1 Введение

1.1 О предмете и содержании курса

Слово "дискретный" является противоположным по значению слову "непрерывный", а непрерывными могут быть только бесконечные образования. Дискретная математика имеет дело с конечными объектами: конечными множествами и их преобразованиями (функциями, определенными на конечных множествах и принимающими конечные множества значений). Элементы конечных множеств можно обозначать целыми числами, поэтому можно сказать, что дискретная математика оперирует целыми числами, результаты всех вычислений — целые числа. Исторически неотрицательные целые числа появились раньше всех остальных, они выражают количество элементов множества. Так пришли к понятию натурального числа древние люди, так учат маленьких детей, показывая и сравнивая множества сначала одинаковых предметов (палочек, кубиков, шариков), а затем и разнородных. Позже понятие числа расширяется в связи с практическими действиями — счетом, арифметическими операциями и обратными к ним. Число 0 не изменяет исходное при сложении, отрицательные числа появляются при выполнении вычитания, действия, обратного сложению. Рациональные числа — результат деления, действия, обратного умножению. Иррациональные и комплексные числа — результат извлечения корней, действий, обратных возведению в степень.

Даже школьники могут убедиться, что задачи с целочисленным по смыслу результатом довольно сильно отличаются от аналогичных задач без такого ограничения: уравнения, неравенства и их системы могут не иметь решения и, напротив, решение всего лишь одного уравнения с несколькими неизвестными может быть единственным.

В дискретной математике, в силу конечности рассматриваемых множеств, невозможен предельный переход и, следовательно, неприменимы основанные на понятии предела методы дифференциального и интегрального исчисления. Необходимы иные подходы, обусловленные спецификой дискретных задач, и систематизация их в особом разделе математики. В XX веке дискретная математика получила дополнительный стимул к развитию в связи с появлением и широким применением цифровой техники. Любое такое устройство конечно, и в нем цифрами можно представить лишь конечное множество чисел, как бы велико оно ни было. Этим схожи и простейший древний вычислительный инструмент абак (счеты), и современный суперкомпьютер.

Однако не следует противопоставлять дискретную и непрерывную математику. Они, как будет видно, находятся в тесной взаимосвязи, методы одной применяются как инструмент в другой, их трудно разделить. Овладение и дискретными, и непрерывным методами необходимо для выработки математической культуры

и успешного применения математики в любой сфере деятельности.

Излагаемый здесь курс состоит из трех частей. Первая часть — это методы комбинаторных вычислений, подсчета различных конечных объектов. Вторая часть — модели и методы теории графов, современного раздела математики, позволяющего анализировать всевозможные отношения между парой элементов конечного множества. Теория графов обладает большой степенью универсальности, красотой и наглядностью, позволяющей считать ее аналогом геометрии при конечном множестве точек. Третья, заключительная часть — целочисленная арифметика, она обладает, как уже говорилось, удивительными (на первый взгляд) особенностями, позволяющими в ряде случаев значительно сократить объем вычислений и избежать ошибок. Результаты первой части существенно используются в последующих.

1.2 Рекомендуемая литература

1. Набебин А. А. Дискретная математика — М.: Научный мир, 2010.

2. Иванов Б. Н. Дискретная математика. Алгоритмы и программы — М.: Лаб. баз. знаний, 2002.

3. Набебин А. А. Сборник заданий по дискретной математике — М.: Научный мир, 2009.

Ни одна из книг не является обязательной. Для овладения курсом и успешного выполнения заданий достаточно публикуемого здесь материала. Но полезно знать, что такие книги есть, как и множество других, в заглавии которых присутствуют слова "дискретная математика".

1.3 Применяемые обозначения

$\mathbb{N} = \{1,\ 2,\ \ldots\}$ — множество натуральных чисел.

$\mathbb{Z} = \{0,\ \pm 1,\ \pm 2,\ \ldots\}$ — множество целых чисел.

$\mathbb{Z}_+ = \{0,\ 1,\ 2,\ \ldots\}$ — множество неотрицательных целых чисел.

$\mathbb{R} = (-\infty; +\infty)$ — множество вещественных чисел.

$\mathbb{C} = \{z = x + iy,\ x, y \in \mathbb{R}\}$ — множество комплексных чисел, где i — мнимая единица, $i^2 = -1$.

$\lfloor x \rfloor$ — целая часть вещественного x, наибольшее целое, не превосходящее x.

$\lceil x \rceil$ для вещественного числа x — наименьшее целое M такое, что $M \geq x$.

$\square$ означает конец доказательства, "требуемое получено", "теорема доказана".

2 Вычисление конечных сумм

В задачах дискретной математики приходится довольно часто выполнять некоторые стандартные вычисления. Рассмотрим методы вычисления сумм, зависящих от нескольких параметров, одним из параметров всегда является число слагаемых. Этими несложными техническими приемами необходимо овладеть для успешного решения более сложных и содержательных задач. Отметим, что принципиальным отличием этих вычислений от суммирования рядов методами высшей математики (точнее, математического анализа) является конечность числа слагаемых и невозможность предельного перехода. В математическом анализе такие ситуации часто приводят к приближенному результату (погрешность которого можно, тем не менее, оценить). Мы же будем искать точные значения сумм натуральных чисел. Напомним, что результатом всегда должно быть целое число.

Рассмотрим довольно общее семейство сумм

$$S_n(k) = \sum_{j=1}^{n} j^k = 1^k + 2^k + \cdots + n^k, \tag{1}$$

зависящих от двух целочисленных параметров $n \geq 1$ и $k \geq 0$.

1.1 При $k = 0$ без труда находим

$$S_n(0) = \sum_{j=1}^{n} j^0 = \sum_{j=1}^{n} 1 = n,$$

$$S_n(0) = n. \tag{1.1}$$

1.2. При $k = 1$ запишем сумму $S_n(1)$ в прямом и обратном порядке:

$$S_n(1) = 1 + 2 + 3 + \cdots + (n-2) + (n-1) + n,$$

$$S_n(1) = n + (n-1) + (n-2) + \cdots + 3 + 2 + 1.$$

Сложив эти равенства, получим

$$2S_n(1) = (1+n) + (2+n-1) + (3+n-2) + \cdots + (n-2+3) + (n-1+2) + (n+1).$$

В правой части теперь сумма n одинаковых слагаемых $(n+1)$, откуда

$$S_n(1) = \frac{n(n+1)}{2}. \tag{1.2}$$

Великий немецкий математик Карл Фридрих Гаусс (1777–1855) придумал такой способ вычисления этой суммы в 7-летнем возрасте.

Рассмотрим иной способ. Он использует сумму $S_{n+1}(2)$. С одной стороны,

$$S_{n+1}(2) = S_n(2) + (n+1)^2 = S_n(2) + n^2 + 2n + 1.$$

С другой стороны,

$$S_{n+1}(2) = \sum_{j=0}^{n}(j+1)^2 = \sum_{j=0}^{n}(j^2 + 2j + 1) = S_n(2) + 2S_n(1) + (n+1).$$

Таким образом,

$$S_n(2) + n^2 + 2n + 1 = S_n(2) + 2S_n(1) + n + 1,$$

откуда после элементарных преобразований $2S_n(1) = n^2 + n$. Получаем тот же результат (1.2). При любом натуральном n произведение $n(n+1)$ четно, поэтому $S_n(1)$ целое.

Второй способ можно модифицировать для вычисления, как мы покажем, и более сложных сумм.

1.3 (**сумма первых n членов арифметической прогрессии** $a_1, a_2 = a_1 + d$, $a_3 = a_1 + 2d, \ldots$ **с разностью** d)

$$A_n(d) = \sum_{j=1}^{n} a_j = \sum_{j=1}^{n}(a_1 + (j-1)d).$$

Преобразуя сумму и используя (1.2), получаем

$$A_n(d) = na_1 + d(1 + 2 + \cdots + n - 1) = na_1 + d(n-1)n/2.$$

Элементарными преобразованиями приходим к известным со школы формулам

$$A_n(d) = \frac{n(2a_1 + (n-1)d)}{2} = \frac{n(a_1 + a_n)}{2}. \tag{1.3}$$

1.4. Вычислим $S_n(2)$ способом, аналогичным второму методу вычисления суммы $S_n(1)$. Имеем

$$S_{n+1}(3) = S_n(3) + (n+1)^3 = S_n(3) + n^3 + 3n^2 + 3n + 1.$$

С другой стороны,

$$S_{n+1}(3) = \sum_{j=0}^{n}(j+1)^3 = \sum_{j=0}^{n}(j^3 + 3j^2 + 3j + 1) = S_n(3) + 3S_n(2) + 3S_n(1) + (n+1).$$

Таким образом,

$$S_n(3) + n^3 + 3n^2 + 3n + 1 = S_n(3) + 3S_n(2) + 3S_n(1) + n + 1.$$

С учетом (1.2) получаем

$$n^3 + 3n^2 + 3n = 3S_n(2) + 3n(n+1)/2 + n,$$

.

$$S_n(2) = \frac{n(n+1)(2n+1)}{6}. \tag{1.4}$$

Убедимся, что выражение из правой части (1.4) целое. Из двух последовательных чисел ровно одно четно, поэтому числитель дроби делится на 2. Проверить, что он делится и на 3 (следовательно, на $6 = 2 \cdot 3$) можно, рассмотрев возможные остатки от деления на 3 числа n (случаи $n = 3m,\ 3m+1,\ 3m+2$, где $m \in Z$). Сделайте это самостоятельно.

1.5. Аналогично вычислим $S_n(3)$. Из выражений

$$S_{n+1}(4) = S_n(4) + (n+1)^4 = S_n(4) + n^4 + 4n^3 + 6n^2 + 4n + 1,$$

$$S_{n+1}(4) = \sum_{j=0}^{n}(j+1)^4 = \sum_{j=0}^{n}(j^4 + 4j^3 + 6j^2 + 4j + 1) =$$

$$= S_n(4) + 4S_n(3) + 6S_n(2) + 4S_n(1) + (n+1)$$

следует равенство

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

Подставляя в него (1.1), (1.2), (1.4), получим

$$n^4 + 4n^3 + 6n^2 + 4n = 4S_n(3) + n(n+1)(2n+1) + 2n(n+1) + n,$$

откуда $4S_n(3) = n^4 + 2n^3 + n^2$ и, наконец,

$$S_n(3) = \frac{n^2(n+1)^2}{4}. \tag{1.5}$$

1.6. Таким же путем последовательно вычисляются суммы $S_n(4),\ S_n(5), \ldots$. В частности,

$$S_n(4) = \sum_{j=1}^{n} j^4 = \frac{n(6n^4 + 15n^3 + 10n^2 - 1)}{30}.$$

Выведите эту формулу самостоятельно.

1.7. Зная $S_n(0),\ S_n(1),\ S_n(2), \ldots, S_n(m)$ и используя свойство линейности сумм, можно вычислить **сумму многочленов степени m, зависящих от j**:

$$\sum_{j=1}^{n}(a_m j^m + a_{m-1} j^{m-1} + \cdots + a_1 j + a_0) =$$

$$= a_m S_n(m) + a_{m-1} S_n(m-1) + \cdots a_1 S_n(1) + a_0 S_n(0).$$

2. **Сумма первых членов геометрической прогрессии со знаменателем q**

$$G_n(q) = 1 + q + q^2 + \cdots + q^n$$

вычисляется по следующим формулам:

$$G_n(1) = n + 1,$$

$$G_n(-1) = 0 \text{ при четных } n, \qquad G_n(-1) = 1 \text{ при нечетных } n,$$

$$G_n(q) = \frac{q^{n+1} - 1}{q - 1} \text{ при } |q| \neq 1.$$

Пример. Вот содержательная задача, в которой используется сумма $G_n(q)$. Каково количество десятичных целых чисел от 0 до 10^n, не содержащих находящихся рядом одинаковых цифр?

Обозначим искомую величину как x_n. Легко найти $x_1 = 10,\ x_2 = 100 - 9 = 91$. Пусть найдено число x_n. Тогда $x_{n+1} = x_n + \Delta_{n+1}$, где Δ_{n+1} — количество чисел, содержащих ровно $n+1$ цифр $d_1, d_2, \ldots, d_{n+1}$, при этом $d_1 \neq 0$, т. е. d_1 может принимать любое из 9 значений $1, \ldots, 9$. Тогда и для каждого $j = 2, \ldots, n+1$ цифра d_j может принимать любое из 9 значений, принадлежащих множеству $\{0, 1, \ldots, 9\} \setminus \{d_{j-1}\}$. Все $n+1$ цифр могут принимать, таким образом, 9^{n+1} значений (это частный случай общего *правила произведения*, часто используемого в различных задачах дискретной математики). Следовательно, $\Delta_{n+1} = 9^{n+1}$, $x_{n+1} = x_n + 9^{n+1}$,

$$x_n = 10 + 9^2 + 9^3 + \cdots + 9^n = G_n(9) = \frac{9^{n+1} - 1}{8}.$$

Задание для самостоятельного решения

Вариант задания — Ваш номер в списке группы.

Решения присылайте мне, Мещанинову Дмитрию Германовичу, по адресу MeshchaninovDG@mpei.ru

Необходимо выполнить по одному варианту каждого из трех заданий — вычислить указанные суммы целых чисел.

Задание 1

1.1. $\displaystyle\sum_{j=1}^{n} j^2(j-3).$

1.2. $\sum_{j=1}^{n} j^2(2j+1).$

1.3. $\sum_{j=1}^{n} (j^3 - 3j).$

1.4. $\sum_{j=1}^{n} (2j^3 + j - 1).$

1.5. $\sum_{j=1}^{n} (3j^3 - 4).$

1.6. $\sum_{j=1}^{n} (j^3 + 4j).$

1.7. $\sum_{j=1}^{n} (j^3 + 3j^2).$

1.8. $\sum_{j=1}^{n} (j^3 - 3j - 1).$

1.9. $\sum_{j=1}^{n} j^2(j+2).$

1.10. $\sum_{j=1}^{n} j(j^2 + 2j + 1).$

1.11. $\sum_{j=1}^{n} (j^3 + 3j - 1).$

1.12. $\sum_{j=1}^{n} (j^3 + 2j + 1).$

1.13. $\sum_{j=1}^{n} ((j+1)^3 - j).$

1.14. $\sum_{j=1}^{n} (2j^3 - (j-1)^2).$

1.15. $\sum_{j=1}^{n} (3j^2 + j^2(j-1)).$

Задание 2

2.1. $\sum_{j=0}^{n}(-1)^j 2j.$

2.2. $\sum_{j=0}^{n}(-1)^j (2-j).$

2.3. $\sum_{j=0}^{n}(-1)^j (2j-1).$

2.4. $\sum_{j=0}^{n}(-1)^{j+1} 2j.$

2.5. $\sum_{j=0}^{n}(-1)^{j-1} (2j+1).$

2.6. $\sum_{j=0}^{n}(-1)^j (4j+2).$

2.7. $\sum_{j=0}^{n}(-1)^{j-1} (j+1).$

2.8. $\sum_{j=0}^{n}(-1)^{j^3} (3-j).$

2.9. $\sum_{j=0}^{n}(-1)^j (2j-3).$

2.10. $\sum_{j=0}^{n}(-1)^j (1-j).$

2.11. $\sum_{j=0}^{n}(-1)^{(11j)} (j-1).$

2.12. $\sum_{j=0}^{n}(-1)^{(21j)} 2j.$

2.13. $\sum_{j=0}^{n}(-1)^{(3j)} (j-3).$

2.14. $\sum_{j=0}^{n}(-1)^{j+4} (j-4).$

2.15. $\sum_{j=0}^{n}(-1)^{j^2} 2j.$

Задание 3

Найдите число, являющееся значением суммы.

3.1. $\sum_{j=0}^{11}(1+(-2)^j)$.

3.2. $\sum_{j=0}^{9}((-1)^j+(-2)^j)$.

3.3. $\sum_{j=0}^{5}(-15+(-3)^j)$.

3.4. $\sum_{j=0}^{6}((-1)^{j^3}+(-4)^j)$.

3.5. $\sum_{j=0}^{5}(3^j+(-2)^j)$.

3.6. $\sum_{j=0}^{6}(4^j+(-2)^j)$.

3.7. $\sum_{j=0}^{6}((-2)^{2j}-(-2)^j)$.

3.8. $\sum_{j=0}^{6}((-1)^j+(-2)^j)$.

3.9. $\sum_{j=0}^{5}(2^{2j}+(-1)^j)$.

3.10. $\sum_{j=0}^{10}(2^j+(-2)^j)$.

3.11. $\sum_{j=0}^{7}(2(-1)^j+(-2)^{2j})$.

3.12. $\sum_{j=0}^{4}((-3)^{2j}+(-2)^{3j})$.

3.13. $\sum_{j=0}^{6}((-1)^{3j}+(-3)^j)$.

3.14. $\sum_{j=0}^{11}((-1)^{2j}+(-2)^j)$.

3.15. $\sum_{j=0}^{11}((-1)^{j^2}+(-2)^j)$.

3 Основные комбинаторные конфигурации и числа

Комбинаторика, комбинаторный анализ — это раздел математики, в котором рассматриваются подмножества конечных множеств. Подмножества определенного вида называются *комбинаторными конфигурациями*. Подсчет количества комбинаторных конфигураций (*комбинаторных чисел*) составляет суть перечислительных задач комбинаторного анализа. Такие задачи приходится решать как части более сложных задач дискретной математики.

3.1 Простейшие правила комбинаторных вычислений

При подсчете комбинаторных конфигураций применяются два очень простых правила.

Правило произведения. *Если объект O_1 можно выбрать N_1 различными способами, а объект O_2 выбирается ровно N_2 способами, то пару объектов $\{O_1, O_2\}$ можно выбрать ровно $N_1 \cdot N_2$ различными способами.* [1]

Правило суммы. *Если объект O_1 можно выбрать N_1 различными способами, а объект O_2 выбирается ровно N_2 способами, и при этом выбор O_1 и O_2 одновременно невозможен* [2]*, то выбор "O_1 или O_2" можно осуществить ровно $N_1 + N_2$ различными способами.*

Эти правила позволяют легко вычислить количество некоторых часто применяемых комбинаторных конфигураций.

Пример. Из города A ровно m_1 дорог ведут в город B и n_1 дорог — в город C. Ровно m_2 дорог ведут из B в город D, ровно n_2 дорог — из C в D. Из A в D можно проехать только через город B или город C. Сколькими способами можно попасть из A в D?

Применяя правило произведения, находим число $m_1 m_2$ путей из A в D через B и число $n_1 n_2$ путей из A в D через C. Далее по правилу суммы получаем ответ $m_1 m_2 + n_1 n_2$.

Теорема 1. *Конечное множество $U = \{e_1, \ldots, e_n\}$ из n элементов имеет ровно 2^n подмножеств (включая пустое и само множество U).*

Доказательство. Пусть B — подмножество множества U. Каждое такое подмножество однозначно определяется принадлежностью или непринадлежностью ему каждого из элементов $e_1, \ldots, e_n$. Итак, для каждого $j = 1, \ldots, n$ надо выбрать одно из двух условий: $e_j \in B$ или $e_j \notin B$. Есть ровно $n_j = 2$ способа выбора такого условия для каждого $j = 1, \ldots, n$. Применяя правило произведения, получаем

[1] отсюда и название правила, имеется также аналогия с произведением событий

[2] это условие очень важно, его игнорирование приводит к смысловым ошибкам

число $2 \times \cdots \times 2 = 2^n$ способов выбора условий для всех $j = 1, \ldots, n$, т. е. число различных подмножеств множества U. $\square$

Пример 1. Множество из 3 элементов $\{E_1, E_2, E_3\}$ имеет ровно $2^3 = 8$ подмножеств:

$$\emptyset,\ \{E_1\},\ \{E_2\},\ \{E_3\},\ \{E_1, E_2\},\ \{E_1, E_3\},\ \{E_2, E_3\},\ \{E_1, E_2, E_3\}.$$

Подмножества взаимно однозначно соответствуют бинарным векторам (x_1, x_2, x_3), где $x_j = 1$, если E_j принадлежит подмножеству, и $x_j = 0$ в противном случае.

Следствие 1. *Количество бинарных векторов* $(x_1, \ldots, x_n)$ *длины* n *равно* 2^n.

Такие векторы часто применяют при подсчете комбинаторных конфигураций.

Бинарные векторы — универсальный способ кодирования, т. е. записи любой информации в языке с алфавитом $\{0, 1\}$. Рассмотрим аналогичный способ записи в языке с любым конечным алфавитом. Дадим точные определения и выведем довольно простые, но важные результаты, широко применяемые в дискретной математике.

3.2 Слова в конечном алфавите

Конечное множество, скажем, из k элементов, $A = \{a_1, \ldots, a_k\}$ называется *алфавитом*, его элементы a_j — *символами*, или буквами. *Словом длины* n *в алфавите* A называется конечная последовательность символов алфавита A:

$$a_{j(1)} a_{j(2)} \ldots a_{j(n)}, \qquad a_{j(1)}, a_{j(2)}, \ldots, a_{j(n)} \in A.$$

Множество всех слов длины n в алфавите A обозначается как A^n.

Число элементов произвольного конечного множества M обозначается как $|M|$ и называется *мощностью конечного множества* M. Очевидно, $|\emptyset| = 0$. Натуральные числа и 0 — это все мощности конечных множеств. Именно таким образом у древних людей сформировалось абстрактное понятие натурального числа, именно так учат числам маленьких детей.

По правилу произведения легко выводится обобщение следствия 1.

Следствие 2. *Количество слов длины* n *в алфавите из* k *букв равно* k^n. Это же можно записать так: если $|A| = k$, то $|A^n| = k^n$ (частный случай правила произведения).

При записи слов фиксированного алфавита удобно располагать слова в некотором порядке, позволяющем легко их просматривать и проверять, все ли нужные слова присутствуют, нет ли повторений. Общепринятым является *лексикографический порядок*. Этим способом перечисляются слова в словарях, справочниках, энциклопедиях, списках имен и названий и т. п. Слова сначала упорядочиваются по первой букве, затем слова с одинаковой первой буквой упорядочиваются по

второй и так далее. Если есть слова разной длины, то порядок слов с одинаковыми первыми буквами таков, что сначала выписываются короткие слова, у которых нет следующей буквы, затем уже остальные слова (с теми же первыми буквами) упорядочиваются по следующей букве.

Пример 3. Выпишем в лексикографическом порядке все $3^2 = 9$ слов длины 2 в алфавите $\{a, b, c\}$ мощности 3:

$$aa,\ ab,\ ac,\ ba,\ bb,\ bc,\ ca,\ cb,\ cc.$$

Пример 4. Выпишем в лексикографическом порядке слова разной длины в алфавите $\{a, b, c\}$ из множества $\{bcaa, b, cca, cbac, acb, bcab, abcc, bcca, bbc, cc\}$:

$$abcc,\ acb,\ b,\ bbc,\ bcaa,\ bcab,\ bcca,\ cbac,\ cc,\ cca.$$

Процесс упорядочивания различных списков называется их *сортировкой*. Сортировка часто применяется в различных задачах обработки информации. Сложность сортировки оценивается методами дискретной математики.

Симметричные относительно своей середины слова называются *палиндромами*. Примеры палиндромов в русском языке — имя Алла, слово "казак". Найдем число палиндромов длины n в алфавите мощности k. В палиндроме четной длины n произвольно можно задать только первые $n/2$ букв, остальные — те же первые $n/2$ букв, записанные в обратном порядке. Число палиндромов четной длины n равно $k^{n/2}$. В палиндроме нечетной длины $n = 2m+1$ произвольно можно задать первые m букв и еще одну — центральную. Число таких палиндромов равно k^{m+1}. В математике принято обозначение $\lceil x \rceil$ для наименьшего целого числа N такого, что $N \geq x$, где x — произвольное вещественное число. Так, $\lceil 0.7 \rceil = 1$, $\lceil \pi \rceil = 4$, $\lceil (-5) \rceil = -5$. Результаты наших наблюдений над палиндромами можно записать как

Следствие 3. *Число палиндромов длины n в алфавите мощности k равно* $k^{\lceil n/2 \rceil}$.

Пример 5. Выпишем в лексикографическом порядке все палиндромы длины не более 3 в алфавите $\{a, b, c\}$.

Имеем $k = 3$. Число палиндромов длины 1 равно $3^{\lceil 1/2 \rceil} = 3^1 = 3$, длины 2 — $3^{\lceil 2/2 \rceil} = 3^1 = 3$, длину 3 имеют $3^{\lceil 3/2 \rceil} = 3^2 = 9$ палиндромов. Осталось выписать все $3 + 3 + 9 = 15$ палиндромов в лексикографическом порядке:

$$a,\ aa,\ aaa,\ aba,\ aca,\ b,\ bab,\ bb,\ bbb,\ bcb,\ c,\ cac,\ cbc,\ cc,\ ccc.$$

Некоторые мастера слова проявляют немало искусства в составлении осмысленных палиндромов, например, "Анна, Вас и тина манит, и саванна". Эта фраза содержит 24 буквы русского алфавита. Общее число палиндромов такой длины

есть 33^{12}, но из них надо еще выбрать синтаксически правильно записываемые, а из последних — осмысленные. Требуется виртуозное владение языком!

Пример 6. Автомобильные номера содержат 3 десятичные цифры и 4 буквы из 12, общих для кириллического и латинского алфавитов. Найдем число всех возможных номеров. Три цифры можно выбрать, по правилу прооизведения, 10^3 способами. Аналогично 4 буквы можно выбрать $12^4 = 20\ 736$ способами. Выбирая и цифры и буквы, получаем, по правилу произведения, 20 736 000 номеров. Некоторые люди считают престижными "зеркальные" номера, в которых слово, составленное из цифр, есть палиндром. Число таких номеров оказывается, в соответствии с уже изложенными результатами, $12^2 10^3 = 144\ 000$.

3.3 Размещения, перестановки, сочетания

Пусть фиксировано n-элементное множество $U = \{E_1, \ldots, E_n\}$. Его неупорядоченные k-элементные подмножества

$$\{E_{j(1)}, \ldots, E_{j(k)}\},\ 1 \le j(1) < \cdots < j(k) \le n,\ \ 0 \le k \le n,$$

называются *сочетаниями из n элементов по k* (употребляются фигурные скобки). Число сочетаний из n элементов по k обозначается как C_n^k.

Упорядоченные k-элементные подмножества

$$(E_{j(1)}, \ldots, E_{j(k)}),\ 1 \le j(1) < \cdots < j(k) \le n,\ \ 0 \le k \le n,$$

называются *размещениями из n элементов по k* (употребляются круглые скобки, как при указании элементов векторов и матриц). Число размещений из n элементов по k обозначается как A_n^k. Размещение из k элементов k по называется *перестановкой* этих k *элементов.*

Теорема 2. *Если $0 \le k \le n$, то*

$$A_n^k = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$ [3]

В частности,

$$A_k^k = k!.$$

Доказательство. Пусть A — размещение, состоящее из k элементов множества $U = \{E_1, \ldots, E_n\}$. Оно однозначно определяется выбором своих элементов $E_{j(1)}, \ldots, E_{j(k)}$. Элемент $E_{j(1)}$ можно выбрать n способами (любой из n элементов множества Ω), $E_{j(2)}$ — $(n-1)$ способом (любой из элементов множества U кроме

[3] Если k — положительное целое, то $k! = 1 \times 2 \times \cdots \times k$ и по определению 0!=1

$E_{j(1)}$), $E_{j(3)}$ — $(n-2)$ способами и так далее. Последний элемент $E_{j(k)}$ размещения можно выбрать $(n-(k-1))$ способами (любой в U кроме $E_{j(1)},\ldots,E_{j(k-1)}$. Применяя правило произведения, получаем $A_n^k = n(n-1)(n-2)\cdots(n-k+1)$. □

Пример 7. Выпишем в лексикографическом порядке все $k!$ перестановок k элементов для $k = 2, 3, 4$. Имеем $2! = 2,\ 3! = 6,\ 4! = 24$. Это число перестановок. Укажем сами перестановки в нужном порядке.

$$k = 2: \qquad 12,\ 21.$$

$$k = 3: \qquad 123,\ 132,\ 213,\ 231,\ 312,\ 321.$$

$$k = 4: \qquad 1234,\ 1243,\ 1324,\ 1342,\ 1423,\ 1432,$$
$$2134,\ 2143,\ 2314,\ 2341,\ 2413,\ 2431,$$
$$3124,\ 3142,\ 3214,\ 3241,\ 3412,\ 3421,$$
$$4123,\ 4132,\ 4213,\ 4231,\ 4312,\ 4321.$$

Пример 8. На праздник пришли супружеская пара с двумя детьми, семья с одним ребенком, две пары без детей и свободный мужчина. Они хотя встать шеренгой для совместного фото. Сколькими способами можно это сделать, если все члены каждой семьи хотят быть рядом друг с другом?

Будем считать каждую семью (и одного мужчину) как единый объект. Имеем 5 объектов, которые можно переставить 5! способами. Но надо еще упорядочить всех представителей каждой семьи-объекта. Применяя правило произведения, находим $5!4!3!(2!)^2 1! = 69\ 120$ способов.

Анаграммой слова w называется слово, полученное перестановкой всех букв слова w. Слово "слон" имеет 4! анаграмм, а слово "жаба" — не 4!, а только 12 (в лексикографическом порядке: аабж, аажб, абаж, абжа, ажаб, ажба, бааж, бажа, бжаа, жааб, жаба, жбаа), поскольку буква "а" повторяетя дважды, перестановки этих букв не меняют слово. Аналогично слово "какаду" имеет не 6!, а $6!/(2!)^2$ анаграмм, в этом слове по два раза повторяются буквы "а" и "к". Нетрудно вывести общую формулу: *если слово имеет длину n и содержит k, $k \le n$, различных букв, повторяющихся $k_1,\ldots,k_n$ раз (при этом $k_1+\cdots+k_n = n$), то число анаграмм такого слова есть*

$$\frac{n!}{k_1!\cdots k_n!}.$$

Анаграммы часто используются как псевдонимы (вымышленные имена). Например, Франсуа Рабле подписывал свой остросатирический роман "Гаргантюа и Пантагрюэль"(1533–1551) псевдонимом Алькофрибас Назье (Alcofribas Nasier — полная анаграмма, включая пробел, подлинного имени Francois Rabelais). Другой

пример: весьма успешного художника XX века Сальвадора Дали (Salvador Dali) друзья называли Avida Dollars ("Гребущий Деньги").

Теорема 3. *Если* $0 \le k \le n$, *то*

$$C_n^k = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}. \qquad (1)$$

Доказательство. Заметим, что $C_n^k = A_n^k / A_k^k$ и применим теорему 2. □

Функция $k!$ очень быстро растет ($(k+1)! = k!(k+1),\ 1! = 1,\ 2! = 2,\ 3! = 6,\ 4! = 24,\ 5! = 120,\ 6! = 720$), вычисление C_n^k по формуле (1) ограничено техническими возможностими аппаратуры. Для более эффективного вычисления применяются следующие свойства.

Замечание. Чтобы не записывать ограничения для значения верхних индексов k и придавать им любое неотрицательное целое значение, принято соглашение

$$A_n^k = C_n^k = 0 \text{ при } k > n.$$

Теорема 4 (свойства чисел C_n^k).

1. $C_n^0 = C_n^n = 1$.
2. $C_n^1 = C_n^{n-1} = n$.
3. $C_n^2 = C_n^{n-2} = n(n-1)/2$.
4. $C_n^k = C_n^{n-k}$.
5. $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$.
6. *Числа* C_n^k *образуют бесконечную матрицу, называемую треугольником Паскаля. Ее строки соответствуют значениям* $n = 0, 1, 2\ldots$, *столбцы — значениям* $k = 0, 1, \ldots, n$. *Вот первые строки треугольника Паскаля*:

$$\begin{array}{ccccccc}
1 & & & & & & \\
1 & 1 & & & & & \\
1 & 2 & 1 & & & & \\
1 & 3 & 3 & 1 & & & \\
1 & 4 & 6 & 4 & 1 & & \\
1 & 5 & 10 & 10 & 5 & 1 & \\
1 & 6 & 15 & 20 & 15 & 6 & 1
\end{array}$$

7. *Если* $n = 2m$, *то* $C_n^0 < C_n^1 < \ldots < C_n^{m-1} < C_n^m > C_n^{m+1} > \cdots > C_n^n$.
Если $n = 2m+1$, *то* $C_n^0 < C_n^1 < \ldots < C_n^{m-1} < C_n^m = C_n^{m+1} > C_n^{m+2} > \cdots > C_n^n$.
8. *Свертка-развертка*:

$$C_{N_1+N_2}^K = \sum_{M=0}^{K} C_{N_1}^M C_{N_2}^{K-M}.$$

Переход от правой части этой формулы к левой называется *сверткой* (формула становится короче), в другую сторону — *разверткой*.

Доказательство. Существует немало способов вывода этих свойств. Мы изложим доказательство, использующее содержательный смысл чисел C_n^k. Пусть $U = \{e_1, \ldots, e_n\}$.

1. Число C_n^0 — это количество 0-элементных подмножеств множества U. Ясно, что такое подмножесво одно — пустое, $C_n^0 = 1$. Множество U имеет также ровно одно подмножество мощности n — само U. Отсюда $C_n^n = 1$.

2. Аналогично, C_n^1 — количество одноэлементных подмножеств множества U. Имеется ровно n таких подмножеств: $\{e_1\}, \ldots, \{e_n\}$. Далее, каждое $(n-1)$-элементное подмножество B в U однозначно определяется ровно одним элементом из U, не входящим в B. Такой элемент выбирается ровно n способами, поэтому $C_n^{n-1} = n$.

3. Эти формулы — частный случай формулы (1).

4. Каждому k-элементному подмножеству B в U взаимно однозначно соответствует $(n-k)$-элементное множество $\overline{B}$ (оно называется *дополнением* B в U, или *разностью* $U \setminus B$ *множеств* U и B), состоящее в точности из всех элементов в U, не входящих в B. Число C_n^k множеств B равно числу C_n^{n-k} множеств $\overline{B}$.

5. Положим $U_1 = \{e_1, \ldots, e_{n-1}\}$. Все C_n^k подмножеств B мощности k в U можно разбить на две непересекающиеся группы:
1) содержащие элемент e_n, их количество есть C_{n-1}^{k-1}, так как элементами подмножества U_1 заполняются лишь $k-1$ мест в множестве B (одно место в B занято элементом e_n);
2) не содержащие e_n, их количество есть C_{n-1}^k, так как элементами подмножества U_1 заполняются все k мест в множестве B.
По правилу суммы получаем $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$.

6. Каждый k-ый элемент $(1 \le k \le n-1)$ строки n треугольника вычисляется по формуле 5 сложением соответствующих элементов предыдущей строки. Значения элементов при $k = 0$ и $k = n$ определяются свойством 1.

7. Следует из формулы (1) и свойства 4. Легко видеть в треугольнике Паскаля.

8. Придадим входящим в формулу числам содержательный смысл. Пусть имеется N_1 мужчин и N_2 женщин. Из них надо выбрать K человек любого пола. Используем распространенный прием — подсчет двумя способами. С одной стороны, это можно сделать $C_{N_1+N_2}^K$ способами. Применим второй способ. Пусть в выбранной группе ровно M мужчин и $K-M$ женщин. Состав такой группы можно выбрать, по правилу произведения, $C_{N_1}^M C_{N_2}^{K-M}$ способами. При этом $M = 0, \ldots, K$. Остается применить правило суммы. $\square$

3.4 Формулы бинома и полинома. Биномиальные и полиномиальные коэффициенты

Теорема 5. *Формула бинома Ньютона*:

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k. \tag{2}$$

Выражение, стоящее в левой части этой формулы, называется *биномом* (сумма двух слагаемых, возведенная в степень), а числа C_n^k называются в связи с этим *биномиальными коэффициентами*.

Доказательство проведем с использованием комбинаторного смысла, но есть множество других способов.

Запишем левую часть в виде произведения n одинаковых множителей: $(a+b)^n = (a+b)(a+b)\cdots(a+b)$. Произведение сумм преобразуем в сумму произведений. Каждое произведение-слагаемое суммы содержит ровно n множителей, каждый из них — a или b. Если такое произведение содержит ровно k множителей b, то каждый из остальных $n-k$ множителей — это a. Число слагаемых, содержащих ровно k множителей b, равно C_n^k (из множества $\{1,\ldots,n\}$ номеров перемножаемых сумм $(a+b)$ выбираются k сумм, от которых берется слагаемое b. Слагаемые преобразованного выражения отличаются значением k, которое может быть $0,\ldots,n$. Остается применить правило суммы. $\square$

Примерами биномиальной формулы являются хорошо известные из школьного курса формулы

$$(a\pm b)^2 = a^2 \pm 2ab + b^2, \quad (a\pm b)^3 = a^3 \pm 3a^2b + 3a^2b \pm b^3$$

и более сложные

$$(a\pm b)^4 = a^4 \pm 4a^3b + 6a^2b^2 \pm 4ab^3 + b^4, \quad (a+b)^5 = a^5 \pm 5a^4b + 10a^3b^2 \pm 10a^2b^3 + 5ab^4 \pm b^5.$$

Теорема 6. *Справедливы следующие свойства сумм биномиальных коэффициентов*:

$$\sum_{k=0}^{n} C_n^k = 2^n, \tag{3}$$

$$\sum_{k=0}^{n} (-1)^k C_n^k = 0, \tag{4}$$

$$C_n^0 + C_n^2 + C_n^4 + \cdots = C_n^1 + C_n^3 + C_n^5 + \cdots = 2^{n-1}. \tag{5}$$

Доказательство. Первая сумма — это сумма всех элементов строки n треугольника Паскаля. Равенство (3) получается из (2) при $a = b = 1$. Вторая сумма

— это сумма всех элементов строки n треугольника Паскаля, имеющих чередующиеся знаки. Равенство (4) получается из (2) при $a = 1, b = -1$. Рассмотрим третью сумму. Положим

$$S_0 = C_n^0 + C_n^2 + C_n^4 + \cdots, \qquad S_1 = C_n^1 + C_n^3 + C_n^5 + \cdots.$$

Запишем суммы (3) и (4) в виде

$$C_n^0 + C_n^1 + C_n^2 + C_n^3 + \cdots + C_n^n = 2^n,$$

$$C_n^0 - C_n^1 + C_n^2 - C_n^3 + \cdots + (-1)^n C_n^n = 0.$$

Сложив два последних равенства, получим $2C_n^0 + 2C_n^2 + 2C_n^4 + \cdots = 2^n$, т. е. $2S_0 = 2^n$, откуда $S_0 = 2^n/2 = 2^{n-1}$, $S_1 = 2^n - S_0 = 2^n - 2^{n-1} = 2^{n-1}$. □

Обобщением биномиальной формулы является полиномиальная формула для степени суммы m слагаемых, в которой присутствуют полиномиальные коэффициенты.

Теорема 7 (полиномиальная формула).

$$(x_1 + \cdots + x_m)^n = \sum_{k_1+\cdots+k_m=n} \frac{k!}{k_1! \cdots k_m!} x_1^{k_1} \cdots x_m^{k_m}.$$

Суммирование ведется по всем неотрицательным целым числам $k_1, \ldots, k_m$ таким, что $k_1 + \cdots + k_m = n$.

Числа

$$\frac{k!}{k_1! \cdots k_m!}$$

называются *полиномиальными коэффициентами*. Их сумма равна m^n:

$$\sum_{k_1+\cdots+k_m=n} \frac{k!}{k_1! \cdots k_m!} = m^n.$$

Формула бинома — частный случай полиномиальной формулы при $m = 2$.

Пример 2. Запишем полиномиальную формулу для $(x_1+x_2+x_3)^4$. Вычислим

полиномиальнве коэффициенты:

k_1	k_2	k_3	$4!/(k_1!k_2!k_3!)$
0	0	4	1
0	1	3	4
0	2	2	6
0	3	1	4
0	4	0	1
1	0	3	4
1	1	2	12
1	2	1	12
1	3	0	4
2	0	2	6
2	1	1	12
2	2	0	6
3	0	1	4
3	1	0	4
4	0	0	1

Теперь можно выписать всю формулу, изменив для красоты порядок слагаемых:

$$(x_1+x_2+x_3)^4 = x_1^4+x_2^4+x_3^4+4(x_1^3x_2+x_1x_2^3+x_1^3x_3+x_1x_3^3+x_2^3x_3+x_2x_3^3)+$$
$$+6(x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2)+12(x_1^2x_2x_3+x_1x_2^2x_3+x_1x_2x_3^2).$$

Пример Вычислим, с какой вероятностью P слагаемое разложения $(x_1 + x_2 + x_3 + x_4)^3$ содержит квадрат переменной. По определению классической вероятности $P = M/N$. Найдем — число N всех слагаемых разложения. Они соответствуют векторам (k_1, k_2, k_3, k_4) с неотрицательными целыми координатами такими, что $k_1 + k_2 + k_3 + k_4 = 3$. Выпишем все такие векторы (для краткости скобки опускаем):

$$0003,\ 0012,\ 0021,\ 0030,\ 0102,\ 0111,\ 0201,\ 0210,\ 0300,$$

$$1002,\ 1011,\ 1020,\ 1101,\ 1110,\ 1200,\ 2001,\ 2010,\ 2100,\ 3000.$$

Их, как видим, 19. Из них 11 содержат координату, равную 2. Таким образом, $M = 11$ и $P = 11/19$.

3.5 Размещения и сочетания с повторениями

Если мы выбираем подмножество B мощности k множества $U = \{e_1, \ldots, e_n\}$, упорядоченное (размещение) или неупорядоченное (сочетание), то каждый из элементов $e_1, \ldots, e_n$ может входить в подмножество B только 0 или 1 раз (если входит, то не повторяется). Вызывают интерес и имеют содержательный смысл и такие выборки, состоящие из k элементов (их уже нельзя называть подмножествами множества U), в которых выбранные объекты могут повторяться. Простейшим примером являются слова фиксированной длины в конечном алфавите. Буквы в одном слове могут повторяться. Дадим точные математические определения таких комбинаторных конфигураций, научимся их подсчитывать и приведем другие содержательные примеры.

Пусть $U = \{e_1, \ldots, e_n\}$ — множество *типов* элементов, элементы каждого типа имеются в неограниченном количестве. Рассмотрим совокупность из k элементов, каждый элемент имеет тип из множества U. Упорядоченная такая совокупность называется *размещением с повторениями*, неупорядоченная — *сочетанием с повторениями по k элементов n типов*. Для числа размещений и сочетаний с повторениями приняты обозначения $\hat{A}_n^k$ и, соответственно, $\hat{C}_n^k$.

Теорема 8. *Число размещений с повторениями определяется формулой*

$$\hat{A}_n^k = n^k.$$

Доказательство. Каждое из мест выборки можно заполнить ровно n способами (элементом любого типа $e_1, \ldots, e_n$). Заполнить надо все k мест. Остается применить правило произведения. □

Замечание. Размещения с повторениями по k элементов n типов взаимно однозначно соответствуют словам длины k в алфавите мощности n. (Обратите внимание, что символы n и k поменялись ролями, и не путайте!)

Теорема 9. *Число сочетаний с повторениями выражается через число сочетаний без повторений формулами*

$$\hat{C}_n^k = C_{n+k-1}^k = C_{n+k-1}^{n-1}.$$

Доказательство. Пусть B — сочетание по k элементов n типов. Оно однозначно определяется вектором $(x_1, \ldots, x_n)$, где x_j — число вхождения в B элемента типа e_j:

$$B \leftrightarrow (x_1, \ldots, x_n), \quad \sum_{j=1}^{n} x_j = k, \quad x_j \geq 0.$$

Положим $y_j = x_j + 1$, тогда сочетанию B взаимно однозначно соответствует вектор

$$Y = (y_1, \ldots, y_n), \quad y_j \in \mathbb{N}, \quad \sum_{j=1}^{n} y_j = \sum_{j=1}^{n} (x_j + 1) = \sum_{j=1}^{n} x_j + k = n + k.$$

Количество сочетаний равно количеству таких векторов Y, а оно равно количеству разбиений $n + k = y_1 + \cdots + y_n$ числа $n + k \in \mathbb{N}$ в сумму n натуральных слагаемых. Найдем его. Будем (как древние люди или маленькие дети) представлять натуральное число m рядом из m точек. Разбиение такого числа на q слагаемых представляется $q - 1$ перегородками (палочками) между точками. Группы неразделенных точек соответствуют слагаемым, например, разбиение $7 = 3 + 2 + 1 + 1$ можно представить как $\cdots|\cdot\cdot|\cdot|\cdot$. Количество требуемых разбиений — это количество способов поставить $n - 1$ палочек между $n + k$ точками. Палочки ставятся в промежутки между точками, число промежутков есть $n + k - 1$, число способов — C_{n+k-1}^{n-1}. $\square$

Пример Люди, не играющие в домино, могут не знать особенности этой игры, в частности, сколько в домино костей. Найдем это число. Кость можно представить как неупорядоченную (кость можно перевернуть) пару $\{x_1, x_2\}$, где x_1, x_2 — количество очков на половинке кости, $x_1, x_2 \in \{0, 1, \ldots 6\}$. Число 0 изображается пустым квадратом, остальные числа — соответствующим количеством точек. Таким образом, $U = \{0, 1, \ldots 6\}$, и число костей домино есть

$$\hat{C}_7^2 = C_{7+2-1}^2 = C_8^2 = 8 \cdot 7/2 = 28.$$

4 Рекуррентные уравнения

Во многих комбинаторных задачах искомые числа являются членами некоторой последовательности, между которыми задано или выводится соотношение, называемое *рекуррентным*. В общем случае рекуррентное уравнение для членов последовательности $x_0, x_1, \ldots, x_n, x_{n+1}, \ldots$имеет вид

$$F(x_n, x_{n-1}, \ldots, x_0) = 0.$$

Рекуррентные уравнения называются также возвратными (этот термин отражает главное свойство членов последовательности). В информатике рекуррентности выражаются рекурсивными процедурами, главным свойством которых является самоприменимость. Вызов такой процедуры из себя называется рекурсией.

Рассмотрим ряд примеров, в которых мы выведем, а в ряде случаев и решим (т. е. найдем все числа последовательности) рекуррентные уравнения.

Пример 1 (задача о разрезании пиццы). Пицца разрезается n прямолинейными движениями ножа, при которых каждые две линии разреза пересекаются, но никакие три не пересекаются в одной точке. Сколько кусков пиццы образуется? Можно абстрагироваться от формы и размера пиццы и сформулировать задачу на математическом языке: на сколько частей делят плоскость n прямых, из которых любые две пересекаются, но никакие три не пересекаются в одной точке?

Пусть x_n — число таких частей. Ясно, что $x_0 = 1,\ x_1 = 2,\ x_2 = 4$. Исходя из этих условий, применим индукцию. В методе математической индукции главное — индуктивный переход.

Пусть проведены n прямых $a_1, \ldots, a_n$. Проведем следующую, $(n+1)$-ую прямую b. По условию она пересекается с прямыми $a_1, \ldots, a_n$. Рассмотрим точки пересечения $A_1, \ldots, A_n$. Эти n точек делят прямую b на $n+1$ частей, каждая из которых принадлежит своей новой части плоскости. Таким образом, количество частей увеличилось на $n+1$. Получено уравнение

$$x_{n+1} = x_n + n + 1 \tag{1}$$

с условием (оно называется начальным)

$$x_0 = 1. \tag{2}$$

Решим уравнение. Последовательно применяя формулу (1), получим

$$x_n = x_{n-1} + n = x_{n-2} + (n-1) + n = x_{n-3} + (n-2) + (n-1) + n =$$

$$= \cdots = x_0 + (1 + 2 + \cdots + n).$$

Используя (2) и формулу для суммы первых n членов арифметической прогрессии, окончательно находим

$$x_n = 1 + n(n-1)/2.$$

Пример 2 (задача о ханойской башне). Имеется n колец размеров $1, 2, \ldots, n$, нанизанных на вертикальный стержень A, в виде пирамидки с уменьшающимися снизу вверх размерами колец. Имееются также еще два стержня B и C без колец. Требуется переместить все кольца со стержня A на C, используя стержень B так, чтобы в любой момент никакое большее кольцо не находилось выше меньшего. Сколько операций перекладывания достаточно сделать?

Пусть x_n — оптимальное число операций. Ясно, что $x_0 = 0,\ x_1 = 1$. Нарисовав стержни, нетрудно подсчитать $x_2 = 3$ и даже, проявив терпение, $x_3 = 7$. Основная идея при проведении таких операций, состоит в следующем. Чтобы выполнялось условие на расположение колец по размерам, при любом способе решения придется сначала переместить верхние $n-1$ колец со стержня A на B, используя как вспомогательный стержень C, после чего самое большое кольцо размера n перекладывается с A на C, а затем остальные $n-1$ колец перекладываются с B на C с использованием в качестве вспомогательного стержня A. Из этих соображений получаем уравнение

$$x_n = 2x_{n-1} + 1 \tag{3}$$

с начальным условием $x_0 = 0$. Покажем, как можно его решить. Сделаем замену переменной (распространенный прием при решении многих видов уравнений) $x_n = y_n - 1$. Тогда $y_n - 1 = x_n = 2x_{n-1} = 2(y_{n-1} - 1) + 1$,

$$y_n = 2y_{n-1}, \qquad y_0 = 1,$$

откуда $y_n = 2^n,\ \ x_n = 2^n - 1$.

Эту задачу придумал в 1883 г. как головоломку французский инженер Эдуард Люка на основе восточной легенды о том, что Будда повелел жрецам провести такое перекладывание 64 золотых колец, из которых построена башня в городе Ханое. Жрецы трудятся день и ночь вот уже несколько тысячелетий, но конца их работе, как мы теперь знаем, в обозримом будущем не предвидится.

Пример 3. Он уже был рассмотрен в разд. 1. Если x_n — количество десятичных целых чисел от 0 до 10^n, не содержащих находящихся по соседству одинаковых цифр, то для для последовательности $x_0, x_1, x_2, \ldots$ получаем рекуррентное уравнение с начальным условием

$$x_{n+1} = x_n + 9^{n+1}, \qquad x_0 = 1.$$

Используя формулу суммы геометрической прогрессии со знаменателем 9, находим $x_n = (9^{n+1} - 1)/8$.

Пример 4 (задача о прозвонке кабеля). Имеется кабель, состоящий из N проводов. Требуется найти соответствие между проводами на левом и правом концах кабеля ("прозвонить" его) за минимальное число опытов x_N.

Рассмотрим такой алгоритм (он применяется и для других задач, в частности, для сортировки). Предположим, что N есть степень двойки. Разделим множество из N проводов на левом конце кабеля на две равные части (свяжем $N/2$ проводов). Теперь на левом конце кабеля две связки, на правом — N проводов. Прозвоним одну связку на левом конце с каждым из N проводов на правом конце и найдем соответствие. Далее разделим каждую из связок левого конца пополам еще раз, придем к двум аналогичным задачам с параметром $N/2$. Таким образом,

$$x_N = 2x_{N/2} + N.$$

Этому рекуррентному уравнению удовлетворяет, как нетрудно проверить, последовательность $x_N = N \log_2 N$. (Как найти такое решение — это отдельная задача, не будем ее рассматривать.) Нетрудно понять, что ограничение $N = 2^m$ не является принципиальным, на каждом шаге можно делить множество не точно, а примерно пополам, суть процесса не изменится. Можно показать, что порядок роста $N \log N$ функции x_N при $N \to \infty$ является оптимальным. Для этого заметим, что всего возможно $N!$ вариантов соответствия между N проводами на левом и N проводами на правом концах кабеля. Один опыт прозвонки имеет два исхода: успех (соответствие между одним проводом слева и одним проводом справа обнаружено) и неудачу. Пусть K — число операций прозвонки. Тогда $2^K \geq N!$. Используя формулу Стирлинга $N! \sim CN^N$ при $N \to \infty$, где C — некоторая постоянная, убеждаемся, что $K \geq N \log_2 N + \log_2 C$.

Пример 5 (задача о кроликах Фибоначчи). Имеется пара новорожденных кроликов, самец и самка. Кролики взрослеют 2 месяца, а затем начинают плодиться: каждый месяц они рождают еще пару, также самца и самку. С ними происходит то же самое: они два месяца взрослеют, а затем каждый месяц рождают пару из самца и самки, которые через два месяца начинают плодиться тем же образом. Так и происходит неограниченное размножение кроликов, смертности среди них абсолютно никакой нет. В реальной жизни это невозможно, но как модель вполне красиво. Задачу описал и проанализировал в XIII в. монах Леонардо Фибоначчи из г. Пиза. Задача состоит в нахождении количества x_n пар кроликов через n месяцев от даты рождения начальной пары. (Позднее появилось название "числа Фибоначчи". Удивительно, что они проявляются в огромном множестве самых разнообразных явлений и ситуаций и тесно связаны с не менее известным количественным соотношением, называемым "золотым сечением".) Числа Фибоначчи обладают многочисленными замечательными и красивыми свойствами (см. Воробьев Н.Н. Числа Фибоначчи — М.: Наука, 1984), мы покажем, как их найти.

Итак, $x_0 = x_1 = 1$ (два первых месяца кролики взрослеют). Но далее получаем $x_2 = 2$ (начальная пара размножилась впервые), $x_3 = 3$ (начальная пара размножилась уже дважды, а кролики, рожденные в прошлом месяце, еще не выросли), $x_4 = 5$ (стала размножаться и вторая пара), аналогично $x_5 = 8$, $x_6 = 13$, $x_7 = 21$ и вообще условия задачи описываются рекуррентным уравнением

$$x_n = x_{n-1} + x_{n-2}, \quad n \geq 2, \tag{4}$$

с начальными условиями

$$x_0 = x_1 = 1. \tag{5}$$

Приведем еще две содержательные комбинаторные задачи, описываемые тем же самым уравнением (4).

Пример 5'. Пусть y_n — количество перестановок $\pi(j)$ элементов $j = 1, 2, \ldots, n$, при которых каждый элемент j либо остается на месте, либо перемещается только на соседнее место, т. е.

$$\pi(1) \in \{1, 2\}, \quad \pi(n) \in \{n-1, n\}, \quad \pi(j) \in \{j-1, j, j+1\},\ 2 \leq j \leq n-1.$$

Пусть π — одна из y_n искомых перестановок n элементов. Если $\pi(n) = n$, надо переставить при тех же условиях $n-1$ предыдущих элементов. Если $\pi(n) = n-1$, то $\pi(n-1) = n$ и надо переставить при тех же условиях предыдущие $n-2$ элементов. По правилу суммы получаем

$$y_n = y_{n-1} + y_{n-2}, \quad n \geq 3.$$

Очевидно, $y_1 = 1, y_2 = 2! = 2$. Значение y_0 не имеет содержательного смысла, но для получения той же последовательности $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ удобно принять соглашение $y_0 = 1$.

Пример 5". Пусть z_n — количество бинарных векторов $b_1 \ldots b_n$ длины n, не имеющих двух и более нулей подряд. Очевидно, $z_1 = 2$, $z_2 = 3$ $(01, 10, 11)$. Пусть $b_1 \ldots b_n$ — такой вектор. Если $b_n = 1$, то этому же условию удовлетворяет вектор $b_1 \ldots b_{n-1}$. Если же $b_n = 0$, то $b_{n-1} = 1$ и указанному условию удовлетворяет вектор $b_1 \ldots b_{n-2}$. По правилу суммы

$$z_n = z_{n-1} + z_{n-2}, \quad n \geq 3.$$

Чтобы получившаяся последовательность как можно меньше отличалась от предыдущих, согласимся, что $z_0 = 1$ (получим последовательность $1, 2, 3, 5, 8, \ldots$).

5 Линейные рекуррентные уравнения

5.1 Однородные уравнения

Уравнение

$$x_{n+p} = a_{p-1}x_{n+p-1} + a_{p-2}x_{n+p-2} + \cdots + a_1x_{n+1} + a_0x_n \tag{1}$$

называется *линейным однородным рекуррентным уравнением порядка p для последовательности* $x_0, x_1, \ldots$. В этом уравнении неизвестными являются члены x_n последовательности (требуется найти формулу для x_n), числа $a_0, \ldots, a_{p-1}$ заданы, они называются *коэффициентами уравнения* (1). Коэффициенты и неизвестные могут быть любыми комплексными числами, но содержательный смысл, важный для задач комбинаторики, имеют целые неотрицательные решения. (Из примеров предыдущего раздела линейным однородным является только уравнение (4).) Опишем метод решения таких уравнений.

Характеристическое уравнение для уравнения (1) имеет вид

$$t^p = a_{p-1}t^{p-1} + a_{p-2}t^{p-2} + \cdots + a_1t + a_0. \tag{2}$$

Это алгебраическое уравнение степени p относительно неизвестной t. Оно имеет ровно p комплексных корней с учетом кратности.

Пусть $t_1, \ldots, t_m$ — все корни характеристического уравнения (2), и они имеют кратности $k_1, \ldots, k_s$, $k_1 + \cdots + k_m = p$, т. е. имеет место разложение на множители

$$t^p - a_{p-1}t^{p-1} - a_{p-2}t^{p-2} - \cdots - a_1t - a_0 = (t-t_1)^{k_1}(t-t_2)^{k_2}\cdots(t-t_m)^{k_m}.$$

Тогда *общее решение* уравнени (1) описывается формулой

$$x_n = \sum_{j=1}^{m} P_j(n)t_j^n, \tag{3}$$

где $P_j(n)$ — многочлены от n степени $k_j - 1$, т. е.

$$P_j(n) = b_{j,k_j-1}n^{k_j-1} + b_{j,k_j-2}n^{k_j-2} + \cdots + b_{j,1}n + b_{j,0}.$$

В частности, если t_j — корень кратности 1, то $P_j(n)$ есть постоянная C_j. Многочлен $P_j(n)$ полностью определяется своими коэффициентами b_{j,k_j-1}, b_{j,k_j-2},..., $b_{j,1}$, $b_{j,0}$. Таким образом, общее решение содержит ровно p произвольных постоянных b_{j,k_j-1}, b_{j,k_j-2},..., $b_{j,1}$, $b_{j,0}$, $j = 1, \ldots, m$. Если вместо всех букв $b_{j,i}$ подставить конкретные комплексные числа, то получим *частное решение*. Таким образом, из общего решения можно получить бесконечное множество частных решений. Для

однозначного определения частного решения уравнения порядка p задают p *начальных условий* — числа $x_0, x_1, \ldots, x_{p-1}$. Тогда неизвестные коэффициенты $b_{j,i}$ находятся из системы p линейных алгебраических уравнений.

Пример 1. Решим уравнение

$$x_{n+4} = -x_{n+3} + 3x_{n+2} + x_{n+1} - 2x_n$$

с начальными условиями

$$x_0 = 3, \quad x_1 = 2, \quad x_2 = 5, \quad x_3 = 4.$$

Это однородное уравнение порядка 4. Составим характеристическое уравнение:

$$t^4 = -t^3 + 3t^2 + t - 2.$$

Имеем многочлен степени 4 с целыми коэффициентами $f(t) = t^4 + t^3 - 3t^2 - t + 2$. Требуется найти все его (возможно, комплексные) корни. Известно, что целые корни многочлена с целыми коэффициентами являются делителями его свободного коэффициента. В нашем случае свободный коэффициент -2 имеет делители $\pm 1, \pm 2$. Легко вычисляем $f(1) = 0$. Это значит, $t_1 = 1$ является корнем. По теореме Безу многочлен $f(t)$ делится на $t - 1$. Разделив, находим частное $t^3 + 2t^2 - t - 2$, т. е.

$$f(t) = (t-1)(t^3 + 2t^2 - t - 2)$$

. Многочлен $g(t) = t^3 + 2t^2 - t - 2$ имеет уже меньшую степень 3, его свободный коэффициент -2 делится, в частности, на 1. Легко вычисляем $g(1) = 0$, находим корень $t = 1$ и, разделив на $t - 1$, представляем $g(t) = (t-1)(t^2 + 3t + 2)$, откуда

$$f(t) = (t-1)g(t) = (t-1)^2(t^2 + 3t + 2).$$

Далее, $t^2 + 3t + 2 = (t+1)(t+2)$ и

$$f(t) = (t-1)^2(t+1)(t+2).$$

Все корни характеристического уравнения есть $t_1 = 1, t_2 = -1, t_3 = -2$, они имеют кратности $k_1 = 2, k_2 = k_3 = 1$, поэтому общее решение рекуррентного уравнения имеет вид

$$x_n = (An + B)1^n + C(-1)^n + D(-2)^n$$

(здесь для краткости переименованы коэффициенты, указанные в формуле (3): $A = b_{11}, B = b_{10}, C = C_2, D = C_3$). Коэффициенты A, B, C, D найдем из начальных условий:

$$\begin{array}{rrrrrr} x_0 = & & B & +C & +D & = 3 \\ x_1 = & A & +B & -C & -2D & = 2 \\ x_2 = & 2A & +B & +C & +4D & = 5 \\ x_3 = & 3A & +B & -C & -8D & = 4 \end{array}$$

Эта система линейных уравнений имеет единственное решение $A = 1$, $B = 2$, $C = 1$, $D = 0$, поэтому частным решением, удовлетворяющим заданным начальным условиям, является $x_n = n + 2 + (-1)^n$.

Ответ: $x_n = n + 2 + (-1)^n$.

Пример 2. Решим задачу Фибоначчи

$$x_{n+2} = x_{n+1} + x_n, \quad x_0 = x_1 = 1.$$

Уравнение однородное порядка 2. Характеристическое уравнение $t^2 = t + 1$ имеет корни

$$t_1 = \frac{1 - \sqrt{5}}{2}, \quad t_2 = \frac{1 + \sqrt{5}}{2}$$

кратности 1, общее решение имеет вид $x_n = C_1 t_1^n + C_2 t_2^n$. Начальные условия задают систему уравнений

$$\begin{array}{rr} C_1 & +C_2 = 1 \\ (1 - \sqrt{5})C_1 & +(1 + \sqrt{5})C_2 = 2 \end{array}$$

Решая ее и подставляя C_1, C_2 в формулу общего решения, находим после элементарных преобразований частное решение в красивом виде

$$x_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{n+1} \right].$$

Формула содержит иррациональности, но все члены последовательности Фибоначчи, вычисляемые по ней (с применением формулы бинома), целые. Можно при наличии терпения в этом убедиться при небольших значениях n. Проделав такие опыты, нетрудно понять, что для нахождения членов последовательности проще использовать рекуррентное уравнение, чем выведенную только что формулу. Это характерно для многих других комбинаторных чисел и показывает пользу рекуррентных уравнений.

5.2 Неоднородные уравнения, сводящиеся к однородным

Неоднородное линейное рекуррентное уравнение вида

$$x_{n+p} = a_{p-1} x_{n+p-1} + a_{p-2} x_{n+p-2} + \cdots + a_1 x_{n+1} + a_0 x_n + b, \tag{4}$$

где $b \neq 0$ — числовой коэффициент, в большом числе случаев можно свести к однородному линейной заменой переменных (метод применяется для решения многих уравнений в различных областях математики). Продемонстрируем метод замены переменных на примере.

Пример 3. Рассмотрим уравнение с начальными условиями

$$x_{n+2} = 4x_n + b, \quad x_0 = 1, \quad x_1 = 6.$$

Для всех $n = 0, 1, 2, \ldots$ положим $x_n = y_n + \gamma$, где постоянная γ пока неизвестна. Подставим эти выражения в исходное уравнение:

$$y_{n+2} + \gamma = 4(y_n + \gamma) + b,$$

откуда

$$y_{n+2} = 4y_n + (3\gamma + b).$$

Уравнение для чисел y_n станет однородным, если $3\gamma + b = 0$, т. е. $\gamma = -b/3$. При таком выборе γ находим общее решение однородного уравнения $y_{n+2} = 4y_n$:

$$y_n = C_1(-2)^n + C_2 2^n,$$

откуда

$$x_n = C_1(-2)^n + C_2 2^n - b/3.$$

Найдем C_1, C_2 из начальных условий. Решая систему уравнений

$$\begin{array}{rrr} C_1 & +C_2 & -b/3 = 1 \\ -2C_1 & +2C_2 & -b/3 = 6, \end{array}$$

получим $C_1 = -1 + b/12$, $C_2 = 2 + b/4$ и тогда

$$x_n = (-1 + b/12)(-2)^n + (2 + b/4)2^n - b/3.$$

Задания для самостоятельного решения

4. Решите однородное рекуррентное уравнение с начальными условиями

$$x_{k+3} = (N-2)x_{k+2} + (2N-1)x_{k+1} + Nx_k, \ x_0 = 2, \ x_1 = 2N+1, \ x_2 = 2N^2 - 2.$$

5. Решите неоднородное рекуррентное уравнение с начальным условием

$$x_{k+1} = (N+2)x_k + N, \qquad x_0 = N - 1.$$

Номер варианта N остается таким же, как в предыдущих заданиях.

Решения присылайте по прежнему адресу MeshchaninovDG@mpei.ru
Мещанинову Дмитрию Германовичу

6 Метод включений-исключений

Он часто применяется для решения задач не только в комбинаторике и дискретной математике, но и в других областях.

Пример 1. Будем обозначать символами $|M|$ число элементов конечного множества M. Как найти $|A \cup B|$? Формула $|A \cup B| = |A| + |B|$ в общем случае неверна, некоторые элементы могут принадлежать обоим множествам A и B, в такой формуле они учтены дважды. Правильной является формула

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{1}$$

Аналогично поставим вопрос о вычислении $|A \cup B \cup C|$. Положим $D = A \cup B$. Тогда $x = |A \cup B \cup C| = |D \cup C|$ и, согласно (1), находим $x = |D| + |C| - |D \cap C|$. Подставим сюда $D = A \cup B$ и снова применим (1):

$$x = |A| + |B| - |A \cap B| + |C| - |(A \cup B) \cap C| =$$

$$= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| =$$

$$= |A| + |B| - |A \cap B| + |C| - (|A \cap C| + |B \cap C| - |A \cap B \cap C|.$$

Окончательно получаем

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \tag{2}$$

Еще длиннее оказывается формула для $|A \cup B \cup C \cup D|$, получаемая с использованием (1) и (2):

$$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D| -$$

$$-|A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D| +$$

$$+|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|. \tag{3}$$

А как найти $|A_1 \cup \cdots \cup A_m|$?

Это примеры формул включения (соответствующего слагаемым со знаком $+$) и исключения (слагаемые со знаком $-$).

Общая формулировка задачи

Имеется N объектов, которые могут обладать или не обладать свойствами $P_1, \ldots, P_m$. Для каждого набора $(j_1, \ldots, j_r)$, $1 \le r \le m$, $1 \le j_1 < j_2 < \cdots < j_r \le m$, известно количество $N(j_1, \ldots, j_r)$ объектов, обладающих свойствами $P_{j_1}, \ldots, P_{j_r}$ (и, возможно, другими). Требуется найти *число N_k объектов, обладающих ровно k свойствами* $(0 \le k \le m)$.

Укажем способ вычисления N_k. Положим:

$$S_0 = N,$$

$$S_r = \sum_{1 \le j_1 < j_2 < \cdots < j_r \le m} N(j_1, \ldots, j_r), \quad r = 1, \ldots, m. \tag{4}$$

Тогда

$$N_k = \sum_{r=k}^{m} (-1)^{r-k} C_r^k S_r. \tag{5}$$

Выражение (5) называется *общей формулой включений-исключений* (C_r^k — биномиальные коэффициенты). Если $k = 0$, то

$$N_0 = \sum_{r=0}^{m} (-1)^r S_r = N - S_1 + S_2 - \cdots + (-1)^r S_r. \tag{6}$$

Это *частная формула включений-исключений для числа N_0 объектов, не обладающих ни одним из свойств $P_1, \ldots, P_m$.*

В формулах включения-исключения числа $N(j_1, \ldots, j_r)$ предполагаются известными, хотя они не всегда указаны в условии задачи. В таких случаях их надо найти с помощью правил комбинаторных вычислений. Рассмотрим ряд примеров.

Вернемся к **примеру 1** и интерпретируем его как частный случай рассмотренной общей постановки задачи. Объекты здесь — элементы множества $U = A_1 \cup \cdots \cup A_m$, при этом $N = |U|$, свойство P_j состоит в принадлежности элемента множеству A_j, $j = 1, \ldots, m$. Каждый из элементов принадлежит хотя бы одному множеству A_j, т. е. каждый объект обладает хотя бы одним из свойств, поэтому $N_0 = 0$. Условие "объект обладает свойствами $P_{j_1}, \ldots, P_{j_r}$" равносильно принадлежности элемента пересечению $A_{j_1} \cap \cdots \cap A_{j_r}$, поэтому $N(j_1, \ldots, j_r) = |A_{j_1} \cap \cdots \cap A_{j_r}|$.

Подставляя эти значения в (4), (6), получаем,

$$0 = |U| + \left(\sum_{r=1}^{m} (-1)^r \sum_{1 \le j_1 < j_2 < \cdots < j_r \le m} |A_{j_1} \cap \cdots \cap A_{j_r}| \right),$$

откуда

$$|U| = |A_1 \cup \cdots \cup A_m| = - \left(\sum_{r=1}^{m} (-1)^r \sum_{1 \le j_1 < j_2 < \cdots < j_r \le m} |A_{j_1} \cap \cdots \cap A_{j_r}| \right),$$

т.е.

$$|A_1 \cup \cdots \cup A_m| = \left(\sum_{r=1}^{m} (-1)^{r+1} \sum_{1 \le j_1 < j_2 < \cdots < j_r \le m} |A_{j_1} \cap \cdots \cap A_{j_r}| \right).$$

При $m = 2, 3, 4$ эта общая формула имеет вид (1), (2) и (3) соответственно.

Пример 2. Найдем количество $\pi(100)$ простых чисел p таких, что $p \le 100$. Натуральное число p называется простым, если $p \ge 2$ и его делителями являются только 1 и само p. Для этого воспользуемся давно (еще в античные времена) известной теоремой: число m простое тогда и только тогда, когда оно не делится ни на одно простое число q такое, что $q \le \sqrt{m}$. Доказать теорему очень легко: надо разложить число на простые множители, такое разложение для любого натурального единственно с точностью до порядка записи множителей. Найдем количество натуральных чисел среди первых 100, не делящихся ни на 2, ни на 3, ни на 5, ни на 7. Будем считать числа $1, \dots, 100$ объектами, делимость на q — свойством P_q. Тогда

$$N = S_0 = 100,$$

$$N(2) = 100/2 = 50,\ N(3) = \lfloor 100/3 \rfloor = 33,\ N(5) = 100/5 = 20,\ N(7) = \lfloor 100/7 \rfloor = 14,$$

$$N(2,3) = \lfloor 100/6 \rfloor = 16,\ N(2,5) = 100/10 \rfloor = 10,\ N(2,7) = \lfloor 100/14 \rfloor = 7,$$

$$N(3,5) = \lfloor 100/15 \rfloor = 6,\ N(3,7) = \lfloor 100/21 \rfloor = 4,\ N(5,7) = \lfloor 100/35 \rfloor = 2,$$

$$N(2,3,5) = \lfloor 100/30 \rfloor = 3,\ N(2,3,7) = \lfloor 100/42 \rfloor = 2,\ N(2,5,7) = \lfloor 100/70 \rfloor = 1,$$

$$N(3,5,7) = \lfloor 100/105 \rfloor = 0,\ N(2,3,5,7) = \lfloor 100/210 \rfloor = 0,$$

$$S_1 = N(2) + N(3) + N(5) + N(7) = 117,$$

$$S_2 = N(2,3) + N(2,5) + N(2,7) + N(3,5) + N(3,7) + N(5,7) = 45,$$

$$S(3) = N(2,3,5) + N(2,3,7) + N(2,5,7) + N(3,5,7) = 6,\ S_4 = N(2,3,5,7) = 0.$$

По формуле (6) получаем

$$N_0 = S_0 - S_1 + S_2 - S_3 + S_4 = 100 - 117 + 45 - 6 + 0 = 22.$$

Среди этих 22 чисел оказывается и число 1, не являющееся простым по определению, а простые числа 2, 3, 5, 7 отсутствуют, поэтому

$$\pi(100) = 22 - 1 + 4 = 25.$$

Вот все простые числа не большие, чем 100: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$ $43{,}47, 53, 59, 61, 67, 71, 73, 79,\ 83, 89, 97$. Заметим, что следующее число 101 также простое. [4]

Пример 3. Таким же образом можно анализировать перестановки с неподвижными элементами. Объекты — все $m!$ перестановок $\alpha(x)$ элементов $x = 1, 2, \dots, m$.

[4] В общем случае соотношение

$$\pi(x) \sim \frac{x}{\ln x}$$

при $x \to \infty$ для любого вещественного положительного числа x установлено во второй половине XIX в. русским математиком и механиком Чебышёвым Пафнутием Львовичем и французскими математиками Жаком Адамаром и Шарлем де ла Валле Пуссеном.

Свойство P_j состоит в неподвижности элемента j ($\alpha(j) = j$), $j = 1, \ldots, m$, т. е. переставляются только элементы, отличные от j. Тогда

$$N = m!, \qquad N(j_1, \ldots, j_r) = (m - r)!,$$

число перестановок, имеющих ровно k неподвижных элементов, находится как N_k по формуле (5).

Задание для самостоятельного решения

6. Найдите число перестановок элементов $1, \ldots, m$, оставляющих ровно k элементов неподвижными.

N	m	k
1	4	0
2	5	1
3	4	1
4	6	1
5	4	2
6	5	0
7	5	2
8	5	3
9	4	3
10	5	4
11	6	2
12	5	5
13	7	7
14	6	3
15	7	6
16	6	4

Номер варианта N остается таким же, как в предыдущих заданиях.
Решения присылайте по прежнему адресу MeshchaninovDG@mpei.ru Мещанинову Дмитрию Германовичу

7 Основные понятия теории графов

Важным инструментом дискретной математики являются графы.

Графом называется пара множеств $G = (V, E)$, $V = \{v_1, \ldots, v_n\}$, $E = \{e_1, \ldots, e_m\}$. Элементы v_i множества V называются *вершинами* графа G, элементы e_j множества E — *ребрами*, это пары $e_j = \{v_{j_1}, v_{j_2}\}$ различных вершин. Если вершины

v_{j_1}, v_{j_2} образуют ребро e_j, они называются *смежными*, при этом вершина v_{j_1} и ребро e_j называются *инцидентными* друг другу, это же справедливо и для вершины v_{j_2} и того же ребра e_j. Число ребер, инцидентных вершине v_i, называется степенью этой вершины и обозначается $d(v_i)$. $V\ E\ (\ n\ m)$.

Пример 1. Рассмотрим граф G со следующими вершинами и ребрами:

$$V = \{v_1, \ldots, v_7\}, \quad E = \{e_1, e_2, e_3, e_4, e_5\},$$

$$e_1 = \{v_1, v_2\},\ e_2 = \{v_1, v_3\},\ e_3 = \{v_2, v_3\},\ e_4 = \{v_2, v_4\},\ e_5 = \{v_5, v_6\}.$$

Тогда $n = 7,\ m = 5$, G неориентированный и имеет следующие степени вершин:

i	1	2	3	4	5	6	7
$d(v_i)$	2	3	2	1	1	1	0

Если сложить степени, то получим $2 + 3 + 2 + 1 + 1 + 1 + 0 = 2 \cdot 5$.

Теорема 1. *Сумма степеней всех вершин графа равна удвоенному числу ребер*:

$$\sum_{i=1}^{n} d(v_i) = 2m. \tag{1}$$

Доказательство. Пусть $d(v_i, v_j)$ — это число ребер, соединяющих вершины v_i и v_j. Тогда $d(v_i, v_j) = d(v_j, v_i) \in \{0, 1\}$,

$$\sum_{i=1}^{n} d(v_i) = \sum_{i=1}^{n} \sum_{j=1}^{n} d(v_i, v_j) = \sum_{j=1}^{n} \sum_{i=1}^{n} d(v_i, v_j),$$

и в левой части равенства (1) каждое ребро учтено ровно дважды: в слагаемых $d(v_i)$ и $d(v_j)$. $\square$

Следствие 1. *Число вершин нечетной степени в графе четно.*

В **примере 1** четыре вершины нечетной степени v_2, v_4, v_5, v_6. Вершина v_7 имеет четную степень 0, такая вершина называется *изолированной.*

Приведем пример, в котором графы и степени вершин применяются для решения логической задачи.

Пример 2. Ученики одного класса проводили на уроке математики круговой турнир по игре в "крестики-нолики". Участников было пятеро. Когда прозвенел звонок с урока, турнир прервали, в этот момент оказалось сыграно 6 партий. Больше всего игр, по три, провели только Алена и Вася. Сколько игр провели остальные участники? Кто с кем играл?

Опишем турнир графом с 5 вершинами, соответствующими участникам. Соединим пару вершин ребром, если соответствующие участники сыграли друг с другом. Назовем участников A (Алена), B (Вася), C(Саша), D (Даша) и E (Егор),

так же обозначим и вершины. Тогда число партий, сыгранным каждым участником X, есть степень $d(X)$ вершины X. В силу теоремы 1 имеем

$$d(A) + d(B) + d(C) + d(D) + d(E) = 2 \cdot 6, \quad d(A) = d(B) = 3.$$

Не ограничивая общности, полагаем $d(C) \geq d(D) \geq d(E)$. Тогда $d(C) < 3$ и

$$d(C), d(D), d(E) \in \{0, 1, 2\}, \tag{2}$$

$$d(C) + d(D) + d(E) = 6. \tag{3}$$

Если $d(E) = 0$, то $d(C) + d(D) = 6$ и условия (2) и (3) не могут выполняться одновременно. Если $d(E) = 1$, то $d(C) + d(D) = 5$ и условия (2) и (3) также не выполняются одновременно. Остается единственная возможность $d(E) = 2$. При этом и $d(C) = d(D) = 2$. Необходимо проверить, что такая возможность действительно реализуется, т. е. построить граф турнира. Это можно сделать единственным способом, соответствующим следующему множеству из 6 игравших пар (ребер графа): A и C, A и D, A и E, B и C, B и D, B и E.

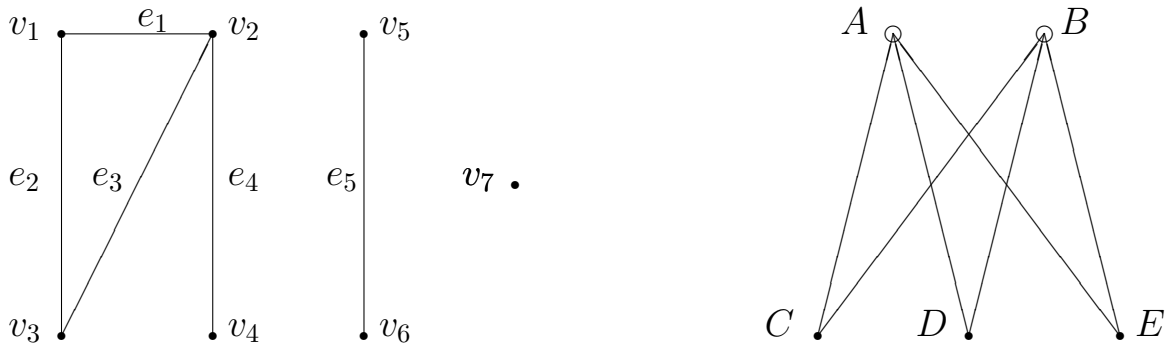
Рассмотрим **способы задания графов**.

1. Указанием списков вершин и ребер.
Этим способом были заданы графы в приведенных примерах.

2. Диаграмой на плоскости (графическим изображением).

Вершинам соответствуют точки на плоскости, их расположение не имеет значения. Ребра графа изображаются отрезками или дугами кривых, соединяющими пары точек.

Графы из примеров 1 и 2 можно задать следующими изображениями.



3. Матрицами из нулей и единиц.

Матрица смежности $A(G)$ графа $G = (\{v_1, \ldots, v_n\}, \{e_1, \ldots, e_m\})$ — квадратная порядка n, она устроена следующим образом: $A(G) = (a_{ij})_{n \times n}$, где

$$a_{ij} = \begin{cases} 1, & \text{если вершины } v_i \text{ и } v_j \text{ смежны,} \\ 0, & \text{в противном случае.} \end{cases}$$

Матрица $A(G)$ симметрична, ее диагональные элементы равны 0, число единиц в строке i (как и число единиц в столбце i) равно $d(v_i)$, общее число единиц в матрице равно $2m$.

Матрица инциденций $B(G)$ графа G имеет размер $m \times n$, $B(G) = (b_{ij})_{m \times n}$, где

$$b_{ij} = \begin{cases} 1, & \text{если ребро } e_i \text{ и вершина } v_j \text{ инцидентны,} \\ 0, & \text{в противном случае.} \end{cases}$$

Каждая строка матрицы $B(G)$ содержит ровно две единицы, число единиц в столбце j равно $d(v_j)$.

Матрицы и списки применяются при решении задач о графах на компьютере. При "ручном" решении задач на небольших графах привычнее диаграммы, они обладают наглядностью и лаконичностью. Каждый из способов полностью определяет граф и легко преобразуется в другой способ представления этого же графа. Мы часто будем использовать матрицы и списки, чтобы не рисовать диаграммы.

Для графа из **примера 1** получаем

$$A(G) = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad B(G) = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Методами комбинаторных вычислений нетрудно получить

Следствие 2. *Число различных графов, имеющих вершины* $v_1, \ldots, v_n$, *равно* $2^{n(n-1)/2}$. *Число различных графов, имеющих вершины* $v_1, \ldots, v_n$ *и ровно* m *ребер, составляет* $C^m_{n(n-1)/2}$.

Введем еще несколько важнейших понятий. *Маршрут, соединяющий вершины* v_i *и* v_j графа, — это чередующаяся последовательность инцидентных друг другу вершин и ребер, крайними элементами которой являются v_i и v_j. Если $v_i = v_j$, то маршрут называется *циклом*. Число ребер в маршруте называется его *длиной*.

В графе из **примера 1** последовательность $v_1e_1v_2e_4v_4e_4v_2e_3v_3$ образует маршрут длины 4, последовательность $v_1e_1v_2e_3v_3e_2v_1$ — цикл длины 3.

Граф называется *связным*, если любые две его вершины можно соединить некоторым маршрутом. Граф $G_1(V_1, E_1)$ называется *подграфом графа* $G(V, E)$, если

множества его вершин и ребер образуют подмножества $V_1 \subseteq V$, $E_1 \subseteq E$. Максимальный связный подграф графа называется его *компонентой связности*. Связный граф имеет ровно одну компоненту связности. Если имеется не менее двух компонент, граф несвязен. Если граф G имеет n вершин и $k \geq 2$ компонент, содержащих $n_1, \dots n_k$ вершин, $n_1 + \dots + n_k = n$, то его матрица смежности разбивается на блоки — подматрицы порядков $n_1, \dots, n_k$, окруженные лишь нулевыми элементами. (Это хорошо видно в матрице для графа из примера 1, в других случаях для большей наглядности удобно провести перестановку строк (и столбцов) матрицы $A(G)$.) Граф из **примера 1** несвязен, он имеет три компоненты

$$G_1 = (\{v_1, v_2, v_3, v_4\}, \{e_1, e_2, e_3, e_4\}), \quad G_2 = (\{v_5, v_6\}, \{e_5\}), \quad G_3 = (\{v_7\}, \emptyset);$$

граф из **примера 2** связен.

Некоторые циклы особенно важны. *Эйлеровым*[5] называется цикл, проходящий через каждое ребро графа ровно один раз. Если, например, вершины графа соответсвуют пунктам на местности, а ребра — дорогам, соединяющим эти пункты, то эйлеров цикл дает возможность оказаться на каждой дороге (чтобы выполнить какое-либо действие на ней, например, установить знак) ровно один раз и вернуться в место старта. В такой постановке эта задача и появилась впервые, в 1752 г., как задача о кенигсбергских мостах. Роль вершин графа играли участки суши — берега и острова протекающей в г. Кенигсберге (ныне Калининград) реки Преголь, ребер — мосты. Леонард Эйлер, работавший в то время в Петербургской Академии наук, дал исчерпывающее решение задачи. Им доказана

Теорема 2. *Эйлеров цикл в графе существует тогда и только тогда, когда выполнены два условия*:

1) *граф связен,*

2) *степень каждой вершины четна.*

Этот факт иногда называют исторически первой теоремой теории графов, хотя Л. Эйлер и его современники такого понятия не знали и не вводили.

В **примере 1** эйлерова цикла нет, так как граф G не является связным. Эйлерова цикла нет и в компоненте связности G_1 этого графа, так как вершины v_2, v_4, v_5, v_6 имеют нечетные степени.

[5]Леонард Эйлер (1707–1783) — математик, физик и астроном, родился в Швейцарии, работал в Германии и России

Пример 3. Пусть граф задан матрицей смежности

$$A(G) = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Матрица $A(G)$ не разбивается на блоки, поэтому граф связен. Число единиц в каждой строке четно, т. е степень каждой вершины четна. По теореме 2 существует эйлеров цикл. Укажем ребра в порядке их прохождения эйлеровым циклом:

$$e_1 = \{v_1, v_2\},\ e_2 = \{v_2, v_3\},\ e_3 = \{v_3, v_6\},\ e_4 = \{v_6, v_2\},\ e_5 = \{v_2, v_4\},$$

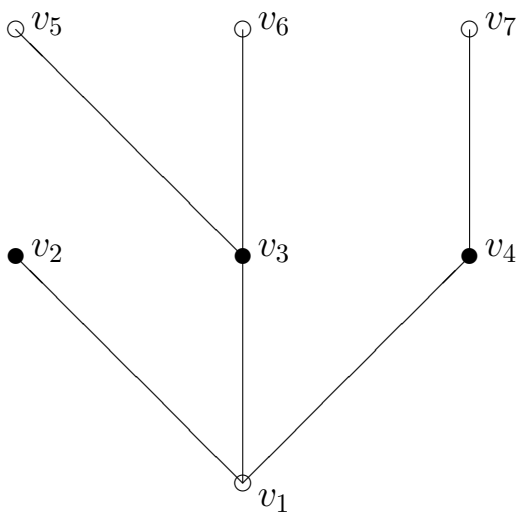
$$e_6 = \{v_4, v_6\},\ e_7 = \{v_6, v_5\},\ e_8 = \{v_5, v_4\},\ e_9 = \{v_4, v_1\}.$$

Гамильтоновым[6] называется цикл, проходящий ровно один раз через каждую вершину графа. Задача о существовании гамильтонова цикла, известна с XIX в. и, в отличие от задачи об эйлеровом цикле, не решена до сих пор. В графе из **примера 3** есть гамильтонов цикл $(v_1, v_2, v_3, v_6, v_5, v_4, v_1)$ (указаны только вершины), в **примере 1** он отсутствует в силу несвязности графа. Рассмотрим **пример 2**. Цикл, содержащий вершины A и B, приводит вновь в одну из этих вершин, так как каждая из вершин C, D, E смежна только с A и B. Таким образом, гамильтонов цикл в этом графе отсутствует.

Во многих прикладных задачах используются графы, называемые деревьями. Дерево — это связный граф без циклов.Деревьями удобно представлять иерархические структуры, т. е. множества объектов, из корых одни находятся в подчинении относительно других. Всем известны генеалогические деревья, описывающие родословные семей в истории, происхождение организмов и видов в биологии, структуры данных в информатике и многое другое. Вот один из примеров дерева.

[6]Уильям Гамильтон (1805–1865) — ирландский математик. Задачу о таком цикле в графе с 20 вершинами он использовал в 1859 г. как основу для игрушки-головоломки, получив патент и наладив (хотя и без коммерческого успеха) ее производство.

Пример 4.



Дерево обладает замечательными свойствами. Укажем некоторые из них.

Теорема 3. *Если G — дерево, имеющее n вершин и m ребер, то*

1) $m = n - 1$;

2) *любые две различные вершины соединены единственным маршрутом без повторений входящих в него вершин и ребер;*

3) *при удаление любого ребра образуется ровно две компоненты связности:*

4) *при добавлении ребра, соединяющего любые две не смежные прежде вершины, образуется ровно один цикл.*

Эти свойства легко видеть на диаграмме из **примера 4**.

Раскраской графа с вершинами $v_1, \ldots, v_n$ называется набор *цветов* — натуральных чисел $c_1, \ldots c_n$, приписанных вершинам так, что любые две смежные вершины v_i и v_j имеют различные цвета $c_i \neq c_j$. Минимальное число цветов, достаточное для раскраски графа G, называется его *хроматическим числом* $\chi(G)$.

Граф называется *полным*, если он содержит n вершин и все $n(n-1)/2$ ребер, соединяющих все пары вершин. Каждый внедиагональный элемент матрицы смежности полного графа равен 1. Полный граф, имеющий n вершин, обозначается K_n.

Теорема 4 (свойства хроматического числа).

1. *Если граф G содержит ровно n вершин, то $\chi(G) \leq n$.*
2. *Если граф G содержит подграф G_1, то $\chi(G) \geq \chi(G_1)$.*
3. $\chi(K_p) = p$.
4. *Если граф G содержит подграф K_p, то $\chi(G) \geq p$.*
5. *Если $n \geq 3$ и граф C_n представляет собой n-угольник (цикл из n вершин и*

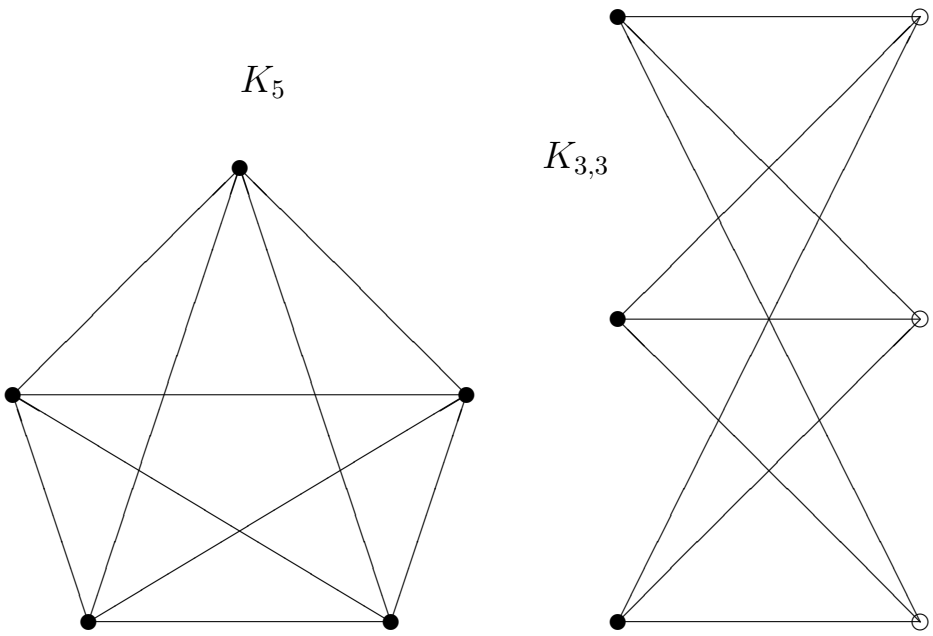
n ребер, при этом $C_3 = K_3$), то

$$\chi(C_n) = \begin{cases} 2, & \text{если } n \text{ четно,} \\ 3, & \text{если } n \text{ нечетно.} \end{cases}$$

6. *Если граф G — дерево, то $\chi(G) = 2$.*

7. *Если граф G планарный, т. е. может быть изображен диаграммой на плоскости, в которой ребра пересекаются только в вершинах, то $\chi(G) \leq 4$ (теорема о 4 красках).*

Простейшими непланарными графами являются K_5 и $K_{3,3}$.



В силу свойства 3 имеем $\chi(K_5) = 5$. А для второго графа, как нетрудно проверить, $\chi(K_{3,3}) = 2$.

В **примере 1** граф G содержит треугольник, поэтому $\chi(G) \geq 3$. С другой стороны, можно построить раскраску в 3 цвета, например,

$$c(v_3) = c(v_4) = c(v_6) = c(v_7) = 1,\ c(v_1) = c(v_5) = 2,\ c(v_2)3,$$

поэтому $\chi(G) \leq 3$. Таким образом, $\chi(G) = 3$.

Графы из **примеров 2 и 3** имеют хроматические числа 2 и 3 соответственно. Дерево из **примера 4** имеет в силу свойства 6 хроматическое число 2, на диаграмме представлена его раскраска в 2 цвета (темные и светлые кружки).

Задание для свмостоятельного решения

Постройте матрицы смежности и инциденций графа.

Постройте эйлеров и гамильтонов циклы или докажите, что соответствующий цикл не существует.

Найдите хроматическое число и оптимальную раскраску вершин графа.

Все графы имеют множество вершин $\{1, 2, 3, 4, 5, 6\}$. Ребра определяются в варианте задания. Для краткости они указываются без скобок и запятых.

1. **Ребра 12, 14, 23, 24, 35, 36, 45, 56.**
2. **Ребра 12, 14, 16, 23, 25, 26, 36, 45.**
3. **Ребра 12, 14, 24, 25, 35, 36, 45, 56.**
4. **Ребра 12, 14, 23, 24, 25, 35, 36, 45.**
5. **Ребра 12, 14, 15, 23, 26, 35, 45, 56.**
6. **Ребра 12, 14, 23, 24, 25, 35, 36, 56.**
7. **Ребра 12, 14, 23, 24, 26, 36, 45, 56.**
8. **Ребра 12, 14, 15, 25, 34, 36, 45, 56.**
9. **Ребра 12, 13, 14, 24, 25, 26, 36, 45.**
10. **Ребра 12, 13, 14, 23, 24, 36, 45, 56.**
11. **Ребра 12, 14, 16, 23, 25, 35, 45, 46.**
12. **Ребра 12, 13, 14, 23, 25, 45, 46, 56.**
13. **Ребра 12, 14, 25, 26, 35, 36, 45, 56.**
14. **Ребра 12, 14, 15, 23, 26, 35, 36, 45.**
15. **Ребра 12, 14, 23, 24, 25, 26, 35, 45.**
16. **Ребра 12, 13, 15, 16, 23, 34, 36, 56.**
17. **Ребра 12, 14, 23, 24, 34, 35, 36, 56.**
18. **Ребра 13, 14, 15, 23, 25, 36, 46, 56.**
19. **Ребра 12, 14, 15, 23, 25, 26, 35, 45.**

8 Алгебра вычетов по модулю m

Пусть m — натуральное число, $m \geq 2$. На множестве $\mathbb{Z}$ целых чисел определим двухместные операции $+,\ -,\ \cdot \pmod m$ *сложения, вычитания и умножения по модулю* m как функции $\mathbb{Z} \to \{0, 1, \ldots, m-1\}$.

Результатом операции $x+y,\ x-y,\ x \cdot y \pmod m$ является остаток от деления обычной суммы (соответственно разности, произведения) целых чисел x, y на m. Например, $6+11 = 2 \pmod 5$, $9-20 = 1 \pmod 6$, $3 \cdot 12 = 4 \pmod 8$, $2^3 = 2 \cdot 2 \cdot 2 = 1 \pmod 7$. Числа $0, 1, \ldots, m-1$ называются *наименьшими неотрицательными вычетами по модулю* m. Множество $\{0, 1, \ldots, m-1\}$ с операциями $+, \cdot \pmod m$ называется *алгеброй вычетов по модулю* m и обозначается как $\mathbb{Z}_m$:

$$\mathbb{Z}_m = (\{0, 1, \ldots, m-1\};\ +,\ \cdot \pmod m).$$

Операции $+, \cdot \pmod m$ достаточно задать только на множестве $\{0, 1, \ldots, m-1\}$. Это можно сделать, указывая результаты операций в двух таблицах размера $m \times m$, например,

$+ \pmod 2$

y \ x	0	1
0	0	1
1	1	0

$\cdot \pmod 2$

y \ x	0	1
0	0	0
1	0	1

(часто $x+y \pmod 2$ записывют как $x \oplus y$),

$+ \pmod 3$

y \ x	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot \pmod 3$

y \ x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$+ \pmod 4$

y \ x	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot \pmod 4$

y \ x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

В алгебре важнейшей задачаей является решение уравнений. Рассмотрим простейшее уравнение

$$ax = b \pmod m \tag{1}$$

в алгебре вычетов.

Теорема 1 (о решении уравнения первой степени в алгебре вычетов). *Пусть* $d = НОД(a, m)$ *(наибольший общий делитель), тогда справедливо следующее.*

1. *Если число* b *не делится на* d*, то уравнение* (1) *не имеет решения.*

2. *Если* b *кратно* d*, то уравнение* (1) *имеет в множестве* $\{0, 1, \ldots, m-1\}$ *ровно* d *различных решений. Если* x_0 *— решение, то остальные* $d-1$ *решений есть*

$$x_k = x_0 + k(m/d) \pmod{m}, \quad k = 1, \ldots, d-1.$$

Пример 1. Уравнение $12x = 45 \pmod{32}$ не имеет решений, так как $НОД(12, 32) = 4$, а 45 нечетно.

Пример 2. Рассмотрим уравнение

$$20x = 44 \pmod{108}. \tag{2}$$

Имеем $НОД(20, 108) = 4$, 44 кратно 4. Разделим обе части уравнения (2) и модуль на 4, получим более простое уравнение

$$5x = 11 \pmod{27}. \tag{3}$$

Для него $НОД(5, 27) = 1$, поэтому уравнение (3) имеет ровно одно решение $x_0 \in \{0, 1, \ldots, 26\}$. Нетрудно проверить, что $x_0 = 13$. (К сожалению, найти решение можно только перебором различных элементов конечного множества вычетов, хотя во многих случаях перебор не полный.) Тогда остальные решения уравнения (2) в множестве $\{0, 1, \ldots, 107\}$ есть

$$x_1 = 13 + 27 = 40, \; x_2 = 13 + 2 \cdot 27 = 67, \; x_3 = 12 + 3 \cdot 27 = 94.$$

Ответ: $x = 13, 40, 67, 94$.

Поясним, как можно сократить перебор при решении уравнения (3). Числа 11 и $11 + 27n$, $n \in \mathbb{Z}$, имеют одинаковый остаток от деления на 27, поэтому достаточно найти такое наименьшее натуральное n, чтобы число $11 + 27n$ делилось на 5. Для $n = 1$ число $11 + 27 = 38$ не делится на 5, для $n = 2$ получаем число $11 + 27 \cdot 2 = 65$, кратное 5. Таким образом, уравнение (3) равносильно уравнению $5x = 65 \pmod{27}$, откуда $x = x_0 = 65/5 = 13$.

К уравнению (1) сводятся и более сложные виды уравнений в алгебре вычетов.

Рассмотрим **систему линейных уравнений** по модулю m с квадратной матрицей.

Теорема 2. *Если квадратная система линейных уравнений*

$$\begin{cases} a_{11}x_1+ \ \cdots \ +a_{1n}x_n = b_1 \pmod m \\ \quad \vdots \qquad\qquad\qquad \vdots \\ a_{n1}x_1+ \ \cdots \ +a_{nn}x_n = b_n \pmod m \end{cases}$$

имеет определитель Δ *такой, что* $НОД(\Delta, m) = 1$*, то эта система уравнений имеет ровно одно решение* $(x_1, \ldots, x_n)$ *в множестве* $\{0, 1, \ldots, m-1\}^n$.

Пример 3. Решим систему порядка 2

$$\begin{cases} 3x - 2y = \ 1 \pmod m \\ 4x + 7y = \ 2 \pmod m \end{cases}$$

для модулей $m = 4, 9, 10, 16, 20, 30, 50, 100$. Определитель системы $3 \cdot 7 + 2 \cdot 4 = 29$ является простым числом, условие теоремы 2 выполняется, система имеет единственное решение для каждого модуля. Найдем его. Вычитая из второго уравнения первое, получаем

$$x + 9y = 1 \pmod m. \tag{4}$$

Умножим уравнение (4) на 3 и вычтем из результата первое уравнение исходной системы, получим

$$29y = 2, \quad x = 1 - 9y \pmod m.$$

Эти формулы однозначно определяют решение. Запишем решения (пары (x, y)) для каждого из рассматриваемых модулей в таблицу:

m	4	9	10	16	20	30	50	100
x	3	1	9	7	19	19	9	59
y	2	1	8	10	18	28	38	38

Квадратное уравнение

$$ax^2 + bx + c = 0 \pmod m$$

можно решить несколькими способами. Один из них — разложение на множители

$$ax^2 + bx + c = a(x - x_1)(x - x_2) \pmod m.$$

Другой способ состоит в применении теоремы Виета[7] и формул для корней

$$x_1 + x_2 = a^{-1}b, \quad x_1x_2 = a^{-1}c \pmod m.$$

Третий способ состоит в применении общей формулы для корней квадратного уравнения в арифметике по модулю m:

$$x = (2a)^{-1}(-b \pm \sqrt{b^2 - 4ac}\ ) \pmod m.$$

[7] Франсуа Виет (1540–1603) — французский математик, "отец алгебры"

Применять ее можно только при нечетном модуле m. В этом случае формулу можно упростить:

$$x = a^{-1}(-2^{-1}b \pm \sqrt{(2^{-1}b)^2 - ac}\,) \pmod m. \tag{5}$$

Пример 4. Решим уравнение $x^2 + x + 2 = 0 \pmod{11}$. Его можно записать в виде $x^2 - 10x + 24 = 0 \pmod{11}$ и разложить

$$x^2 + x + 2 = x^2 - 10x + 24 = (x-4)(x-6) \pmod{11},$$

откуда

$$x_1 = 4, \quad x_2 = 6. \tag{6}$$

Легко проверить выполнимость формул Виета: $4+6 = -1$, $4\times 6 = 2 \pmod{11}$. Если же применить третий способ и формулу (5), то

$$x = -2^{-1} \pm \sqrt{(2^{-1})^2 - 2} = -6 \pm \sqrt{6^2 - 2} = 5 \pm \sqrt{1} \pmod{11}.$$

Имеется два значения квадратного корня из 1 по модулю 11: $\sqrt{1} = 1 \pmod{11}$ и $\sqrt{1} = -1 = 10 \pmod{11}$, поэтому получаем те же решения (6).

9 Уравнения в целых числах

В дискретной математике применяются только целые числа, а разрешимость уравнений в целых числах определяется свойствами делимости. Например, очень простое уравнение $2x = 1$ не имеет целочисленных решений. В алгебре вычетов рассматриваются остатки от деления целых чисел на модуль, поэтому вычеты применяются при анализе и решении целочисленных уравнений. Рассмотрим одно из таких уравнений — линейное уравнение относительно n неизвестных

$$a_1x_1 + \cdots + a_nx_n = c.$$

Здесь коэффициенты $a_1, \ldots, a_n, c$ и неизвестные $x_1, \ldots, x_n$ — целые числа. Необходимым условием разрешимости такого уравнения является делимость коэффициента c на НОД$(a_1, \ldots, a_n)$. Интересно, что это же условие является и достаточным для разрешимости уравнения. Если $n = 1$, то решение, когда оно существует, единственно: $x_1 = c/a_1$. При $n \geq 2$ уравнение в случае разрешимости имеет бесконечное множество решений.

Рассмотрим уравнение с двумя неизвестными. Для упрощения обозначений запишем его в виде

$$ax + by = c, \quad a > 0, \quad b \neq 0. \tag{1}$$

Теорема. *Пусть* $d = НОД(a, |b|)$. *Тогда*:
если c *не кратно* d, *то уравнение* (1) *неразрешимо,*
если c *кратно* d, *то уравнение* (1) *имеет бесконечное множество решений, зависящих от целочисленного параметра* k*:*

$$x = x_0 + bk, \quad y = \frac{c - ax_0}{b} - ak, \quad k \in \mathbb{Z}, \tag{2}$$

где

$$ax_0 = c \pmod{|b|} \quad \textit{при } |b| > 1,$$

x_0 — *любое целое при* $b = \pm 1$.

Пример. Рассмотрим уравнение $3x - 7y = -24$. Имеем $a = 3$, $b = -7$, $d = \text{НОД}(3, 7) = 1$, уравнение разрешимо. Из уравнения в алгебре вычетов $3x_0 = -24 \pmod 7$ находим $x_0 = 6$. Тогда, согласно (2),

$$x = 6 - 7k, \quad y = \frac{-24 - 3 \cdot 6}{-7} - 3k = 6 - 3k, \quad k \in \mathbb{Z}.$$

Полезно бывает сделать **проверку**. Подставляя полученные выражения $x = x(k)$, $y = y(k)$ в левую часть исходного уравнения, видим, что слагаемые, содержащие k, уничтожаются и получается число -24.

Формулы (2) определяют *общее решение*. Из него заменой переменной k на конкретные целые числа получается бесконеское множество *частных решений*. В рассмотренном примере при $k = 0$ получаем частное решение $(x, y) = (6, 6)$, при $k = 1$ — частное решение $(x, y) = (-1, 3)$ и так далее.

Задача (последняя) для самостоятельного решения.
Решите следующее уравнение в целых числах.

1. $2x - 11y = 5$.
2. $4x + 7y = -20$.
3. $9x - 5y = 10$.
4. $15x - 4y = -2$.
5. $12x + 5y = 6$.
6. $3x + 16y = 5$.
7. $14x - 9y = -3$.
8. $5x + 16y = 8$.
9. $7x + 11y = 9$.
10. $11x - 3y = -20$.
11. $7x + 12y = -6$.
12 $8x - 17y = 4$.
13. $16x - 7y = -5$.
14. $12x + 5y = 10$.
15. $9x - 7y = -30$.
16. $11x + 8y = 6$.
17. $5x - 14y = 3$.
18. $4x + 17y = -6$.
19. $9x - 11y = 8$.
20. $9x + 13y = -7$.

Решения всех задач присылайте по адресу MeshchaninovDG@mpei.ru

10 Числа Стирлинга 2-го рода и числа Белла

Количество разбиений n-множества на k непустых подмножеств обозначается как $S_{n,k}$. Значения $S_{n,k}$, $n, k \geq 0$, называются *числами Стирлинга 2-го рода.*

Например, $S_{3,2} = 3$, так как имеется ровно 3 разбиения множества $\{1, 2, 3\}$ на 2 подмножества, одно из которых содержит ровно один элемент, а второе — два: $1|23,\ 2|13,\ 3|12$.

Укажем **простейшие свойства** этих чисел.

Если $n \geq 1$, *то* $S_{n,1} = S_{n,n} = 1$, $S_{n,0} = 0$.

Для числа $S_{0,0}$, не имеющего содержательного смысла, примем формальное соглашение $S_{0,0} = 1$.

Теорема 1. *Для чисел* $S_{n,k}$ *справедлива следующая рекуррентная формула*:

$$S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}.$$

Доказательство. Рассмотрим универсальное множество $U = \{e_1, \ldots, e_{n-1}, e_n\}$. Все его разбиения на k непустых подмножеств разделим на две группы:

содержащие одноэлементное подмножество $\{e_n\}$, количество таких разбиений равно числу $S_{n-1,k-1}$ разбиений $(n-1)$ подмножества $\{e_1, \ldots, e_{n-1}\}$ на $k-1$ непустых подмножеств;

не содержащие подмножества $\{e_n\}$, при этом элемент e_n может оказаться в любом из k непустых подмножеств $(n-1)$-множества $\{e_1, \ldots e_{n-1}\}$, количество таких разбиений равно $kS_{n-1,k}$.

Остается применить правило суммы. □

Например,

$$S_{4,3} = S_{3,2} + 3S_{3,3} = 3 + 3 \cdot 1 = 6, \qquad S_{5,4} = S_{4,3} + 4S_{4,4} = 6 + 4 \cdot 1 = 10.$$

Эти свойства позволяют заполнить конечное множество первых строк бесконечной таблицы для чисел $S_{n,k}$, аналогичной треугольнику Паскаля для биномиальных коэффициентов:

n / k	0	1	2	3	4	5
0	1					
1	0	1				
2	0	1	1			
3	0	1	3	1		
4	0	1	7	6	1	
5	0	1	15	25	10	1

Числа Стирлинга 2-го рода применяются, в частности при решении следующей задачи.

Пример. Имеется n различных (по внешнему виду пирожков) и k тарелок. Каждая тарелка достаточно большая и может вместить все n пирожков. Сколькими способами пирожки можно разложить на тарелки так, чтобы пустых тарелок не было? Ответ: $k!S_{n,k}$.

Числом Белла B_n называется количество всех разбиений n-множества на непустые подмножества/

Следствие. *Справедливы равенства*

$$B_0 = B_1 = 1, \qquad B_n = \sum_{k=0}^{n} S_{n,k}.$$

Теорема 2. *Для чисел Белла справедлива следующая рекуррентная формула*:

$$B_{n+1} = \sum_{k=0}^{n} C_n^k B_k.$$

Доказательство. Рассмотрим универсальное $(n+1)$-множество $U = \{e_1, \ldots, e_n, e_{n+1}\}$. Фиксируем целое k, $0 \le k \le n$. Для каждого из C_n^k подмножеств $A \subseteq \{e_1, \ldots, e_n\}$, состоящих из k элементов, имеется ровно B_k разбиений множества A на непустые подмножества (назовем их *блоками*). Если элемент e_{n+1} занести в любой из этих блоков, то получим разбиение множества U. $\square$

Укажем первые члены последовательности чисел Белла:

n	0	1	2	3	4	5	6	...
B_n	1	1	2	5	15	52	203	...

В частности, все $B_3 = 5$ разбиений множества $\{1, 2, 3\}$ есть

$$1|2|3, \quad 1|23, \quad 2|13, \quad 3|12, \quad 123.$$