УДК 512.62
DOI: 10.25559/SITITO.16.202002.314-320

О порядках элементов квадратичного расширения конечного поля характеристики 2

В. М. Максимов[1], В. И. Ремезова[2*]
[1] ФГБОУ ВО «Российский государственный гуманитарный университет», г. Москва, Россия
125993, Россия, г. Москва, пл. Миусская, д. 6
[2] ФГАОУ ВО «Российский университет дружбы народов», г. Москва, Россия
117198, Россия, г. Москва, ул. Миклухо-Маклая, д. 6
[*] remezova.98@mail.ru

Аннотация

Пусть $F(2^m)$ произвольное поле характеристики 2, его квадратичное расширение мы будем рассматривать как алгебру с базисом $\mathbf{1}, e$ над полем $F(2^m)$. Здесь $\mathbf{1}$ рассматривается как единичный элемент алгебры, а элемент e удовлетворяет соотношению $e^2 = e + \alpha$. Элемент α может быть произвольным из поля $F(2^m)$, но неудовлетворяющий условию $\alpha = x + x^2$ при некотором x из $F(2^m)$.

Пусть $n_0(\alpha)$ обозначает порядок элемента e. Тогда основной результат работы можно сформулировать так: Неприводимый полином $1 + t + \alpha t^2$ делит полином $1 + t^n$ тогда и только тогда, когда $n_0(\alpha)$ делит натуральное n.

Аналогичные результаты для произвольных элементов поля $F(2^{2m})$ следуют из этого. Доказательство базируется на свойствах рекуррентных соотношений между полиномами $P_n(\alpha)$ и $Q_n(\alpha)$, определяемые для всех $n = 0,1,2, \dots$ из соотношений $e^n = P_n(\alpha) + Q_n(\alpha)e$. Формулы для производящих рядов этих полиномов содержат наиболее важные такие свойства. Эти формулы были получены и имеют вид:

$$\sum_0^\infty P_k(\alpha)t^k = \frac{1+t}{1+t+\alpha t^2} \text{ и } \sum_0^\infty Q_k(\alpha)t^k = \frac{t}{1+t+\alpha t^2}.$$

Ключевые слова: конечное поле, характеристика 2, порядок элемента, квадратичное расширение поля, дискретный логарифм, неприводимый полином, рекуррентная последовательность, производящий ряд.

Для цитирования: Максимов, В. М. О порядках элементов квадратичного расширения конечного поля характеристики 2 / В. М. Максимов, В. И. Ремезова. – DOI 10.25559/SITITO.16.202002.314-320 // Современные информационные технологии и ИТ-образование. – 2020. – Т. 16, № 2. – С. 314-320.

On the Orders of the Elements of a Square Extension of a Finite Field of Characteristic 2

V. M. Maximov[a], V. I. Remezova[b*]
[a] Russian State University for the Humanities, Moscow, Russia
6 Miusskaya Sq., Moscow 125993, GSP-3, Russia
[b] Peoples' Friendship University of Russia, Moscow, Russia
6 Miklukho-Maklaya St., Moscow 117198, Russia
[*] remezova.98@mail.ru

Abstract

Let $F(2^m)$ will be an arbitrary finite field of characteristic 2. It's square extension will be considered as an algebra with basic elements 1 and e over the field $F(2^m)$. Here **1** is considered as the unit element of the algebra, and e satisfies the relation: $e^2 = e + \alpha$. An element α maybe arbitrary from the field $F(2^m)$, but it is not satisfying to the condition $\alpha = x + x^2$ for some x element from $F(2^m)$.
Let us $n_0(\alpha)$ denote the order of basis element e. Then the main result of the paper can be formulated as: The irreducible polynomial $1 + t + \alpha t^2$ divides the polynomial $1 + t^n$ if and only the order if $n_0(\alpha)$ divides a natural n.
The similar results for arbitrary elements of field $F(2^{2m})$ follow from main theorem. The proof of main result based on the properties of the recurrence relations between the polynomials $P_n(\alpha)$ and $Q_n(\alpha)$, definite for all $n = 0,1,2,\ldots$ by the relations $e^n = P_n(\alpha) + Q_n(\alpha)e$. The formulas for the generating series of these polynomials contain the most important such properties. The formulas were obtained and we have:
$\sum_0^\infty P_k(\alpha)t^k = \frac{1+t}{1+t+\alpha t^2}$, $\sum_0^\infty Q_k(\alpha)t^k = \frac{t}{1+t+\alpha t^2}$.

Keywords: Finite field, characteristic 2, order of element, square extension over a field, discrete logarithm, irreducible polynomial, recursive sequence, generating series.

For citation: Maximov V.M., Remezova V.I. On the Orders of the Elements of a Square Extension of a Finite Field of Characteristic 2. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2020; 16(2):314-320. DOI: https://doi.org/10.25559/SITITO.16.202002.314-320

1. Введение

Квадратичное расширение поля $F(2^m)$ (из 2^m элементов) и которое является полем $F(2^{2m})$, включающее поле $F(2^m)$, удобно рассматривать как алгебру с базисом $\mathbf{1}, e$ над полем $F(2^m)$, где $\mathbf{1}$ – единичный элемент алгебры и $e^2 = e + \alpha\mathbf{1}$ и $\alpha -$ может быть произвольным элементом $F(2^m)$, который нельзя представить в виде $t + t^2, t \in F(2^m)$.
В таком виде квадратичное расширение поля $F(2^m)$ рассматривалось в [1] и применялось для усложнения дискретного логарифма. Идея такого подхода состоит в том, что в поле $F(2^{2m})$ можно пытаться указать элементы порядка $2^{2m} - 1$ или близких к этому. Основанием для этого является то, что каждый элемент из $F(2^{2m})$ представляется в виду $x + ye$, где x, y элементы $F(2^n)$. При этом первым претендентом на роль такого элемента является базисный элемент e.
Могут быть различные принципы отбора элементов – претендентов иметь «большой» порядок и каждый из них требует особого исследования.
Доказательство существования «большого» порядка ($> 2^{1000}$) у какого – нибудь элемента из $F(2^{1024})$ $(m = 512)$, означало бы решение проблемы дискретрого логарифма при уровне возможностей современных ЭВМ. Поэтому существует большое число работ, посвященных этой тематике. В связи с этим, укажем некоторые из них [2-12].
Результатом нашего исследования является обнаружение некоторых свойств порядка базисного элемента e.

2. Полиномы $P_n(\alpha)$ и $Q_n(\alpha)$

Будем рассматривать степени e^n. При этом элемент α, который является параметром при вычислениях, рассматривается просто как элемент $F(2^m)$. Поэтому $2\alpha = 0$ и $\alpha^{2^m} = \alpha$, хотя для каждого α имеются ещё специальные соотношения, например, $\alpha^{d_0} = 1$, где $d_0 -$ порядок элемента α. При изучении соотношений между полиномами специальные соотношения для α использоваться не будут. Так как $e^2 = e + \alpha$, $e^3 = e^2 e = \alpha + (1 + \alpha)e$, $e^4 = e + \alpha + \alpha^2$ и т.д., то можно положить

$$e^n = P_n(\alpha) + Q_n(\alpha)e, \quad n = 0, 1, 2, \ldots \tag{1}$$

где $e^0 = \mathbf{1}$, $e^1 = e$. Поэтому $P_0(\alpha) = 1$, $Q_0(\alpha) = 0$; $P_1(\alpha) = 0$, $Q_1(\alpha) = 1$.
На выражения $P_n(\alpha)$ и $Q_n(\alpha)$ мы будем смотреть как на полиномы над полем $F_2 = \{0, 1\}$, при произвольных значениях $\alpha \in F(2^m)$. Однако, при необходимости рассматриваются соотношения для фиксированного α. Тогда для значений полиномов $P_n(\alpha)$ и $Q_n(\alpha)$ легко написать рекуррентные соотношения. Действительно,

$$e^{n+1} = P_{n+1}(\alpha) + Q_{n+1}(\alpha)e = [P_n(\alpha) + Q_n(\alpha)e]e = \\ = P_n(\alpha)e + Q_n(\alpha)(e + \alpha) = \alpha Q_n(\alpha) + [P_n(\alpha) + Q_n(\alpha)]e.$$

Следовательно,

$$P_{n+1}(\alpha) = \alpha Q_n(\alpha), \; Q_{n+1}(\alpha) = P_n(\alpha) + Q_n(\alpha) \tag{2}$$

с начальными условиями $P_0(\alpha) = 1$, $Q_0(\alpha) = 0$ или $P_1(\alpha) = 0$, $Q_1(\alpha) = 1$.
Тогда заменяя $P_n(\alpha)$ на $Q_{n-1}(\alpha)$ во втором уравнении (2), получаем рекурренту для полиномов $Q_n(\alpha)$

$$Q_{n+1}(\alpha) = Q_n(\alpha) + \alpha Q_{n-1}(\alpha) \tag{3}$$

Если начальными условиями считать $Q_0(\alpha) = 0$, $Q_1(\alpha) = 1$, то все дальнейшие значения $Q_2(\alpha), Q_3(\alpha), \ldots$ этой рекурренты являются полиномами (1). Аналогично, заменяя, значения во втором уравнении (2), $Q_{n+1}(\alpha)$ на $\frac{1}{\alpha} P_{n+2}(\alpha)$, $Q_n(\alpha)$ на $\frac{1}{\alpha} P_{n+1}(\alpha)$, получим такую же рекурренту, но с другими начальными условиями. Итак, имеем

$$P_{n+2}(\alpha) = P_{n+1}(\alpha) + \alpha P_n(\alpha) \tag{4}$$

при начальных условиях $P_0(\alpha) = 1$, $P_1(\alpha) = 0$. Получаемая последовательность из рекурренты очевидно совпадает с $P_n(\alpha)$ из (2).
Рекурренты (3) и (4) дают оценки снизу для натурального n_0, для которого впервые $P_{n_0}(\alpha) = 1$, $Q_{n_0}(\alpha) = 0$. Именно при таком n_0, $n_0 > 0$, впервые $e^{n_0} = \mathbf{1}$, $n_0 -$ порядок элемента e. Так как n_0 зависит от элемента α, $e^2 = e + \alpha$, то там, где требуется подчеркнуть эту зависимость, мы будем писать $n_0(\alpha)$.

Предложение 1. Для того, чтобы $n_0(\alpha)$ был порядком элемента e, необходимо и достаточно, чтобы

$$P_0(\alpha) + P_1(\alpha) + \cdots + P_{n_0(\alpha)-1}(\alpha) = Q_0(\alpha) + Q_1(\alpha) + \cdots + \\ Q_{n_0(\alpha)-1}(\alpha) = 0 \tag{5}$$

где по определению выше $P_0(\alpha) = 1$, $Q_0(\alpha) = 0$.

Доказательство. Пусть $e^{n_0(\alpha)} = 1$. Тогда рассмотрим сумму $\mathbf{1} + e + \cdots + e^{n_0(\alpha)-1}$. Так как эта сумма в поле $F(2^{2m})$, то справедлива формула геометрической прогрессии. Тогда имеем

$$\mathbf{1} + e + \cdots + e^{n_0(\alpha)-1} = \frac{(\mathbf{1} + e^{n_0(\alpha)})}{(\mathbf{1} + e)} = \frac{\mathbf{1+1}}{(\mathbf{1} + e)} = \mathbf{0}.$$

Следовательно,

$$\mathbf{1} + e + \cdots + e^{n_0(\alpha)-1} = \\ = [P_0(\alpha) + Q_0(\alpha)e] + [P_1(\alpha) + Q_1(\alpha)e] + \cdots \\ + \left[P_{n_0(\alpha)-1}(\alpha) + Q_{n_0(\alpha)-1}(\alpha)e\right] = \mathbf{0}.$$

Таким образом

$$P_0(\alpha) + P_1(\alpha) + \cdots + P_{n_0(\alpha)-1}(\alpha) \\ = Q_0(\alpha) + Q_1(\alpha) + \cdots + Q_{n_0(\alpha)-1}(\alpha) = \mathbf{0}$$

Обратно, допустим, что справедливо (5). Тогда, очевидно, что

$$\mathbf{1} + e + \dots + e^{n_0(\alpha)-1} = 0 = \frac{(\mathbf{1} + e^{n_0(\alpha)})}{(\mathbf{1} + e)}.$$

Следовательно, $\mathbf{1} + e^{n_0(\alpha)} = \mathbf{0}$ и $e^{n_0(\alpha)} = \mathbf{1}$ ■

Заметим, так как $e^{n_0(\alpha)} = \mathbf{1}$ следует $P_{n_0(\alpha)}(\alpha) = \mathbf{1}, Q_{n_0(\alpha)}(\alpha) = \mathbf{0}$,
то из равенства $P_{n+1}(\alpha) = \alpha Q_n(\alpha)$, $n = 0, 1, 2, \dots$, следует

$$P_1(\alpha) + \dots + P_{n_0(\alpha)}(\alpha) = \alpha Q_0(\alpha) + \dots + \alpha Q_{n_0(\alpha)-1}(\alpha) = \mathbf{0} \qquad (6)$$

Очевидно, (6) также следует из предложения 1, так как $P_0(\alpha) = \mathbf{1}, P_{n_0(\alpha)}(\alpha) = \mathbf{1}$.
Найдём также обратный элемент для $(\mathbf{1} + e)$, так как он необходим при вычислении суммы $\mathbf{1} + e + \dots + e^k = \frac{(\mathbf{1}+ e^{k+1})}{(\mathbf{1}+ e)}$.
Из очевидного соотношения $e^2 = e + \alpha$, имеем, $e^2 + e = \alpha = e(\mathbf{1} + e)$. Следовательно,

$$(\mathbf{1} + e)^{-1} = \alpha^{-1} e \qquad (7)$$

Таким образом, имеем

$$\mathbf{1} + e + \dots + e^k = \frac{(\mathbf{1}+ e^{k+1})}{(\mathbf{1}+ e)} = \alpha^{-1}(e + e^{k+2}) \qquad (8)$$

Следовательно, из (8) получаем

$$P_0(\alpha) + P_1(\alpha) + \dots + P_k(\alpha) = \frac{1}{\alpha}(P_1(\alpha) + P_{k+2}(\alpha)) \qquad (9)$$
$$Q_0(\alpha) + Q_1(\alpha) + \dots + Q_k(\alpha) = \frac{1}{\alpha}(Q_1(\alpha) + Q_{k+2}(\alpha))$$

Нетрудно показать, что эти формулы являются также следствием (3), (4).
Обозначим $S\,(P_n) = P_1(\alpha) + \dots + P_{n-1}(\alpha)$, $S\,(Q_n) = Q_1(\alpha) + \dots + Q_{n-1}(\alpha)$. тогда из формул (2) и (3) вытекает
Предложение 2. Последовательности $S\,(P_n)$ и $S\,(Q_n)$ являются рекуррентами вида (3) и (2). Кроме того, имеет место

$$P_{n+1}(\alpha) = \alpha + \alpha S\,(P_n) \text{ и } Q_{n+1}(\alpha) = \mathbf{1} + \alpha S\,(Q_n) \qquad (10)$$

Доказательство. Запишем цепочку соотношений (2)

$$\begin{aligned} &Q_{n+1}(\alpha) = Q_n(\alpha) + \alpha Q_{n-1}(\alpha) \\ &Q_n(\alpha) = Q_{n-1}(\alpha) + \alpha Q_{n-2}(\alpha) \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ &Q_3(\alpha) = Q_2(\alpha) + \alpha Q_1(\alpha) \end{aligned} \qquad (11)$$

Делая очевидные сокращения и складывая. Получим

$$Q_{n+1}(\alpha) = Q_2(\alpha) + \alpha S\,(Q_n)$$

Аналогично получим

$$P_{n+1}(\alpha) = P_2(\alpha) + \alpha S\,(P_n)$$

Осталось заметить, что $P_2(\alpha) = \alpha$, $Q_2(\alpha) = \mathbf{1}.$ Тем самым равенства (10) доказаны.
Сложим теперь все равенства (11). Замечая, что $Q_2(\alpha) = \mathbf{1}$, $Q_1(\alpha) = \mathbf{1}$, получаем $S(Q_{n+2}) = S(Q_{n+1}) + \alpha S(Q_n) + 1$. В случае полиномов $P_k(\alpha)$ к суммам слева и справа требуется добавить $P_2(\alpha) + P_1(\alpha)$. Так как $P_2(\alpha) = a$, $P_1(\alpha) = 0$, то в итоге получим
$S(P_{n+2}) = S(P_{n+1}) + \alpha S(P_n) + a$ ■

3. Производящие ряды для полиномов $P_n(\alpha)$ и $Q_n(\alpha)$

Вначале несколько слов об алгебре формальных рядов от одной формальной образующей t с коэффициентами из конечного поля $F(2^m)$. Элементы такой алгебры представляются формально рядами $\sum_0^\infty c_k t^k$, $c_k \in F(2^m)$. Здесь не может быть речи ни о какой сходимости, кроме того, что между рядами установлена операция сложения (сложение коэффициентов при одинаковых степенях t), а умножение рядов, как обычное умножение, т.е. $(\sum c_k t^k)(\sum d_n t^n) = \sum_{m=0}^\infty \sum_m (\sum_{k+n=m} c_k\, d_n)\, t^m$ и умножение ряда на элемент $c \in F(2^m)$, как умножение коэффициентов на этот элемент. Таким образом, множество всех таких рядов становится алгеброй над полем $F(2^m)$.
Таким образом, производящие ряды

$$P(t) = \sum_0^\infty P_n(\alpha) t^n \text{ и } Q\,(t) = \sum_0^\infty Q_n(\alpha) t^n \qquad (12)$$

являются формальными рядами из введённой алгебры формальных рядов над полем $F(2^m)$. Можно рассмотреть также формальный ряд для степеней $e^{\,n}$, т.е. формальный ряд уже над полем $F(2^{2m})$. Тогда имеем

$$\mathbf{1} + et + \dots + e^2 t^2 + \dots = \frac{\mathbf{1}}{1+\mathrm{et}} = P(t) + Q(t)e \qquad (13)$$

Отсюда легко находим выражения для $P(t)$ и $Q(t)$.
Действительно, из (13) имеем

$\mathbf{1} = (\mathbf{1} + et)(P(t) + Q(t)e) = P(t) + Q(t)e + tP(t)e + tQ(t)(e + \alpha)$, так как $e^2 = e + \alpha$

Откуда, сравнивая коэффициенты, получаем

$$\begin{aligned} &P(t) + t\alpha Q(t) = \mathbf{1} \\ &tP(t) + (\mathbf{1} + t)Q(t) = \mathbf{0} \end{aligned} \qquad (14)$$

Определитель этой системы равен $1 + t + at^2 = \frac{1}{a}(a + at + (at)^2)$. Он отличен от нуля в силу свойства элемента a: элемент a не может быть представлен суммой $U + U^2$, $U \in F(2^m)$, ни при каком $U \in F(2^m)$. Поэтому единственными решениями $P(t)$ и $Q(t)$ будут

$$P(t) = \frac{1+t}{1+t+at^2},\quad Q(t) = \frac{t}{1+t+at^2} \qquad (15)$$
И

$$P(t)+Q(t)=\frac{1}{1+t+at^2} \quad (16)$$

Так как многочлен $1+t+at^2$ не разлагается на линейные множители, то мы не можем представить ряды также, как это делают в обычном анализе.

К рекуррентным соотношениям можно подойти несколько по иному. Так как $P_{n+1}(a)=aQ_n(a)$ и $Q_{n+1}(a)=P_n{}^{(a)}+Q_n(a)$, то эти равенства можно представить в матричном виде

$$\begin{pmatrix}P_{n+1}(a)\\ Q_{n+1}(a)\end{pmatrix}=\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}\begin{pmatrix}P_n(a)\\ Q_n(a)\end{pmatrix}, n=0,1,2,\dots \quad (17)$$

Отсюда следует, что

$$\begin{pmatrix}P_n(a)\\ Q_n(a)\end{pmatrix}=\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}^n\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}^{n-1}\begin{pmatrix}0\\ 1\end{pmatrix} \quad (18)$$

Отсюда легко можно связать производящий ряд степеней матрицы $W=\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}$ с производящими рядами $P_n(a)$ и $Q_n(a)$. Положим

$$W(t)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}t+\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}^2 t^2+\cdots \quad (19)$$

который очевидно представляется в виде

$$W(t)=\frac{1}{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}+\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}t}=\frac{1}{\begin{pmatrix}1 & \alpha t\\ t & 1+t\end{pmatrix}} \quad (20)$$

Поскольку определитель $\begin{vmatrix}1 & \alpha t\\ t & 1+t\end{vmatrix}=1+t+at^2$, который как формальный ряд отличен от нуля, то обратная матрица будет равна $W(t)=\frac{1}{1+t+at^2}\begin{pmatrix}1+t & \alpha t\\ t & 1\end{pmatrix}$.

Поэтому $\begin{pmatrix}P_n(a)\\ Q_n(a)\end{pmatrix}=W(t)\begin{pmatrix}1\\ 0\end{pmatrix}$ и вновь получаем $P(t)=\frac{1+t}{1+t+at^2}$, $Q(t)=\frac{t}{1+t+at^2}$.

Очевидно, что порядок матрицы $W=\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}$ должен быть точно связан с порядком элемента e. Точнее имеет место

Предложение 3. Порядок элемента e равен порядку матрицы $W=\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}$.

Доказательство. Пусть $W^n=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. Тогда из (18) следует, что $P_n(\alpha)=1$, $Q_n(\alpha)=0$. То есть $e^n=P_n(\alpha)+Q_n(\alpha)e=\mathbf{1}$. Обратно, пусть $e^n=\mathbf{1}$ и $W^n=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Тогда из равенства (18) имеем $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}$. Откуда следует $a=1, c=0$. Следовательно, $W^n=\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}$. Так как матрица $W^n=\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}$ перестановочна с $W=\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}$, то получаем

$$\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}=\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}\begin{pmatrix}0 & \alpha\\ 1 & 1\end{pmatrix}.$$

Выполним с обеих сторон умножение и, сравнив элементы, получим $b=0, ad=a+b$. Т.е. $d=1$ и $W^n=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. Таким образом, если порядок W равен n_1, т.е. $W^{n_1}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ и $W^k\neq\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ при $1\le k<n_1$, а n_0 – порядок e, т.е. $e^{n_0}=\mathbf{1}$ и $e^k\neq\mathbf{1}$ при $1\le k<n_0$. Тогда с одной стороны, из $W^{n_1}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ следует, что $e^{n_1}=\mathbf{1}$ и следовательно n_1 кратно n_0 и поэтому $n_0\le n_1$. А с другой стороны, аналогично имеем, что n_0 кратно n_1 и поэтому $n_1\le n_0$. Следовательно, $n_0=n_1$ ■

4. Основная теорема

Естественно возникает вопрос, насколько полезны полученные выше формулы для рекуррент и производящих рядов для нахождения элементов в поле $F(2^{2m_0})$ «больших» порядков. Оказывается, на основании этих формул можно получить интересное предложение, которое может быть использовано для оценки порядков конкретных элементов из $F(2^{2m_0})$. Например, e и его порядка $n_0(a)$ в каждом конкретном случае элемента a.

Теорема 1 (основная). Для того, чтобы многочлен $1+t^n$ делился на неприводимый $1+t+at^2$, необходимо и достаточно делимости n на $n_0(a)$.

Доказательство. Пусть n – кратно $n_0(a)$ – порядок элемента e. Тогда $e^n=\mathbf{1}$ и, следовательно, $Q_n(\alpha)=0$, $Q_{n+1}(\alpha)=Q_1(\alpha),\dots,Q_{n+2}(\alpha)=Q_2(\alpha),\dots,Q_{2n}(\alpha)=Q_n(\alpha)=0$ и т.д. Если обозначить многочлен $Q_0(\alpha)+Q_1(\alpha)t+\ \dots+Q_{n-1}(\alpha)t^{n-1}=q(t)$, то ряд $Q(t)$ равен

$$Q(t)=\ q(t)+q(t)t^n+q(t)t^{2n}+\cdots=q(t)\frac{1}{1+t^n}$$

Так как $Q(t)$ удовлетворяет (15), то имеем $\frac{t}{1+t+at^2}=\frac{q(t)}{1+t^n}$ или $q(t)=\frac{t(1+t^n)}{1+t+at^2}$

Так как многочлены t и $1+t+at^2$ взаимопросты, то многочлен $1+t^n$ делится на $1+t+at^2$.

Аналогичный результат получается, если вместо $Q_n(a)$ и $Q(t)$ рассматривать полиномы $P_n(a)$ и $P(t)$.

Допустим теперь, что многочлен $1+t^n$ делится на $1+t+at^2$. Тогда положим $q_1(t)=\frac{t(1+t^n)}{1+t+at^2}$, где $q_1(t)$ есть многочлен степени $n-1$.

Отсюда, следует, $\frac{q_1(t)}{1+t^n}=\frac{t}{1+t+at^2}=Q(t)$.

Следовательно, имеем,

$$Q(t)=Q_0(\alpha)+Q_1(\alpha)t+\ \dots=q_1(t)+q_1(t)t^n+\cdots,$$

Откуда многочлен $q_1(t)$ равен $Q_0(\alpha)+Q_1(\alpha)t+\ \dots+Q_{n-1}(\alpha)t^{n-1}$ и $Q_{n-1}(\alpha)\neq 0$, так как $q_1(t)$ степени $n-1$. А $q_1(t)\,t^n$ имеет минимальную степень $\ge n$. Так как из вида $q_1(t)$ имеем $q_1(0)=0$. Следовательно, коэффициент $Q_n(\alpha)$ при t^n в этом производящем ряде равен $Q_0(\alpha)=0$. Т.е. если многочлен $1+t^n$ делится на $1+t+at^2$, то $Q_n(\alpha)=0$. Аналогично рассмотрим полином $p_1(t)=\frac{(1+t)(1+t^n)}{1+t+at^2}$, который также имеет степень $n-1$. Тогда имеем

$\frac{p_1(t)}{1+t^n}=p_1(t)+p_1(t)t^n+\dots=\frac{1+t}{1+t+at^2}=P(t)$, согласно (15).

Поэтому $p_1(t)+p_1(t)t^n+\cdots=P_0(a)+P_1(a)t+\cdots+P_n(a)t^n+\cdots$

Так как степень $p_1(t)$ равна $n-1$, то $p_1(t)=P_0(a)+P_1(a)t^n+\cdots+P_{n-1}(a)t^{n-1}$ и коэффициент $P_n(a)$ при t^n равен $P_0(a)=1$. То есть $e^n=P_n(a)+Q_n(a)e=1$. Итак, имеем $P_n(a)=1$, $Q_n(a)=0$. Следовательно, n – кратно $n_0(a)$.

Следствие 1. Порядок элемента e есть наименьшая степень многочленов вида (1+t^n) делящихся на многочлен $1+t+at^2$. Элемент e есть фиксированный базисный элемент квадратичного расширения $F(2^{2m})$. Поэтому каждый элемент квадратичного расширения имеет вид $\mu+\alpha e$; $\mu,\alpha\in F(2^{2m})$. Интересно иметь условия аналогичные теореме 1 для элементов $\mu+\alpha e$. Прежде всего надо заметить, что порядок элемента αe, очевидно, равно Н.О.К. порядков элементов α и e. Поэтому достаточно рассматривать порядки элементов вида $\mu+e$. Обозначим $\beta=\mu+\mu^2$, $e_1=e+\mu$, n_1 – порядок элемента e_1.

Теорема 2. Для того, чтобы степень многочлена $1+t^n$ была крана n_1 необходимо и достаточно, чтобы многочлен $1+t^n$ делился на $1+t+(a+\beta)t^2$.

Доказательство. Действительно, $e_1^2=(e+\mu)^2=e^2+\mu^2=e+a+\mu^2=e+\mu+a+\mu+\mu^2=e_1+a+\beta$. Этим доказательство фактически заканчивается, так как $e_1=e_1+\mu$ является также базисным элементом квадратичного расширения $F(2^{2m})$ и поэтому элемент $\alpha+\beta$ не может быть представлен в виде суммы $x+x^2$ при некотором $x\in F(2^{2m})$, [1]. Однако, это сразу видно и без обращения к [1]. Если допустить, что $\alpha+\beta=x+x^2$, то так как $\beta=\mu+\mu^2$ получим $\alpha=(x+\mu)+(x+\mu)^2$, что противоречит выбору α. Поэтому к элементу e_1 применима теорема 1 ■

Следствие 2. Порядок элемента e_1 равен наименьшей степени многочленов вида $(1+t^n)$ кратных $1+t+(a+\beta)t^2$.

Теорема 1 допускает эквивалентную формулировку в терминах рассматриваемых выше рекуррентных последовательностей.

Теорема 3. Пусть задана рекуррентная последовательность $c_{k+1}=c_k+ac_{k-1}$ с начальными условиями $c_0=c_1=\mathbf{1}$. Тогда порядок n_0 базисного элемента e, $e^2=e+a$ квадратичного расширения поля $F(2^m)$ есть такое наименьшее число, при котором $c_{n_0-3}=\frac{1}{a^2}$, $c_{n_0-2}=\frac{1}{a}$.

Доказательство. Рассмотрим многочлен в котором коэффициенты образуют рекурренту с начальными условиями $c_0=c_1=\mathbf{1}$ и $c_{n_0-3}=\frac{1}{a^2}$, $c_{n_0-2}=\frac{1}{a}$ и при этом в этой последовательности нет коэффициентов с наименьшим порядком k, для которых $c_k=\frac{1}{a^2}$, $c_{k+1}=\frac{1}{a}$. Определим многочлен $\varphi(t)=c_0+c_1t+\cdots+c_{n_0-3}t^{n_0-3}+c_{n_0-2}t^{n_0-2}$. Тогда произведя умножение $\varphi(t)(1+t+at^2)$ получим многочлен $1+t^{n_0}$. Согласно теореме 1, n_0 кратен порядку e. С другой стороны, если искать многочлен $\varphi(t)$ удовлетворяющий условию $\varphi(t)(1+t+at^2)=1+t^{n_0}$, то он однозначно определит свойства указанных коэффициентов. ■

Список использованных источников

[1] Максимов, В. М. Об усложнении дискретного логарифмирования в полях характеристики 2 / В. М. Максимов, Э. А. Применко // International Journal of Open Information Technologies. – 2018. – Т. 6, № 11. – С. 16-20. – URL: https://www.elibrary.ru/item.asp?id=36379613 (дата обращения: 13.08.2020). – Рез. англ.

[2] Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: Научное издательство ТВПЛ, 2001.

[3] Максимов, В. М. Статистический подход к задаче дискретного логарифмирования / В. М. Максимов, Э. А. Применко, А. В. Борисов // Международный гуманитарный научный форум «Гуманитарные чтения РГГУ-2019 «Непрерывность и разрывы: «Социальногуманитарные измерения». – М.: Янус-К, 2019. – С. 38-42. – URL: https://www.elibrary.ru/item.asp?id=39235884 (дата обращения: 13.08.2020).

[4] Кузьмин, А. С. Криптографические алгоритмы на группах и алгебрах / А. С. Кузьмин, В. Т. Марков, А. А. Михалев, А. В. Михалев, А. А. Нечаев // Фундаментальная и прикладная математика. – 2015. – Т. 20, № 1. – С. 205-222. – URL: https://www.elibrary.ru/item.asp?id=25686556 (дата обращения: 13.08.2020). – Рез. англ.

[5] Moldovyan, N. Vector Finite Groups as Primitives for Fast Digital Signature Algorithms / N. Moldovyan, A. Moldovyan. – DOI 10.1007/978-3-642-00304-2_22 // Information Fusion and Geographic Information Systems. Lecture Notes in Geoinformation and Cartography; V. V. Popovich, C. Claramunt, M. Schrenk, K. V. Korolenko (ed.) Springer, Berlin, Heidelberg. – 2009. – Pp. 317-330. – URL: https://link.springer.com/chapter/10.1007%2F978-3-642-00304-2_22 (дата обращения: 13.08.2020).

[6] Adleman, L. M. A Subexponential Algorithm for Discrete Logarithms over All Finite Fields / L. M. Adleman, J. DeMarrais. – DOI 10.1007/3-540-48329-2_13 // Advances in Cryptology — CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science; D. R. Stinson (ed.) Springer, Berlin, Heidelberg. – 1994. – Vol. 773. – Pp. 147-158. – URL: https://link.springer.com/chapter/10.1007/3-540-48329-2_13 (дата обращения: 13.08.2020).

[7] Herlestam, T. On computing logarithms over $GF(2^p)$ / T. Herlestam, R. Johannesson. – DOI 10.1007/BF01941467 // BIT Numerical Mathematics. – 1981. – Vol. 21, Issue 3. – Pp. 326-334. – URL: https://link.springer.com/article/10.1007%2FBF01941467 (дата обращения: 13.08.2020).

[8] ElGamal, T. On Computing Logarithms Over Finite Fields / T. ElGamal. – DOI 10.1007/3-540-39799-X_28 // Advances in Cryptology – CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science; H. C. Williams (ed.) Springer, Berlin, Heidelberg. – 1986. – Vol. 218. – Pp. 396-402. – URL: https://link.springer.com/chapter/10.1007/3-540-39799-X_28 (дата обращения: 13.08.2020).

[9] Coppersmith, D. Fast evaluation of logarithms in fields of characteristic two / D. Coppersmith. – DOI 10.1109/TIT.1984.1056941 // IEEE Transactions on Information Theory. – 1984. – Vol. 30, Issue 4. – Pp. 587-594. – URL: https://ieeexplore.ieee.org/abstract/document/1056941 (дата обращения: 13.08.2020).

[10] Thomé, E. Computation of Discrete Logarithms in / E. Thomé. – DOI 10.1007/3-540-45682-1_7 // Advances in Cryptolo-

gy — ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science; C. Boyd (ed.) Springer, Berlin, Heidelberg. – 2001. – Vol. 2248. – Pp. 107-124. – URL: https://link.springer.com/chapter/10.1007%2F3-540-45682-1_7 (дата обращения: 13.08.2020).

[11] Thomé, T. Fast computation of linear generators for matrix sequences and application to the block Wiedemann algorithm / E. Thomé. – DOI 10.1145/384101.384145 // Proceedings of the 2001 international symposium on Symbolic and algebraic computation (ISSAC '01). – Association for Computing Machinery, New York, NY, USA, 2001. – Pp. 323-331. – URL: https://dl.acm.org/doi/10.1145/384101.384145 (дата обращения: 13.08.2020).

[12] Semaev, I. New algorithm for the discrete logarithm problem on elliptic curves / I. Semaev // arXiv:1504.01175. – 2015. – URL: https://arxiv.org/abs/1504.01175 (дата обращения: 13.08.2020).

Поступила 13.08.2020; принята к публикации 10.09.2020; опубликована онлайн 30.09.2020.

Об авторах:

Максимов Валерий Михайлович, заведующий кафедрой фундаментальной и прикладной математики, Институт информационных наук и технологий безопасности, ФГБОУ ВО «Российский государственный гуманитарный университет» (125993, Россия, г. Москва, пл. Миусская, д. 6), доктор физико-математических наук, профессор, ORCID: http://orcid.org/0000-0001-6514-6076, vm_maximov@mail.ru

Ремезова Виктория Ивановна, магистрант факультета физико-математических и естественных наук, ФГАОУ ВО «Российский университет дружбы народов» (117198, Россия, г. Москва, ул. Миклухо-Маклая, д. 6), ORCID: http://orcid.org/0000-0002-8622-6865, remezova.98@mail.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Maksimov V.M., Primenko E.A. The Complication of Discrete Logarithms in Fields of Characteristic 2. *International Journal of Open Information Technologies*. 2018; 6(11):16-20. Available at: https://www.elibrary.ru/item.asp?id=36379613 (accessed 13.08.2020). (In Russ., abstract in Eng.)

[2] Koblitz N. A Course in Number Theory and Cryptography. *Graduate Texts in Mathematics*. 1987; 114. Springer, New York, NY. (In Eng.) DOI: https://doi.org/10.1007/978-1-4684-0310-7

[3] Maksimov V.M., Primenko E.A., Borisov A.V. *Statisticheskij podhod k zadache diskretnogo logarifmirovanija* [Statistical approach to the discrete logarithm problem]. In: Proceeding of the Humanitarian Readings of RSUH. Moscow, Yanus-K; 2019. p. 38-42. Available at: https://www.elibrary.ru/item.asp?id=39235884 (accessed 13.08.2020). (In Russ.)

[4] Kuzmin A.S., Markov V.T., Mikhalev A.A., Mikhalev A.V., Nechaev A.A. Cryptographic Algorithms on Groups and Algebras. *Fundamentalnaya i Prikladnaya Matematika* = Fundamental and Applied Mathematics. 2015; 20(1):205-222. Available at: https://www.elibrary.ru/item.asp?id=25686556 (accessed 13.08.2020). (In Russ., abstract in Eng.)

[5] Moldovyan N., Moldovyan A. Vector Finite Groups as Primitives for Fast Digital Signature Algorithms. In: Popovich V.V., Claramunt C., Schrenk M., Korolenko K.V. (ed.) Information Fusion and Geographic Information Systems. *Lecture Notes in Geoinformation and Cartography*. Springer, Berlin, Heidelberg; 2009. p. 317-330. (In Eng.) DOI: https://doi.org/10.1007/978-3-642-00304-2_22

[6] Adleman L.M., DeMarrais J. A Subexponential Algorithm for Discrete Logarithms over All Finite Fields. In: Stinson D.R. (ed.) Advances in Cryptology – CRYPTO' 93. CRYPTO 1993. *Lecture Notes in Computer Science*. 1994; 773:147-158. Springer, Berlin, Heidelberg. (In Eng.) DOI: https://doi.org/10.1007/3-540-48329-2_13

[7] Herlestam T., Johannesson R. On computing logarithms over $GF(2^p)$. *BIT Numerical Mathematics*. 1981; 21(3):326-334. (In Eng.) DOI: https://doi.org/10.1007/BF01941467

[8] ElGamal T. On Computing Logarithms Over Finite Fields. In: Williams H.C. (ed.) Advances in Cryptology – CRYPTO '85 Proceedings. CRYPTO 1985. *Lecture Notes in Computer Science*. 1986; 218: 396-402. Springer, Berlin, Heidelberg. (In Eng.) DOI: https://doi.org/10.1007/3-540-39799-X_28

[9] Coppersmith D. Fast evaluation of logarithms in fields of characteristic two. *IEEE Transactions on Information Theory*. 1984; 30(4):587-594. (In Eng.) DOI: https://doi.org/10.1109/TIT.1984.1056941

[10] Thomé E. Computation of Discrete Logarithms in . In: Boyd C. (ed.) Advances in Cryptology – ASIACRYPT 2001. ASIACRYPT 2001. *Lecture Notes in Computer Science*. 2001; 2248:107-124. (In Eng.) DOI: https://doi.org/10.1007/3-540-45682-1_7

[11] Thomé E. Fast computation of linear generators for matrix sequences and application to the block Wiedemann algorithm. In: *Proceedings of the 2001 international symposium on Symbolic and algebraic computation (ISSAC '01)*. Association for Computing Machinery, New York, NY, USA; 2001. p. 323-331. (In Eng.) DOI: https://doi.org/10.1145/384101.384145

[12] Semaev I. New algorithm for the discrete logarithm problem on elliptic curves. *arXiv*: 1504.01175. 2015. Available at: https://arxiv.org/abs/1504.01175 (accessed 13.08.2020). (In Eng.)

Submitted 13.08.2020; revised 10.09.2020; published online 30.09.2020.

About the authors:

Valery M. Maximov, Head of the Department of Fundamental and Applied Mathematics, Institute of Information Sciences and Security Technologies, Russian State University for the Humanities (6 Miusskaya Sq., Moscow 125993, GSP-3, Russia), Dr.Sci. (Phys.-Math.), Professor, ORCID: http://orcid.org/0000-0001-6514-6076, vm_maximov@mail.ru

Victoria I. Remezova, Undergraduate Student of the Faculty of Science, Peoples' Friendship University of Russia (6 Miklukho-Maklaya St., Moscow 117198, Russia), ORCID: http://orcid.org/0000-0002-8622-6865, remezova.98@mail.ru

All authors have read and approved the final manuscript.