# Дискретные структуры

МФТИ, осень 2013

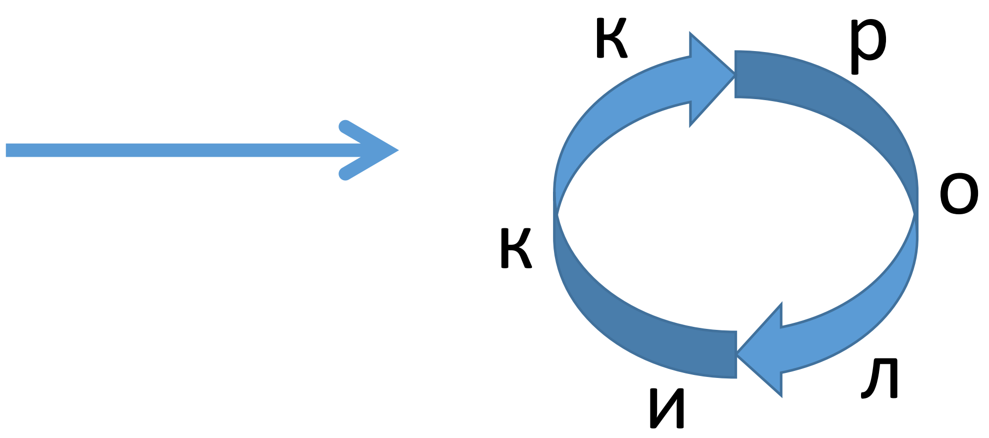
Александр Дайняк

www.dainiak.com

# Циклические слова

Циклическое слово (последовательность) — это обычное слово, «замкнутое в круг»:

кролик

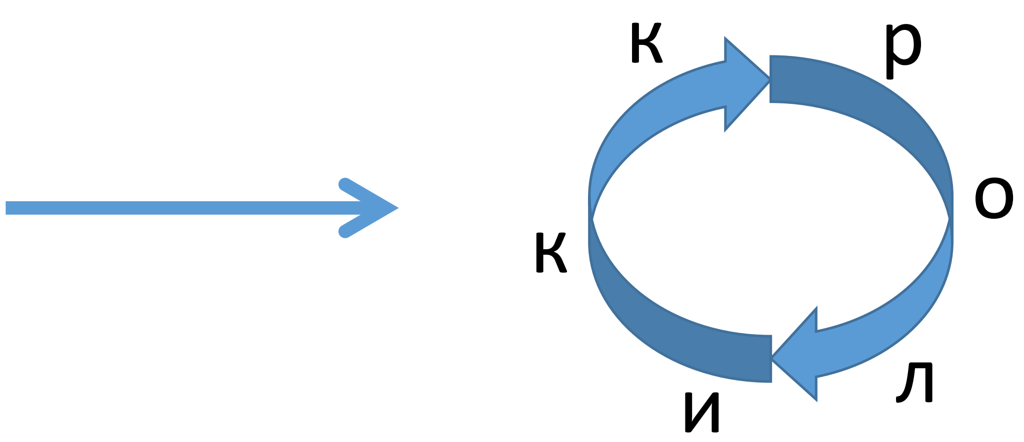



(Формально: циклическое слово — это класс эквивалентности обычных слов относительно циклического сдвига)

# Циклические слова

Разные «линейные» слова могут порождать одно и то же циклическое слово:

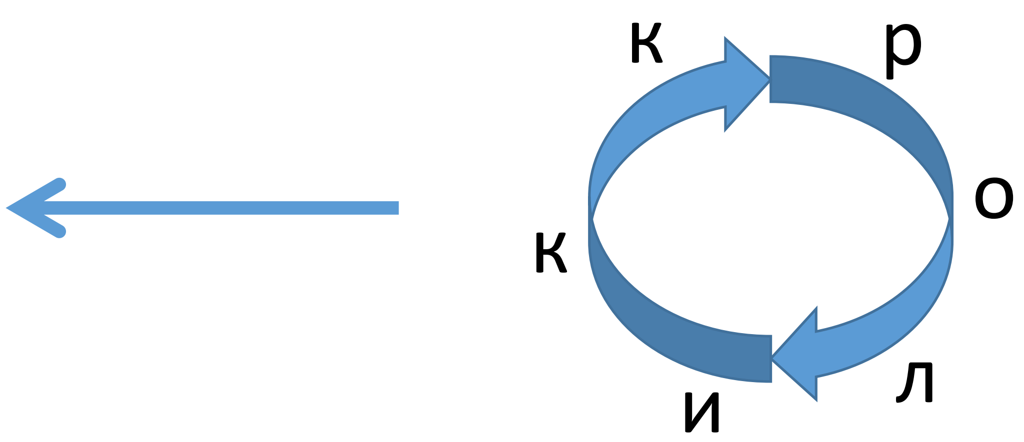
кролик
роликк
оликкр
ликкро
иккрол
ккроли



# Циклические слова

Можно мыслить и наоборот: одно циклическое слово порождает много линейных.

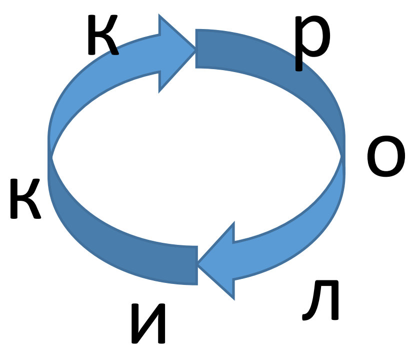
кролик
роликк
оликкр
ликкро
иккрол
ккроли



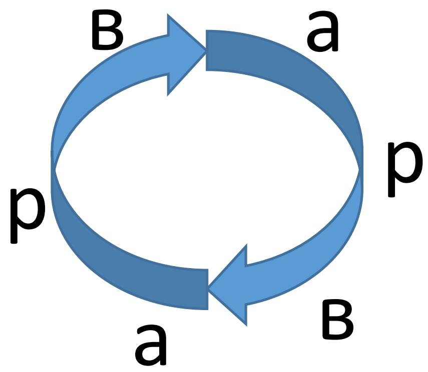
# Циклические слова

А сколько линейных слов порождает одно циклическое слово?

кролик
роликк
оликкр
ликкро
иккрол
ккроли




варвар
арварв
рварва

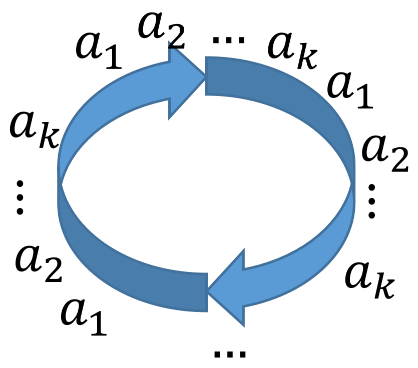


# Циклические слова

Всё определяется периодом!

$$a_1 a_2 \ldots a_k a_1 a_2 \ldots a_k \ldots \ldots a_1 a_2 \ldots a_k$$
$$a_2 a_3 \ldots a_k a_1 a_2 \ldots a_k \ldots \ldots a_1 \ldots a_k a_1$$
$$\vdots$$
$$a_k a_1 \ldots a_k a_1 a_2 \ldots a_k \ldots \ldots a_1 a_2 \ldots a_{k-1}$$

$$\xleftrightarrow{k \text{ слов}}$$



# Циклические слова

Подытожим:

- Из циклического слова периода $k$ получается ровно $k$ линейных слов
- Если $n$ — длина слова, а $k$ — период, то $k|n$

Следовательно

$$\#\text{лин. сл. длины } n = \sum_{k|n} k \cdot \#\text{ц. сл. периода } k$$

# Число циклических слов

Обозначим через $r$ мощность алфавита, а через $n$ длину слов.

Наша задача: найти $T_r(n)$ — количество соответствующих циклических слов.

Если бы мы знали для каждого $k$ число циклических слов длины $n$ и периода $k$, то всё было бы просто:

$$\#\text{ц. сл. длины } n = \sum_{k|n} \#\text{ц. сл. периода } k$$

# Число циклических слов

$$r^n = \sum_{k|n} k \cdot \#\text{ц. сл. периода } k$$

не знаем

$$T_r(n) = \sum_{k|n} \#\text{ц. сл. периода } k$$

# Формула обращения Мёбиуса

Пусть функции $f(x)$ и $g(x)$ таковы, что для любого натурального $n$ функция $f$ выражается через $g$ по формуле

$$f(n) = \sum_{k|n} g(k)$$

Тогда для любого натурального $m$ функция $g$ выражается через $f$ по формуле

$$g(m) = \sum_{l|m} f(l) \cdot \mu(m/l)$$

# Функция Мёбиуса

Функция Мёбиуса определяется так:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1 \\ 0, & \text{если } \exists p \text{ т. что } p^2 | n \\ (-1)^s, & \text{если } n = p_1 \cdot \ldots \cdot p_s \end{cases}$$

Примеры:

- $\mu(75) = 0$
- $\mu(42) = -1$
- $\mu(77) = 1$

# Функция Мёбиуса

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1 \\ 0, & \text{если } \exists p \text{ т. что } p^2 | n \\ (-1)^s, & \text{если } n = p_1 \cdot \ldots \cdot p_s \end{cases}$$

**Лемма.**

$$\sum_{k|n} \mu(k) = \begin{cases} 1, \text{если } n = 1 \\ 0, \text{если } n > 1 \end{cases}$$

*Доказательство.* Пусть $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$.

Имеем

$$\sum_{k|n} \mu(k) = \mu(1) + \sum_{k=p_i} \mu(k) + \sum_{k=p_i p_j} \mu(k) + \cdots + \sum_{k=p_1 p_2 \ldots p_s} \mu(k) =$$

$$= 1 + \binom{s}{1} \cdot (-1)^1 + \binom{s}{2} \cdot (-1)^2 + \cdots + \binom{s}{s} \cdot (-1)^s = 0$$

# Доказательство формулы Мёбиуса

Пусть $f(n) = \sum_{k|n} g(k)$.

Тогда

$$\sum_{l|m} f(l) \cdot \mu(m/l) = \sum_{l|m} \sum_{k|l} g(k) \cdot \mu(m/l) =$$

$$= \sum_{k|m} \sum_{l:\, k|l,\, l|m} g(k) \cdot \mu(m/l) =$$

$$= \sum_{k|m} g(k) \sum_{l:\, k|l,\, l|m} \mu(m/l) = \sum_{k|m} g(k) \sum_{t:\, t|(m/k)} \mu(t) = g(m)$$

# Применение формулы Мёбиуса

$$f(n) = \sum_{(k|n)} g(k) \quad \Rightarrow \quad g(m) = \sum_{(l|m)} f(l) \cdot \mu(m/l)$$

Мы ранее вывели, что

$$r^n = \sum_{k|n} k \cdot \#\text{ц. сл. периода } k$$

Значит

$$m \cdot \#\text{ц. сл. периода } m = \sum_{l|m} r^l \cdot \mu(m/l)$$

$$\#\text{ц. сл. периода } m = \frac{1}{m} \sum_{l|m} r^l \cdot \mu(m/l)$$

# Число циклических слов

$$\#\text{ц. сл. периода } m = \frac{1}{m}\sum_{l|m} r^l \cdot \mu(m/l)$$

Наконец,

$$T_r(n) = \sum_{k|n} \#\text{ц. сл. периода } k = \sum_{k|n} \frac{1}{k} \sum_{l|k} r^l \cdot \mu(k/l)$$

Окончательная формула:

$$T_r(n) = \sum_{k|n} \frac{1}{k} \sum_{l|k} r^l \cdot \mu(k/l)$$

# Число циклических слов

Формула для числа циклических слов:

$$T_r(n) = \sum_{k|n} \frac{1}{k} \sum_{l|k} r^l \cdot \mu(k/l)$$

Пример применения:

$$T_2(6) = 2^1\mu(1) +$$
$$+\frac{1}{2}\left(2^1\mu(2) + 2^2\mu(1)\right) +$$
$$+\frac{1}{3}\left(2^1\mu(3) + 2^3\mu(1)\right) +$$
$$+\frac{1}{6}\left(2^1\mu(6) + 2^2\mu(3) + 2^3\mu(2) + 2^6\mu(1)\right)$$

# Асимптотика числа циклических слов

**Утверждение.** При любом фиксированном $r$ при $n \to \infty$ выполнено

$$T_r(n) \sim \frac{r^n}{n}$$

*Доказательство:*

Одно и то же циклическое слово длины $n$ порождает не более $n$ обычных слов, поэтому

$$r^n \leq n \cdot T_r(n) \quad \Rightarrow \quad T_r(n) \geq \frac{r^n}{n}$$

Осталось оценить $T_r(n)$ сверху…

# Асимптотика числа циклических слов

$$T_r(n) = \sum_{k|n} \frac{1}{k} \sum_{l|k} r^l \cdot \mu(k/l) \leq \sum_{k|n} \frac{1}{k} \sum_{l|k} r^l \leq \sum_{k|n} \frac{1}{k} \left( r^k + \sum_{l \leq k/2} r^l \right) \leq$$

$$\leq \sum_{k|n} \frac{1}{k} \left( r^k + \tfrac{k}{2} \cdot r^{k/2} \right) \leq$$

$$\leq \tfrac{1}{n} \left( r^n + \tfrac{n}{2} \cdot r^{n/2} \right) + n \cdot \left( r^{n/2} + \tfrac{n}{4} \cdot r^{n/4} \right) \lesssim r^n / n$$

# Разбиения чисел на слагаемые

Разбиение натурального числа — это представление его в виде суммы одного или нескольких *положительных* слагаемых.

Если порядок слагаемых учитывается, разбиение *упорядоченное*.

Иначе — *неупорядоченное*.

Обозначение:

- $P(N)$ — количество упорядоченных разбиений $N$,
- $p(N)$ — количество неупорядоченных разбиений $N$.

# Разбиения чисел на слагаемые

Например, $P(3) = 4$:
$3 = 3$
$3 = 1 + 2$
$3 = 2 + 1$
$3 = 1 + 1 + 1$

При этом $p(3) = 3$:
$3 = 3$
$3 = 1 + 2$
$3 = 1 + 1 + 1$

(Считать неупорядоченные разбиения — то же, что считать разбиения, в которых слагаемые идут по возрастанию.)

# Упорядоченные разбиения

Справедливо простое равенство:

$$P(N) = 2^{N-1}$$

Доказательство на примере:

$10 \ =$ ❍❍❍❍❍❍❍❍❍❍

На каждую из этих 9 позиций
можно вставить знак ``+’’

# Рекуррентное соотношение для числа упорядоченных разбиений

Пусть $P(N;\ n_1, \dots, n_s)$ — количество способов разбить $N$ на слагаемые, каждое из которых равно одному из чисел $n_i$ (порядок слагаемых учитывается).

Рекуррентное соотношение:

$$P(N;\ n_1, \dots, n_s) =$$
$$= P(N - n_1; n_1, \dots, n_s) + P(N - n_2; n_1, \dots, n_s) + \cdots +$$
$$+P(N - n_s; n_1, \dots, n_s)$$

Идея доказательства: смотрим, чему равно первое слагаемое в разбиении, — *не что иное, как метод выделенного элемента*.

# Неупорядоченные разбиения

**Задача.**
Сколькими способами можно разменять 50 рублей монетами достоинством в 10, 5, 2 и 1 рубль?

**Математическая постановка.**
Найти количество способов представить число 50 в виде суммы слагаемых, каждое из которых равно 1, 2, 5 или 10.
(Порядок слагаемых не учитывается.)

# Неупорядоченные разбиения

Обозначение:

$$p(N;\ n_1, n_2, \dots, n_s)$$

— количество способов разбить $N$ на слагаемые, каждое из которых равно одному из чисел $n_i$ (*без учёта порядка слагаемых*).

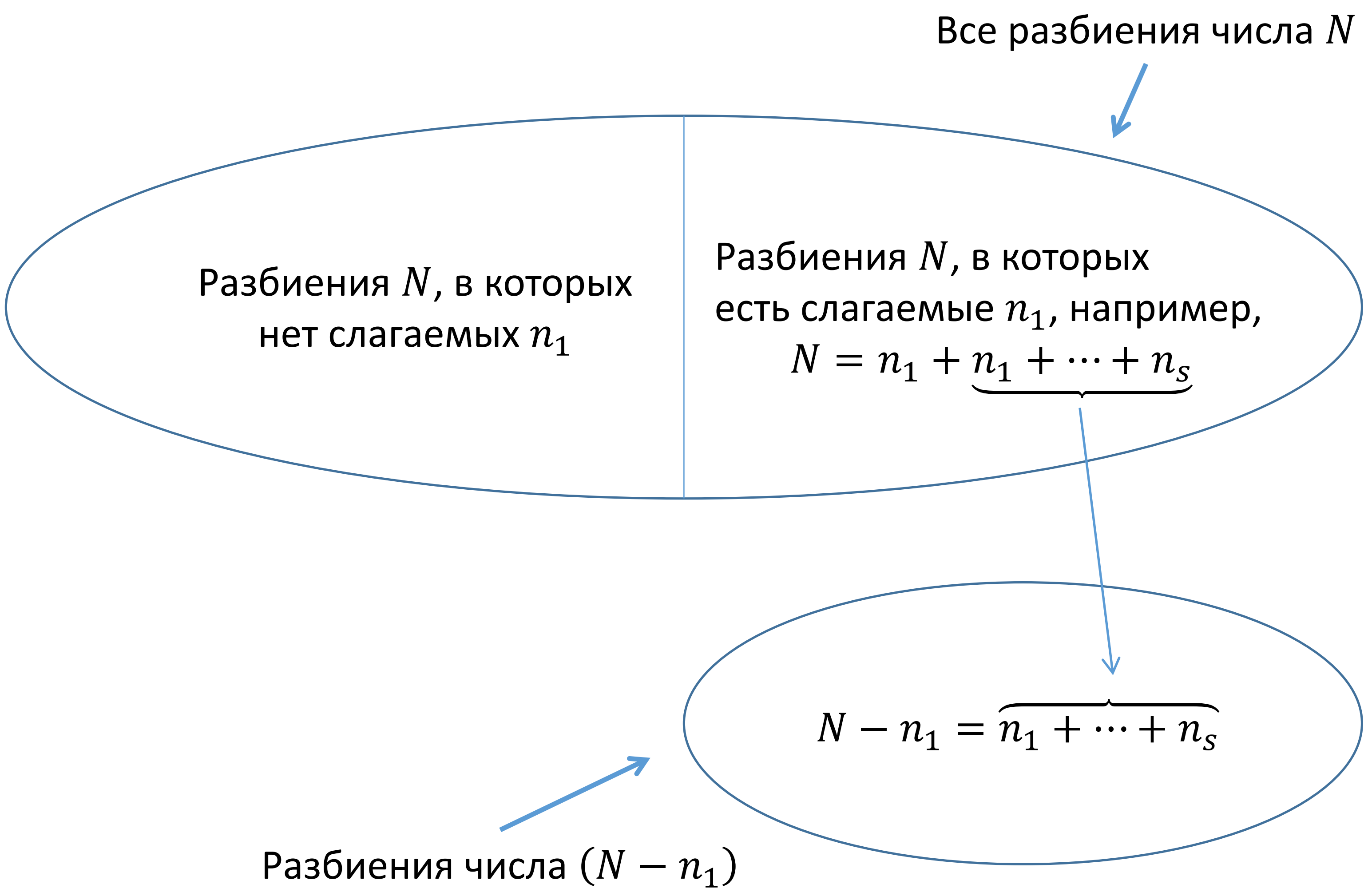
Таким образом, наша задача эквивалентна нахождению $p(50;\ 1, 2, 5, 10)$

# Рекуррентное соотношение для числа упорядоченных разбиений

Рекуррентное соотношение:

$$p(N;\ n_1, n_2, \dots, n_s) = p(N;\ n_2, \dots, n_s) + p(N - n_1;\ \ n_1, n_2, \dots, n_s)$$

# Доказательство соотношения



# Рекуррентное соотношение для числа упорядоченных разбиений

Используя соотношение

$$p(N;\ n_1, n_2, \dots, n_s) =$$
$$= p(N;\ n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_s) + p(N - n_i;\ \ n_1, n_2, \dots, n_s)$$

в принципе всегда можно вычислить $p(\dots)$:

$$p(10;\ 1, 2, 5) = p(10;\ 1, 2) + \underbrace{p(5;\ 1, 2, 5)}_{=4}$$

$$p(10;\ 1, 2) = \underbrace{p(10;\ 1)}_{=1} + p(8;\ 1, 2)$$

и так далее…

# Формула Харди—Рамануджана

Простой формулы для $p(N)$ нет, но есть асимптотика:

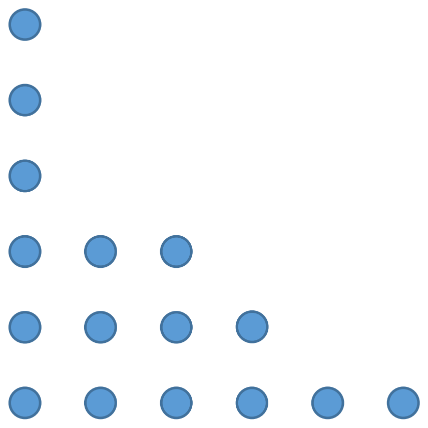
$$p(N) \sim \frac{1}{4N\sqrt{3}} \cdot e^{\pi\sqrt{2N/3}}$$

# Диаграммы разбиений

Разбиение:

$$16 = 1 + 1 + 1 + 3 + 4 + 6$$

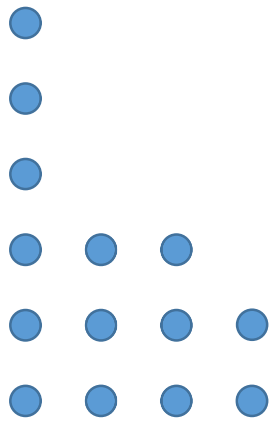
Диаграмма:



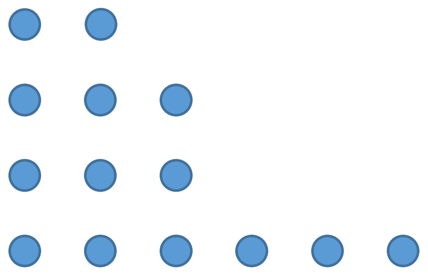
Математически можно считать диаграмму матрицей из нулей и единиц (*0,1-матрицей*).

# Диаграммы разбиений

Диаграмма:

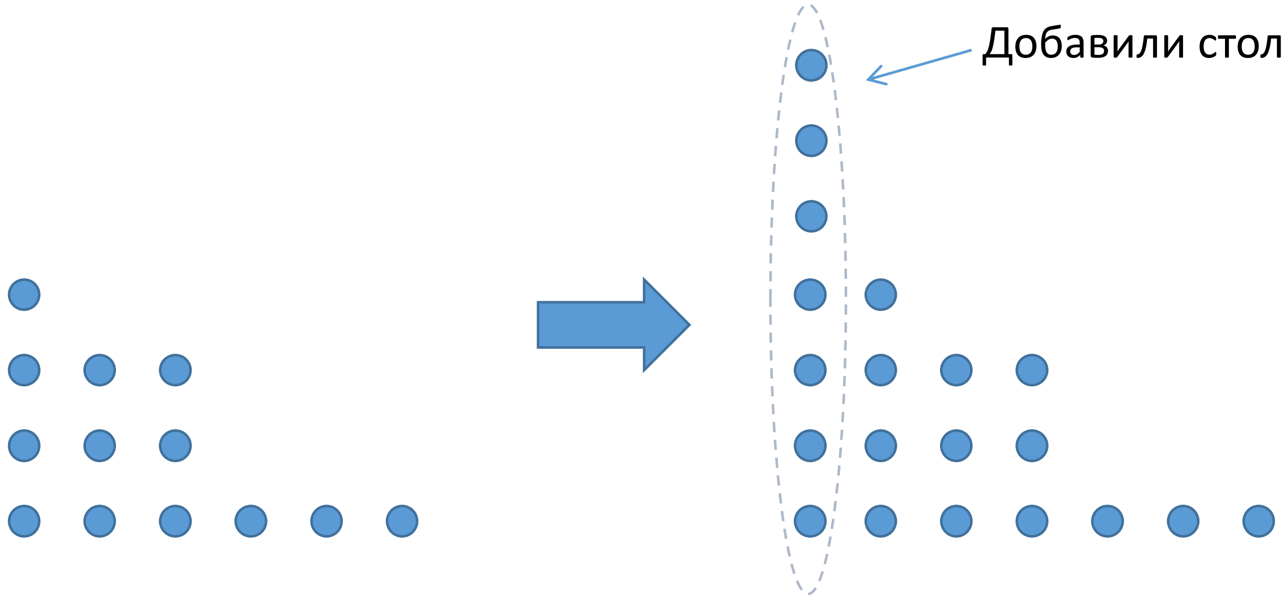


Двойственная диаграмма (транспонируем матрицу):



**Теорема.** Количество (неупорядоченных) разбиений числа $N$ на $k$ слагаемых равно количеству разбиений $N$ на слагаемые, максимальное из которых равно $k$.

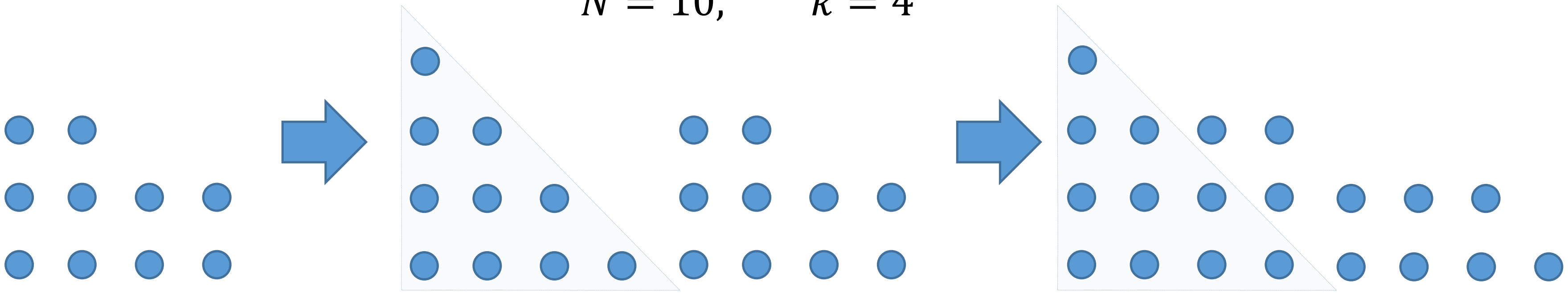
# Диаграммы разбиений




**Теорема.** Количество (неупорядоченных) разбиений числа $N$ на *не более чем* $k$ слагаемых равно количеству разбиений $N + k$ *ровно* на $k$ слагаемых.

# Диаграммы разбиений

$N = 10, \qquad k = 4$



**Теорема.** Количество (неупорядоченных) разбиений числа $N$ на не более чем $k$ слагаемых равно количеству разбиений $N + \frac{k(k+1)}{2}$ на $k$ *различных* слагаемых.

# Теорема Эйлера

Обозначим $p_{\text{чёт}}(N)$ и $p_{\text{неч}}(N)$ количества неупорядоченных разбиений $N$ соответственно на чётное и нечётное число различных слагаемых (чётность самих слагаемых любая!).

**Теорема.**

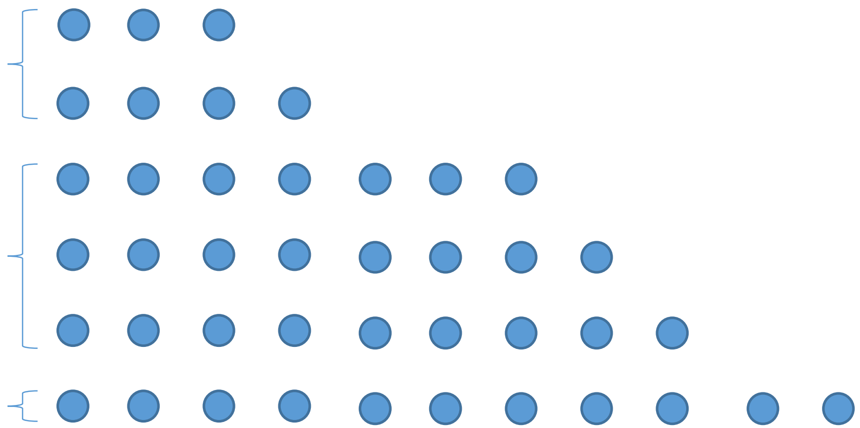
$$p_{\text{чёт}}(N) - p_{\text{неч}}(N) = \begin{cases} (-1)^k, & \text{если } N = \frac{3k^2 \pm k}{2} \\ 0, & \text{иначе} \end{cases}$$

(То есть разбиений на чётное/нечётное число слагаемых почти поровну.)

# Доказательство теоремы Эйлера

*Доказательство:*

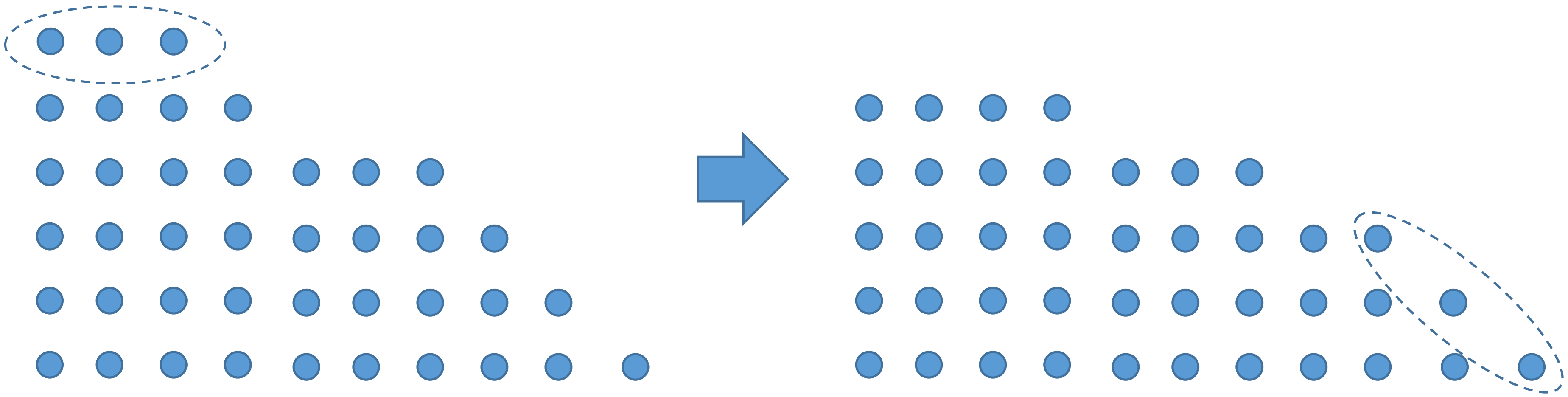
Диаграмма разбиения на различные слагаемые представляет собой набор трапеций. Укажем преобразование, меняющее чётность количества строк в диаграмме…



# Доказательство теоремы Эйлера: преобразования диаграмм

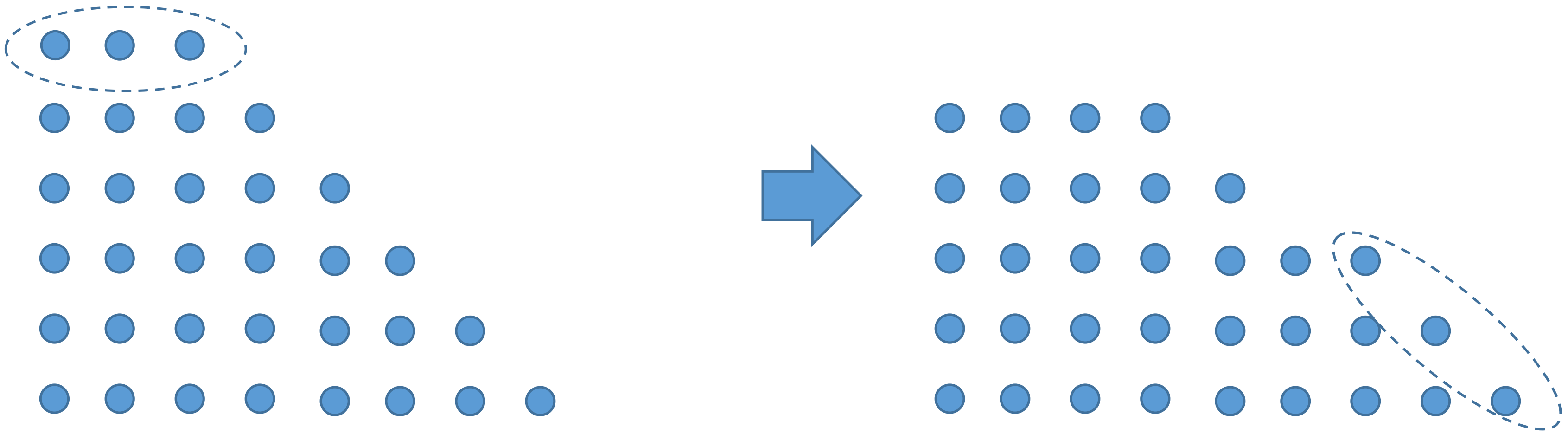
Пусть в первой строке диаграммы $m$ точек, а в нижней трапеции $k$ строк.

Если $m \leq k$, то выполним преобразование $\Pi_1$: отбросим первую строку диаграммы, «раздав» её точки строкам нижней трапеции:



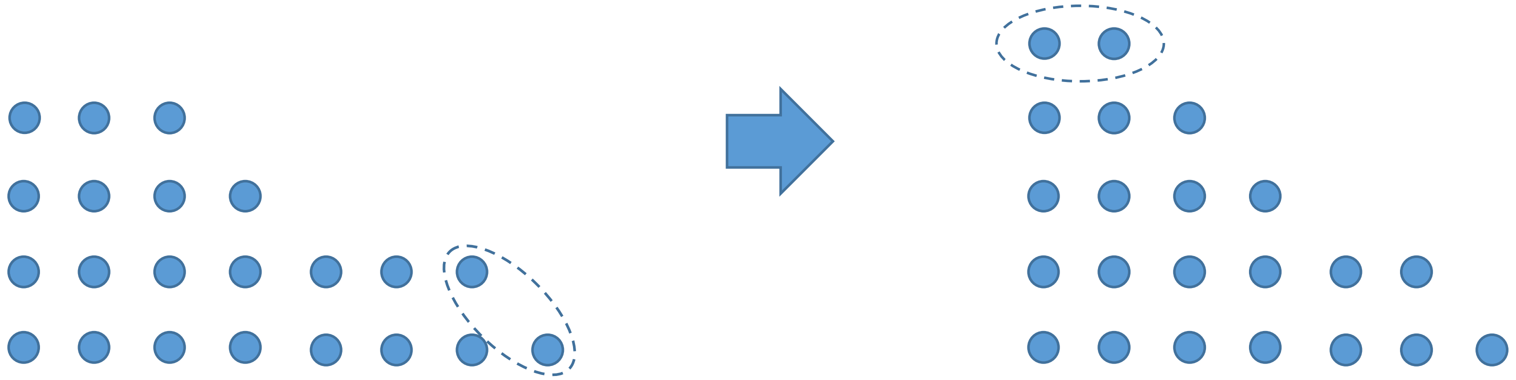
# Доказательство теоремы Эйлера: преобразования диаграмм

Аналогичное преобразование можно сделать, если трапеция была всего одна, но выполнялось неравенство $m \le k-1$.



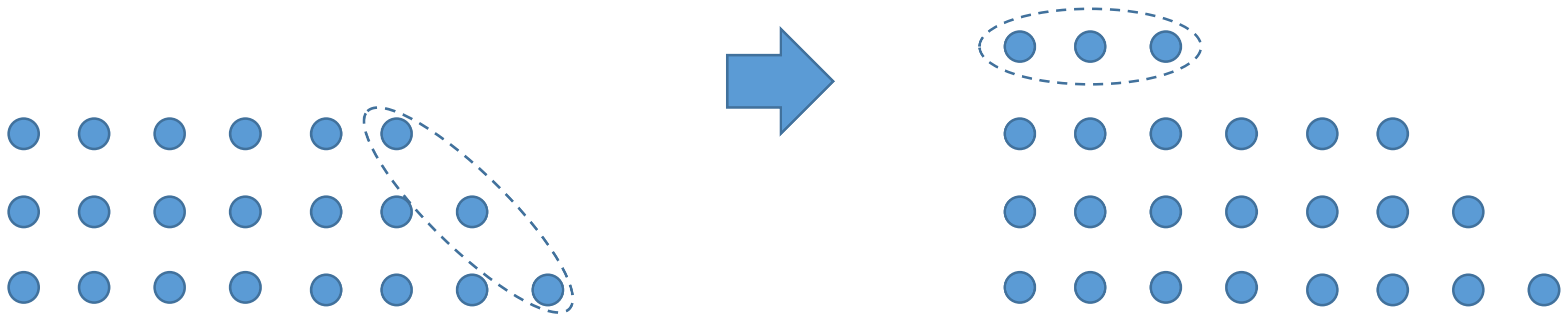
# Доказательство теоремы Эйлера: преобразования диаграмм

Если же у нас по крайней мере две трапеции, и $m > k$, то выполним преобразование $\Pi_2$: от каждой строки нижней трапеции берём по точке, и составляем из них новую верхнюю строку.



# Доказательство теоремы Эйлера: преобразования диаграмм

Аналогичное преобразование можно сделать, если трапеция была всего одна, но выполнялось неравенство $m > k + 1$.



# Доказательство теоремы Эйлера: свойства преобразований $\Pi_1$ и $\Pi_2$

К одной и той же диаграмме нельзя применить одновременно оба преобразования $\Pi_1$ и $\Pi_2$.

Преобразования $\Pi_1$ и $\Pi_2$ взаимно обратные: если применить их к диаграмме последовательно, получится исходная диаграмма.

Значит, из разных диаграмм при этих преобразованиях получаются разные.

Преобразования $\Pi_1$ и $\Pi_2$ меняют чётность числа строк в диаграмме.

# Доказательство теоремы Эйлера: случай, когда есть биекция

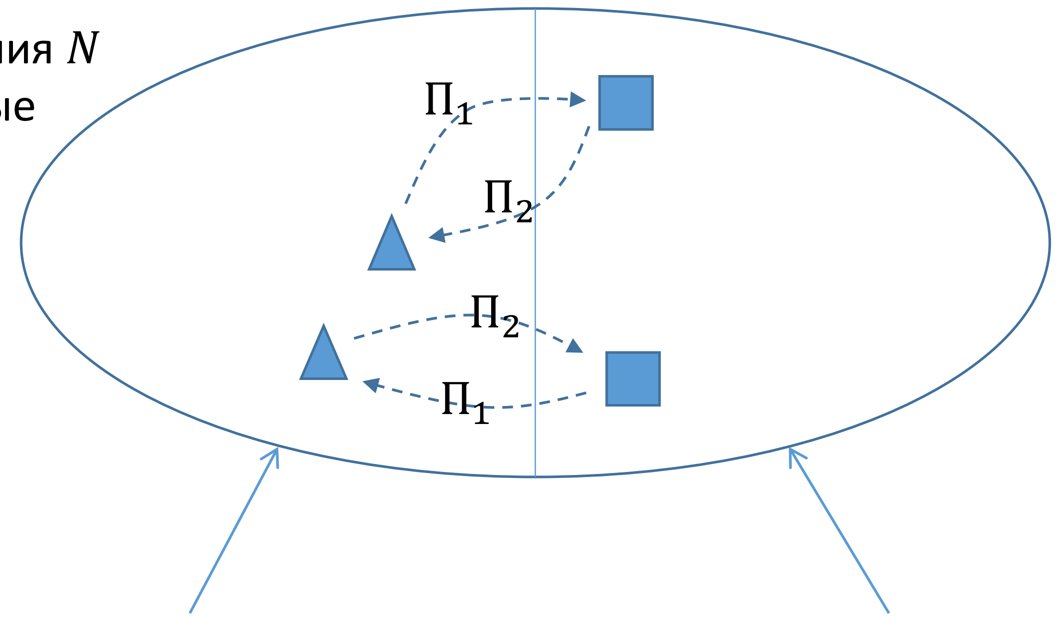
Из указанных свойств $\Pi_1$ и $\Pi_2$ следует, что если к любой диаграмме разбиения числа $N$ на различные слагаемые применимо одно из преобразований $\Pi_1, \Pi_2$, то *есть взаимно однозначное соответствие между разбиениями с чётным и нечётным числом слагаемых*, и следовательно для таких $N$

$$p_{\text{чёт}}(N) - p_{\text{неч}}(N) = 0$$

# Доказательство теоремы Эйлера: иллюстрации

Случай, когда к любой диаграмме применимо $\Pi_1$ или $\Pi_2$: тогда у нас биекция

Все разбиения $N$
на различные
слагаемые




Разбиения с нечётным числом слагаемых $\leftrightarrow$ Разбиения с чётным числом слагаемых

# Доказательство теоремы Эйлера: случай, когда нет биекции

А для каких диаграмм неприменимы $\Pi_1, \Pi_2$?

Ответ: для тех, где ровно одна трапеция, и при этом либо $m = k$, либо $m = k + 1$.

В случае $m = k$ имеем

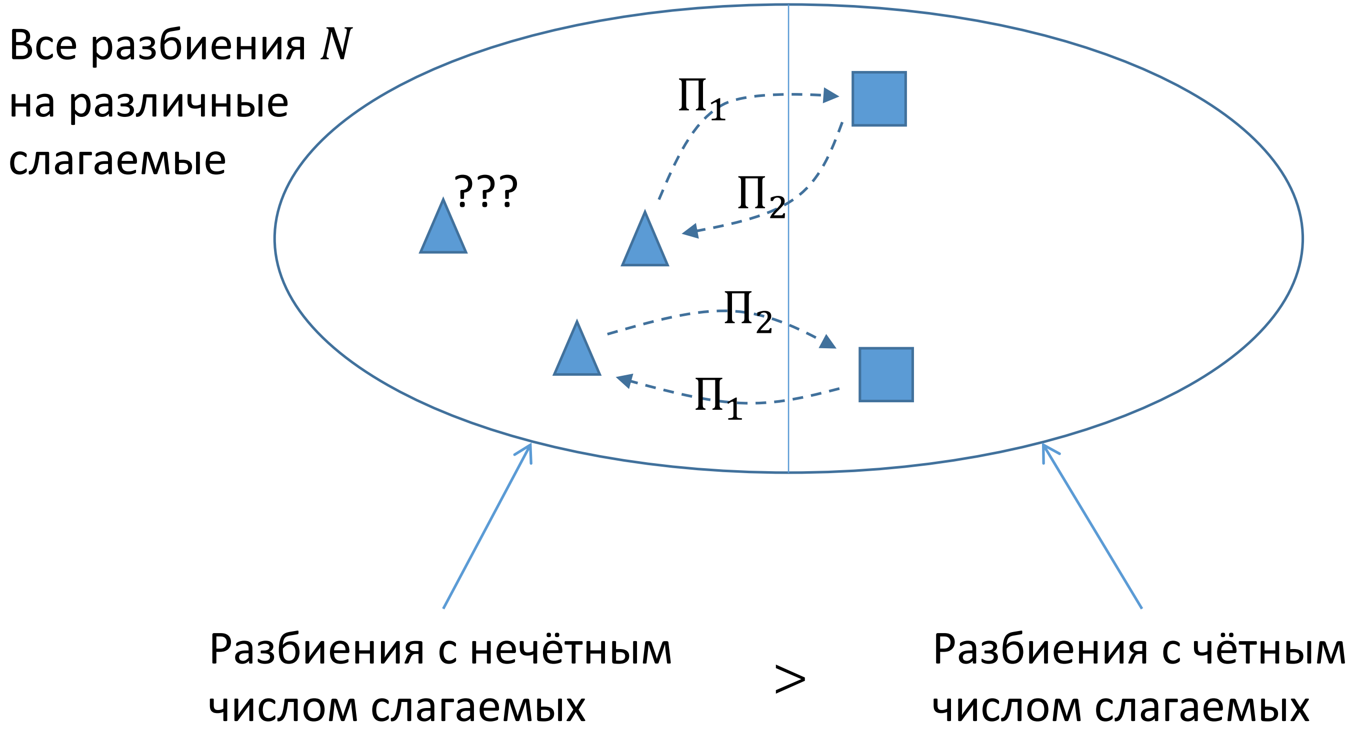
$$N = \sum_{i=k}^{2k-1} i = \frac{3k^2 - k}{2}$$

В случае $m = k + 1$ имеем

$$N = \sum_{i=k+1}^{2k} i = \frac{3k^2 + k}{2}$$

# Доказательство теоремы Эйлера: иллюстрации

Случай, когда есть «плохая» диаграмма к которой неприменимы ни $\Pi_1$ ни $\Pi_2$: тогда у нас биекция между всеми остальными, кроме неё



# Доказательство теоремы Эйлера: случай, когда нет биекции

Таким образом, если у числа $N$ есть разбиение, диаграмма которой представляет собой одиночную трапецию с $m = k$ или $m = k + 1$ то

$$N = \frac{3k^2 - k}{2} \quad \text{или} \quad N = \frac{3k^2 - k}{2}$$

и при чётных $k$ это разбиение имеет чётное число слагаемых, и тогда $p_{\text{чёт}}(N) = 1 + p_{\text{неч}}(N)$ а при нечётных $k$ — нечётное число слагаемых, и тогда $p_{\text{неч}}(N) = 1 + p_{\text{чёт}}(N)$.

То есть в любом из этих случаев

$$p_{\text{чёт}}(N) - p_{\text{неч}}(N) = (-1)^k$$