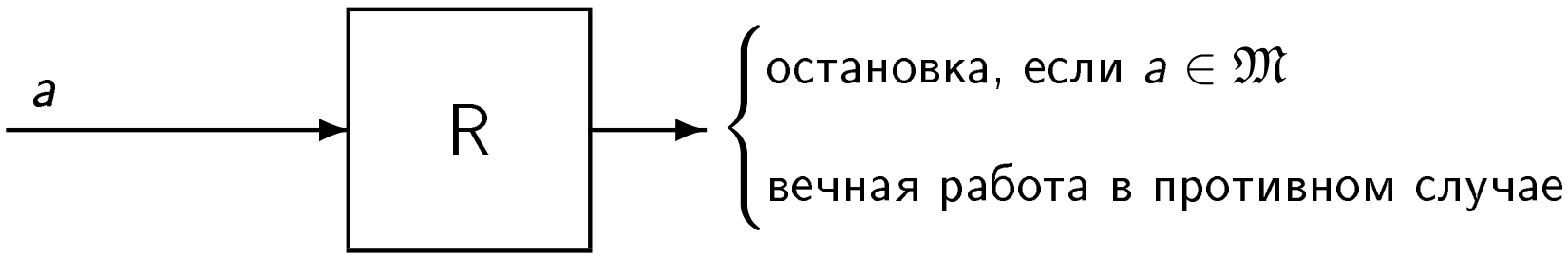
Гипотеза Martin'a Davis'a (=DPRM-теорема)

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

Перечислимые множества

Определение. Множество $\mathfrak{M}$ натуральных чисел называется *перечислимым*, если можно написать программу R для регистровой машины, такую что



При запуске машины число a помещено в регистр R1, все остальные регистры содержат нули.

От регистровой машины к диофантову уравнению

От регистровой машины к диофантову уравнению

1. Преобразовать программу так, чтобы в момент остановки все регистры были пустыми.

От регистровой машины к диофантову уравнению

1. Преобразовать программу так, чтобы в момент остановки все регистры были пустыми.
2. Описать работу регистровой машины соотношениями между содержимым протокола в соседние моменты времени

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^{+} s_{k,t} - \sum_{\ell}^{-} z_{\ell n,t} s_{k,t}$$

$$s_{d,t+1} = \sum_{d}^{+} s_{k,t} + \sum_{d}^{-} z_{\ell,t} s_{k,t} + \sum_{d}^{0} (1 - z_{\ell,t}) s_{k,t}$$

$$z_{\ell,t} = \begin{cases} 1, \text{ если } r_{\ell,t} > 0 \\ 0 \text{ в противном случае} \end{cases}$$

От регистровой машины к диофантову уравнению

1. Преобразовать программу так, чтобы в момент остановки все регистры были пустыми.
2. Описать работу регистровой машины соотношениями между содержимым протокола в соседние моменты времени

$$r_{\ell,t+1} = r_{\ell,t} + \sum_{\ell}^{+} s_{k,t} - \sum_{\ell}^{-} z_{\ell n,t} s_{k,t}$$

$$s_{d,t+1} = \sum_{d}^{+} s_{k,t} + \sum_{d}^{-} z_{\ell,t} s_{k,t} + \sum_{d}^{0} (1 - z_{\ell,t}) s_{k,t}$$

$$z_{\ell,t} = \begin{cases} 1, \text{ если } r_{\ell,t} > 0 \\ 0 \text{ в противном случае} \end{cases}$$

и добавить начальные и конечные условия

$$r_{1,0} = a \qquad r_{2,0} = \cdots = r_{n,0} = 0$$

$$s_{1,0} = 1 \qquad s_{2,0} = \cdots = s_{m,0} = 0$$

$$s_{m,q} = 1 \qquad s_{1,q} = \cdots = s_{m-1,q} = 0$$

$$r_{1,q} = \cdots = r_{n,q} = 0$$

От регистровой машины к диофантову уравнению

3. Описать работу регистровой машины соотношениями между закодированным содержимым протокола:

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} \quad = \quad br_\ell + b\sum\nolimits_\ell^+ s_k - b\sum\nolimits_\ell^- (z_\ell \wedge s_k)$$

$$s_d - s_{d,0} = b\sum\nolimits_d^+ s_k + b\sum\nolimits_d^+ (z_\ell \wedge s_k) + b\sum\nolimits_d^0 ((e - z_\ell) \wedge s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^c f \wedge ((2^c - 1)f + r_\ell) = 2^c z_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

$$2^c f \wedge r_\ell = 0 \qquad s_m = b^q$$

От регистровой машины к диофантову уравнению

3. Описать работу регистровой машины соотношениями между закодированным содержимым протокола:

$$b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} \quad = \quad br_\ell + b\sum\nolimits_\ell^+ s_k - b\sum\nolimits_\ell^- (z_\ell \wedge s_k)$$

$$s_d - s_{d,0} = b\sum\nolimits_d^+ s_k + b\sum\nolimits_d^+ (z_\ell \wedge s_k) + b\sum\nolimits_d^0 ((e - z_\ell) \wedge s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^c f \wedge ((2^c - 1)f + r_\ell) = 2^c z_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

$$2^c f \wedge r_\ell = 0 \qquad s_m = b^q$$

От регистровой машины к диофантову уравнению

3. Описать работу регистровой машины соотношениями между закодированным содержимым протокола:

$$2a = 2r_{\ell,0} < b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} \quad = \quad br_\ell + b\sum\nolimits_\ell^+ s_k - b\sum\nolimits_\ell^- (z_\ell \wedge s_k)$$

$$s_d - s_{d,0} = b\sum\nolimits_d^+ s_k + b\sum\nolimits_d^+ (z_\ell \wedge s_k) + b\sum\nolimits_d^0 ((e - z_\ell) \wedge s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^c f \wedge ((2^c - 1)f + r_\ell) = 2^c z_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

$$2^c f \wedge r_\ell = 0 \qquad s_m = b^q$$

От регистровой машины к диофантову уравнению

4. Переписать полученные соотношения, используя вместо операции поразрядного умножения биномиальные коэффициенты (и дополнительные переменные)

От регистровой машины к диофантову уравнению

4. Переписать полученные соотношения, используя вместо операции поразрядного умножения биномиальные коэффициенты (и дополнительные переменные)
5. Переписать новые соотношения без использования биномиальных коэффициентов в виде системы *экспоненциально диофантовых уравнений*

От регистровой машины к диофантову уравнению

4. Переписать полученные соотношения, используя вместо операции поразрядного умножения биномиальные коэффициенты (и дополнительные переменные)
5. Переписать новые соотношения без использования биномиальных коэффициентов в виде системы *экспоненциально диофантовых уравнений*

Определение. *Экспоненциально диофантово уравнениие*имеет вид

$$E_{\mathrm{L}}(x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(x_1, x_2, \ldots, x_m)$$

где E_{L} и E_{R} – выражения, построенные по обычным правилам с помощью сложения, умножения и возведения в степень из конкретных натуральных чисел и переменных, допустимыми значениями которых являются также только натуральные числа.

От регистровой машины к диофантову уравнению

6. Свернуть систему экспоненциально диофантовых уравнений в одно экспоненциально диофантово уравнение, дающее *экспоненциально диофантово представление* исходного перечислимого множества, принимаемого регистровой машиной

От регистровой машины к диофантову уравнению

6. Свернуть систему экспоненциально диофантовых уравнений в одно экспоненциально диофантово уравнение, дающее *экспоненциально диофантово представление* исходного перечислимого множества, принимаемого регистровой машиной
7. Преобразовать полученное экспоненциально диофантово уравнение в эквивалентное диофантово уравнение, используя много копий многочлена из диофантова представления возведения в степень:

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

От регистровой машины к экспоненциально диофантову уравнению

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

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \Longleftrightarrow$$
$$\Longleftrightarrow \exists x_1 \ldots x_m \{ E_{\mathrm{L}}(x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(x_1, x_2, \ldots, x_m) \} \quad (1)$$

От регистровой машины к экспоненциально диофантову уравнению

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

$$\langle a_1, \ldots, a_n \rangle \in \mathfrak{M} \iff$$
$$\iff \exists x_1 \ldots x_m \{ E_{\mathrm{L}}(x_1, x_2, \ldots, x_m) \;=\; E_{\mathrm{R}}(x_1, x_2, \ldots, x_m) \} \quad (1)$$

Теорема (Матиясевич [1975]). *Каждое перечислимое множество $\mathfrak{M}$ имеет однократное экспоненциально диофантово представление (1), в котором значения неизвестных $x_1, x_2, \ldots, x_m$, если они существуют, однозначно определяются по значениям параметров $a_1, \ldots, a_n$.*

Однократное кодирование протокола

$$2a = 2r_{\ell,0} < b = 2^{c+1}$$

$$r_\ell - r_{\ell,0} \quad = \quad br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^- (z_\ell \wedge s_k)$$

$$s_d - s_{d,0} = b\sum_d^+ s_k + b\sum_d^+ (z_\ell \wedge s_k) + b\sum_d^0 ((e - z_\ell) \wedge s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^c f \wedge ((2^c - 1)f + r_\ell) = 2^c z_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

$$2^c f \wedge r_\ell = 0 \qquad s_m = b^q$$

Однократное кодирование протокола

$$b = 2^{c+1} \quad c = a + q + 1$$

$$r_\ell - r_{\ell,0} \quad = \quad br_\ell + b\sum_\ell^+ s_k - b\sum_\ell^- (z_\ell \wedge s_k)$$

$$s_d - s_{d,0} = b\sum_d^+ s_k + b\sum_d^+ (z_\ell \wedge s_k) + b\sum_d^0 ((e - z_\ell) \wedge s_k)$$

$$e = \frac{b^q - 1}{b - 1}$$

$$2^c f \wedge ((2^c - 1)f + r_\ell) = 2^c z_\ell \quad f = \frac{b^{q+1} - 1}{b - 1}$$

$$2^c f \wedge r_\ell = 0 \qquad s_m = b^q$$

Однократность поразрядного умножения

$$c = a \wedge b \iff \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \& \\ \& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

Однократность поразрядного умножения

$$c = a \wedge b \iff \binom{a}{c} \text{ нечетн. } \& \binom{b}{c} \text{ нечетн. } \& \\ \& \binom{(a-c)+(b-c)}{a-c} \text{ нечетн.}$$

$$\iff \exists x_1 x_2 x_3 \left\{ \binom{a}{c} = 2x_1 + 1 \,\& \binom{b}{c} = 2x_2 + 1 \,\& \\ \& \binom{(a-c)+(b-c)}{a-c} = 2x_3 + 1 \right\}$$

Однократность биномиальных коэффициентов

$$c = \binom{m}{n} \iff \exists upq\{(1+u)^m = pu^{n+1} + cu^n + q \,\&\, c < u \,\&\, q < u^{n-1} \,\&\, u > 2^m\}$$

Однократность биномиальных коэффициентов

$$c = \binom{m}{n} \iff \exists upq\{(1+u)^m = pu^{n+1} + cu^n + q \,\&\, c < u \,\&\, q < u^{n-1} \,\&\, u > 2^m\}$$

$$\iff \exists upqxy\{(1+u)^m = pu^{n+1} + cu^n + q \,\&\, c + x + 1 = u \,\&\, q + y + 1 = u^{n-1} \,\&\, u = 2^m + 1\}$$

От регистровой машины к диофантову уравнению

7. Преобразовать полученное экспоненциально диофантово уравнение в эквивалентное диофантово уравнение, используя много копий многочлена из диофантова представления возведения в степень:

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

От регистровой машины к диофантову уравнению

7. Преобразовать полученное экспоненциально диофантово уравнение в эквивалентное диофантово уравнение, используя много копий многочлена из диофантова представления возведения в степень:

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

$$\exists c \{a = 2^c\} \Longleftrightarrow \exists x_1 \ldots x_m \{P(a, x_1, \ldots, x_m) = 0\}$$

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	2^1	2^2	2^3	...
3	3^0	3^1	3^2	3^3	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	2^1	2^2	2^3	...
3	3^0	3^1	3^2	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	2^1	2^2	2^3	...
3	3^0	3^1	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	2^1	2^2	2^3	...
3	3^0	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	2^1	2^2	2^3	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	2^1	2^2	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	2^1	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	2^0	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	1^3	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	1^2	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	1^1	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	1^0	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	0^3	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	0^2	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	0^1	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	$0^1 = 0$	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	$0^1 = 0$	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	$0^1 = 0$	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	0^0	$0^1 = 0$	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	$0^0 = 1$	$0^1 = 0$	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	$0^0 = 1$	$0^1 = 0$	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

Возведение в степень

	0	1	2	3	...
0	$0^0 = 1$	$0^1 = 0$	$0^2 = 0$	$0^3 = 0$	...
1	$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$	...
2	$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	...
3	$3^0 = 1$	$3^1 = 3$	$3^2 = 9$	$3^3 = 27$	...
⋮	⋮	⋮	⋮	⋮	⋱

	0	1	2	3	...
b	$\beta_b(0) = b^0$	$\beta_b(1) = b^1$	$\beta_b(2) = b^2$	$\beta_b(3) = b^3$	...

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

Рекуррентные последовательности второго порядка

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

Рекуррентные последовательности второго порядка

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

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

Рекуррентные последовательности второго порядка

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

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

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

Рекуррентные последовательности второго порядка

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

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

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

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

Рекуррентные последовательности второго порядка

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

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

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

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

Рекуррентные последовательности второго порядка

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

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

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

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

Рекуррентные последовательности второго порядка

$$\beta_b(0) = 1 \qquad \beta_b(n+1) = b\beta_b(n)$$

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

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

$$\begin{aligned} \alpha_b(n+2) &= b\alpha_b(n+1) - \alpha_b(n) \\ &\geq 2\alpha_b(n+1) - \alpha_b(n) \\ &= \alpha_b(n+1) + (\alpha_b(n+1) - \alpha_b(n)) \\ &> \alpha_b(n+1) \end{aligned}$$

Рекуррентные последовательности второго порядка

$$\alpha_3(0), \alpha_3(1), \ldots, \alpha_3(n), \ldots$$

Рекуррентные последовательности второго порядка

$$\alpha_3(0), \alpha_3(1), \ldots, \alpha_3(n), \ldots$$

Рекуррентные последовательности второго порядка

$$\alpha_3(0), \alpha_3(1), \ldots, \alpha_3(n), \ldots$$

$$0, 1, 3, 8, 21, 55, \ldots$$

Рекуррентные последовательности второго порядка

$$\alpha_3(0), \alpha_3(1), \ldots, \alpha_3(n), \ldots$$

$$0, 1, 3, 8, 21, 55, \ldots$$

$$\phi(0) = 0 \qquad \phi(1) = 1 \qquad \phi(n+2) = \phi(n+1) + \phi(n)$$

Рекуррентные последовательности второго порядка

$$\alpha_3(0), \alpha_3(1), \ldots, \alpha_3(n), \ldots$$

$$0, 1, 3, 8, 21, 55, \ldots$$

$$\phi(0) = 0 \qquad \phi(1) = 1 \qquad \phi(n+2) = \phi(n+1) + \phi(n)$$

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

Рекуррентные последовательности второго порядка

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

Рекуррентные последовательности второго порядка

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

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

Рекуррентные последовательности второго порядка

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

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

$$\alpha_b(-1) = b\alpha_b(0) - \alpha_b(1)$$

Рекуррентные последовательности второго порядка

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

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

$$\alpha_b(-1) = b\alpha_b(0) - \alpha_b(1) = -1$$

Рекуррентные последовательности второго порядка

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

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

$$\alpha_b(-1) = b\alpha_b(0) - \alpha_b(1) = -1$$

$$\alpha_b(0) = 0 = -\alpha_b(0) \qquad \alpha_b(-1) = -1 = -\alpha(1)$$

Рекуррентные последовательности второго порядка

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

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

$$\alpha_b(-1) = b\alpha_b(0) - \alpha_b(1) = -1$$

$$\alpha_b(0) = 0 = -\alpha_b(0) \qquad \alpha_b(-1) = -1 = -\alpha(1) \qquad \alpha_b(-n) = -\alpha_b(n)$$

Диофантовость последовательности $\alpha_b(k)$

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

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

Скорость роста

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

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

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

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

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

От α к β

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

От α к β

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

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

От α к β

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

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

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

От α к β

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

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

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

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

От α к β

$$(b-1)^n \le \alpha_b(n+1) \le b^n$$

$$b^n \le \alpha_{b+1}(n+1) \le (b+1)^n$$

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

$$(bd-1)^n \le \alpha_{bd}(n+1) \le (bd)^n \le \alpha_{bd+1}(n+1) \le (bd+1)^n$$

$$(d-1)^n \le \alpha_d(n+1) \le d^n \le \alpha_{d+1}(n+1) \le (d+1)^n$$

От α к β

$$(b-1)^n \le \alpha_b(n+1) \le b^n$$

$$b^n \le \alpha_{b+1}(n+1) \le (b+1)^n$$

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

$$(bd-1)^n \le \alpha_{bd}(n+1) \le (bd)^n \le \alpha_{bd+1}(n+1) \le (bd+1)^n$$

$$(d-1)^n \le \alpha_d(n+1) \le d^n \le \alpha_{d+1}(n+1) \le (d+1)^n$$

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

От α к β

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

От α к β

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

$$a = b^n \iff \frac{\alpha_{bd}(n+1)}{\alpha_{d+1}(n+1)} \le a \le \frac{\alpha_{bd+1}(n+1)}{\alpha_d(n+1)} \le \frac{\alpha_{bd}(n+1)}{\alpha_{d+1}(n+1)} + \frac{1}{2}$$

Матрицы

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Матрицы

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

Матрицы

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

Матрицы

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

$$\mathrm{E} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Матрицы

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

$$\mathrm{E} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathrm{EB} = \mathrm{BE} = \mathrm{B}$$

Определители

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

Определители

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$\det(\mathrm{AB}) = \det(\mathrm{A})\det(\mathrm{B})$$

Матричное представление

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

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

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

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

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} \alpha_b(1) & -\alpha_b(0) \\ \alpha_b(0) & -\alpha_b(-1) \end{pmatrix}$$

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} 1 & -\alpha_b(0) \\ \alpha_b(0) & -\alpha_b(-1) \end{pmatrix}$$

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ \alpha_b(0) & -\alpha_b(-1) \end{pmatrix}$$

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ 0 & -\alpha_b(-1) \end{pmatrix}$$

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ 0 & -\alpha_b(-1) \end{pmatrix}$$

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ 0 & -\alpha_b(-1) \end{pmatrix}$$

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Матричное представление

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

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

$$A_b(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{E}$$

Матричное рекуррентное соотношение первого порядка

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

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

Матричное рекуррентное соотношение первого порядка

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

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

$$A_b(n+1) = \begin{pmatrix} \alpha_b(n+2) & -\alpha_b(n+1) \\ \alpha_b(n+1) & -\alpha_b(n) \end{pmatrix}$$

Матричное рекуррентное соотношение первого порядка

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

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

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

Матричное рекуррентное соотношение первого порядка

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

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

$$\begin{aligned} A_b(n+1) &= \begin{pmatrix} \alpha_b(n+2) & -\alpha_b(n+1) \\ \alpha_b(n+1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} b\alpha_b(n+1) - \alpha(n) & -\alpha_b(n+1) \\ b\alpha_b(n) - \alpha(n-1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \\ &= A_b(n)\Psi_b \end{aligned}$$

Матричное рекуррентное соотношение первого порядка

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

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

$$\begin{aligned} A_b(n+1) &= \begin{pmatrix} \alpha_b(n+2) & -\alpha_b(n+1) \\ \alpha_b(n+1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} b\alpha_b(n+1) - \alpha(n) & -\alpha_b(n+1) \\ b\alpha_b(n) - \alpha(n-1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \\ &= A_b(n)\Psi_b \end{aligned}$$

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

Матричное рекуррентное соотношение первого порядка

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

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

$$\begin{aligned} A_b(n+1) &= \begin{pmatrix} \alpha_b(n+2) & -\alpha_b(n+1) \\ \alpha_b(n+1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} b\alpha_b(n+1) - \alpha(n) & -\alpha_b(n+1) \\ b\alpha_b(n) - \alpha(n-1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \\ &= A_b(n)\Psi_b \end{aligned}$$

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

Матричное рекуррентное соотношение первого порядка

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

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

Матричное рекуррентное соотношение первого порядка

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

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

$$A_b(n) =$$

Матричное рекуррентное соотношение первого порядка

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

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

$$A_b(n) = A_b(0)\Psi_b^n$$

Матричное рекуррентное соотношение первого порядка

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

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

$$A_b(n) = A_b(0)\Psi_b^n = \Psi_b^n$$

Определитель

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

Определитель

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \qquad A_b(n) = \Psi_b^n$$

Определитель

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \qquad A_b(n) = \Psi_b^n$$

$\det(A_b(n))$

Определитель

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \qquad A_b(n) = \Psi_b^n$$

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

Определитель

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \qquad A_b(n) = \Psi_b^n$$

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

Определитель

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \qquad A_b(n) = \Psi_b^n$$

$$\det(A_b(n)) = \det(\Psi_b^n) = (\det \Psi_b)^n = 1^n$$

Определитель

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \qquad A_b(n) = \Psi_b^n$$

$$\det(A_b(n)) = \det(\Psi_b^n) = (\det \Psi_b)^n = 1^n = 1$$

Определитель

$$\Psi_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \qquad A_b(n) = \Psi_b^n$$

$$\det(A_b(n)) = \det(\Psi_b^n) = (\det \Psi_b)^n = 1^n = 1$$

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

Характеристическое уравнение

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

Характеристическое уравнение

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

$$\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$$

Характеристическое уравнение

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

$$\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$$

$$\alpha_b^2(n) - \alpha_b(n+1)\alpha_b(n-1)$$

Характеристическое уравнение

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

$$\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$$

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

Характеристическое уравнение

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

$$\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$$

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

Характеристическое уравнение

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

$$\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$$

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

Характеристическое уравнение

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

$$\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$$

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

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

Характеристическое уравнение

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

$$\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$$

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

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

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

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

Индукция по y: случай $y = 0$

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

Индукция по y: случай $y = 0$

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

$x^2 = 1$

Индукция по y: случай $y = 0$

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

$x^2 = 1$, следовательно $x = 1$.

Индукция по y: случай $y = 0$

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

$x^2 = 1$, следовательно $x = 1$. Полагая $n = 0$, имеем

$$x = 1 = \alpha_b(1) = \alpha_b(n+1)$$

$$y = 0 = \alpha_b(0) = \alpha_b(n)$$

Индукция по y: случай $y > 0$

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

Индукция по y: случай $y > 0$

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

$$y - 1$$

Индукция по y: случай $y > 0$

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

$$n - 1$$

Индукция по y: случай $y > 0$

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

$$n - 1$$

Мы ожидаем, что

Индукция по y: случай $y > 0$

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

$$n - 1$$

Мы ожидаем, что

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

Индукция по y: случай $y > 0$

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

$$n - 1$$

Мы ожидаем, что

$$\alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$$

Индукция по y: случай $y > 0$

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

$$n - 1$$

Мы ожидаем, что

$$\alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$$

Индукция по y: случай $y > 0$

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

$$n - 1$$

Мы ожидаем, что

$$\alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$$

$$\alpha_b(n-1) = b\alpha_b(n) - \alpha_b(n+1)$$

Индукция по y: случай $y > 0$

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

$$n - 1$$

Мы ожидаем, что
$by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$\alpha_b(n-1) = b\alpha_b(n) - \alpha_b(n+1)$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$by - x \overset{?}{\ge} 0$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$by - x \stackrel{?}{\ge} 0$$

$$x = by + \frac{1 - y^2}{x}$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$by - x \stackrel{?}{\ge} 0$$

$$x = by + \frac{1 - y^2}{x} \le by \qquad z = by - x$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$by - x \stackrel{?}{\ge} 0$$

$$x = by + \frac{1 - y^2}{x} \le by \qquad z = by - x$$

Мы знаем, что $0 \le z = by - x$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$z \overset{?}{\le} y$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$z \overset{?}{\le} y$$

$$x = by + \frac{1}{x} - \frac{y^2}{x}$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$z \overset{?}{\le} y$$

$$\begin{aligned} x &= by + \frac{1}{x} - \frac{y^2}{x} \\ &> by - \frac{y^2}{y} \\ &= by - y \end{aligned}$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$z \overset{?}{\le} y$$

$$\begin{aligned} x &= by + \frac{1}{x} - \frac{y^2}{x} \\ &> by - \frac{y^2}{y} \\ &= by - y \end{aligned}$$

Мы знаем, что $0 \le z = by - x < y$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$y^2 - byz + z^2 \stackrel{?}{=} 1$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$y^2 - byz + z^2 \stackrel{?}{=} 1$$

$$y^2 - byz + z^2$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$$

$$y^2 - byz + z^2 \stackrel{?}{=} 1$$

$$y^2 - byz + z^2 \;=\; y^2 - by(by - x) + (by - x)^2$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$y^2 - byz + z^2 \stackrel{?}{=} 1$$

$$\begin{aligned} y^2 - byz + z^2 &= y^2 - by(by - x) + (by - x)^2 \\ &= x^2 - bxy + y^2 \end{aligned}$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что
$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$y^2 - byz + z^2 \stackrel{?}{=} 1$$

$$\begin{aligned} y^2 - byz + z^2 &= y^2 - by(by - x) + (by - x)^2 \\ &= x^2 - bxy + y^2 \\ &= 1 \end{aligned}$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что
$z = by - x = \alpha_b(n-1), \qquad y = \alpha_b(n), \qquad x = \alpha_b(n+1)$

$$y^2 - byz + z^2 \stackrel{?}{=} 1$$

$$\begin{aligned} y^2 - byz + z^2 &= y^2 - by(by - x) + (by - x)^2 \\ &= x^2 - bxy + y^2 \\ &= 1 \end{aligned}$$

Мы знаем, что $0 \le z = by - x < y$, $y^2 - byz + z^2 = 1$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что

$z = by - x = \alpha_b(n-1) \quad y = \alpha_b(n) \quad x = \alpha_b(n+1)$

Мы знаем, что $0 \leq z = by - x < y$, $y^2 - byz + z^2 = 1$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что
$z = by - x = \alpha_b(n-1) \quad y = \alpha_b(n) \quad x = \alpha_b(n+1)$

Мы знаем, что $0 \le z = by - x < y$, $y^2 - byz + z^2 = 1$
По индукционному предположению существует m такое, что

$$y = \alpha_b(m+1), \qquad z = \alpha_b(m)$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что
$z = by - x = \alpha_b(n-1) \quad y = \alpha_b(n) \quad x = \alpha_b(n+1)$

Мы знаем, что $0 \le z = by - x < y$, $y^2 - byz + z^2 = 1$
По индукционному предположению существует m такое, что

$$y = \alpha_b(m+1), \qquad z = \alpha_b(m)$$

$$x = by - z = b\alpha_b(m+1) - \alpha_b(m) = \alpha_b(m+2)$$

Индукция по y: случай $y > 0$

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

Мы ожидаем, что
$z = by - x = \alpha_b(n-1) \quad y = \alpha_b(n) \quad x = \alpha_b(n+1)$

Мы знаем, что $0 \le z = by - x < y$, $y^2 - byz + z^2 = 1$
По индукционному предположению существует m такое, что

$$y = \alpha_b(m+1), \qquad z = \alpha_b(m)$$

$$x = by - z = b\alpha_b(m+1) - \alpha_b(m) = \alpha_b(m+2)$$

$$n = m + 1$$

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:

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

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.

$$m = n + k\ell, \qquad 0 \le n < k$$

Свойства делимости

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

Доказательство.

$$m = n + k\ell, \qquad 0 \le n < k$$

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

Свойства делимости

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

Доказательство.

$$m = n + k\ell, \qquad 0 \le n < k$$

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

Свойства делимости

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

Доказательство.

$$m = n + k\ell, \qquad 0 \le n < k$$

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

Свойства делимости

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

Доказательство.

$$m = n + k\ell, \qquad 0 \le n < k$$

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

Свойства делимости

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

Доказательство.

$$m = n + k\ell, \qquad 0 \le n < k$$

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

Свойства делимости

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

Доказательство.

$$m = n + k\ell, \qquad 0 \le n < k$$

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

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

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

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

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

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

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

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

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

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

$$m = n + k\ell, \qquad 0 \le n < k$$

Свойства делимости

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

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

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

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

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

$$m = n + k\ell, \qquad 0 \le n < k$$

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

Свойства делимости

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

Свойства делимости

$$\begin{aligned} A_b(m) &= A_b^{\ell}(k) \\ &= [\alpha_b(k)\Psi_b - \alpha_b(k-1)E]^{\ell} \end{aligned}$$

Свойства делимости

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

Свойства делимости

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

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

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

Свойства делимости

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

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

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

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

Свойства делимости

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

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

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).

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

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

Новые свойства делимости

Лемма (доказанная).

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

Лемма (обратная).

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

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

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

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

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

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

Сравнение последовательностей

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

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

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

Сравнение последовательностей

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

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

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

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

Сравнение последовательностей

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

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

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

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

Сравнение последовательностей

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

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

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

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

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

Сравнение последовательностей

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

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

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

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

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

Сравнение последовательностей

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

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

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

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

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

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

Первый шаг

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

Первый шаг

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

$$\alpha_2(n) = n$$

Первый шаг

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

$$\alpha_2(n) = n$$

Функция arem

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

Функция 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

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

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

Сравнение последовательностей

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

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

$$\alpha_{b''}(n) = \mathrm{arem}(\alpha_{b'}(n), b' - b'') \quad \text{provided} \quad 2\alpha_{b''}(n) \leq b' - b''$$

Второй шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \quad \Longleftrightarrow \quad \exists n\{x = \alpha_b(n) \,\&\&\, k = \alpha_2(n)\}$$

Второй шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \quad \Longleftrightarrow \quad \exists n\{x = \alpha_b(n) \,\&\&\, k = \alpha_2(n)\}$$

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists y\{x = \alpha_b(n) \,\&\&\, k = \mathrm{arem}(x, b-2)\}$$

$$\text{provided} \quad 2n \leq b-2$$

Второй шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \quad \Longleftrightarrow \quad \exists n\{x = \alpha_b(n) \,\&\&\, k = \alpha_2(n)\}$$

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists y\{x = \alpha_b(n) \,\&\&\, k = \mathrm{arem}(x, b-2)\}$$

$$\text{provided} \quad 2n \leq b-2$$

Третий шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists y\{x = \alpha_b(n) \,\&\&\, k = \mathrm{arem}(x, b-2)\}$$
$$\text{provided} \quad 2n \leq b-2$$

Третий шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists y\{x = \alpha_b(n) \,\&\&\, k = \mathrm{arem}(x, b-2)\}$$
$$\text{provided} \quad 2n \le b-2$$

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n) \,\&\&$$
$$x = \mathrm{arem}(X, B-b) \,\&\&\, k = \mathrm{arem}(X, B-2)\}$$
$$\text{provided} \quad 2\alpha_b(n) \le B-b \,\&\&\, 2n \le B-2$$

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

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

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

Специальный период

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

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 $\mathrm{arem}(\alpha_b(0), v), \mathrm{arem}(\alpha_b(1), v), \ldots, \mathrm{arem}(\alpha_b(n), v), \ldots$ имеет период длины $2m$.

Четвертый шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n)\,\&\&$$
$$x = \mathrm{arem}(X, B - b)\,\&\&\, k = \mathrm{arem}(X, B - 2)\}$$
$$\text{при условии} \quad 2\alpha_b(n) \le B - b\,\&\&\, 2n \le B - 2$$

Четвертый шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n)\,\&\&$$
$$x = \mathrm{arem}(X, B - b)\,\&\&\, k = \mathrm{arem}(X, B - 2)\}$$
$$\text{при условии} \quad 2\alpha_b(n) \le B - b\,\&\&\, 2n \le B - 2$$

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

Четвертый шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n)\,\&\&$$
$$x = \mathrm{arem}(X, B-b)\,\&\&\, k = \mathrm{arem}(X, B-2)\}$$
при условии $\quad 2\alpha_b(n) \le B - b\,\&\&\, 2n \le B - 2$

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

$$v \mid B - b$$

Четвертый шаг

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n)\ \&\&$$
$$x = \mathrm{arem}(X, B - b)\ \&\&\ k = \mathrm{arem}(X, B - 2)\}$$
$$\text{при условии} \quad 2\alpha_b(n) \le B - b\ \&\&\ 2n \le B - 2$$

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

$$v | B - b$$

$$\langle x, k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n)\ \&\&$$
$$x = \mathrm{arem}(X, v)\ \&\&\ k = \mathrm{arem}(X, B - 2)\}$$
$$\text{при условии} \quad 2\alpha_b(n) \le v\ \&\&\ 2n \le B - 2$$

Пятый шаг

$$v|B-b$$

$$\langle x,k\rangle \in \mathfrak{N}_b \iff \exists X\{X=\alpha_B(n)\,\&\&\, x=\mathrm{arem}(X,v)\,\&\&\, k=\mathrm{arem}(X,B-2)\}$$

$$\text{provided}\quad 2\alpha_b(n)\le v\,\&\&\,2n\le B-2$$

Пятый шаг

$$v|B-b$$

$$\langle x,k\rangle \in \mathfrak{N}_b \iff \exists X\{X=\alpha_B(n)\,\&\&\, x=\mathrm{arem}(X,v)\,\&\&\, k=\mathrm{arem}(X,B-2)\}$$
$$\text{provided}\quad 2\alpha_b(n)\le v\,\&\&\,2n\le B-2$$

$$u|B-2$$

Пятый шаг

$$v|B-b$$

$$\langle x,k\rangle \in \mathfrak{N}_b \iff \exists X\{X=\alpha_B(n)\,\&\&\, x=\mathrm{arem}(X,v)\,\&\&\, k=\mathrm{arem}(X,B-2)\}$$
$$\text{provided}\quad 2\alpha_b(n)\le v\,\&\&\,2n\le B-2$$

$$u|B-2$$

$$\langle x,k\rangle \in \mathfrak{N}_b \iff \exists X\{X=\alpha_B(n)\,\&\&\, x=\mathrm{arem}(X,v)\,\&\&\, k=\mathrm{arem}(X,u)\}$$
$$\text{при условии}\quad 2\alpha_b(n)\le v\,\&\&\,2n\le u$$

Ключевая идея

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

$$u|B-2$$

$$\langle x,k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n)\ \&\&$$
$$x = \mathrm{arem}(X,v)\ \&\&\ k = \mathrm{arem}(X,u)\}$$
$$\text{при условии} \quad 2\alpha_b(n) \le v\ \&\&\ 2n \le u$$

Ключевая идея

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

$$u|B-2$$

$$\langle x,k\rangle \in \mathfrak{N}_b \iff \exists X\{X = \alpha_B(n)\,\&\&\, x = \mathrm{arem}(X,v)\,\&\&\, k = \mathrm{arem}(X,u)\}$$

при условии $2\alpha_b(n) \le v \,\&\&\, 2n \le u$

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 $u \mid m$.

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*

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

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

$$r < s,$$

$$u^2 \mid s,$$

$$v = bs - 2r,$$

$$v \mid B - b,$$

$$u \mid B - 2,$$

$$B > 2,$$

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

$$2x < u,$$

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

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

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”

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

Часть “тогда”

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

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

Часть “тогда”

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

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

Часть “тогда”

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

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

$$v = bs - 2r$$

Часть “тогда”

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

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

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

Часть “тогда”

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

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

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

Часть “тогда”

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

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

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

$$u^2 \mid s$$

Часть “тогда”

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

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

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

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

Часть “тогда”

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

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

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

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

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”

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

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

Часть “тогда”

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

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

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

Часть “тогда”

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

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

$$\begin{aligned} A_b(n) &= \psi_b^n \\ &= \psi_b^{2lm \pm j} \end{aligned}$$

Часть “тогда”

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

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

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

Часть “тогда”

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

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

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

Часть “тогда”

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

Часть “тогда”

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

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

Часть “тогда”

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

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

Часть “тогда”

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

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

Часть “тогда”

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

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

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

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”

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

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

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

$$v = bs - 2r,$$

$$u^2 \mid s,$$

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

$$v \mid B - b,$$

$$u \mid B - 2,$$

$$2x < u,$$

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

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

Часть “только тогда”

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

Часть “только тогда”

$$\begin{aligned} u = \alpha_b(l), t = \alpha_b(l+1) &\Rightarrow u^2 - but + t^2 = 1 \\ l \text{ is big} &\Rightarrow 2x < u \end{aligned}$$

Часть “только тогда”

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

Часть “только тогда”

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

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

Часть “только тогда”

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

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

Часть “только тогда”

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

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

$$v = bs - 2r$$

Часть “только тогда”

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

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

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

Часть “только тогда”

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

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

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

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”

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

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

Часть “только тогда”

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

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

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

Часть “только тогда”

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

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

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

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

Часть “только тогда”

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

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

Часть “только тогда”

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

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

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

$$2x < u$$