

КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кафедра системного анализа и информационных технологий

Ш.Т. ИШМУХАМЕТОВ, Б.Г. МУБАРАКОВ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ.
ПРОИЗВОДЯЩИЕ ФУНКЦИИ

Учебно-методическое пособие

Казань 2021

УДК 512.624
ББК 22.144

*Принято на заседании кафедры системного анализа и
информационных технологий
Протокол № 5 от 10 февраля 2021*

*Принято на заседании учебно-методической комиссии Института
вычислительной математики и информационных технологий
Протокол № 8 от 19 марта 2021*

РЕЦЕНЗЕНТ:

кандидат физико-математических наук, доцент
каф. теоретической кибернетики **В.С. Кугураков**

Ишмухаметов Ш.Т., Мубараков Б.Г. Математические основы криптографии. Производящие функции/ Учебно-методическое пособие./ Ш.Т. Ишмухаметов, Б.Г. Мубараков .–Казань: Казанский ун-т, 2021.– 23 с.

Учебное пособие представляет собой введение в раздел "Производящие функции" курса "Математические основы информационной безопасности" и содержит базовые сведения из этого раздела дискретной математики. Пособие снабжено описанием ряда алгоритмов и учебными примерами и заданиями для самостоятельной подготовки по курсу.

©Ш.Т. Ишмухаметов, 2021
©Казанский университет, 2021

Содержание

1	Задача о некоммутативном размене	4
2	Производящие функции	5
3	Вычисление формулы ряда Фибоначчи	7
4	Вычисления n -члена рекуррентной последовательности	9
5	Тест Люка проверки простоты натуральных чисел	11
6	Решение рекуррентных уравнений	12
7	Нахождение производящей функции по ряду	14
8	Анализ алгоритма сортировки	17
9	Решение комбинаторных задач	18
10	Формула включений и исключений	20

Введение

Производящие функции - это специальный вид числовых рядов, используемый для решения различных комбинаторных задач и оценки сложности рекуррентных алгоритмов. Они были введены и рассмотрены Леонардом Эйлером в середине 50-х годов 18 века для решения рекуррентных уравнений.

В современной математике производящие функции изучаются в курсе "Дискретная математика".

1 Задача о некоммутативном размене

Начнем изучение производящих функций с одной комбинаторной задачи:

Найти число способов размена n рублей монетами по 1 и 2 рубля, причем размен - некоммутативный, то есть разбиения типа $3 = 1 + 2$ и $3 = 2 + 1$ считаются различными.

Обозначим через f_n искомое число, тогда $f_1 = 1$, $f_2 = 2, \dots$. Число f_3 равно 3 т.к. 3 рубля можно разменять тремя способами:

$$3 = 1 + 1 + 1 = 1 + 2 = 2 + 1.$$

Выведем теперь общую формулу для f_n . Заметим, что все разложения числа n можно разбить на два класса: содержащие первым слагаемым 1 и содержащие первым слагаемым 2. Мощность первого класса равна числу разбиений оставшейся суммы $n - 1$, т.е. f_{n-1} , а мощность второго класса равна f_{n-2} , значит,

$$f_n = f_{n-1} + f_{n-2}. \quad (1.1)$$

Числовой ряд, начинающийся с двух единиц и формулой общего члена (1.1), называется рядом Фиббоначчи. Первыми членами его являются числа

$$1, 1, 2, 3, 5, 8, 13, 21, \dots$$

Наша задача состоит в том, чтобы найти формулу общего члена ряда Фиббоначчи. Будем решать эту задачу, вводя общие понятия теории производящих функций.

2 Производящие функции

Пусть задана числовая последовательность $\{a_n\}$. Производящей функцией для этой последовательности называется функция (комплексной переменной) $A(z)$:

$$A(z) = a_0 + a_1z + a_2z^2 + \dots = \sum_{n=0}^{\infty} a_n z^n$$

Простейшей производящей функцией является функция, построенная для последовательности $\{a_n\}$, $a_n = 1$, состоящей из одних единиц:

$$A(z) = \sum_{n=0}^{\infty} z^n = 1 + z + z^2 + \dots = \frac{1}{1-z}. \quad (2.2)$$

Такой ряд представляет собой бесконечную геометрическую последовательность со знаменателем z , которая сходится к сумме $1/(1-z)$ при условии $|z| < 1$. Сумма ряда $1/(1-z)$ называется *производящей функцией* для последовательности $\{a_n\}$, состоящей из единиц.

Выполняя в (2.2) постановку $f(z) \rightarrow z$ в, получим другие примеры производящих функций. Подставим, например, $2z$ вместо z :

$$A(z) = \sum_{n=0}^{\infty} (2z)^n = 1 + 2z + 4z^2 + \dots + 2^n z^n + \dots = \frac{1}{1-2z}. \quad (2.3)$$

Подставляя в (1) $-z$ вместо z , получим:

$$A(z) = \sum_{n=0}^{\infty} (-z)^n = 1 - z + z^2 - \dots + (-1)^n z^n + \dots = \frac{1}{1+z}. \quad (2)$$

Определим линейную комбинацию производящих функций следующим образом:

$$\alpha F(z) + \beta G(z) = \sum_{n \geq 0} \alpha f(z) + \beta g(z),$$

Пример. Пусть $A(z)$ такое, как в (2.3), а $B(z)$ задано следующим образом:

$$B(z) = \sum_{n=0}^{\infty} (nz)^n = 1 + 2z + 3z^2 + \dots + nz^n + \dots \quad (3)$$

Определим линейную комбинацию $2A(z) + 5B(z)$:

$$2A(z) + 5B(z) = \sum_{n=0}^{\infty} (2 \cdot 2^n + 5n) z^n$$

Дифференцирование производящих функций

Пусть задана производящая функция

$$A(z) = a_0 + a_1z + a_2z^2 + \dots = \sum_{n=0}^{\infty} a_n z^n$$

Дифференцируя этот ряд, получим

$$A'(z) = a_1 + 2a_2z + 3a_3z^2 + \dots = \sum_{n=1}^{\infty} n a_n z^{n-1}$$

Изменим нумерацию слагаемых так, что она опять начиналась с нуля (для этого подставим везде $n + 1$ вместо n). Получим

$$A'(z) = \sum_{n=0}^{\infty} (n + 1) a_{n+1} z^n$$

Пример. Продифференцируем ряд (1) $A(z) = \sum_{n=0}^{\infty} z^n = 1/(1 - z)$:

$$A'(z) = \left(\frac{1}{1 - z} \right)' = \frac{1}{(1 - z)^2} = \sum_{n=0}^{\infty} (n + 1) z^n = 1 + 2z + 3z^2 + \dots$$

Интегрирование производящих функций

Аналогичным образом проинтегрируем геометрическую прогрессию $A(z) = \sum_{n=0}^{\infty} a_n z^n$. Получим ряд:

$$\int A(z) dz = \sum_{n=0}^{\infty} a_n \int z^n dz = \sum_{n=0}^{\infty} \frac{a_n}{n + 1} z^{n+1} + C$$

Значение константы C можно найти, подставляя в полученное выражение значение $z = 0$.

Пример. Проинтегрируем ряд (1) $\int \frac{1}{1-z} dz = \sum_{n=0}^{\infty} \int z^n dz$. Получим:

$$-\ln |1 - z| = \sum_{n=0}^{\infty} \frac{1}{n + 1} z^{n+1} = z + z^2/2 + z^3/3 + \dots$$

Таблица производящих функций

№	Числовой ряд	Производящая функция
1	$1 + z + z^2 + \dots = \sum_{n=0}^{\infty} z^n$	$1/(1 - z)$
2	$\sum_{n=0}^{\infty} (-1)^n z^n$	$1/(1 + z)$
3	$1 + z^2 + z^4 + \dots$	$1/(1 - z^2)$
4	$1 - z + z^2 + \dots + (-1)^n z^n + \dots$	$1/(1 + z)$
5	$1 + 2z + 3z^2 + \dots = \sum_{n=0}^{\infty} (n + 1)z^n$	$1/(1 - z)^2$
6	$\sum_{n=0}^{\infty} (n + 2)(n + 1)z^n$	$2/(1 - z)^3$
7	$\sum_{n=0}^{\infty} (n + k)(n + k - 1) \dots (n + 1)z^n$	$k!/(1 - z)^{k+1}$
8	$1 + z/2 + z^2/3 + \dots + z^n/(n + 1) + \dots$	$\ln(1/1 - z)$

3 Вычисление формулы ряда Фибоначчи

Ряд Фибоначчи определяется рекуррентными формулами

$$f_{n+2} = f_{n+1} + f_n, \quad (3.4)$$

где $f_0 = 1$, $f_1 = 1$. Составляя соответствующую производящую функцию, получим

$$F(z) = 1 + z + 2z^2 + 3z^3 + 5z^4 + \dots = \sum_n f_n z^n.$$

Умножим равенство (3.4) на z^{n+2} и просуммируем по всем n . Получим:

$$\sum_{n=0}^{\infty} f_{n+2} z^{n+2} = \sum_{n=0}^{\infty} f_{n+1} z^{n+2} + \sum_{n=0}^{\infty} f_n z^{n+2}, \text{ откуда}$$

$$F(z) - f_0 - f_1 z = z \cdot \sum_{n=0}^{\infty} f_{n+1} z^{n+1} + z^2 \cdot \sum_{n=0}^{\infty} f_n z^n, \text{ или}$$

$$F(z) - z - 1 = z(F(z) - 1) + z^2 F(z), \text{ или раскрывая скобки}$$

$$F(z) - zF(z) - z^2 F(z) = 1, \text{ откуда}$$

$$F(z) = \frac{1}{1 - z - z^2} = \frac{-1}{z^2 + z - 1} = \frac{-1}{(z - z_1)(z - z_2)}, \quad (4)$$

где $z_1 = (-1 - \sqrt{5})/2$, $z_2 = (-1 + \sqrt{5})/2$ - корни квадратного уравнения $z^2 + z - 1 = 0$.

Дробь $F(z) = -1/(z^2 + z - 1)$ представим в виде суммы двух более простых слагаемых:

$$F(z) = \frac{A}{z - z_1} + \frac{B}{z - z_2}, \text{ где } A, B - \text{ некие константы.}$$

Для нахождения этих констант приведем сумму к общему знаменателю:

$$F(z) = \frac{A(z - z_2) + B(z - z_1)}{z^2 + z - 1} = \frac{(A + B)z - (Az_2 + Bz_1)}{z^2 + z - 1} = \frac{-1}{z^2 + z - 1}$$

откуда

$$\begin{cases} A + B = 0 \\ Az_2 + Bz_1 = 1 \end{cases}$$

Решая эту систему найдем

$$A = \frac{1}{z_2 - z_1} = \frac{1}{\sqrt{5}}, \quad B = -\frac{1}{\sqrt{5}}.$$

Подставим эти значения в выражение для $F(z)$:

$$F(z) = \frac{1}{\sqrt{5}(z - z_1)} - \frac{1}{\sqrt{5}(z - z_2)} = -\frac{1}{z_1\sqrt{5}(1 - z/z_1)} + \frac{1}{z_2\sqrt{5}(1 - z/z_2)}$$

Представим дроби $1/(1 - z/z_1)$ и $1/(1 - z/z_2)$ в виде рядов

$$\frac{1}{1 - z/z_i} = 1 + \frac{z}{z_i} + \frac{z^2}{z_i^2} + \dots = \sum_{n=0}^{\infty} \frac{z^n}{z_i^n}$$

$$\begin{aligned} F(z) &= \frac{1}{z_2\sqrt{5}} \sum_{n=0}^{\infty} \frac{z^n}{z_2^n} - \frac{1}{z_1\sqrt{5}} \sum_{n=0}^{\infty} \frac{z^n}{z_1^n} = \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \left(\frac{1}{z_2^{n+1}} - \frac{1}{z_1^{n+1}} \right) z^n = \\ &= \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \left(\frac{z_1^{n+1} - z_2^{n+1}}{z_2^{n+1} z_1^{n+1}} \right) z^n = \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} (-1)^{n+1} (z_2^{n+1} - z_1^{n+1}) z^n, \end{aligned}$$

так как $z_1 z_2 = -1$ по теореме Виета. Отсюда получим выражение для n -о слагаемого ряда Фибоначчи:

$$f_n = \frac{1}{\sqrt{5}} (-1)^{n+1} (z_1^{n+1} - z_2^{n+1}), \quad (3.5)$$

где

$$z_i = \frac{-1 \pm \sqrt{5}}{2}.$$

Пример. Вычислим по формуле (3.5) слагаемое f_2 :

$$\begin{aligned} f_2 &= \frac{1}{\sqrt{5}}(-1)^3 \left(\left(\frac{-1 + \sqrt{5}}{2} \right)^3 - \left(\frac{-1 - \sqrt{5}}{2} \right)^3 \right) = \\ &= \frac{(-1)}{\sqrt{5}} \cdot \frac{(-16\sqrt{5})}{8} = 2 \end{aligned}$$

4 Вычисления n -члена рекуррентной последовательности

Формула (3.5) не удобна для вычисления значения n -о члена ряда Фибоначчи, поэтому мы рассмотрим здесь полиномиальный алгоритм вычисления f_n . Будем описывать общий алгоритм нахождения n -о члена произвольной рекуррентной последовательности.

Входными данными этого алгоритма являются коэффициенты a и b характеристического уравнения $x^2 - ax + b$, связанного с рекуррентной последовательностью

$$\{a_n\}_{n=0}^{\infty}$$

(для ряда Фибоначчи это уравнение имеет вид $x^2 - x - 1$, т.е. $a = 1$ и $b = -1$).

Свяжем с числами a и b определитель $\Delta = a^2 - 4b$, равный 5 для ряда Фибоначчи. Для работы алгоритма необходимо, чтобы этот определитель не являлся полным квадратом. Определим вспомогательную числовую последовательность $\{V_n\}_n$ следующим образом:

$$V_0 = 2, \quad V_1 = a, \quad V_{n+2} = aV_{n+1} - bV_n$$

Пример. Построим по этим формулам несколько начальных членов последовательности $\{V_n\}$ для ряда Фибоначчи:

$$V = \{2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, \dots\}$$

Вторая последовательность U_n задается аналогично:

$$U_0 = 0, \quad U_1 = a, \quad U_{n+2} = aU_{n+1} - bU_n$$

Теория рекуррентных последовательностей дает нам следующую формулу для первой последовательности

$$V_{j+k} = V_j V_k - b^k V_{k-j}, \quad (4.6)$$

которая выполняется при $0 \leq j \leq k$.

Подставляя в эту формулу специальные значения $j = k - 1$ и $j = k$ получим формулы:

$$\begin{cases} V_{2k} = V_k^2 - 2b^k \\ V_{2k+1} = V_k V_{k+1} - ab^k \end{cases} \quad (4.7)$$

Используя формулы (4.7), может вычислить значение произвольного члена последовательности $\{V_n\}$ за $O(\log_2 n)$ шагов.

Покажем, как вычислить, например, V_{97} . Для этого представим $n = 97$ в двоичном виде $97 = 1100001_2$. Начальная пара индексов равна $(0, 1)$. Ориентируясь на 2-е представление 97 применяем к начальной паре $(0, 1)$ дважды преобразование 2-типа, потом 4 раза - преобразование 1-типа и завершает одним преобразованием 2-типа:

$$(0, 1) \rightarrow (1, 2) \rightarrow (3, 4) \rightarrow (6, 7) \rightarrow (12, 13) \rightarrow (24, 25) \rightarrow (48, 49) \rightarrow (97, 98).$$

Вторая последовательность $\{U_k\}$ связана с первой последовательностью $\{V_k\}$ формулой

$$U_k = \frac{2V_{k+1} - aV_k}{a^2 - 4b} \quad (4.8)$$

Пример. Найти значение десятого члена ряда Фибоначчи.

Решение. Представим 10 в двоичном виде $10 = 1010_2$. Такому представлению соответствует последовательность операций:

$$(0, 1) \rightarrow (1, 2) \rightarrow (2, 3) \rightarrow (5, 6) \rightarrow (10, 11).$$

Соответствующие пары (V_k, V_{k+1}) образуют следующую последовательность

$$(2, 1) \rightarrow (3, 4) \rightarrow (11, 18) \rightarrow (123, 199).$$

Покажем только вычисление последнего шага. Дано $(V_5, V_6) = (11, 18)$. Подставляем эти значения в формулы (4.7) при $k = 5$:

$$\begin{aligned} V_{10} &= V_5^2 - 2b^5 = 121 - 2(-1)^5 = 123 \\ V_{11} &= V_5 \cdot V_6 - ab^5 = 198 + 1 = 199. \end{aligned}$$

Далее по формулам (4.8) вычислим f_{10} :

$$f_{10} = \frac{2V_{11} - aV_{10}}{a^2 - 4b} = \frac{2 \cdot 199 - 123}{5} = 55.$$

5 Тест Люка проверки простоты натуральных чисел

Тест простоты Люка использует последовательность Фиббоначчи. Он основан на следующей теореме.

Теорема 5.1 Пусть n - нечетное простое число. Определим число e равным символу Лежандра

$$e = \left(\frac{n}{5}\right) = \begin{cases} 0, & \text{если } n \bmod 5 = 0, \\ 1, & \text{если } n \bmod 5 \in \{1, 4\}, \\ -1, & \text{если } n \bmod 5 \in \{2, 3\}, \end{cases}$$

Тогда

$$f_{n-e} \equiv 0 \pmod{n}. \quad (5.9)$$

Таким образом, если число n – простое, то выполняется условие (5.9). Обратное не всегда верно, и составные числа, удовлетворяющие условию (5.9), называются псевдопростыми по Люку.

Тест Люка выполняется следующим образом. Рассматриваем нечетное простое число n . Вычисляем символ Лежандра $e = (n/5)$, находим число Фиббоначчи f_{n-e} и остаток $r = f_{n-e} \bmod n$. Если $r \neq 0$, то объявляем число n составным, иначе, n -вероятно простое.

Пример. Проверим на простоту число $n = 11$. Символ Лежандра $e = 1$, так как $n \bmod 5 = 1$ - квадрат.

Имеем, $n - e = 11 - 1 = 10$, $f_{10} = 55$, $f_{10} \bmod n = 55 \bmod 11 = 0$, значит, число 11 является вероятно простым по Люку.

Термин "вероятно простое" подчеркивает факт, что n может оказаться, на самом деле, составным. Составные числа, удовлетворяющие (5.9), называются псевдопростыми по Люку.

Упражнение 5.1 Написать программу для проверки натуральных чисел с помощью теста Люка. Найти первые 100 псевдопростых по Люку чисел.

Упражнение 5.2 Написать программу для проверки натуральных чисел с помощью теста Люка и с помощью одной итерации теста простоты Миллера-Рабина при $a = 2$. Найти наименьшее составное нечетное число n , проходящее успешно оба эти теста.

Упражнение 5.3 Используя программу предыдущего упражнения, найди количество составных чисел, проходящих проверку итерации теста Миллера-Рабина при $a = 2$ и теста Люка (псевдопростых по Миллеру-Рабину и Люку одновременно) до границы $X = 2 \cdot 10^6$.

6 Решение рекуррентных уравнений

Определение. Рекуррентным уравнением n -порядка называется уравнение вида:

$$A(n) = \sum_{k=0}^n c_k A(k), \quad \text{где } c_k \text{ — заданные константы,}$$

с начальными условиями $A(0) = a_0, A(1) = a_1, \dots, A(n-1) = a_{n-1}$.

Уравнение (3) для ряда Фибоначчи является классическим примером рекуррентного уравнения 2-о порядка. Рассмотрим на примере решение рекуррентного уравнения 1-о порядка.

Пример. Решить рекуррентное уравнение: $a_{n+1} = 2a_n + 1, a_0 = 1$.

Решение. Рассмотрим производящую функцию для последовательности $\{a_n\}$:

$$A(z) = \sum_{n=0}^{\infty} a_n z^n.$$

Домножим уравнение $a_{n+1} = 2a_n + 1$ на z^{n+1} и просуммируем по n от 0 до ∞ :

$$\sum_{n=0}^{\infty} a_{n+1} z^{n+1} = 2 \sum_{n=0}^{\infty} a_n z^{n+1} + \sum_{n=0}^{\infty} z^{n+1}, \quad \text{откуда}$$

$$A(z) - 1 = 2zA(z) + \frac{z}{1-z}, \quad \text{так как } \sum_{n=0}^{\infty} z^{n+1} = z \sum_{n=0}^{\infty} z^n = z \cdot \frac{1}{1-z}.$$

$$A(z)(1-2z) = 1 + \frac{z}{1-z}, \quad \text{или } A(z) = \frac{1}{(1-z)(1-2z)}$$

Разложим дробь $A(z)$ на сумму элементарных слагаемых:

$$\begin{aligned} A(z) &= \frac{1}{(1-z)(1-2z)} = \frac{C}{1-z} + \frac{D}{1-2z} = \frac{C(1-2z) + D(1-z)}{(1-z)(1-2z)} = \\ &= \frac{(-2C - D)z + C + D}{(1-z)(1-2z)} \end{aligned}$$

Приравнивая числители первой и последней дробей, получим систему линейных уравнений:

$$\begin{cases} 2C + D = 0 \\ C + D = 1 \end{cases}$$

откуда $C = -1$, $D = 2$. Тогда,

$$A(z) = \frac{(-1)}{1-z} + \frac{2}{1-2z} = \sum_{n=0}^{\infty} z^n (-1 + 2^{n+1}) z^n.$$

Ответ: $a_n = 2^{n+1} - 1$

Общее решение рекуррентного уравнения 2-о порядка

Рассмотрим рекуррентное уравнение 2-о порядка

$$x(n+2) = ax(n+1) + bx(n)$$

при начальных условиях $x(0) = x_0$, $x(1) = x_1$. Обозначим через $X(z)$ производящую функцию ряда $X(z) = \sum_{n=0}^{\infty} x(n)z^n$.

Домножая рекуррентное уравнение на z^{n+2} и суммируя по всем n получим:

$$\begin{aligned} X(z) - x_0 - x_1z &= za(X(z) - x_0) + bz^2X(z), \text{ откуда,} \\ X(z) &= \frac{x_0 + x_1z - ax_0z}{1 - za - z^2b} = \frac{(ax_0 - x_1)z - x_0}{bz^2 + az - 1} \end{aligned} \quad (5)$$

Рассмотрим дискриминант $D = a^2 + 4b$ квадратное уравнения $bz^2 + az - 1 = 0$. При $a^2 + 4b > 0$ это уравнение имеет два различных корня $z_1 = (-a - \sqrt{D})/2b$ и $z_2 = (-a + \sqrt{D})/2b$, и (5) можно разложить в сумму

$$X(z) = \frac{C}{z - z_1} + \frac{D}{z - z_2}.$$

Константы C и D можно искать, как и в уравнении ряда Фибоначчи, приводя эту сумму к общему знаменателю.

Если дискриминант $D = a^2 + 4b$ равен 0, то уравнение $bz^2 + az - 1 = 0$ имеет корень $z_0 = -a/2b$ кратности 2. В этом случае функция $X(z)$ раскладывается в сумму вида

$$X(z) = \frac{C}{z - z_0} + \frac{D}{(z - z_0)^2}.$$

В случае $D < 0$ уравнение $bz^2 + az - 1 = 0$ не имеет корней, но решение рекуррентного уравнения существует, но выражается через трансцендентные функции типа \arctgz .

Упражнение 6.1 *Найти формулу члена ряда, задаваемого рекуррентными формулами*

$$a_{n+2} = 2a_{n+1} - a_n, \quad a_0 = 2, a_1 = 1.$$

Параметры этого уравнения равны $a = 2$, $b = -1$, $x_0 = 1$, $x_1 = 1$. Составим сразу уравнение (5):

$$A(z) = \frac{-3z + 2}{z^2 - 2z + 1}$$

Дискриминант D уравнения $z^2 - 2z + 1 = 0$ равен 0, и уравнение имеет корень $z_0 = 1$ кратности 2. Значит, наша функция может быть разложена в сумму

$$A(z) = \frac{C}{1-z} + \frac{D}{(1-z)^2}.$$

Найдем коэффициенты C и D :

$$A(z) = \frac{C(1-z) + D}{z^2 - 2z + 1} = \frac{-Cz + C + D}{z^2 - 2z + 1} = \frac{-3z + 2}{z^2 - 2z + 1}.$$

Отсюда, $C = 3$, $D = -1$, и

$$A(z) = \frac{3}{1-z} - \frac{1}{(1-z)^2} = \sum_{n=0}^{\infty} 3z^n - (n+1)z^n = \sum_{n=0}^{\infty} (2-n)z^n, \quad \text{откуда } a_n = 2-n.$$

7 Нахождение производящей функции по ряду

Одной из часто встречающихся задач является задача вычисления производящей функции по последовательности $\{a_n\}$. В этом случае бывает полезным использование готовых функций из таблицы ПФ.

Упражнение 7.1 *Вычислить производящую функцию для последовательности $a_n = 2n^2 + 3n - 2$.*

Решение. Воспользуемся шаблонами производящих функций для полиномов:

$$\begin{aligned}\sum_{n=0}^{\infty} z^n &= \frac{1}{1-z}, \\ \sum_{n=0}^{\infty} (n+1)z^n &= \frac{1}{(1-z)^2}, \\ \sum_{n=0}^{\infty} (n+2)(n+1)z^n &= \frac{2}{(1-z)^3}.\end{aligned}$$

Представим искомое значение в виде линейной комбинации выписанных рядов:

$$a_n = 2n^2 + 3n - 2 = 2(n+2)(n+1) - 6n - 4 + 3n - 2 = 2(n+2)(n+1) - 3(n+1) - 3.$$

$$\begin{aligned}\sum_{n=0}^{\infty} a_n z^n &= 2 \sum_{n=0}^{\infty} (n+2)(n+1)z^n - 3 \sum_{n=0}^{\infty} (n+1)z^n - 3 \sum_{n=0}^{\infty} z^n = \\ &= \frac{4}{(1-z)^3} - \frac{3}{(1-z)^2} - \frac{3}{1-z}.\end{aligned}$$

Вычисление производящей функции для ряда частичных сумм

Пусть задана производящая функция

$$A(z) = \sum_{n=0}^{\infty} a_n z^n$$

Требуется найти производящую функцию

$$B(z) = \sum_{n=0}^{\infty} b_n z^n,$$

где

$$b_n = a_0 + a_1 + \dots + a_n,$$

т.е. b_n является частичной суммой первого ряда.

Теорема. Производящая функция $B(z)$ последовательности частичных сумм равна $A(z)/(1-z)$.

Доказательство. Рекуррентное уравнение для последовательности b_n имеет вид:

$$b_0 = a_0, \quad b_{n+1} = b_n + a_{n+1}.$$

Домножим это уравнение на z^{n+1} и просуммируем по всем n .

$$\sum_{n=0}^{\infty} b_{n+1}z^{n+1} = \sum_{n=0}^{\infty} b_n z^{n+1} + \sum_{n=0}^{\infty} a_{n+1}z^{n+1}.$$

Перепишем суммы в виде функций:

$$B(z) - b_0 = zB(z) + A(z) - a_0$$

Учитывая, что $a_0 = b_0$, получим $B(z) = A(z)/(1 - z)$ ч.т.д.

Упражнение 7.2 Найти выражение для суммы $b_n = 1 + 2 + \dots + n + 1$.

Решение. Рассмотрим ряд $a_n = n + 1$. Его производящая функция

$$A(z) = 1 + 2z + 3z^2 + \dots = \frac{1}{(1 - z)^2}.$$

Ряд $\{b_n\}$ является рядом частичных сумм для последовательности $\{a_n\}$:

$$b_n = \sum_{i=0}^n a_i$$

По теореме о ряде частичных сумм производящая функция ряда имеет

$$B(z) = \frac{A(z)}{1 - z} = \frac{1}{(1 - z)^3}$$

По таблице производящих функций

$$\frac{2}{(1 - z)^3} = \sum_n (n + 1)(n + 2),$$

откуда

$$b_n = 1 + 2 + \dots + (n + 1) = \frac{(n + 1)(n + 2)}{2}.$$

Переписывая формулу для $n - 1$, получим известную формулу суммы арифметической последовательности:

$$1 + 2 + \dots + n = \frac{n(n + 1)}{2}.$$

Упражнение 7.3 Найти выражение для суммы $b_n = 1 + 2^2 + \dots + (n + 1)^2$.

8 Анализ алгоритма сортировки

Рассмотрим пример использования производящих функций для анализа алгоритма быстрой сортировки массива. Этот алгоритм может быть описан следующим образом:

Вход: массив $A = \{a_1, a_2, \dots, a_n\}$.

1. Разбивает A на два подмассива длин $k < n$ и $n - k$.
2. Сортируем каждый массив по-отдельности.
3. Выполняем соединение (слияние merge) полученных частей в один отсортированный массив.

Обозначим через \bar{Q}_n число операций сравнения, выполненных при сортировке n -элементного массива. Тогда рекуррентная формула для \bar{Q}_n будет выглядеть так:

$$\bar{Q}_n = p_n + \sum_{k=0}^{n-1} \pi_{n,k} (\bar{Q}_k + \bar{Q}_{n-k}). \quad (8.10)$$

В этой формуле p_n обозначает количество сравнений при выполнении слияния двух массивов, а $\pi_{n,k}$ обозначает вероятность разбиения массива длины n на массивы длин k и $n - k$. Предполагая значение k , распределенным равномерно, получим $\pi_{n,k} = 1/n$.

Рекуррентное уравнение (8.10) может быть решено обычным способом:

$$\bar{Q}_n = 2(n+1)H_{n+1} - 4n - 2, \quad \text{где } H_n = \sum_{i=1}^n \frac{1}{i}$$

Аппроксимируя сумму $\sum_i 1/i$, получим

$$H_n = \sum_{i=1}^n \frac{1}{i} \sim \int_1^n \frac{dt}{t} = \ln n,$$

откуда

$$\bar{Q}_n \sim 2n \ln n,$$

что при примерно на 40% больше теоретического минимума $n \log_2 n$.

Выполним теперь оценку \bar{Q}_n , используя теорию производящих функций. Для получения производящей функции домножим каждое слагаемое в (8.10) на z^n и просуммируем по n от 1 до бесконечности:

$$Q(z) = \sum_{i=1}^{\infty} \bar{Q}_i z^i = p(z) + 2 \int_0^z \frac{Q(t)}{t-1} dt, \quad \text{где } p(z) = \sum_{i=1}^{\infty} p_i z^i.$$

Дифференцируя по z последнее уравнение, получим

$$Q'(z) = p'(z) + \frac{2Q(z)}{1-z}$$

Решая это уравнение, получим

$$Q(z) = \frac{1}{(1-z)^2} \int_0^z p'(t)(1-t)^2 dt$$

Используя

$$p(z) = \frac{z^2}{1-z^2},$$

получим,

$$Q(z) = \frac{2 \ln(1-z)^{-1}}{(1-z)^2} - \frac{2z}{(1-z)^2} \quad (8.11)$$

Используя таблицу 1 производящих функций, найдем коэффициент при z^n для первого слагаемого функции $Q(z)$:

$$[z^n] \frac{2 \ln(1-z)^{-1}}{(1-z)^2} \sim n \ln n$$

9 Решение комбинаторных задач

Задача о количестве путей в квадрате $n \times n$.

Рассмотрим следующую комбинаторную задачу: найти число путей из левого нижнего угла квадрата $n \times n$ в правый верхний угол таких, что передвигаться можно только вправо или вверх до узловых точек с целыми координатами (i, j) , причем путь не может спускаться ниже главной диагонали.

Решение. Обозначим число допустимых путей в квадрате $n \times n$ через C_n . Определим $C_1 = 1$. Найдем C_2 и C_3 простым перебором:

n	0	1	2	3
C_n	1	1	2	5

Числа C_n называются *числами Каталана*. Нам надо найти рекуррентную формулу для чисел Каталана. Удобнее эту задачу свести к другой задаче: триангуляции $n + 2$ -угольника (то есть разбиение $n + 2$ -угольника на треугольники непересекающимися диагоналями).

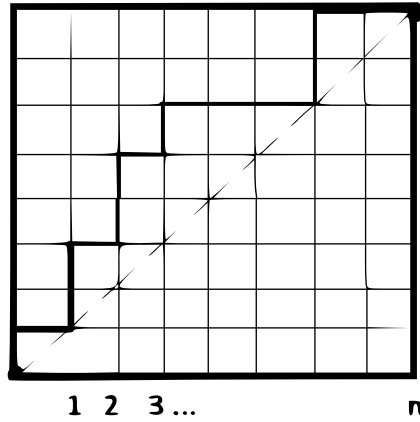


Рис. 1: Допустимый путь

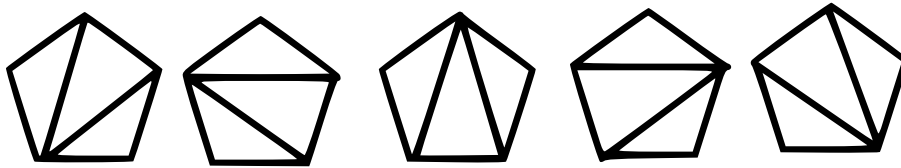
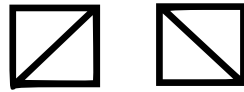


Рис. 2: Триангуляции квадрата и 5-угольника

Пусть задан $n + 2$ -угольник. Перенумеруем последовательно его вершины. Зафиксируем вершину 1. Соединим ее с вершиной i , $2 \leq i \leq n + 1$. Всего возможно из одной вершины провести n диагоналей. Выбранная диагональ делит $(n + 2)$ -угольник на $(i + 1)$ -угольник и $(n + 1 - i)$ -угольник, каждый из которых можно разбить на треугольники с непересекающимися диагоналями C_{i-1} и C_{n-i-1} способами. Значит, для каждого i , $2 \leq i \leq n + 1$, существует $C_{i-1} \cdot C_{n-i}$ разбиений. Всего же получим, что

$$C_n = \sum_{i=2}^{n+1} C_{i-1} \cdot C_{n-i} \text{ или}$$

$$C_n = \sum_{i=1}^n C_i \cdot C_{n-i-1}.$$

Обозначим через $C(z)$ производящую функцию ряда Каталана:

$$C(z) = 1 + 2z + 5z^2 + \dots = \sum_n C_n z^n$$

Возведем ряд $C(z)$ в квадрат и домножим на z . Получим:

$$zC^2(z) = C_0^2 z + (C_0 C_1 + C_1 C_0) z^2 + (C_0 C_2 + C_1 C_1 + C_2 C_0) z^3 + \dots =$$

$$= z + C_2 z^2 + C_3 z^3 + \dots = C(z) - 1, \text{ откуда}$$

$$zC^2(z) - C(z) + 1 = 0$$

$$C(z) = 1 + z \cdot C(z)^2 \rightarrow C(z) = \frac{1}{2z}(1 - \sqrt{1 - 4z}), \text{ и } C_n - \text{ числа Каталана.}$$

Раскроем $\sqrt{1 - 4z}$ по формуле бинома Ньютона

$$(1 + x)^\alpha = \sum_{i=0} C_\alpha^i x^i = 1 + C_{1/2}^1 x + C_{1/2}^2 x^2 +$$

где C_n^k - биномиальный коэффициент

$$C_n^k = \frac{n \cdot (n - 1) \cdot \dots \cdot (n + 1 - k)}{k!} = \frac{n!}{k!(n - k)!}$$

Получим следующее выражение для коэффициентов ряда Каталана

$$C_n = \frac{1}{n + 1} C_{2n}^n = \frac{2n!}{n! \cdot n!(n + 1)}$$

Пример.

$$C_3 = \frac{6!}{3! \cdot 3! \cdot 4} = \frac{6 \cdot 5 \cdot 4}{3! \cdot 4} = \frac{30}{6} = 5.$$

10 Формула включений и исключений

Формула включений-исключений (или принцип включений-исключений) - комбинаторная формула, позволяющая определить мощность объединения конечного числа конечных множеств, которые в общем случае могут пересекаться друг с другом.

В случае двух множеств A, B формула включений-исключений имеет вид:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

В случае n множеств эта формула получает более сложный вид:

$$|\bigcup_{i=1}^n A_i| = \sum_i |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.$$

Мы будем использовать эту формулу в другой формулировке - через свойства предметов. Пусть дано конечное множество U , состоящее из N элементов, каждый из которых может обладать несколькими свойствами из множества $A = \{a_1, \dots, a_k\}$ (или не обладать ни одним).

Обозначим через $N(a_{i_1}, a_{i_2}, \dots, a_{i_s})$ - количество элементов U , обладающих свойствами a_{i_1}, \dots, a_{i_s} .

Также через $N(\bar{a}_{i_1}, \bar{a}_{i_2}, \dots, \bar{a}_{i_s})$ - количество элементов U , не обладающих не одним из свойств a_{i_1}, \dots, a_{i_s} . Тогда,

$$N(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_k) = N - \sum_i N(a_i) + \sum_{i < j} N(a_i, a_j) - \dots + (-1)^k N(a_1, a_2, \dots, a_k). \quad (10.12)$$

Доказательство формулы Эйлера

Докажем формулу Эйлера

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

для $n = p_1^{r_1} \cdot \dots \cdot p_k^{r_k}$, используя формулу включений-исключений (10.12). Напомним, что функция Эйлера $\varphi(n)$ равна по определению числу натуральных чисел $k \leq n$, взаимно-простых с n . Обозначим через U множество чисел $\{k \mid k \leq n\}$, а через a_i свойство делиться на i -е простое число. Тогда

$$\begin{aligned} \varphi(n) &= n - \sum_i \frac{n}{p_i} + \sum_{i < j} \frac{n}{p_i p_j} - \dots + (-1)^k \frac{n}{p_1 \dots p_k} = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

Решение задач на формулу включений и исключений

Упражнение 10.1 *Сколько существует чисел, меньших или равных 1000, которые не делятся на 3, 5 и 7.*

Решение. Множество рассматриваемых чисел U содержит $N = 1000$ чисел. Обозначим через a_i свойство делиться на число p_i , $p_i \in P = \{3, 5, 7\}$. Количество чисел, не делящихся ни на одно $p \in P$, равно по определению

$$N(\bar{a}_1, \bar{a}_2, \bar{a}_3) = N - \sum_{i=1}^3 N(a_i) + \sum_{i < j} N(a_i, a_j) -$$

$$- \sum_{i < j < k} N(a_i, a_j, a_k) = 1000 - \sum_i \left[\frac{1000}{p_i} \right] + \sum_{i < j} \left[\frac{1000}{p_i p_j} \right] - \left[\frac{1000}{p_1 p_2 p_3} \right] =$$

где квадратные скобки означают целую часть от числа.

$$= 1000 - \left(\left[\frac{1000}{3} \right] + \left[\frac{1000}{5} \right] + \left[\frac{1000}{7} \right] \right) + \left(\left[\frac{1000}{3 \cdot 5} \right] + \left[\frac{1000}{3 \cdot 7} \right] + \left[\frac{1000}{5 \cdot 7} \right] \right) - \left[\frac{1000}{3 \cdot 5 \cdot 7} \right] = 1000 - (333 + 200 + 142) + (66 + 47 + 28) - 9 = 457$$

Используя формулу включений и исключений, решить следующие задачи.

Упражнение 10.2 *Найти количество простых чисел, меньших 100.*

Подсказка. Простые числа, меньшие 100, это нечетные числа, не делящиеся на простые числа $\leq \sqrt{100} = 10$, то есть на 3, 5 и 7.

Упражнение 10.3 *В группе 40 туристов. Из них 20 человек говорят по-английски, 15 — по-французски, 11 — по-испански. Английский и французский знают семь человек, английский и испанский — пятеро, французский и испанский — трое. Два туриста говорят на всех трёх языках. Сколько человек группы не знают ни одного из этих языков?*

Упражнение 10.4 *Сколько существует четырёхзначных чисел, в записи которых есть хотя бы одна чётная цифра?*

Упражнение 10.5 *На плоскости нарисованы перекрывающиеся квадрат и круг. Вместе они занимают площадь 2018 см². Площадь пересечения составляет 137 см². Площадь круга равна 1371 см². Чему равна площадь квадрата?*

Упражнение 10.6 *В кружок робототехники берут только тех, кто знает математику, физику или программирование. Известно, что 8 членов кружка знают физику, 7 — математику, 11 — программирование. При этом известно, что не менее двоих знают одновременно физику и математику, не менее троих — математику и программирование, и не менее четырёх — физику и программирование. Какое наибольшее количество участников кружка может быть при этих условиях?*

Упражнение 10.7 Из 100 туристов, выехавших на отдых в Турцию, 10 человек не знают ни английского, ни французского языков, 76 человек знают английский и 83 – французский. Сколько туристов знают оба эти языка?

Упражнение 10.8 Из 100 человек студентов, сдавших сессию, 48 человек сдали экономику, 42 студента – математику и 37 человек – логику. По экономике или математике сдали экзамен 76 человек, по экономике или логике также 76 человек, а по математике или логике – 66 человек. Сколько человек сдали хотя бы один экзамен, если все три предмета сдали 5 человек? Сколько человек не сдали ни одного экзамена? Сколько человек сдали только один экзамен по логике?

Литература

- [1] Apostol T. *Introduction to Analytic Number Theory*/ Springer, 1976, 338 p.
- [2] Ландо С.А. Лекции о производящих функциях, изд.3, М.: МЦНМО, 2007, 144 с.