ЧИСЛЕННЫЕ МЕТОДЫ И АНАЛИЗ ДАННЫХ

ВЫЧИСЛЕНИЕ ПРЕОБРАЗОВАНИЙ ФУРЬЕ–ГАЛУА В РЕДУЦИРОВАННЫХ БИНАРНЫХ СИСТЕМАХ СЧИСЛЕНИЯ

В.М. Чернов [1,2]

[1] *Институт систем обработки изображений РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН, Самара, Россия,*
[2] *Самарский национальный исследовательский университет имени академика С.П. Королева, Самара, Россия*

Аннотация

В работе предлагается новый метод вычисления преобразований Фурье–Галуа (теоретико-числовых преобразований), являющихся модулярным аналогом дискретного преобразования Фурье. Ряд специфических проблем, связанных с вычислением преобразований в конечном поле, удаётся решить с помощью представления элементов этих полей в «экзотических» системах счисления, являющихся редукциями канонических систем счисления И. Катаи при отображении соответствующего кольца целых квадратичного поля в поле классов вычетов по простому модулю. Подробно исследуется случай бинарных редуцированных систем счисления. Доказывается, что такие системы счисления существуют для любого простого числа.

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

Цитирование: **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.

Введение

Основной объект исследования работы – преобразования Фурье–Галуа (синонимы: теоретико-числовые преобразования, ТЧП) [1, 2], являющиеся модулярной версией дискретного преобразования Фурье в конечном поле ($\mathrm{mod}\, p$):

$$\hat{x}(m) = \sum_{n=0}^{N-1} x(n)\omega^{mn},$$
$$\omega^N \equiv 1(\mathrm{mod}\, p), \qquad (1)$$
$$x(n) \in \mathbf{Z},\ \mathrm{m} = 0,1,\ldots \mathrm{N}-1.$$

Считалось, что такие преобразования были введены в [3] в 1972, пока не было обнаружено, что такое преобразование было использовано Штрассеном и Шёнхаге в работе по умножению больших целых чисел [4] в 1966 году (заметим, что их приоритет иногда оспаривается также с упоминанием работ Фараджиева и Цыпкина 1965-1966 гг. См., например, [5]).

Преобразования (1) обладают рядом полезных свойств, главное из которых – отсутствие вычислительной погрешности, что, например, для задач, возникающих в криптографии, является принципиальным. Пик популярности исследований ТЧП приходился на 90-е годы, причём эти исследования не ограничивались только теоретическими. Наряду с ними проводились и аппаратные разработки [6].

Следует отметить, что, в отличие от традиционного «комплексного» дискретного преобразования Фурье (ДПФ), его модулярная версия (1) обладает рядом специфических недостатков, затрудняющих его вычисление:

- операции ($\mathrm{mod}\, p$) не являются «элементарными» компьютерными операциями;
- длина преобразования и простое число p связаны соотношением делимости $N|(p-1)$;
- зачастую делители числа $(p-1)$ таковы, что вычисление (1) исключает дополнительную алгоритмическую поддержку за счёт применения модулярных аналогов быстрых алгоритмов ДПФ.

В ряде случаев удаётся выбрать параметры преобразования (в частности, простое число p), при которых перечисленные выше вычислительные недостатки проявляются в минимальной степени.

Наиболее известны в этом контексте простые числа Ферма $p = 2^B + 1$, $B = 2^k$, простые числа Мерсенна $p = 2^k - 1$, по модулю которых в соответствующих конечных полях относительно просто реализуются арифметические операции при представлении элементов этих полей в бинарной арифметике со множеством цифр $\Lambda = \{0, 1\}$ [1, 2]. Менее известны простые числа Голомба [7] $p = 3\cdot 2^k + 1$ и Люка $p = 5\cdot 2^k + 1$, для которых также возможна не очень сложная реализация операций в бинарной системе счисления, и вообще для простых чисел $p = 2^n - 2^m + 1$ [5]. Естественно, что для этих чисел наиболее эффективная реализация в двоичной $\{0,1\}$-арифметике будет при $\omega \equiv 2(\mathrm{mod}\, p)$, когда умножения на степени ω сводятся к регистровым сдвигам.

Замечание. К сожалению, достаточно общие утверждения о мультипликативных порядках элементов $\omega \equiv 2(\mathrm{mod}\, p)$, то есть о возможных длинах преобразования (1), известны только в простейших случаях. В общем случае эта задача сводится к вычислительно сложной задаче дискретного логарифмирования.

Рассмотрение в преобразовании (1) вместо простых p составных модулей $\mathrm{mod}\, m$ добавляет к отмеченным трудностям необходимость учёта возможных делителей нуля фактор-кольца $\mathbf{Z}/m\mathbf{Z}$. Эта проблема решается, как правило, с помощью распараллеливания вычислений по модулям, равным делителям числа m.

В работах [8–10] идея распараллеливания реализуется также в сочетании с представлением элементов кольца $\mathbf{Z}/m\mathbf{Z}$ в подходящей системе счисления.

Необходимые теоретические сведения и обозначения

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

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

Как известно [13],

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

Согласно [14], элемент $\alpha \in \mathbf{Z}(\sqrt{d})$ *называется основанием канонической системы счисления* в $\mathbf{Z}(\sqrt{d})$, если любой элемент z этого кольца представим в виде

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

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

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

то система счисления называется *канонической системой счисления.* Исчерпывающее описание канонических систем счисления для мнимых квадратичных полей получено в [13].

В работе [14] было предложено обобщение понятия канонической системы счисления: допускался цифровой алфавит Λ, являющийся конечным подмножеством множества $\mathbf{Z}(\sqrt{d})$. Такие системы счисления, следуя [14], будем называть *квазиканоническими системами счисления.*

Как легко следует из ограничений классификационных теорем работы [13], бинарные канонические системы счисления существуют только в кольцах

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

В [14] показано, что в этих кольцах и только в них существуют и квазиканонические системы счисления. Определить цифры z_k разложения (2) можно с помощью рекуррентного процесса [15], [10], но для рассматриваемых колец $\mathbf{Z}(\sqrt{d})$ лучше воспользоваться алгоритмом деления по норме на элемент α [12]. Такой алгоритм реализуем лишь для пяти значений $d \leq 0$, а именно: $d = -1, -2, -3, -7, -11$, то есть и для рассматриваемых колец (4).

Пусть далее для данного простого p число d является квадратичным вычетом $(\mathrm{mod}\, p)$ [17], то есть существуют решения сравнения

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

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

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

так как элемент в правой части (6) принадлежит конечному полю $\mathbf{F}_p$, то есть φ – отображение $\mathbf{Z}(\sqrt{d}) \to \mathbf{F}_p$.

Отображение φ *редукция* $(\mathrm{mod}\, p)$, очевидным образом индуцирует преобразование представления (1) с новыми параметрами: цифрами $\varphi(z_k)$ и основанием $\varphi(\alpha) = g$. Такие представления будем называть представлениями в *редуцированных системах счисления.*

В настоящей работе рассматриваются только *бинарные* редуцированные системы счисления (то есть с двухэлементными цифровыми множествами Λ).

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

$$\xi = \xi_0 g^0 + \xi_1 g^1 + \xi_2 g^2 + ... \leftrightarrow \left(\xi_0, \xi_1, \xi_2, ... \right). \tag{7}$$

Операции над представлениями элементов (2) индуцируют соответствующие им правила преобразований кодов. Отметим, что при такой интерпретации цифры ξ_k при реализации операций играют не роль чисел, а являются исключительно «идентификаторами состояния соответствующего триггера».

Конечные поля, для которых существуют бинарные редуцированные системы 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 бинарные квазиканонические системы счисления.

Колец $\mathbf{Z}(\sqrt{d})$ с условием (b) немного: $\mathbf{Z}(i)$, $\mathbf{Z}(i\sqrt{2})$, $\mathbf{Z}(i\sqrt{7})$. Исследуем, при каких простых p каждое из перечисленных колец удовлетворяет условию (a).

Случай поля $\mathbf{Z}_p(i) \cong \mathbf{F}_p$. Как следует из работы [13] о канонических системах счисления в мнимых квадратичных полях и её обобщений [16] на «квазиканонические» системы счисления, в кольце целых элементов $\mathbf{Z}(i)$ существуют ровно 8 бинарных «квазиканонических» систем счисления, а именно системы счисления с основаниями $\alpha = \alpha^{\pm} = -1 \pm i$ и множествами Λ цифр

$$\{0, 1\}, \{0, i\}, \{0, -1\}, \{0, -i\}.$$

В табл. 1 указаны правила инверсии знака, переноса в старший разряд(ы) для четырех из восьми бинарных систем счисления.

*Табл. 1. Арифметические операции в квазиканонических системах счисления кольца целых квадратичных **Z**(i)*

Система счисления $\{\alpha, \Lambda\}$	Преобразование выражений, возникающих при реализации арифметических операций
$\alpha = -1 + i$, $\Lambda = \{0, i\}$	$i^2 = i\alpha + i$, $-i = i\alpha^4 + i\alpha^3 + i\alpha^2 + i$, $2i = i\alpha^3 + i\alpha^2$
$\alpha = -1 + i$, $\Lambda = \{0, -1\}$	$(-1)^2 = 1 =$ $= (-1)\alpha^4 + (-1)\alpha^3 + (-1)\alpha^2 + (-1)$, $-2 = (-1)\alpha^3 + (-1)\alpha^2$
$\alpha = -1 + i$, $\Lambda = \{0, -i\}$	$(-i)^2 = -1 =$ $= (-i)\alpha^2 + (-i)\alpha + (-i)$, $i = (-i)\alpha^4 + (-i)\alpha^3 +$ $+ (-i)\alpha^2 + (-i)$, $2i = (-i)\alpha^3 + (-i)\alpha^2$
$\alpha = -1 + i$, $\Lambda = \{0, 1\}$	$1^2 = 1$, $-1 = 1\cdot\alpha^4 + 1\cdot\alpha^3 + 1\cdot\alpha^2 + 1$, $2 = 1\cdot\alpha^3 + 1\cdot\alpha^2$

От редуцированного $(\mathrm{mod}\, p)$ кольца $\mathbf{Z}_p(i)$ потребуем, чтобы элемент (–1) являлся квадратичным вычетом $(\mathrm{mod}\, p)$. Хорошо известно (например, [17]), что это условие выполняется для всех простых чисел вида $p = 4k + 1$ (так называемых «пифагоровых простых»):

$$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, \ldots,$$

то есть членов последовательности A00144 по классификации [18].

В этом случае «редуцированная» $(\mathrm{mod}\, p)$ табл. 1 получается формальной заменой основания системы счисления и «цифр» на соответствующие элементы, а именно образы при каноническом отображении редукции $Z(i) \to Z_p(i)$ («приведение $(\mathrm{mod}\, p)$»).

Пример 1. Пусть $p = 13$, η – решение сравнения $\eta^2 \equiv -1 \equiv p - 1 (\mathrm{mod}\, p)$.

В рассматриваемом случае указанное сравнение имеет два решения $\eta_+ \equiv 5$, $\eta_- \equiv 8 (\mathrm{mod}\ 13)$.

Далее, при

$$\eta \equiv 5 (\mathrm{mod}\ 13), \quad \Lambda = \{0, i\} = \{0, 5\},$$
$$\alpha = -1 + i \equiv -1 + 5 = 4 (\mathrm{mod} 13).$$

соответствующие соотношения правого столбца табл. 1 примут вид:

$$\left.\begin{array}{c} 5^2 \equiv 5\cdot 4^1 + 5\cdot 4^0 \\ 8 \equiv 5\cdot 4^4 + 5\cdot 4^3 + 5\cdot 4^2 + 5\cdot 4^0 \\ 2\cdot 5 \equiv 5\cdot 4^3 + 5\cdot 4^2 \end{array}\right\} (\mathrm{mod} 13). \qquad (8)$$

Отметим, что в соотношениях (8) коэффициенты $5 \equiv i (\mathrm{mod}\ 13)$ при реализации операций играют не роль чисел, а являются исключительно идентификаторами состояния соответствующего триггера.

Так как возможная длина N преобразования (1) связана с $(\mathrm{mod}\, p)$ соотношением делимости $N | (p - 1)$, то для $p = 13$ возможные длины преобразований $N = 2, 3, 4, 6, 12$, причём элемент $\alpha \equiv 4$ имеет мультипликативный порядок, равный 12.

Заметим, что в отличие от классических систем счисления в кольце целых рациональных чисел **Z** один и тот же элемент кольца классов вычетов $(\mathrm{mod}\, p)$ может иметь несколько (бинарных) представлений в системе счисления с основанием α.

Пример 2. Пусть

$$p = 5, i \equiv 2 (\mathrm{mod}\, 5),$$
$$\alpha = -1 - i \equiv 2 (\mathrm{mod}\, 5), \Lambda = \{0, 1\}.$$

Свяжем с элементом кольца $\mathbf{S}_p(i)$ его код – вектор цифр:

$$x = x_0\alpha^0 + x_1\alpha^1 + x_2\alpha^2 + \ldots \leftrightarrow (x_0, x_1, x_2, \ldots).$$

Тогда при выбранных выше параметрах имеем:

$$0 \leftrightarrow (0,0,0) \leftrightarrow (1,0,1),$$
$$1 \leftrightarrow (1,0,0,) \leftrightarrow (0,1,1),$$
$$2 \leftrightarrow (0,1,0) \leftrightarrow (1,1,1),$$
$$3 \leftrightarrow (1,1,0),$$
$$4 \leftrightarrow (0,0,1).$$

Случай поля $\mathbf{Z}_p(i\sqrt{2}) \cong \mathbf{F}_p$. Как показано в работе [14], в кольце целых квадратичных чисел $\mathbf{Z}(i\sqrt{2})$ существуют ровно четыре бинарные квазиканонические системы счисления: системы счисления с основаниями $\alpha = \pm i\sqrt{2}$ и множествами цифр $\Lambda^+ = \{0,1\}$, $\Lambda^- \{0,-1\}$.

Так как требуется, чтобы в редуцированном $(\mathrm{mod}\, p)$ кольце элемент (–2) был квадратичным вычетом $(\mathrm{mod}\, p)$, то, вычисляя символ Лежандра [17],

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

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

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

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 энциклопедии [18].

Пример 3. Пусть $p = 11$, η – решение сравнения $\eta^2 \equiv -2 \equiv p - 2 (\mathrm{mod}\, p)$.

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

Далее, при

$$\eta \equiv 3 (\mathrm{mod} 11), \Lambda = \{0,1\},$$
$$\alpha = i\sqrt{2} \equiv 3 (\mathrm{mod} 11)$$

соответствующие соотношения правого столбца табл. 2 примут вид:

$$\left.\begin{array}{c} 10^2 \equiv 1 \\ -1 \equiv 10 \equiv 1\cdot\alpha^2 + 1 \\ 2 \equiv 1\cdot\alpha^4 + 1\cdot\alpha^2 \equiv 1\cdot 81 + 1\cdot 9 \end{array}\right\} (\mathrm{mod}\, 11). \qquad (9)$$

Табл. 2. Арифметические операции в квазиканонических системах счисления кольца целых квадратичных $\mathbf{Z}(i\sqrt{2})$

Система счисления $\{\alpha, \Lambda\}$	Преобразование выражений, возникающих при реализации арифметических операций
$\left\{i\sqrt{2}, \{0,1\}\right\}$	$1^2 = 1,$ $-1 = 1\cdot\alpha^2 + 1,$ $2 = 1\cdot\alpha^4 + 1\cdot\alpha^2$
$\left\{i\sqrt{2}, \{0,-1\}\right\}$	$(-1)^2 = 1,$ $1 = (-1)\cdot\alpha^2 + (-1),$ $2 = (-1)\cdot\alpha^2$

<u>*Случай поля*</u> $\mathbf{Z}_p(i\sqrt{7}) \cong \mathbf{F}_p$. Так как $(-7) \equiv 1 (\mathrm{mod}\, 4)$, то

$$\mathbf{Z}\left(i\sqrt{7}\right) = \left\{\frac{a + bi\sqrt{7}}{2};\, a, b \in \mathbf{Z};\, a \equiv b\,(\mathrm{mod}\, 2)\right\}.$$

Тем не менее, для определения множества простых, для которых существуют редуцированные бинарные системы счисления, удовлетворяющие требованию (а), определим простые, для которых число (–7) является квадратичным вычетом $(\mathrm{mod}\, p)$.

Вычисляя символ Лежандра с использованием квадратичного закона взаимности, имеем

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{p-1/2}\cdot\left(\frac{7}{p}\right) =$$
$$= (-1)^{p-1/2}\,(-1)^{(7-1/2)(p-1/2)}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right).$$

Нетрудно видеть, что квадратичными вычетами $(\mathrm{mod}\, 7)$ являются элементы $1,2,4 (\mathrm{mod}\, 7)$.

Таким образом, при $p \equiv 1,2,4 (\mathrm{mod}\, 7)$ справедливо соотношение $\mathbf{Z}_p(i\sqrt{7}) \cong \mathbf{F}_p$ и в поле $\mathbf{F}_p$ существуют бинарные системы счисления – редукции $(\mathrm{mod}\, p)$ квазиканонических систем счисления в $\mathbf{Z}(i\sqrt{7})$.

Табл. 3. Арифметические операции в квазиканонических системах счисления кольца целых квадратичных $\mathbf{Z}(i\sqrt{7})$

Система счисления $\{\alpha, \Lambda\}$	Преобразование выражений, возникающих при реализации арифметических операций
$\left\{\frac{-1 \pm i\sqrt{7}}{2}, \{0,1\}\right\}$	$1^2 = 1,$ $-1 = 1\cdot\alpha^2 + 1\cdot\alpha + 1$ $2 = 1\cdot\alpha^3 + 1\cdot\alpha$
$\left\{\frac{-1 \pm i\sqrt{7}}{2}, \{0,-1\}\right\}$	$2 = (-1)\alpha^3 + (-1)\alpha,$ $1 = (-1)\alpha^2 + (-1)\alpha + (-1)$

Пример 4. Пусть $p = 11$, η – решение сравнения $\eta^2 \equiv -7 \equiv p - 7 (\mathrm{mod}\, p)$.

В рассматриваемом случае указанное сравнение имеет два решения $\eta_+ \equiv 2$, $\eta_- \equiv 9 (\mathrm{mod}\, 11)$. Далее, при

$$\eta \equiv 2(\mathrm{mod}\, 11),\ \Lambda = \{0,1\},\ 2^{-1} \equiv 6(\mathrm{mod}\, 11),$$
$$\alpha = 2^{-1}\left(-1 - i\sqrt{7}\right) \equiv 7(\mathrm{mod}\, 11),$$

соответствующие соотношения правого столбца табл. 3 примут вид:

$$\left.\begin{array}{l} 2 = 1\cdot\alpha^3 + 1\cdot\alpha \equiv 1\cdot 6^3 + 1\cdot 6 \\ -1 = 1\cdot\alpha^2 + 1\cdot\alpha + 1 \equiv 1\cdot 6^2 + 1\cdot 6 + 1\cdot 6^0 \end{array}\right\} (\mathrm{mod}\, 11).$$

Таким образом, суммируя полученные результаты о полях $\mathbf{Z}_p(i\sqrt{d})$ при $d = 1, 2, 7,$ получаем основное утверждение работы.

Утверждение. Для любого простого p существует по крайней мере одна из бинарных редуцированных систем счисления в $\mathbf{Z}_p$.

Заключение

Отметим, что сфера приложения рассматриваемого подхода, по мнению автора, не ограничивается приложениями к вычислению теоретико-числовых преобразований для их последующего использования в алгоритмах умножения больших целых чисел, при решении криптографических задач и т.п.

Действительно, реальные вычисления при численном решении любой прикладной задачи производятся не над полями действительных или комплексных чисел, а над 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 множества можно считать целыми числами и, более того, вычетами по достаточно большому модулю [19].

Таким образом, рассмотренные «экзотические» системы счисления – бинарные редуцированные системы счисления в определенной мере представляют альтернативу традиционной «битовой» системе счисления.

Отметим также, что разработанная методика применима не только для построения бинарных редуцированных систем. Вопрос о целесообразности таких исследований с ориентацией на приложения зависит от характеристик существующих или перспективных вычислительных устройств.

По крайней мере, представляются интересными и реалистичными исследования тернарных редуцированных систем счисления, например, с «уравновешенным» цифровым алфавитом $\Lambda = \{-1, 0, 1\}$, или каких-либо иных с возможностью простых реализаций базовых арифметических операций.

Благодарности

Работа выполнена при поддержке РФФИ (проект №16-41-630676_р_а) и в рамках госзадания по теме № 0026-2018-0106.

Литература

1. **Нуссбаумер, Г**. Быстрое преобразование Фурье и алгоритмы вычисления свёрток / Г. Нуссбаумер; пер. с англ. – М.: Радио и связь, 1985. – 248 с.
2. **Блейхут, Р.** Быстрые алгоритмы цифровой обработки сигналов / Р. Блейхут; пер с англ. – М: Мир, 1989. – 448 с.
3. **Rader, C.M.** Discrete convolution via Mersenne transforms / C.M. Rader // IEEE Transactions on Computers. – 1972. – Vol. C-21, Issue 12. – P. 1269-1273. – DOI: 10.1109/T-C.1972.223497.
4. **Schönhage, A.** Schnelle Multiplikation großer Zahlen / A. Schönhage, V. Strassen // Computing. – 1966. – Vol. 7, Issue 3-4. – P. 281-292. – DOI: 10.1007/BF02242355.
5. **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.
6. **Alfredson, L.-I.** VLSI architectures and arithmetic operations with application to the Fermat number transform / L.-I. Alfredson. – Linköping, Sweden: Linköping University, 1996. – 296 p. – ISBN: 91-7871-694-2.
7. **Golomb, S.W.** Properties of the sequence $3 \cdot 2^n+1$ / S.W. Golomb // Mathematics of Computation. – 1976. – Vol. 30, Issue 135. – P. 657-663. – DOI: 10.1090/S0025-5718-1976-0404129-8.
8. **Chernov, V.M.** Fast algorithm for “error-free” convolution computation using Mersenne–Lucas codes / V.M. Chernov // Chaos, Solitons and Fractals. – 2006. – Vol. 29, Issue 2. – P. 372-380. – DOI: 10.1016/j.chaos.2005.08.081.
9. **Чернов, В.М.** Квазипараллельный алгоритм безошибочного вычисления свёртки в редуцированных кодах Мерсенна–Люка / В.М. Чернов // Компьютерная оптика. – 2015. – Т. 39, № 2. – С. 241-248. – DOI: 10.18287/0134-2452-2015-39-2-241-248.
10. **Чернов, В.М.** Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов. – М.: Физматлит, 2007. – 264 с. – ISBN: 5-9221-0940-6.
11. **Koblitz, N.** Algebraic aspects of cryptography / N. Koblitz. - Berlin, Heidelberg: Springer-Verlag, 1998. - 206 p. - ISBN: 978-3-540-63446-1.
12. **Боревич, З.И.** Теория чисел / З.И. Боревич, И.Р. Шафаревич. – 3-е изд. – М.: Наука, 1985. – 504 с.
13. **Kátai, I.** Canonical number systems in imaginary quadratic fields / I. Kátai, B. Kovács // Acta Mathematica Hungarica. – 1981. – Vol. 37, Issues 1-3. – P. 159-164. – DOI: 10.1007/BF01904880.
14. **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.
15. **Thuswardner, J.** Elementary properties of canonical number systems in quadratic fields / J. Thuswaldner. – In: Application of Fibonacci numbers / ed. by G.E. Bergum, A. N. Philippou, A.F. Horadam. – Dordrecht: Springer, 1998. – P. 405-414. – DOI: 10.1007/978-94-011-5020-0_45.
16. **Богданов, П.С.** О сходимости некоторых алгоритмов бинарной и тернарной машинной арифметики для вычислений в мнимых квадратичных полях / П.С. Богданов // Компьютерная оптика. – 2015. – Т. 39, № 2. – С. 249-254. – DOI: 10.18287/0134-2452-2015-39-2-249-254.
17. **Айерлэнд, К.** Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен; пер. с англ. – М.: Мир, 1987. – 415 с.
18. The on-line encyclopedia of Integer Sequences® (OEIS®) [Электронный ресурс]. – URL: https://oeis.org/ (дата обращения 10.04.2018 г.).
19. **Грегори, Р.** Безошибочные вычисления. Методы и приложения / Р. Грегори, Е. Кришнамурти; пер. с англ. – М.: Мир, 1988. – 207 с. – ISBN: 5-03-001145-5.

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. 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 18 апреля 2018 г. Окончательный вариант – 28 мая 2018 г.

CALCULATION OF FOURIER-GALOIS TRANSFORMS IN REDUCED BINARY NUMBER SYSTEMS

V.M. Chernov [1,2]

[1] *Image Processing Systems Institute of RAS – Branch of the FSRC “Crystallography and Photonics” RAS, Samara, Russia,*

[2] *Samara National Research University, Samara, Russia*

Abstract

The paper proposes a new method for calculating Fourier-Galois transforms (number-theoretical transforms), which are a modular analog of the discrete Fourier transform. A number of specific problems related to the calculation of transforms in a finite field can be solved by representing the elements of these fields in “exotic” number systems, which are reductions of the canonical number systems proposed by I. Katai when mapping the corresponding ring of an integer quadratic field into a field of the prime residue classes modulo. The case of binary reduced number systems is studied in detail. It is proved that such number systems exist for any prime number.

Keywords: Fourier-Galois transforms, finite fields, canonical and reduced number systems.

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

Acknowledgements: This work was supported by the Russian Foundation for Basic Research under grant No. 16-41-630676_p_a.

References

[1] Nussbaumer HJ. Fast Fourier transform and convolution algorithms. Berlin, Heidelberg: Springer-Verlag; 1982. ISBN: 978-3-540-11825-1.

[2] Blahut RE. Fast algorithms for digital signal processing. Boston, MA: Addison-Wesley Publishing Company, Inc.; 1985. ISBN: 978-0201101553.

[3] Rader C.M. Discrete convolution via Mersenne transforms. IEEE Trans Comp 1972; C-21(12): 1269-1273. DOI: 10.1109/T-C.1972.223497.

[4] Schönhage A, Strassen V. Schnelle Multiplikation großer Zahlen. Computing 1966; 7(3-4): 281-292. DOI: 10.1007/BF02242355.

[5] Varichenko LV, Labunetc VG, Rakov MA. Abstract algebraic systems and digital signal processing [In Russian]. Kiev, "Naukova dumka" Publisher; 1986.

[6] Alfredson L-I. VLSI architectures and arithmetic operations with application to the Fermat number transform. Linköping, Sweden: Linköping University, 1996. ISBN: 91-7871-694-2.

[7] Golomb SW. Properties of the sequence $3 \cdot 2^n+1$. Math Computing 1976; 30(135): 657-663. DOI: 10.1090/S0025-5718-1976-0404129-8.

[8] Chernov VM. Fast algorithm for "error-free" convolution computation using Mersenne–Lucas codes. Chaos, Solitons and Fractals 2006; 29(2): 372-380. DOI: 10.1016/j.chaos.2005.08.081.

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

[10] Chernov VM. Arithmetic methods of fast algorithm of discrete orthogonal transforms synthesis [In Russian]. Moscow: "Fizmathlit" Publisher; 2007. ISBN: 5-9221-0940-6.

[11] Koblitz N. Algebraic aspects of cryptography. Berlin, Heidelberg: Springer-Verlag; 1998. ISBN: 978-3-540-63446-1.

[12] Borevich ZI, Shafarevich IR. Number theory. New York, London: Academic Press Inc; 1966.

[13] Kátai I, Kovács B. Canonical number systems in imaginary quadratic fields. Acta Mathematica Hungarica 1981; 37(1-3): 159-164. DOI: 10.1007/BF01904880.

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

[15] Thuswardner J. Elementary properties of canonical number 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.

[16] Bogdanov PS. On convergence some algorithms of binary and ternary machine arithmetic for calculations in imaginary quadratic fields [In Russian]. Computer Optics 2015; 39(2): 249-254.

[17] Ireland K, Rosen M. A classical introduction to modern number theory. New York: Springer-Verlag; 1982.

[18] The on-line encyclopedia of Integer Sequences® (OEIS®). Source: ⟨https://oeis.org/⟩.

[19] Gregory RT, Krishnamurty EV. Methods and applications of error-free computation. New York: Springer; 1984. ISBN: 978-1-4612-9754-3.

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. Research interests are algebraic methods in digital signal processing, cryptography, computer arithmetic.

Received April 18, 2018. The final version – May 28, 2018.