Что можно делать с вещественными числами и нельзя делать с целыми числами

Ю. В. Матиясевич

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

http://logic.pdmi.ras.ru/~yumat

Что можно делать с вещественными числами и нельзя делать с целыми числами

Ю. В. Матиясевич

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

http://logic.pdmi.ras.ru/~yumat

Что можно делать с вещественными числами и нельзя делать с целыми числами

Часть 2. Десятая проблема Гильберта

Ю. В. Матиясевич

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

http://logic.pdmi.ras.ru/~yumat

Что можно делать с вещественными числами и нельзя делать с целыми числами

Часть 2. Десятая проблема Гильберта

Четвёртая лекция

Ю. В. Матиясевич

Санкт-Петербургское отделение
Математического института им. В. А. Стеклова РАН

http://logic.pdmi.ras.ru/~yumat

Гипотеза Martin'a Davis'a (=DPRM-теорема)

Гипотеза M. Davis'a (DPRM-теорема). *Каждое перечислимое множество является диофантовым.*

Гипотеза Martin'a Davis'a (=DPRM-теорема)

Гипотеза M. Davis'a (DPRM-теорема). *Каждое перечислимое множество является диофантовым.*

Теорема (Davis-Putnam-Robinson [1961]). *Каждое перечислимое множество $\mathfrak{M}$ имеет экспоненциально диофантово представление*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\Longleftrightarrow \exists x_1 \ldots x_m \{ E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, x_2, \ldots, x_m) = E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, x_2, \ldots, x_m) \}$$

Гипотеза Martin'a Davis'a (=DPRM-теорема)

Гипотеза M. Davis'a (DPRM-теорема). *Каждое перечислимое множество является диофантовым.*

Теорема (Davis-Putnam-Robinson [1961]). *Каждое перечислимое множество $\mathfrak{M}$ имеет экспоненциально диофантово представление*

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\Longleftrightarrow \exists x_1 \ldots x_m \{ E_{\mathrm{L}}(a_1, \ldots, a_n, x_1, x_2, \ldots, x_m) = E_{\mathrm{R}}(a_1, \ldots, a_n, x_1, x_2, \ldots, x_m) \}$$

$$a = b^c \Longleftrightarrow \exists x_1 \ldots x_m \{ P(a, b, c, x_1, \ldots, x_m) = 0 \}$$

Рекуррентные последовательности второго порядка

$$\alpha_b(0) = 0 \qquad \alpha_b(1) = 1 \qquad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) \qquad b \geq 2$$

Рекуррентные последовательности второго порядка

$$\alpha_b(0) = 0 \qquad \alpha_b(1) = 1 \qquad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) \qquad b \geq 2$$

$$0 < 1 < \alpha_b(2) < \cdots < \alpha_b(n) < \alpha_b(n+1) < \ldots$$

Диофантовость последовательности $\alpha_b(k)$

Основная лемма. *Существует многочлен* $Q(x, b, k, x_1, \ldots, x_m)$ *такой что*

$$b \geq 4 \ \& \ x = \alpha_b(k) \Longleftrightarrow \exists x_1 \ldots x_m \{Q(x, b, k, x_1, \ldots, x_m) = 0\}$$

Диофантовость последовательности $\alpha_b(k)$

Основная лемма. *Существует многочлен* $Q(x, b, k, x_1, \ldots, x_m)$ *такой что*

$$b \geq 4 \ \& \ x = \alpha_b(k) \Longleftrightarrow \exists x_1 \ldots x_m \{Q(x, b, k, x_1, \ldots, x_m) = 0\}$$

Скорость роста

$$\alpha_b(0) = 0 \qquad \alpha_b(1) = 1 \qquad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) \qquad b \geq 2$$

$$(b-1)\alpha_b(n+1) \leq \alpha_b(n+2) \leq b\alpha_b(n+1)$$

Скорость роста

$$\alpha_b(0) = 0 \qquad \alpha_b(1) = 1 \qquad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) \qquad b \geq 2$$

$$(b-1)\alpha_b(n+1) \leq \alpha_b(n+2) \leq b\alpha_b(n+1)$$

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n \leq \alpha_{b+1}(n+1) \leq (b+1)^n$$

Скорость роста

$$\alpha_b(0) = 0 \qquad \alpha_b(1) = 1 \qquad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) \qquad b \geq 2$$

$$(b-1)\alpha_b(n+1) \leq \alpha_b(n+2) \leq b\alpha_b(n+1)$$

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n \leq \alpha_{b+1}(n+1) \leq (b+1)^n$$

$$\left(\frac{bd-1}{d+1}\right)^n \leq \frac{\alpha_{bd}(n+1)}{\alpha_{d+1}(n+1)} \leq b^n \leq \frac{\alpha_{bd+1}(n+1)}{\alpha_d(n+1)} \leq \left(\frac{bd+1}{d-1}\right)^n$$

Скорость роста

$$\alpha_b(0) = 0 \qquad \alpha_b(1) = 1 \qquad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n) \qquad b \geq 2$$

$$(b-1)\alpha_b(n+1) \leq \alpha_b(n+2) \leq b\alpha_b(n+1)$$

$$(b-1)^n \leq \alpha_b(n+1) \leq b^n \leq \alpha_{b+1}(n+1) \leq (b+1)^n$$

$$\left(\frac{bd-1}{d+1}\right)^n \leq \frac{\alpha_{bd}(n+1)}{\alpha_{d+1}(n+1)} \leq b^n \leq \frac{\alpha_{bd+1}(n+1)}{\alpha_d(n+1)} \leq \left(\frac{bd+1}{d-1}\right)^n$$

$$a = b^n \iff$$

$$\iff \exists d \left\{ \frac{\alpha_{bd}(n+1)}{\alpha_{d+1}(n+1)} \leq a \leq \frac{\alpha_{bd+1}(n+1)}{\alpha_d(n+1)} \leq \frac{\alpha_{bd}(n+1)}{\alpha_{d+1}(n+1)} + \frac{1}{2} \right\}$$

Матричное представление

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$$

Матричное представление

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$$

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

Матричное представление

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$$

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

$$A_b(n+1) \quad = \quad A_b(n)\Psi_b$$

Матричное представление

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$$

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

$$A_b(n+1) \quad = \quad A_b(n)\Psi_b$$

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}$$

Матричное представление

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$$

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

$$A_b(n+1) \quad = \quad A_b(n)\Psi_b$$

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}$$

Матричное представление

$$\alpha_b(0) = 0 \quad \alpha_b(1) = 1 \quad \alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$$

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}$$

$$A_b(n+1) \quad = \quad A_b(n)\Psi_b$$

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}$$

$$A_b(n) = \Psi^n$$

Характеристическое уравнение

$$
\begin{aligned}
\det(A_b(n)) &= \alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1) \\
&= \alpha_b^2(n+1) - b\alpha_b(n+1)\alpha_b(n) + \alpha_b^2(n) \\
&= \alpha_b^2(n-1) - b\alpha_b(n-1)\alpha_b(n) + \alpha_b^2(n) \\
&= \det(\Psi_b^n) \\
&= (\det \Psi_b)^n \\
&= 1
\end{aligned}
$$

Характеристическое уравнение

$$
\begin{aligned}
\det(A_b(n)) &= \alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1) \\
&= \alpha_b^2(n+1) - b\alpha_b(n+1)\alpha_b(n) + \alpha_b^2(n) \\
&= \alpha_b^2(n-1) - b\alpha_b(n-1)\alpha_b(n) + \alpha_b^2(n) \\
&= \det(\Psi_b^n) \\
&= (\det \Psi_b)^n \\
&= 1
\end{aligned}
$$

$$x^2 - bxy + y^2 = 1$$

Характеристическое уравнение

$$\begin{aligned}
\det(A_b(n)) &= \alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1) \\
&= \alpha_b^2(n+1) - b\alpha_b(n+1)\alpha_b(n) + \alpha_b^2(n) \\
&= \alpha_b^2(n-1) - b\alpha_b(n-1)\alpha_b(n) + \alpha_b^2(n) \\
&= \det(\Psi_b^n) \\
&= (\det \Psi_b)^n \\
&= 1
\end{aligned}$$

$$x^2 - bxy + y^2 = 1$$

$$\begin{cases} x = \alpha_b(n+1) \\ y = \alpha_b(n) \end{cases} \qquad \begin{cases} x = \alpha_b(n-1) \\ y = \alpha_b(n) \end{cases}$$

Характеристическое уравнение

Лемма. *Если* $x^2 - bxy + y^2 = 1$, *то найдется число* n *такое, что*

$$\begin{cases} x = \alpha_b(n+1) \\ y = \alpha_b(n) \end{cases} \quad \textit{или же} \quad \begin{cases} x = \alpha_b(n) \\ y = \alpha_b(n+1) \end{cases}$$

Характеристическое уравнение

Лемма. *Если* $x^2 - bxy + y^2 = 1$, *то найдется число* n *такое, что*

$$\begin{cases} x = \alpha_b(n+1) \\ y = \alpha_b(n) \end{cases} \quad \text{или же} \quad \begin{cases} x = \alpha_b(n) \\ y = \alpha_b(n+1) \end{cases}$$

Лемма. *Если* $x^2 - bxy + y^2 = 1$ *и* $y \leq x$, *то найдется число* n *такое, что* $x = \alpha_b(n+1),\ y = \alpha_b(n)$.

Диофантово представление множества чисел α_b

Следствие леммы:

$$x \in \mathfrak{M}_b \quad \Longleftrightarrow \quad x \in \{0, 1, b, \ldots, \alpha_b(n), \ldots\}$$

Диофантово представление множества чисел α_b

Следствие леммы:

$$\begin{aligned} x \in \mathfrak{M}_b \quad &\Longleftrightarrow \quad x \in \{0, 1, b, \ldots, \alpha_b(n), \ldots\} \\ &\Longleftrightarrow \quad \exists y \{x^2 - bxy + y^2 = 1\} \end{aligned}$$

Диофантово представление множества чисел α_b

Следствие леммы:

$$\begin{aligned} x \in \mathfrak{M}_b \quad &\Longleftrightarrow \quad x \in \{0, 1, b, \ldots, \alpha_b(n), \ldots\} \\ &\Longleftrightarrow \quad \exists y \{x^2 - bxy + y^2 = 1\} \end{aligned}$$

Диофантово представление множества чисел α_b

Следствие леммы:

$$\begin{aligned} x \in \mathfrak{M}_b \quad &\Longleftrightarrow \quad x \in \{0, 1, b, \ldots, \alpha_b(n), \ldots\} \\ &\Longleftrightarrow \quad \exists y \{x^2 - bxy + y^2 = 1\} \end{aligned}$$

Требуется:

$$\langle x, k \rangle \in \mathfrak{N}_b \quad \Longleftrightarrow \quad x = \alpha_b(k)$$

Диофантово представление множества чисел α_b

Следствие леммы:

$$\begin{aligned} x \in \mathfrak{M}_b \quad &\Longleftrightarrow \quad x \in \{0, 1, b, \ldots, \alpha_b(n), \ldots\} \\ &\Longleftrightarrow \quad \exists y \{x^2 - bxy + y^2 = 1\} \end{aligned}$$

Требуется:

$$\begin{aligned} \langle x, k \rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

Новые свойства делимости

Лемма (доказанная).

$$\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$$

Новые свойства делимости

Лемма (доказанная).

$$\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$$

Лемма (обратная).

$$k\alpha_b(k) \mid m \Rightarrow \alpha_b^2(k) \mid \alpha_b(m)$$

Новые свойства делимости

Лемма (доказанная).

$$\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$$

Лемма (обратная).

$$k\alpha_b(k) \mid m \Rightarrow \alpha_b^2(k) \mid \alpha_b(m)$$

Новые свойства делимости

$$k\alpha_b(k) \mid m$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

$$A_b(m) \;=\; A_b^{\ell}(k)$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

$$\begin{aligned} A_b(m) &= A_b^{\ell}(k) \\ &= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \end{aligned}$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

$$\begin{aligned} A_b(m) &= A_b^{\ell}(k) \\ &= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\ &= \begin{pmatrix} b\alpha_b(k) - \alpha_b(k-1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \end{aligned}$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

$$\begin{aligned}
A_b(m) &= A_b^{\ell}(k) \\
&= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \begin{pmatrix} b\alpha_b(k) - \alpha_b(k-1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \left[\alpha_b(k) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} - \alpha_b(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]^{\ell}
\end{aligned}$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

$$\begin{aligned}
A_b(m) &= A_b^{\ell}(k) \\
&= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \begin{pmatrix} b\alpha_b(k) - \alpha_b(k-1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \left[\alpha_b(k) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} - \alpha_b(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]^{\ell} \\
&= [\alpha_b(k)\Psi_b - \alpha_b(k-1)E]^{\ell}
\end{aligned}$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

$$\begin{aligned}
A_b(m) &= A_b^{\ell}(k) \\
&= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \begin{pmatrix} b\alpha_b(k) - \alpha_b(k-1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \left[\alpha_b(k) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} - \alpha_b(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]^{\ell} \\
&= [\alpha_b(k)\Psi_b - \alpha_b(k-1)E]^{\ell} \\
&= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k)\alpha_b^{\ell-i}(k-1)\Psi_b^i
\end{aligned}$$

Новые свойства делимости

$$k\alpha_b(k) \mid m \qquad m = k\ell \qquad \alpha_b(k) \mid \ell$$

$$\begin{aligned}
A_b(m) &= A_b^{\ell}(k) \\
&= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \begin{pmatrix} b\alpha_b(k) - \alpha_b(k-1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^{\ell} \\
&= \left[\alpha_b(k) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} - \alpha_b(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]^{\ell} \\
&= [\alpha_b(k)\Psi_b - \alpha_b(k-1)E]^{\ell} \\
&= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k)\alpha_b^{\ell-i}(k-1)\Psi_b^i
\end{aligned}$$

Новые свойства делимости

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m)$$

$$= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k) \alpha_b^{\ell-i}(k-1) \Psi_b^i$$

Новые свойства делимости

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m)$$

$$= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k) \alpha_b^{\ell-i}(k-1) \Psi_b^i$$

$$\equiv (-1)^{\ell} \alpha_b^{\ell}(k-1)E + (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1)\Psi_b \pmod{\alpha_b^2(k)}$$

Новые свойства делимости

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m)$$

$$\begin{aligned} &= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k) \alpha_b^{\ell-i}(k-1) \Psi_b^i \\ &\equiv (-1)^{\ell} \alpha_b^{\ell}(k-1) E \ + \ (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \Psi_b \pmod{\alpha_b^2(k)} \\ &= (-1)^{\ell} \alpha_b^{\ell}(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ + \\ &\quad + (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \pmod{\alpha_b^2(k)} \end{aligned}$$

Новые свойства делимости

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m)$$

$$= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k) \alpha_b^{\ell-i}(k-1) \Psi_b^i$$

$$\equiv (-1)^{\ell} \alpha_b^{\ell}(k-1) E + (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \Psi_b \pmod{\alpha_b^2(k)}$$

$$= (-1)^{\ell} \alpha_b^{\ell}(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} +$$

$$+(-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \pmod{\alpha_b^2(k)}$$

$$\alpha_b(m) \equiv (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \pmod{\alpha_b^2(k)}$$

Новые свойства делимости

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m)$$

$$= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k) \alpha_b^{\ell-i}(k-1) \Psi_b^i$$

$$\equiv (-1)^{\ell} \alpha_b^{\ell}(k-1) E + (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \Psi_b \pmod{\alpha_b^2(k)}$$

$$= (-1)^{\ell} \alpha_b^{\ell}(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} +$$

$$+(-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \pmod{\alpha_b^2(k)}$$

$$\alpha_b(m) \equiv (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \pmod{\alpha_b^2(k)}$$

$$\alpha_b(k) \mid \ell$$

Новые свойства делимости

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} = A_b(m)$$

$$= \sum_{i=0}^{\ell} (-1)^{\ell-i} \binom{\ell}{i} \alpha_b^i(k) \alpha_b^{\ell-i}(k-1) \Psi_b^i$$

$$\equiv (-1)^{\ell} \alpha_b^{\ell}(k-1) E + (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \Psi_b \pmod{\alpha_b^2(k)}$$

$$= (-1)^{\ell} \alpha_b^{\ell}(k-1) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} +$$

$$+(-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \pmod{\alpha_b^2(k)}$$

$$\alpha_b(m) \equiv (-1)^{\ell-1} \ell \alpha_b(k) \alpha_b^{\ell-1}(k-1) \pmod{\alpha_b^2(k)}$$

$$\alpha_b(k) \mid \ell \qquad \alpha_b^2(k) \mid \alpha_b(m)$$

Новые свойства делимости

Лемма.

$$\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$$

Новые свойства делимости

Лемма.

$$\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$$

Лемма (обратная).

$$k\alpha_b(k) \mid m \Rightarrow \alpha_b^2(k) \mid \alpha_b(m)$$

Новые свойства делимости

Лемма.

$$\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$$

Лемма (обратная).

$$k\alpha_b(k) \mid m \Rightarrow \alpha_b^2(k) \mid \alpha_b(m)$$

Следствие.

$$k\alpha_b(k) \mid m \Leftrightarrow \alpha_b^2(k) \mid \alpha_b(m)$$

Диофантовость последовательности $\alpha_b(k)$

Основная лемма. *Существует многочлен* $Q(x, b, k, x_1, \ldots, x_m)$ *такой что*

$$b \geq 4 \ \& \ x = \alpha_b(k) \Longleftrightarrow \exists x_1 \ldots x_m \{Q(x, b, k, x_1, \ldots, x_m) = 0\}$$

Диофантовость последовательности $\alpha_b(k)$

Основная лемма. *Существует многочлен* $Q(x, b, k, x_1, \ldots, x_m)$ *такой что*

$$b \geq 4 \ \& \ x = \alpha_b(k) \Longleftrightarrow \exists x_1 \ldots x_m \{Q(x, b, k, x_1, \ldots, x_m) = 0\}$$

Основная лемма. *Для любого числа b, такого что $b \geq 4$, и любых чисел x и k, равенство $x = \alpha_b(k)$ имеет место тогда и только тогда, когда существуют числа B, r, s, t, u, v, X, Y такие, что*

$$u^2 - but + t^2 = 1,$$
$$s^2 - bsr + r^2 = 1,$$
$$r < s,$$
$$u^2 \mid s,$$
$$v = bs - 2r,$$
$$v \mid B - b,$$
$$u \mid B - 2,$$
$$B \geq 4,$$
$$X^2 - BXY + Y^2 = 1,$$
$$2x < u,$$
$$x = \mathrm{arem}(X, v),$$
$$k = \mathrm{arem}(X, u).$$

Первый шаг

$$\begin{aligned} \langle x, k \rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

Первый шаг

$$\begin{aligned} \langle x, k \rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) =$$

Первый шаг

$$\begin{aligned} \langle x, k \rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) = n$$

Первый шаг

$$\begin{aligned} \langle x, k \rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) = n$$

Первый шаг

$$\begin{aligned} \langle x, k\rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) = n$$

$$\mathfrak{N}_2 \quad = \quad \{\langle k, k\rangle : k \in \mathbb{N}\}$$

Первый шаг

$$\begin{aligned} \langle x, k\rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) = n$$

$$\begin{aligned} \mathfrak{N}_2 \quad &= \quad \{\langle k, k\rangle : k \in \mathbb{N}\} \\ &= \quad \{\langle \alpha_2(k), \alpha_2(k)\rangle : k \in \mathbb{N}\} \end{aligned}$$

Первый шаг

$$\begin{aligned} \langle x, k\rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) = n$$

$$\begin{aligned} \mathfrak{N}_2 &= \{\langle k, k\rangle : k \in \mathbb{N}\} \\ &= \{\langle \alpha_2(k), \alpha_2(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_2\} \end{aligned}$$

Первый шаг

$$\begin{aligned} \langle x, k\rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) = n$$

$$\begin{aligned} \mathfrak{N}_2 &= \{\langle k, k\rangle : k \in \mathbb{N}\} \\ &= \{\langle \alpha_2(k), \alpha_2(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_2\} \end{aligned}$$

$$\mathfrak{N}_b^* = \{\langle \alpha_b(k), \alpha_b(k)\rangle : k \in \mathbb{N}\}$$

Первый шаг

$$\begin{aligned} \langle x, k\rangle \in \mathfrak{N}_b \quad &\Longleftrightarrow \quad x = \alpha_b(k) \\ &\Longleftrightarrow \quad ? \end{aligned}$$

$$\alpha_2(n) = n$$

$$\begin{aligned} \mathfrak{N}_2 &= \{\langle k, k\rangle : k \in \mathbb{N}\} \\ &= \{\langle \alpha_2(k), \alpha_2(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_2\} \end{aligned}$$

$$\begin{aligned} \mathfrak{N}_b^* &= \{\langle \alpha_b(k), \alpha_b(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_b\} \end{aligned}$$

Второй шаг

$$\begin{aligned}\mathfrak{N}_b^* &= \{\langle \alpha_b(k), \alpha_b(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_b\}\end{aligned}$$

Второй шаг

$$\begin{aligned}\mathfrak{N}_b^* &= \{\langle \alpha_b(k), \alpha_b(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_b\}\end{aligned}$$

$$\mathfrak{N}_b = \{\langle \alpha_b(k), \alpha_2(k)\rangle : k \in \mathbb{N}\}$$

Сравнение последовательностей

$$\alpha_{b'}(0) = 0 \quad \alpha_{b'}(1) = 1 \quad \alpha_{b'}(n+2) = b'\alpha_{b'}(n+1) - \alpha_{b'}(n)$$
$$\alpha_{b''}(0) = 0 \quad \alpha_{b''}(1) = 1 \quad \alpha_{b''}(n+2) = b''\alpha_{b''}(n+1) - \alpha_{b''}(n)$$

Сравнение последовательностей

$$\alpha_{b'}(0) = 0 \quad \alpha_{b'}(1) = 1 \quad \alpha_{b'}(n+2) = b'\alpha_{b'}(n+1) - \alpha_{b'}(n)$$
$$\alpha_{b''}(0) = 0 \quad \alpha_{b''}(1) = 1 \quad \alpha_{b''}(n+2) = b''\alpha_{b''}(n+1) - \alpha_{b''}(n)$$

$$b'' \equiv b' \pmod{b' - b''}$$

Сравнение последовательностей

$$\alpha_{b'}(0) = 0 \quad \alpha_{b'}(1) = 1 \quad \alpha_{b'}(n+2) = b'\alpha_{b'}(n+1) - \alpha_{b'}(n)$$
$$\alpha_{b''}(0) = 0 \quad \alpha_{b''}(1) = 1 \quad \alpha_{b''}(n+2) = b''\alpha_{b''}(n+1) - \alpha_{b''}(n)$$

$$b'' \equiv b' \pmod{b' - b''}$$

$$\alpha_{b''}(n) \equiv \alpha_{b'}(n) \pmod{b' - b''}$$

Функции rem и arem

$$z = \mathrm{rem}(y, x) \iff y \equiv z \pmod{x} \& z \leq x - 1$$

Функции rem и arem

$$z = \mathrm{rem}(y, x) \iff y \equiv z \pmod{x} \& z \leq x - 1$$

$$z = \mathrm{arem}(y, x) \iff \big(y \equiv z \pmod{x} \text{ or } y \equiv -z \pmod{x}\big) \& 2z \leq x$$

Сравнение последовательностей

$$b'' \equiv b' \pmod{b' - b''}$$

Сравнение последовательностей

$$b'' \equiv b' \pmod{b' - b''}$$

$$\alpha_{b''}(n) \equiv \alpha_{b'}(n) \pmod{b' - b''}$$

Сравнение последовательностей

$$b'' \equiv b' \pmod{b' - b''}$$

$$\alpha_{b''}(n) \equiv \alpha_{b'}(n) \pmod{b' - b''}$$

Сравнение последовательностей

$$b'' \equiv b' \pmod{b' - b''}$$

$$\alpha_{b''}(n) \equiv \alpha_{b'}(n) \pmod{b' - b''}$$

$$\mathrm{rem}(\alpha_{b''}(n), b' - b'') = \mathrm{rem}(\alpha_{b'}(n), b' - b'')$$

Сравнение последовательностей

$$b'' \equiv b' \pmod{b' - b''}$$

$$\alpha_{b''}(n) \equiv \alpha_{b'}(n) \pmod{b' - b''}$$

$$\mathrm{rem}(\alpha_{b''}(n), b' - b'') = \mathrm{rem}(\alpha_{b'}(n), b' - b'')$$

Сравнение последовательностей

$$b'' \equiv b' \pmod{b' - b''}$$

$$\alpha_{b''}(n) \equiv \alpha_{b'}(n) \pmod{b' - b''}$$

$$\mathrm{rem}(\alpha_{b''}(n), b' - b'') = \mathrm{rem}(\alpha_{b'}(n), b' - b'')$$

$$\alpha_{b''}(n) = \mathrm{rem}(\alpha_{b'}(n), b' - b'') \quad \text{provided} \quad \alpha_{b''}(n) < b' - b''$$

Второй шаг

$$\mathfrak{N}_b^* \quad = \quad \{\langle \alpha_b(k), \alpha_b(k) \rangle : k \in \mathbb{N}\}$$

Второй шаг

$$\begin{aligned}\mathfrak{N}_b^* &= \{\langle \alpha_b(k), \alpha_b(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_b\}\end{aligned}$$

Второй шаг

$$\begin{aligned}\mathfrak{N}_b^* &= \{\langle \alpha_b(k), \alpha_b(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_b\}\end{aligned}$$

$$\mathfrak{N}_b = \{\langle \alpha_b(k), \alpha_2(k)\rangle : k \in \mathbb{N}\}$$

Второй шаг

$$\begin{aligned}\mathfrak{N}_b^* &= \{\langle \alpha_b(k), \alpha_b(k)\rangle : k \in \mathbb{N}\} \\ &= \{\langle x, x\rangle : x \in \mathfrak{M}_b\}\end{aligned}$$

$$\mathfrak{N}_b = \{\langle \alpha_b(k), \alpha_2(k)\rangle : k \in \mathbb{N}\}$$

$$\mathfrak{N}_b^{**} = \{\langle x, \mathrm{rem}(x, b-2)\rangle : x \in \mathfrak{M}_b\}$$

Третий шаг

$$\mathfrak{N}_b^{**} \quad = \quad \{\langle x, \mathrm{rem}(x, b-2)\rangle : x \in \mathfrak{M}_b\}$$

Третий шаг

$$\mathfrak{N}_b^{**} = \{\langle x, \mathrm{rem}(x, b-2)\rangle : x \in \mathfrak{M}_b\}$$

$$\mathfrak{N}_b^{***} = \{\langle \mathrm{rem}(x, B-b), \mathrm{rem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

$$\alpha_b(0) \pmod{v}, \ \alpha_b(1) \pmod{v}, \ldots, \alpha_b(n) \pmod{v}, \ldots$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

$$\alpha_b(0) \pmod{v},\ \alpha_b(1) \pmod{v}, \ldots, \alpha_b(n) \pmod{v}, \ldots$$

$$\alpha_b(m) \equiv \alpha_b(m+p) \pmod{v}$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

$$\alpha_b(0) \pmod{v},\ \alpha_b(1) \pmod{v}, \ldots, \alpha_b(n) \pmod{v}, \ldots$$

$$\begin{aligned} \alpha_b(m) &\equiv \alpha_b(m+p) \pmod{v} \\ \alpha_b(m+1) &\equiv \alpha_b(m+1+p) \pmod{v} \end{aligned}$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

$$\alpha_b(0) \pmod{v},\ \alpha_b(1) \pmod{v}, \ldots, \alpha_b(n) \pmod{v}, \ldots$$

$$\begin{aligned} \alpha_b(m) &\equiv \alpha_b(m+p) \pmod{v} \\ \alpha_b(m+1) &\equiv \alpha_b(m+1+p) \pmod{v} \\ \alpha_b(m+2) &\equiv \alpha_b(m+2+p) \pmod{v} \end{aligned}$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

$$\alpha_b(0) \pmod{v},\ \alpha_b(1) \pmod{v}, \ldots, \alpha_b(n) \pmod{v}, \ldots$$

$$\begin{aligned}
\alpha_b(m) &\equiv \alpha_b(m+p) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m+1+p) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m+2+p) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m+3+p) \pmod{v}
\end{aligned}$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

$$\alpha_b(0) \pmod{v},\ \alpha_b(1) \pmod{v}, \ldots, \alpha_b(n) \pmod{v}, \ldots$$

$$\begin{aligned}
\alpha_b(m-1) &\equiv \alpha_b(m-1+p) \pmod{v} \\
\alpha_b(m) &\equiv \alpha_b(m+p) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m+1+p) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m+2+p) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m+3+p) \pmod{v}
\end{aligned}$$

Периодичность

$$\alpha_b(0), \alpha_b(1), \ldots, \alpha_b(n), \ldots$$

$$\alpha_b(0) \pmod{v},\ \alpha_b(1) \pmod{v}, \ldots, \alpha_b(n) \pmod{v}, \ldots$$

$$\begin{aligned}
\alpha_b(m-1) &\equiv \alpha_b(m-1+p) \pmod{v} \\
\alpha_b(m) &\equiv \alpha_b(m+p) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m+1+p) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m+2+p) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m+3+p) \pmod{v}
\end{aligned}$$

$$\alpha_b(n) \equiv \alpha_b(n+p) \pmod{v}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\alpha_b(0) \quad \equiv \quad \alpha_b(0) = 0 \pmod{v}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned} \alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\ \alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned} \alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\ \alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\ \vdots &\equiv \vdots \end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v}
\end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v}
\end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m-2) \pmod{v}
\end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m-2) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m-3) \pmod{v}
\end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m-2) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m-3) \pmod{v} \\
\vdots &\equiv \vdots
\end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m-2) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m-3) \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(2m-1) &\equiv \alpha_b(1) \pmod{v}
\end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m-2) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m-3) \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(2m-1) &\equiv \alpha_b(1) \pmod{v} \\
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v}
\end{aligned}$$

Специальный период

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$\begin{aligned}
\alpha_b(0) &\equiv \alpha_b(0) = 0 \pmod{v} \\
\alpha_b(1) &\equiv \alpha_b(1) = 1 \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(m) &\equiv \alpha_b(m) \pmod{v} \\
\alpha_b(m+1) &\equiv \alpha_b(m-1) \pmod{v} \\
\alpha_b(m+2) &\equiv \alpha_b(m-2) \pmod{v} \\
\alpha_b(m+3) &\equiv \alpha_b(m-3) \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(2m-1) &\equiv \alpha_b(1) \pmod{v} \\
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v}
\end{aligned}$$

Специальный период

$$\alpha_b(2m) \equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v}$$

Специальный период

$$\begin{aligned} \alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\ \alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \end{aligned}$$

Специальный период

$$\begin{aligned}
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \\
\alpha_b(2m+2) &\equiv -\alpha_b(2) \pmod{v}
\end{aligned}$$

Специальный период

$$
\begin{aligned}
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \\
\alpha_b(2m+2) &\equiv -\alpha_b(2) \pmod{v} \\
\vdots &\equiv \vdots
\end{aligned}
$$

Специальный период

$$
\begin{aligned}
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \\
\alpha_b(2m+2) &\equiv -\alpha_b(2) \pmod{v} \\
\vdots &\equiv \vdots \\
\alpha_b(2m+n) &\equiv -\alpha_b(n) \pmod{v}
\end{aligned}
$$

Специальный период

$$
\begin{aligned}
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \\
\alpha_b(2m+2) &\equiv -\alpha_b(2) \pmod{v} \\
&\vdots \equiv \vdots \\
\alpha_b(2m+n) &\equiv -\alpha_b(n) \pmod{v} \\
&\vdots \equiv \vdots
\end{aligned}
$$

Специальный период

$$
\begin{aligned}
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \\
\alpha_b(2m+2) &\equiv -\alpha_b(2) \pmod{v} \\
&\vdots \equiv \vdots \\
\alpha_b(2m+n) &\equiv -\alpha_b(n) \pmod{v} \\
&\vdots \equiv \vdots \\
\alpha_b(4m+n) &\equiv -\alpha_b(2m+n) \equiv \alpha_b(n) \pmod{v}
\end{aligned}
$$

Специальный период

$$
\begin{aligned}
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \\
\alpha_b(2m+2) &\equiv -\alpha_b(2) \pmod{v} \\
&\vdots \equiv \vdots \\
\alpha_b(2m+n) &\equiv -\alpha_b(n) \pmod{v} \\
&\vdots \equiv \vdots \\
\alpha_b(4m+n) &\equiv -\alpha_b(2m+n) \equiv \alpha_b(n) \pmod{v}
\end{aligned}
$$

При $v = \alpha_b(m+1) - \alpha_b(m-1)$ последовательность

$$\alpha_b(0) \pmod{v}, \alpha_b(1) \pmod{v}, \ldots, \alpha_b(1) \pmod{v}, \ldots$$

имеет период длины $4m$

Специальный период

$$
\begin{aligned}
\alpha_b(2m) &\equiv \alpha_b(0) = 0 = -\alpha_b(0) \pmod{v} \\
\alpha_b(2m+1) &\equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v} \\
\alpha_b(2m+2) &\equiv -\alpha_b(2) \pmod{v} \\
&\vdots \equiv \vdots \\
\alpha_b(2m+n) &\equiv -\alpha_b(n) \pmod{v} \\
&\vdots \equiv \vdots \\
\alpha_b(4m+n) &\equiv -\alpha_b(2m+n) \equiv \alpha_b(n) \pmod{v}
\end{aligned}
$$

При $v = \alpha_b(m+1) - \alpha_b(m-1)$ последовательность

$$\alpha_b(0) \pmod{v}, \alpha_b(1) \pmod{v}, \ldots, \alpha_b(1) \pmod{v}, \ldots$$

имеет период длины $4m$, а последовательность

$$\operatorname{arem}(\alpha_b(0), v), \operatorname{arem}(\alpha_b(1), v), \ldots, \operatorname{arem}(\alpha_b(n), v), \ldots$$

имеет период длины $2m$.

Четвертый шаг

$$\mathfrak{N}_b^{***} \quad = \quad \{\langle \mathrm{rem}(x, B-b), \mathrm{rem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

Четвертый шаг

$$\mathfrak{N}_b^{***} = \{\langle \mathrm{rem}(x, B-b), \mathrm{rem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

Четвертый шаг

$$\mathfrak{N}_b^{***} = \{\langle \mathrm{rem}(x, B-b), \mathrm{rem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

Четвертый шаг

$$\mathfrak{N}_b^{***} = \{\langle \mathrm{rem}(x, B-b), \mathrm{rem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$v | B - b$$

Четвертый шаг

$$\mathfrak{N}_b^{***} = \{\langle \mathrm{rem}(x, B-b), \mathrm{rem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$v | B - b$$

Пятый шаг

$$\mathfrak{N}_b^{****} \quad = \quad \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

Пятый шаг

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

Пятый шаг

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$v | B - b$$

Пятый шаг

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$v | B - b$$

$$\mathfrak{N}_b^{*****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, u)\rangle : x \in \mathfrak{M}_B\}$$

Пятый шаг

$$\mathfrak{N}_b^{****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, B-2)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1)$$

$$v | B - b$$

$$\mathfrak{N}_b^{*****} = \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, u)\rangle : x \in \mathfrak{M}_B\}$$

$$u | B - 2$$

Ключевая идея

Ключевая идея

$$\mathfrak{N}_b^{*****} \quad = \quad \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, u)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1) \qquad v|B-b \qquad u|B-2$$

Ключевая идея

$$\mathfrak{N}_b^{*****} \quad = \quad \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, u)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1) \qquad v|B-b \qquad u|B-2$$

Последовательность

$$\mathrm{arem}(\alpha_B(0), v), \mathrm{arem}(\alpha_B(1), v), \ldots, \mathrm{arem}(\alpha_B(n), v), \ldots$$

имеет период длины $2m$; последовательность

$$\mathrm{arem}(\alpha_B(0), u), \mathrm{arem}(\alpha_B(1), u), \ldots, \mathrm{arem}(\alpha_B(n), u), \ldots$$

имеет период длины u;

Ключевая идея

$$\mathfrak{N}_b^{*****} \quad = \quad \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, u)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1) \qquad v|B-b \qquad u|B-2$$

Последовательность

$$\mathrm{arem}(\alpha_B(0), v), \mathrm{arem}(\alpha_B(1), v), \ldots, \mathrm{arem}(\alpha_B(n), v), \ldots$$

имеет период длины $2m$; последовательность

$$\mathrm{arem}(\alpha_B(0), u), \mathrm{arem}(\alpha_B(1), u), \ldots, \mathrm{arem}(\alpha_B(n), u), \ldots$$

имеет период длины u; мы хотим, чтобы $u \mid m$.

Ключевая идея

$$\mathfrak{N}_b^{*****} \quad = \quad \{\langle \mathrm{arem}(x, v), \mathrm{arem}(x, u)\rangle : x \in \mathfrak{M}_B\}$$

$$v = \alpha_b(m+1) - \alpha_b(m-1) \qquad v|B-b \qquad u|B-2$$

Последовательность

$$\mathrm{arem}(\alpha_B(0), v), \mathrm{arem}(\alpha_B(1), v), \ldots, \mathrm{arem}(\alpha_B(n), v), \ldots$$

имеет период длины $2m$; последовательность

$$\mathrm{arem}(\alpha_B(0), u), \mathrm{arem}(\alpha_B(1), u), \ldots, \mathrm{arem}(\alpha_B(n), u), \ldots$$

имеет период длины u; мы хотим, чтобы $u \mid m$.

$$u = \alpha_b(\ell) \qquad u^2|\alpha_b(m)$$

Основная лемма. *Для любого числа b, такого что $b \geq 4$, и любых чисел x и k, равенство $x = \alpha_b(k)$ имеет место тогда и только тогда, когда существуют числа B, r, s, t, u, v, X, Y такие, что*

$$u^2 - but + t^2 = 1,$$
$$s^2 - bsr + r^2 = 1,$$
$$r < s,$$
$$u^2 \mid s,$$
$$v = bs - 2r,$$
$$v \mid B - b,$$
$$u \mid B - 2,$$
$$B \geq 4,$$
$$X^2 - BXY + Y^2 = 1,$$
$$2x < u,$$
$$x = \mathrm{arem}(X, v),$$
$$k = \mathrm{arem}(X, u).$$

Часть “тогда”

Если $b \geq 4$ *и числа* $x, k, B, r, s, t, u, v, X, Y$ *удовлетворяют условиям*

$$u^2 - but + t^2 = 1,$$
$$s^2 - bsr + r^2 = 1,$$
$$r < s, \qquad v = bs - 2r,$$
$$u^2 \mid s,$$
$$B \geq 4, \qquad X^2 - BXY + Y^2 = 1,$$
$$v \mid B - b,$$
$$u \mid B - 2,$$
$$2a < u,$$
$$x = \operatorname{arem}(X, v),$$
$$k = \operatorname{arem}(X, u).$$

то $x = \alpha_b(k)$.

Часть “тогда”

$$u^2 - but + t^2 = 1$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s \quad \Rightarrow \quad s = \alpha_b(m), \quad r = \alpha_b(m-1)$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s \quad \Rightarrow \quad s = \alpha_b(m), \quad r = \alpha_b(m-1)$$

$$v = bs - 2r$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s \quad \Rightarrow \quad s = \alpha_b(m), \quad r = \alpha_b(m-1)$$

$$v = bs - 2r \quad \Rightarrow \quad v = b\alpha_b(m) - 2\alpha_b(m-1)$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s \quad \Rightarrow \quad s = \alpha_b(m), \quad r = \alpha_b(m-1)$$

$$\begin{aligned} v = bs - 2r \quad &\Rightarrow \quad v = b\alpha_b(m) - 2\alpha_b(m-1) \\ &\Rightarrow \quad v = \alpha_b(m+1) - \alpha_b(m-1) \end{aligned}$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s \quad \Rightarrow \quad s = \alpha_b(m), \quad r = \alpha_b(m-1)$$

$$\begin{aligned} v = bs - 2r \quad &\Rightarrow \quad v = b\alpha_b(m) - 2\alpha_b(m-1) \\ &\Rightarrow \quad v = \alpha_b(m+1) - \alpha_b(m-1) \end{aligned}$$

$$u^2 \mid s$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s \quad \Rightarrow \quad s = \alpha_b(m), \quad r = \alpha_b(m-1)$$

$$\begin{aligned} v = bs - 2r \quad &\Rightarrow \quad v = b\alpha_b(m) - 2\alpha_b(m-1) \\ &\Rightarrow \quad v = \alpha_b(m+1) - \alpha_b(m-1) \end{aligned}$$

$$u^2 \mid s \quad \Rightarrow \quad (\alpha_b(\ell))^2 \mid \alpha_b(m)$$

Часть “тогда”

$$u^2 - but + t^2 = 1 \quad \Rightarrow \quad u = \alpha_b(\ell)$$

$$s^2 - bsr + r^2 = 1, \quad r < s \quad \Rightarrow \quad s = \alpha_b(m), \quad r = \alpha_b(m-1)$$

$$\begin{aligned} v = bs - 2r \quad &\Rightarrow \quad v = b\alpha_b(m) - 2\alpha_b(m-1) \\ &\Rightarrow \quad v = \alpha_b(m+1) - \alpha_b(m-1) \end{aligned}$$

$$\begin{aligned} u^2 \mid s \quad &\Rightarrow \quad (\alpha_b(\ell))^2 \mid \alpha_b(m) \\ &\Rightarrow \quad u \mid m \end{aligned}$$

Часть “тогда”

$$B \geq 4 \& X^2 - BXY + Y^2 = 1$$

Часть “тогда”

$$B \geq 4 \& X^2 - BXY + Y^2 = 1 \quad \Rightarrow \quad X = \alpha_B(n)$$

Часть “тогда”

$$B \geq 4 \& X^2 - BXY + Y^2 = 1 \quad \Rightarrow \quad X = \alpha_B(n)$$
$$\Rightarrow \quad X \equiv \alpha_b(n) \pmod{B - b}$$

Часть “тогда”

$$
\begin{aligned}
B \geq 4 \& X^2 - BXY + Y^2 = 1 \quad &\Rightarrow \quad X = \alpha_B(n) \\
&\Rightarrow \quad X \equiv \alpha_b(n) \pmod{B-b} \\
&\Rightarrow \quad X \equiv n \pmod{B-2}
\end{aligned}
$$

Часть “тогда”

$$
\begin{aligned}
B \geq 4 \& X^2 - BXY + Y^2 = 1 \quad &\Rightarrow \quad X = \alpha_B(n) \\
&\Rightarrow \quad X \equiv \alpha_b(n) \pmod{B-b} \\
&\Rightarrow \quad X \equiv n \pmod{B-2}
\end{aligned}
$$

$$
v \mid B - b
$$

Часть “тогда”

$$
\begin{aligned}
B \geq 4 \& X^2 - BXY + Y^2 = 1 \quad &\Rightarrow \quad X = \alpha_B(n) \\
&\Rightarrow \quad X \equiv \alpha_b(n) \pmod{B-b} \\
&\Rightarrow \quad X \equiv n \pmod{B-2}
\end{aligned}
$$

$$
v \mid B - b \quad \Rightarrow \quad X \equiv \alpha_b(n) \pmod{v},
$$

Часть “тогда”

$$
\begin{aligned}
B \geq 4 \& X^2 - BXY + Y^2 = 1 \quad &\Rightarrow \quad X = \alpha_B(n) \\
&\Rightarrow \quad X \equiv \alpha_b(n) \pmod{B-b} \\
&\Rightarrow \quad X \equiv n \pmod{B-2}
\end{aligned}
$$

$$
v \mid B - b \quad \Rightarrow \quad X \equiv \alpha_b(n) \pmod{v},
$$

$$
u \mid B - 2
$$

Часть “тогда”

$$
\begin{aligned}
B \geq 4 \& X^2 - BXY + Y^2 = 1 \quad &\Rightarrow \quad X = \alpha_B(n) \\
&\Rightarrow \quad X \equiv \alpha_b(n) \pmod{B-b} \\
&\Rightarrow \quad X \equiv n \pmod{B-2}
\end{aligned}
$$

$$
v \mid B - b \quad \Rightarrow \quad X \equiv \alpha_b(n) \pmod{v},
$$

$$
u \mid B - 2 \quad \Rightarrow \quad X \equiv n \pmod{u}
$$

Часть “тогда”

Пусть $j = \mathrm{arem}(n, 2m)$, то есть,

$$n = 2\ell m \pm j, \qquad j \leq m$$

Часть “тогда”

Пусть $j = \mathrm{arem}(n, 2m)$, то есть,

$$n = 2\ell m \pm j, \qquad j \leq m$$

$$A_b(n) \quad = \quad \Psi_b^n$$

Часть “тогда”

Пусть $j = \mathrm{arem}(n, 2m)$, то есть,

$$n = 2\ell m \pm j, \qquad j \leq m$$

$$\begin{aligned} A_b(n) &= \Psi_b^n \\ &= \Psi_b^{2\ell m \pm j} \end{aligned}$$

Часть “тогда”

Пусть $j = \mathrm{arem}(n, 2m)$, то есть,

$$n = 2\ell m \pm j, \qquad j \leq m$$

$$\begin{aligned} A_b(n) &= \Psi_b^n \\ &= \Psi_b^{2\ell m \pm j} \\ &= \left[[\Psi_b^m]^2\right]^\ell \Psi_b^{\pm j} \end{aligned}$$

Часть “тогда”

Пусть $j = \mathrm{arem}(n, 2m)$, то есть,

$$n = 2\ell m \pm j, \qquad j \leq m$$

$$\begin{aligned} A_b(n) &= \Psi_b^n \\ &= \Psi_b^{2\ell m \pm j} \\ &= \left[[\Psi_b^m]^2\right]^\ell \Psi_b^{\pm j} \\ &= \left[[A_b(m)]^2\right]^\ell [A_b(j)]^{\pm 1} \end{aligned}$$

Часть “тогда”

$$A_b(n) \quad = \quad \left[[A_b(m)]^2\right]^{\ell}[A_b(j)]^{\pm 1}$$

Часть “тогда”

$$A_b(n) \quad = \quad \left[[A_b(m)]^2\right]^{\ell}[A_b(j)]^{\pm 1}$$

$$A_b(m) \quad = \quad \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix}$$

Часть “тогда”

$$A_b(n) \;=\; \left[[A_b(m)]^2\right]^{\ell}[A_b(j)]^{\pm 1}$$

$$\begin{aligned} A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ &\equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} \pmod{v} \end{aligned}$$

Часть “тогда”

$$A_b(n) \;=\; \left[[A_b(m)]^2\right]^{\ell}[A_b(j)]^{\pm 1}$$

$$\begin{aligned}
A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\
&\equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} \pmod{v} \\
&= -[A_b(m)]^{-1} \\
[A_b(m)]^2 &\equiv -E \pmod{v} \\
A_b(n) &\equiv \pm[A_b(j)]^{\pm 1} \pmod{v}
\end{aligned}$$

Часть “тогда”

$$A_b(n) \;=\; \left[[A_b(m)]^2\right]^{\ell}[A_b(j)]^{\pm 1}$$

$$\begin{aligned}
A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\
&\equiv -\begin{pmatrix} -\alpha_b(m-1) & \alpha_b(m) \\ -\alpha_b(m) & \alpha_b(m+1) \end{pmatrix} \pmod{v} \\
&= -[A_b(m)]^{-1} \\
[A_b(m)]^2 &\equiv -E \pmod{v} \\
A_b(n) &\equiv \pm[A_b(j)]^{\pm 1} \pmod{v}
\end{aligned}$$

$$X \equiv \alpha_b(n) \equiv \pm\alpha_b(j) \pmod{v}$$

Часть “тогда”

$$x = \mathrm{arem}(X, v) = \alpha_b(j)$$

Часть “тогда”

$$x = \mathrm{arem}(X, v) = \alpha_b(j)$$

$$2\alpha_b(j) \leq 2\alpha_b(m) \leq (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v$$

Часть “тогда”

$$x = \mathrm{arem}(X, v) = \alpha_b(j)$$

$$2\alpha_b(j) \leq 2\alpha_b(m) \leq (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v$$

$$k = \mathrm{arem}(X, u) = \mathrm{arem}(n, u) = j$$

Часть “тогда”

$$x = \mathrm{arem}(X, v) = \alpha_b(j)$$

$$2\alpha_b(j) \leq 2\alpha_b(m) \leq (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v$$

$$k = \mathrm{arem}(X, u) = \mathrm{arem}(n, u) = j$$

$$2j \leq 2\alpha_b(j) = 2x < u$$

Часть “тогда”

$$x = \mathrm{arem}(X, v) = \alpha_b(j)$$

$$2\alpha_b(j) \leq 2\alpha_b(m) \leq (b-2)\alpha_b(m) < b\alpha_b(m) - 2\alpha_b(m-1) = v$$

$$k = \mathrm{arem}(X, u) = \mathrm{arem}(n, u) = j$$

$$2j \leq 2\alpha_b(j) = 2x < u$$

$$x = \alpha_b(k)$$

Часть “только тогда”

Для любых $b \geq 4, xk$, *если* $x = \alpha_b(k)$ *то найдутся числа* B, r, s, t, u, v, X, Y *такие, что*

$$u^2 - but + t^2 = 1,$$
$$s^2 - bsr + r^2 = 1, \qquad r < s,$$
$$v = bs - 2r,$$
$$u^2 \mid s,$$
$$B \geq 4, \qquad X^2 - BXY + Y^2 = 1,$$
$$v \mid B - b,$$
$$u \mid B - 2,$$
$$2x < u,$$
$$x = \operatorname{arem}(X, v),$$
$$k = \operatorname{arem}(X, u).$$

Часть “только тогда”

$$u = \alpha_b(\ell), t = \alpha_b(\ell + 1) \quad \Rightarrow \quad u^2 - but + t^2 = 1$$

Часть “только тогда”

$$u = \alpha_b(\ell), t = \alpha_b(\ell + 1) \quad \Rightarrow \quad u^2 - but + t^2 = 1$$
$$\ell \text{ велико} \quad \Rightarrow \quad 2x < u$$

Часть “только тогда”

$$
\begin{aligned}
u = \alpha_b(\ell), t = \alpha_b(\ell+1) \quad &\Rightarrow \quad u^2 - but + t^2 = 1 \\
\ell \text{ велико} \quad &\Rightarrow \quad 2x < u \\
&\qquad\quad u \equiv 1 \pmod 2
\end{aligned}
$$

Часть “только тогда”

$$\begin{aligned} u = \alpha_b(\ell), t = \alpha_b(\ell+1) &\Rightarrow u^2 - but + t^2 = 1 \\ \ell \text{ велико} &\Rightarrow 2x < u \\ &\quad u \equiv 1 \pmod 2 \end{aligned}$$

$$\begin{aligned} s = \alpha_b(m+1), \quad r = \alpha_b(m) &\Rightarrow s^2 - bsr + r^2 = 1 \\ &\Rightarrow r < s \end{aligned}$$

Часть “только тогда”

$$
\begin{aligned}
u = \alpha_b(\ell), t = \alpha_b(\ell+1) &\Rightarrow u^2 - but + t^2 = 1 \\
\ell \text{ велико} &\Rightarrow 2x < u \\
&\quad u \equiv 1 \pmod 2
\end{aligned}
$$

$$
\begin{aligned}
s = \alpha_b(m+1), \quad r = \alpha_b(m) &\Rightarrow s^2 - bsr + r^2 = 1 \\
&\Rightarrow r < s \\
m = \ell u &\Rightarrow u^2 \mid s
\end{aligned}
$$

Часть “только тогда”

$$\begin{aligned} u = \alpha_b(\ell), t = \alpha_b(\ell+1) &\Rightarrow u^2 - but + t^2 = 1 \\ \ell \text{ велико} &\Rightarrow 2x < u \\ &\quad u \equiv 1 \pmod 2 \end{aligned}$$

$$\begin{aligned} s = \alpha_b(m+1), \quad r = \alpha_b(m) &\Rightarrow s^2 - bsr + r^2 = 1 \\ &\Rightarrow r < s \\ m = \ell u &\Rightarrow u^2 \mid s \end{aligned}$$

$$v = bs - 2r$$

Часть “только тогда”

$$\begin{aligned} u = \alpha_b(\ell), t = \alpha_b(\ell+1) &\Rightarrow u^2 - but + t^2 = 1 \\ \ell \text{ велико} &\Rightarrow 2x < u \\ &\quad u \equiv 1 \pmod 2 \end{aligned}$$

$$\begin{aligned} s = \alpha_b(m+1), \quad r = \alpha_b(m) &\Rightarrow s^2 - bsr + r^2 = 1 \\ &\Rightarrow r < s \\ m = \ell u &\Rightarrow u^2 \mid s \end{aligned}$$

$$v = \quad bs - 2r \quad \geq 4\alpha_b(m) - 2\alpha_b(m-1)$$

Часть “только тогда”

$$\begin{aligned} u = \alpha_b(\ell), t = \alpha_b(\ell+1) &\Rightarrow u^2 - but + t^2 = 1 \\ \ell \text{ велико} &\Rightarrow 2x < u \\ &\quad u \equiv 1 \pmod 2 \end{aligned}$$

$$\begin{aligned} s = \alpha_b(m+1), \quad r = \alpha_b(m) &\Rightarrow s^2 - bsr + r^2 = 1 \\ &\Rightarrow r < s \\ m = \ell u &\Rightarrow u^2 \mid s \end{aligned}$$

$$\begin{aligned} v = \quad bs - 2r \quad &\geq 4\alpha_b(m) - 2\alpha_b(m-1) \\ &> 2\alpha_b(m) \geq 0 \end{aligned}$$

Часть “только тогда”

$$B \geq 4, \quad v \mid B - b, \quad u \mid B - 2$$

$$B \equiv b \pmod{v}, \quad B \equiv 2 \pmod{u}$$

Часть “только тогда”

$$B \geq 4, \quad v \mid B - b, \quad u \mid B - 2$$

$$B \equiv b \pmod{v}, \quad B \equiv 2 \pmod{u}$$

$$d \mid u$$
$$d \mid v$$

Часть “только тогда”

$$B \geq 4, \quad v \mid B - b, \quad u \mid B - 2$$

$$B \equiv b \pmod{v}, \quad B \equiv 2 \pmod{u}$$

$$\begin{aligned} & d \mid u \\ & d \mid v \\ u^2 \mid s \quad \Rightarrow \quad & d \mid s \end{aligned}$$

Часть “только тогда”

$$B \geq 4, \quad v \mid B - b, \quad u \mid B - 2$$

$$B \equiv b \pmod{v}, \quad B \equiv 2 \pmod{u}$$

$$\begin{aligned} & & d \mid u \\ & & d \mid v \\ u^2 \mid s & \Rightarrow & d \mid s \\ v = bs - 2r & \Rightarrow & d \mid 2r \end{aligned}$$

Часть “только тогда”

$$B \geq 4, \quad v \mid B - b, \quad u \mid B - 2$$

$$B \equiv b \pmod{v}, \quad B \equiv 2 \pmod{u}$$

$$\begin{aligned} & & d \mid u \\ & & d \mid v \\ u^2 \mid s & \Rightarrow & d \mid s \\ v = bs - 2r & \Rightarrow & d \mid 2r \\ u \equiv 1 \pmod{2} & \Rightarrow & d \mid r \end{aligned}$$

Часть “только тогда”

$$B \geq 4, \quad v \mid B - b, \quad u \mid B - 2$$

$$B \equiv b \pmod{v}, \quad B \equiv 2 \pmod{u}$$

$$\begin{aligned}
& & d &\mid u \\
& & d &\mid v \\
u^2 \mid s & \Rightarrow & d &\mid s \\
v = bs - 2r & \Rightarrow & d &\mid 2r \\
u \equiv 1 \pmod{2} & \Rightarrow & d &\mid r \\
s^2 - bsr + r^2 = 1 & \Rightarrow & d &\mid 1
\end{aligned}$$

Часть “только тогда”

$$B \geq 4, \quad v \mid B - b, \quad u \mid B - 2$$

$$B \equiv b \pmod{v}, \quad B \equiv 2 \pmod{u}$$

$$\begin{aligned}
& & d &\mid u \\
& & d &\mid v \\
u^2 \mid s & \Rightarrow & d &\mid s \\
v = bs - 2r & \Rightarrow & d &\mid 2r \\
u \equiv 1 \pmod{2} & \Rightarrow & d &\mid r \\
s^2 - bsr + r^2 = 1 & \Rightarrow & d &\mid 1 \\
& \Rightarrow & d &= 1
\end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), Y = \alpha_B(k+1) \quad \Rightarrow \quad X^2 - BXY + Y^2 = 1$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \mathrm{arem}(X, v)$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \mathrm{arem}(X, v)$$

$$\alpha_B(k) \equiv \alpha_b(k) \pmod{B-b}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \mathrm{arem}(X, v)$$

$$\begin{aligned} \alpha_B(k) &\equiv \alpha_b(k) \pmod{B-b} \\ X &\equiv x \pmod{B-b} \end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \mathrm{arem}(X, v)$$

$$\begin{aligned} \alpha_B(k) &\equiv \alpha_b(k) \pmod{B-b} \\ X &\equiv x \pmod{B-b} \\ v \mid B-b \Rightarrow X &\equiv x \pmod{v} \end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \mathrm{arem}(X, v)$$

$$\begin{aligned} \alpha_B(k) &\equiv \alpha_b(k) \pmod{B-b} \\ X &\equiv x \pmod{B-b} \\ v \mid B-b \Rightarrow X &\equiv x \pmod{v} \end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \mathrm{arem}(X, v)$$

$$\begin{aligned} \alpha_B(k) &\equiv \alpha_b(k) \pmod{B-b} \\ X &\equiv x \pmod{B-b} \\ v \mid B-b \Rightarrow X &\equiv x \pmod{v} \end{aligned}$$

$$v = bs - 2r \geq 4\alpha_b(m) - 2\alpha_b(m-1)$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \mathrm{arem}(X, v)$$

$$\begin{aligned} \alpha_B(k) &\equiv \alpha_b(k) \pmod{B-b} \\ X &\equiv x \pmod{B-b} \\ v \mid B-b \Rightarrow X &\equiv x \pmod{v} \end{aligned}$$

$$\begin{aligned} v = \quad bs - 2r &\geq 4\alpha_b(m) - 2\alpha_b(m-1) \\ &> \alpha_b(m) = \alpha_b(\ell u) \end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$x = \operatorname{arem}(X, v)$$

$$\begin{aligned} \alpha_B(k) &\equiv \alpha_b(k) \pmod{B-b} \\ X &\equiv x \pmod{B-b} \\ v \mid B-b \Rightarrow X &\equiv x \pmod{v} \end{aligned}$$

$$\begin{aligned} v = \quad bs - 2r &\geq 4\alpha_b(m) - 2\alpha_b(m-1) \\ &> \alpha_b(m) = \alpha_b(\ell u) \\ &\geq \alpha_b(\ell) = u > 2x \end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$k = \mathrm{arem}(X, u)$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$k = \mathrm{arem}(X, u)$$

$$\alpha_B(k) \equiv \alpha_2(k) \pmod{B-2}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$k = \operatorname{arem}(X, u)$$

$$\alpha_B(k) \equiv \alpha_2(k) \pmod{B-2}$$
$$X \equiv k \pmod{B-2}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$k = \operatorname{arem}(X, u)$$

$$\begin{aligned} & \alpha_B(k) \equiv \alpha_2(k) \pmod{B-2} \\ & X \equiv k \pmod{B-2} \\ u \mid B-2 \quad \Rightarrow \quad & X \equiv k \pmod{u} \end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$k = \operatorname{arem}(X, u)$$

$$\begin{aligned} & \alpha_B(k) \equiv \alpha_2(k) \pmod{B-2} \\ & X \equiv k \pmod{B-2} \\ u \mid B-2 \quad \Rightarrow \quad & X \equiv k \pmod{u} \end{aligned}$$

Часть “только тогда”

$$X = \alpha_B(k), \qquad Y = \alpha_B(k+1)$$

$$k = \operatorname{arem}(X, u)$$

$$\begin{aligned} & \alpha_B(k) \equiv \alpha_2(k) \pmod{B-2} \\ & X \equiv k \pmod{B-2} \\ u \mid B-2 \quad \Rightarrow \quad & X \equiv k \pmod{u} \end{aligned}$$

$$2x < u$$