Vol 7. Dordrecht, Boston, London: Kluwer Acad Publ, 1996: 405-414.

[6] Ananda Mohan, P.V. Residue number systems, Basel: Birkhäuser; 2016. ISBN: 978-3-319-41383-9.

[7] Molahosseini AS, de Sousa LS, Chang C-H, eds. Embedded systems design with special arithmetic and number systems, Springer International Publishing AG; 2017. ISBN: 978-3-319-49741-9

[8] Chernov V. Fast algorithm for “error-free” convolution computation using Mersenne-Lucas codes. Chaos, Solitons and Fractals 2006; 29: 372-380.

[9] Chernov VM. Quasiparallel algorithm for error-free convolution computation using reduced Mersenne-Lucas codes. Computer Optics 2015; 39(2): 241-248. DOI: 10.18287/0134-2452-2015-39-2-241-248.

[10] Nussbaumer HJ. Fast Fourier transform and convolution algorithms. Berlin, Heidelberg: Springer-Verlag; 1981.

[11] Blahut RE. Fast algorithms for digital signal processing. Addison-Wesley Publishing Company Inc; 1985.

[12] Wimp J. Computations with recurrence relations. Boston, MA: Pitman; 1984.

[13] Masáková Z, Pelantová E, Vávra T. Arithmetics in number systems with a negative base. Theoretical Computer Science 2011; 412(8-10): 835-845.

[14] Schönhage A, Strassen V. Schnelle Multiplikation großer Zahlen. Computing 1971; 7: 281-292.

[15] Chernov VM. The implementation of number-theoretic transforms in the codes generated by the redundant number systems [In Russian]. Electronic Simulation 1992; 15(4): 33-37.

[16] 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(1): 91-100.

[17] Chernov VM, Pershina MV. Fibonacci-Mersenne and Fibonacci-Fermat discrete transforms. The Golden Section: Theory and applications. Boletim de Informatica 1999; 9/10: 25-31.

[18] Stakhov AP. The mathematics of harmony: From Euclid to contemporary mathematics and computer science. Singapore: World Scientific; 2009.

[19] Feinberg M. Fibonacci-Tribonacci. The Fibonacci Quarterly 1963; 1(30): 71-74.

Author’s information

Vladimir Mikhailovich Chernov (b. 1949). 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 Protection department at Samara National Research University (SSAU). Research interests are algebraic methods in digital signal processing, cryptography, computer arithmetic.

Received July 31, 2019. The final version – September 5, 2019.