# Дискретные структуры

МФТИ, весна 2014

Александр Дайняк

www.dainiak.com

# Формальные степенные ряды

*Формальный степенной ряд* — это запись вида

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \cdots$$

Числа $a_0, a_1$, … называются *коэффициентами ряда*.

# Операции над рядами

Обозначим

$$A(x) \coloneqq a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \cdots$$
$$B(x) \coloneqq b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k + \cdots$$

- *Сумма* рядов $A$ и $B$ — это ряд
$$c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k + \cdots$$
с коэффициентами $c_k = a_k + b_k$
- *Разность* рядов $A$ и $B$ — это ряд с коэффициентами $c_k = a_k - b_k$

# Операции над рядами

Обозначим

$$A(x) \coloneqq a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \cdots$$
$$B(x) \coloneqq b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k + \cdots$$

- *Произведение* рядов $A$ и $B$ — это ряд

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k + \cdots$$

с коэффициентами

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

# Операции над рядами

Обозначим

$$A(x) \coloneqq a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \cdots$$
$$B(x) \coloneqq b_0 + b_1 x + b_2 x^2 + \cdots + b_k x^k + \cdots$$

Пусть $b_0 \neq 0$.

- *Частное* рядов $A$ и $B$ — это ряд
$$c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k + \cdots$$
коэффициенты которого определяются последовательно из соотношений:
$c_0 \coloneqq \frac{a_0}{b_0}$, $c_1 \coloneqq \frac{a_1 - b_1 c_0}{b_0}$, $c_2 \coloneqq \frac{a_2 - b_2 c_0 - b_1 c_1}{b_0}$, …

# Операции над рядами

*Производная* ряда

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \cdots$$

— это ряд

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k + \cdots$$

с коэффициентами

$$c_k := (k+1) a_{k+1}$$

# Производящие функции

*Производящая функция* числовой последовательности $a_0, a_1, \ldots$ — это сумма ряда

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \cdots$$

(при условии, что в окрестности нуля ряд сходится)

Например, производящая функция последовательности $\binom{n}{0}, \binom{n}{1}, \binom{n}{2} \ldots$ — это ряд

$$\binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \cdots + \binom{n}{n} x^n + \cdots$$

Мы знаем, что этот ряд можно «свернуть»:

$$(1 + x)^n$$

# Производящие функции

*Основное правило применения производящих функций:*

Любая функция может быть производящей функцией не более чем одной последовательности.

А это значит, что если мы взяли две последовательности, на первый взгляд «разные», и доказали, что их производящие функции равны в окрестности нуля, то и сами последовательности совпадают.

# Радиус сходимости

Для применимости метода нужно проверять, что ряды сходятся в окрестности нуля.

*Радиус сходимости* ряда $\sum a_k x^k$ — это такое $r$, что ряд сходится при всех $x$, таких, что $|x| < r$. ($x$ в общем случае комплексное)

Радиус сходимости помогает найти **Теорема Коши:**

$$r = \left( \overline{\lim_{k \to \infty}} \sqrt[k]{a_k} \right)^{-1}$$

# Рациональные производящие функции

**Утверждение.**
Если последовательность $\{a_k\}$ удовлетворяет л.р.с. с п.к.,
то производящая функция $f$ для $\{a_k\}$ представима в виде

$$f(x) = \frac{P(x)}{Q(x)},$$

где $P, Q \in \mathbb{R}[x]$.

# Доказательство утверждения

Пусть п-ть $\{a_k\}$ удовлетворяет соотношению $c_r a_{k+r} + \cdots + c_0 a_k = 0$, или, что то же самое,

$$c_r a_k + c_{r-1} a_{k-1} \ldots + c_1 a_{k-r+1} + c_0 a_{k-r} = 0.$$

Пусть $f(x) \coloneqq \sum a_k x^k$. Имеем

$$c_0 x^r \cdot f(x) = \sum_{k=r}^{\infty} c_0 a_{k-r} x^k$$

$$c_1 x^{r-1} \cdot f(x) = \sum_{k=r-1}^{\infty} c_1 a_{k-r+1} x^k$$

$$\vdots$$

$$c_r \cdot f(x) = \sum_{k=0}^{\infty} c_r a_k x^k$$

Отсюда $(c_0 x^r + c_1 x^{r-1} + \cdots + c_r) \cdot f(x) = P(x) + \sum_{k=r}^{\infty} \underbrace{(c_r a_k + c_{r-1} a_{k-1} \ldots + c_1 a_{k-r+1} + c_0 a_{k-r})}_{=0} x^k$,

где $P$ — многочлен степени не выше $(r-1)$.

# Применение производящих функций

Пусть надо вычислить сумму

$$\sum_{k=0}^{n} k^2 \binom{n}{k} \frac{1}{2^k}$$

Заметим, что она равняется $g(1/2)$, где $g(x)$ — производящая функция для последовательности

$$a_k = k^2 \binom{n}{k}$$

то есть

$$g(x) := \sum_{k=0}^{\infty} k^2 \binom{n}{k} x^k$$

# Применение производящих функций

Имеем $g(x) = \sum_{k=0}^{\infty} k^2 \binom{n}{k} x^k$

Пусть $f(x) := \sum_{k=0}^{\infty} \binom{n}{k} x^k = (1+x)^n$.

Заметим, что $g(x) = x\big(xf'(x)\big)'$, а значит

$$g(x) = x\left(x\big((1+x)^n\big)'\right)' = x(xn(1+x)^{n-1})' =$$
$$= xn\big((1+x)^{n-1} + x(n-1)(1+x)^{n-2}\big)$$

И теперь легко вычислить

$$g(1/2) = \frac{n}{2}\left(\left(\tfrac{3}{2}\right)^{n-1} + \tfrac{1}{2}n(n-1)\cdot\left(\tfrac{3}{2}\right)^{n-2}\right)$$

# Обобщённая формула бинома

«Обычная» формула бинома для $n \in \mathbb{N}$:

$$(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$$

Обобщённая формула бинома для $\alpha \in \mathbb{R}$:

$$(1+x)^\alpha = 1 + \binom{\alpha}{1}x + \binom{\alpha}{2}x^2 + \cdots + \binom{\alpha}{k}x^k + \cdots$$

Здесь $\binom{\alpha}{k}$ — обобщённые биномиальные коэффициенты:

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdot \ldots \cdot \big(\alpha-(k-1)\big)}{k!}$$

# Обобщённая формула бинома

$$(1+x)^{\alpha} = 1 + \binom{\alpha}{1}x + \binom{\alpha}{2}x^2 + \cdots, \quad \text{где } \binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdot\ldots\cdot(\alpha-(k-1))}{k!}$$

**Пример применения:**

$$(1+x)^{1/2} = 1 + \frac{1}{2}x + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)}{2!}x^2 + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)}{3!}x^3 + \cdots =$$

$$= 1 + \frac{1}{2}x + \frac{(1-2)}{2!\cdot 2^2}x^2 + \frac{(1-2)(1-4)}{3!\cdot 2^3}x^3 + \cdots$$

$$= 1 + \frac{1}{2}x - \frac{1}{2!\cdot 2^2}x^2 + \frac{1\cdot 3}{3!\cdot 2^3}x^3 - \frac{1\cdot 3\cdot 5}{4!\cdot 2^4} + \cdots$$

$$= 1 + x\sum_{k=0}^{\infty}(-1)^k \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2k-1)}{(k+1)!\,2^{k+1}}x^k$$

# Обобщённая формула бинома

Ещё немного преобразуем:

$$(1+x)^{1/2} = 1 + x\sum_{k=0}^{\infty}(-1)^k \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2k-1)}{(k+1)!\,2^{k+1}}x^k$$

$$= 1 + x\sum_{k=0}^{\infty}(-1)^k \frac{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot \ldots \cdot (2k-2)(2k-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot (2k-2)\cdot (k+1)!\,2^{k+1}}x^k$$

$$= 1 + x\sum_{k=0}^{\infty}(-1)^k \frac{(2k-1)!}{2^{k-1}(k-1)!\cdot (k+1)!\,2^{k+1}}x^k$$

$$= 1 + x\sum_{k=0}^{\infty}\frac{(2k-1)!}{(k-1)!\cdot (k+1)!}\left(-\tfrac{1}{4}x\right)^k$$

# Числа Каталана

Одно из многочисленных определений:

Число Каталана $a_n$ — это количество правильных скобочных последовательностей из $n$ пар скобок

Пример, при $n = 3$ имеем $a_3 = 5$:

$$\big((\ \ )\big),\ (\ \ )(\ \ ),\ (\ \ )\big((\ \ )\big),\ \big((\ \ )\big)(\ \ ),\ (\ \ )(\ \ )(\ \ )$$

# Числа Каталана: рекуррентное соотношение

**Рекуррентное соотношение для чисел Каталана:**

$$a_{n+1} = \sum_{k=0}^{n} a_k a_{n-k}$$

Обоснование:

$$\underbrace{(\text{прав. ск. посл.})}_{\text{внутри } k \text{ пар скобок}} \underbrace{\text{прав. ск. посл.}}_{(n-k) \text{ пар скобок}}$$

**Начальные условия:** $a_0 = a_1 = 1$

# Числа Каталана: производящая функция

Рассмотрим производящую функцию для последовательности чисел Каталана:

$$A(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

Заметим, что соотношение $a_{n+1} = \sum_{k=0}^{n} a_k a_{n-k}$ похоже по форме на то, что возникает при произведении рядов. Рассмотрим

$$A(x) \cdot A(x) =$$
$$= a_0^2 + (a_0 a_1 + a_1 a_0)x + (a_0 a_2 + a_1 a_1 + a_2 a_0)x^2$$
$$+ (a_0 a_3 + a_1 a_2 + a_2 a_1 + a_3 a_0)x_3 + \cdots =$$
$$= a_1 + a_2 x + a_3 x^2 + a_4 x^3 + \cdots$$

# Числа Каталана: производящая функция

Итак,

$$\big(A(x)\big)^2 = a_1 + a_2 x + a_3 x^2 + a_4 x^3 + \cdots$$

Отсюда

$$a_0 + x\big(A(x)\big)^2 = a_0 + a_1 x + a_2 x^2 + \cdots = A(x)$$

Получаем уравнение для производящей функции $A$:

$$a_0 + x\big(A(x)\big)^2 = A(x)$$

# Числа Каталана: производящая функция

Уравнение для производящей функции:

$$x\big(A(x)\big)^2 - A(x) + 1 = 0$$

Отсюда

$$A(x) = \frac{1 \pm \sqrt{1 - 4x}}{2x}$$

Теперь воспользуемся обобщённой формулой бинома, чтобы записать $A(x)$ в виде ряда:

$$A(x) = \frac{1 \pm (1 + (-4x))^{1/2}}{2x}$$

# Числа Каталана: вывод формулы

$$A(x) = \frac{1 \pm (1 + (-4x))^{1/2}}{2x}$$

где по формуле обобщённого бинома

$$(1 + (-4x))^{1/2} =$$

$$= 1 + \frac{1}{2}(-4x) + \frac{\frac{1}{2}\left(\frac{1}{2} - 1\right)}{2!}(-4x)^2 + \frac{\frac{1}{2}\left(\frac{1}{2} - 1\right)\left(\frac{1}{2} - 2\right)}{3!}(-4x)^3 + \cdots$$

Отсюда уже видно, что на самом деле

$$A(x) = \frac{1 - (1 + (-4x))^{1/2}}{2x}$$

# Числа Каталана: вывод формулы

Подставим в выражение для $A(x)$ ряд для $(1+(-4x))^{1/2}$:

$$A(x)=\frac{1-\left(1+(-4x)\sum_{k=0}^{\infty}\frac{(2k-1)!}{(k-1)!\cdot(k+1)!}x^k\right)}{2x}$$

Отсюда

$$A(x)=2\sum_{k=0}^{\infty}\frac{(2k-1)!}{(k-1)!\cdot(k+1)!}x^k$$

В итоге

$$a_k=2\frac{(2k-1)!}{(k-1)!\cdot(k+1)!}=\frac{(2k-1)!\cdot 2k}{(k-1)!\cdot k\cdot(k+1)!}=\frac{(2k)!}{k!\cdot(k+1)!}=\frac{\binom{2k}{k}}{k+1}$$

# Числа Каталана

Итак,

$$a_k = \frac{\binom{2k}{k}}{k+1}$$

Асимптотика:

$$a_k \sim \frac{4^k}{\sqrt{\pi} \cdot k^{3/2}}$$

# Теорема Эйлера

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

**Теорема.**

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

# Производящая функция для числа неупорядоченных разбиений

**Утверждение.**

Если $p(N)$ — количество неупорядоченных разбиений числа $N$, то для производящей функции последовательности $p(0), p(1), \ldots$ справедлива формула

$$\sum_{n=0}^{\infty} p(n) \cdot x^n = \prod_{k=1}^{\infty} \frac{1}{1 - x^k}$$

# Производящая функция для числа неупорядоченных разбиений

Т.к. $(1-t)^{-1} = 1 + t + t^2 + \cdots,$ то

$$\prod_{k=1}^{\infty}\left(1-x^k\right)^{-1} = \left(\sum_{i_1} x^{i_1}\right)\left(\sum_{i_2} x^{2i_2}\right)\left(\sum_{i_3} x^{3i_3}\right)\cdot \ldots = \sum_{n=0}^{\infty} a_n x^n$$

где $a_n$ — количество наборов $(i_1, i_2, i_3, \ldots)$ таких, что

$$n = i_1 + 2i_2 + 3i_3 + \cdots$$

# Производящая функция для числа неупорядоченных разбиений

$$\prod_{k=1}^{\infty}\left(1-x^k\right)^{-1}=\sum_{n=0}^{\infty}a_n x^n$$

где $a_n$ — количество наборов $(i_1, i_2, i_3, \dots)$ таких, что

$$n = i_1 + 2i_2 + 3i_3 + \cdots$$

Любой такой набор $(i_1, i_2, i_3, \dots)$ однозначно соответствует разбиению числа $n$, в котором $i_1$ слагаемых равны $1$, $i_2$ слагаемых равны $2$, и т.д.

Отсюда следует, что $a_n = p(n)$.

# Вывод рекуррентного соотношения для числа неупорядоченных разбиений

Итак,

$$\prod_{k=1}^{\infty} \frac{1}{1-x^k} = \sum_{n=0}^{\infty} p(n)x^n$$

Отсюда

$$\left(\sum_{n=0}^{\infty} p(n)x^n\right) \cdot \left(\prod_{k=1}^{\infty} \left(1-x^k\right)\right) = 1$$

# Вывод рекуррентного соотношения для числа неупорядоченных разбиений

$$\left(\sum_{n=0}^{\infty} p(n)x^n\right) \cdot \left(\prod_{k=1}^{\infty}\left(1-x^k\right)\right) = 1$$

Разложим в ряд произведение $\prod_{k=1}^{\infty}\left(1-x^k\right)$:

$$(1-x)(1-x^2)(1-x^3)\cdot \ldots = \sum_{m=0}^{\infty} b_m x^m$$

где $b_m = p_{\text{чёт}}(m) - p_{\text{неч}}(m)$.

# Вывод рекуррентного соотношения для числа неупорядоченных разбиений

$$\left(\sum_{n=0}^{\infty} p(n)x^n\right)\cdot\left(\sum_{m=0}^{\infty} b_m x^m\right)=1$$

где

$$b_m=\begin{cases}(-1)^k, & \text{если } \exists k: m=\frac{3k^2\pm k}{2}\\ 0, & \text{иначе}\end{cases}$$

Итак,

$$\left(\sum_{n=0}^{\infty} p(n)x^n\right)\cdot\left(1+\sum_{k=1}^{\infty}(-1)^k\left(x^{(3k^2-k)/2}+x^{(3k^2+k)/2}\right)\right)=1$$

# Вывод рекуррентного соотношения для числа неупорядоченных разбиений

$$\left(\sum_{j=0}^{\infty} p(j)x^j\right)\cdot\left(1+\sum_{k=1}^{\infty}(-1)^k\left(x^{(3k^2-k)/2}+x^{(3k^2+k)/2}\right)\right)=1$$

При раскрытии скобок и приведении подобных слагаемых коэффициенты при всех положительных степенях $x$ должны быть нулевыми, отсюда для любого $m>0$ выполнено

$$p(m)+\sum_{k>0}(-1)^k\left(p\left(m-\frac{3k^2-k}{2}\right)+p\left(m-\frac{3k^2+k}{2}\right)\right)=0$$

(считаем формально, что $p(N)=0$ при любом $N<0$)

# Рекуррентное соотношение для числа неупорядоченных разбиений

**Теорема.**

Для любого $m > 0$ выполнено равенство

$$p(m) = \sum_{k>0} (-1)^{k+1} \left( p\left(m - \frac{3k^2-k}{2}\right) + p\left(m - \frac{3k^2+k}{2}\right) \right)$$

Несколько первых слагаемых ряда:

$$p(m) =$$
$$= p(m-1) + p(m-2) - p(m-5) - p(m-7) + p(m-12)$$
$$+ p(m-15) - \cdots$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

Пусть $f_1, f_2, \ldots$ — последовательность *всех* простых нормногочленов над $\mathbb{Z}_p$, в порядке неубывания их степеней.

Обозначим $d_i \coloneqq \deg f_i$.

Любой нормногочлен $f$ представляется единственным образом в виде

$$f = \left(f_{i_1}\right)^{\alpha_{i_1}} \cdot \ldots \cdot \left(f_{i_s}\right)^{\alpha_{i_s}}$$

где $i_1 < i_2 < \cdots < i_s$ и $\alpha_{i_1}, \ldots, \alpha_{i_s} > 0$. При этом

$$\deg f = d_{i_1}\alpha_{i_1} + \cdots + d_{i_s}\alpha_{i_s}$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

Любой нормногочлен $f$ представляется единственным образом в виде

$$f = \left(f_{i_1}\right)^{\alpha_{i_1}} \cdot \ldots \cdot \left(f_{i_s}\right)^{\alpha_{i_s}}$$

где $i_1 < i_2 < \cdots < i_s$ и $\alpha_{i_1}, \ldots, \alpha_{i_s} > 0$.

Поэтому для любого $n$ число наборов $(\alpha_1, \alpha_2, \alpha_3, \ldots)$, удовлетворяющих уравнению

$$n = d_1\alpha_1 + d_2\alpha_2 + d_3\alpha_3 + \cdots$$

равно $p^n$ (т.к. каждому такому набору $(\alpha_1, \alpha_2, \alpha_3, \ldots)$ можно взаимно однозначно сопоставить многочлен степени $n$).

# Количество неприводимых многочленов над $\mathbb{Z}_p$

**Утверждение.**
Выполнено равенство

$$\frac{1}{1-pt} = \prod_{i=1}^{\infty} \frac{1}{1-t^{d_i}}$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

*Доказательство:*

Т.к. $\left(1-t^{d_i}\right)^{-1}=1+t^{d_i}+t^{2d_i}+t^{3d_i}+\cdots$, то

$$\prod_{i=1}^{\infty}\left(1-t^{d_i}\right)^{-1}=\left(\sum_{j_1=0}^{\infty}t^{d_1j_1}\right)\left(\sum_{j_2=0}^{\infty}t^{d_2j_2}\right)\left(\sum_{j_3=0}^{\infty}t^{d_3j_3}\right)\ldots=\sum_{k=0}^{\infty}a_kt^k$$

где $a_k$ — количество наборов $(j_1,j_2,j_3,\ldots)$, удовлетворяющих соотношению $k=d_1j_1+d_2j_2+\cdots$. Значит, $a_k=p^k$, и отсюда

$$\prod_{i=1}^{\infty}\left(1-t^{d_i}\right)^{-1}=\sum_{k=0}^{\infty}p^kt^k=\sum_{k=0}^{\infty}(pt)^k=\frac{1}{1-pt}$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

$$\frac{1}{1-pt} = \prod_{i=1}^{\infty} \frac{1}{1-t^{d_i}}$$

Пусть $M_k$ — количество простых нормногочленов степени $k$.

Тогда

$$\frac{1}{1-pt} = \prod_{k=1}^{\infty} \left( \frac{1}{1-t^k} \right)^{M_k}$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

$$\frac{1}{1-pt} = \prod_{k=1}^{\infty} \left( \frac{1}{1-t^k} \right)^{M_k}$$

Прологарифмируем обе части:

$$\ln \frac{1}{1-pt} = \sum_{k=1}^{\infty} M_k \ln \frac{1}{1-t^k}$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

$$\ln\frac{1}{1-pt}=\sum_{k=1}^{\infty}M_k\ln\frac{1}{1-t^k}$$

Если разложить $\ln\left((1-x)^{-1}\right)$ в ряд, получится

$$\ln\left((1-x)^{-1}\right)=\sum_{j=1}^{\infty}\frac{x^j}{j}$$

Отсюда следует

$$\sum_{j=1}^{\infty}\frac{(pt)^j}{j}=\sum_{k=1}^{\infty}M_k\sum_{j=1}^{\infty}\frac{t^{kj}}{j}$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

$$\sum_{j=1}^{\infty} \frac{(pt)^j}{j} = \sum_{k=1}^{\infty} M_k \sum_{j=1}^{\infty} \frac{t^{kj}}{j}$$

Коэффициенты при $t^n$ для каждого $n$ должны совпадать в левой и правой частях равенства.

Поэтому

$$\frac{p^n}{n} = \sum_{k|n} \frac{M_k}{n/k}$$

Окончательно,

$$p^n = \sum_{k|n} kM_k$$

# Количество неприводимых многочленов над $\mathbb{Z}_p$

$$p^n = \sum_{k|n} kM_k$$

Применяя обращение Мёбиуса, получаем следующую теорему.

**Теорема.**
Число нормногочленов степени $n$, неприводимых над $\mathbb{Z}_p$, равно

$$\frac{1}{n}\sum_{k|n} p^k \mu(n/k)$$

где $\mu$ — функция Мёбиуса.

# Количество неприводимых многочленов над $\mathbb{Z}_p$

**Следствие 1.**
При каждом $p$ и при каждом $n \geq 2$ существует хотя бы один неприводимый над $\mathbb{Z}_p$ нормногочлен степени $n$.

**Следствие 2.**
Число нормногочленов степени $n$, неприводимых над $\mathbb{Z}_p$,
при $n \to \infty$ асимптотически равно

$$\frac{p^n}{n}$$

(*См. доказательство асимптотики для числа циклических слов*)