

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

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

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

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

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

$$\begin{aligned} \langle a_1, \dots, a_n \rangle \in \mathfrak{M} &\iff \\ &\iff \exists x_1 \dots x_m \{ E_L(a_1, \dots, a_n, x_1, x_2, \dots, x_m) = \\ &= E_R(a_1, \dots, a_n, x_1, x_2, \dots, x_m) \} \end{aligned}$$

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

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

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

$$\begin{aligned} \langle a_1, \dots, a_n \rangle \in \mathfrak{M} &\iff \\ &\iff \exists x_1 \dots x_m \{ E_L(a_1, \dots, a_n, x_1, x_2, \dots, x_m) = \\ &= E_R(a_1, \dots, a_n, x_1, x_2, \dots, x_m) \} \end{aligned}$$

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

## Рекуррентные последовательности второго порядка

## Рекуррентные последовательности второго порядка

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

## Рекуррентные последовательности второго порядка

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

$$0 < 1 < \alpha_b(2) < \dots < \alpha_b(n) < \alpha_b(n+1) < \dots$$

## Рекуррентные последовательности второго порядка

$$\alpha_2(0), \alpha_2(1), \dots, \alpha_2(n), \dots$$

## Рекуррентные последовательности второго порядка

$$\alpha_2(0), \alpha_2(1), \dots, \alpha_2(n), \dots$$



## Рекуррентные последовательности второго порядка

$$\alpha_2(0), \alpha_2(1), \dots, \alpha_2(n), \dots$$

$$0, 1, 2, 3, 4, 5, \dots$$

## Рекуррентные последовательности второго порядка

$$\alpha_2(0), \alpha_2(1), \dots, \alpha_2(n), \dots$$

$$0, 1, 2, 3, 4, 5, \dots$$

$$\alpha_2(n+2) = 2\alpha_2(n+1) - \alpha_2(n)$$

## Рекуррентные последовательности второго порядка

$$\alpha_2(0), \alpha_2(1), \dots, \alpha_2(n), \dots$$

$$0, 1, 2, 3, 4, 5, \dots$$

$$\begin{aligned}\alpha_2(n+2) &= 2\alpha_2(n+1) - \alpha_2(n) \\ &= 2(n+1) - n\end{aligned}$$

## Рекуррентные последовательности второго порядка

$$\alpha_2(0), \alpha_2(1), \dots, \alpha_2(n), \dots$$

$$0, 1, 2, 3, 4, 5, \dots$$

$$\begin{aligned}\alpha_2(n+2) &= 2\alpha_2(n+1) - \alpha_2(n) \\ &= 2(n+1) - n \\ &= n+2\end{aligned}$$

## Диофантовость последовательности $\alpha_b(k)$

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

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

## Диофантовость последовательности $\alpha_b(k)$

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

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

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

## Матричное представление

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

## 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

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

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

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

## Матричное представление

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

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

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

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

## Матричное представление

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

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

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

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

## Матричное представление

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

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

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

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

$$A_b(n+1) = A_b(n)\Psi$$

## Характеристическое уравнение

$$\det(A_b(n)) = \alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1)$$

## Характеристическое уравнение

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

## Характеристическое уравнение

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

## Характеристическое уравнение

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



## Характеристическое уравнение

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

## Характеристическое уравнение

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

## Характеристическое уравнение

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

## 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

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

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

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

## Характеристическое уравнение

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

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

## 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  $x = \alpha_b(n+1)$ ,  $y = \alpha_b(n)$ .

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$



## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

**Доказательство.**

$$m = n + kl, \quad 0 \leq n < k$$

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

**Доказательство.**

$$m = n + kl, \quad 0 \leq n < k$$

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

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

**Доказательство.**

$$m = n + kl, \quad 0 \leq n < k$$

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

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

**Доказательство.**

$$m = n + kl, \quad 0 \leq n < k$$

$$\begin{aligned} A_b(m) &= \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \\ &= \Psi_b^m \\ &= \Psi_b^{n+kl} \end{aligned}$$

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

**Доказательство.**

$$m = n + k\ell, \quad 0 \leq n < k$$

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

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

**Доказательство.**

$$m = n + k\ell, \quad 0 \leq n < k$$

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

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

**Доказательство.**

$$m = n + k\ell, \quad 0 \leq n < k$$

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

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^{\ell} \pmod{\alpha_b(k)}$$



## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

$$\begin{aligned} & \begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \\ & \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^\ell \pmod{\alpha_b(k)} \\ & \alpha_b(m) \equiv \alpha_b(n)\alpha_b^\ell(k+1) \pmod{\alpha_b(k)} \end{aligned}$$

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^{\ell} \pmod{\alpha_b(k)}$$

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^{\ell}(k+1) \pmod{\alpha_b(k)}$$

$$\alpha_b(k) \mid \alpha_b(n)$$

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^\ell \pmod{\alpha_b(k)}$$

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^\ell(k+1) \pmod{\alpha_b(k)}$$

$$\alpha_b(k) \mid \alpha_b(n)$$

$$m = n + k\ell, \quad 0 \leq n < k$$

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^\ell \pmod{\alpha_b(k)}$$

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b^\ell(k+1) \pmod{\alpha_b(k)}$$

$$\alpha_b(k) \mid \alpha_b(n)$$

$$m = n + k\ell, \quad 0 \leq n < k$$

$$n = 0 \quad m = k\ell$$

## Свойства делимости

$$m = k\ell$$

$$A_b(m) = A_b^\ell(k)$$

## Свойства делимости

$$m = k\ell$$

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

## Свойства делимости

$$m = k\ell$$

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

## Свойства делимости

$$m = k\ell$$

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



## Свойства делимости

$$m = k\ell$$

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

## Свойства делимости

$$m = k\ell$$

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

## Свойства делимости

$$m = k\ell$$

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

## Свойства делимости

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

## Свойства делимости

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

## Свойства делимости

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

## Свойства делимости

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

## Свойства делимости

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



## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

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

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

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

$$\alpha_b(k) \mid \ell \alpha_b^{\ell-1}(k-1)$$

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

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

$$\alpha_b(k) \mid \ell \alpha_b^{\ell-1}(k-1)$$

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

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

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

$$\alpha_b(k) \mid \ell \alpha_b^{\ell-1}(k-1)$$

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

$$m = k\ell$$

## Свойства делимости

**Лемма.**  $\alpha_b^2(k) \mid \alpha_b(m) \Rightarrow k\alpha_b(k) \mid m$

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

$$\alpha_b(k) \mid \ell \alpha_b^{\ell-1}(k-1)$$

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

$$m = k\ell$$

## 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).**

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

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



## Новые свойства делимости

**Лемма (доказанная).**

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

**Лемма (обратная).**

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

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

## Первый шаг

$$x \in \mathfrak{M}_b \iff x \in \{0, 1, b, \dots, \alpha_b(n), \dots\}$$

## Первый шаг

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

## Первый шаг

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

## Первый шаг

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

$$\begin{aligned}\langle x, k \rangle \in \mathfrak{N}_b &\iff x = \alpha_b(k) \\ &\alpha_2(n) = n\end{aligned}$$

## Первый шаг

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

$$\begin{aligned}\langle x, k \rangle \in \mathfrak{N}_b &\iff x = \alpha_b(k) \\ &\alpha_2(n) = n\end{aligned}$$

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

## Первый шаг

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

$$\begin{aligned}\langle x, k \rangle \in \mathfrak{N}_b &\iff x = \alpha_b(k) \\ &\alpha_2(n) = n\end{aligned}$$

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

## Первый шаг

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

$$\begin{aligned}\langle x, k \rangle \in \mathfrak{N}_b &\iff x = \alpha_b(k) \\ &\alpha_2(n) = n\end{aligned}$$

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



## Первый шаг

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

$$\begin{aligned}\langle x, k \rangle \in \mathfrak{N}_b &\iff x = \alpha_b(k) \\ &\alpha_2(n) = n\end{aligned}$$

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

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

## Первый шаг

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

$$\begin{aligned}\langle x, k \rangle \in \mathfrak{N}_b &\iff x = \alpha_b(k) \\ &\alpha_2(n) = n\end{aligned}$$

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

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

## Второй шаг

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

## Второй шаг

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

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

## Сравнение последовательностей

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

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

## Сравнение последовательностей

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

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

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

## Функции rem и arem

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

## Функции rem и arem

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

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



## 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

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

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

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

## Сравнение последовательностей

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

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

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

## Сравнение последовательностей

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

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

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

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

## Второй шаг

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

## Второй шаг

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

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

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



## Третий шаг

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

## Третий шаг

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

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

## Периодичность

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

## Периодичность

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

$$\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(n) \pmod{\nu}, \dots$$

## Периодичность

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

$$\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(n) \pmod{\nu}, \dots$$

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

## Периодичность

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

$$\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(n) \pmod{\nu}, \dots$$

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

$$\alpha_b(m + 1) \equiv \alpha_b(m + 1 + p) \pmod{\nu}$$

## Периодичность

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

$$\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(n) \pmod{\nu}, \dots$$

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

$$\alpha_b(m + 1) \equiv \alpha_b(m + 1 + p) \pmod{\nu}$$

$$\alpha_b(m + 2) \equiv \alpha_b(m + 2 + p) \pmod{\nu}$$

## Периодичность

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

$$\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(n) \pmod{\nu}, \dots$$

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

$$\alpha_b(m + 1) \equiv \alpha_b(m + 1 + p) \pmod{\nu}$$

$$\alpha_b(m + 2) \equiv \alpha_b(m + 2 + p) \pmod{\nu}$$

$$\alpha_b(m + 3) \equiv \alpha_b(m + 3 + p) \pmod{\nu}$$



## Периодичность

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

$$\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(n) \pmod{\nu}, \dots$$

$$\alpha_b(m-1) \equiv \alpha_b(m-1+p) \pmod{\nu}$$

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

$$\alpha_b(m+1) \equiv \alpha_b(m+1+p) \pmod{\nu}$$

$$\alpha_b(m+2) \equiv \alpha_b(m+2+p) \pmod{\nu}$$

$$\alpha_b(m+3) \equiv \alpha_b(m+3+p) \pmod{\nu}$$

## Периодичность

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

$$\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(n) \pmod{\nu}, \dots$$

$$\alpha_b(m-1) \equiv \alpha_b(m-1+p) \pmod{\nu}$$

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

$$\alpha_b(m+1) \equiv \alpha_b(m+1+p) \pmod{\nu}$$

$$\alpha_b(m+2) \equiv \alpha_b(m+2+p) \pmod{\nu}$$

$$\alpha_b(m+3) \equiv \alpha_b(m+3+p) \pmod{\nu}$$

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

## Специальный период

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

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

$$\alpha_b(1) \equiv \alpha_b(1) = 1 \pmod{v}$$

$$\vdots \equiv \vdots$$

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

$$\alpha_b(m+1) \equiv \alpha_b(m-1) \pmod{v}$$

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

$$\alpha_b(m+3) \equiv \alpha_b(m-3) \pmod{v}$$

$$\vdots \equiv \vdots$$

$$\alpha_b(2m-1) \equiv \alpha_b(1) \pmod{v}$$

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

$$\alpha_b(2m+1) \equiv \alpha_b(-1) = -1 = -\alpha_b(1) \pmod{v}$$

## Специальный период

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

## Специальный период

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

При  $\nu = \alpha_b(m+1) - \alpha_b(m-1)$  последовательность  $\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(1) \pmod{\nu}, \dots$  имеет период длины  $4m$

## Специальный период

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

При  $\nu = \alpha_b(m+1) - \alpha_b(m-1)$  последовательность  $\alpha_b(0) \pmod{\nu}, \alpha_b(1) \pmod{\nu}, \dots, \alpha_b(1) \pmod{\nu}, \dots$  имеет период длины  $4m$ , а последовательность  $\text{arem}(\alpha_b(0), \nu), \text{arem}(\alpha_b(1), \nu), \dots, \text{arem}(\alpha_b(n), \nu), \dots$  имеет период длины  $2m$ .

## Четвертый шаг

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

## Четвертый шаг

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

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



## Четвертый шаг

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

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

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

## Четвертый шаг

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

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

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

$$v | B - b$$

## Четвертый шаг

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

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

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

$$v | B - b$$

## Пятый шаг

$$\mathfrak{M}_b^{****} = \{ \langle \text{arem}(x, \nu), \text{arem}(x, b - 2) \rangle : x \in \mathfrak{M}_B \}$$

## Пятый шаг

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

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

## Пятый шаг

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

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

$$v | B - b$$

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

## Пятый шаг

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

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

$$v | B - b$$

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

$$u | B - 2$$

Ключевая идея



## Ключевая идея

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

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

## Ключевая идея

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

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

Последовательность

$$\text{arem}(\alpha_B(0), v), \text{arem}(\alpha_B(1), v), \dots, \text{arem}(\alpha_B(n), v), \dots$$

имеет период длины  $2m$ ; последовательность

$$\text{arem}(\alpha_B(0), u), \text{arem}(\alpha_B(1), u), \dots, \text{arem}(\alpha_B(n), u), \dots$$

имеет период длины  $u$ ;

## Ключевая идея

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

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

Последовательность

$$\text{arem}(\alpha_B(0), v), \text{arem}(\alpha_B(1), v), \dots, \text{arem}(\alpha_B(n), v), \dots$$

имеет период длины  $2m$ ; последовательность

$$\text{arem}(\alpha_B(0), u), \text{arem}(\alpha_B(1), u), \dots, \text{arem}(\alpha_B(n), u), \dots$$

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

## Ключевая идея

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

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

Последовательность

$$\text{arem}(\alpha_B(0), v), \text{arem}(\alpha_B(1), v), \dots, \text{arem}(\alpha_B(n), v), \dots$$

имеет период длины  $2m$ ; последовательность

$$\text{arem}(\alpha_B(0), u), \text{arem}(\alpha_B(1), u), \dots, \text{arem}(\alpha_B(n), u), \dots$$

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

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

**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

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

$$s^2 - bsr + r^2 = 1,$$

$$r < s,$$

$$u^2 \mid s,$$

$$v = bs - 2r,$$

$$v \mid B - b,$$

$$u \mid B - 2,$$

$$B \geq 4,$$

$$X^2 - BXY + Y^2 = 1,$$

$$2x < u,$$

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

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

## Часть “тогда”

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

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

$$s^2 - bsr + r^2 = 1,$$

$$r < s, \quad v = bs - 2r,$$

$$u^2 \mid s,$$

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

$$v \mid B - b,$$

$$u \mid B - 2,$$

$$2a < u,$$

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

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

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”

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

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

$$v = bs - 2r$$

Часть “тогда”

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

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

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

## Часть “тогда”

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

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

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

## Часть “тогда”

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

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

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

$$u^2 \mid s$$

## Часть “тогда”

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

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

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

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

## Часть “тогда”

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

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

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

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



Часть “тогда”

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

Часть “тогда”

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

## Часть “тогда”

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

## Часть “тогда”

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

## Часть “тогда”

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

$$v \mid B - b$$

## Часть “тогда”

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

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

## Часть “тогда”

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

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

$$u \mid B - 2$$

## Часть “тогда”

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

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

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



## Часть “тогда”

Let  $j = \text{arem}(n, 2m)$ , that is,

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

## Часть “тогда”

Let  $j = \text{arem}(n, 2m)$ , that is,

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

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

## Часть “тогда”

Let  $j = \text{arem}(n, 2m)$ , that is,

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

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

## Часть “тогда”

Let  $j = \text{arem}(n, 2m)$ , that is,

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

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

## Часть “тогда”

Let  $j = \text{arem}(n, 2m)$ , that is,

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

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

Часть “тогда”

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

Часть “тогда”

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

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

## Часть “тогда”

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

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



## Часть “тогда”

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

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

$$[A_b(m)]^2 \equiv -E \pmod{\nu}$$

$$A_b(n) \equiv \pm [A_b(j)]^{\pm 1} \pmod{\nu}$$

## Часть “тогда”

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

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

$$[A_b(m)]^2 \equiv -E \pmod{\nu}$$

$$A_b(n) \equiv \pm [A_b(j)]^{\pm 1} \pmod{\nu}$$

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

Часть “тогда”

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

Часть “тогда”

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

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

Часть “тогда”

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

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

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

Часть “тогда”

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

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

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

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

## Часть “тогда”

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

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

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

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

$$x = \alpha_b(k)$$

## Часть “только тогда”

For every  $b \geq 4, x, k$ , if  $x = \alpha_b(k)$  then there are numbers  $x, k, B, r, s, t, u, v, X, Y$  are such that

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

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

$$v = bs - 2r,$$

$$u^2 \mid s,$$

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

$$v \mid B - b,$$

$$u \mid B - 2,$$

$$2x < u,$$

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

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



Часть “только тогда”

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

## Часть “только тогда”

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

$$\ell \text{ велико} \Rightarrow 2x < u$$

## Часть “только тогда”

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

$$\ell \text{ велико} \Rightarrow 2x < u$$

$$u \equiv 1 \pmod{2}$$

## Часть “только тогда”

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

$$\ell \text{ велико} \Rightarrow 2x < u$$

$$u \equiv 1 \pmod{2}$$

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

$$\Rightarrow r < s$$

## Часть “только тогда”

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

$$\ell \text{ велико} \Rightarrow 2x < u$$

$$u \equiv 1 \pmod{2}$$

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

$$\Rightarrow r < s$$

$$m = \ell u \Rightarrow u^2 \mid s$$

## Часть “только тогда”

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

$$\ell \text{ велико} \Rightarrow 2x < u$$

$$u \equiv 1 \pmod{2}$$

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

$$\Rightarrow r < s$$

$$m = \ell u \Rightarrow u^2 \mid s$$

$$v = bs - 2r$$

## Часть “только тогда”

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

$$\ell \text{ велико} \Rightarrow 2x < u$$

$$u \equiv 1 \pmod{2}$$

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

$$\Rightarrow r < s$$

$$m = \ell u \Rightarrow u^2 \mid s$$

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

## Часть “только тогда”

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

$$\ell \text{ велико} \Rightarrow 2x < u$$

$$u \equiv 1 \pmod{2}$$

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

$$\Rightarrow r < s$$

$$m = \ell u \Rightarrow u^2 \mid s$$

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

$$> 2\alpha_b(m) \geq 0$$



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”

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

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

$$d \mid u$$

$$d \mid v$$

$$u^2 \mid s \Rightarrow d \mid s$$

## Часть “только тогда”

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

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

$$d \mid u$$

$$d \mid v$$

$$u^2 \mid s \Rightarrow d \mid s$$

$$v = bs - 2r \Rightarrow d \mid 2r$$

## Часть “только тогда”

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

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

$$d \mid u$$

$$d \mid v$$

$$u^2 \mid s \Rightarrow d \mid s$$

$$v = bs - 2r \Rightarrow d \mid 2r$$

$$u \equiv 1 \pmod{2} \Rightarrow d \mid r$$

## Часть “только тогда”

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

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

$$d \mid u$$

$$d \mid v$$

$$u^2 \mid s \Rightarrow d \mid s$$

$$v = bs - 2r \Rightarrow d \mid 2r$$

$$u \equiv 1 \pmod{2} \Rightarrow d \mid r$$

$$s^2 - bsr + r^2 = 1 \Rightarrow d \mid 1$$

## Часть “только тогда”

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

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

$$d \mid u$$

$$d \mid v$$

$$u^2 \mid s \Rightarrow d \mid s$$

$$v = bs - 2r \Rightarrow d \mid 2r$$

$$u \equiv 1 \pmod{2} \Rightarrow d \mid r$$

$$s^2 - bsr + r^2 = 1 \Rightarrow d \mid 1$$

$$\Rightarrow d = 1$$

Часть “только тогда”

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



Часть “только тогда”

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

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

## Часть “только тогда”

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

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

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

$$X \equiv x \pmod{B - b}$$

$$v \mid B - b \Rightarrow X \equiv x \pmod{v}$$

## Часть “только тогда”

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

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

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

$$X \equiv x \pmod{B - b}$$

$$v \mid B - b \Rightarrow X \equiv x \pmod{v}$$

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

$$> \alpha_b(m) = \alpha_b(\ell u)$$

$$\geq \alpha_b(\ell) = u > 2x$$

Часть “только тогда”

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

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

## Часть “только тогда”

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

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

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

$$X \equiv k \pmod{B - 2}$$

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

$$2x < u$$