Вестник Сыктывкарского университета.
Серия 1: Математика. Механика. Информатика. 2022.
Выпуск 2 (43)
Bulletin of Syktyvkar University.
Series 1: Mathematics. Mechanics. Informatics. 2022; 2 (43)

ПРИКЛАДНАЯ МАТЕМАТИКА И МЕХАНИКА

Научная статья

УДК 512.622
https://doi.org/10.34130/1992-2752_2022_2_4

ГЕОМЕТРИЧЕСКИЕ И АНАЛИТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПОСТРОЕНИЯ МНОГОЧЛЕНА ДЕЛЕНИЯ КРУГА

Татьяна Михайловна Банникова, Ольга Михайловна Немцова
Удмуртский государственный университет

Аннотация. Обсуждается проблема нахождения многочленов деления круга с условием задания некоторых их коэффициентов. Задача существования многочленов такого вида является решенной, но проблема неоднозначности нахождения многочленов деления круга с заданным простым или составным коэффициентом, а также особенности его номера (такие, как разложение на простые множители и значительный порядок по отношению к заданному коэффициенту), может быть использована в задании открытого ключа в криптографических системах. Так, известно использование корней многочленов деления круга в качестве генератора циклической группы в алгоритме Берлекэмпа – Месси. Теоретические основы имеющихся исследований и вычислительные инструменты предлагают различные способы нахождения многочленов деления круга, но не гарантируют практического пути реализации проблемы нахождения многочленов с заведомо заданным коэффициентом. Нахождение таких многочленов на практике является задачей, требующей больших временных и ресурсных затрат. Как и в задаче факторизации, задача нахождения кругового многочлена по заданным коэффициентам представляется задачей понятной, но вычислительно сложной, что дает несомненное преимущество при использовании ее в крипто-

графических системах. Свойства многочлена деления круга, такие как неприводимость, симметричность, изменение свойств при рассмотрении в полях различных характеристик, также интересны для использования в шифровании.

Работа выполнена в рамках государственного задания Министерства науки и высшего образования РФ 121030100003-7.

Ключевые слова: многочлены деления круга, криптографическая система, генерация ключей, шифротекст

Для цитирования: Банникова Т. М., Немцова О. М. Геометрические и аналитические характеристики построения многочлена деления круга // *Вестник Сыктывкарского университета. Сер. 1: Математика. Механика. Информатика.* 2022. Вып. 2 (43). С. 4–20. https://doi.org/10.34130/1992-2752_2022_2_4

Applied mathematics and mechanics

Original article

Geometrical and analytical characteristics of the constructing the polynomial of a circle division

Tatyana M. Bannikova, Olga M. Nemtsova
Udmurt State University

Abstract. The problem of finding circle division polynomials with the condition of specifying some of their coefficients is discussed. The problem of the existence of polynomials of this type is solved, but the problem of the ambiguity of finding circle division polynomials with a given simple or composite coefficient, as well as features of its number (such as decomposition into prime factors and a significant order with respect to a given coefficient) can be used in setting an open key in cryptographic systems. So it is known to use the roots of circle division polynomials as a cyclic group generator in the Berlekamp-Massey algorithm. The theoretical foundations of the available research and computational tools offer various ways to find circle division polynomials, but do not guarantee a practical way to implement the problem of finding polynomials with a known coefficient. Finding such polynomials in practice is a task that requires a lot of time and resources. As in the factorization problem, the problem of finding a circular polynomial for given coefficients seems

to be an understandable task, but computationally difficult, which gives an undoubted advantage when used in cryptographic systems. The properties of the circle division polynomial, such as irreducibility, symmetry, change in properties when considered in fields of various characteristics, are also interesting for use in encryption.

The work was carried out within the framework of the state task of the Ministry of Science and Higher Education of the Russian Federation 121030100003-7.

Keywords: circle division polynomials, cryptosystem, key's generation, ciphertext.

For citation: Bannikova T. M., Nemtsova O. M. Geometrical and analytical characteristics of the constructing the polynomial of a circle division. *Vestnik Syktyvkarskogo universiteta. Seriya 1: Matematika. Mekhanika. Informatika=Bulletin of Syktyvkar University, Series 1: Mathematics. Mechanics. Informatics*, 2022, No. 2 (43), pp. 4–20. https://doi.org/10.34130/1992-2752_2022_2_4

Введение

Известные методы, алгоритмы и протоколы защиты информации охватывают ряд функций, обладающих свойствами, позволяющими использовать их для формирования ключей в криптографических системах. Главной особенностью использования таких функций является возможность «простого» шифрования и «сложности» обратной задачи, такой, например, как дискретное логарифмирование [1]. Многочлены деления круга имеют геометрические и аналитические характеристики, которыми обладают некоторые многочлены, уже широко используемые в шифровании данных и генерации ключей, такие как неприводимость, нахождение корней вблизи нуля и др. Классы таких функций увеличиваются, появляются видоизменения их приложений. Продолжается расширение классов функций для генерации шифротекста, преобразуется метод нескольких многочленов. Строятся схемы шифрования на основе многочленов Чебышева [2]. На основе неприводимых многочленов в полях простой характеристики строятся матрицы для применения их при построении обобщенных генераторов псевдослучайных последовательностей p-ичных чисел [3]. Продолжаются исследования в области применения примитивных многочленов в кодовом уплотнении данных [4]. Используются коэффициенты многочленов третьего и пятого порядков

для кодирования информации кодами Рида – Соломона [5; 6]. Рассматриваются циклотомические многочлены в гиперэллиптическом поле [7]. Строится криптосистема, основанная на кубическом поле, связанном с кубическим уравнением Пелла и рациональными функциями Редея [8]. С помощью эллиптических кривых происходит обучение нейронных сетей [9].

В настоящее время известны свойства круговых многочленов, позволяющие говорить об их структуре, геометрических и аналитических характеристиках [10; 11]. Одним из наиболее интересных приложений круговых многочленов до сих пор было доказательство теоремы Веддерберна о коммутативности конечного тела [10]. В последних исследованиях многочлены деления круга использовались для определения сложности различения двоичных слов [12], исследовались группы Галуа для классов многочленов с использованием корней многочлена деления круга [13]. Было доказано свойство характеристического многочлена для изучения строения комплексной гиперповерхности [14]. Применяются многочлены деления круга при определении элементов обобщенных двумерных и трехмерных регулярных решеток [15], как корни многочленов деления круга в качестве генератора циклической группы в алгоритме Берлекэмпа – Месси. Из-за множества приложений, таких как быстрое преобразование Фурье, теория кодирования и криптография для эффективного выполнения вычислений в конечных полях и т. д., широко обсуждаются примитивные нормальные элементы и примитивные нормальные многочлены над конечными полями [16–18].

Рассматривается неприводимость многочленов в факторизации многочленов над конечными полями, которая играет важную роль в самых разных технологических ситуациях, включая криптографию, цифровую систему отслеживания, в кодах с исправлением ошибок. При этом используются и многочлены деления круга [19–25].

Математическое обоснование

У многочлена $z^n - 1$ есть n различных комплексных корней, числа вида $\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ для $k = 0, 1, \ldots, n-1$, которые называются *корнями из единицы n-й степени*. Соответствующие точки на комплексной плоскости располагаются на единичной окружности с центром в нуле и образуют правильный n-угольник. ζ — корень из единицы n-й степени

называется *примитивным*, если $\zeta^m \neq 1$ для все натуральных m меньше n.

Многочлен деления круга — это

$$\Phi_n(x) = (x - \zeta_1)(x - \zeta_2)(x - \zeta_3)\dots(x - \zeta_{\phi(n)}),$$

где $\zeta_1, \zeta_2, \dots, \zeta_{\phi(n)}$ — все примитивные корни n-й степени из 1.

Пусть $\mathbb{Q}$ – поле рациональных чисел, т. е. простое поле характеристики нуль. Рассмотрим уравнение деления круга

$$\Phi_n(x) = 0.$$

Корни n-й степени из единицы в поле комплексных чисел делят единичную окружность на n равных дуг. Пусть p — простое число, на которое не делится число n. Тогда вместе с примитивным ζ также и ζ^p является примитивным корнем n-й степени из единицы, и этот элемент удовлетворяет некоторому целочисленному неразложимому уравнению $g(\zeta^p) = 0$, левая часть которого имеет содержание 1. Полагая $f(x) = x^{n-1}$, получаем, что многчлен $f(x)$ раскладывается на n различных линейных множителей. Далее, многочлен $g(x^p)$ имеет ζ своим корнем, а потому должен делить $f(x)$. Тогда

$$g(x^p) \equiv g(x)^p \mod p.$$

Все корни многочлена $\Phi_n(x)$ удовлетворяют уравнению $f(x) = 0$, и $\Phi_n(x)$ не имеет кратных корней. Более того, в простом поле характеристики ноль многочлен $\Phi_n(x)$ неразложим, а значит, все его корни сопряженные.

Если теперь K — поле характеристики p, то положим $n = p^m h$, где h не делится на p. Для каждого корня n-й степени из единицы имеет место равенство

$$(\zeta^h - 1)^{p^m} = \zeta^{hp^m} - 1 = \zeta^n - 1 = 0.$$

Следовательно, $\zeta^h - 1 = 0$.

Таким образом, корни n-й степени из единицы являются одновременно корнями h-й степени из единицы, где h не делится на характеристику поля. В случае характеристики ноль можно положить $h = n$. В обоих случаях $\zeta^h = 1$, где h не делится на характеристику поля.

Соотношение

$$\prod_{d|n} \Phi_{d(x)} = x^n - 1 \tag{1}$$

в кольце целочисленных многочленов позволяет заключить, что каждый многочлен деления круга является целочисленным многочленом и не зависит от характеристики поля.

С помощью функции Мёбиуса и (1) получается выражение для $\Phi_n(x)$ через $x^d - 1$, где d пробегает делители n:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}. \tag{2}$$

Выражение (2) также позволяет утверждать, что коэффициенты многочлена Φ_n являются целыми числами. Следующее свойство используется для нахождения многочленов с целыми коэффициентами, отличными от ± 1. Пусть $n > 1$ – нечетное число. Тогда

$$\Phi_{2n}(x) = \Phi_n(-x). \tag{3}$$

Действительно, если $\zeta_1, \zeta_2, \ldots, \zeta_{\phi(n)}$ — первообразные корни степени n, то $-\zeta_1, \ldots, -\zeta_{\phi(n)}$ — первообразные корни степени $2n$. Таким образом, из (3) вытекает

$$\Phi_n(-x) = (-x - \zeta_1)(-x - \zeta_2) \ldots (-x - \zeta_{\phi(n)}), \tag{4}$$

$$\Phi_{2n}(x) = (x + \zeta_1)(x + \zeta_2) \ldots (x + \zeta_{\phi(n)}). \tag{5}$$

Из того, что степень многочлена Φ_n четна, получается, что выражения (4) и (5) равны между собой, т. е. верно необходимое равенство.

В зависимости от номера n вид и коэффициенты многочлена меняются. Так для простого $n = p$ и натурального k получается:

$$\Phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1, \tag{6}$$

$$\Phi_{p^{k+1}} = x^{(p-1)p^k} + x^{(p-2)p^k} + \cdots + x^{p^k} + 1. \tag{7}$$

Для различных нечетных простых p и q имеет место выражение

$$\Phi_{pq} = \frac{x^{p(q-1)} + x^{p(q-2)} + \cdots + x + 1}{x^{q-1} + x^{q-2} + \cdots + x + 1}. \tag{8}$$

Таким образом, из (6), (7), (8) все многочлены деления круга с номерами вида p, p^{k+1}, pq имеют коэффициенты 0 или ± 1.

Далее рассмотрим положительное нечетное число t, т. е. $t \geq 3$, найдем t простых чисел $p_1 < p_2 < \cdots < p_t$, для которых выполняется неравенство $p_1 + p_2 > p_t$ (такие p_t всегда найдутся).

Пусть $n = p_1 \cdot p_2 \cdot \cdots \cdot p_t$ и рассмотрим многочлен $\Phi_n(x)$ по модулю x^{p_t+1}. Так как t — нечетное, то

$$\Phi_{p_1 \dots p_t} = \frac{(x^{p_1} - 1) \dots (x^{p_t} - 1)}{x - 1} \cdot \frac{\prod (x^{p_i p_j p_k} - 1)}{\prod (x^{p_i p_j} - 1)} \cdot \dots . \tag{9}$$

Из неравенства $1 + p_t \leq p_1 + p_2 \leq p_i + p_j \leq p_i p_j$ и (9) следует, что

$$x^{p_i p_j} \equiv 0 \mod x^{p_t+1}, \quad x^{p_i p_j p_k} \equiv 0 \mod x^{p_t+1}, \quad \dots .$$

Поэтому для нечетного t

$$\Phi_{p_1 \dots p_t} = \frac{(1 - x^{p_1}) \dots (1 - x^{p_t})}{(1 - x)} \mod x^{p_t+1}. \tag{10}$$

Из неравенства $p_i + p_j \geq p_1 + p_2 > p_i = p_t$ следует, что

$$(1 - x^{p_1}) \dots (1 - x^{p_t}) \equiv (1 - x^{p_1} - \cdots - x^{p_t}) \mod x^{p_t+1}. \tag{11}$$

Очевидно, что

$$\frac{1}{1 - x} \equiv (1 + x + \cdots + x^{p_t}) \mod x^{p_t+1}.$$

Поэтому из (10) и (11) получаем:

$$\Phi_{p_1 \dots p_t} \equiv (1 + x + \cdots + x_t^p)(1 - x^{p_1} - \cdots - x^{p_t}) \mod x^{p_t+1}. \tag{12}$$

Раскроем в (12) скобки и выразим коэффициенты при x^{p_t} и x^{p_t-2} в выражении $(1 + x + \cdots + x^{p_t})(1 - x^{p_1} - \cdots - x^{p_t})$. Используя неравенство $0 < p_i \leq p_t$ и то, что в первый множителей входят все степени x, которые меньше чем p, можно вывести формулу для нахождения коэффициента при x^{p_t}:

$$-x^p - x^{p_{t-1}} x^{p_t - p_{t-1}} - x^{p_{t-2}} x^{p_t - p_{t-2}} - \cdots - x^{p_1} x^{p_t - p_1} + 1 \cdot x^{p_t} =$$

$$= x^{p_t} - \prod_{i=1}^{t} x^{p_i} x^{p_t - p_i} = x^{p_t} - t x^{p_t} = (1 - t) x^{p_t}. \tag{13}$$

Коэффициент при x^{p_t-2} получается соответственно:

$$-x^{p_t-2} - x^{p_{t-1}}x^{(p_t-2)-p_{t-1}} - x^{p_{t-2}}x^{(p_t-2)-p_{t-2}} \cdots - x^{p_1}x^{(p_t-2)-p_1} + 1 \cdot x^{p_t-2}.$$

$$= x^{p_t-2} - \prod_{i=1}^{t-1} x^{p_i}x^{(p_t-2)-p_i} = x^{p_t-2} - (t-1)x^{p_t-2} = (2-t)x^{p_t}. \quad (14)$$

Когда t пробегает все нечетные числа, начиная с 3, числа $1-t$ и $2-t$ в (13) и (14) пробегают все отрицательные числа.

Чтобы получить в качестве коэффициентов круговых многочленов все положительные числа, рассмотрим $\Phi_{2p_1\dots p_t}$, где $p_1 \geq 3$ и $p_1 + p_2 > p_t$. Число $n = p_1 \cdot p_2 \cdot \cdots \cdot p_t$ нечетно, поэтому $\Phi_{2n}(x) = \Phi_n(-x)$, как было уже показано в (3). Это означает, что у многочленов Φ_{2n} и Φ_n коэффициенты при нечетных степенях x отличаются знаком, т. е. у многочлена $\Phi_{2p_1\dots p_t}$ коэффициенты при x^{p_t} и x^{p_t-2} равны $t-1$ и $t-2$ соответственно. Это позволяет утверждать, что любое целое число может быть использовано в качестве коэффициента многочлена деления круга, способ нахождения такого многочлена и степени x, коэффициентом которого является выбранное число.

1. Нахождение многочлена деления круга с заданным коэффициентом

Опишем алгоритм нахождения многочлена деления круга при заданном коэффициенте, не равном ± 1. Этот коэффициент, как было показано ранее, может быть как положительным, так и отрицательным целым числом.

Алгоритм

Вход: целое число $k \neq \pm 1$.

Выход: многочлен Φ_n, содержащий число k в качестве одного из коэффициентов.

Если $k < 0$, то выполнить проверку:

Если k-четное, то задать $t = 1 - k$.

Иначе, задать $t = 2 - k$.

Иначе.

Если k-четное, то задать $t = 1 + k$.

Иначе, задать $t = 2 + k$.

Найти минимальные простые $p_1 < p_2 < \cdots < p_t$, для которых выполняется $p_1 + p_2 > p_t$.

Если $k < 0$, то найти $n = p_1 \cdot p_2 \dots p_t$.

Иначе $n = 2p_1 \cdot p_2 \dots p_t$.
Вычислить Φ_n (или его коэффициенты при соответствующих степенях, так, коэффициент k будет при x^{p_t} для четного k и при x^{p_t-2} для нечетного k).

Для решения данной задачи можно воспользоваться системой компьютерной алгебры WolframMathematica [26]. В этой системе можно получить все коэффициенты кругового многочлена заданного номера, исключая дубли. Так, например, код

$$\text{Select[Table[}\{c[n], n\}\text{,}\{n, 1, 200\}\text{],MemberQ[\#,-3,3]\&]}$$

ищет среди коэффициентов круговых многочленов с номерами от 1 до 200 коэффициент, равный «-3». Результатом является список из перечня коэффициентов и номеров кругового многочлена, у которого хотя бы один коэффициент равен «-3».

Рассмотрим несколько примеров при малых k:

1. Для $k = -2$ круговой многочлен Φ_n с наименьшим номером, где хотя бы один коэффициент равен «-2», находится при

$$t = 1 - k = 3, \qquad n = 3 \cdot 5 \cdot 7 = 105, \qquad 3 + 5 > 7,$$

количество множителей равно трем. $\Phi_{105} = \dots - 2x^7 - x^8 - \dots$ (это первый из известных многочленов такого вида [14]).

2. Для $k = -3$, действуя по алгоритму, находим:

$$t = 2 - k = 5, \qquad p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 1062347,$$

$$\Phi_{11\cdot13\cdot17\cdot19\cdot23} = \Phi_{1062347} = \dots - 3x^{21} + \dots.$$

При этом для $k = -3$ существует многочлен деления круга Φ_n с меньшим номером. Он находится при $n = 5\cdot7\cdot11$, $5+7 > 11$, количество множителей 3, что не соответствует алгоритму

$$\Phi_{385} = \Phi_{5\cdot7\cdot11} = \dots - 3x^{119} - 3x^{120} - 3x^{121} - \dots.$$

3. Для $k = 2$, действуя по алгоритму, находим:

$$t = 1 + k = 3, \qquad p_1 \cdot p_2 \cdot p_3 = 3 \cdot 5 \cdot 7 = 105, \qquad 3 + 5 > 7,$$

количество множителей 3.

$$\Phi_{2p_1p_2p_3} = \Phi_{2\cdot3\cdot5\cdot7} = \Phi_{210} = \cdots + 2x^7 + \dots.$$

И опять, есть многочлен Φ_n с меньшим номером, он находится при $n = 3 \cdot 5 \cdot 11 = 165$, количество множителей 3, но $3 + 5 < 11$, что не соответствует алгоритму.

$$\Phi_{165} = \Phi_{3\cdot5\cdot11} = \cdots + 2x^{16} + 2x^{17} + \cdots + 2x^{31} + 2x^{32} + 2x^{33} + \dots$$

$$\cdots + 2x^{47} + 2x^{48} + 2x^{49} + 2x^{63} + \dots,$$

и при этом номер нечетный.

4. Для $k = 3$, действуя по алгоритму, находим

$$t = 2 + k = 5, \qquad p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 1062347,$$

$$11 + 13 > 23,$$

количество множителей 5.

$$\Phi_{2p_1p_2p_3p_4p_5} = \Phi_{2\cdot11\cdot13\cdot17\cdot19\cdot23} = \Phi_{2124694} = \cdots + 3x^{21} + \dots.$$

Многочлен с меньшим номером $\Phi_{595} = \Phi_{5\cdot7\cdot17} = \cdots + 3x^{240} + \dots$ с нечетным номером.

5. Для $k = -4$, действуя по алгоритму, находим

$$t = 1 - k = 5, \qquad p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 1062347,$$

$$11 + 13 > 23,$$

количество множителей 5. $\Phi_{p_1p_2p_3p_4p_5} = \Phi_{11\cdot13\cdot17\cdot19\cdot23} = \Phi_{1062347} = \cdots - 4x^{23} + \dots$ Многочлен с меньшим номером

$$\Phi_{1365} = \Phi_{3\cdot5\cdot7\cdot13} = \cdots - 4x^{196} + \cdots - 4x^{206} + \cdots - 4x^{265} + \cdots - 4x^{275} + \dots$$

$$\cdots - 4x^{301} + \cdots - 4x^{311} + \cdots - 4x^{370} + \cdots - 4x^{380}.$$

Заключение

В результате проделанной работы удалось собрать в единую схему геометрические и аналитические характеристики многочлена деления круга, позволяющие явно выписать алгоритм нахождения многочленов деления круга, содержащие в качестве коэффициентов целые числа, не равные нулю, одному и минус одному.

Найдена группа многочленов необходимой характеристики и проанализирован результат, позволяющий выявить направления исследований. Вопрос о неоднозначности нахождения многочленов деления круга с заданным простым или составным коэффициентом позволяет продолжить исследования в разработке алгоритма нахождения многочлена с наименьшим номером, а также нахождения многочлена наименьшей степени с такими же характеристиками. Для этого требуются дальнейшие теоретические исследования свойств многочленов деления круга.

Неоднозначность нахождения многочленов деления круга с заданным простым или составным коэффициентом, а так же особенности его номера, такие как, разложение на простые множители и значительный порядок по отношению к заданному числу, способствует использованию многочленов деления круга в задании открытого ключа в криптографических системах.

Список источников

1. **Tripathi S. K., Gupta B., Soundra Pandian K. K.**. An alternative practical publickey cryptosystems based on the Dependent RSA Discrete Logarithm Problems // *Expert Systems With Applications*, 164 (2021), 114047.

2. **Sreedharan S., Eswaran C.**. A lightweight encryption scheme using Chebyshev polynomial maps // *Optik - International Journal for Light and Electron Optics*, 240 (2021), 166786.

3. **Билецкий А. А.**. Криптографические приложения обобщенных матриц Галуа и Фибоначчи // *Защита информации.* 15:2 (2013). С. 128–132.

4. **Зеленевский В. В., Зеленевский В. Ю., Зеленевский А. В. и др**. Статистический и корреляционный анализ адресных последовательностей в каналах передачи с кодовым уплотнением данных // *Известия Института инженерной физики.* 4:58 (2020). С. 31–34.

5. **Dai Z., Huang M.**. A criterion for primitivity of integral polynomial Mod 2d // *Chinese Science Bulletin*, 15 (1990), pp. 1128–1130.

6. **Zhu Y., Wang X.**. A criterion for primitive polynomials over Galois rings // *Discrete Mathematics*, 303 (2005), pp. 244–256.

7. **Федоров Г. В.**. О длине периода функциональной непрерывной дроби над числовым полем // *Доклады Российской академии наук. Математика, информатика, процессы управления.* 495:1 (2020). С. 78-83.

8. **Susilo W., Tonien J.** A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equation // *Theoretical Computer Science*, 885 (2021), pp. 125–130.

9. **Pousin J.** Least squares formulations for some elliptic second order problems, feedforward neural network solutions and convergence results // *Journal of Computational Mathematics and Data Science*, 2 (2022), 100023.

10. **Прасолов В. В.** Многочлены / МЦНМО. М., 2003.

11. **Ван дер Варден Б. Л.** Алгебра. М.: Наука, 1979.

12. **Вялый М. Н., Гимадеев Р. А.** О различении слов вхождениями подслов // *Дискретный анализ и исследование операций.* 21:1(115) (2014). С. 3–14.

13. **Галиева Л. И., Галяутдинов И. Г.** Об одном классе уравнений, разрешимых в радикалах // *Известия высших учебных заведений. Математика.* 2011. № 2. С. 22–30.

14. **Савельев И. В.** Круговые многочлены и особенности комплексных гиперповерхностей // *УМН.* 48:2 (290) (1993). С. 197–198.

15. **Лиопо В. А., Сабуть А. В.** Точечные группы и сингонии некристаллографической симметрии // *Вестник Гродненского государственного университета имени Янки Купалы. Серия 2. Математика. Физика. Информатика, вычислительная техника и управление*. 1:148 (2013). С. 115–126.

16. **Fan S., Wang X.** Primitive normal polynomials with the specified last two coefficientss // *Discrete Mathematics*, 309 (2009), pp. 4502-4513.

17. **Fan S. Q., Han W. B., Feng K. Q.** Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result // *Finite Fields and Their Applications*, 13:4 (2007), pp. 1029–1044.

18. **Fan S. Q., Han W. B., Feng K. Q., Zhang X. Y.** Primitive normal polynomials with the first two coefficients prescribed: A revised p-adic method // *Finite Fields and Their Applications*, 13 (2007), pp. 577–604.

19. **Brochero Martinez F. E., Reis L., Silva–Jesus L.** Factorization of composed polynomials and applications // *Discrete Mathematics*, 342 (2019), 111603.

20. **Bakshi G. K., Raka M.** A class of constacyclic codes over a finite field // *Finite Fields Appl.*, 18:6 (2012), 362–377.

21. **Brochero Martinez F. E., Giraldo Vergara C. R., de Oliveira L.** Explicit factorization of xn - 1 ∈ Fq[x] // *Des. Codes Cryptogr.*, 77 (2015), pp. 277–286.

22. **Brochero Martinez F. E., Reis L.** Factoring polynomials of the form f(xn) ∈ Fq[x] // *Finite Fields Appl.*, 49 (2018), pp. 166–179.

23. **Li F., Yue Q.** The primitive idempotents and weight distributions of irreducible constacyclic codes // *Des. Codes Cryptogr.*, 86 (2018), pp. 771–784.

24. **Liu L., Li L., Wang L., Zhu S.** Repeated-root constacyclic codes of length nlps // *Discrete Math.*, 340:9 (2017), 2250–2261.

25. **Wu Y., Yue Q., Fan S.** Further factorization of xn - 1 over a finite fiel // *Finite Fields Appl.*, 54 (2018), pp. 197–215.

26. WOLFRAM MATHEMATICA ONLINE [Электронный ресурс], WolframAlpha.com (2022). URL: https://www.wolfram.com/mathematica/online/ (дата обращения: 05.06.2022).

References

1. **Tripathi S. K., Gupta B., Soundra Pandian K. K.** An alternative practical publickey cryptosystems based on the Dependent RSA Discrete Logarithm Problems. *Expert Systems With Applications*, 164 (2021), 114047.

2. **Sreedharan S., Eswaran C.** A lightweight encryption scheme using Chebyshev polynomial maps. *Optik - International Journal for Light and Electron Optics*, 240 (2021), 166786.

3. **Biletsky A. A.** Cryptografy applications of primitive matrices Galois and Fibonacci. *Zashhita informacii* [Information Security Research Journal], 15:32 (2013), pp. 128–132. (In Russ.)

4. **Zelenevsky V. V., Zelenevsky V. Yu., Zelenevsky A. V. et al**. Statisticheskiy i korrelyatsionnyy analiz adresnykh posledovatel'nostey v kanalakh peredachi s kodovym mul'tipleksirovaniyem dannykh. *Izvestiya Instituta inzhenernoy fiziki* [Proceedings of the Institute of Engineering Physics]. 4:58 (2020), pp. 31–34. (In Russ.)

5. **Dai Z., Huang M.** A criterion for primitivity of integral polynomial Mod 2d. *Chinese Science Bulletin*, 15 (1990), pp. 1128–1130.

6. **Zhu Y., Wang X.** A criterion for primitive polynomials over Galois rings. *Discrete Mathematics*, 303 (2005), pp. 244–256.

7. **Fedorov G. V.** On the Period Length of a Functional Continued Fraction over a Number Field. *Doklady Rossijskoj akademii nauk. Matematika, informatika, processy upravleniya* [Papers of the Russian Academy of Sciences. Mathematics, computer science, control processes], 102 (2020), pp. 513–517. (In Russ.)

8. **Susilo W., Tonien J.** A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equation. *Theoretical Computer Science*, 885 (2021), pp. 125–130.

9. **Pousin J.** Least squares formulations for some elliptic second order problems, feedforward neural network solutions and convergence results. *Journal of Computational Mathematics and Data Science*, 2 (2022), 100023.

10. **Prasolov V. V.** *Mnogochleny* [Polynomials], Moscow Center For Continuous Mathematical Education, M., 2003 (In Russ.)

11. **Van der Waerden B. L.** Algebra. M.: Nauka, 1979. (In Russ.)

12. **Vyalyi M. N., Gimadeev R. A.** Separation of words by positions of subwords. Discretnyy analiz i issledovaniye operatsiy [Discrete Analysis and Operations Research], 21:1(115) (2014), pp. 3–14. (In Russ.)

13. **Galieva L. I., Galyautdinov I. G.** On a class of equations solvable in radicals. Izvestiya vysshix uchebnyx zavedenij. Matematika [Russian Math. (Iz. VUZ)], 55:2 (2011), pp. 18–25. (In Russ.)

14. **Savel'ev I. V.** Circular polynomials and singularities of complex hypersurfaces. Uspekhi Mat. Nauk [Advances in Mathematical Sciences], 48:2 (290) (1993), pp. 197–198. (In Russ.)

15. **Liopo V. A., Sabut A. V.** Point groups and syngonies of noncrystallographic symmetry. *Vestnik Grodnenskogo gosudarstvennogo universiteta imeni Yanki Kupaly‘. Seriya 2. Matematika. Fizika. Informatika, vy‘chislitel‘naya texnika i upravlenie* [Bulletin of Grodno State University named after Yanka Kupala. Series 2. Mathematics. Physics. Informatics, computer technology and management], 1:148 (2013), pp. 115–126. (In Russ.)

16. **Fan S., Wang X.** Primitive normal polynomials with the specified last two coefficientss. *Discrete Mathematics*, 309 (2009), pp. 4502–4513.

17. **Fan S. Q., Han W. B., Feng K. Q.** Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result. *Finite Fields and Their Applications*, 13:4 (2007), pp. 1029–1044.

18. **Fan S. Q., Han W. B., Feng K. Q., Zhang X. Y.** Primitive normal polynomials with the first two coefficients prescribed: A revised p-adic method. *Finite Fields and Their Applications*, 13 (2007), pp. 577–604.

19. **Brochero Martнnez F. E., Reis L., Silva–Jesus L.** Factorization of composed polynomials and applications. *Discrete Mathematics*, 342 (2019), 111603.

20. **Bakshi G. K., Raka M.** A class of constacyclic codes over a finite field. *Finite Fields Appl.*, 18:6 (2012), pp. 362–377.

21. **Brochero Martнnez F. E., Giraldo Vergara C. R., de Oliveira L.** Explicit factorization of xn - 1 ∈ Fq[x] . D*es. Codes Cryptogr.*, 77 (2015), pp. 277–286.

22. **Brochero Martнnez F. E., Reis L.** Factoring polynomials of the form f(xn) ∈ Fq[x] . *Finite Fields Appl.*, 49 (2018), pp. 166–179.

23. **Li F., Yue Q.** The primitive idempotents and weight distributions of irreducible constacyclic codes. *Des. Codes Cryptogr.*, 86 (2018), pp. 771–784.

24. **Liu L., Li L., Wang L., Zhu S.** Repeated-root constacyclic codes of length nlps. *Discrete Math.*, 340:9 (2017), pp. 2250–2261.

25. **Wu Y., Yue Q., Fan S.** Further factorization of xn - 1 over a finite fiel. *Finite Fields Appl.*, 54 (2018), pp. 197–215.

26. WOLFRAM MATHEMATICA ONLINE [Электронный ресурс], WolframAlpha.com (2022), Available at: https://www.wolfram.com/mathematica/online/ (accessed 05.06.2022).

Сведения об авторах / Information about authors
Татьяна Михайловна Банникова / Tatyana M. Bannikova
к.п.н., доцент кафедры алгебры и топологии / Candidate of Pedagogical Sciences, Associate Professor of the Algebra and Topology Department
Удмуртский государственный университет / Udmurt State University
426034, Удмуртская Республика, г. Ижевск, ул. Университетская, 1 / 426034, Udmurt Republic, Izhevsk, Universitetskaya St., 1

Ольга Михайловна Немцова / Olga M. Nemtsova
к.ф.-м.н., доцент кафедры информатики и математики / Candidate of Physics and Mathematics, Associate Professor of the Informatics and Mathematics Department
Удмуртский государственный университет / Udmurt State University
426034, Удмуртская Республика, г. Ижевск, ул. Университетская, 1 / 426034, Udmurt Republic, Izhevsk, Universitetskaya St., 1

Статья поступила в редакцию / The article was submitted 06.06.2022
Одобрено после рецензирования / Approved after reviewing 25.06.2022
Принято к публикации / Accepted for publication 25.06.2022