

Гиперэллиптические последовательности и криптосистемы с открытым ключом

Андрей Илларионов

ХО ИПМ ДВО РАН;

Дальневосточный центр математических исследований

Вторая конференция математических центров
7–11 ноября 2022 г., МГУ, МИАН, г. Москва

Эллиптическая (делимостьная) последовательность $h : \mathbb{Z} \rightarrow \mathbb{Q}$

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \quad (1)$$

M. Ward (1940-e), R. Shipsey (2000), C. Swart (2003), ...

Эллиптическая (делимостьная) последовательность $h : \mathbb{Z} \rightarrow \mathbb{Q}$

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \quad (1)$$

M. Ward (1940-e), R. Shipsey (2000), C. Swart (2003), ...

Последовательность Сомос-4

$$S_{m+4}S_m = \alpha S_{m+3}S_{m+1} + \beta S_{m+2}^2 \quad (2)$$

Эллиптическая (делимостьная) последовательность $h : \mathbb{Z} \rightarrow \mathbb{Q}$

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \quad (1)$$

M. Ward (1940-e), R. Shipsey (2000), C. Swart (2003), ...

Последовательность Сомос-4

$$S_{m+4}S_m = \alpha S_{m+3}S_{m+1} + \beta S_{m+2}^2 \quad (2)$$

Последовательность Сомос- k

$$S_{n+k}S_n = \sum_{j=1}^{[k/2]} \alpha_j S_{n+k-j}S_{n+j} \quad (3)$$

M. Somos (1989), A.N.W. Hone, A.J. van der Poorten, C. Swart, H.W. Braden, V.Z. Enol'skii, Yu.N. Fedorov, S. Fomin, A. Zelevinskii, D. Gale, R. Schroepel, R. Wm. Gosper, ...

Определение (Быковский, 2014)

Пусть $\mathbb{F}$ — поле. Пусть последовательность $\{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ удовлетворяют разложениям

$$A_{m+n}A_{m-n} = \sum_{j=1}^{N_0} a_j(m)b_j(n), \quad (4)$$

$$A_{m+n+1}A_{m-n} = \sum_{j=1}^{N_1} \tilde{a}_j(m)\tilde{b}_j(n) \quad (5)$$

с некоторыми $a_j, b_j, \tilde{a}_j, \tilde{b}_j : \mathbb{Z} \rightarrow \mathbb{F}$ и минимально возможными $N_0, N_1 \in \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$.

Определение (Быковский, 2014)

Пусть $\mathbb{F}$ — поле. Пусть последовательность $\{A_n\}_{n=-\infty}^{+\infty} \subset \mathbb{F}$ удовлетворяют разложениям

$$A_{m+n}A_{m-n} = \sum_{j=1}^{N_0} a_j(m)b_j(n), \quad (4)$$

$$A_{m+n+1}A_{m-n} = \sum_{j=1}^{N_1} \tilde{a}_j(m)\tilde{b}_j(n) \quad (5)$$

с некоторыми $a_j, b_j, \tilde{a}_j, \tilde{b}_j : \mathbb{Z} \rightarrow \mathbb{F}$ и минимально возможными $N_0, N_1 \in \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$. Тогда A будем называть гиперэллиптической последовательностью, а величины $R_0(A) = N_0, \quad R_1(A) = N_1$ — ее рангами.

Примеры

① $A_n = a^n$

Примеры

$$\textcircled{1} \quad A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, \quad A_{n+m+1}A_{n-m} = a^{2n+1}$$

Примеры

① $A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, A_{n+m+1}A_{n-m} = a^{2n+1} \implies$
 $R_0(A) = R_1(A) = 1.$

Примеры

① $A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, A_{n+m+1}A_{n-m} = a^{2n+1} \implies$
 $R_0(A) = R_1(A) = 1.$

② $A_n = a^{n^2} \implies$

Примеры

① $A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, A_{n+m+1}A_{n-m} = a^{2n+1} \implies$
 $R_0(A) = R_1(A) = 1.$

② $A_n = a^{n^2} \implies$

$$A_{n+m}A_{n-m} = a^{(n+m)^2} a^{(n-m)^2} = a^{2n^2} a^{2m^2} \implies R_0(A) = 1.$$

Примеры

① $A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, A_{n+m+1}A_{n-m} = a^{2n+1} \implies$
 $R_0(A) = R_1(A) = 1.$

② $A_n = a^{n^2} \implies$

$$A_{n+m}A_{n-m} = a^{(n+m)^2} a^{(n-m)^2} = a^{2n^2} a^{2m^2} \implies R_0(A) = 1.$$

③ $A_n = a^n + b^n \implies$

Примеры

$$\textcircled{1} \quad A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, \quad A_{n+m+1}A_{n-m} = a^{2n+1} \implies \\ R_0(A) = R_1(A) = 1.$$

$$\textcircled{2} \quad A_n = a^{n^2} \implies$$

$$A_{n+m}A_{n-m} = a^{(n+m)^2} a^{(n-m)^2} = a^{2n^2} a^{2m^2} \implies R_0(A) = 1.$$

$$\textcircled{3} \quad A_n = a^n + b^n \implies$$

$$A_{n+m}A_{n-m} = (a^{n+m} + b^{n+m})(a^{n-m} + b^{n-m}) =$$

Примеры

$$\textcircled{1} \quad A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, \quad A_{n+m+1}A_{n-m} = a^{2n+1} \implies \\ R_0(A) = R_1(A) = 1.$$

$$\textcircled{2} \quad A_n = a^{n^2} \implies$$

$$A_{n+m}A_{n-m} = a^{(n+m)^2} a^{(n-m)^2} = a^{2n^2} a^{2m^2} \implies R_0(A) = 1.$$

$$\textcircled{3} \quad A_n = a^n + b^n \implies$$

$$A_{n+m}A_{n-m} = (a^{n+m} + b^{n+m})(a^{n-m} + b^{n-m}) = \\ = (a^{2n} + b^{2n}) + a^n b^n (a^m b^{-m} + a^{-m} b^m).$$

Примеры

$$\textcircled{1} \quad A_n = a^n \implies A_{n+m}A_{n-m} = a^{2n}, \quad A_{n+m+1}A_{n-m} = a^{2n+1} \implies \\ R_0(A) = R_1(A) = 1.$$

$$\textcircled{2} \quad A_n = a^{n^2} \implies$$

$$A_{n+m}A_{n-m} = a^{(n+m)^2} a^{(n-m)^2} = a^{2n^2} a^{2m^2} \implies R_0(A) = 1.$$

$$\textcircled{3} \quad A_n = a^n + b^n \implies$$

$$A_{n+m}A_{n-m} = (a^{n+m} + b^{n+m})(a^{n-m} + b^{n-m}) = \\ = (a^{2n} + b^{2n}) + a^n b^n (a^m b^{-m} + a^{-m} b^m).$$

$$\textcircled{4} \quad B_n = A_n a^n b^{n^2} \implies R_j(A) = R_j(B).$$

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Пусть $A_n = f(vn + w)$, $n \in \mathbb{Z}$.

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Пусть $A_n = f(vn + w)$, $n \in \mathbb{Z}$.

Тогда A — гиперэллиптическая последовательность.

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Пусть $A_n = f(vn + w)$, $n \in \mathbb{Z}$.

Тогда A — гиперэллиптическая последовательность.

❶ f — многочлен

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Пусть $A_n = f(vn + w)$, $n \in \mathbb{Z}$.

Тогда A — гиперэллиптическая последовательность.

① f — многочлен или тригонометрический многочлен.

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Пусть $A_n = f(vn + w)$, $n \in \mathbb{Z}$.

Тогда A — гиперэллиптическая последовательность.

- ① f — многочлен или тригонометрический многочлен.
- ② $\mathbb{F} = \mathbb{C}$, f — квазимногочлен. Функция f называется квазимногочленом, если $f(z) = P_1(z)e^{\lambda_1 z} + \dots + P_r(z)e^{\lambda_r z}$, где $P_1, \dots, P_r$ — многочлены.

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Пусть $A_n = f(vn + w)$, $n \in \mathbb{Z}$.

Тогда A — гиперэллиптическая последовательность.

- ① f — многочлен или тригонометрический многочлен.
- ② $\mathbb{F} = \mathbb{C}$, f — квазимногочлен. Функция f называется квазимногочленом, если $f(z) = P_1(z)e^{\lambda_1 z} + \dots + P_r(z)e^{\lambda_r z}$, где $P_1, \dots, P_r$ — многочлены.
- ③ $f = \theta$, $f = \sigma$.

Примеры

Пусть $f : F \rightarrow F$, причем

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (6)$$

Пусть $A_n = f(vn + w)$, $n \in \mathbb{Z}$.

Тогда A — гиперэллиптическая последовательность.

- ❶ f — многочлен или тригонометрический многочлен.
- ❷ $\mathbb{F} = \mathbb{C}$, f — квазимногочлен. Функция f называется квазимногочленом, если $f(z) = P_1(z)e^{\lambda_1 z} + \dots + P_r(z)e^{\lambda_r z}$, где $P_1, \dots, P_r$ — многочлены.
- ❸ $f = \theta$, $f = \sigma$.
- ❹ $f = L\theta$, где L — композиция линейных дифференциальных и разностных операторов с квазимногочленами в качестве коэффициентов.

Связь с функциональными уравнениями (при $\mathbb{F} = \mathbb{C}$)

Пусть f — целая 1-периодическая $\mathbb{C} \rightarrow \mathbb{C}$.

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (7)$$

Связь с функциональными уравнениями (при $\mathbb{F} = \mathbb{C}$)

Пусть f — целая 1-периодическая $\mathbb{C} \rightarrow \mathbb{C}$.

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (7)$$

$$f(z) = \sum_{n \in \mathbb{Z}} A_n e^{2\pi i n z}. \quad (8)$$

Связь с функциональными уравнениями (при $\mathbb{F} = \mathbb{C}$)

Пусть f — целая 1-периодическая $\mathbb{C} \rightarrow \mathbb{C}$.

$$f(x+y)f(x-y) = \sum_{j=1}^N \alpha_j(x)\beta_j(y). \quad (7)$$

$$f(z) = \sum_{n \in \mathbb{Z}} A_n e^{2\pi i n z}. \quad (8)$$

Теорема (А.И., М. Романов, 2017)

Целая функция $f : \mathbb{C} \rightarrow \mathbb{C}$ удовлетворяет (7), (8) $\iff$

$$\begin{cases} A_{m+n}A_{m-n} &= \sum_{j=1}^{N_0} a_j(m)b_j(n), \\ A_{m+n+1}A_{m-n} &= \sum_{j=1}^{N_1} \tilde{a}_j(m)\tilde{b}_j(n) \end{cases} \quad (9)$$

причем $N = N_0 + N_1$.

Детерминантные уравнения

Если $A: \mathbb{Z} \rightarrow \mathbb{F}$ и $m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}$, то полагаем

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

Детерминантные уравнения

Если $A: \mathbb{Z} \rightarrow \mathbb{F}$ и $m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}$, то полагаем

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

Лемма

Неравенство $R_0(A) \leq k$

(т.е. разложение $A_{n+m}A_{n-m} = a_1(n)b_1(m) + \dots + a_k(n)b_k(m)$)

эквивалентно тому, что

$$D_A \begin{pmatrix} n_0 & \dots & n_k \\ m_0 & \dots & m_k \end{pmatrix} = 0 \quad \text{для всех } m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}.$$

$$\begin{aligned}\hat{D}_A \begin{pmatrix} n_0 & \dots & n_k \\ m_0 & \dots & m_k \end{pmatrix} &= D_A \begin{pmatrix} n_0 + 1/2 & \dots & n_k + 1/2 \\ m_0 + 1/2 & \dots & m_k + 1/2 \end{pmatrix} = \\ &= \det \begin{pmatrix} A_{n_0+m_0+1} A_{n_0-m_0} & \dots & A_{n_0+m_k+1} A_{n_0-m_k} \\ \vdots & & \vdots \\ A_{n_k+m_0+1} A_{n_k-m_0} & \dots & A_{n_k+m_k+1} A_{n_k-m_k} \end{pmatrix}.\end{aligned}$$

$$\hat{D}_A \begin{pmatrix} n_0 & \dots & n_k \\ m_0 & \dots & m_k \end{pmatrix} = D_A \begin{pmatrix} n_0 + 1/2 & \dots & n_k + 1/2 \\ m_0 + 1/2 & \dots & m_k + 1/2 \end{pmatrix} =$$

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

Лемма

Неравенство $R_1(A) \leq k$

(т.е. разложение $A_{n+m+1} A_{n-m} = \tilde{a}_1(n) \tilde{b}_1(m) + \dots + \tilde{a}_k(n) \tilde{b}_k(m)$)

эквивалентно тому, что

$$\hat{D}_A \begin{pmatrix} n_0 & \dots & n_k \\ m_0 & \dots & m_k \end{pmatrix} = 0 \quad \text{для всех } m_0, \dots, m_k, n_0, \dots, n_k \in \mathbb{Z}.$$

Криптографические приложения

(Richard Schroepel, Hilarie Orman, R. Wm. Gosper;
Kristin E. Lauter, Katherine E. Stange и др.)

Пусть $R_0(A) \leq 2$, $R_1(A) \leq 2$,

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma. \quad (10)$$

(11)

(12)

Криптографические приложения

(Richard Schroepel, Hilarie Orman, R. Wm. Gosper;
Kristin E. Lauter, Katherine E. Stange и др.)

Пусть $R_0(A) \leq 2$, $R_1(A) \leq 2$,

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma. \quad (10)$$

Тогда для всех целых n, k

(11)

(12)

Криптографические приложения

(Richard Schroepel, Hilarie Orman, R. Wm. Gosper;
Kristin E. Lauter, Katherine E. Stange и др.)

Пусть $R_0(A) \leq 2$, $R_1(A) \leq 2$,

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma. \quad (10)$$

Тогда для всех целых n, k

$$D_A \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+k}A_{n-k} & A_{n+1}A_{n-1} & A_n^2 \\ A_{1+k}A_{1-k} & 0 & 1 \\ A_kA_{-k} & -1 & 0 \end{vmatrix} = 0, \quad (11)$$

$$(12)$$

Криптографические приложения

(Richard Schroepel, Hilarie Orman, R. Wm. Gosper;
Kristin E. Lauter, Katherine E. Stange и др.)

Пусть $R_0(A) \leq 2$, $R_1(A) \leq 2$,

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma. \quad (10)$$

Тогда для всех целых n, k

$$D_A \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+k}A_{n-k} & A_{n+1}A_{n-1} & A_n^2 \\ A_{1+k}A_{1-k} & 0 & 1 \\ A_kA_{-k} & -1 & 0 \end{vmatrix} = 0, \quad (11)$$

$$\implies A_{n+k}A_{n-k} = -A_kA_{-k}A_{n+1}A_{n-1} + A_{1+k}A_{1-k}A_n^2 \quad (12)$$

Криптографические приложения

(Richard Schroepel, Hilarie Orman, R. Wm. Gosper;
Kristin E. Lauter, Katherine E. Stange и др.)

Пусть $R_0(A) \leq 2$, $R_1(A) \leq 2$,

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma. \quad (10)$$

Тогда для всех целых n, k

$$D_A \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+k}A_{n-k} & A_{n+1}A_{n-1} & A_n^2 \\ A_{1+k}A_{1-k} & 0 & 1 \\ A_kA_{-k} & -1 & 0 \end{vmatrix} = 0, \quad (11)$$

$$\implies A_{n+k}A_{n-k} = -A_kA_{-k}A_{n+1}A_{n-1} + A_{1+k}A_{1-k}A_n^2 \quad (12)$$

$$\implies A_{-n} = -A_n \text{ (последовательность } A \text{ нечетная)}$$

Криптографические приложения

(Richard Schroepel, Hilarie Orman, R. Wm. Gosper;
Kristin E. Lauter, Katherine E. Stange и др.)

Пусть $R_0(A) \leq 2$, $R_1(A) \leq 2$,

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma. \quad (10)$$

Тогда для всех целых n, k

$$D_A \begin{pmatrix} n & 1 & 0 \\ k & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+k}A_{n-k} & A_{n+1}A_{n-1} & A_n^2 \\ A_{1+k}A_{1-k} & 0 & 1 \\ A_kA_{-k} & -1 & 0 \end{vmatrix} = 0, \quad (11)$$

$$\Rightarrow A_{n+k}A_{n-k} = -A_kA_{-k}A_{n+1}A_{n-1} + A_{1+k}A_{1-k}A_n^2 \quad (12)$$

$$\Rightarrow A_{-n} = -A_n \text{ (последовательность } A \text{ нечетная)}$$

$$\Rightarrow A_{n+k}A_{n-k} = A_k^2A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2.$$

Т.о. выполняются уравнения

Т.о. выполняются уравнения

$$A_{n+k}A_{n-k} = A_k^2 A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2, \quad (13)$$

$$A_{n+k+1}A_{n-k} = A_k A_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_n A_{n+1}. \quad (14)$$

Т.о. выполняются уравнения

$$A_{n+k}A_{n-k} = A_k^2 A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2, \quad (13)$$

$$A_{n+k+1}A_{n-k} = A_k A_{k+1} A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_n A_{n+1}. \quad (14)$$

$$\begin{aligned} \Rightarrow \quad A_{n+2}A_{n-2} &= A_{n+1}A_{n-1} - \beta A_n^2, \\ A_{n+2}A_{n-3} &= \beta A_{n+1}A_{n-2} - \gamma A_{n-1}A_n. \end{aligned} \quad (15)$$

Т.о. выполняются уравнения

$$A_{n+k}A_{n-k} = A_k^2 A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2, \quad (13)$$

$$A_{n+k+1}A_{n-k} = A_k A_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_n A_{n+1}. \quad (14)$$

$$\begin{aligned} \Rightarrow A_{n+2}A_{n-2} &= A_{n+1}A_{n-1} - \beta A_n^2, \\ A_{n+2}A_{n-3} &= \beta A_{n+1}A_{n-2} - \gamma A_{n-1}A_n. \end{aligned} \quad (15)$$

Заменяя в (13), (14) n на $n+k$, получаем формулы «удвоения»

$$A_{n+2k} = A_n^{-1} \left(A_k^2 A_{n+k+1}A_{n+k-1} - A_{k+1}A_{k-1}A_{n+k}^2 \right), \quad (16)$$

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

Т.о. выполняются уравнения

$$A_{n+k}A_{n-k} = A_k^2 A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2, \quad (13)$$

$$A_{n+k+1}A_{n-k} = A_k A_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_n A_{n+1}. \quad (14)$$

$$\begin{aligned} \Rightarrow A_{n+2}A_{n-2} &= A_{n+1}A_{n-1} - \beta A_n^2, \\ A_{n+2}A_{n-3} &= \beta A_{n+1}A_{n-2} - \gamma A_{n-1}A_n. \end{aligned} \quad (15)$$

Заменяя в (13), (14) n на $n+k$, получаем формулы «удвоения»

$$A_{n+2k} = A_n^{-1} \left(A_k^2 A_{n+k+1}A_{n+k-1} - A_{k+1}A_{k-1}A_{n+k}^2 \right), \quad (16)$$

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

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

Т.о. выполняются уравнения

$$A_{n+k}A_{n-k} = A_k^2 A_{n+1}A_{n-1} - A_{k+1}A_{k-1}A_n^2, \quad (13)$$

$$A_{n+k+1}A_{n-k} = A_k A_{k+1}A_{n+2}A_{n-1} - A_{k+2}A_{k-1}A_n A_{n+1}. \quad (14)$$

$$\begin{aligned} \Rightarrow A_{n+2}A_{n-2} &= A_{n+1}A_{n-1} - \beta A_n^2, \\ A_{n+2}A_{n-3} &= \beta A_{n+1}A_{n-2} - \gamma A_{n-1}A_n. \end{aligned} \quad (15)$$

Заменяя в (13), (14) n на $n+k$, получаем формулы «удвоения»

$$A_{n+2k} = A_n^{-1} \left(A_k^2 A_{n+k+1}A_{n+k-1} - A_{k+1}A_{k-1}A_{n+k}^2 \right), \quad (16)$$

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

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

Лемма 2

Пусть заданы начальные данные $(\beta, \gamma, \mathbb{F})$ и четверки $S(n)$, $S(k)$, $S(n+k)$ (номер n неизвестен!). Тогда можно вычислить четверку $S(n+2k)$, используя $O(1)$ элементарных операций в поле $\mathbb{F}$.

Последовательность A определена выше.

$$S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$$

Последовательность A определена выше.

$$S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$$

Задача 1

Дано $\beta, \gamma, \mathbb{F}$, четверка $S(n)$ и номер m (номер n неизвестен).

Найти $S(n + m)$.

Последовательность A определена выше.

$$S(n) = (A_{n-1}, A_n, A_{n+1}, A_{n+2})$$

Задача 1

Дано $\beta, \gamma, \mathbb{F}$, четверка $S(n)$ и номер m (номер n неизвестен).

Найти $S(n + m)$.

Следствие 1

Существует алгоритм решения задачи 1 сложность которого равна сложности выполнения $O(\ln m)$ элементарных операций в поле $\mathbb{F}$.

Доказательство =

= лемма 2 + бинарный алгоритм возведения в степень.

Аналог алгоритма Диффи-Хеллмана

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.

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 $S(k_1)$ и посылает абоненту B_2 сообщение $S(k_1)$ (номер k_1 хранится в секрете).

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 $S(k_1)$ 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).

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 $S(k_1)$ 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 , зная номер k_2 и четверку $S(k_1)$, вычисляет $S(k_1 + k_2)$. Абонент $B_1 \dots$

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 $S(k_1)$ 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 , зная номер k_2 и четверку $S(k_1)$, вычисляет $S(k_1 + k_2)$. Абонент $B_1 \dots$

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

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 $S(k_1)$ 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 , зная номер k_2 и четверку $S(k_1)$, вычисляет $S(k_1 + k_2)$. Абонент $B_1 \dots$

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

Пассивный противник знает четверки $S(k_1)$ и $S(k_2)$. Номера k_1 и k_2 ему неизвестны; $S(k_1 + k_2) = ?$

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 $S(k_1)$ 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 , зная номер k_2 и четверку $S(k_1)$, вычисляет $S(k_1 + k_2)$. Абонент $B_1 \dots$

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

Пассивный противник знает четверки $S(k_1)$ и $S(k_2)$. Номера k_1 и k_2 ему неизвестны; $S(k_1 + k_2) = ?$

Задача (противника). Найти номер k , зная $(A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Аналог алгоритма Эль-Гамалья

Общие параметры: поле $\mathbb{F}$, $\beta, \gamma \in \mathbb{F}$ и $n \in \mathbb{N}$.

Секретный ключ абонента В: $k \in \mathbb{N}$.

Открытый ключ: четверка $S(k) = (A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Аналог алгоритма Эль-Гамала

Общие параметры: поле $\mathbb{F}$, $\beta, \gamma \in \mathbb{F}$ и $n \in \mathbb{N}$.

Секретный ключ абонента В: $k \in \mathbb{N}$.

Открытый ключ: четверка $S(k) = (A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Алгоритм шифрования

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

Аналог алгоритма Эль-Гамала

Общие параметры: поле $\mathbb{F}$, $\beta, \gamma \in \mathbb{F}$ и $n \in \mathbb{N}$.

Секретный ключ абонента В: $k \in \mathbb{N}$.

Открытый ключ: четверка $S(k) = (A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Алгоритм шифрования

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

- 1 Выбираем сеансовый ключ $r \in \mathbb{N}$.

Аналог алгоритма Эль-Гамала

Общие параметры: поле $\mathbb{F}$, $\beta, \gamma \in \mathbb{F}$ и $n \in \mathbb{N}$.

Секретный ключ абонента В: $k \in \mathbb{N}$.

Открытый ключ: четверка $S(k) = (A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Алгоритм шифрования

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

- 1 Выбираем сеансовый ключ $r \in \mathbb{N}$.
- 2 Вычисляем четверки $S(n+r)$ и $S(n+k+r)$.

Аналог алгоритма Эль-Гамала

Общие параметры: поле $\mathbb{F}$, $\beta, \gamma \in \mathbb{F}$ и $n \in \mathbb{N}$.

Секретный ключ абонента В: $k \in \mathbb{N}$.

Открытый ключ: четверка $S(k) = (A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Алгоритм шифрования

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

- 1 Выбираем сеансовый ключ $r \in \mathbb{N}$.
- 2 Вычисляем четверки $S(n+r)$ и $S(n+k+r)$.
- 3 Вычисляем $y = y_{-1}y_0y_1y_2 \in \mathbb{F}^4$ по формулам: $y_j = x_j \cdot A_{n+k+r+j}$.

Аналог алгоритма Эль-Гамала

Общие параметры: поле $\mathbb{F}$, $\beta, \gamma \in \mathbb{F}$ и $n \in \mathbb{N}$.

Секретный ключ абонента В: $k \in \mathbb{N}$.

Открытый ключ: четверка $S(k) = (A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Алгоритм шифрования

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

- 1 Выбираем сеансовый ключ $r \in \mathbb{N}$.
- 2 Вычисляем четверки $S(n+r)$ и $S(n+k+r)$.
- 3 Вычисляем $y = y_{-1}y_0y_1y_2 \in \mathbb{F}^4$ по формулам: $y_j = x_j \cdot A_{n+k+r+j}$.
- 4 Высылаем абоненту В шифртекст $(S(n+r), y)$.

Аналог алгоритма Эль-Гамала

Общие параметры: поле $\mathbb{F}$, $\beta, \gamma \in \mathbb{F}$ и $n \in \mathbb{N}$.

Секретный ключ абонента В: $k \in \mathbb{N}$.

Открытый ключ: четверка $S(k) = (A_{k-1}, A_k, A_{k+1}, A_{k+2})$.

Алгоритм шифрования

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

- 1 Выбираем сеансовый ключ $r \in \mathbb{N}$.
- 2 Вычисляем четверки $S(n+r)$ и $S(n+k+r)$.
- 3 Вычисляем $y = y_{-1}y_0y_1y_2 \in \mathbb{F}^4$ по формулам: $y_j = x_j \cdot A_{n+k+r+j}$.
- 4 Высылаем абоненту В шифртекст $(S(n+r), y)$.

Абонент В получает шифртекст $(S(n+r), y)$. Вычисляет $S(n+k+r)$ и находит открытый текст $x = x_{-1}x_0x_1x_2$ по формулам $x_j = y_j \cdot A_{n+k+r+j}^{-1}$, $j = -1, 0, 1, 2$.

Вопрос о существовании

Пусть $\mathbb{F}$ — произвольное (конечное) поле.

Вопрос о существовании

Пусть $\mathbb{F}$ — произвольное (конечное) поле.

Задача 1

Пусть $\beta, \gamma \in \mathbb{F}$. При каких условиях на β, γ существует единственная последовательность A такая, что

$$R_0(A) \leq 2, \quad R_1(A) \leq 2, \quad (17)$$

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma? \quad (18)$$

Вопрос о существовании

Пусть $\mathbb{F}$ — произвольное (конечное) поле.

Задача 1

Пусть $\beta, \gamma \in \mathbb{F}$. При каких условиях на β, γ существует единственная последовательность A такая, что

$$R_0(A) \leq 2, \quad R_1(A) \leq 2, \quad (17)$$

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma? \quad (18)$$

Задача 2

Пусть $\alpha_0, \alpha_1, \dots, \alpha_5 \in \mathbb{F}$ и $n_0 \in \mathbb{Z}$. При каких условиях на α_j существует единственная последовательность A , удовлетворяющая (17) и начальным условиям: $A_{n_0+j} = \alpha_j, j = 0, 1, \dots, 5$?

Вопрос о существовании

Пусть $\mathbb{F}$ — произвольное (конечное) поле.

Задача 1

Пусть $\beta, \gamma \in \mathbb{F}$. При каких условиях на β, γ существует единственная последовательность A такая, что

$$R_0(A) \leq 2, \quad R_1(A) \leq 2, \quad (17)$$

$$A_{-1} = -1, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma? \quad (18)$$

Задача 2

Пусть $\alpha_0, \alpha_1, \dots, \alpha_5 \in \mathbb{F}$ и $n_0 \in \mathbb{Z}$. При каких условиях на α_j существует единственная последовательность A , удовлетворяющая (17) и начальным условиям: $A_{n_0+j} = \alpha_j, j = 0, 1, \dots, 5$?

Если $\mathbb{F} = \mathbb{C}$, то ответ вытекает из известных результатов.

Результаты о существовании

Теорема 1

Пусть $\alpha, \beta, \gamma \in \mathbb{F}$, причем $\alpha\beta \neq 0$. Существует единственная последовательность A такая, что

$$A_{-1} = -\alpha, \quad A_0 = 0, \quad A_1 = A_2 = 1, \quad A_3 = \beta, \quad A_4 = \gamma; \quad (19)$$

$$R_0(A) \leq 2, \quad R_1(A) \leq 2. \quad (20)$$

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

$$A_{-n} = -\alpha^n A_n, \quad (21)$$

$$A_{n+k} A_{n-k} = \alpha^{k-1} \left(A_k^2 A_{n+1} A_{n-1} - A_{k+1} A_{k-1} A_n^2 \right), \quad (22)$$

$$A_{n+k+1} A_{n-k} = \alpha^{k-1} \left(A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1} \right). \quad (23)$$

Схема доказательства

$$D_A \begin{pmatrix} n & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-2} & A_{n+1}A_{n-1} & A_n^2 \\ -\alpha\beta & 0 & 1 \\ -1 & -\alpha & 0 \end{vmatrix} = 0. \quad (24)$$

$$\hat{D}_A \begin{pmatrix} n-1 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-3} & A_{n+1}A_{n-2} & A_nA_{n-1} \\ -\alpha\gamma & 0 & 1 \\ -\beta & -\alpha & 0 \end{vmatrix} = 0. \quad (25)$$

Схема доказательства

$$D_A \begin{pmatrix} n & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-2} & A_{n+1}A_{n-1} & A_n^2 \\ -\alpha\beta & 0 & 1 \\ -1 & -\alpha & 0 \end{vmatrix} = 0. \quad (24)$$

$$\hat{D}_A \begin{pmatrix} n-1 & 1 & 0 \\ 2 & 1 & 0 \end{pmatrix} = \begin{vmatrix} A_{n+2}A_{n-3} & A_{n+1}A_{n-2} & A_nA_{n-1} \\ -\alpha\gamma & 0 & 1 \\ -\beta & -\alpha & 0 \end{vmatrix} = 0. \quad (25)$$

Определяем последовательность A по формулам

$$A_{n+2} = \alpha \frac{A_{n+1}A_{n-1} - \beta A_n^2}{A_{n-2}} \quad \text{при } n \geq 3, \quad A_{n-2} \neq 0, \quad (26)$$

$$A_{n+2} = -\alpha\gamma \frac{A_nA_{n-1}}{A_{n-3}} \quad \text{при } n \geq 3, \quad A_{n-2} = 0. \quad (27)$$

$$A_{-n} = -\alpha^n A_n, \quad n \geq 2. \quad (28)$$

Достаточно доказать, что

$$\begin{aligned} A_{n+k} A_{n-k} &= \alpha^{k-1} (A_k^2 A_{n+1} A_{n-1} - A_{k+1} A_{k-1} A_n^2), \\ A_{n+k+1} A_{n-k} &= \alpha^{k-1} (A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1}). \end{aligned} \quad (29)$$

Достаточно доказать, что

$$\begin{aligned} A_{n+k}A_{n-k} &= \alpha^{k-1} (A_k^2 A_{n+1} A_{n-1} - A_{k+1} A_{k-1} A_n^2), \\ A_{n+k+1}A_{n-k} &= \alpha^{k-1} (A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1}). \end{aligned} \quad (29)$$

❶ Из определения A (формула (26)) «почти сразу» вытекает, что

$$A_{n+2}A_{n-2} = \alpha (A_{n+1}A_{n-1} - \beta A_n^2), \quad (30)$$

Достаточно доказать, что

$$\begin{aligned} A_{n+k}A_{n-k} &= \alpha^{k-1} (A_k^2 A_{n+1} A_{n-1} - A_{k+1} A_{k-1} A_n^2), \\ A_{n+k+1}A_{n-k} &= \alpha^{k-1} (A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1}). \end{aligned} \quad (29)$$

- ❶ Из определения A (формула (26)) «почти сразу» вытекает, что

$$A_{n+2}A_{n-2} = \alpha (A_{n+1}A_{n-1} - \beta A_n^2), \quad (30)$$

- ❷ Используя (30) и индукцию по n , доказываем, что

$$A_{n+3}A_{n-2} = \alpha (\beta A_{n+2}A_{n-1} - \gamma A_n A_{n+1}). \quad (31)$$

Достаточно доказать, что

$$\begin{aligned} A_{n+k}A_{n-k} &= \alpha^{k-1} (A_k^2 A_{n+1} A_{n-1} - A_{k+1} A_{k-1} A_n^2), \\ A_{n+k+1}A_{n-k} &= \alpha^{k-1} (A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1}). \end{aligned} \quad (29)$$

1 Из определения A (формула (26)) «почти сразу» вытекает, что

$$A_{n+2}A_{n-2} = \alpha (A_{n+1}A_{n-1} - \beta A_n^2), \quad (30)$$

2 Используя (30) и индукцию по n , доказываем, что

$$A_{n+3}A_{n-2} = \alpha (\beta A_{n+2}A_{n-1} - \gamma A_n A_{n+1}). \quad (31)$$

3 Вычисляя $A_{n+3}A_{n-2}A_{n-1}$ двумя способами
($A_{n+3}A_{n-1} = \dots$ и $A_{n+3}A_{n-2} = \dots$), получаем

$$\beta(\alpha A_n^3 + A_{n-1}^2 A_{n+2} + A_{n+1}^2 A_{n-2}) = (\alpha + \gamma) A_{n-1} A_n A_{n+1}. \quad (32)$$

Достаточно доказать, что

$$\begin{aligned} A_{n+k}A_{n-k} &= \alpha^{k-1} (A_k^2 A_{n+1} A_{n-1} - A_{k+1} A_{k-1} A_n^2), \\ A_{n+k+1}A_{n-k} &= \alpha^{k-1} (A_k A_{k+1} A_{n+2} A_{n-1} - A_{k+2} A_{k-1} A_n A_{n+1}). \end{aligned} \quad (29)$$

- 1 Из определения A (формула (26)) «почти сразу» вытекает, что

$$A_{n+2}A_{n-2} = \alpha (A_{n+1}A_{n-1} - \beta A_n^2), \quad (30)$$

- 2 Используя (30) и индукцию по n , доказываем, что

$$A_{n+3}A_{n-2} = \alpha (\beta A_{n+2}A_{n-1} - \gamma A_n A_{n+1}). \quad (31)$$

- 3 Вычисляя $A_{n+3}A_{n-2}A_{n-1}$ двумя способами
($A_{n+3}A_{n-1} = \dots$ и $A_{n+3}A_{n-2} = \dots$), получаем

$$\beta(\alpha A_n^3 + A_{n-1}^2 A_{n+2} + A_{n+1}^2 A_{n-2}) = (\alpha + \gamma) A_{n-1} A_n A_{n+1}. \quad (32)$$

- 4 После этого, (29) получаются индукцией по $k = 2, 3, \dots$

Следствие 2

Пусть $\alpha_{-1}, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F} \setminus \{0\}$, $\alpha_4 \in \mathbb{F}$. Тогда существует единственная последовательность A такая, что

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

Следствие 2

Пусть $\alpha_{-1}, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F} \setminus \{0\}$, $\alpha_4 \in \mathbb{F}$. Тогда существует единственная последовательность A такая, что

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

Следствие 2

Пусть $\alpha_{-1}, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F} \setminus \{0\}$, $\alpha_4 \in \mathbb{F}$. Тогда существует единственная последовательность A такая, что

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

Лемма

Если поле $\mathbb{F}$ конечно, то последовательность A имеет период ω , причем $\omega \leq |\mathbb{F}|^4$ и ω делится на $\text{ord}(\alpha)$, $\alpha = -\alpha_{-1}\alpha_1^{-1}$.

Другие варианты начальных данных

Если $R_j(A) \leq 2$ и $B_n = A_{-n}$, $C_n = A_{n+n_0}$, то $R_j(B) \leq 2$ и $R_j(C) \leq 2$.

(33)

(34)

Другие варианты начальных данных

Если $R_j(A) \leq 2$ и $B_n = A_{-n}$, $C_n = A_{n+n_0}$, то $R_j(B) \leq 2$ и $R_j(C) \leq 2$.

Поэтому осталось рассмотреть 2 варианта:

(33)

(34)

Другие варианты начальных данных

Если $R_j(A) \leq 2$ и $B_n = A_{-n}$, $C_n = A_{n+n_0}$, то $R_j(B) \leq 2$ и $R_j(C) \leq 2$.

Поэтому осталось рассмотреть 2 варианта:

$$A_0 = 0, \quad A_j = \alpha_j, \quad j = 1, \dots, 5; \quad (33)$$

$$(34)$$

Другие варианты начальных данных

Если $R_j(A) \leq 2$ и $B_n = A_{-n}$, $C_n = A_{n+n_0}$, то $R_j(B) \leq 2$ и $R_j(C) \leq 2$.

Поэтому осталось рассмотреть 2 варианта:

$$A_0 = 0, \quad A_j = \alpha_j, \quad j = 1, \dots, 5; \quad (33)$$

$$A_{-2} = \alpha_{-2}, \quad A_{-1} = \alpha_{-1}, \quad A_0 = 0, \quad A_j = \alpha_j, \quad j = 1, 2, 3. \quad (34)$$

Другие варианты начальных данных

Если $R_j(A) \leq 2$ и $B_n = A_{-n}$, $C_n = A_{n+n_0}$, то $R_j(B) \leq 2$ и $R_j(C) \leq 2$.

Поэтому осталось рассмотреть 2 варианта:

$$A_0 = 0, \quad A_j = \alpha_j, \quad j = 1, \dots, 5; \quad (33)$$

$$A_{-2} = \alpha_{-2}, \quad A_{-1} = \alpha_{-1}, \quad A_0 = 0, \quad A_j = \alpha_j, \quad j = 1, 2, 3. \quad (34)$$

Следствие 4

Последовательность A такая, что $R_j(A) \leq 2$ и выполняются (33) существует $\iff \alpha_4 \alpha_2^3 \neq \alpha_1 \alpha_3^3$. Если такая последовательность существует, то она единственна.

Другие варианты начальных данных

Если $R_j(A) \leq 2$ и $B_n = A_{-n}$, $C_n = A_{n+n_0}$, то $R_j(B) \leq 2$ и $R_j(C) \leq 2$.
Поэтому осталось рассмотреть 2 варианта:

$$A_0 = 0, \quad A_j = \alpha_j, \quad j = 1, \dots, 5; \quad (33)$$

$$A_{-2} = \alpha_{-2}, \quad A_{-1} = \alpha_{-1}, \quad A_0 = 0, \quad A_j = \alpha_j, \quad j = 1, 2, 3. \quad (34)$$

Следствие 4

Последовательность A такая, что $R_j(A) \leq 2$ и выполняются (33) существует $\iff \alpha_4 \alpha_2^3 \neq \alpha_1 \alpha_3^3$. Если такая последовательность существует, то она единственна.

Следствие 5

Последовательность A такая, что $R_j(A) \leq 2$ и выполняются (34) существует $\iff \alpha_{-2} \alpha_1 = \alpha_2 \alpha_{-1}^2$. Для единственности необходимо и достаточно задать дополнительное условие: $A_4 = \alpha_4$.

$$A_{-2} = \alpha_{-2}, \quad A_{-1} = \alpha_{-1}, \dots, A_3 = \alpha_3. \quad (35)$$

Случай «нулей нет»

$$A_{-2} = \alpha_{-2}, \quad A_{-1} = \alpha_{-1}, \dots, A_3 = \alpha_3. \quad (35)$$

Теорема 2

Пусть $\alpha_j \in \mathbb{F} \setminus \{0\}$, $j = -2, -1, \dots, 3$, 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 $\mathbf{A}$ такая, что $R_j(\mathbf{A}) \leq 2$ и выполняются начальные условия (35).

Схема доказательства

Последовательность A должна удовлетворять условию:

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

$$\implies A_{n+2}A_{n-2} = aA_{n+1}A_{n-1} + bA_n^2, \quad (36)$$

$$A_{n+2} = \frac{aA_{n+1}A_{n-1} + bA_n^2}{A_{n-2}}, \quad n \geq 4; \quad (37)$$

$$A_{n-2} = \frac{aA_{n+1}A_{n-1} + bA_n^2}{A_{n+2}}, \quad n \leq -3. \quad (38)$$

Если среди элементов A встретился ноль, то все сводится к ранее изученному случаю.

Пусть последовательность A не содержит нулей. Положим

$$T = \frac{A_1^2 A_{-2} + A_{-1}^2 A_2 + a A_0^3}{A_{-1} A_0 A_1}.$$

Существует последовательность $\{W_n\} \subset \mathbb{F}(\sqrt{a})$ такая, что

$$\begin{aligned} W_{\pm 1} &= \pm 1, \quad W_0 = 0, \quad W_2 = -\sqrt{a}, \quad W_3 = -b, \quad W_4 = \sqrt{a}(a^2 + Tb), \\ W_{-n} &= -W_n, \\ W_{n+k} W_{n-k} &= W_k^2 W_{n+1} W_{n-1} - W_{k+1} W_{k-1} W_n^2, \\ -\sqrt{a} W_{n+k+1} W_{n-k} &= W_k W_{k+1} W_{n+2} W_{n-1} - W_{k+2} W_{k-1} W_{n+1} W_n. \end{aligned} \quad (39)$$

Используя индукцию по k , доказываем, что

$$A_{n+k} A_{n-k} = W_k^2 A_{n+1} A_{n-1} - W_{k-1} W_{k+1} A_n^2, \quad (40)$$

$$A_{n+k+1} A_{n-k} = -\frac{W_{k+1} W_k}{\sqrt{a}} A_{n+2} A_{n-1} + \frac{W_{k+2} W_{k-1}}{\sqrt{a}} A_{n+1} A_n. \quad (41)$$

THE END.
THANK YOU!