Фибоначчи, трибоначчи, ..., гексаначчи и параллельная безошибочная машинная арифметика

В.М. Чернов [1,2]
[1] ИСОИ РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН,
443001, Россия, г. Самара, ул. Молодогвардейская, д. 151,
[2] Самарский национальный исследовательский университет имени академика С.П. Королёва,
443086, Россия, г. Самара, Московское шоссе, д. 34

Аннотация

В работе предлагается новый метод синтеза систем машинной арифметики для «безошибочных» параллельных вычислений. Отличием предлагаемого подхода от вычислений в традиционных системах остаточных классов в прямой сумме модулярных колец является параллелизация вычислений в конечных редукциях неквадратичных глобальных полей, элементы которых представлены в системах счисления порожденными последовательностями степеней корней характеристического полинома для последовательности *n*-Фибоначчи.

Ключевые слова: конечные поля, числа *n*-Фибоначчи и *n*-Люка, параллельная машинная арифметика.

Цитирование: **Чернов, В.М.** Фибоначчи, трибоначчи, ..., гексаначчи и параллельная безошибочная машинная арифметика / В.М. Чернов // Компьютерная оптика. – 2019. – Т. 43, № 6. – С. 1072-1078. – DOI: 10.18287/2412-6179-2019-43-6-1072-1078.

Введение

Теория конечных полей уже более полувека является математическим фундаментом, на котором основываются, наряду со ставшими уже традиционными приложениями в задачах криптографии или теории кодирования, также и методы решения не только структурных, но вычислительных задач информатики, в частности цифровой обработки сигналов.

Во многом это объясняется тем, что реальные вычисления при решении любой прикладной задачи производятся не с элементами полей действительных или комплексных чисел, а с элементами некоторого множества их рациональных аппроксимаций. Кроме того, априорная информация о предметном происхождении обрабатываемых данных, возможности используемых вычислительных средств выделяют во множестве рациональных чисел *конечное* подмножество – некую «рабочую, пользовательскую зону». После соответствующего масштабирования элементы этого конечного множества можно считать целыми числами и, более того, вычетами по некоторому достаточно большому модулю p.

Отметим также, что если в кольцах целых элементов некоторых полей вещественных или мнимых алгебраических чисел существуют «хорошие» позиционные системы счисления с просто реализуемой машинной арифметикой, то гомоморфные отображения (редукции) этих колец в конечные кольца классов вычетов индуцируют и редуцированные системы счисления также с «хорошими» правилами арифметических операций. Такие «экзотические» системы счисления (то есть *редуцированные* $(\mathrm{mod}\, p)$ системы счисления) в определённой мере представляют альтернативу традиционной «битовой» системе счисления [1].

Кроме того, постановка некоторых задач (например, в криптографии) *принципиально* не принимает 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, и во вполне безобидных задачах [2 – 3].

Арифметические операции $(\mathrm{mod}\, p)$ не являются для большинства вычислительных устройств элементарными компьютерными операциями. Но для некоторых простых p арифметика конечного поля $\mathbf{GF}(p)$ может быть более «дружественной компьютеру». Наиболее известными примерами таких простых чисел являются:

- простые числа Мерсенна $p = 2^q - 1$,
- простые числа Ферма $p = 2^{2^k} + 1$,
- простые числа Голомба $p = 3 \cdot 2^q + 1$

и т.д. [4, 5].

В этих и некоторых других случаях [4 – 6] при «естественном» для этих полей Мерсенна и Ферма представлении элементов полей в редуцированной двоичной системе счисления умножения сводятся к сложениям представляющих элементы бинарных кодов и к их (циклическим) регистровым сдвигам. Для упомянутых классов простых чисел разработаны как алгоритмические, так и аппаратные средства вычислений в соответствующих модулярных кольцах (полях) [4 – 7].

К сожалению, простых чисел Мерсенна, находящихся в «пользовательском диапазоне» специалиста-прикладника, очень мало (простых чисел Ферма ещё меньше). Использование в качестве модулей составных чисел добавляет к непосредственно вычислительным проблемам принципиальные теоретические трудности, связанные с существованием в модуляр-

ных кольцах по составным модулям делителей нуля и, как следствие, с возможной необратимостью элементов соответствующих колец.

При (паллиативном) распараллеливании вычислений в системе остаточных классов (СОК) [8, 9] характерные преимущества «битовой» реализации арифметических операций в кольцах, 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.

Отметим также, что синтез СОК представляет собой скорее чисто технологическую, а не теоретическую задачу, так как тезис

«если алгебраическая структура $\mathbf{A}$ *изоморфна прямой сумме структур той же категории* $\mathbf{A} \cong \mathbf{A}_1 \oplus \mathbf{A}_2 \oplus ... \mathbf{A}_r$, *то вычисления в структуре* $\mathbf{A}$ *можно распараллелить и заменить «покомпонентными» вычислениями в* $\mathbf{A}_1$, $\mathbf{A}_2$, ... $\mathbf{A}_r$*»*

является давно известным, хрестоматийным фактом, частные случаи систематического использования которого восходят едва ли не к методу координат Р. Декарта, несмотря на то, что в теории СОК этот факт используется в специфической версии «китайской теоремы об остатках».

1. Основные идеи

Основное отличие от вычислений в системах остаточных классов и суть предлагаемого в данной работе подхода состоит в следующем.

1) Рассматривается линейная рекуррентная функция $\Psi(k)$ со значениями в кольце целых элементов некоторого поля алгебраических чисел.

2) В некоторых случаях элементы рассматриваемого кольца могут быть представлены в «позиционной системе счисления с базисом $\{\Psi(k)\}$» (например, в так называемой системе счисления Цекендорфа [10 – 12] для последовательности Фибоначчи).

3) Значения $\Psi(k)$ являются линейными комбинациями показательных функций с основаниями, равными корням характеристического полинома для рекуррентности $\Psi(k)$, что позволяет говорить о представлении элементов рассматриваемого кольца линейной комбинацией элементов, представленных, в свою очередь, в системах счисления «традиционного» вида с экспоненциальными базисами.

4) Если реализация арифметических операций в терминах таких представлений (т.е. в системах счисления с основаниями базисов, порождённых корнями характеристического полинома рекуррентности $\Psi(k)$) относительно проста, то весьма вероятно, что столь же «хорошими» свойствами будут обладать и редуцированные системы счисления в фактор-кольцах исходного кольца.

Такая схема синтеза систем машинной арифметики для «безошибочных» (точнее, модулярных) вычислений предложена автором в [13] и в комбинации с традиционными подходами к синтезу СОК рассматривалась в [14 – 15].

2. Предварительные теоретические сведения и обозначения

Следуя [16 – 18], будем называть рекуррентную последовательность

$$\Psi\left(k+n\right) = \Psi(k+(n-1)) + ... + \Psi\left(k+1\right) + \Psi\left(k\right) \quad (1)$$

n-рекуррентностью Фибоначчи (*Fibonacci n-Step Number Sequence*).

Хорошо известно (например, [19 – 20]): если все корни α_j характеристического полинома

$$f_n(w) = w^n - w^{n-1} - w^{n-2} - ... - w^0 \quad (2)$$

различны, то общим решением уравнения (1) является функция

$$\Psi(k) = \sum_{j=o}^{n-1} C_j \alpha_j^k,$$

где константы C_j взаимно-однозначно определяются начальными значениями последовательности (1)

$$(\Psi(0), ..., \Psi(n-1)) \leftrightarrow (C_0, ..., C_{n-1}).$$

В частности:

- если $(\Psi(0), ..., \Psi(n-1)) = (1, ..., 1)$, то последовательность $\Psi(k)$ называется *n-последовательностью Фибоначчи;*
- если $(\Psi(0), ..., \Psi(n-1))$ таковы, что $(C_0, ..., C_{n-1}) = (1, ..., 1)$, то есть если

$$\Psi(k) = \sum_{j=o}^{n-1} \alpha_j^k, \quad (3)$$

то последовательность $\Psi(k)$ называется *n-последовательностью Люка.*

Табл. 1. n-последовательности Фибоначчи и Люка

n	Название рекуррентной последовательности	Номер n-последовательности Люка по On-Line Encyclopedia of Integer Sequences (OEIS, [21])
2	Fibonacci (Lucas)	A000032
3	tribonacci	A001644
4	tetranacci	A073817
5	pentanacci	A074048
6	hexanacci	A074584
7	heptanacci	A104621

Существенную роль в дальнейших рассуждениях будут играть обобщения теоремы Цекендорфа [10 – 12] для случаев n-последовательностей Фибоначчи и Люка.

Теорема Цекендорфа*. Всякое натуральное число можно единственным образом представить в виде суммы одного или нескольких различных чисел Фибоначчи так, чтобы в этом представлении не оказалось двух соседних чисел из последовательности Фибоначчи.* ■

В строгой формулировке:

Для любого натурального числа N существуют однозначно определённые натуральные числа

$$c_i \geq 2,\ c_{i+1} > c_i + 1,$$

такие, что

$$N = \sum_{i=0}^{s} F_{c_i},$$

где F_k – k-е число Фибоначчи.

Эта сумма называется *представлением Цекендорфа числа N*.

Для любого заданного натурального числа его цекендорфово находится при помощи *жадного алгоритма*, когда на каждом последующем этапе построения представления выбирается наибольшее возможное число Фибоначчи.

С использованием критерия Бруна [22] можно доказать, что множество чисел *n*-боначчи *полно*, то есть любое натуральное число *N* есть сумма чисел *n*-боначчи (или *n*-Люка) и, более того, оно имеет единственное «цекендорфоподобное» представление, когда сумма, представляющая число *N* не содержит *n* последовательных чисел *n*-боначчи. И, как и в прототипном случае 2-чисел Фибоначчи, это представление также можно найти с помощью жадного алгоритма.

Несмотря на усилия энтузиастов по разработке программных и аппаратных средств, реализующих арифметические вычисления для чисел, представленных в системе счисления Цекендорфа [23 – 25], эта система счисления даже в «базовом» случае чисел Фибоначчи обладает органическим недостатком. А именно: произведения чисел базиса Фибоначчи уже таковыми не являются в отличие от элементов базисов традиционных *g*-ичных систем счисления.

В данной работе предлагается метод распараллеливания вычислений, связанный с представлением/разложением не вычислительной *структуры в целом*, а с представлением/разложением *отдельных элементов* в конечном множестве систем счисления с возможностью эффективных и параллельных реализаций арифметических операций.

3. Синтез конечного поля – основной вычислительной структуры

Структура дальнейших рассуждений инвариантна относительно конкретного значения *n*, а формальные выкладки имеют вполне понятные отличия в зависимости от *n*. Потому, чтобы не загромождать работу «общими» обозначениями, заслоняющими основные совершенно прозрачные идеи, ограничимся рассмотрением принципиального случая $n = 3$, то есть случаем последовательности трибоначчи.

Пусть далее $\mathbf{K}_n(\mathbf{Q})$ есть расширение поля $\mathbf{Q}$, а именно, поле разложения характеристического полинома $f_n(w)$ степени *n* для рекуррентности (1) *n*-боначчи.

Пусть простое число *p* таково, что характеристический полином $f_n(w) = w^n - w^{n-1} - w^{n-2} - \ldots - w^0$ рекуррентного соотношения (1) неприводим над $\mathbf{GF}(p) = \mathbf{F}_p$. Рассмотрим фактор-кольцо кольца полиномов $\mathbf{F}_p[w]$ над $\mathbf{F}_p$ по главному идеалу, порождённому полиномом $f_n(w)$:

$$\mathbf{F}_p[w] \Big/ \left[f_n(w) \right] \cong \mathbf{GF}(q) = \mathbf{GF}(p^n).$$

Пример 1. Пусть $n = 3$ и полином

$$f_3(w) = w^3 - w^2 - w^1 - 1 \qquad (4)$$

неприводим (mod3).

Тогда

$$\mathbf{F}_p[w] \Big/ \left[f_n(w) \right] \cong \mathbf{GF}(3^3) =$$

$$= \left\{ a \cdot \omega^0 + b \cdot \omega^1 + c \cdot \omega^2 : a, b, c \in \mathbf{F}_3 ; \omega^3 = \omega^2 + \omega^1 + 1 \right\}.$$

По построению поля $\mathbf{GF}(3^3)$ как фактор-кольца, элемент ω равен одному из корней α полинома (4), два другие корня получаются действием автоморфизма Фробениуса $\theta : z \to z^3$ на элемент α:

$$\alpha = \theta^0(\alpha),\ \beta = \theta(\alpha) = \alpha^3,\ \gamma = (\theta \circ \theta)(\alpha) = \alpha^9.$$

Аналогично, при $n = 3$ полином (4) неприводим и по (mod5). Корни полинома $f_3(w)$ в соответствующем кубическом расширении $\mathbf{GF}(5^3)$ поля $\mathbf{GF}(5)$ имеют вид:

$$\alpha = \alpha^1,\ \beta = \alpha^5,\ \gamma = \beta^5 = \alpha^{25}.$$

Так как мультипликативная группа элементов конечного поля циклична, то в рассматриваемых случаях мультипликативные порядки корней α, β, γ совпадают и равны для $\mathbf{GF}(3^3)$

$$\mathrm{Ord}(\alpha) \left(\text{или } \mathrm{Ord}(\beta), \mathrm{Ord}(\gamma) \right) \in \{2, 13, 26\}$$

или для $\mathbf{GF}(5^3)$

$$\mathrm{Ord}(\alpha) \left(\text{или } \mathrm{Ord}(\beta), \mathrm{Ord}(\gamma) \right) \in \{2, 4, 31, 62, 124\}. \blacksquare$$

Далее, исходя из наличия априорной информации о диапазоне обрабатываемых целочисленных данных и характеристик используемых вычислительных средств (разрядность, степень распараллеливания и т.п.), выберем значения *n* порядка рекуррентности (1) и простого числа *p* с условием неприводимости характеристического полинома $f_n(w)$ в поле $\mathbf{GF}(p)$.

В соответствии с выбранными параметрами n, p рассмотрим расширение $\mathbf{GF}(q) = \mathbf{GF}(p^n)$ поля $\mathbf{GF}(p)$, которое далее будем рассматривать как основную структуру, в которой будем синтезировать алгоритмы параллельной системы вычислений.

4. Синтез системы параллельных вычислений в трибоначчи-кодах

Пусть $n = 3,\ a, b, c \in \mathbf{K}_3(\mathbf{Q}) = \mathbf{K}$ – корни полинома

$$f_3(w) = w^3 - w^2 - w^1 - 1;\ ;\ a, b, c \notin \mathbf{Q}; \qquad (5)$$

пусть $\Psi(k)$ – последовательность трибоначчи-Люка:

$$\Psi(k) = a^k + b^k + c^k. \qquad (6)$$

Тогда в силу (6), наряду с представлением целых неотрицательных чисел *z* в бинарной системе счисления Цекендорфа–Люка

$$z=\sum_{j=0}^{s(z)}\xi_j\Psi(j);\ \xi_j\in\{0,1\}, \tag{7}$$

имеет место и представление

$$z=\sum_{j=0}^{s(z)}\xi_j a^j+\sum_{j=0}^{s(z)}\xi_j b^j+\sum_{j=0}^{s(z)}\xi_j c^j;\ \xi_j\in\{0,1\}, \tag{8}$$

то есть представление числа z тремя суммами – суммами для слагаемых числа z, представленных в бинарных системах счисления «традиционного вида» с основаниями a, b, c.

Замечание 1. Использование в качестве начальных значений для $\Psi(k)$ значений, порождающих именно последовательность n-Люка, существенно для вычислений. В частности, последовательности цифр ξ_j во всех трёх суммах (8) одинаковые. ■

Пусть g – любой корень $f_3(w)$, тогда справедливы равенства

$$\begin{aligned}&g^3-g^2-g-1=0,\\&2=g^3-g^2-g+1,\\&-1=-g^3+g^2+g,\\&-2=-g^3+g^2+g-1.\end{aligned} \tag{9}$$

Равенства (9) позволяют эффективно и 3-параллельно производить сложения целых чисел z, представленных в форме (8), но уже в трёх *тернарных* системах счисления с цифровым множеством $\Lambda=\{-1,0,+1\}$.

Сложнее обстоит дело с параллельной реализацией умножения элементов, представленных в форме (8). Связано это с отсутствием в общем случае возможности простым образом связать основания трёх систем счисления в (8) между собой и эффективно учесть эту связь при реализации умножения элементов.

С учётом имеющейся априорной информации о решаемой прикладной вычислительной задаче выберем простое число p настолько большим, чтобы целочисленные обрабатываемые данные $z\notin\mathbf{Z}$ и результаты вычислений в $\mathbf{Z}\subset\mathbf{K}_3(\mathbf{Q})$ представлялись бы в системе счисления n-Цекендорфа в форме (7)

$$z=\sum_{k=0}^{d-1}\xi_k\Psi(k),\quad \xi_k\in\{0,1\},$$

где $\Psi(k)$ – последовательность чисел n-Люка (в рассматриваемом случае – чисел трибоначчи-Люка), чтобы для всех рассматриваемых данных в представлении выполнялось бы неравенство

$$p>\sum_{k=0}^{d-1}\Psi(k), \tag{10}$$

где, в свою очередь, число p определяется свойствами рассматриваемого ниже гомоморфизма.

Рассмотрим для простого числа p и $n=3$ гомоморфизм τ над $\mathbf{GF}(p)$

$$\tau:\mathbf{K}_3(\mathbf{Q})\to\mathbf{F}_p[w]\Big/\big[f_3(w)\big]\cong\mathbf{F}_q=\mathbf{GF}(p^3)$$

такой, что

$$\tau(a)=\alpha,\ \tau(b)=\beta,\ \tau(c)=\gamma,$$

где a,b,c – корни полинома $f_3(w)$ в поле $\mathbf{K}_3(\mathbf{Q})$; $\alpha,\beta,\gamma\notin\mathbf{GF}(p)$ – корни полинома f_3 в расширении $\mathbf{GF}(p^3)$.

Пусть d – порядок элемента $\alpha=\tau(a)$ в мультипликативной группе поля $\mathbf{GF}(p^3)$. Тогда в поле $\mathbf{GF}(p^3)$ имеет место редуцированное представление, аналогичное (8):

$$\tau(z)=\sum_{j=0}^{d-1}\xi_j\alpha^j+\sum_{j=0}^{d-1}\xi_j\beta^j+\sum_{j=0}^{d-1}\xi_j\gamma^j=z_\alpha+z_\beta+z_\gamma. \tag{11}$$

Кроме того, для $\omega\in\{\alpha,\beta,\gamma\}$ в поле $\mathbf{GF}(p^3)$, наряду с редукциями равенств (9):

$$\begin{aligned}&\omega^3-\omega^2-\omega-1=0,\\&2=\omega^3-\omega^2-\omega+1,\\&-2=-\omega^3+\omega^2+\omega-1,\end{aligned} \tag{12}$$

справедливы и равенства

$$\omega^d=1,\ \omega=\alpha,\beta=\alpha^p,\gamma=\beta^p=\alpha^{p^2}. \tag{13}$$

Как и обычно, в случае замены (аппроксимации) целочисленных вычислений редуцированными модулярными при «достаточно большом $(\mathrm{mod}\,p)$» такая аппроксимация приводит к точному результату. А именно: если целочисленные данные x, обрабатываемые некоторой вычислительной процедурой $x\to\Im x=y$ и априорно ожидаемые результаты y таковы, что $0\le x$, $y<p$, то переход от арифметических действий в целочисленной арифметике к модулярной приводит к точным результатам [2]. Поэтому переход от арифметических действий с суммами (8) к арифметическим операциям с их гомоморфными τ-образами (11) при «достаточно больших p,d», границы для которых несложно определить в каждом конкретном случае, не порождает «вычислительных погрешностей».

Замечание 2. При умножении элементов поля $\mathbf{GF}(p^3)$ в форме (11)

$$\begin{aligned}&\tau(z)\cdot\tau(y)=(z_\alpha+z_\beta+z_\gamma)\cdot(y_\alpha+y_\beta+y_\gamma)=\\&=z_\alpha y_\alpha+z_\alpha y_\beta+z_\alpha y_\gamma+z_\beta y_\alpha+z_\beta y_\beta+z_\beta y_\gamma+\\&+z_\gamma y_\alpha+z_\gamma y_\beta+z_\gamma y_\gamma\end{aligned}$$

в реальности требуется не девять, а только три умножения, так как:

$$\begin{aligned}&\tau(z)\cdot\tau(y)=(z_\alpha y_\alpha+z_\alpha y_\beta+z_\alpha y_\gamma)+\\&+\theta(z_\alpha y_\alpha+z_\alpha y_\beta+z_\alpha y_\gamma)+\theta\circ\theta(z_\alpha y_\alpha+z_\alpha y_\beta+z_\alpha y_\gamma),\end{aligned}$$

где θ – автоморфизм Фробениуса поля $\mathbf{GF}(p^3)$. ■

Замечание 3. Нетрудно также заметить, что

$$\sum_{j=0}^{d-1}\xi_j\beta^j=\sum_{j=0}^{d-1}\xi_{\sigma(j)}\alpha^j,$$

где перестановка индексов $\sigma:j\to pj\,(\mathrm{mod}\,d)$ индуцируется автоморфизмом Фробениуса $\theta:z\to z^p$. ■

Заключение

В работе рассматривается один из прикладных аспектов теории систем счисления в алгебраических структурах, а именно: методы синтеза систем счисления в конечных алгебраических расширениях поля рациональных чисел **Q**. Если системы счисления в поле **Q** являются классическим и хорошо изученным объектом как с теоретической стороны, так и с точки зрения эффективности их применения в вычислительных задачах, то системы счисления в полях алгебраических чисел исследованы в значительно меньшей степени. Некоторым исключением являются квадратичные поля благодаря глубоким работам венгерских математиков (I. Katai, B. Kovacs и др.), подробно описавших класс т.н. «канонических систем счисления для квадратичных полей». Следует отметить, правда, что многочисленные работы последних десятилетий почти не касаются прикладных аспектов теории. Системы счисления в неквадратичных расширениях (за редкими исключениями) вообще почти не исследовались, не говоря уж о задаче построения систем счислений с «дружественными» компьютерам свойствами.

Настоящая работа представляет собой попытку синтеза систем счисления для неквадратичных полей алгебраических чисел.

Связь предложенного метода именно с числами n-боначчи не является необходимой. Вполне достаточно существование для выбранного рекуррентного соотношения (избыточной) системы счисления «типа Цекендорфа», которая гарантировала бы позиционное представление в ней целых элементов рассматриваемого поля с цифровым алфавитом небольшой мощности и с «машинно-комфортными алгоритмами», реализующими арифметические операции. В частности, в работе [15] рассматривается случай $n=2$ для систем счисления, порожденных «нефибоначчиевыми» рекуррентностями второго порядка.

Автор неоднократно пояснял свою позицию в отношении «фибоначчиведения» в целом. Действительно, несмотря на давнее и эффективное использование чисел Фибоначчи, «золотого сечения» и т.п. в прикладных задачах (сортировка данных, построение квадратурных формул для численного интегрирования, моделирования «хаотических» и фрактальных процессов или объектов и т.д.), значительная масса публикаций связана фактически с нумерологией, к «научному жанру» не относящейся. Несмотря на то, что и автор настоящей работы использовал числа Фибоначчи, Люка и т.п. для решения локальных задач обработки сигналов (см., напр., монографию [26]), он не разделяет энтузиазма в поисках «Всеобщей Гармонии» и/или построения «Общей Теории Всего» на основе анализа тех или иных числовых феноменов.

Несмотря на некоторую одиозность подобных исследований и категоричность выводов некоторых авторов, вполне серьёзные профессиональные исследования в тематике, связанной, в частности, с теорией и приложениями последовательности чисел Фибоначчи, проводятся под эгидой *Fibonacci Association.* Регулярно проводятся конференции, издаются книги и журнал *Fibonacci Quarterly.* К сожалению, большинство из этих изданий малодоступны российскому читателю.

Приоритет в области применения теории чисел Фибоначчи к задачам информатики в СССР принадлежит А.П. Стахову (например, [23–25] и др.), рассматривавшему на раннем этапе своих исследований представления данных в системе счисления Фибоначчи (Цекендорфа) исключительно как средство построения отказоустойчивых машинных кодов. Разумеется, вопрос о *целесообразности* широкого использования «процессоров Фибоначчи» остаётся открытым с неоднозначным к нему отношением, хотя, скорее всего, в настоящее время создание таких процессоров не представляет принципиальной *технологической* трудности.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования 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. **Vasundara, P.** Multi-valued logic addition and multiplication in Galois field / P. Vasundara, K.S. Gurumurthy // Proceedings of the 2009 IEEE International Conference on Advances in Computing, Control and Telecommunication Technologies. – 2009. – P. 752-755. – DOI: 10.1109/ACT.2009.190.
2. **Грегори, Р.** Безошибочные вычисления. Методы и приложения / Р. Грегори, Е. Кришнамурти; пер. с англ. – М.: Мир, 1988. – 207 с.
3. **Дэвенпорт, Дж.** Компьютерная алгебра / Дж. Дэвенпорт, И. Сирэ, Э. Турнье; пер. с англ. – М.: Мир, 1991. – 352 с.
4. **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.
5. **Нуссбаумер, Г.** Быстрое преобразование Фурье и алгоритмы вычисления свёрток / Г.Нуссбаумер; пер. с англ. – М.: Радио и связь, 1985. – 248 с.
6. **Golomb, S.W.** Protierties of the sequence $3\cdot 2^n+1$ / S.W.Golomb // Mathematics and computing. – 1976. – Vol. 30, Issue 135. – P. 657-663.
7. **Alfredson, L.-I.** VLSI architectures and arithmetic operations with application to the Fermat number transform / L.-I. Alfredson. – Linköping: 1996.
8. **Ananda Mohan, P.V.** Residue number systems / P.V. Ananda Mohan. – Switzerland: Springer International Publishing, 2016. – 351 p. – ISBN: 978-3-319-41385-3.
9. **Molahosseini, A.S.** Embedded systems design with special arithmetic and number systems / A.S. Molahosseini, L.S. de Sousa, C.-H. Chang. – Springer-Verlag; 2017. – 389 p. – ISBN: 978-3-319-49742-6.
10. **Zeckendorf, E.** Representation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de

Lucas / E. Zeckendorf // Bulletin de la Societe Royale des Sciences de Liege. – 1972. – Vol. 41. – P. 179-182.
11. **Freitag, H.T.** Elements of Zeckendorf arithmetic / H.T. Freitag, G.M. Phillips. – In: Applications of Fibonacci Numbers / ed. by G.E. Bergum, A.N. Philippou, A.F. Horadam. – Dordrecht: Springer Science+Business Media, 1998. – P. 129-132.
12. **Fraenkel, A.S.** Systems of numeration / A.S. Fraenkel // The American Mathematical Monthly. – 1985. – Vol. 92, Issue 2. – P. 105-114.
13. **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.
14. **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.
15. **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.
16. **Feinberg, M.** Fibonacci-Tribonacci / M. Feinberg // The Fibonacci Quarterly. – 1963. – Vol. 1, Issue 30. – P. 71-74.
17. **Flores, I.** Direct calculation of *k*-generalized Fibonacci numbers, Fibonacci Quarterly. – 1976. – Vol. 5. – P. 259-266.
18. **Noe, T.D.** Primes in Fibonacci *n*-step and Lucas *n*-step sequences / T.D. Noe, J.V. Post // Journal of Integer Sequences. – 2005. – Vol. 8. – 05.4.4.
19. **Гельфонд, А.О.** Исчисление конечных разностей. / А.О. Гельфонд. – 4-е изд. – М.: URSS, 2006.
20. **Wimp, J.** Computations with recurrence relations / J. Wimp. – Boston, MA: Pitman, 1984.
21. The on-line encyclopedia of integer sequences® (OEIS®) [Electronical Resource]. – URL: https://oeis.org/ (request date 10.10.2019).
22. **Brown, J.L.** Note on complete sequences of integers / J.L. Brown // The American Mathematical Monthly. – 1961. – Vol. 68, Issue 6. – P. 557-560. – DOI: 10.2307/2311150.
23. **Стахов, А.П.** Алгоритмическая теория измерения / А.П. Стахов. – М.: Знание, серия Математика и кибернетика, 1979. – Вып. 6.
24. **Стахов, А.П.** Коды золотой пропорции / А.П. Стахов // М.: Радио и связь, 1984. – 152 с.
25. **Stakhov, A.P.** The mathematics of harmony. From Euclid to contemporary mathematics and computer science / A.P. Stakhov. – World Scientific, 2009.
26. **Чернов, В.М.** Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов. – М.: Физматлит, 2007. – 264 с – ISBN: 5-9221-0940-6.

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 .
Поступила в редакцию 25 сентября 2019 г. Окончательный вариант – 14 октября 2019 г.

Fibonacci, tribonacci,…,hexanacci and parallel “error-free” machine arithmetic

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, 34, Moskovskoye shosse, 443086, Samara, Russia

Abstract

The paper proposes a new method of synthesis of machine arithmetic systems for “error-free” parallel computations. The difference of the proposed approach from calculations in traditional Residue Number Systems (RNS) for the direct sum of rings is the parallelization of calculations in finite reductions of non-quadratic global fields whose elements are represented in number systems generated by sequences of powers of roots of the characteristic polynomial for the *n*-Fibonacci sequence.

Keywords: finite fields, *n*-Fibonacci and *n*-Lucas numbers, parallel machine arithmetic.
Citation: Chernov VM. Fibonacci,tribonacci, ..., hexanacci and parallel "error-free" machine arithmetic. Computer Optics 2019; 43(6): 1072-1078. DOI: 10.18287/2412-6179-2019-43-6-1072-1078.
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 (“Number systems”) and by Russian Foundation for Basic Research under grants 19-07-00357 A and 18-29-03135_ мк (“Machine arithmetic”).

References

[1] Vasundara P. Multi-valued logic addition and multiplication in Galois field. Proc IEEE Int Conf Adv Comput Control Telecomm Technol 2009: 752-755. DOI: 10.1109/ACT.2009.190.

[2] Gregory RT, Krishnamurty EV. Method and applications of error-free computation. New York: Springer-Verlag; 1984.

[3] Davenport JH, Siret Y, Tournier E. Computer algebra: Systems and algorithms for algebraic computation. Academic Press; 1988.

[4] Varichenko LV, Labunets VG, Rakov MA. Abstract algebraic systems and digital signal processing [In Russian]. Kyiv, "Naukova Dumka" Publisher; 1986.

[5] Nussbaumer HJ. Fast Fourier transform and convolution algorithms. – Berlin, Heidelberg: Springer Verlag; 1982.

[6] Golomb SW. Protierties of the sequence $3 \cdot 2^n+1$. Math Computing 1976; 30(135): 657-663.

[7] Alfredson L-I. VLSI architectures and arithmetic operations with application to the Fermat number transform. Linköping: 1996.

[8] Ananda Mohan PV. Residue number systems. Switzerland: Springer International Publishing; 2016. ISBN: 978-3-319-41385-3.

[9] Molahosseini AS, de Sousa LS, Chang C-H, eds. Embedded systems design with special arithmetic and number systems. Springer-Verlag; 2017. ISBN: 978-3-319-49742-6.

[10] Zeckendorf E. Representation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas. Bull Soc Roy Sci Liege 1972; 41: 179-182.

[11] Freitag HT, Phillips GM. Elements of Zeckendorf arithmetic. In Book: Bergum GE, Philippou AN, Horadam AF, eds. Applications of Fibonacci numbers. Dordrecht: Springer Science+Business Media; 1998: 129-132.

[12] Fraenkel AS. Systems of numeration. Amer Math Monthly 1985; 92: 105-114.

[13] 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.

[14] 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.

[15] Chernov VM. Number systems in modular rings and their applications to "error-free" computations. Computer Optics 2019; 42(5): 901-911. DOI: 10.18287/2412-6179-2019-43-5-901-911.

[16] Feinberg M. Fibonacci-Tribonacci. Fibonacci Quart 1963; 1(30): 71-74.

[17] Flores I. Direct calculation of *k*-generalized Fibonacci numbers, Fibonacci Quart 1967; 5: 259-266.

[18] Noe TD, Post JV. Primes in Fibonacci *n*-step and Lucas *n*-step sequences. J Integer Seq 2005; 8: 05.4.4.

[19] Gel'fond AO. Calculus of finite differences [In Russian]. 4-th ed. Moscow: "URSS" Publisher; 2006.

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

[21] The on-line encyclopedia of integer sequences® (OEIS®). Source: ⟨https://oeis.org/⟩.

[22] Brown JL. Note on complete sequences of integers. Amer Math Monthly 1961; 68(6): 557-560. DOI: 10.2307/2311150.

[23] Stakhov AP. Algorithmic measurement theory [In Russian]. Moscow: "Znanie" Publisher; 1979.

[24] Stakhov AP. Goden ratio codes [In Russian]. Moscow: "Radio i svyas" Publisher; 1984.

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

[26] Chernov VM. Arithmetic methods for fast algorithms of discrete orthogonal transforms synthesis [In Russian]. Moscow: "Fizmatlit" Publisher; 2007. ISBN: 5-9221-0940-6.

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 September 25, 2019. The final version – October 14, 2019.