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

Ю. В. Матиясевич

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

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

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

Ю. В. Матиясевич

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

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

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

Часть 2. Десятая проблема Гильберта

Третья лекция

Ю. В. Матиясевич

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

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

Теорема Куммера

$$\binom{m+n}{m} = C_{m+n}^{m}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C_{m+n}^{m} \\ &= \frac{(m+n)!}{m!n!}\end{aligned}$$

Теорема Куммера

$$\begin{aligned}
\binom{m+n}{m} &= C_{m+n}^{m} \\
&= \frac{(m+n)!}{m!n!} \\
&= 2^{\alpha_2(m,n)} 3^{\alpha_3(m,n)} \dots p^{\alpha_p(m,n)} \dots
\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C^{m}_{m+n} \\ &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

Теорема (Ernst Eduard Kummer [1852]). *Запишем числа m и n в позиционной системе счисления с основанием p и сложим их «в столбик»;*

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= C^m_{m+n} \\ &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

Теорема (Ernst Eduard Kummer [1852]). *Запишем числа m и n в позиционной системе счисления с основанием p и сложим их «в столбик»; $\alpha_p(m,n)$ равно количеству переносов из разряда в разряд при этом сложении.*

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

$$\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n)$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

$$p, 2p, 3p, \ldots,$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

$$p, 2p, 3p, \ldots, \left\lfloor \frac{k}{p} \right\rfloor p$$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \ldots, \left\lfloor \frac{k}{p} \right\rfloor p$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \ldots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \ldots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \ldots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \ldots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3: $p^3, 2p^3, 3p^3, \ldots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \ldots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \ldots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3: $p^3, 2p^3, 3p^3, \ldots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

$\vdots$

Теорема Куммера

$$k! = 1 \cdot 2 \cdot 3 \cdots k = 2^{\beta_2(k)} 3^{\beta_3(k)} \ldots p^{\beta_p(k)} \ldots$$

Имеется $\left\lfloor \frac{k}{p} \right\rfloor$ чисел кратных p: $p, 2p, 3p, \ldots, \left\lfloor \frac{k}{p} \right\rfloor p$

Имеется $\left\lfloor \frac{k}{p^2} \right\rfloor$ чисел кратных p^2: $p^2, 2p^2, 3p^2, \ldots, \left\lfloor \frac{k}{p^2} \right\rfloor p^2$

Имеется $\left\lfloor \frac{k}{p^3} \right\rfloor$ чисел кратных p^3: $p^3, 2p^3, 3p^3, \ldots, \left\lfloor \frac{k}{p^3} \right\rfloor p^3$

$\vdots$

$$\beta_p(k) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \ldots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

$$\alpha_p(m,n) = \beta_p(m+n) - \beta_p(m) - \beta_p(n)$$

Теорема Куммера

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!n!} \\ &= 2^{\alpha_2(m,n)}3^{\alpha_3(m,n)}\dots p^{\alpha_p(m,n)}\dots\end{aligned}$$

$$k! = 2^{\beta_2(k)}3^{\beta_3(k)}\dots p^{\beta_p(k)}\dots$$

$$\begin{aligned}\alpha_p(m,n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\ &= \left\lfloor\frac{m+n}{p}\right\rfloor + \left\lfloor\frac{m+n}{p^2}\right\rfloor + \left\lfloor\frac{m+n}{p^3}\right\rfloor + \dots \\ &\quad - \left\lfloor\frac{m}{p}\right\rfloor - \left\lfloor\frac{m}{p^2}\right\rfloor - \left\lfloor\frac{m}{p^3}\right\rfloor - \dots \\ &\quad - \left\lfloor\frac{n}{p}\right\rfloor - \left\lfloor\frac{n}{p^2}\right\rfloor - \left\lfloor\frac{n}{p^3}\right\rfloor - \dots\end{aligned}$$

Теорема Куммера

$$\begin{aligned}\alpha_p(m,n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\ &= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\ &\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\ &\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots\end{aligned}$$

Теорема Куммера

$$
\begin{aligned}
\alpha_p(m,n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\
&= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\
&\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\
&\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots \\
&= \left(\left\lfloor \frac{m+n}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{m+n}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + \\
&\quad + \left(\left\lfloor \frac{m+n}{p^3} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + \dots
\end{aligned}
$$

Теорема Куммера

$$\left\lfloor \frac{m+n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor = \begin{cases} 1, & \text{если есть перенос} \\ 0, & \text{если нет переноса} \end{cases}$$

Теорема Куммера

$$\left\lfloor \frac{m+n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor = \begin{cases} 1, & \text{если есть перенос} \\ 0, & \text{если нет переноса} \end{cases}$$

$m = \sum_{j=0}^{r} m_j p^j =$	m_r	$\dots$	m_k	m_{k-1}	$\dots$	m_0
$n = \sum_{j=0}^{r} n_j p^j =$	n_r	$\dots$	n_k	n_{k-1}	$\dots$	n_0
$m+n = \sum_{j=0}^{r} \ell_j p^j =$	ℓ_r	$\dots$	ℓ_k	ℓ_{k-1}	$\dots$	ℓ_0

$\lfloor m/p^k \rfloor =$	m_r	$\dots$	m_k
$\lfloor n/p^k \rfloor =$	n_r	$\dots$	n_k
$\lfloor (m+n)/p^k \rfloor =$	ℓ_r	$\dots$	ℓ_k

Теорема Куммера

$$\begin{aligned}\alpha_p(m,n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\ &= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\ &\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\ &\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots\end{aligned}$$

Теорема Куммера

$$
\begin{aligned}
\alpha_p(m,n) &= \beta_p(m+n) - \beta_p(m) - \beta_p(n) \\
&= \left\lfloor \frac{m+n}{p} \right\rfloor + \left\lfloor \frac{m+n}{p^2} \right\rfloor + \left\lfloor \frac{m+n}{p^3} \right\rfloor + \dots \\
&\quad - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \dots \\
&\quad - \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor - \dots \\
&= \left(\left\lfloor \frac{m+n}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor - \left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{m+n}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + \\
&\quad + \left(\left\lfloor \frac{m+n}{p^3} \right\rfloor - \left\lfloor \frac{m}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + \dots
\end{aligned}
$$

Следствия теоремы Куммера

Следствия теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не происходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ является нечетным

Следствия теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не происходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ является нечетным, то есть существует натуральное число d такое, что

$$\binom{a+b}{a} = 2d + 1.$$

Следствия теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не происходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ является нечетным, то есть существует натуральное число d такое, что

$$\binom{a+b}{a} = 2d + 1.$$

Лемма. Биномиальный коэффициент $\binom{a}{b}$ является нечетным тогда и только тогда, когда каждый двочный разряд числа a не меньше соответствующего двоичного разряда числа b:

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad a_k \geq b_k$$

Следствия теоремы Куммера

Лемма. При сложении чисел a и b в двоичной системе счисления не происходит ни одного переноса из разряд в разряд в том и только том случае, когда биномиальный коэффициент $\binom{a+b}{a}$ является нечетным, то есть существует натуральное число d такое, что

$$\binom{a+b}{a} = 2d + 1.$$

Лемма. Биномиальный коэффициент $\binom{a}{b}$ является нечетным тогда и только тогда, когда каждый двочный разряд числа a не меньше соответствующего двоичного разряда числа b:

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad a_k \geq b_k$$

$$\binom{a}{b} = \binom{b + (a-b)}{b}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a - c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b - c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$c = a \& b$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a - c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b - c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$c = a \& b$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a - c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b - c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$c = a\&b \Longrightarrow \begin{pmatrix} a \\ c \end{pmatrix}$ нечетн.

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a - c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b - c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$$c = a\&b \Longrightarrow \binom{a}{c} \text{ нечетн.} \quad \wedge \binom{b}{c} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a-c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b-c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$$c = a\&b \Longrightarrow \begin{pmatrix} a \\ c \end{pmatrix} \text{ нечетн. } \wedge \begin{pmatrix} b \\ c \end{pmatrix} \text{ нечетн. } \wedge$$

$$\wedge \begin{pmatrix} (a-c)+(b-c) \\ a-c \end{pmatrix} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a-c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b-c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$$c = a\&b \Longrightarrow \begin{pmatrix} a \\ c \end{pmatrix} \text{ нечетн. } \wedge \begin{pmatrix} b \\ c \end{pmatrix} \text{ нечетн. } \wedge$$

$$\wedge \begin{pmatrix} (a-c)+(b-c) \\ a-c \end{pmatrix} \text{ нечетн.}$$

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a-c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b-c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$$c = a\&b \Longleftarrow \binom{a}{c} \text{ нечетн. } \wedge \binom{b}{c} \text{ нечетн. } \wedge$$

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

Поразрядное умножение

$$a = \sum_{k=0}^{\infty} a_k 2^k \qquad b = \sum_{k=0}^{\infty} b_k 2^k \qquad c = \sum_{k=0}^{\infty} c_k 2^k$$

a	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	1	$\ldots$
b	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	1	$\ldots$
c	$\ldots$	0	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$
$a-c$	$\ldots$	0	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$
$b-c$	$\ldots$	0	$\ldots$	1	$\ldots$	0	$\ldots$	0	$\ldots$

$$c = a\&b \iff \binom{a}{c} \text{ нечетн.} \quad \wedge \binom{b}{c} \text{ нечетн.} \quad \wedge$$

$$\wedge \begin{pmatrix} (a-c)+(b-c) \\ a-c \end{pmatrix} \text{ нечетн.}$$

Биномиальные коэффициенты

Биномиальные коэффициенты

$$(1+u)^m = \binom{m}{m} u^m + \binom{m}{m-1} u^{m-1} + \binom{m}{m-2} u^{m-2} + \\ + \cdots + \binom{m}{n} u^n + \cdots + \binom{m}{1} u + \binom{m}{0}$$

Биномиальные коэффициенты

$$(1+u)^m = \binom{m}{m} u^m + \binom{m}{m-1} u^{m-1} + \binom{m}{m-2} u^{m-2} + \\ + \cdots + \binom{m}{n} u^n + \cdots + \binom{m}{1} u + \binom{m}{0}$$

$$2^m = \binom{m}{0} + \cdots + \binom{m}{n} + \cdots + \binom{m}{m}$$

Биномиальные коэффициенты

$$(1+u)^m = \binom{m}{m}u^m + \binom{m}{m-1}u^{m-1} + \binom{m}{m-2}u^{m-2} + \\ + \cdots + \binom{m}{n}u^n + \cdots + \binom{m}{1}u + \binom{m}{0}$$

$$2^m = \binom{m}{0} + \cdots + \binom{m}{n} + \cdots + \binom{m}{m}$$

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

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

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

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

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

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

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

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

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

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

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

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

Рекуррентные последовательности второго порядка

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

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

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

Рекуррентные последовательности второго порядка

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

Рекуррентные последовательности второго порядка

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

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

Рекуррентные последовательности второго порядка

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

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

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

Рекуррентные последовательности второго порядка

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

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

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

Рекуррентные последовательности второго порядка

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

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

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

Диофантовость последовательности $\alpha_b(k)$

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

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

Диофантовость последовательности $\alpha_b(k)$

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

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

Скорость роста

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

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

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

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

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

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

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

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

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

$$a = b^n \iff$$

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

Матричное представление

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

Матричное представление

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

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

Матричное представление

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

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

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

Матричное представление

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

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

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

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

Матричное представление

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

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

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

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

Матричное представление

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

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

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

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

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

Характеристическое уравнение

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

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

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

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

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

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* $y \le x$, *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* $y \leq x$, *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* $y \le x$, *то найдется число* n *такое, что* $x = \alpha_b(n+1),\ y = \alpha_b(n)$.

Мы ожидаем, что

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

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

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

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

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

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

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

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

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

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

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

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

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

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* $y \leq x$, *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 $0 \leq z = by - x < y$, $y^2 - byz + z^2 = 1$
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.

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

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

Свойства делимости

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

Доказательство.

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

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

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

$$m = k\ell$$

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

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

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

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

Свойства делимости

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

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

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

Свойства делимости

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

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

Свойства делимости

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

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

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

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

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

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

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

$$m = k\ell$$