S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 16, стр. 144–144 (2019) УДК 519.719.2;
517.965
DOI 10.33048/semi.2019.16.xxx MSC 94A60;
11Bxx

СУЩЕСТВОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, УДОВЛЕТВОРЯЮЩИХ РЕКУРРЕНТНЫМ СООТНОШЕНИЯМ БИЛИНЕЙНОГО ТИПА

А.А. Илларионов

Abstract. We study sequences $\{A_n\}_{n=-\infty}^{+\infty}$ of elements of a field $\mathbb{F}$ that satisfy decompositions of the form

$$A_{m+n}A_{m-n} = a_1(m)b_1(n) + a_2(m)b_2(n),$$
$$A_{m+n+1}A_{m-n} = \tilde{a}_1(m)\tilde{b}_1(n) + \tilde{a}_2(m)\tilde{b}_2(n),$$

where $a_1, a_2, b_1, b_2 : \mathbb{Z} \to \mathbb{F}$. We obtained some results concerning with existence and uniqueness of such sequences. The results are used to construct analogues of the ElGamal encryption system and Diffie–Hellman key exchange. The discrete logarithm problem is posed in the group $(S, +)$, where the set S consists of fours $S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$, $n \in \mathbb{Z}$, and $S(n) + S(m) = S(n + m)$.
Keywords: nonlinear recurrence sequences, Somos sequences, asymmetric cryptography, public-key cryptography

1. Введение

Пусть $\mathbb{F}$ — некоторое поле. Рассмотрим последовательность $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$, удовлетворяющую условиям: существуют целые неотрицательные N_0, N_1 и последовательности $a_i, b_i, \tilde{a}_j, \tilde{b}_j : \mathbb{Z} \to \mathbb{F}$, $i = 1, \ldots, N_0$, $j = 1, \ldots, N_1$ такие, что

Illarionov A.A., Existence of sequences satisfying recurrent relations of bilinear typ.

Работа поддержана РНФ (грант N 19-11-00065).
Поступила .

для всех $n, m \in \mathbb{Z}$ выполнены разложения

$$A_{n+m}A_{n-m} = \sum_{i=1}^{N_0} a_i(n)b_i(m), \tag{1}$$

$$A_{n+m+1}A_{n-m} = \sum_{i=1}^{N_0} \tilde{a}_i(n)\tilde{b}_i(m). \tag{2}$$

Эта конструкция была предложена В.А. Быковским [1] при $\mathbb{F} = \mathbb{C}$. В этом случае, она тесно связана (см. [2]) с решениями функционального уравнения

$$f(x+y)f(x-y) = \sum_{j=1}^{N} \phi_j(x)\psi_j(y),$$

возникающего в теории эллиптических функций и полилинейных функционально-дифференциальных уравнений.

Последовательности вида (1), (2) также связаны с последовательностями Сомоса (см. [2]), которые обладают рядом замечательных свойств и изучались многими авторами (см. [7, 8, 9, 4, 10, 5, 11, 12, 6, 13] и ссылки там).

В [2] описаны все последовательности A комплексных чисел, удовлетворяющих разложниями (1), (2) при $N_0 + N_1 \leq 4$.

Если поле $\mathbb{F}$ конечно, то последовательности вида (1), (2) могут быть использованы для построения криптосистем с открытым ключом (см. § 4). Однако открытым является вопрос о существовании таких последовательностей в произвольном поле. Этот пробел частично восполняется в настоящей заметке. В § 3 мы получаем результаты о существовании последовательностей A произвольного поля $\mathbb{F}$, удовлетворяющих разложениями (1), (2) при $N_0, N_1 \leq 2$ и в § 4 используем эти факты для построения асимметричных шифров (аналогов алгоритмов Диффи-Хеллмана и Эль-Гамаля).

Ниже всюду считаем, что $\mathbb{F}$ — поле с операциями сложения $+$ и умножения $\cdot$. Нейтральные элементы по сложению и умножению обозначаем 0 и 1. Если $a, b \in \mathbb{F}$, то (как обычно) $a/b = ab^{-1}$, где b^{-1} — обратный (по умножению) элемент к b.

2. Некоторые свойства

Пусть $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$. Пишем $R_j(A) = N_j$, $j = 0, 1$, если N_0, N_1 — наименьшие неотрицательные целые для которых существуют последовательности $a_i, b_i, \tilde{a}_j, \tilde{b}_j : \mathbb{Z} \to \mathbb{F}$, $i = 1, \ldots, N_0$, $j = 1, \ldots, N_1$, удовлетворяющие разложениям (1), (2) для всех $n, m \in \mathbb{Z}$.

Используя определение нетрудно проверить следующие свойства.

1. Пусть $B_n = A_{n_0+n}$ (или $B_n = A_{n_0-n}$). Тогда $R_j(A) \leq 2$, $j = 0, 1$, если и только если $R_j(B) \leq 2$, $j = 0, 1$.
2. Если $a, b, c \in \mathbb{F} \setminus \{0\}$ и $B_n = A_n a^{n^2} b^n c$, то $R_j(B) = R_j(A)$, $j = 0, 1$.

Для любой последовательности $A \subset \mathbb{F}$ и целых n_j, m_j определим

$$D_A\begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = \det\begin{pmatrix} A_{m_0+n_0}A_{m_0-n_0} & \dots & A_{m_0+n_k}A_{m_0-n_k} \\ \vdots & & \vdots \\ A_{m_k+n_0}A_{m_k-n_0} & \dots & A_{m_k+n_k}A_{m_k-n_k} \end{pmatrix},$$

$$\tilde{D}_A\begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = \det\begin{pmatrix} A_{m_0+n_0+1}A_{m_0-n_0} & \dots & A_{m_0+n_k+1}A_{m_0-n_k} \\ \vdots & & \vdots \\ A_{m_k+n_0+1}A_{m_k-n_0} & \dots & A_{m_k+n_k+1}A_{m_k-n_k} \end{pmatrix}.$$

Лемма 1. *Пусть $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ и $k \in \mathbb{Z}_+ = \mathbb{Z} \cap [0, +\infty)$.*

1. *Неравенство $R_0(A) \le k$ эквивалентно тому, что*
$$D_A\begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = 0 \quad \text{для всех } m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}.$$
2. *Неравенство $R_1(A) \le k$ эквивалентно тому, что*
$$\tilde{D}_A\begin{pmatrix} m_0 & \dots & m_k \\ n_0 & \dots & n_k \end{pmatrix} = 0 \quad \text{для всех } m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}.$$

Лемма 2. *Пусть $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ и $R_0(A) \le 2$, причем $A_0 = 0$, $A_1A_2A_3 \ne 0$. Тогда последовательность A однозначно определяется своими членами с номерами ± 1 и $2, 3, 4$. Кроме того, если $A_{-1} = 0$, то $A_n = 0$ при всех $n \notin \{1, 2, 3, 4\}$.*

Эти леммы доказаны в [2, леммы 5.1, 6.1] при $\mathbb{F} = \mathbb{C}$. Однако приведенные там доказательства остается верными и в случае произвольного поля. Поэтому мы их опускаем.

3. Существование последовательностей с $R_j(A) \le 2$

Пусть $\alpha_0, \alpha_1 \dots, \alpha_5 \in \mathbb{F}$ и $n_0 \in \mathbb{Z}$. В этом разделе мы рассматриваем следующий вопрос: при каких условиях на α_j существует единственная последовательность $A : \mathbb{Z} \to \mathbb{F}$, удовлетворяющая начальным условиям

$$A_{n_0+j} = \alpha_j, \quad j = 0, 1, \dots, 5,$$

для которой $R_i(A) \le 2$, $i = 0, 1$. Согласно свойству 1 из § 2 выбор n_0 не важен. Кроме того, мы ограничимся случаем, когда среди начальных данных $\alpha_0, \dots, \alpha_5$ есть не более одного нуля.

3.1. **Случай, когда среди начальных данных есть ровно один нуль.** Основной результат этого пункта заключается в следующем.

Теорема 1. *Пусть $\alpha, \beta, \gamma \in \mathbb{F}$, причем $\alpha\beta \ne 0$. Существует единственная последовательность $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ такая, что*

$$A_{-1} = -\alpha, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma; \tag{3}$$

$$R_0(A) \le 2, \quad R_1(A) \le 2. \tag{4}$$

Более того, для всех $n, k \in \mathbb{Z}$

$$A_{-n} = -\alpha^n A_n, \tag{5}$$

$$A_{n+k}A_{n-k} = \alpha^{k-1}\left(A_k^2 A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2\right), \tag{6}$$

$$A_{n+k+1}A_{n-k} = \alpha^{k-1}\left(A_kA_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_nA_{n+1}\right). \tag{7}$$

Единственность вытекает из леммы 2. Перейдем к доказательству существования. Если A удовлетворяет (3), (4), то согласно лемме 1

$$D_A\begin{pmatrix} n & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-2} & A_{n+1}A_{n-1} & A_n^2 \\ -\alpha\beta & 0 & 1 \\ A_{-2} & -\alpha & 0 \end{vmatrix} = \\ = \alpha A_{n+2}A_{n-2} + A_{-2}A_{n+1}A_{n-1} + \beta\alpha^2 A_n^2 = 0.$$

Исходя из (5), положим $A_{-2} = -\alpha^2$. Следовательно, наша последовательность должна удовлетворять соотношению (уравнение Сомос-4)

$$A_{n+2}A_{n-2} = \alpha A_{n+1}A_{n-1} - \alpha\beta A_n^2. \tag{8}$$

Так как последовательность A содержит нулевые члены, то ее нельзя однозначно восстановить используя только уравнение (8). Прежде всего, нам нужна дополнительная информация о расположении нулевых членов.

Лемма 3. *Пусть последовательность $A = \{A_n\}_{n=-1}^{+\infty} \subset \mathbb{F}$ удовлетворяет начальным условиям* (3) *и уравнению* (8) *для всех $n \in \mathbb{N}$ таких, что $A_{n-2} \neq 0$. Тогда*

a) *если $n_1, n_2 \in \mathbb{N}$, причем $A_{n_1} = A_{n_2} = 0$, то $|n_1 - n_2| \geq 4$;*
b) *уравнение* (8) *выполняется для всех $n \in \mathbb{N}$.*

Доказательство. 1. Докажем, что последовательность A не имеет двух соседних членов, равных нулю. Предположим противное. Пусть m — наименьший номер такой, что $A_m = A_{m+1} = 0$. Тогда $m \geq 4$ и $A_{m-1} \neq 0$.

Докажем, что $A_{m-3} \neq 0$. Если $A_{m-4} = 0$, то это следует из выбора m. Если $A_{m-4} \neq 0$, то уравнение (8) выполнено при $n = m-2$, то есть $0 = \alpha A_{m-1}A_{m-3} - \alpha\beta A_{m-2}^2$. Поэтому $A_{m-3} = 0 \Longrightarrow A_{m-2} = 0$. Значит, $A_{m-3} \neq 0$ согласно выбору номера m.

Так как $A_{m-3} \neq 0$, то уравнение (8) выполнено при $n = m-1$. Но тогда $0 = -\alpha\beta A_{m-1}^2$, то есть $A_{m-1} = 0$. Пришли к противоречию.

2. Предположим, что утверждение a) не верно. Тогда найдется номер m такой, что

$$A_m = 0, \quad A_{m+1}A_{m+2}A_{m+3} = 0.$$

Пусть m — наименьший номер, удовлетворяющий этим свойствам. Тогда

$$m \geq 4, \quad A_{m-3}A_{m-2}A_{m-1} \neq 0.$$

Кроме того, $A_{m+1} \neq 0$ согласно доказанному выше. Так как $A_{m-1}A_{m-2} \neq 0$, то (8) верно при $n = m+1$ и $n = m$, то есть

$$A_{m+3}A_{m-1} = -\alpha\beta A_{m+1}^2 \neq 0 \quad \Longrightarrow \quad A_{m+3} \neq 0,$$
$$A_{m+2}A_{m-2} = \alpha A_{m+1}A_{m-1} \neq 0 \quad \Longrightarrow \quad A_{m+2} \neq 0.$$

Пришли к противоречию. Значит, свойство a) выполняется.

3. Предположим, что утверждение b) не верно. Тогда найдется номер m такой, что

$$A_{m-2} = 0, \quad \underbrace{A_{m+2}A_{m-2}}_{0} \neq \alpha A_{m+1}A_{m-1} - \alpha\beta A_m^2.$$

Пусть m — наименьший номер, удовлетворяющий этим условиям. Тогда $m \geq 6$ и уравнение (8) выполнено для всех $1 \leq n < m$. Выбирая в нем $n = m-4, m-3, m-2, m-1$, получаем четыре равенства

$$\beta A_{m-4}^2 = A_{m-3}A_{m-5}, \quad A_{m-1}A_{m-5} = -\alpha\beta A_{m-3}^2,$$
$$\alpha A_{m-1}A_{m-3} = A_m A_{m-4}, \quad A_{m+1}A_{m-3} = -\alpha\beta A_{m-1}^2.$$

Следовательно, (перемножаем равенства, причем третье из них берем два раза)

$$\beta A_{m-4}^2 A_{m-1}A_{m-5}(\alpha A_{m-1}A_{m-3})^2 A_{m+1}A_{m-3} =$$
$$= A_{m-3}A_{m-5}(-\alpha\beta A_{m-3}^2)(A_m A_{m-4})^2(-\alpha\beta A_{m-1}^2).$$

Так как $A_{m-5}A_{m-4}A_{m-3}A_{m-1}A_m A_{m+1} \neq 0$ согласно утверждению а), то отсюда следует, что $\alpha A_{m+1}A_{m-1} = \alpha\beta A_m^2$. Так как $A_{m-2} = 0$, то уравнение (8) выполняется и при $n = m$. □

Построим теперь последовательность A. Элементы с номерами от -1 до 4 определим с помощью (3). Элементы с номерами $n \geq 5$ вычислим по формулам

$$A_{n+2} = \alpha\frac{A_{n+1}A_{n-1} - \beta A_n^2}{A_{n-2}} \quad \text{при } n \geq 3, \quad A_{n-2} \neq 0, \tag{9}$$

$$A_{n+2} = -\alpha\gamma\frac{A_n A_{n-1}}{A_{n-3}} \quad \text{при } n \geq 3, \quad A_{n-2} = 0. \tag{10}$$

Если $A_{n-2} = A_{n-3} = 0$, то полагаем $A_{n+2} = 0$. Однако нетрудно заметить, что полученная последовательность удовлетворяет условиям леммы 3. Поэтому случай $A_{n-2} = A_{n-3} = 0$ невозможен. Отметим, что формула (10) получена из равенства

$$\tilde{D}_A\begin{pmatrix} n-1 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = 0.$$

Элементы $A_{-2}, A_{-3}, \ldots$ определим по формуле

$$A_{-n} = -\alpha^n A_n \quad \text{при } n \geq 2. \tag{11}$$

Осталось проверить, что построенная последовательность A удовлетворяет уравнениям (6), (7) (неравенства (4) вытекают из (6), (7) по определению величин $R_j(A)$).

Лемма 4. *Пусть последовательность $A \subset \mathbb{F}$ определяется соотношениями* (3), (9), (10), (11). *Тогда уравнения* (6), (7) *выполнены при $k = 2$. Кроме того,*

$$\forall n \in \mathbb{Z} \qquad \beta(\alpha A_n^3 + A_{n-1}^2 A_{n+2} + A_{n+1}^2 A_{n-2}) = (\alpha+\gamma)A_{n-1}A_n A_{n+1}. \tag{12}$$

Доказательство. 1. Докажем, что (6) выполнено при $k = 2$, то есть справедливо равенство (8). Из (9) и леммы 3 следует выполнение (8) при $n \geq 1$. Используя этот факт, условия (3) и (11), нетрудно проверить, что (8) имеет место и для $n \leq 0$.

2. Докажем, что (7) выполнено при $k = 2$, то есть

$$A_{n+3}A_{n-2} = \alpha\beta A_{n+2}A_{n-1} - \alpha\gamma A_{n+1}A_n. \tag{13}$$

2.1. Используя метод математической индукции, докажем (13) при $n \geq -3$. *База индукции* вытекает из (3) и (11).

Шаг индукции от $(n-1)$ к n. Если $A_{n-1}=0$, то (13) вытекает из (10), в котором n заменяем на $n+1$. Пусть $A_{n-1}\neq 0$. Тогда (13) равносильно соотношению

$$A_{n+3}A_{n-1}A_{n-2}=\alpha\beta A_{n+2}A_{n-1}^2-\alpha\gamma A_{n+1}A_nA_{n-1}.$$

Согласно (8) левая часть этого соотношения равна $\alpha A_{n+2}A_nA_{n-2}-\alpha\beta A_{n+1}^2A_{n-2}$. Значит, (13) эквивалентно равенству

$$A_{n+2}(A_nA_{n-2}-\beta A_{n-1}^2)=A_{n+1}(\beta A_{n+1}A_{n-2}-\gamma A_{n-1}A_n).$$

Так как $\beta A_{n+1}A_{n-2}-\gamma A_{n-1}A_n=\alpha^{-1}A_{n+2}A_{n-3}$ (по предположению индукции), то это равенство равносильно тому, что

$$A_{n+2}(A_{n+1}A_{n-3}-\alpha A_nA_{n-2}+\alpha\beta A_{n-2}^2)=0.$$

Последнее соотношение выполнено в силу (8).

2.2. Выполнение (13) при $n<-3$ легко проверяется с помощью начальных условий (3), свойства (11) и утверждения из п. 2.1.

3. Осталось проверить свойство (12). Дважды применяя (8), получаем, что

$$\begin{aligned}A_{n+3}A_{n-2}A_{n-1}=(A_{n+3}A_{n-1})A_{n-2}&=\alpha(A_{n+2}A_nA_{n-2}-\beta A_{n+1}^2A_{n-2})=\\&=\alpha\left((\alpha A_{n+1}A_{n-1}-\alpha\beta A_n^2)A_n-\beta A_{n+1}^2A_{n-2}\right).\end{aligned}$$

С другой стороны, в силу (13)

$$A_{n+3}A_{n-2}A_{n-1}=(\alpha\beta A_{n+2}A_{n-1}-\alpha\gamma A_{n+1}A_n)A_{n-1}.$$

Следовательно,

$$(\alpha A_{n+1}A_{n-1}-\alpha\beta A_n^2)A_n-\beta A_{n+1}^2A_{n-2}=\beta A_{n+2}A_{n-1}^2-\gamma A_{n+1}A_nA_{n-1}.$$

Нетрудно заметить, что это равенство равносильно (12). □

Замечание. Если последовательность A не имеет нулевых членов, то можно ввести новую последовательность $\tau_n=(A_{n-1}A_{n+1})/A_n^2$. В этих терминах (12) принимает вид

$$\beta(\alpha+\tau_n^2\tau_{n+1}+\tau_n^2\tau_{n-1})=(\alpha+\gamma)\tau_n.$$

Это соотношение хорошо известно в теории последовательностей Сомос-4 (см., например, [15] и ссылки там).

Доказательство теоремы 1. Единственность искомой последовательности следует из леммы 2. Пусть A — последовательность из леммы 4. Осталось доказать, что она удовлетворяет условиям (6), (7). Действительно, неравенства (4) являются следствиями (по определению) из (6), (7), а условие (5) — из (11). Согласно (5) уравнения (6), (7) достаточно проверить только при $k\geq 0$. Для этого используем индукцию по k.

База индукции. Согласно начальным условиям (3) и свойству (5) соотношения (6), (7) выполнены при $k=0,1$. Из леммы 4 вытекает, что они также верны при $k=2$.

Шаг индукции от k к $(k+1)$.

1. Докажем, что выполнено равенство (6), в котором k заменяем на $k+1$, то есть

$$A_{n+k+1}A_{n-k-1}=\alpha^k(A_{k+1}^2A_{n+1}A_{n-1}-A_{k+2}A_kA_n^2). \tag{14}$$

1.1. Пусть $A_{n+k}A_{n-k}\neq 0$. Тогда (14) равносильно соотношению

$$A_{n+k+1}A_{n-k-1}A_{n+k}A_{n-k}=\alpha^k(A_{k+1}^2A_{n+1}A_{n-1}-A_{k+2}A_kA_n^2)A_{n+k}A_{n-k}. \tag{15}$$

Согласно предположению индукции (7) левая часть этого соотношения равна

$$A_{n+k+1}A_{n-k-1}A_{n+k}A_{n-k} = (A_{n+k+1}A_{n-k})(A_{n+k}A_{n-k-1}) = \\ = \alpha^{2k-2}\left(A_kA_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_nA_{n+1}\right)\times \\ \times\left(A_kA_{k+1}A_{n+1}A_{n-2} - A_{k+2}A_{k-1}A_{n-1}A_n\right),$$

а в силу (6) правая часть равна

$$\alpha^{2k-1}(A_{k+1}^2A_{n+1}A_{n-1} - A_{k+2}A_kA_n^2)(A_k^2A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2)$$

Поэтому (15) можно переписать в следующем эквивалентном виде (раскрываем скобки в левой и правой части)

$$A_k^2A_{k+1}^2A_{n-2}A_{n-1}A_{n+1}A_{n+2} - A_{k-1}A_kA_{k+1}A_{k+2}A_nA_{n-1}^2A_{n+2} - \\ - A_{k-1}A_kA_{k+1}A_{k+2}A_{n-2}A_nA_{n+1}^2 + A_{k-1}^2A_{k+2}^2A_{n-1}A_n^2A_{n+1} = \\ = \alpha(A_k^2A_{k+1}^2A_{n+1}^2A_{n-1}^2 - A_{k-1}A_{k+1}^3A_{n-1}A_n^2A_{n+1} - A_k^3A_{k+2}A_{n-1}A_n^2A_{n+1} + \\ + A_{k-1}A_kA_{k+1}A_{k+2}A_n^4)$$

Согласно (8) разность первых слагаемых в левой и правой части равна

$$A_k^2A_{k+1}^2A_{n-1}A_{n+1}(A_{n+2}A_{n-2} - \alpha A_{n+1}A_{n-1}) = -\alpha\beta A_k^2A_{k+1}^2A_{n-1}A_n^2A_{n+1}.$$

поэтому требуемое равенство равносильно равносильно тому, что

$$A_{n-1}A_n^2A_{n+1}\left(-\alpha\beta A_k^2A_{k+1}^2 + A_{k-1}^2A_{k+2}^2 + \alpha A_{k-1}A_{k+1}^3 + \alpha A_k^3A_{k+2}\right) = \\ = A_{k-1}A_kA_{k+1}A_{k+2}A_n\left(A_{n-1}^2A_{n+2} + A_{n-2}A_{n+1}^2 + \alpha A_n^3\right).$$

Учитывая, что согласно (8)

$$-\alpha\beta A_k^2A_{k+1}^2 + \alpha A_{k-1}A_{k+1}^3 = A_{k+1}^2(\alpha A_{k-1}A_{k+1} - \alpha\beta A_k^2) = A_{k+1}^2A_{k+2}A_{k-2},$$

перепишем последнее соотношение в эквивалентном виде:

$$A_{n-1}A_n^2A_{n+1}A_{k+2}(A_{k+1}^2A_{k-2} + A_{k-1}^2A_{k+2}^2 + \alpha A_k^3A_{k+2}) = \\ = A_{k-1}A_kA_{k+1}A_{k+2}A_n\left(A_{n-1}^2A_{n+2} + A_{n-2}A_{n+1}^2 + \alpha A_n^3\right).$$

Оно выполняется в силу (12). Случай $A_{n+k}A_{n-k} \neq 0$ полностью рассмотрен.

1.2. Пусть $A_{n+k-1}A_{n-k+1} \neq 0$. Умножая (14) на $A_{n+k-1}A_{n-k+1}$ и учитывая, что по предположению индукции

$$A_{n+k-1}A_{n-k+1} = A_{n+(k-1)}A_{n-(k-1)} = \alpha^{k-2}\left(A_{k-1}^2A_{n+1}A_{n-1} - A_kA_{k-2}A_n^2\right),$$
$$A_{n+k+1}A_{n-k+1} = A_{(n+1)+k}A_{(n+1)-k} = \alpha^{k-1}\left(A_k^2A_{n+2}A_n - A_{k+1}A_{k-1}A_{n+1}^2\right),$$
$$A_{n+k-1}A_{n-k-1} = A_{(n-1)+k}A_{(n-1)-k} = \alpha^{k-1}\left(A_k^2A_nA_{n-2} - A_{k+1}A_{k-1}A_{n-1}^2\right),$$

приходим к выводу, что (14) эквивалентно равенству

$$\left(A_k^2A_{n+2}A_n - A_{k+1}A_{k-1}A_{n+1}^2\right)\left(A_k^2A_nA_{n-2} - A_{k+1}A_{k-1}A_{n-1}^2\right) = \\ = (A_{k+1}^2A_{n+1}A_{n-1} - A_{k+2}A_kA_n^2)\left(A_{k-1}^2A_{n+1}A_{n-1} - A_kA_{k-2}A_n^2\right).$$

Последнее после раскрытия скобок и сокращения одинаковых слагаемых принимает вид

$$A_k^4A_{n+2}A_{n-2}A_n^2 - A_{k-1}A_k^2A_{k+1}A_n(A_{n-1}^2A_{n+2} + A_{n-2}A_{n+1}^2) = \\ = -A_{n-1}A_n^2A_{n+1}A_k(A_{k-2}A_{k+1}^2 + A_{k-1}^2A_{k+2}) + A_{k-2}A_k^2A_{k+2}A_n^4$$

Подставляя в это равенство соотношения (применили (8))

$$\begin{aligned} A_k^4 A_{n+2} A_{n-2} A_n^2 &= \alpha A_k^4 A_{n-1} A_n^2 A_{n+1} - \alpha\beta A_k^4 A_n^4, \\ A_{k-2} A_k^2 A_{k+2} A_n^4 &= \alpha A_{k-1} A_k^2 A_{k+1} A_n^4 - \alpha\beta A_k^4 A_n^4, \end{aligned}$$

перепишем его в виде

$$\begin{aligned} &\alpha A_k^4 A_{n-1} A_n^2 A_{n+1} - A_{k-1} A_k^2 A_{k+1} A_n (A_{n-1}^2 A_{n+2} + A_{n-2} A_{n+1}^2) = \\ &\qquad = -A_{n-1} A_n^2 A_{n+1} A_k (A_{k-2} A_{k+1}^2 + A_{k-1}^2 A_{k+2}) + \alpha A_{k-1} A_k^2 A_{k+1} A_n^4 \end{aligned}$$

или

$$\begin{aligned} &A_{n-1} A_n^2 A_{n+1} A_k (\alpha A_k^3 + A_{k-2} A_{k+1}^2 + A_{k-1}^2 A_{k+2}) = \\ &\qquad = A_{k-1} A_k^2 A_{k+1} A_n (A_{n-1}^2 A_{n+2} + A_{n-2} A_{n+1}^2 + \alpha A_n^3). \end{aligned}$$

Это равенство выполнено в силу (12)

1.3. Осталось рассмотреть случай, когда $A_{n+k} A_{n-k} = A_{n+k-1} A_{n-k+1} = 0$. Так как последовательность A не может иметь двух соседних нулевых членов, то тогда $A_{n+k} A_{n-k+1} \neq 0$ или $A_{n+k-1} A_{n-k} \neq 0$. Эти два случая рассматриваются также как и предыдущие. В первом случае равенство (14) нужно домножить на $A_{n+k} A_{n-k+1}$, а во втором — на $A_{n+k-1} A_{n-k}$. После этого остается применить предположение индукции, элементарные преобразования и формулу (12).

2. Докажем выполнение формулы (7), в которой k заменяем на $k+1$, то есть

$$A_{n+k+2} A_{n-k-1} = \alpha^k \left(A_{k+1} A_{k+2} A_{n+2} A_{n-1} - A_{k+3} A_k A_n A_{n+1} \right). \tag{16}$$

2.1 Пусть $A_{n+k+1} A_{n-k} \neq 0$. Умножая (16) на $A_{n+k+1} A_{n-k}$ и учитывая, что по предположению индукции и формуле (14)

$$\begin{aligned} A_{n+k+1} A_{n-k} &= \alpha^{k-1} \left(A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1} \right), \\ A_{n+k+2} A_{n-k} &= A_{(n+1)+(k+1)} A_{(n+1)-(k+1)} = \alpha^k \left(A_{k+1}^2 A_{n+2} A_n - A_{k+2} A_k A_{n+1}^2 \right), \\ A_{n+k+1} A_{n-k-1} &= A_{n+(k+1)} A_{n-(k+1)} = \alpha^k \left(A_{k+1}^2 A_{n+1} A_{n-1} - A_{k+2} A_k A_n^2 \right), \end{aligned}$$

приходим к выводу, что (16) эквивалентно равенству

$$\begin{aligned} &\alpha \left(A_{k+1}^2 A_{n+2} A_n - A_{k+2} A_k A_{n+1}^2 \right) \left(A_{k+1}^2 A_{n+1} A_{n-1} - A_{k+2} A_k A_n^2 \right) = \\ &= \left(A_{k+1} A_{k+2} A_{n+2} A_{n-1} - A_{k+3} A_k A_n A_{n+1} \right) \left(A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1} \right). \end{aligned}$$

Последнее после раскрытия скобок и элементарных преобразований, принимает вид

$$\begin{aligned} &A_{k+1} A_{n-1} A_n A_{n+1} A_{n+2} \left(\alpha A_{k+1}^3 + A_{k-1} A_{k+2}^2 + A_k^2 A_{k+3} \right) + \\ &+ \alpha A_k^2 A_{k+2}^2 A_n^2 A_{n+1}^2 = A_k A_{k+1}^2 A_{k+2} \left(\alpha A_n^3 A_{n+2} + \alpha A_{n-1} A_{n+1}^3 + A_{n-1}^2 A_{n+2}^2 \right) + \\ &\qquad + A_{k-1} A_k A_{k+2} A_{k+3} A_n^2 A_{n+1}^2. \end{aligned} \tag{17}$$

Разность последних слагаемых в правой и левой части этого равенства равна

$$A_k A_{k+2} A_n^2 A_{n+1}^2 (A_{k+3} A_{k-1} - \alpha A_k A_{k+2}) = -\alpha\beta A_k A_{k+1}^2 A_{k+2} A_n^2 A_{n+1}^2.$$

Поэтому (17) равносильно соотношению

$$\begin{aligned} &A_{k+1} A_{n-1} A_n A_{n+1} A_{n+2} \left(\alpha A_{k+1}^3 + A_{k-1} A_{k+2}^2 + A_k^2 A_{k+3} \right) = \\ &\qquad = A_k A_{k+1}^2 A_{k+2} \left(\alpha A_n^3 A_{n+2} + \alpha A_{n-1} A_{n+1}^3 + A_{n-1}^2 A_{n+2}^2 - \alpha\beta A_n^2 A_{n+1}^2 \right). \end{aligned}$$

Последнее выполнено в силу (12) и равенства

$$\alpha A_n^3 A_{n+2} - \alpha\beta A_n^2 A_{n+1}^2 = A_n^2(\alpha A_n A_{n+2} - \alpha\beta A_{n+1}^2) = A_n^2 A_{n+3} A_{n-1}.$$

2.2. Пусть $A_{n+k+1}A_{n-k} = 0$. Поскольку последовательность A не имеет двух соседних членов равных нулю, хотя бы одно из произведений $A_{n+k}A_{n-k}$, $A_{n+k}A_{n-k+1}$ или $A_{n+k+1}A_{n-k+1}$ отлично от нуля. Эти случаи рассматриваются аналогично исследованным выше. □

Замечание. Если A — последовательность из теоремы 1, то $R_0(A) = R_1(A) = 2$. Действительно, из начальных условий вытекает, что

$$D_A\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix} = \begin{vmatrix}0 & 1\\ -\alpha & 0\end{vmatrix} = \alpha \neq 0, \quad \tilde{D}_A\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix} = \begin{vmatrix}0 & 1\\ -\alpha & 0\end{vmatrix} = \alpha \neq 0.$$

Отсюда по лемме 1 следует, что $R_j(A) \geq 2$, $j = 0, 1$. Значит, $R_0(A) = R_1(A) = 2$.

Следствие 1. *Пусть $\alpha_{-1}, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F} \setminus \{0\}$, $\alpha_4 \in \mathbb{F}$. Тогда существует единственная последовательность $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ такая, что*

$$A_j = \alpha_j, \ \ j = \pm 1, 2, 3, 4, \quad A_0 = 0; \qquad R_j(A) \leq 2, \ \ j = 0, 1.$$

Более того, для всех $n \in \mathbb{Z}$ справедливы равенства

$$A_{-n} = -\left(-\alpha_{-1}\alpha_1^{-1}\right)^n A_n,$$

$$-\frac{\alpha_{-1}\alpha_2^2}{\alpha_1^3}A_n^3 + A_{n-1}^2 A_{n+2} + A_{n+1}^2 A_{n-2} = \left(-\frac{\alpha_{-1}\alpha_2^4}{\alpha_1^4\alpha_3} + \frac{\alpha_4\alpha_1}{\alpha_2\alpha_3}\right) A_{n-1}A_nA_{n+1}.$$

Доказательство. Сделаем замену: $B_n = A_n\alpha_1^{-1}(\alpha_1/\alpha_2)^{n-1}$. Как отмечалось в § 2 $R_j(B) = R_j(A) \leq 2$. Кроме того,

$$B_{-1} = \frac{\alpha_{-1}\alpha_2^2}{\alpha_1^3}, \quad B_0 = 0, \quad B_1 = B_2 = 1, \quad B_3 = \frac{\alpha_1\alpha_3}{\alpha_2^2}, \quad B_4 = \frac{\alpha_4\alpha_1^2}{\alpha_2^3}.$$

Согласно теореме 1 такая последовательность B существует и единственна, причем $B_n = -(-B_{-1})^n B_n$ и выполняется равенство (12), в котором $\alpha = -B_{-1}$, $\beta = B_3$, $\gamma = B_4$ и A_n заменено на B_n. Отсюда вытекают оставшиеся утверждения леммы.

□

Следствие 2. *Пусть последовательность $A = \{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ такая, что $R_0(A) \leq 2$ и $A_0 = 0$, $A_{-1}A_1A_2A_3 \neq 0$. Тогда $R_1(A) \leq 2$.*

Доказательство. Согласно следствию 1 существует последовательность B такая, что $R_j(B) \leq 2$, $j = 0, 1$ и $B_i = A_i$, $-1 \leq i \leq 4$. Используя лемму 2, получаем, что $A = B$. □

Через $|F|$ обозначаем мощность множества F.

Лемма 5. *Пусть, в дополнение к условиям следствия 1, поле $\mathbb{F}$ конечно. Тогда последовательность A имеет период ω, причем $\omega \leq |\mathbb{F}|^4$ и ω делится на порядок элемента $\alpha = -\alpha_{-1}\alpha_1^{-1}$.*

Доказательство. Используя замену из доказательства следствия 1, нетрудно заметить, что последовательность A удовлетворяет уравнениям вида (8), (12). Из них вытекает, что существуют функции $f_+, f_- : \mathbb{F}^4 \to \mathbb{F}$ такие, что

$$A_n = f_+(A_{n-1}, A_{n-2}, A_{n-3}, A_{n-4}), \quad A_n = f_-(A_{n+1}, A_{n+2}, A_{n+3}, A_{n+4}).$$

Так как множество $\mathbb{F}$ конечно, то отсюда следует, что последовательность A имеет период $\omega \le |\mathbb{F}|^4$. Используя этот факт и формулу $A_{-n} = -\alpha^n A_n$, где $\alpha = -\alpha_{-1}\alpha_1^{-1}$, получаем, что

$$A_{-n-\omega} = -\alpha^{n+\omega}A_{n+\omega} = -\alpha^{n+\omega}A_n = \alpha^\omega A_{-n} = \alpha^\omega A_{-n-\omega} \quad \Longrightarrow \quad \alpha^\omega = 1.$$

□

Рассмотрим теперь другие варианты, когда среди начальных данных есть ровно один нуль. В силу следствия 1 и свойства 1 из § 2, достаточно рассмотреть только два варианта:

$$A_0 = 0, \quad A_j = \alpha_j,\ j = 1, \dots, 5; \tag{18}$$

$$A_{-2} = \alpha_{-2}, \quad A_{-1} = \alpha_{-1}, \quad A_0 = 0, \quad A_j = \alpha_j,\ j = 1, 2, 3. \tag{19}$$

Следствие 3. *Пусть $\alpha_j \in \mathbb{F}\setminus\{0\}$, $j = 1, \dots, 5$. Последовательность $A : \mathbb{Z} \to \mathbb{F}$, удовлетворяющая* (4), (18)*, существует тогда и только тогда, когда $\alpha_4\alpha_2^3 \ne \alpha_1\alpha_3^3$. Если такая последовательность существует, то она единственна.*

Доказательство. Если искомая последовательность существует, то

$$D_A\begin{pmatrix}3 & 2 & 1\\ 2 & 1 & 0\end{pmatrix} = \begin{vmatrix}\alpha_5\alpha_1 & \alpha_4\alpha_2 & \alpha_3^2\\ 0 & \alpha_3\alpha_1 & \alpha_2^2\\ \alpha_3 A_{-1} & 0 & \alpha_1^2\end{vmatrix} = \alpha_5\alpha_3\alpha_1^4 + \alpha_3 A_{-1}\Delta = 0.$$

где $\Delta = \alpha_4\alpha_2^3 - \alpha_1\alpha_3^3$. Очевидно, что $\Delta \ne 0$. Тогда $A_{-1} = \alpha_{-1}$, где $\alpha_{-1} = -\alpha_1^2\alpha_5\alpha_1^2\Delta^{-1}$. Согласно следствию 1 существует единственная последовательность $\tilde{A}$ такая, что

$$R_i(\tilde{A}) \le 2,\ i = 1, 2; \quad \tilde{A}_j = \alpha_j,\ j = \pm 1, 2, 3, 4, \quad \tilde{A}_0 = 0.$$

Нетрудно проверить, что $\tilde{A}_5 = \alpha_5$. Значит, $\tilde{A} = A$ — искомая последовательность. □

Следствие 4. *Пусть $\alpha_j \in \mathbb{F} \setminus \{0\}$, $j = \pm 1, \pm 2, \pm 3$. Если $\alpha_{-2}\alpha_1 \ne \alpha_2\alpha_{-1}^2$, то не существует последовательности $A : \mathbb{Z} \to \mathbb{F}$, удовлетворяющей* (4), (19)*. Если $\alpha_{-2}\alpha_1 = \alpha_2\alpha_{-1}^2$, то для любого $\alpha_4 \in \mathbb{F}$ существует единственная последовательность $A : \mathbb{Z} \to \mathbb{F}$, удовлетворяющая* (4), (19) *и дополнительному условию $A_4 = \alpha_4$.*

Доказательство. Так как

$$D_A\begin{pmatrix}2 & 1 & 0\\ 2 & 1 & 0\end{pmatrix} = \begin{vmatrix}0 & \alpha_3\alpha_1 & \alpha_2^2\\ \alpha_3\alpha_{-1} & 0 & \alpha_1^2\\ \alpha_2\alpha_{-2} & \alpha_1\alpha_{-1} & 0\end{vmatrix} = \alpha_1\alpha_2\alpha_3(\alpha_1^2\alpha_{-2} + \alpha_{-1}^2\alpha_2) = 0,$$

то условие $\alpha_1^2\alpha_{-2} + \alpha_{-1}^2\alpha_2 = 0$ необходимо для существования искомой последовательности.

Возьмем любой $\alpha_4 \in \mathbb{F}$. Согласно следствию 1 существует единственная последовательность $\tilde{A}$ такая, что

$$R_i(\tilde{A}) \le 2,\ i = 1, 2; \quad \tilde{A}_j = \alpha_j,\ j = \pm 1, 2, 3, 4, \quad \tilde{A}_0 = 0.$$

Если, дополнительно, $\alpha_1^2\alpha_{-2} + \alpha_{-1}^2\alpha_2 = 0$, то нетрудно проверить, что $\tilde{A}_{-2} = \alpha_{-2}$. Значит, $\tilde{A} = A$ — искомая последовательность. □

3.2. **Случай, когда среди начальных данных нет нулей.** Пусть $a, b, T \in \mathbb{F}$; $ab \neq 0$. Определим расширение $\mathbb{F}(\sqrt{a})$ поля $\mathbb{F}$ следующим образом: если $\sqrt{a} \in \mathbb{F}$ (т.е. уравнение $x^2 = a$ разрешимо в $\mathbb{F}$), то полагаем $\mathbb{F}(\sqrt{a}) = \mathbb{F}$; в противном случае

$$\mathbb{F}(\sqrt{a}) = \{x + y\sqrt{a} : x, y \in \mathbb{F}\}$$

с операциями сложения и умножения определяемыми естественным образом. Другими словами, $\mathbb{F}(\sqrt{a})$ состоит из пар $(x, y) \in \mathbb{F}^2$ и

$$(x_1, y_1)\cdot(x_2, y_2) = (x_1x_2 + ay_1y_2, x_1y_2 + x_2y_1), \quad (x_1, y_1)+(x_2, y_2) = (x_1+x_2, y_1+y_2).$$

Нулем является $(0, 0)$, а единицей — $(1, 0)$. Отображение $x \in \mathbb{F} \to (x, 0) \in \mathbb{F}(\sqrt{a})$ задает вложение $\mathbb{F} \subset \mathbb{F}(\sqrt{a})$.

Согласно следствию 1 существует единственная последовательность $W : \mathbb{Z} \to \mathbb{F}(\sqrt{a})$ такая, что

(20) $W_{-1} = -1,\ W_0 = 0,\ W_1 = 1,\ W_2 = -\sqrt{a},\ W_3 = -b,\ W_4 = \sqrt{a}(a^2 + Tb)$;

(21) $W_{-n} = -W_n; \quad R_i(W) \leq 2,\ i = 0, 1.$

Используя эти соотношения и равенства

$$D_W \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = 0, \quad \tilde{D}_W \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = 0,$$

нетрудно проверить, что для всех $n, k \in \mathbb{Z}$

$$W_{n+k}W_{n-k} = W_k^2W_{n+1}W_{n-1} - W_{k+1}W_{k-1}W_n^2, \tag{22}$$

$$-\sqrt{a}W_{n+k+1}W_{n-k} = W_kW_{k+1}W_{n+2}W_{n-1} - W_{k+2}W_{k-1}W_{n+1}W_n. \tag{23}$$

Замечание. В случае $\mathbb{F} = \mathbb{C}$ последовательность W изучена в [3]. При $\mathbb{F} = \mathbb{Q}$ ее называют эллиптической (делимостной) последовательностью.

Лемма 6. *Для любого $n \in \mathbb{Z}$ верно, что $W_{2n+1} \in \mathbb{F}$, $\sqrt{a}W_{2n} \in \mathbb{F}$.*

Доказательство. Выбирая в (22), (23) $k = n - 1$, имеем

$$W_{2n-1} = W_{n-1}^3W_{n+1} - W_n^3W_{n-2}, \quad -\sqrt{a}W_{2n} = W_{n-1}^2W_nW_{n+2} - W_{n-2}W_nW_{n+1}^2.$$

Используя эти соотношение и начальные условия (20), нетрудно проверить требуемое утверждение, используя индукцию по $n = 1, 2, \ldots$ □

Лемма 7. *Пусть последовательность $A : \mathbb{Z} \to \mathbb{F}$ не содержит нулевых членов и удовлетворяет для любых $n \in \mathbb{Z}$ соотношению*

$$A_{n+2}A_{n-2} = aA_{n+1}A_{n-1} + bA_n^2. \tag{24}$$

Последовательность $W : \mathbb{Z} \to \mathbb{F}(\sqrt{a})$ удовлетворяет условиям (20), (21), *где*

$$T = \frac{A_1^2A_{-2} + A_{-1}^2A_2 + aA_0^3}{A_{-1}A_0A_1}.$$

Тогда для всех $k, n \in \mathbb{Z}$

$$A_{n+k}A_{n-k} = W_k^2A_{n+1}A_{n-1} - W_{k-1}W_{k+1}A_n^2, \tag{25}$$

$$A_{n+k+1}A_{n-k} = -\frac{W_{k+1}W_k}{\sqrt{a}}A_{n+2}A_{n-1} + \frac{W_{k+2}W_{k-1}}{\sqrt{a}}A_{n+1}A_n. \tag{26}$$

Доказательство. Так как $k \not\equiv k+1 \pmod 2$ и $k+2 \not\equiv k-1 \pmod 2$, то в силу леммы 6

$$\frac{W_{k+1}W_k}{\sqrt{a}} \in \mathbb{F}, \quad \frac{W_{k+2}W_{k-1}}{\sqrt{a}} \in \mathbb{F}.$$

Соотношение (22) при $k = 2$ принимает вид

$$W_{n+2}W_{n-2} = aW_{n+1}W_{n-1} + bW_n^2. \tag{27}$$

1. Положим $f_n = A_{n-1}A_{n+1}A_n^{-2}$. Тогда согласно (24)

$$f_{n-1}f_n^2f_{n+1} = af_n + b.$$

Отсюда вытекает, что величина $f_n(f_{n-1} + f_{n+1}) + a/f_n$ не зависит от n. Доказательство этого факта, приведенное в [15, лемма 2.1] остается в силе в случае произвольного поля. Поэтому мы его повторять не будем. Возвращаясь к последовательности A, получаем, что элемент

$$\frac{A_{n+1}^2A_{n-2} + A_{n-1}^2A_{n+2} + aA_n^3}{A_{n-1}A_nA_{n+1}}$$

не зависит от n. Следовательно, для всех $n \in \mathbb{Z}$

$$A_{n+1}^2A_{n-2} + A_{n-1}^2A_{n+2} + aA_n^3 = TA_{n-1}A_nA_{n+1}. \tag{28}$$

Из следствия 1 и начальных условий (20) вытекает, что последовательность W удовлетворяет аналогичному уравнению

$$W_{n+1}^2W_{n-2} + W_{n-1}^2W_{n+2} + aW_n^3 = TW_{n-1}W_nW_{n+1}. \tag{29}$$

2. Докажем соотношения (25). В силу свойства (21) их достаточно проверить при $k \geq 0$. Для этого используем индукцию по $k = 0, 1, \ldots$

База индукции. Согласно (20) соотношения (25) выполняются при $k = 0, 1, 2$.

Шаг индукции от k к $k+1$ ($k \geq 2$). Нужно доказать, что

$$A_{n+k+1}A_{n-k-1} = W_{k+1}^2A_{n+1}A_{n-1} - W_kW_{k+2}A_n^2. \tag{30}$$

Умножим (30) на $A_{n+k-1}A_{n-k+1}$ и учтем, что по предположению индукции

$$\begin{aligned}
A_{n+k-1}A_{n-k+1} &= A_{n+(k-1)}A_{n-(k-1)} = W_{k-1}^2A_{n+1}A_{n-1} - W_{k-2}W_kA_n^2,\\
A_{n+k-1}A_{n-k-1} &= A_{(n-1)+k}A_{(n-1)-k} = W_k^2A_nA_{n-2} - W_{k-1}W_{k+1}A_{n-1}^2,\\
A_{n+k+1}A_{n-k+1} &= A_{(n+1)+k}A_{(n+1)-k} = W_k^2A_nA_{n+2} - W_{k-1}W_{k+1}A_{n+1}^2.
\end{aligned}$$

В итоге, приходим к эквивалентному равенству

$$\begin{aligned}
&\left(W_k^2A_nA_{n-2} - W_{k-1}W_{k+1}A_{n-1}^2\right)\left(W_k^2A_nA_{n+2} - W_{k-1}W_{k+1}A_{n+1}^2\right) =\\
&\quad = \left(W_{k+1}^2A_{n+1}A_{n-1} - W_kW_{k+2}A_n^2\right)\left(W_{k-1}^2A_{n+1}A_{n-1} - W_{k-2}W_kA_n^2\right)
\end{aligned}$$

Раскрывая скобки и сокращая одинаковые слагаемые, имеем

$$\begin{aligned}
&W_k^4A_{n-2}A_n^2A_{n+2} + A_{n-1}A_n^2A_{n+1}W_k(W_{k+1}^2W_{k-2} + W_{k-1}^2W_k) =\\
&\quad = W_k^2W_{k+2}W_{k-2}A_n^4 + W_{k-1}W_k^2W_{k+1}A_n(A_{n+2}A_{n-1}^2 + A_{n-2}A_{n+1}^2)
\end{aligned} \tag{31}$$

Согласно (24) и (27) первые слагаемые в обеих частях последнего равенства можно записать как

$$\begin{aligned}
W_k^4A_{n-2}A_n^2A_{n+2} &= aW_k^4A_n^2A_{n+1}A_{n-1} + bW_k^4A_n^4,\\
W_k^2W_{k+2}W_{k-2}A_n^4 &= aW_k^2A_n^4W_{k+1}W_{k-1} + bW_k^4A_n^4.
\end{aligned}$$

Поэтому (31) равносильно тому, что

$$A_{n-1}A_n^2A_{n+1}W_k(aW_k^3+W_{k+1}^2W_{k-2}+W_{k-1}^2W_k)= \\ =W_{k-1}W_k^2W_{k+1}A_n(aA_n^3+A_{n+2}A_{n-1}^2+A_{n-2}A_{n+1}^2).$$

Это равенство выполняется согласно (28), (29). Соотношения (25) доказаны.

3. Докажем равенства (26). В силу (21) их достаточно проверить при $k\geq 0$. Для этого используем индукцию по $k=0,1,\ldots$

База индукции. Согласно (20) уравнения (26) выполняются при $k=0,1$.

Шаг индукции от k к $k+1$ ($k\geq 1$). Нужно доказать, что

$$A_{n+k+2}A_{n-k-1}=-a^{-1/2}W_{k+2}W_{k+1}A_{n+2}A_{n-1}+a^{-1/2}W_{k+3}W_kA_{n+1}A_n. \tag{32}$$

Умножим (32) на $aA_{n+k+1}A_{n-k}$, учтем (26) и то, что согласно (25)

$$A_{n+k+2}A_{n-k}=A_{(n+1)+(k+1)}A_{(n+1)-(k+1)}=W_{k+1}^2A_{n+2}A_n-W_kW_{k+2}A_{n+1}^2,$$
$$A_{n+k+1}A_{n-k-1}=A_{n+(k+1)}A_{n-(k+1)}=W_{k+1}^2A_{n+1}A_{n-1}-W_kW_{k+2}A_n^2.$$

В итоге, получаем эквивалентное соотношение

$$a\left(W_{k+1}^2A_{n+2}A_n-W_kW_{k+2}A_{n+1}^2\right)\left(W_{k+1}^2A_{n+1}A_{n-1}-W_kW_{k+2}A_n^2\right)= \\ =\left(W_{k+2}W_{k+1}A_{n+2}A_{n-1}-W_{k+3}W_kA_{n+1}A_n\right)\times \\ \times\left(W_{k+1}W_kA_{n+2}A_{n-1}-W_{k+2}W_{k-1}A_{n+1}A_n\right),$$

которое после раскрытия скобок и элементарных преобразований принимает вид

$$A_{n-1}A_nA_{n+1}A_{n+2}W_{k+1}\left(aW_{k+1}^3+W_k^2W_{k+3}+W_{k-1}W_{k+2}^2\right)= \\ =W_kW_{k+1}^2W_{k+2}\left(aA_{n+1}^3A_{n-1}+aA_{n+2}A_n^3+A_{n-1}^2A_{n+2}^2\right)+ \\ +A_{n+1}^2A_n^2W_kW_{k+2}\left(W_{k-1}W_{k+3}-aW_kW_{k+2}\right). \tag{33}$$

Учитывая, что

$$W_{k-1}W_{k+3}-aW_kW_{k+2}=bW_{k+1}^2,$$
$$aA_{n+1}^3A_{n-1}+bA_{n+1}^2A_n^2=A_{n+1}^2(aA_{n+1}A_{n-1}+bA_n^2)=A_{n+1}^2A_{n+2}A_{n-2},$$

нетрудно заметить, что (33) равносильно равенству

$$A_{n-1}A_nA_{n+1}A_{n+2}W_{k+1}\left(aW_{k+1}^3+W_k^2W_{k+3}+W_{k-1}W_{k+2}^2\right)= \\ =W_kW_{k+1}^2W_{k+2}A_{n+2}\left(aA_n^3+A_{n-1}^2A_{n+2}+A_{n+1}^2A_{n-2}\right).$$

Последнее выполнено в силу (28), (29). Равенства (26) доказаны. □

Теорема 2. *Пусть $\alpha_j\in\mathbb{F}\setminus\{0\}$, $j=-2,-1,\ldots,3$, причем $\Delta_1\neq 0$, где*

$$\Delta_1=\begin{vmatrix}\alpha_2\alpha_0 & \alpha_1^2\\ \alpha_1\alpha_{-1} & \alpha_0^2\end{vmatrix}=\alpha_2\alpha_0^3-\alpha_{-1}\alpha_1^3.$$

Тогда существует единственная последовательность $A:\mathbb{Z}\to\mathbb{F}$, удовлетворяющая (4) и начальным условиям

$$A_j=\alpha_j,\quad -2\leq j\leq 3. \tag{34}$$

Доказательство. Искомая последовательность A должна удовлетворяет равенству

$$D_A\begin{pmatrix} n & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-2} & A_{n+1}A_{n-1} & A_n^2 \\ \alpha_3\alpha_{-1} & \alpha_2\alpha_0 & \alpha_1^2 \\ \alpha_2\alpha_{-2} & \alpha_1\alpha_{-1} & \alpha_0^2 \end{vmatrix} = \\ = \Delta_1 A_{n+2}A_{n-2} - \Delta_2 A_{n+1}A_{n-1} + \Delta_3 A_n^2 = 0,$$

где $\Delta_1, \Delta_2, \Delta_3$ — соответствующие миноры второго порядка. Так как $\Delta_1 \neq 0$, то выполняется уравнение (24), в котором $a = \Delta_2/\Delta_1$, $b = -\Delta_3/\Delta_1$. Отметим, что a и b не могут одновременно обращаться в ноль (иначе $A_{n+2}A_{n-2} = 0$, а это противоречит начальным условиям (34)). Поэтому возможны три случая.

1. Пусть $a = 0$, то есть $A_{n+2}A_{n-2} = bA_n^2$. Тогда

$$b = \frac{\alpha_2\alpha_{-2}}{\alpha_0^2}, \quad \alpha_3\alpha_{-1}\alpha_0^2 = \alpha_1^2\alpha_2\alpha_{-2} \text{ (так как } \Delta_2 = 0).$$

Положим

$$A_{2k} = \alpha_0\left(\frac{\alpha_0}{\alpha_{-2}}\right)^k\left(\frac{\alpha_2\alpha_{-2}}{\alpha_0^2}\right)^{k(k+1)/2},$$
$$A_{2k+1} = \alpha_1\left(\frac{\alpha_1}{\alpha_{-1}}\right)^k\left(\frac{\alpha_3\alpha_{-1}}{\alpha_1^2}\right)^{k(k+1)/2}.$$

Тогда $A_{n+2}A_{n-2} = bA_n^2$ и выполняются начальные условия (25). Нетрудно также проверить, что выполняются (1), (2) с $N_0 = N_1 = 2$.

2. Пусть $b = 0$, то есть $A_{n+2}A_{n-2} = aA_{n+1}A_{n-1}$. Тогда

$$a = \frac{\alpha_2\alpha_{-2}}{\alpha_1\alpha_{-1}}, \quad \alpha_3\alpha_{-1}^2\alpha_1 = \alpha_2^2\alpha_{-2}\alpha_0.$$

Положим

$$A_n = \left(\frac{\alpha_2\alpha_{-2}}{\alpha_1\alpha_{-1}}\right)^{n(n-1)/6}\left(\frac{\alpha_2}{\alpha_{-1}}\right)^{n/3} f_n, \quad f_n = \begin{cases} \alpha_0, & n \equiv 0 \pmod 3, \\ \alpha_1\alpha_{-1}^{1/3}\alpha_2^{-1/3}, & n \equiv 1 \pmod 3, \\ \alpha_1^{1/3}\alpha_{-1}\alpha_{-2}^{-1/3}, & n \equiv 2 \pmod 3. \end{cases}$$

Последовательность A_n определена «формально», но корректно (если отдельно рассмотреть случаи, когда $n \equiv 0, 1, 2 \pmod 3$, то в каждом из них все степени, входящие в определение A_n, оказываются целыми). Кроме того, $A_{n+2}A_{n-2} = aA_{n+1}A_{n-1}$ и выполняются начальные условия (34). Нетрудно также проверить, что выполняются разложения (1), (2), где $N_0 = N_1 = 2$.

3. Пусть $ab \neq 0$. Начнем вычислять элементы последовательности A по формулам

$$A_{n+2} = \frac{aA_{n+1}A_{n-1} + bA_n^2}{A_{n-2}} \quad \text{при } n \geq 2,$$
$$A_{n-2} = \frac{aA_{n+1}A_{n-1} + bA_n^2}{A_{n+2}} \quad \text{при } n \leq -1.$$

Возможны два варианта.

3.1. Все полученные члены оказались ненулевыми. Тогда A — последовательность без нулей, удовлетворяющая (24). Согласно лемме 7 выполняются (25), (26). Поэтому $R_j(A) \leq 2$, $j = 0, 1$.

3.2. Существует номер m такой, что $A_m = 0$. Не умаляя общности, рассмотрим случай, когда $m > 0$. Пусть m — наименьшее натуральное такое, что $A_m = 0$. Тогда $m \geq 4$ и $A_n \neq 0$ при $-2 \leq n \leq m-1$. Элемент A_{m+1} найдем из соотношения

$$A_{m+1}A_{m-3} = aA_mA_{m-2} + bA_{m-1}^2 \quad \Longrightarrow \quad A_{m+1} = \frac{bA_{m-1}^2}{A_{m-3}}.$$

Ясно, что $A_{m+1} \neq 0$. Рассмотрим последовательность $B_n = A_{m-n}$. Тогда

$$B_{-1} = A_{m+1}, \quad B_0 = 0, \quad B_j = A_{m-j} \text{ при } j = 1, 2, 3, 4.$$

Согласно следствию 1 существует ровно одна последовательность B, удовлетворяющая указанным выше начальным условиям, такая, что $R_j(B) \leq 2$, $j = 0, 1$. Положим теперь $\tilde{A}_n = B_{m-n}$. Тогда

$$\tilde{A}_n = A_n \text{ при } m-4 \leq n \leq m+1; \quad R_j(\tilde{A}) \leq 2,\ j = 0, 1. \tag{35}$$

Докажем, что $\tilde{A}_n = A_n$ при $-2 \leq n \leq m+1$. Так как $R_0(\tilde{A}) \leq 2$, то выполняется разложение вида (1). Выбирая в нем $m = 0, 1, 2$, получаем три соотношения левые части которых линейно зависимы над $\mathbb{F}$. Поэтому существует тройка $(\tilde{\Delta}_1, \tilde{\Delta}_2, \tilde{\Delta}_3) \in \mathbb{F}^3 \setminus \{0\}$ такая, что

$$\tilde{\Delta}_1\tilde{A}_{n+2}\tilde{A}_{n-2} = \tilde{\Delta}_2\tilde{A}_{n+1}A_{n-1} + \tilde{\Delta}_3\tilde{A}_n^2.$$

Выбирая в последнем соотношении $n = m-1$ и $n = m-2$, учитывая (35), имеем

$$\tilde{\Delta}_1A_{m+1}A_{m-3} = \tilde{\Delta}_3A_{m-1}^2, \quad \tilde{\Delta}_2A_{m-1}A_{m-3} + \tilde{\Delta}_3A_{m-2}^2 = 0.$$

Сравнивая эти соотношения с (24), в котором $n = m-1$ и $n = m-2$, приходим к выводу, что $a = \tilde{\Delta}_2/\tilde{\Delta}_1$, $b = \tilde{\Delta}_3/\tilde{\Delta}_1$, то есть $\tilde{A}$ удовлетворяет уравнению (24). Поэтому $\tilde{A}_n = A_n$ при $-2 \leq n \leq m+1$. Значит, $\tilde{A}$ — искомая последовательность. □

4. Построение асимметричных криптосистем

Всюду в этом разделе считаем, что A — последовательность из теоремы 1, причем $\alpha = 1$. Тогда последовательность A — нечетная, то есть $A_{-n} = -A_n$.

Через S обозначаем последовательность, состоящую из четверок

$$S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2}), \quad n \in \mathbb{Z}.$$

4.1. **Алгоритм «быстрого» вычисления четверок $S(n)$.** Полагая в (6), (7), $n = m + k$, получаем формулы

$$A_{m+2k} = A_m^{-1}\left(A_k^2A_{m+k+1}A_{m+k-1} - A_{k+1}A_{k-1}A_{m+k}^2\right), \tag{36}$$

$$A_{m+2k+1} = A_m^{-1}\left(A_kA_{k+1}A_{m+k+2}A_{m+k-1} - A_{k+2}A_{k-1}A_{m+k}A_{m+k+1}\right), \tag{37}$$

Лемма 8. *Зная начальные данные $(\beta, \gamma, \mathbb{F})$, четверки $S(n)$, $S(l)$, $S(n+l)$ и номер l (номер n неизвестен) можно вычислить четверку $S(n+2l)$, используя $O(1)$ элементарных операций в поле $\mathbb{F}$.*

Доказательство. Не умаляя общности, можно считать, что $l \in \mathbb{N}$. Если $l = 1$, то доказательство тривиально (достаточно использовать формулы (9), (10)).

Пусть $l > 1$. Нам известны члены последовательности A с номерами

$$n-1,\ n,\ n+1,\ n+2;\ l-1,\ l,\ l+1,\ l+2;\ n+l-1,\ n+l,\ n+l+1,\ n+l+2.$$

Нужно найти члены с номерами $n+2l-1$, $n+2l$, $n+2l+1$, $n+2l+2$. Вычислим A_{l-2}, используя (6) (или (7) при $A_{l+2}=0$) в котором $k=2$, $n=l$.

1. Пусть $A_n \neq 0$. Тогда элементы A_{n+2l}, A_{n+2l+2} находятся из (36), в котором $m=n$ и $k=l, l+1$, а элементы $A_{n+2l\pm1}$ — из (37), в котором $m=n$ и $k=l-1, l$.

2. Пусть $A_n=0$. Тогда $A_{n\pm1}\neq 0$ согласно лемме 3 а). Используя (9), (10), вычислим A_{l+3}. После этого элементы A_{n+2l+1} и A_{n+2l+2} находим из (36) и (37), в которых $m=n-1$, $k=l+1$, а элементы A_{n+2l-1} и A_{n+2l} — из (36) и (37), в которых $m=n+1$, $k=l-1$. □

С помощью леммы 8 стандартным образом (по аналогии с бинарным алгоритмом возведения в степень), строится алгоритм «быстрого» вычисления $S(n+k)$ при заданных $S(n)$ и k (номер n неизвестен). Пусть $k\in\mathbb{N}$ и

$$k=(\epsilon_{s-1}\dots\epsilon_0)_2=\epsilon_0+2\epsilon_1+\dots+\epsilon_{s-1}2^{s-1}\quad(\epsilon_j\in\{0,1\},\ \epsilon_{s-1}=1)$$

— представление k в двоичной системе исчисления. Сразу отметим, что если конечная последовательность $k_1,\dots,k_s$ определена соотношениями:

$$k_1=1,\quad k_{j+1}=2k_j+\epsilon_{s-j-1},\quad j=1,\dots,s-1,$$

то $k_j=(\epsilon_{s-1}\dots\epsilon_{s-j})_2$ и $k_s=k$ соответственно.

Алгоритм 1.

Данные: поле $\mathbb{F}$, начальные данные β,γ, номер $k\in\mathbb{N}$ и четверка $S(n)$ (номер n неизвестен).

Найти: четверку $S(n+k)$.

Шаг 1. Полагаем $j=1$, $k_1=1$ и вычисляем $S(n+1)$.

Шаг 2. Если $\epsilon_{s-j-1}=0$, то вычисляем

$$k_{j+1}=2k_j,\quad S(k_{j+1})=S(2k_j),\quad S(n+k_{j+1})=S(n+2k_j).$$

Если $\epsilon_{s-j-1}=1$, то вычисляем

$$k_{j+1}=2k_j+1,\quad S(k_{j+1})=S(2k_j+1),\quad S(n+k_{j+1})=S(n+2k_j+1).$$

Шаг 3. Если $j<s-1$, то увеличиваем j на 1 и возвращаемся к шагу 2.

Шаг 4. Полагаем $S(n+k)=S(n+k_{j+1})$. Конец.

Согласно лемме 8 для выполнения шага 2 нужно выполнить $O(1)$ элементарных операций в поле $\mathbb{F}$. Так как $s\le\log_2 k+1$, то из леммы 8 вытекает следующий результат.

Следствие 5. *Сложность алгоритма 1 равна сложности выполнения $O(\ln k)$ элементарных операций в поле $\mathbb{F}$.*

4.2. **Аналог алгоритма Диффи-Хеллмана.** Абоненты B_1, B_2, используя открытый канал связи, выбирают поле $\mathbb{F}$ и начальные данные β,γ. После этого они вырабатывают общий секретный ключ $K\in\mathbb{F}^4$, используя следующий алгоритм.

(1) Абонент B_1 выбирает $k_1\in\mathbb{N}$, вычисляет $S(k_1)$, используя алгоритм 1, и посылает абоненту B_2 сообщение $S(k_1)$ (номер k_1 хранится в секрете).

(2) Абонент B_2 выбирает $k_2\in\mathbb{N}$, вычисляет $S(k_2)$ и посылает абоненту B_1 сообщение $S(k_2)$ (номер k_2 хранится в секрете).

(3) Абонент B_2 (абонент B_1), зная номер k_2 (номер k_1) и четверку $S(k_1)$ (четверку $S(k_2)$), вычисляет $S(k_1+k_2)$, используя алгоритм 1.

Общим секретом является $K = S(k_1 + k_2)$.

Пассивный противник знает четверки $S(k_1)$ и $S(k_2)$. Для того чтобы найти секретный ключ $S(k_1+k_2)$, ему достаточно определить номер k_1 (или номер k_2). Для этого нужно решить задачу определения номера k по заданному элементу $S(k)$. Она представляет собой задачу дискретного логарифмирования в группе $(S, +)$, где $S(n) + S(m) = S(n + m)$.

4.3. **Аналог алгоритма Эль-Гамаля.** Пусть поле $\mathbb{F}$, начальные данные $\beta, \gamma \in \mathbb{F}$ и целое число n — это *общий параметр* всех пользователей. *Секретным ключом абонента* B является некое $k \in \mathbb{N}$, а *открытым ключом* — четверка $S(k)$.

Алгоритм шифрования сообщения $x = x_{-1}x_0x_1x_2 \in \mathbb{F}^4$, отправляемого абоненту B.

(1) Выбираем сеансовый ключ $r \in \mathbb{N}$.
(2) Вычисляем четверки $S(n + r)$ и $S(n + k + r)$. Для этого можно использовать алгоритм 1, так как нам известны номера r, n и четверка $S(k)$.
(3) Если хотя бы один элемент из $A_{n+k+r+j}$, $j = -1, 0, 1, 2$ равен 0, то возвращаемся к шагу 1.
(4) Вычисляем $y = y_{-1}y_0y_1y_2 \in \mathbb{F}^4$ по формулам: $y_j = x_j \cdot A_{n+k+r+j}$, $j = -1, 0, 1, 2$.
(5) Высылаем абоненту B шифртекст $(S(n + r), y)$.

Алгоритм расшифрования шифртекста $(S(n + r), y)$ абонентом B.

(1) Абонент B вычисляет $S(n + k + r)$, используя алгоритм 1 (напомним, что B знает четверку $S(n + r)$ и номер k).
(2) Находит открытый текст $x = x_{-1}x_0x_1x_2$ по формулам $x_j = y_j \cdot A^{-1}_{n+k+r+j}$, $j = -1, 0, 1, 2$.

Корректность алгоритма расшифровки очевидна.

Замечание. Аналогичным образом можно построить алгоритм электронный цифровой подписи (наподобие ГОСТ 34.10-2012 или FIPS-186-4), использующий последовательность из теоремы 1 вместо группы точек на эллиптической кривой.

References

[1] M.O. Avdeeva, V.A. Bykovskii, *Hyperelliptic system of sequences and functions*, Dal'nevost. Mat. Zh., **16**:2 (2016), 115–122 (in russian).
[2] A.A. Illarionov, *Hyperelliptic systems of sequences of rank 4*, Sbornik: Mathematics, **210**:9 (2019), 1259–1287.
[3] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math., **70** (1948), 31–74.
[4] A.N.W. Hone, *Elliptic curves and quadratic reccurence sequences*, Bull. Lond. Math. Soc., **37** (2005), 161–171
[5] A.N.W. Hone, *Sigma function solution of the initial value problem for Somos 5 sequences*, Trans. AMS, **359**:10 (2007), 5019–5034.
[6] Y. Fedorov, A.N. Hone, *Sigma-function solution to the general Somos-6 recurrence via hyperelliptic Prym varieties*, Journal of Integrable Systems, **1**:1 (2016).
[7] R.M. Robinson, *Periodicity of Somos sequences*, Proc. AMS, **116**:3 (1992), 613–619.
[8] R. Shipsey, *Elliptic Divisibility Sequences*, PhD Thesis, L.: Univ. London, 2000.
[9] C.S. Swart, *Elliptic curves and related sequences*, PhD Thesis, L.: Royal Holloway, Univ. London, 2003.
[10] A.J. van der Poorten, C.S. Swart, *Recurrence relations for elliptic sequences: every Somos 4 is a Somos k*, Bull. Lond. Math. Soc., **38**:4 (2006), 546–554.

[11] A.N. Hone, C. Swart, *Integrality and the Laurent phenomenon for Somos 4 and Somos 5 sequences*, Math. Proc. Camb. Philos. Soc., **145**:1 (2008), 65–85.
[12] A.N. Hone, *Analytic solutions and integrability for bilinear recurrences of order six*, Applicable Analysis: An International Journal, **89**:4 (2010), 473–492.
[13] V.A. Bykovskii, A.V. Ustinov, *Somos-4 and elliptic systems of sequences*, Dokl. Math., **94** (2016), 611–614.
[14] S. Fomin, A. Zelevinsky, *The Laurent Phenomenon*, Adv. Appl. Math., **28** (2002), 119–144.
[15] A.V. Ustinov, *An Elementary Approach to the Study of Somos Sequences*, Proc. Steklov Inst. Math. **305** (2019), 305–317

Andrei Illarionov
Institute of Applied Mathematics, Khabarovsk Division,
off. 312, 60 Seryshev Street,
680038, Khabarovsk, Russia
E-mail address: illar_a@list.ru