ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

конспект лекции (часть 1)

А.С. Джумадильдаев

27 февраля 2005 г.

Оглавление

Книжка содержит конспект лекции, прочитанные в Казахско-Турецком и в Казахско-Британском университетах по курсу "Дискретная математика" за первые 7 недель. В лекциях затрагиваются элементы теории множеств, комбинаторики и теории чисел. В части 2 будут приведены лекции за 8 – 15 недель. В ней будут обсуждены следующие темы:

- Алгебраические структуры
- Логика высказывании и булевы функции
- Элементы теории графов

Автор будет признателен всем за замечания и комментарии об опечатках и ошибках, как в математическом так и в грамматическом смыслах.

Глава 1

Множества

1.1 Множества, подмножества и элементы

Множество состоит из элементов. Элементы должны быть различимы. Это означает, что для любых двух предметов, входящих в данное множество, мы должны иметь возможность сказать различны они или одинаковы. Элементы должны быть определенны. Условие определенности означает, что если дано какое-то множество и некоторый предмет, то можно сказать является ли данный предмет элементом рассматриваемого множества или нет.

Запись $x \in M$ означает, что элемент x принадлежит множеству M, $x \notin M$ – x не принадлежит M. Множество можно задать двумя способами: перечислением или описанием.

Если M состоит из элементов $x_1, x_2, \ldots$, то пишут

$$M = \{x_1, x_2, \ldots\}$$

Если M состоит из элементов x таких, что выполнено некоторое свойство $P(x)$, то пишут

$$M = \{x \mid P(x)\}.$$

Количество элементов множества называется порядком. Порядок множества A обозначается так: $|A|$.

Порядок может быть конечным или бесконечным. Например, $|A|$ конечен, более точно $|A| = 42$, если A – множество букв казахского алфавита. Пример бесконечного множества – $\mathbf{N}$.

Пример.

- $\mathbf{N}$ – множество натуральных чисел $\{1, 2, 3, \ldots\}$
- $\mathbf{Z}$ – множество целых чисел $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- $\mathbf{Z}^+$ – множество целых неотрицательных чисел $\{0, 1, 2, \ldots\}$
- $\mathbf{Q}$ – множество рациональных чисел $\{p/q : p, q \in \mathbf{Z}, q \neq 0\}$
- $\mathbf{R}$ – множество действительных чисел

- $\mathbf{C}$ – множество комплексных чисел, т.е., множество чисел вида $a + bi$, где $a, b \in \mathbf{R}$.

Пример. Множество "неделя" можно задать описанием: "неделя" состоит из дней недели. Все знают что такое дни недели и это есть корректное определение множества "неделя". Это же множество можно задать перечислением всех его элементом:

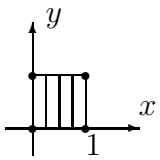
"неделя"={ понедельник, вторник, среда четверг, пятница, суббота, воскресенье}.

Пример. Множество "Граждане Казахстана" проще задать описанием. Есть простой способ определить гражданство: человек предъявляет удостоверение личности или паспорт. Задать множество "Граждане Казахстана" перечислением затруднительно чисто в техническом плане.

Не следует искать глубокий смысл в различиях способов задания множеств. Эти различия достаточно условны. Главное – должна быть эффективная процедура, которая позволяла бы вам определить лежит ли рассматриваемый элемент в вашем множестве или нет.

Пример. Множество умных людей. Является ли это множеством в математическом смысле ? Нет, поскольку нет формальной процедуры, которая позволила бы вам определить является ли интересующий вас человек умным или нет.

Пример. Единичный квадрат можно задать рисунком на координатной плоскости



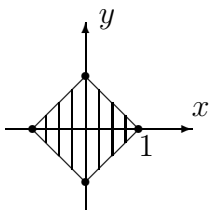
или в виде множества решении неравенств

$$\{(x, y) \in \mathbf{R}^2 |\ 0 \leq x \leq 1,\ 0 \leq y \leq 1\},$$

или, еще проще, в виде решении неравенств

$$|x - 1/2| \leq 1/2, \quad |y - 1/2| \leq 1/2.$$

Пример. Повернутый на $\pi/4$ квадрат со стороной $\sqrt{2}$ можно задать в виде картинки



в виде множества решении неравенств

$$\begin{array}{lll} x + y & \leq 1, & \text{если} \quad 0 \leq x \leq 1, 0 \leq y \leq 1 \\ x - y & \geq -1, & \text{если} \quad -1 \leq x \leq 0, 0 \leq y \leq 1 \\ x + y & \geq -1, & \text{если} \quad -1 \leq x \leq 0, -1 \leq y \leq 1 \\ x - y & \leq 1, & \text{если} \quad 0 \leq x \leq 1, -1 \leq y \leq 0, \end{array} \ '$$

или проще, неравенства

$$|x| + |y| \leq 1.$$

B – *подмножество* множества A, если $\forall x \in B \Rightarrow x \in A$.

Различие между $\in$ и $\subset$. Первый относится к элементам, второй к подмножествам. Например, $1 \in \mathbf{N}$, но $\{1\} \subset \mathbf{N}$. Итак, если есть элемент x , то из него можно построить одноэлементное множество $\{x\}$, взяв его в фигурную скобку.

1.2 Парадокс Рассела

Пример. В полку один из солдат, который умеет брить назначаен парикмахером. Генерал издал приказ: парикмахер должен брить тех и только тех, которые не бреются сами. Сможет ли парикмахер брить самого себя ?

Пусть A – множество солдат, которые не бреются сами. Тогда $\bar{A}$ – множество солдат, которые бреются сами. Допустим, что парикмахера зовут Билл. Вопрос состоит в том, что

$$\text{Билл } \in A \quad \text{или} \quad \text{Билл } \in \bar{A}.$$

Покажем, что на этот вопрос нет непротиворечивого ответа. В этом и состоит парадокс. Это означает, что A нельзя рассматривать как множество.

Пусть Билл $\in A$. Тогда Билл сам себя не бреет. Значит, согласно приказу генерала его должен брить парикмахер (он же Билл). Иными словами, парикмахер бреет самого себя. Противоречие: Билл $\in \bar{A}$.

Рассмотрим теперь случай Билл $\in \bar{A}$. Тогда Билл сам себя бреет. Значит, согласно приказу генерала Билла парикмахер брить не должен. Поскольку Билл и парикмахер оно и то же лицо, это означает, что Билл не бреет самого себя. Противоречие: Билл $\in A$.

Имеется система аксиом теории множеств, которая носит имена Цермело- Френкеля. Она запрещает возникновение такого рода парадоксов. Мы не можем углубляться в аксиоматические дебри теории множеств. К счастью, множества рассматриваемые на нашем курсе (конечные множества, числовые множества, и т.д.) лишены такого рода трудностей.

1.3 Булеан. Диаграммы Венна

Пустое множество обозначается так: $\emptyset$. Это множество, в котором нет никаких элементов. Пустое множество является подмножеством любого множества.

Универсальное множество определяется из контекста. Это множество, которое содержит все рассматриваемые множества. Стандартное обозначение универсального множества, применяемого в этой работе – U.

Булеан множества – множество всех подмножеств множества

Диаграмма Венна – представление множества в виде геометрических фигур (обычно в виде кружка).

Равенство множеств. Множества A и B равны, обозначение: $A = B$, если $A \subseteq B$ и $B \subseteq A$.

Пример. Пусть $A = \{a, b, c\}$ и $B = \{c, b, a, c\}$. Тогда

$$A \subseteq B,$$

поскольку

$$a \in A \Rightarrow a \in B,$$
$$b \in A \Rightarrow b \in B,$$
$$c \in A \Rightarrow c \in B.$$

Обратно,

$$B \subseteq A,$$

поскольку

$$c \in B \Rightarrow c \in A,$$
$$b \in B \Rightarrow b \in A,$$
$$a \in B \Rightarrow a \in A,$$
$$c \in B \Rightarrow c \in A.$$

Следовательно,

$$A = B.$$

Этот пример показывает что, порядок перечисления или повторение элементов в множествах не имеют значения. Обычно стараются перечислять элементы в порядке возрастания или убывания относительно какого-то порядка и стараются по возможности не повторять одни и те же элементы несколько раз.

1.4 Тождества алгебры множеств

Операции на множествах удовлетворяют следующим тождествам

- $A \cup A = A, \quad A \cap A = A$ (идемпотентность)
- $A \cup B = B \cup A, \quad A \cap B = B \cap A$ (коммутативность)
- $(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C)$ (ассоциативность)
- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C), \quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (дистрибутивность)
- $A \cup \emptyset = A, \quad A \cap U = A,$
  $A \cup U = U, \quad A \cap \emptyset = \emptyset$ (нейтральность)
- $\bar{\bar{A}} = A$(инволютивность)
- $A \cup \bar{A} = U, \quad A \cap \bar{A} = \emptyset$
  $\bar{U} = \emptyset, \quad \bar{\emptyset} = U$ (дополнение)
- $\overline{(A \cup B)} = \bar{A} \cap \bar{B}, \quad \overline{(A \cap B)} = \bar{A} \cup \bar{B}$ (Де Морган)

Есть два способа доказательств такого рода тождеств. Первое – с помощью диаграмм Венна. Второе доказательство основано на формальном определении равенства. Чтобы установить $X = Y$ надо проверить, что

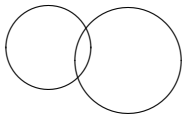
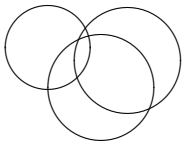
$$x \in X \Rightarrow x \in Y$$

и

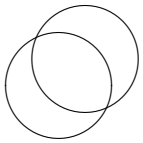
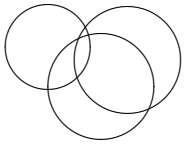
$$y \in Y \Rightarrow y \in X.$$

Проиллюстрируем оба способа доказательств на примере тождеств алгебр множеств.

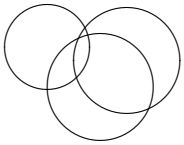
Докажем тождество ассоциативности по объединению с помощью диаграмм Венна. Имеем

$A \cup B =$  $(A \cup B) \cup C =$ 

С другой стороны,

$B \cup C =$  $A \cup (B \cup C) =$ 

Поэтому

$(A \cup B) \cup C =$  $= A \cup (B \cup C)$

Докажем вторым способом тождество Де Моргана

$$\overline{(A \cup B)} = \bar{A} \cap \bar{B}.$$

С одной стороны,

$$x \in \overline{(A \cup B)} \Rightarrow x \in U, x \notin (A \cup B) \Rightarrow x \in U, x \notin A, x \notin B \Rightarrow x \in \bar{A}, x \in \bar{B}.$$

Следовательно

$$\overline{(A \cup B)} \subseteq \bar{A} \cap \bar{B}$$

С другой стороны,

$$x \in \bar{A} \cap \bar{B} \Rightarrow x \in \bar{A}, x \in \bar{B} \Rightarrow x \in U, x \notin A, x \notin B \Rightarrow x \in U, x \notin A \cup B \Rightarrow x \in \overline{(A \cup B)}.$$

Следовательно

$$\bar{A} \cap \bar{B} \subseteq \overline{(A \cup B)}.$$

Тождество Де Моргана доказано полностью.

1.5 Задачи

1. Можно ли определить множество капель в стакане воды ?

2. Можно ли определить множество множеств не содержащих себя в качестве элемента ?

3. Является ли множество круглых квадратов подмножеством множества **N** ?

4. Какие из следующих утверждении верно ? В случае отрицательного ответа привести контрпример.

- $\{5,6\} \in \{\{1,2,3,5,6\},\{1,3\},3,5,6\}$
- $7 \in \{\{5,6,7,8\}\}$,
- $\{1\} \in \mathbf{N}$
- $1 \in \mathbf{N}$
- $\{a\} \subseteq \{\{a\}\}$
- $\{a\} \in \{\{a\}\}$

5. Какие из следующих утверждении верно ? В случае отрицательного ответа привести контрпример.

- Если $A \in B, B \in C$, то $A \in C$.
- Если $A \subseteq B, B \subseteq C$ то $A \subseteq C$
- Если $x \in A$, то $\{x\} \subseteq A$.
- Если $\{x\} \subseteq A$, то $x \in A$.

6. Какие из следующих множеств равны $\{a,b,c\},\{c,b,a,c\},\{b,c,b,a\},\{c,a,c,b\}$?

7. Равны ли множества
a)$\{\{1,2\}\}$ и $\{1,2\}$
b)$\{\{1,2\},\{2,3\}\}$ $\{1,2,3\}$

8. Заданы множества $\emptyset, A = \{1\}, B = \{1, 3\}, C = \{1, 5, 9\}, D = \{1, 2, 3, 4, 5\}, E = \{1, 3, 5, 7, 9\}, U = \{1, 2, \ldots, 9\}$. Какую из знаков $\subseteq$ или $\not\subseteq$ необходимо ставить между следующими парами: $\emptyset, A$; A, B; B, C; B, E; C, D; C, E; D, E; D, U.

9. Докажите, что из условия $A \cup B = A \cup C$ не следует, что $B = C$.

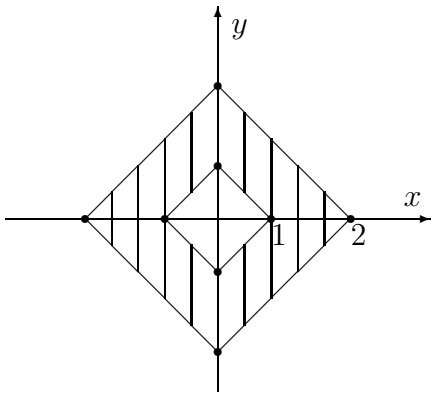
10. Пусть $U = \mathbf{N}, A = \{1, 2, 3, 4\}, B = \{3, 4, 5, 6, 7\}, C = \{6, 7, 8, 9\}$ E– множество четных натуральных чисел. Найти

- $\bar{A}, \bar{B}, \bar{C}$
- $A \setminus B, B \setminus C, C \setminus E$,
- $A \cup B, B \cap C, A \cap B$,
- $A \oplus B, A \oplus C, B \oplus C$.

11. Задайте следующие множества с помощью описания элементов

- $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- $\{2, 4, 6, 8, 10\}$
- $\{1, 4, 9, 16, 25, \ldots\}$
- $\{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\}$
- $\{-1, 1\}$

12. Задать следующее множество с помощью неравенств



13. Задайте следующие множества с помощью перечисления элементов

- $\{x \in \mathbf{Z} : 2x^2 - 3x + 1 = 0\}$
- $\{x \in \mathbf{R} : 2x^2 - 3x + 1 = 0\}$
- $\{x \in \mathbf{R} : (x - 1)(x^3 + 1) = 0\}$
- $\{x \in \mathbf{C} : (x - 1)(x^3 + 1) = 0\}$

14. Пусть $n\mathbf{Z} = \{na : a \in \mathbf{Z}\}$ – множество чисел кратных на n. Рассмотрим множества $2\mathbf{Z}, 3\mathbf{Z}, 5\mathbf{Z}, 6\mathbf{Z}$, множество целых чисел оканчивающихся на 0 и множество степеней 2. Какие из этих множеств являются подмножествами других ? Что является их общим надмножеством ?

15. Найти объединения и пересечения множеств $3\mathbf{Z} \cup 12\mathbf{Z}$ и $3\mathbf{Z} \cap 2\mathbf{Z}$, $3\mathbf{Z} \cap 12\mathbf{Z}$, $12\mathbf{Z} \cap 15\mathbf{Z}$.

16. Найдите булеан множества $\{1, 2, 3, 4\}$.

17. Докажите тождества алгебры множеств двумя методами (с помощью диаграмм Венна и с помощью исследования элементов в левых и правых частях равенств). Обратите внимание на дуальность тождеств.

18. С помощью тождеств алгебры множеств доказать, что

$$(A \cup B) \cap (A \cup \bar{B}) = A$$

$$(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Этот результат показывает, что симметрическую разность $A \oplus B$ можно определить двумя способами.

19. Пусть $A = \{a, b, c, d\}$. Найти класс подмножеств, которые содержат по три элемента. Найти класс подмножеств, которые содержат a и два других элемента. Сколько элементов имеют эти классы множеств и который из них является подклассом другого ?

20. Пусть $A = \{1, 2, \ldots, 9\}$. Какие из следующих совокупностей подмножеств задают разбиение множества A ?

- $[\{1, 3, 5\}, \{2, 6\}, \{4, 8, 9\}]$
- $[\{1, 3, 5\}, \{2, 4, 6, 8\}, \{5, 7, 9\}]$
- $[\{1, 3, 5\}, \{2, 4, 6, 8\}, \{7, 9\}]$

Глава 2

Отношения и функции

2.1 Декартово произведение и отношения

Декартово (или прямое) произведение множеств $A_1, A_2, \ldots, A_n$ определяется как множество упорядоченных последовательностей $\{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_2, a_2 \in A_2, \ldots, a_n \in A_n\}$. Обозначение: $A_1 \times A_2 \times \cdots A_n$ или $\prod_{i=1}^{n} A_i$ или, кратко, $\prod_i A_i$.

Пример. Пусть $A_1 = \{x, y\}, A_2 = \{p, q, r\}, A_3 = \{1, 2\}$. Тогда

$$A_1 \times A_2 \times A_3 = \{(x, p, 1), (x, p, 2), (x, q, 1), (x, q, 2),$$

$$(x, r, 1), (x, r, 2), (y, p, 1), (y, p, 2), (y, q, 1), (y, q, 2), (y, r, 1), (y, r, 2)\}.$$

Отношение. Для множеств A и B отношение определяется как подмножество $R \subset A \times B$. Если $(a, b) \in R$ то будем писать aRb. Если $(a, b) \notin R$ то будем писать $a \not R b$.

Универсальное отношение. $R = A \times A$

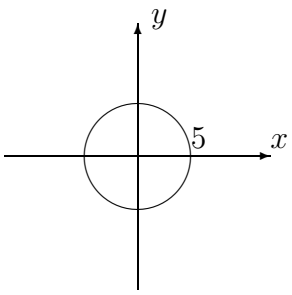
Пустое отношение. $R = \emptyset \subset A \times A$

Пример. Пусть $A = \{$яйцо, молоко, кукуруза$\}$ и $B = \{$корова, коза, курица$\}$. Определим отношение R из A в B по правилу aRb, если b производит a. Тогда

$$\text{яйцо} \quad \not R \quad \text{корова}$$

$$R = \{(\text{яйцо,курица}),(\text{молоко, корова}),(\text{молоко,коза})\}.$$

Пример. Определим отношение на множестве $\mathbf{R}$ по правилу xRy, если $x^2 + y^2 = 25$. Тогда R можно представить в виде окружности радиуса 5 на плоскости:



Пусть R – бинарное отношение из A в B.

Область определения,

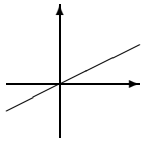
$$Dom(R) = \{a \mid (a,b) \in R, \text{ для некоторого } b \in B\}.$$

Область значении,

$$Im(R) = \{b \mid (a,b) \in R, \text{ для некоторого } a \in A\}.$$

Отношение на (конечных) множествах можно задать

- перечислением, например, $R = \{(a,b),(a,c),(b,d)\}$
- матрицей
$$(\lambda_{i,j}), \quad \lambda_{i,j} = \begin{cases} 1, & a_i R a_j \\ 0, & \text{в противоположном случае} \end{cases}$$
- описанием, например, в множестве людей aRb, если b– отец a.
- в виде графика функции, например, xRy, если $y = x/2$.



Типы отношении $R \subseteq A \times A$:

- R– *рефлексивно*, если aRa, для любого $a \in A$. Пример, "жить в одном городе".
- R– *антирефлексивно,* если $a \not R a$ для всех $a \in A$. Пример, "быть сыном".
- R– *симметрическо*, если $aRb \Rightarrow bRa$. Пример, "работать на одной фирме".
- R– *антисимметрично*, если $aRb, bRa \Rightarrow a = b$. Пример, "быть начальником".
- R– *транзитивно*, если $aRb, bRc \Rightarrow aRc$. Пример, "быть моложе".

2.2 Отношение эквивалентности

Эквивалентность. R – отношение эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Пример. Универсальное отношение является отношением эквивалентности.

Пример. Пусть $A \neq \emptyset$ и $a \in A$. Поскольку $(a,a) \notin \emptyset$, пустое отношение не является отношением рефлексивности. Поэтому пустое отношение не является отношением эквивалености.

Класс эквивалентности элемента $a \in A$ относительно отношения эквивалентности R определяется как подмножество элементов $b \in A$ находящихся в отношении R с a:

$$R(a) = \{b \mid (a,b) \in R\}.$$

Тогда

$$R(a) \cup R(b) \neq \emptyset \Rightarrow R(a) = R(b),$$
$$A = \cup_{a \in A} R(a).$$

(Докажите !)

Полная система классов эквивалентности. Назовем систему классов эквивалентности $R(a_1), R(a_2), \ldots,$ полной системой, если

- $R(a_1), R(a_2), \ldots,$ – различные классы эквивалентности,
- $A = \cup_{i \geq 1} R(a_i)$.

Элемент $b \in A$ называется *представителем* класса $R(a)$, если $b \in R(a)$, т.е., $(a, b) \in R$.

Фактор-множество. Для отношения эквивалентности R множество $\rho(A) = \{R(a_1), R(a_2), \ldots\}$, элементами которых являются полные системы классов эквивалентности, называется фактор-множеством. Вместо $\rho(A)$ часто используется обозначение: A/R.

Пример. Пусть $A = \mathbf{Z}$. Определим отношение $(a, b) \in R$, если $a - b$ делится на n. Обычно в таких случаях пишут $a \equiv b (mod\ n)$. Имеется n различных классов эквивалентности

$$R(0) = \{nk \mid k \in \mathbf{Z}\},$$
$$R(1) = \{1 + nk \mid k \in \mathbf{Z}\},$$
$$\vdots$$
$$R(n-1) = \{n - 1 + nk \mid k \in \mathbf{Z}\}.$$

Таким образом, фактор-множество состоит из n элементов. Обычно фактор-множество обозначается так: $\mathbf{Z}/n\mathbf{Z}$.

Разбиение множества A – представление множества A в виде объединения непересекающихся непустых подмножеств $A_i, i \in I$, где I некоторое множество индексов. Другими словами,

- $A = \cup_{i \in I} A_i$
- $A_i \cup A_j = \emptyset$ если $i \neq j$.
- $A_i \neq \emptyset$ для всех $i \in I$.

Теорема. Разбиение $\{A_i, i \in I\}$ множества A задает отношение эквивалентности

$$R = \{(a, b) \mid \exists i \in I \text{ такой, что } a, b \in A_i\}.$$

Обратно, пусть $R \subseteq A \times A$ отношение эквивалентности. Тогда полная система классов эквивалентности $\{R(a_1), R(a_2), \ldots\}$ задает разбиение множества A.

Пример. Пусть $A = \{1, 2, 3, 4, 5, 6\}$. Тогда $A = A_1 \cup A_2 \cup A_3$– разбиение, где $A_1 = \{1, 3\}, A_2 = \{2, 4, 6\}, A_3 = \{5\}$. Этому разбиению соответствует следующее отношение эквивалентности

$$R = \{(1,3), (3,1), (2,4), (4,2), (2,6), (6,2), (4,6), (6,4),$$

$$(1,1),(2,2),(3,3),(4,4),(5,5),(6,6)\}$$

Пример. Пусть $A=\{a,b,c,d,e,f\}$. Тогда

$$R=\{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),(a,b),(b,a),(c,e),(e,c),$$

$$(a,f),(f,a),(b,f),(f,b)\}$$

является отношением эквивалентности. Ему соответствует разбиение $A=A_1\cup A_2\cup A_3$, где $A_1=\{a,b,f\}, A_2=\{c,e\}, A_3=\{d\}$

Пример. Имеется всего 5 различных отношении эквивалентности на множестве из трех элементов $A=\{a,b,c\}$:

$$R_1=A\times A,$$

$$R_2=\{(a,a),(b,b),(c,c),(a,b),(b,a)\},$$
$$R_3=\{(a,a),(b,b),(c,c),(a,c),(c,a)\},$$
$$R_4=\{(a,a),(b,b),(c,c),(b,c),(c,b)\},$$
$$R_5=\{(a,a),(b,b),(c,c)\}.$$

Этим отношениям соответствуют разбиения

$$A=A_1,\quad A_1=\{a,b,c\},$$

$$A=A_1\cup A_2,\quad A_1=\{a,b\},A_2=\{c\},$$
$$A=A_1\cup A_2,\quad A_1=\{a,c\},A_2=\{b\},$$
$$A=A_1\cup A_2,\quad A_1=\{b,c\},A_2=\{a\},$$
$$A=A_1\cup A_2\cup A_3,\quad A_1=\{a\},A_2=\{b\},A_3=\{c\}.$$

Отношение толерантности – рефлексивное и симметрическое отношение. Всякое отношение эквивалентности является отношением толерантности.

Приведем примеры отношении толерантности.

Пример. Пусть $A=\mathbf{N}$ и aRb, если числа a и b имеют хотя бы одну общую цифру.

Пример. Пусть A – множество прямых двумерной плоскости $\mathbf{R}^2$ и aRb, если прямые a и b имеют точки пересечения.

Пример. Множество A состоит из четырехбуквенных русских слов – нарицательных существительных в именительном падеже. Определим отношение aRb на множестве A по правилу: aRb, если слова a и b отличаются не более чем на одну букву.

Как "превратить муху в слона" в терминах этого отношения толерантности ? Например, так:

Муха – мура – тура –тара – кара – каре – кафе – кафр – каюр – каюк – крюк – крок – срок – сток – стон – слон.

2.3 Отношение порядка

Отношение R задает отношение порядка, если оно рефлексивно, антисимметрично и транзитивно.

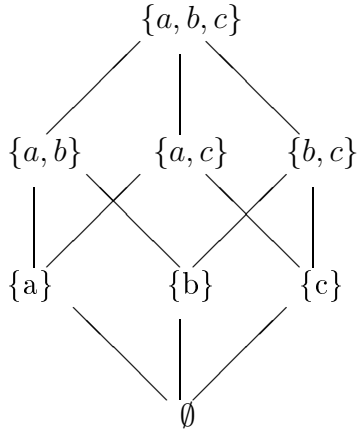
Пример. Отношение $a \prec b$ определенное по правилу $a|b$ задает порядок на множестве $\mathbf{N}$.

Частично упорядоченное множество – Множество с отношением порядка.

Пример. Булеан относительно включения $(P(A), \subseteq)$ - частично упорядочено.

Пусть $(A, \leq)$ частично упорядоченное множество. Говорят, что $x \in A$ покрывает $y \in A$, если $x \leq y$ и не существует такого элемента $z \in A$, что $x < y < z$. Диаграмма Хассе множества $(A, \leq)$: точки соответствуют элементам множества A и две вершины x и y соединены, если y покрывает x, причем x расположен ниже чем y.

Пример. Булеан $P(\{a, b, c\})$ и его диаграмма Хассе



Пример. Множество $(\mathbf{N}, \prec)$, где $a \prec b \Leftrightarrow a|b$ частично упорядочено.

Квазипорядок (или предпорядок) – рефлексивное и транзитивное отношение.

Пример. Множество $(\mathbf{Z}, \prec)$ относительно порядка $a \prec b \Leftrightarrow a|b$ квазиупорядочено. Это множество не является частично упорядоченным. Например, $-3 \prec 3$, $3 \prec -3$, но $-3 \neq 3$.

Линейный порядок. Порядок R на множестве A линеен, если для любых $a, b \in A$ имеет место aRb или bRa.

Линейно упорядоченное множество – Множество с отношением линейного порядка.

Пример. $(\mathbf{N}, <)$ линейно упорядочено относительно обычного порядка $<$.

2.4 Операции над отношениями

Поскольку отношения являются подмножествами, все операции над множествами допустимы над отношениями. Для $R_1, R_2 \subseteq A \times B$ естественными путями определяются новые отношения (объединенеие, пересечение, разность, симметрическая разность отношении) $R_1 \cup R_2, R_1 \cap R_2, R_1 \setminus R_2, R_1 \oplus R_2 \subseteq A \times B$.

Обратное отношение. Для $R \subseteq A \times B$ обратное отношение определяется так:

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

Имеется еще одна операция, которую нельзя получить из операции алгебры множеств. Эта операция – композиция отношении $R_1 \circ R_2$.

Композиция отношении. Пусть $R_1 \in A \times B, R_2 \subseteq B \times C$, Тогда отношение $R_1 \circ R_2 \subseteq A \times C$ определяется по правилу

$$R_1 \circ R_2 = \{(a,b) \mid \exists b \in B, (a,b) \in R_1, (b,c) \in R_2\}.$$

Теорема. Композиция отношении – ассоциативна.

Определим степени отношении $R \subseteq A \times A$ по правилу

$$R^1 = R, \quad R^n = R \circ R^{n-1}, \text{ если } n > 1.$$

Пример. Пусть A множество людей и отношение $R \in\subseteq A \times A$ определяется так: $(a,b) \in R$, если a – отец b. Тогда aR^2b означает, что a – дед a.

Замыкания отношении. Пусть $R \subseteq A \times A$. Определим

$$R^{ref} = R \cup \{(a,a) | a \in A\} \quad \text{рефлексивное замыкание,}$$

$$R^{sym} = R \cup R^{-1} \quad \text{симметрическое замыкание,}$$

$$R^* = \cup_{i=1}^{\infty} R^i (\text{транзитивное замыкание}).$$

Пример. Если $A = \mathbf{R}$, $R = \{(a,b) | a < b\}$, то $R^{ref} = \{(a,b) | a \leq b\}$.

Пример. Если $A = \mathbf{R}$, $R = \{(a,b) | a < b\}$, то $R^{sym} = \{(a,b) | a \neq b\}$

Заметим что

$$R^* = \{(a,b) \mid \exists k \in \mathbf{N},\ (a,c_1),(c_1,c_2),\ldots,(c_k,b) \in R\}.$$

Теорема. Если $|A| = n$, то $R^* = \cup_{i=1}^{n} R^i$.

Доказательство. Допустим, что существует последовательность элементов $x_0, x_1, \ldots, x_m \in A$ такой, что $(x_0,x_1),(x_1,x_2),\ldots,(x_{m-1},x_m) \in R$, и $x_0 = a, x_m = b$. Докажем, что для любых $a, b \in A$ длину последовательности m можно подобрать таким, что $m \leq n$, если $a = b$ и $m < m$, если $a \neq b$.

Рассмотрим случай $a = b$. Допустим, что $m \geq n+1$. Тогда по принципу Дирихле среди m элементов $x_1, x_2, \ldots, x_m \in \{a_1, \ldots, a_n\}$ существуют по крайней мере 2 одинаковых. Пусть например, $x_i = x_j, 0 < i < j \leq m$. Тогда имеется последовательность $x_0 = a, x_1, x_2, \ldots, x_i, x_{j+1}, \ldots, x_m = a \in A$ длины $< m$ такой, что $(a,x_1),\ldots,(x_{i-1},x_i),(x_j,x_{j+1}),\ldots,(x_{m-1},a) \in R$. Повторяя многократно эту процедуру многократно можно построить последовательность длины $m \leq n$ требуемыми свойствами.

Случай $a \neq b$ оставляется в качестве упражнения.

Пример. Если $A = \{x,y,z\}$ и $R = \{(x,y),(y,z),(z,z)\}$, то

$$R^{(2)} = \{(x,z),(y,z),(z,z)\},$$

$$R^{(3)} = \{(x,z),(y,z),(z,z)\} = R^{(2)}.$$

Поэтому

$$R^* = R \cup R^{(2)} \cup R^{(3)} = \{(x,y),(y,z),(z,z),(x,z)\}.$$

2.5 Функции

Отношение $f \subseteq A \times B$ называется функцией, если

- $Dom\, f = A$
- $Im\, f \subseteq B$
- $(a, b_1) \in f, (a, b_2) \in f \Rightarrow b_1 = b_2$.

Таким образом, функции – частный случай отношении. Чтобы задать функцию нужно задать три вещи: правило f, область определения A и область значении B, при этом одному значению $x \in A$ соответствует ровно одно значение $y \in B$. Обычно пишут $y = f(x)$. Другие обозначения для функции: $f : A \to B, \quad A \xrightarrow{f} B, f : x \mapsto f(x)$.

Инъективность. Функция $f : A \to B$ называется инъективной, если $f(a) = f(a_1) \Rightarrow a = a_1$. Иногда вместо термина "инъективный" используются другие слова: мономорфизм, вложение или отображение "в".

Сюръективность. Функция $f : A \to B$ называется сюръективной, если для любого $b \in B$ существует $a \in A$ такое, что $b = f(a)$. Иногда вместо термина "сюръективный" используются другие слова: эпиморфизм, наложение или отображение "на".

Биекция. Функция $f : A \to B$ биективна (взаимно однозначна), если f инъективна и сюръективна.

Пример. $f : \mathbf{R} \to \mathbf{R}, \quad x \mapsto x^2$, – не инъективна и не сюръективна.
Пример. $f : \mathbf{R} \to \mathbf{R}^+, \quad x \mapsto x^2$, – сюръективна, но не инъективна.
Пример. $f : \mathbf{Z} \to \mathbf{Z}, \quad x \mapsto 2x$, – инъективна, но не сюръективна.
Пример. $f : \mathbf{R} \to \mathbf{R}, \quad x \mapsto 2x$ – биекция.

Композиция функции $f : A \to B, g : B \to C$ определяется как функция

$$g \circ f : A \to C, \quad (g \circ f)(a) = g(f(a)).$$

Пример. Пусть $f : \mathbf{R} \to \mathbf{R},\ x \mapsto 2x + 1$ и $g : \mathbf{R} \to \mathbf{R},\ x \mapsto x^2 + 2$. Тогда

$$g \circ f : \mathbf{R} \to \mathbf{R},\ x \mapsto 4x^2 + 4x + 3,$$

$$f \circ g : \mathbf{R} \to \mathbf{R},\ x \mapsto 2x^2 + 5.$$

Этот пример показывает что операция композиции на множестве функции не является коммутативной: $f \circ g \neq g \circ f$.

Теорема. Композиция функции ассоциативна. Для любых трех функции $A \xrightarrow{f} B, B \xrightarrow{g} C, C \xrightarrow{h} D$ выполнено равенство

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Доказательство.

$$(h \circ (g \circ f))(a) = h(g \circ f)(a)) = h(g(f(a))) = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a).$$

Обозначение для множества функции из A в B: $\mathcal{F}(A, B)$ или B^A.

Операции. Пусть $A^n = \underbrace{A \times \cdots \times A}_{n}$. Функция $f : A^n \to A$ называется n-местной операцией на .

При малых n имеются специальные названия: 1-местная операция – унарна, 2-местная операция – бинарна. Бинарную операцию часто называют умножением. Умножение элементов $f(a, b)$ иногда обозначается так: $a \times b$, $a + b$, $a \cdot b$, $a \circ b$ или $a \star b$ и т.д.

Пример. Всякую функцию $f : A \to A$ можно рассматривать как унарную операцию.

Пример. Пусть $A = \mathcal{F}(X, X)$. Композицию функции из X в X можно рассматривать как операцию умножения в множестве функции $\mathcal{F}(X, X)$.

Пример. Пусть $A = Mat_n$ – множество квадратных матриц. Умножение матриц задает бинарную операцию на множестве Mat_n.

Операции композиция функции и умножение матриц – ассоциативны, но не коммутативны:

$$h \circ (g \circ f) = (h \circ g) \circ f,$$

для любых функции или матриц f, g, h но

$$f \circ g \neq g \circ f$$

для некоторых функции (матриц) f, g.

Пример. Операция вычитания $\mathbf{Z}$ неассоциативна:

$$(a - b) - c \neq a - (b - c), \text{ например, } 5 - (3 - 2) = 4 \neq 0 = (5 - 3) - 2.$$

Пример. Операции объединения и пересечения множеств ассоциативны.

Пример. Операция разности множеств неассоциативна:

$$A \setminus (B \setminus C) \neq (A \setminus B) \setminus C.$$

Например для $A = \{a, b, c\}, B = \{b, c\}, C = \{c\}$, имеем

$$A \setminus B = \{a\}, B \setminus C = \{b\} \Rightarrow (A \setminus B) \setminus C = \{a\} \neq A \setminus (B \setminus C) = \{a, c\}.$$

Пример. Пусть $A = \mathbf{R}[x]$ – множество полиномов и $\partial : \mathbf{R}[x] \to \mathbf{R}[x]$, $f(x) \mapsto \frac{\partial f(x)}{\partial x}$ – дифференцирование. Например, $\partial(x^2 - 3x) = 5x - 3$. Для $a, b \in A$ определим $a \circ b$ по правилу $a \circ b = a\partial(b)$. Тогда

$$a \circ (b \circ c) \neq (a \circ b) \circ c,$$

для некоторых $a, b, c \in A$. Например,

$$1 \circ (1 \circ x^2) = 2, \quad (1 \circ 1) \circ x^2 = 0,$$

и

$$1 \circ (1 \circ x^2) \neq (1 \circ 1) \circ x^2.$$

На самом деле имеет место тождество:

$$a \circ (b \circ c) - (a \circ b) \circ c = b \circ (a \circ c) - (b \circ a) \circ c,$$

для всех $a, b, c \in A$. (Докажите !)

2.6 Задачи

1. Пусть $A = \{1, 2\}, B = \{a, b\}$. Найти $A \times B$; $B \times A$; $B \times B$.

2. Пусть $A = \{1, 2\}, B = \{a, b, c\}, C = \{5, 6\}$. Найти $A \times B \times C$.

3. Пусть $A = \{0, 1\}, B = \{x, y, z\}$, $C = \{x, w\}$. Найти $(A \times B) \cap (A \times C)$ и $B \cap C$.

4. Доказать, что $(A \times B) \cap (A \times C) = A \times (B \cap C)$.

5. Сколько отношении существуют из $A = \{x, y, z\}$ к $B = \{0, 1\}$?
Ответ: Существует 6 элементов $A \times B$. Следовательно $2^6 = 64$ подмножеств множества $A \times B$. Значит существуют 64 соотношении из A к B.

6. Сколько различных отношении эквивалентности существуют на множестве из n элементов, где $a)n = 1, b)n = 2, c)n = 3, d)n = 4$. ?

7. Сколько различных отношении существуют на множестве из n элементов ?

8. Сколько существуют инъективных отображении из множества n элементов в множество из m элементов, если $(n, m) = (4, 3), (3, 3), (3, 4)$?

9. Сколько существуют сюръективных отображении из множества n элементов на множество из m элементов, если $(n, m) = (4, 3), (3, 3), (3, 4)$?

10. Сколько существуют рефлексивных отношении на множестве из n элементов ?

11. Сколько существуют транзитивных отношении на множестве из n элементов для $a)n = 1$; $b)n = 2$; $c)n = 3$?

12. Пусть R, S рефлексивные отношения. Доказать или опровергнуть следующие утверждения.

- $R \cup S$ рефлексивное
- $R \cap S$ рефлексивное
- $R \oplus S$ не рефлексивное
- $R \setminus S$ не рефелексивное
- $R \circ S$ рефлексивное

13. Пусть R – рефлексивное и транзитивное отношение. Доказать, что $R^n = R$ для любого $n \in \mathbf{N}$.

14. Пусть R – рефлексивное отношение. Доказать, что R^n рефлексивно для любого $n \in \mathbf{N}$.

15. Пусть R – симметрическое отношение. Доказать, что отношение R^n симметрично для любого $n \in \mathbf{N}$.

16. Доказать, что R рефлексивно тогда и только тогда, когда R^{-1} рефлексивно.

17. Доказать, что отношение R симметрично тогда и только тогда, когда $R = R^{-1}$.

18. Пусть R не рефлексивно. Всегда ли отношение R^2 не рефлексивно?

19. Пусть A – множество студентов и B – множество книг в библиотеке. Рассмотрим отношения R_1 и R_2 из A в B, определенные следующим образом: aR_1b, если студенту a необходимо прочитать книгу b и aR_2b, если студент a читал книгу b. Опишите упорядоченные пары следующих отношении: a)$R_1 \cup R_2$ b) $R_1 \cap R_2$ c)$R_1 \oplus R_2$ d) $R_1 \setminus R_2$ e) $R_2 \setminus R_1$.

20. Определим на множестве людей отношения R и S по правилу aRb, если a – родитель b и aSb, если a и b близнецы. Найти $R \circ S$ и $S \circ R$.

21. Пусть R_1 R_2 – отношения на множестве A заданные матрицами

$$M_{R_1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad M_{R_2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Найти матрицы соответствующие отношениям a)$R_1 \cup R_2$ b) $R_1 \cap R_2$ c)$R_1 \oplus R_2$ d) $R_1 \circ R_1$ e) $R_2 \circ R_1$

22. Пусть $M_R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $M_S = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Вычислить $M_{R \cup S}$, $M_{R \cap S}$, $M_{\bar{R}}$, $M_{\bar{R} \cup \bar{S}}$, $M_{\overline{R \cap S}}$.

23. Пусть $M_R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $M_S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$. Вычислить $M_{R \circ S}$.

24. Найти симметрическое замыкание отношения $R = \{(a, b) | a > b\}$ на $\mathbf{Z}$.

25. Найти рефлексивное замыкание отношения $R = \{(a, b) | a \neq b\}$ на множестве $\mathbf{Z}$.

26. Пусть M_R матрица отношения R на множестве из n элементов. Тогда матрица транзитивного замыкания R^*

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \cdots \vee M_R^{[n]}.$$

27. Пусть $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$ и R – отношение из A к B заданное по правилу

$$R = \{(1, y), (1, z), (3, y), (4, x), (4, z)\}.$$

Для отношения R

- найти матрицу отношения
- нарисовать диаграмму стрелок
- найти обратное отношение
- найти область определения и образ

28. Пусть $A = \{1, 2, 3, 4, 6\}$. Определим на A отношение R как x делит y: $(x, y) \in R \Leftrightarrow x|y$.

- Представить R как множество упорядоченных пар
- Нарисовать граф отношения R.
- Найти R^{-1}. Как описать R^{-1} словами ?

29. На множестве $A = \{1, 2, 3\}$ рассмотрим следующие отношения

$$R = \{(1,1),(1,2),(1,3),(3,3)\}, S = \{(1,1),(1,2),(2,1),(2,2),(3,3)\},$$

$$T = \{(1,1),(1,2),(2,2),(2,3)\}, \emptyset = \text{пустое отношение},$$

$$A \times A = \text{универсальное отношение}.$$

Какие из этих отношении являются рефлексивными, симметрическими, транзитивными и антисимметрическими ?

30. На множестве $A = \{a, b, c\}$ задано отношение

$$R = \{(a,a),(a,b),(b,c),(c,c)\}.$$

Найдите рефлексивные, симметрические и транзитивные замыкания R.

31. Отношение подобия на множестве треугольников есть отношение эквивалентности. Доказать.

32. Проверьте, что отношение принадлежности одному курсу есть отношение эквивалентности. Найти фактор-множество для множества студентов КБТУ относительно этого отношения.

33. На множестве целых чисел $\mathbf{Z}$ введем отношение $x \equiv y (mod\, n)$ если $n|x - y$. Доказать, что это отношение является отношением эквивалентности и найти соответствующее разбиение множества $\mathbf{Z}$. Как устроено фактор-множество $\mathbf{Z}/\equiv$?

34. Введем на множестве $A = \{(a, b)|a, b \in \mathbf{Z}, b \neq 0\}$ отношение R по правилу $(a, b)R(c, d)$, если $ad = bc$. Доказать, что R – отношение эквивалентности. Описать классы эквивалентности. Установить биекцию фактор-множества A/R в множество рациональных чисел $\mathbf{Q}$.

35. Определим на множестве $A = \{1, 2, 3, 4, 5, 6\}$ отношение

$$R = \{(1,1), (1,5), (2,2), (2,3), (2,6), (3,2), (3,3), (3,6),$$

$$(4,4), (5,1), (5,5), (6,2), (6,3), (6,6)\}.$$

Доказать, что является отношением эквивалентности. Найти разбиение A/R.

36. Для отношений $P = \{(x,y) \in \mathbf{R}^2 | x = y^2\}$ и $Q = \{(x,y) \in \mathbf{R}^2 | x \cdot y > 0\}$ найти $P \circ Q, Q \circ P, P \circ P$ и P^{-1}.

37. Доказать следующие тождества

$$R_1 \circ (R_2 \circ R_3) = (R_1 \circ R_2) \circ R_3,$$

$$R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3),$$
$$R_1 \circ (R_2 \cap R_3) = (R_1 \circ R_2) \cap (R_1 \circ R_3),$$
$$(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3),$$
$$(R_1 \cap R_2) \circ R_3 = (R_1 \circ R_3) \cap (R_2 \circ R_3),$$

где $R_1, R_2, R_3 \subseteq A \times A$.

38. Пусть $A = \mathbf{R}[x]$ – пространство многочленов. Определим умножение на A по правилу

$$f(x) \circ g(x) = f(x) \frac{\partial g(x)}{\partial x}.$$

Например, $x \circ x^4 = 4x^4$ Доказать, что выполнены тождества

$$(a \circ b) \circ c - a \circ (b \circ c) = (b \circ a) \circ c - b \circ (c \circ a),$$

$$(a \circ b) \circ c = (a \circ c) \circ b,$$

для любых $a, b, c \in A$,

39. Пусть $A = \mathbf{R}[x]$ – пространство многочленов. Определим умножение на A по правилу

$$f(x) \circ g(x) = f(x) \int_0^x g(x)\, dx.$$

Например, $x \circ x^4 = x^6/5$. Доказать, что выполнено тождество

$$(a \circ b) \circ c = a \circ (b \circ c + c \circ b),$$

для любых $a, b, c \in A$,

Глава 3

Комбинаторика и теория чисел

3.1 Принципы счета

Имеется два основных правила для счета.

Правило суммы. Допустим, что необходимо выполнить задания T_1 и T_2. Предположим, что существует n_1 и n_2 возможностей для выполнения задании T_1 и T_2, причем задания T_1 и T_2 одновременно невыполнимы. Тогда существует $n_1 + n_2$ возможностей для выполнения одного из задании T_1 и T_2.

Обобщенное правила суммы. Допустим, что для возникновения задании $T_1, T_2, \ldots, T_{k-1}$ и T_k существуют $n_1, n_2, \ldots, n_{k-1}$ и n_k возможностей соответственно, причем никакие два разных задания одновременно невыполнимы. Тогда существует $n_1 + \cdots + n_k$ возможностей для выполнения одного из этих задании.

В терминах теории множеств обобщенное правило суммы выглядит так. Пусть заданы k множеств $A_1, A_2, \ldots, A_k$ такие, что $A_i \cap A_j = \emptyset$ для любых $i \neq j$. Тогда

$$|A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|.$$

Доказательство. Пусть задание T_i состоит в выборе элементов из множества A_i, где $i = 1, \ldots, k$. Тогда существует n_i возможностей для выполнения задания T_i. Тогда по правилу суммы существует $n_1 + \cdots + n_k$ возможностей для выполнения одного из этих задании. Иными словами,

$$|A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|.$$

Пример. Студент должен выбрать одну тему для курсовой работы. Существует 3 темы по физике и 5 тем по химии. Сколько возможностей существует для выбора тем ?

Ответ: 3+5=8 возможностей.

Правило произведения. Допустим, что задание T можно разделить на два подзадания T_1, T_2 так, что эти задания можно выполнить последовательно, сначала задание T_1 и затем задание T_2. Задание T_1 выполнимо n_1 способами и задание T_2 выполнимо n_2 способами. Тогда задание T выполнимо $n_1 n_2$ способами.

Обобщенное правило произведения. Допустим, что задание T можно разделить на k подзадания $T_1, T_2, \ldots, T_k$ так, что эти задания можно выполнить последовательно, сначала задание T_1, затем задание T_2 и т.д. Задание T_1 выполнимо n_1 спо-

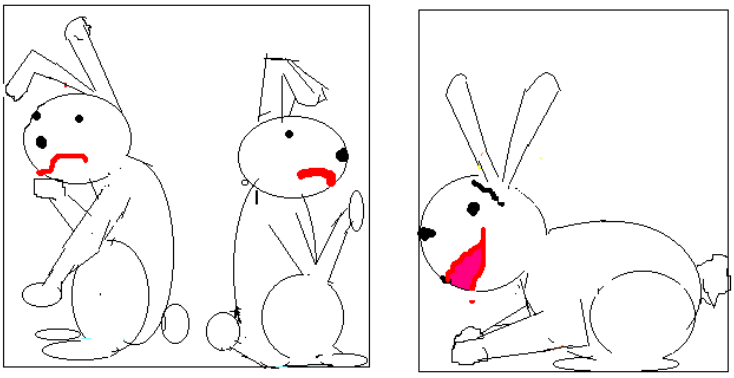


Рис. 3.1: Как бы ни сажали трех зайцев в две клетки всегда найдется клетка, в которой содержится по крайней мере два зайца.

собами, задание T_2 выполнимо n_2 способами, и так далее задание T_k выполнимо n_k способами. Тогда задание T выполнимо $n_1 n_2 \cdots n_k$ способами.

Обобщенное правило произведения в терминах теории множеств:

$$|A_1 \times A_2 \times \cdots \times A_k| = |A_1||A_2| \cdots |A_k|$$

Пример. По вкусу мороженое бывают ванильные и шоколадные. По размерам они бывают большие, средние и маленькие. Сколько типов мороженых существуют ?

Ответ: $2 \times 3 = 6$ типов.

Пример. Пусть $\mathcal{F}(A, B) = \{f : A \to B\}$ множество функции из множества порядка n в множество порядка m. Найти порядок множества $\mathcal{F}(A, B)$.

Ответ: m^n.

3.2 Принцип Дирихле

Принцип Дирихле. Заданы n предметов и m ящиков. Требуется разместить предметы по ящикам. Если $n > m$, то всегда найдется ящик, в котором находятся по крайней мере два предмета.

Принцип Дирихле легче всего формулировать в терминах зайцев и клеток. Основное требование: зайцев должно быть больше чем клеток. Тогда как бы вы не пытались улучшить жилищные условия зайцев, вам это не удастся. Всегда найдутся по крайней мере два зайца, которые будут недовольны тем, что живут в одной клетке (рис.1).

Чтобы применить принцип Дирихле необходимо определиться что понимать под зайцами и что под клетками. Например, в следующей задаче под зайцами следует понимать школьников, а под клетками -дни года.

Пример. Среди любых $n+1$ целых чисел не превосходящих $2n$ найдется число, которое делится на другое.

Решение. Представим числа $a_1, \ldots, a_{n+1} < 2n$ в виде $a_i = 2^{k_i} q_i, 1 \leq i \leq n+1$, где q_i – нечетны. Рассмотрим последовательность нечетных чисел $q_1, \ldots, q_{n+1}$. Поскольку все они не превосходят $2n$ и количество таких нечетных чисел не больше чем n, среди них по принципу Дирихле имеются по крайней мере два равных. Пусть, $q_i = q_j = q$. Тогда $a_i = 2^{k_i} q, a_j = 2^{k_j} q$. Если $k_i < k_j$, то a_j делится на a_i. Если $k_i > k_j$, то a_i делится на a_j.

Пример. (P. Erdös, G. Szekeres) Для каждого $n \in \mathbf{Z}^+$ любая последовательность различных действительных чисел длины $n^2 + 1$ содержит убывающую или возрастающую подпоследовательность длины $n + 1$. Доказать.

Доказательство. Пусть $a_1, \ldots, a_{k^2+1}$ последовательность $n^2 + 1$ различных действительных чисел. Пусть i_k – максимальная длина возрастающей подпоследовательности, начинающийся с a_k и d_k – максимальная длина убывающей подпоследовательности, начинающийся с a_k.

Допустим, что $i_k \leq n, d_k \leq n$, для любых $1 \leq k \leq n^2 + 1$. Тогда по правилу произведения существуют n^2 возможностей для (i_k, d_k). Значит по принципу Дирихле $(i_s, d_s) = (i_t, d_t)$, для некоторых $s < t$. Покажем, что это невозможно.

Если $a_s < a_t$, то подставив в начало возрастающей подпоследовательности начинающейся с a_t число a_s мы получаем возрастающую подпоследовательность длины $i_t + 1$ начинающийся с a_s. Поскольку $i_s = i_t$, получаем противоречие с максимальностью длины возрастающей подпоследовательности начинающейся с a_s.

Если $a_s > a_t$, то подставив в начало убывающей подпоследовательности начинающейся с a_t число a_s, мы получаем убывающей подпоследовательность длины i_s+1 начинающийся с a_s. Поскольку $i_s = i_t$, получаем противоречие с максимальностью длины убывающей подпоследовательности начинающейся с a_s.

Пример. Допустим, что в группе из шести человек любые два являются либо друзьями, либо врагами. Доказать, что в группе имеются 3 человек, любые два из которых являются друзьями, либо врагами.

Доказательство. Пусть A один из шести. По принципу Дирихле существует по крайней мере $3 > 5/2$ человек друзей A или врагов A. Допустим, что B, C, D – друзья A. Если по крайней мере два человека среди B, C, D являются друзьями, то они с A образует группу из трех друзей. Если все B, C, D образует множество взаимных врагов, то получаем множество из трех человек врагов.

Пример. Докажите, что среди любых 11 действительных положительных чисел, не превосходящих 100 найдутся по крайней мере два (обозначим их x, y) такие, что $0 < |\sqrt{x} - \sqrt{y}| < 1$.

Решение. Пусть $a_1, \ldots, a_{11}$ – произвольная последовательность действительных чисел между 0 и 100. Рассмотрим последовательность 11 чисел $\sqrt{a_1}, \ldots, \sqrt{a_{11}}$. Они лежат на отрезке 1 и 10. Поэтому по принципу Дирихле найдутся два, обозначим их через $\sqrt{x}, \sqrt{y}$, которые лежат на одном отрезке длины 1. Тогда $0 < |\sqrt{x} - \sqrt{y}| < 1$.

3.2.1 Задачи

1. В школе учатся 367 школьников. Докажите, что найдутся два школьника, у которых одинаковы дни рождения.

Указание. Сколько дней в году?

2. На кафедре высшей математики работают 13 преподавателей. Докажите, что найдутся два преподавателя, которые родились в один и тот же месяц.

Указание. Зайцы – преподаватели. Клетки – 12 месяцев.

3. Любое множество состоящее из 41 казахских слов содержит по крайней мере два слова начинающие из одинаковых букв. Доказать.

Указание. Казахский алфавит содержит 42 букв. Слово не может начинаться с букв "ъ" и "ь".

4. Пусть $S \subset \mathbf{Z}^+$, где $|S| = 25$. Тогда S содержит по крайней мере два элемента которые имеют одинаковый остаток от деления на 24.

5. Всякое подмножество порядка 6 множества $S = \{1, 2, \ldots, 9\}$ имеет два элемента с суммой 10.

6. Среди пяти точек выбранных внутри равностороннего треугольнике со стороной 1 имеется две, расстояние между которыми меньше чем 1/2. Доказать.

7. Найти последовательность четырех различных действительных чисел, которые не содержат убывающую или возрастающую подпоследовательность длины 3.

8. Найти последовательность девяти различных действительных чисел, которые не содержат убывающую или возрастающую подпоследовательность длины 4.

9. Доказать, что в задаче P. Erdös, G.Szekeres заменить $n^2 + 1$ на n^2 нельзя. Постройте последовательность различных действительных чисел длины n^2 не содержащей убывающей и возрастающей подпоследовательности длины $n + 1$.

3.3 Формула включения - исключения

Теорема. $|\cup_{i=1}^n A_i| = \sum_{s=1}^n (-1)^{s+1} \sum_{1 \le i_1 < \cdots < i_s \le n} |A_{i_1} \cup \cdots \cup A_{i_s}|$.

Доказательство будем проводить индукцией по n. При $n = 1$ утверждение очевидно.

Докажем утверждение для $n = 2$. Имеем

$$A_1 \cup A_2 = (A_1 \setminus A_2) \cup A_2.$$

Заметим, что

$$|A_1 \setminus A_2| = |A_1| - |A_1 \cap A_2|,$$
$$(A_1 \setminus A_2) \cap A_2 = \emptyset.$$

Поэтому

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Допустим, что утверждение верно для $n \ge 2$. Пусть

$$A = \cup_{i=1}^n A_i.$$

Согласно тождеству дистрибутивности

$$A \cap A_{n+1} = (A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \cdots \cup (A_n \cup A_{n+1}).$$

Заметим, что

$$(A_{i_1} \cap A_{n+1}) \cap \cdots \cap (A_{i_s} \cap A_{n+1}) = A_{i_1} \cap \cdots \cap A_{i_s} \cap A_{n+1}.$$

Поэтому, по предположению индукции

$$|A \cap A_{n+1}| = \sum_{s=1}^{n} (-1)^{s+1} \sum_{0<i_1<\cdots<i_s\leq n} |A_{i_1} \cap \cdots \cap A_{i_s} \cap A_{n+1}|.$$

Как было замечено выше наше утверждение верно для $n = 2$. Поэтому по предположению индукции

$$|A \cup A_{n+1}| = |A| + |A_{n+1}| - |A \cap A_{n+1}| =$$

$$\sum_{s=1} (-1)^{s+1} \sum_{0<i_1<\cdots<i_s\leq n} |A_{i_1} \cap \cdots \cap A_{i_s}| + |A_{n+1}| - \sum_{s=1}^{n} (-1)^{s+1} |A_{i_1} \cap \cdots \cap A_{i_s} \cap A_{n+1}| =$$

$$\sum_{s=1}^{n+1} (-1)^{s+1} \sum_{0<i_1<\cdots<i_s\leq n+1} |A_{i_1} \cap \cdots A_{i_s}|.$$

Индукционный переход установлен. Теорема доказана полностью.

Пример. Шахтеры раздобыли 100 брикетов руды, содержащие железо, свинец и олово. Оказалось, что брикеты содержащее железо обязательно содержит и свинец, 60 брикетов содержат олово и 50 брикетов содержат железо и олово. Сколько брикетов содержит железо ?

Решение. Пусть A_1, A_2 и A_3 множество брикет содержащее, соответственно, железо, свинец и олово. По условию задачи $A_1 \subseteq A_2$, поэтому

$$A_1 \cup A_2 = A_2, \quad A_1 \cup A_2 \cup A_3 = A_2 \cup A_3.$$

Кроме того,

$$|A_3| = 60, \quad |A_1 \cup A_3| = 50,$$

и

$$|A_1 \cup A_2 \cup A_3| =$$

$$|A_1| + |A_2| + |A_3| - |A_1 \cup A_2| - |A_1 \cup A_3| - |A_2 \cup A_3| + |A_1 \cup A_2 \cup A_3| =$$

$$|A_1| + |A_3| - |A_1 \cup A_3|.$$

Поэтому

$$|A_1| = 100 - 60 + 50 = 90.$$

Пример. Функция Эйлера. Пусть $n \in \mathbf{N}$. Найти порядок множества чисел между 1 и n, взаимно простых с n. Это число обозначается $\phi(n)$. Функция $\phi : \mathbf{N} \to \mathbf{N}$ называется функцией Эйлера.

Докажем, что

$$\phi(n) = n\prod_{i=1}^{k}(1-\frac{1}{p_i}),$$

где $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ – каноническое разложение в произведение простых сомножителей числа n.

Пусть

$$A_i = \{p_i m \mid m \in \mathbf{N}, 0 < p_i m < n\}.$$

Тогда

$$|A_i| = n/p_i.$$

Более того, для любых $0 < i_1 < \ldots < i_s \leq k$ множество $A_{i_1} \cap \cdots \cap A_{i_s}$ состоит из чисел, которые не делятся на $p_{i_1}\cdots p_{i_s}$, и

$$|A_{i_1} \cap \cdots \cap A_{i_s}| = n/p_{i_1}\cdots p_{i_s}.$$

Поэтому по формуле включения-исключения

$$|A_1 \cup \cdots \cup A_k| =$$

$$\sum_{s\geq 1}(-1)^{s+1} n/p_{i_1}\cdots p_{i_s} =$$

$$n(1-\prod_{s=1}^{k}(1-1/p_s)).$$

Здесь используется следующая лемма, которую легко доказать индукцией по k.

Лемма. Для любых k чисел $x_1, \ldots, x_k$, справедливо равенство

$$1 + \sum_{s=1}^{k}(-1)^s \sum_{1\leq i_1<\cdots<i_s\leq k} x_{i_1}\cdots x_{i_s} = \prod_{s=1}^{k}(1-x_s).$$

Поскольку множество $A_1 \cup \cdots \cup A_k$ состоит из чисел, которые имеют хотя бы один делитель вида p_i для некоторого $1 \leq i \leq k$, множество

$$\{m \mid 0 < m < n, \text{НОД}(m,n) = 1\}$$

совпадает с дополнением $\overline{A_1 \cup \cdots \cup A_k}$, где в качестве универсального множества взято множество $\{1, 2, \ldots, n\}$. Таким образом,

$$\phi(n) = n\prod_{s=1}^{k}(1-1/p_s).$$

Пример. Беспорядки. Перестановка $f \in Sym_n$ называется беспорядком, если $f(i) \neq i$, для любого $i \in \{1, 2, \ldots, n\}$. Найти количество беспорядков.

Докажем, что количество беспорядков равна

$$D(n) = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!}).$$

Пусть

$$A_i = \{f \in Sym_n \mid f(i) = i\}, \quad i = 1, 2, \ldots, n.$$

Тогда для любого $0 < i_1 < \cdots < i_s \leq n$,

$$|A_{i_1} \cap \cdots \cap A_{i_s}| = (n-s)!$$

В множестве из n элементов подмножество порядка s выбирается $\binom{n}{s}$ способами. Другими словами, количество выборок $(i_1, \ldots, i_s)$, таких, что $0 < i_1 < \cdots < i_s \leq n$ равно $\binom{n}{s}$. Таким образом, формула включения-исключения приобретает вид

$$|A_1 \cup \cdots \cup A_n| =$$

$$\sum_{s=1}^{n}(-1)^{s+1} \sum_{0<i_1<\cdots<i_s\leq n} |A_{i_1} \cap \cdots \cap A_{i_s}| =$$

$$\sum_{s=1}^{n}(-1)^{s+1}\binom{n}{s}(n-s)! =$$

$$\sum_{s=1}^{n}(-1)^{s+1}\frac{n!}{s!}.$$

Поэтому

$$D_n = |\overline{A_1 \cup \cdots \cup A_n}| =$$
$$|Sym_n| - |A_1 \cup \cdots \cup A_n| =$$
$$n!(\sum_{s\geq 0}(-1)^s\frac{1}{s!}).$$

Пример. Количество сюръективных функции. Пусть $\mathcal{F}^{on}(A, B) = \{f : A \to B\}$ – множество сюръективных функции из множества из n элементов в множество из m элементов. Тогда

$$|\mathcal{F}^{on}(A, B)| = \sum_{s=0}^{m}(-1)^s\binom{m}{s}(m-s)^n.$$

Например, при $n = 3, m = 2$ существуют $6 = 8 - 2$ сюръективных функции.

Доказательство этого факта будет приведено в следующем пункте.

3.3.1 Задачи

1. В кружке по подготовке к олимпиадам школьники изучают математику и инфороматику. Из них 25 школьников изучают информатику, 13 учат математику и 8 изучают математику и информатику. Сколько школьников посещают кружок?

2. В колледже учатся 1807 студентов. Из них 453 изучают английский, 567 изучают немецкий, и 299 изучают английский и немецкий. Сколько студентов не изучают ни английского, ни немецкого ?

3. Сколько элементов содержат множество $A_1 \cup A_2$, если A_1 содержит 12 элементов, A_2 имеет 18 элементов и

- $A_1 \cap A_2 = \emptyset$
- $|A_1 \cap A_2| = 1$
- $|A_1 \cap A_2| = 6$
- $A_1 \subseteq A_2$

4. Найти количество целочисленных неотрицательных решении уравнения $x_1 + x_2 + x_3 + x_4 = 8$ с условиями $x_i \leq 7$, для всех $i = 1, 2, 3, 4$.

5. Сколько неотрицательных целочисленных решении имеет уравнение $x_1 + x_2 + x_3 = 11$ относительно неизвестных x_1, x_2, x_3 таких, что $x_1 \leq 3$, $x_2 \leq 4$ и $x_3 \leq 6$. ?

6. Сколько существуют функции "на" из множества порядка шесть на множество порядка три?

7. Сколько чисел останутся в множестве $\{1, 2, \ldots, 1000\}$ после вычеркивания чисел кратных $2, 3, 5, 7$?

8. Сколько чисел в множестве $\{1, 2, \ldots, 100\}$ не делятся в квадрат какого либо целого числа большей чем 1 ?

9. Беспорядком множества $\{1, 2, \ldots, n\}$ называется перестановка $\sigma \in Sym_n$ такая, что $\sigma(i) \neq i$, для всех $i = 1, 2, \ldots, n$. Перечислить все беспорядки множества $\{1, 2, 3, 4\}$.

10. Сколькими способами можно переставить цифры $\{0, 1, 2, \ldots, 9\}$ так, чтобы ни одно четное число не стояло на своем месте ?

11. Сколько перестановок из 42 букв казахского алфавита не содержат последовательности *көже, тары, құрт* ?

12. (Неравенства Бонферрони) Доказать неравенства:

$$\sum_{k=1}^{q} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} |\bigcap_{i \in I} A_i| \leq |\bigcup_{i=1}^{n} A_i|,$$

если q четно,

$$\sum_{k=1}^{q} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} |\bigcap_{i \in I} A_i| \geq |\bigcup_{i=1}^{n} A_i|,$$

если q нечетно.

3.4 Биномиальные коэффициенты

Факториал $n! = 1 \cdot 2 \cdot 3 \cdots n$. Биективная функция $f : \underline{n} \to \underline{n}$, где $\underline{n} = \{1, 2, \ldots, n\}$, называется перестановкой. Пусть Sym_n множество перестановок. Тогда

$$|Sym_n| = n!.$$

Биномиальный коэффициент

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!}, \quad n \in \mathbf{Z}, \quad i \in \mathbf{Z}^+.$$

Другие обозначения: C_n^i, $C(n,i)$. По определению $\binom{n}{i} = 0$, если $i > n$. Обратим внимание на то, что биномиальный коэффициент можно определить и для отрицательных n. Если $n \in \mathbf{Z}^+$, то

$$\binom{n}{i} = \frac{n!}{i!(n-i)!},$$

$$\binom{-n}{i} = (-1)^i \binom{n+i-1}{i}.$$

Пример. Дано множество порядка n. Найти количество подмножеств порядка k.

Решение. Пусть $A = \{a_1, \ldots, a_n\}$ – множество порядка n и $P_k(A) = \{B \subseteq A || B| = k\}$ – множество подмножеств порядка k. Пусть $C_n^k = |P_k(A)|$. Пусть $B \subseteq A$ – подмножество порядка k. Возможно два взаимно исключающих случая.

Первый случай: $a_n \in B$. Тогда $B \backslash \{a_n\} \subseteq A \backslash \{a_n\}$ и $|B \backslash \{a_n\}| = k-1$. Количество таких подмножеств – C_{n-1}^{k-1}.

Второй случай: $a_n \notin B$. Тогда $B \subseteq A \setminus \{a_n\}$ и $|A \setminus \{a_n\}| = n-1$. Количество таких подмножеств – C_{n-1}^k.

Таким образом,

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k.$$

Очевидно, что

$$C_1^0 = 1, \quad C_1^1 = 1.$$

Как будет установлено внизу из этих условии следует, что

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Ответ: $\binom{n}{k}$.

Сочетание – размещение i неразличимых предметов по n ящикам, не более чем по одному в ящик. Количество сочетании $\binom{n}{i}$.

Сочетание с повторениями – размещение i неразличимых предметов по n ящикам. Число сочетании с повторениями – $\binom{n+i-1}{i}$.

Пример. Ящик содержит шары k цветов. Шаров каждого цвета не меньше чем n. Сколькими способами можно выбрать n шаров ?

Решение. Допустим, что выборка из n шаров содержит i_1 шаров цвета 1, i_2 шаров цвета 2, и т.д. Расположим их по порядку по цветам и между ними поставим перегородки.

Пусть A – множество шаров (их n штук) выборок и перегородок (их $k-1$ штук). Тогда $|A| = n + k - 1$ и наша задача равносильна выбору подмножества порядка $k-1$ (перегородки) множества порядка $n+k-1$ (шары и перегородки).

Ответ: $\binom{n+k-1}{k-1}$.

Пример. Сколько неотрицательных целочисленных решении имеет уравнение $x_1 + \cdots + x_k = n$

Эта вопрос эквивалентен предыдущему вопросу. Представьте, что x_i – количество шаров i-ого цвета, где $i = 1, 2 \ldots, k$.

Ответ: $\binom{n+k-1}{k-1}$.

Треугольник Паскаля

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

Элементы каждой следующей строки определяются как суммы двух чисел стоящих по бокам сверху.

Обозначим через C_n^i i-ый элемент n-ой строки. Положим $C_n^i = 0$ если $i < 0$ или $i > n$. Тогда свойство, порождающее треугольник Паскаля задается так

$$C_n^i = C_{n-1}^i + C_{n-1}^{i-1}.$$

3.4.1 Задачи

1. Доказать, что

$$C_n^i = \binom{n}{i}.$$

2. $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$.

3. (Бином Ньютона) $(x+y)^n = \sum_{i=1}^{n} \binom{n}{i} x^i y^{n-i}$.

4. $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

5. $\sum_{i=0}^{n}(-1)^i\binom{n}{i}=0$.

6. Доказать, что $\binom{n}{i}$ делится на p, если $n=p,\ 0<i<p$, и p– простое.

7. Найти количество подмножеств порядка 2 множества порядка 6.
Ответ. 15.

8. В ящике содержатся шары трех цветов. Сколькими способами можно выбрать 4 шара ? (Шаров каждого цвета не меньше 4)
Ответ: 15.

9. Сколько неотрицательных целочисленных решении имеет уравнение $x_1+x_2+x_3=4$?

10. Пусть $u^{(k)}=\frac{\partial^k u}{\partial x}$ – k-ая производная функции $u=u(x)$. Доказать, что

$$(u+v)^{(n)}=\sum_{i=0}^{n}\binom{n}{i}u^{(i)}v^{(n-i)}.$$

3.5 Функции на конечных множествах

Обозначения:

- $\mathcal{F}(A,B)=\{f:A\to B\}$ – множество всех функции из A в B.
- $\mathcal{F}^{in}(A,B)$ – множество инъективных функции из A в B,
- $\mathcal{F}^{on}(A,B)$ – множество сюръективных функции из A в B.

Пусть

$$A_m^n=m\cdot(m-1)\cdots(m-n+1)$$

– число перестановок n элементов из m различных элементов без повторений. По определению,

$$A_m^n=0,\ \text{если } m<n.$$

Теорема. Пусть A,B – множества порядка n и m соответственно. Тогда

$$|\mathcal{F}(A,B)|=m^n,$$

$$|\mathcal{F}^{in}(A,B)|=A_m^n,$$

$$|\mathcal{F}^{on}(A,B)|=\sum_{s=0}^{m}(-1)^s\binom{m}{s}(m-s)^n.$$

Доказательство. Пусть $A=\{a_1,\dots,a_n\}$ и $B=\{b_1,\dots,b_m\}$.

Всякая функция $f\in\mathcal{F}(A,B)$ однозначно определяется своими значениями $f(a_i)\in B$, где $i=1,\dots,n$. Элемент $f(a_i)$ может принимать одно из m значении $b_1,\dots,b_m$. Таким образом, по правилу произведения для $(f(a_1),\dots,f(a_n))\in\underbrace{B\times\cdots\times B}_{n}$ имеется m^n возможностей. Иными словами,

$$|\mathcal{F}(A,B)|=m^n.$$

Пусть $f \in \mathcal{F}^{in}(A,B)$. Тогда множество элементов $Im\, f = \{f(a_1), \ldots, f(a_n)\}$ определяют n элементное подмножество множества B. Таким образом, выбор множества $Im\, f$ равносильно выбору n элементного подмножества множества B. Как мы знаем это можно сделать $\binom{m}{n}$ способами. Пусть $A' = \{b'_1, \ldots, b'_n\}$ любое n элементное подмножество множества B. Существуют $n!$ функции с множеством элементов образов A'. Именно, функции f_σ, где $\sigma \in Sym_n$, заданными по правилам

$$f_\sigma(a_i) = b'_{\sigma(i)},$$

обладают таким свойством. Итак, по правилу произведения,

$$|\mathcal{F}^{in}(A,B)| = \binom{m}{n} n! = m(m-1)\cdots(m-n+1).$$

Пусть $f \in \mathcal{F}^{on}(A,B)$. Пусть $\mathcal{F}_i = \{f \in \mathcal{F}(A,B) \mid f(a) \neq b_i,\ \forall a \in A\}$ – подмножество функции, не принимающие значения b_i. Тогда f можно рассматривать как функцию из A со значениями в $m-1$ элементном множестве $B \setminus \{b_i\}$:

$$f \in \mathcal{F}_i \Rightarrow f \in \mathcal{F}(A, B \setminus b_i), \quad |B \setminus \{b_i\}| = m-1.$$

Таким образом,

$$|\mathcal{F}_i| = (m-1)^n, \quad i = 1, \ldots, n.$$

По аналогичными причинами, любую функцию $f \in \mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_s}$ можно рассматривать как функцию $f \in \mathcal{F}(A, B \setminus \{b_{i_1}, \ldots, b_{i_s}\}$ и

$$|\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_s}| = (m-s)^n.$$

Мы знаем, что строки $(i_1, \ldots, i_s)$ такие, что $1 \leq i_1 < \cdots < i_s \leq m$ можно выбрать $\binom{m}{s}$ способами. Итак, по правилу включения-исключения

$$|\mathcal{F}_1 \cup \cdots \cup \mathcal{F}_m| = \sum_{s=1}^{m} (-1)^{s+1} \sum_{1 \leq i_1 < \cdots < i_s \leq m} |\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_s}| = \sum_{s=1}^{m} (-1)^{s+1} \binom{m}{s} (m-s)^n.$$

Очевидно, что множество сюръективных функции совпадает с дополнением $\overline{\mathcal{F}_1 \cup \cdots \cup \mathcal{F}_m}$, где в качестве универсального множества выступает множество всех функции $\mathcal{F}(A,B)$. Таким образом,

$$|\mathcal{F}^{on}(A,B)| = |\overline{\mathcal{F}_1 \cup \cdots \cup \mathcal{F}_m}| = |\mathcal{F}(A,B)| - |\mathcal{F}_1 \cup \cdots \cup \mathcal{F}_m| =$$

$$m^n - \sum_{s=1}^{m} (-1)^{s+1} \binom{m}{s} (m-s)^n = \binom{m}{0} (m-0)^n + \sum_{s=1}^{m} (-1)^s \binom{m}{s} (m-s)^n =$$

$$\sum_{s=0}^{m} (-1)^s \binom{m}{s} (m-s)^n.$$

Следствие.

$$\sum_{s=0}^{m} (-1)^s \binom{m}{s} (m-s)^m = 0, \text{ если } m < n.$$

Доказательство. По принципу Дирихле, сюръективных функции нет, если $n > m$.

Теорема. Пусть $|A| = |B| = n$ и $f \in \mathcal{F}(A,B)$. Следующие условия эквивалентны:

- f – инъективен
- f – сюръективен
- f – биективен.

Доказательство. Пусть $f \in \mathcal{F}^{in}(A,B)$, но $f \notin \mathcal{F}^{on}(A,B)$. Иными словами, количество элементов подмножества образов $Im\, A \subset B$ меньше чем n. Тогда по принципу Дирихле существуют по крайней мере два элемента $a, a' \in A$ такие, что $f(a) = f(a')$. Это противоречит тому, что f инъективен.

Обратно, пусть $f \in \mathcal{F}^{on}(A,B)$, но $f \notin \mathcal{F}^{in}(A,B)$. Тогда найдутся по крайней мере два элемента $a, a' \in A$ такие, что $f(a) = f(a')$. Таким образом, $|Im\, A| < n$. Это противоречит тому, что f сюръективен.

Итак, мы доказали, что инъективность и сюръективность при $|A| = |B|$ понятия эквивалентные. Другими словами, все три понятия инъективность, сюръективность и биективность при $|A| = |B|$ эквивалентны.

Следствие.

$$|Sym_n| = n!.$$

Доказательство. Подставим $m = n$ в формуле

$$|\mathcal{F}^{in}(A,B)| = A_m^n = m(m-1)\cdots(m-n+1).$$

Следствие.

$$\sum_{s=0}^{m}(-1)^s\binom{m}{s}(m-s)^m = m!.$$

Доказательство. Подставим $n = m$ в формуле

$$|\mathcal{F}^{on}(A,B)| = \sum_{s=0}^{m}(-1)^{s+1}\binom{m}{s}(m-s)^n.$$

Получаем, что при $|A| = |B| = m$,

$$|\mathcal{F}^{on}(A,B)| = \sum_{s=0}^{m}(-1)^{s+1}\binom{m}{s}(m-s)^m.$$

Мы доказали выше, что если $|A| = |B|$, то

$$|\mathcal{F}^{on}(A,B)| = |\mathcal{F}^{in}(A,B)|.$$

Осталось применить предыдущее следствие

$$|\mathcal{F}^{in}(A,B)| = |Sym_m| = m!$$

чтобы завершить доказательство.

Пример. Трем лентяям предложили заняться одним из следующих дел: копать картошку, пасти скот или убирать мусор. Каждый из них могут ничем не заниматься и если заниматься, то не более чем одним делом. Сколько способов их поведения существуют ?

Решение. Пусть A – множество лентяев:

$$A = \{\text{лентяй}_1, \text{лентяй}_2, \text{лентяй}_3\}.$$

Пусть B – множество из четырех элементов

$$B = \{\text{копать картошку, пасти скот, убирать мусор, ничем не заниматься}\}.$$

Поэтому отображение $A \to B,\ a \mapsto b$, состоящая в том, что a выбирает занятие b является функцией. Таким образом, существует $4^3 = 256$ способов поведения лентяев.

Ответ: 256.

Пример. Каждый из четырех другов решили купить по галстуку, прием никто не хочет выбирать галстук такой же, как у другого. Имеются галстуки шести видов. Сколькими способами друзья могут осуществить свои выбор ?

Решение. Пусть A – множество друзей и B – множество галстуков. Тогда отображение $A \to B,\ a \mapsto b$, состоящая в том, что a выбирает галстук b является функцией (каждый выбирает по галстуку), причем иньективной (все выбранные галстуки различны). Таким образом, количество способов выбора галстуков равно

$$|\mathcal{F}^{in}(A, B)| = 6 \cdot 5 \cdot 4 \cdot 3 = 360.$$

Ответ: 360.

Пример. Четыре конструктора обязаны выполнить проект, который состоит из трех частей. Каждый из конструкторов выбирает одну из частей проекта, причем эту часть может выбрать и другой конструктор. Сколькими способами констукторы могут организовать работу над проектом ?

Решение. Пусть A – множество констукторов и B – множество частей проекта. Тогда отображение $A \to,\ a \mapsto b$, состоящая в том, что конструктор a выбирает часть b проекта является функцией, причем сюръективной (проект должен быть выполнен). Поэтому количество способов работы над проектом равно

$$|\mathcal{F}^{on}(A, B)| = (-1)^0 \binom{3}{0}(3-0)^4 + (-1)^1 \binom{3}{1}(3-1)^4 + (-1)^2 \binom{3}{2}(3-2)^4 + 0 = 36.$$

Ответ: 36.

3.6 Математическая индукция

Математическая индукция. Пусть $P(n)$ – некоторое утверждение зависящее от $n = 1, 2, \ldots$. Допустим, что удастся доказать следующие вещи.

Основание индукции: $P(1)$ верно.

Индукционный переход: если $P(n)$ верно, то $P(n+1)$ верно.

Вывод: тогда $P(n)$ верно для любого n.

В этом состоит метод математической индукции.

Пример. Докажем, что сумма нечетных последовательных целых чисел является полным квадратом. Именно, пусть утверждение $P(n)$ состоит в том, что

$$1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2. \tag{3.1}$$

Основание индукции:

$$P(1) : 1 = (0+1)^2.$$

Итак, основание индукции имеется.

Индуктивный переход: Допустим, что $P(n)$ верно, т.е.,

$$1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2.$$

Тогда

$$1 + 3 + 5 + \cdots + (2n+1) + (2n+3)$$

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

Иными словами $P(n+1)$ верно. Таким, образом, индукционный переход верен.

Вывод: (3.1) верно для любого n.

Пример. $\sum_{i=0}^{n} \binom{m+i}{i} = \binom{n+m+1}{n}$.

Решение. Будем рассуждать индукцией по $n = 0, 1, 2, \ldots$. При $n = 0$ утверждение верно. Допустим, что оно верно для n. Тогда

$$\sum_{i=0}^{n+1} \binom{m+i}{i} = \binom{n+m+1}{n+1} + \sum_{i=0}^{n} \binom{m+i}{i} =$$

$$\binom{n+m+1}{n+1} + \binom{n+m+1}{m+1} = \binom{n+m+1}{m} + \binom{n+m+1}{m+1} = \binom{n+m+2}{n+1}$$

Таким образом, утверждение верно для n. Индуктивный переход установлен. Иными словами, утверждение верно для всех $n \in \mathbf{Z}^+$.

3.6.1 Задачи

Докажите следующие формулы для сумм.

1. $\sum_{i=1}^{n} i = n(n+1)/2$.

2. $\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$.

3. $\sum_{i=1}^{n} i^3 = (n(n+1)/2)^2$.

4. $\sum_{i=1}^{n} i^4 = (3n^2 + 3n - 1)(2n+1)(n+1)n/30$.

5. $\sum_{i=1}^{n} i^5 = (2n^2 + 2n - 1)(n+1)^2 n^2/12$.

6. Докажите, что сумма n последовательных нечетных чисел является полным квадратом.

7. Докажите, что сумма кубов n последовательных целых чисел является полным квадратом.

8. Докажите, что n теңге для любого $n \geq 8$ можно разменять с помощью 3 и 5 теңге.

9. Докажите, что если $x + 1/x \in \mathbf{Z}$, то $x^n + 1/x^n \in \mathbf{Z}$, для любого $n \in \mathbf{N}$.

10. Пусть x_1, x_2 – корни уравнения $x^2 + 5x - 7 = 0$. Докажите, что для любого натурального n число $x_1^n + x_2^n$ является целым.

11. Докажите, что число $2^{3^n} + 1$ делится на 3^{n+1}.

12. У бабушки был внучек, который очень любил варенье, особенно то, которое в литровой банке, но бабушка не позволяла его трогать. И внучек задумал обмануть бабушку. Он решил съедать каждый день по 0.1 литра из самой лучшей банки и доливать ее водой (тщательно перемещав). Через сколько дней бабушка обнаружит обман, если варенье останется прежним на вид при разбавлении его водой наполовину ?

Указание. Индукцией по n докажите, что через n дней останется 0.9^n литров варенья. Заметим, что $0.5^6 < 1/2 < 0.5^7$. Поэтому через 6 дней обман все еще не обнаружится, но через 7 дней бабушка обман обнаружит.

Ответ. 7 дней.

13. Вычислить сторону правильного 2^n-угольника, вписанного в круг радиуса r.

Указание. $a_{2^{n+1}} = \sqrt{2r^2 - 2r\sqrt{r^2 - \frac{a_{2^n}^2}{4}}}$

14. (Теорема Юнга) На плоскости дано n точек, расстояние между любыми двумя из которых не превосходит единицы. Доказать, что все эти точки можно заключить в круг радиуса $1/\sqrt{3}$.

Гармонические числа определяются по формуле

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Например,

$$H_1 = 1, H_2 = 3/2, H_3 = 11/6.$$

Установить следующие свойства гармонических чисел.

15. $\sum_{j=1}^{n} H_j = (n+1)H_n - n$ для всех $n \in \mathbf{N}$.

16. $H_{2^n} \geq n/2 + 1$ для любого $n \in \mathbf{N}$.

17. Для любого $n \in \mathbf{Z}^+$

$$\sum_{j=1}^{n} jH_j = \frac{(n+1)nH_{n+1}}{2} - \frac{(n+1)n}{4}.$$

18. Пусть a_n – целочисленная последовательность такая, что

$$a_1 = 1, a_2 = 2, a_n = a_{n-1} + a_{n-2}, n \geq 3.$$

Найдите значения a_3, a_4, a_5, a_6, a_7 и докажите, что $a_n < (7/4)^n$ для любого $n \geq 1$.

Доказать неравенства:

19. Если $n > 3$, то $2^n < n!$.

20. Если $n > 4$, то $n^2 < 2^n$.

21. Заметим, что

$$1 = 1$$
$$2 + 3 + 4 = 1 + 8$$
$$5 + 6 + 7 + 8 + 9 = 8 + 27$$
$$10 + 11 + 12 + 13 + 14 + 15 + 16 = 27 + 64$$

Попробуйте сформулировать общую гипотезу и доказать ее.

3.7 Числа Фиббоначчи

Решать все задачи необязательно.
Числа Фиббоначчи определяются по индукции

$$F_1 = F_2 = 1, F_n = F_{n-1} + F_{n-2}.$$

Например, первые десять чисел Фиббоначчи выглядят так:

$$F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8,$$

$$F_7 = 13, F_8 = 21, F_9 = 34, F_{10} = 55.$$

Прекрасный способ проверить насколько освоен метод математической индукции дают числа Фиббоначчи. Установите следующие свойства чисел F_n.

3.7.1 Задачи

1. $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

2. $F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$.

3. $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$.
Указание. $F_k F_{k+1} - F_{k-1} F_k = F_k^2$.

4. (Мини-Тетрис) Сколькими способами можно покрыть без наложении прямоугольник $n \times 2$ с помощью квадратов 2×2 и 1×1.

5. (Кузнечик-попрыгунчик) Кузнечик путешествует на двумерной координатной плоскости по оси x слева направо прыгая по целочисленным вершинам на один или два шага. Сколькими способами он может добраться из точки 1 в точку n?

Ответ. F_n.

6.

$$F_{n+m} = F_{n-1}F_m + F_nF_{m+1} \tag{3.2}$$

Указание. Это утверждение можно доказать с помощью индукции по m. Второй способ доказательство основан на задаче о кузнечике. Из точки $x = 1$ он может попасть в точку $x = n + m$ с помощью F_{n+m} способов. Он может попасть в это точку двумя путями в зависимости от того попадает ли он в точку $x = n$ или обходит. Первый путь: сначала он добирается до точки $x = n - 1$ (это он сможет сделать F_{n-1} способами), затем перепрыгивает на 2 шага в точку $x = n+1$ и отсюда в точку $x = n + m$ (это он сможет сделать F_m способами). Второй путь: сначала кузнечик попадает в точку $x = n$ с помощью F_n способов, затем из точки $x = n$ в точку $x = n + m$ с помощью F_{m-1} способов.

7. Доказать, что F_{2n} делится на F_n.
Указание. Возьмите $n = m$ в (3.2).

8. $F_{2n} = F_{n+1}^2 - F_{n-1}^2$.
Указание. В предыдущей задаче воспользуйтесь тем, что $F_n = F_{n+1} - F_{n-1}$.

9. $F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3$.
Указание. Возьмите $m = 2n$ в задаче (3.2).

10. $\sum_{i=1}^{2n-1} F_iF_{i+1} = F_{2n}^2$.

11. $\sum_{i=1}^{2n} F_iF_{i+1} = F_{2n+1}^2 - 1$.

12. $\sum_{i=1}^{2n-1}(n + 1 - i)F_i = F_{n+4} - (n + 3)$.

13. $\sum_{i=1}^{2n-1} iF_i = nF_{n+2} - F_(n + 3) + 2$.

14. Если n делится на m, то и F_n делится на F_m.

15. Для любого целого числа n среди первых n^2-1 чисел Фиббоначчи найдется хотя бы одно, делящееся на n.

16. Соседние числа Фиббоначчи взаимно просты.

17. Для целых чисел m, n через (m, n) обозначим их наибольший общий делитель. Тогда наибольший общий делитель чисел Фиббоначчи также является числом Фиббоначчи:

$$(F_n, F_m) = F_{(n,m)}.$$

Указание. Примените алгоритм Евклида

18. F_n делится на F_m тогда и только тогда, когда n делится на m.

19. Число Фиббоначчи четно тогда и только тогда, когда его номер делится на 3.

20. Число Фиббоначчи делится на 3 тогда и только тогда, когда его номер делится на 4.

21. Число Фиббоначчи делится на 4 тогда и только тогда, когда его номер делится на 6.

22. Число Фиббоначчи делится на 5 тогда и только тогда, когда его номер делится на 5.

23. Число Фиббоначчи делится на 7 тогда и только тогда, когда его номер делится на 8.

24. Число Фиббоначчи делится на 16 тогда и только тогда, когда его номер делится на 12.

25. Если число Фиббоначчи имеет нечетный номер, то все его нечетные делители имеют вид $4k+1$

3.8 Реккурентные соотношения

Однородное реккурентное соотношение. Пусть $f_n = af_{n-1} + bf_{n-2}$ реккурентное соотношение, где a и b константы. Допустим, что q_1 и q_2 – корни уравнения

$$x^2 = ax + b.$$

Тогда f_n имеет вид

$$f_n = cq_1^n + dq_2^n, \quad \text{если } q_1 \neq q_2,$$

$$f_n = (c + dn)q_1^n, \quad \text{если } q_1 = q_2,$$

для некоторых констант c, d.

Доказательство. Рассмотрим случай различных корней. Сначала покажем, что $f_n = cq_1^n + dq_2^n$ удовлетворяет нашим реккурентным соотношениям. Имеем

$$af_{n-1} + bf_{n-2} = acq_1^{n-1} + adq_2^{n-1} + bcq_1^{n-2} + bdq_2^{n-2} = cq_1^{n-2}(aq_1 + b) + dq_2^{n-2}(aq_2 + b)$$

Поскольку q_1, q_2 – корни уравнения $x^2 - ax - b = 0$,

$$aq_1 + b = q_1^2, \quad aq_2 + b = q_2^2,$$

и поэтому,

$$af_{n-1} + bf_{n-2} = cq_1^n + dq_2^n = f_n.$$

Теперь покажем, что обратно, любое решение реккурентного уравнения имеет вид $f_n = cq_1^n + dq_2^n$ для некоторых констант c, d. Допустим, что заданы начальные условия $f_0 = A_0, f_1 = A_1$.

Начальные условия дают следующие условия

$$\begin{cases} A_0 = c + d \\ A_1 = cq_1 + dq_2 \end{cases}$$

Определитель этой системы невырожден:

$$\begin{vmatrix} 1 & 1 \\ q_1 & q_2 \end{vmatrix} = q_2 - q_1 \neq 0.$$

Поэтому

$$c = \frac{A_0 q_2 - A_1}{q_2 - q_1}, \quad d = \frac{A_1 - A_0 q_1}{q_2 - q_1}.$$

Реккурентные соотношения однозначно определяют f_n по начальным данным. Таким образом в случае $q_1 \neq q_2$, наше реккурентное соотношение имеет решение в виде $f_n = cq_1^n + dq_2^n$.

Случай $q_1 \neq q_2$ разобран полностью. Случай $q_1 = q_2$ оставляется в виде упражнения.

Пример. (Числа Фиббоначчи) Решить уравнение $f_n = f_{n-1} + f_{n-2}$ с граничными условиями $f_0 = 0, f_1 = 1$.

Решение. Характеристическое уравнение $\chi(t) = t^2 - t - 1$ имеет корни $t_1 = \frac{1+\sqrt{5}}{2}, t_2 = \frac{1-\sqrt{5}}{2}$. Поэтому $f_n = c(\frac{1+\sqrt{5}}{2})^n + d(\frac{1-\sqrt{5}}{2})^n$ для некоторых констант c и d. Чтобы найти константы воспользуемся начальными условиями. Имеем

$$f_0 = 0 \Rightarrow c + d = 0,$$

и

$$f_1 = 1 \Rightarrow c\frac{1+\sqrt{5}}{2} + d\frac{1-\sqrt{5}}{2} = 1 \Rightarrow c = \frac{1}{\sqrt{5}}.$$

Таким образом,

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

Пример. Решить уравнение $f_{n+2} = 4f_{n+1} - 4f_n$ с граничными условиями $f_0 = 1, f_1 = 4$.

Решение. Характеристическое уравнение $\chi(t) = t^2 - 4t + 4$ имеет двукратный корень $t = 2$. Поэтому $f_n = (c + dn)2^n$ для некоторых констант c и d. Чтобы найти константы воспользуемся начальными условиями. Имеем

$$f_0 = 1 \Rightarrow c = 1,$$

$$f_1 = 4 \Rightarrow c + d = 2 \Rightarrow d = 1.$$

Таким образом, $f_n = (n+1)2^n$.

Пример. Найти реккурентное соотношение для количество разбиении множества порядка n.

Решение. Пусть B_n – количество разбиении множества порядка n. Положим $B_0 = 1$. Пусть $A = \{a_1, \ldots, a_n, a_{n+1}\}$ – множество порядка $n+1$. Пусть $X \subseteq A$ – подмножество порядка $k+1$ содержащее элемент a_{n+1}. Тогда подмножество $X \setminus \{a_{n+1}\} \subseteq A \setminus \{a_{n+1}\}$ можно выбрать $\binom{n}{k}$ способами. Дополнение $A \setminus X$ можно разбить B_n способами. Таким образом, по правилу произведения и по правилу суммы

$$B_{n+} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} = \sum_{k=0}^{n} \binom{n}{n-k} B_{n-k} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

Ответ. $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.
Например,

$$B_1 = 1,$$

$$B_2 = \binom{1}{0} B_0 + \binom{1}{1} B_1 = 1 \times 1 + 1 \times 1 = 2,$$

$$B_3 = \binom{2}{0} B_0 + \binom{2}{1} B_1 + \binom{2}{2} B_2 = 1 \times 1 + 2 \times 1 + 1 \times 2 = 5.$$

Число B_n называется числом Белла.

3.8.1 Задачи

1. Решить реккурентные уравнения

- $a_n = a_{n-1} + 6a_{n-2}, n \geq 2, a_0 = 3, a_1 = 6$
- $a_n = 7a_{n-1} - 10a_{n-2}, n \geq 2, a_0 = 2, a_1 = 1$
- $a_{n+2} = -4a_{n+1} + 5a_n, n \geq 0, a_0 = 1, a_1 = 8$
- $a_n = a_{n-2}/4, n \geq 2, a_0 = 1, a_1 = 0$
- $a_n = a_{n-1} + 2a_{n-2}, n \geq 2, a_0 = 2, a_1 = 7$

2. (Числа Лукаса) Заданы реккурентное соотношение

$$L_n = L_{n-1} + L_{n-2}, L_0 = 2, L_1 = 1.$$

Доказать, что

$$L_n = F_{n-1} + F_{n+1}, \quad n = 2, 3, \ldots,$$

где F_n числа Фиббоначчи. Найти точную формулу для чисел Лукаса.

3. Докажите, что число $\lfloor (2+\sqrt{3})^n \rfloor$ является нечетным. Здесь $\lfloor \alpha \rfloor$ обозначает целую часть числа $\alpha \in \mathbf{R}$, т.е., целое число n такое, что $n \leq \alpha < n+1$.
Указание. Пусть $a_n = (2+\sqrt{3})^n$. Проверьте, что $a_{n+1} = 4a_n - a_{n-1}$. Поэтому $\lfloor a_{n+1} \rfloor = 4\lfloor a_n \rfloor - \lfloor a_{n-1} \rfloor + 2, \quad \lfloor a_1 \rfloor = 3$.

4. Показать, что число $\frac{1}{2}((1+\sqrt{2})^n + (1-\sqrt{2})^n)$ целое для любого $n \in \mathbf{Z}$.
Указание. $a_{n+2} = 2a_{n+1} + a_n$ и $a_0 = a_1 = 1$.

5. Доказать, что число $(6+\sqrt{37})^{999}$ имеет по крайней мере 999 нулей после десятичной запятой.
Указание. Последовательность $x_n = (6+\sqrt{37})^n - (6-\sqrt{37})^n$ удовлетворяет условиям $x_{n+2} = 12x_{n+1} + x_n$, и $x_0 = 2, x_1 = 12$. Поэтому $x_n \in \mathbf{Z}$ для всех $n \geq 0$. Заметим, что $\sqrt{37} - 6 < 0.1$

6. (Другие способы вычисления беспорядков) Доказать, что число беспорядков D_n удовлетворяют следующим реккурентным соотношениям.

- $D_n = (n-1)(D_{n-1} + D_{n-2}), \quad D_1 = 0, D_0 = 0.$
- $D_n = nD_{n-1} + (-1)^n, \quad D_1 = 0, D_0 = 0.$

Заметьте, что эти соотношения не попадают в класс реккурентных соотношении с постоянными коэффициентами. То же самое относится к реккурентным соотношениям для чисел Белла.

3.9 Производящие функции

Пусть a_n последовательность чисел, где $n \in \mathbf{Z}^+$ и Γ – множество последовательностей. Определим на множестве Γ операцию суммы

$$(a+b)_n = a_n + b_n,$$

операцию умножения на скаляр

$$(\lambda a)_n = \lambda a_n$$

и операцию умножения (конволюция)

$$(a \star b)_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Пусть $0 \in \Gamma$–последовательность, состоящая из одних нулей: $0_n = 0$, для всех n. Обозначим через $1 \in \Gamma$ последовательность нулевая компонента которой равна 1, а остальные равны 0.

Тогда $(\Gamma, 0, 1, +, \star)$ –коммутативная ассоциативная алгебра с единицей. Иными словами, выполнены следующие тождества

$$0 + a = a,$$

$$1 \star a = a,$$

$$a + b = b + a,$$

$$a \star b = b \star a,$$

$$\lambda(a+b) = \lambda a + \lambda b,$$

$$a + (b + c) = (a + b) + c,$$

$$(a+b) \star c = a \star c + b \star c,$$

$$a \star (b \star c) = (a \star b) \star c,$$

где $a, b, c \in \Gamma$.

Для последовательности a производящая функция строится по правилу

$$G(a) = \sum_{i \geq 0} a_i x^i.$$

Это, вообще говоря, формальный ряд, т.е., ряд с бесконечными ненулевыми членами.

Пример. Найти производящую функцию для последовательности $1, 1, 1, 1, \ldots$.

Решение. Для последовательности $a_n = 1$ имеем

$$G(a) = 1 + x + x^2 + \cdots = \frac{1}{1-x}.$$

Ответ. $G(a) = \frac{1}{1-x}$.

Для чисел λ и для формальных рядов $f(x) = \sum_{i\geq 0} a_i x^i, g(x) = \sum_{i\geq 0} b_i x^i$, положим

$$\lambda f(x) = \sum_{i\geq 0} \lambda a_i x^i,$$

$$f(x) + g(x) = \sum_{i\geq 0} (a_i + b_i) x^i,$$

$$f(x)g(x) = \sum_{n\geq 0} (\sum_{i\geq 0} a_i b_{n-i}) x^n.$$

Множество формальных рядов $\mathbf{C}[[x]]$ относительно этих операции также образует *коммутативную ассоциативную алгебру с единицей.* (Проверьте !) Нуль этой алгебры образует ряд $0 = \sum_{i\geq 0} 0x^i$ и единицу – ряд $1 = 1 + \sum_{i>0} 0x^i$.

Теорема. Отображение $\Gamma \to \mathbf{C}[[x]], \quad a \mapsto G(a)$ является гомоморфизмом алгебр:

$$G(0) = 0,$$

$$G(1) = 1,$$

$$G(\lambda a) = \lambda G(a),$$

$$G(a + b) = G(a) + G(b),$$

$$G(a \star b) = G(a)G(b).$$

Следствие 1. Порождающая функция для последовательности a_n полученной из последовательностей b_n, c_n путем сложения: $a_n = b_n + c_n$, получается из порождающих функции $G(a)$ и $G(b)$ также путем сложения:

$$G(a) = G(b) + G(c).$$

Следствие 2. Порождающая функция для последовательности a_n полученной из последовательности b_n путем умножения на число: $a_n = \alpha b_n$, получается из порождающей функции $G(b)$ также путем умножения на число:

$$G(a) = \alpha G(b).$$

Пример. Найти производящую функцию для последовательности $1, 3, 5, 7, \ldots$.

Решение. Пусть $a_n = 2n + 1$, $b_n = n + 1$, $c_n = 1$. Тогда $a_n = 2b_n - 1$ и согласно следствиям 1 и 2,

$$G(a) = 2G(b) - G(c) = 2/(1-x)^2 - 1/(1-x) = (1+x)/(1-x)^2.$$

Ответ: $\frac{x+1}{(1-x)^2}$

Следствие 3. Пусть b_n – последовательность, полученная из последовательности a_n со сдвигом на k вправо:

$$b_i = 0, i \leq k, b_k = a_0, b_{k+1} = a_1, \ldots.$$

Тогда

$$G(b) = x^k G(a).$$

Следствие 4. Пусть b_n – последовательность, полученная из последовательности a_n со сдвигом на k влево:

$$b_1 = a_k, b_2 = a_{k+1}, b_3 = a_{k+2}, \ldots.$$

Тогда

$$G(b) = (G(a) - a_0 - a_1 x - \cdots - a_{k-1}x^{k-1})/x^k.$$

Следствие 5. Пусть α – число и последовательность b_n получена из последовательности a_n путем формулы $b_n = \alpha^n a_n$. Тогда производящая функция $G(b)$ получается из $G(a)$ путем подстановки αx вместо x.

Пример. $\frac{1}{1-2x}$ – производящая функция для последовательности $1, 2, 4, 8, 16, 32, \ldots$

Следствие 6. Пусть задана последовательность $a_0, a_1, \ldots$ и b_n – ее разжижение: $b_{sk} = a_k$ и $b_n = 0$, если n не делится на s. Тогда $G(b)$ получается из $G(a)$ путем подстановки x^s вместо x.

Пример. $\frac{1}{1-x^3}$ – производящая функция для последовательности $1, 0, 0, 1, 0, 0, 1, 0, 0, 1 \ldots$.

Обычно производящие функции строятся с помощью комбинации вышеуказанных методов.

Пример. Пусть $a_n = 2^{\lfloor n/2 \rfloor}$ т.е., $a = 1, 1, 2, 2, 3, 3, 4, 4, \ldots$. Найти производящую функцию $G(a)$.

Решение. Как было установлено выше, последовательность $b = 1, 2, 4, 8, \ldots$ имеет такую производящую функцию

$$G(b) = \frac{1}{1-2x}.$$

Поэтому ее разжижение $c = 1, 0, 2, 0, 4, 0, 6, \cdots$ имеет такую производящую функцию

$$G(c) = \frac{1}{1-2x^2}.$$

Следовательно ее сдвиг на 1 шаг направо $d = 0, 1, 0, 2, 0, 4, 0, 8, \cdots$ имеет такую производящую функцию

$$G(d) = \frac{x}{1-2x^2}.$$

Заметим, что $a_n = c_n + d_n$. Поэтому

$$G(a) = G(c) + G(d) = \frac{1+x}{1-2x^2}.$$

Еще одна операция с производящими функциями связана с операциями дифференцирования и интегрирования. Пусть $b_n = na_n$. Тогда

$$G(b) = G(a).$$

Пусть $c_n = b_n/(n+1)$. Тогда

$$G(c) = \int_0^x G(a)dx.$$

Пример. Найти производящую функцию для последовательности $1, 2, 3, \ldots$.

Решение 1. Пусть $a_n = 1$ для всех $n \in \mathbf{Z}^+$. С помощью индукции по $n \in \mathbf{Z}^+$ легко доказать, что $(a \star a)_n = n + 1$. Поэтому

$$G(a \star a) = G(a)G(a) = \frac{1}{(1-x)^2}.$$

Решение 2. Пусть $b_n = n + 1$, для $n \in \mathbf{Z}^+$. Тогда

$$G(b) = 1 + 2x + 3x^2 + 4x^3 + \cdots = \partial(1 + x + x^2 + \cdots) = \frac{\partial(1 + x + x^2 + x^3 + \cdots)}{\partial x} =$$

$$\frac{\partial(1-x)^{-1}}{\partial x} = \frac{1}{(1-x)^2}.$$

Ответ: $\frac{1}{(1-x)^2}$

Пример. Найти производящую функцию для чисел Фиббоначчи.

Решение. Пусть $G(x)$ – искомая производящая функция. Имеем

$$F_n = F_{n-1} + F_{n-2}, n \geq 2, \Rightarrow F_n x^n = F_{n-1}x^n + F_{n-2}x^n$$

$$\Rightarrow \sum_{n\geq 2} F_n x^n - x\sum_{n\geq 2} F_{n-1}x^{n-1} - x^2 \sum_{n\geq 2} F_{n-2}x^{n-2} = 0.$$

Заметим, что

$$\sum_{n\geq 2} F_n x^n = \sum_{n\geq 1} F_n x^n = G(x) - x,$$

$$\sum_{n\geq 2} F_{n-1}x^{n-1} = \sum_{n\geq 1} F_n x^n = G(x),$$

$$\sum_{n\geq 2} F_{n-2}x^{n-2} = \sum_{n\geq 1} F_n x^n = G(x), \text{ поскольку } F_0 = 0.$$

Таким образом,

$$(G(x) - x) - xG(x) - x^2G(x) = 0,$$

или

$$G(x) = \frac{x}{1 - x - x^2}.$$

Ответ: $\frac{x}{1-x-x^2}$

Пример. Пусть $n \in \mathbf{Z}^+$. Доказать, что $\binom{2n}{n} = \sum_{i=0}^{n} \binom{n}{i}^2$.

Доказательство. Сравним коэффициенты у x^n в обеих частях тождества

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

В левой части этот коэффициент равен $\binom{2n}{n}$ и в правой –

$$\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} = \sum_{i=0}^{n} \binom{n}{i}^2.$$

Пример. Доказать, что последовательность $a_n = \binom{n+k-1}{n}$ имеет производящую функцию $\frac{1}{(1-x)^k}$.

Решение. Рассмотрим последовательность $a^{(k)}$ определенную по правилам

$$a_n^{(k)} = \binom{n+k-1}{n}, \quad n \in \mathbf{Z}^+.$$

Тогда

$$a_n^{(1)} = 1, \quad \forall n \in \mathbf{Z}^+.$$

Будем рассуждать индукцией по $k = 1, 2, \ldots$. При $k = 1$ как мы установили выше $G(a^{(1)}) = \frac{1}{1-x}$, т.е., основание индукции верно.

Допустим, что утверждение верно для k. Как было установлено в примере секции 3.6 имеет место формула

$$\sum_{i=0}^{n} \binom{m+i}{i} = \binom{n+m+1}{n}.$$

Поэтому

$$\binom{n+k-1}{n} = \sum_{i=0}^{n} \binom{k-2+i}{i}.$$

Итак,

$$a_n^{(k)} = \sum_{i=0}^{n} \binom{k-2+i}{i} \times 1 = \sum_{i=0}^{n} a_i^{(k-1)} a_{n-i}^{(1)}.$$

Другими словами,

$$a^{(k)} = a^{(k-1)} \star a^{(1)},$$

и

$$G(a^{(k)} = G(a^{(k-1)}) G(a^{(1)}) = \frac{1}{(1-x)^{k-1}} \frac{1}{1-x} = \frac{1}{(1-x)^k}.$$

Пример. Ящик содержит 30 белых 40 черных и 50 красных шаров. Шары одинаково цвета неразличимы. Сколькими путями можно выбрать 70 шаров ?

Решение. Число способов выбора 70 шаров равно коэффициенту при x^{70} в произведении

$$(1 + x + x^2 + \cdots + x^{30})(1 + x + x^2 + \cdots + x^{40})(1 + x + x^2 + \cdots + x^{50})$$

$$= \frac{1}{(1-x)^3}(1 - x^{31})(1 - x^{41})(1 - x^{51}).$$

Имеет место разложение

$$\frac{1}{(1-x)^3} = (\sum_{i\geq 0} \binom{i+2}{2} x^i.$$

(см. предыдущую задачу при $k = 3$). Поэтому

$$(1 + x + x^2 + \cdots + x^{30})(1 + x + x^2 + \cdots + x^{40})(1 + x + x^2 + \cdots + x^{50})$$

$$= (\sum_{i\geq 0} \binom{i+2}{2} x^i)(1 - x^{31} - x^{41} - x^{51} + O(x^{70})).$$

Поэтому коэффициент при x^{70} равен

$$\binom{70+2}{2} - \binom{70+2-31}{2} - \binom{70+2-41}{2} - \binom{70+2-51}{2} = 1061.$$

Ответ. 1061.

Пример. Найти количество решении уравнения $x_1 + \cdots + x_k = n$ в натуральных числах.

Решение. Если $x_i \in \mathbf{N}, i = 1, \ldots, k$, удовлетворяют условию $x_1 + \cdots + x_k = n$, то $y_i = x_i - 1 \in \mathbf{Z}^+, i = 1, \ldots, k$, удовлетворяют условию $y_1 + \cdots + y_k = n - k$. Обратно, любое решение уравнения $y_1 + \cdots + y_k = n - k$ в целых неотрицательных числах позволяет построить решение уравнения $x_1 + \cdots + x_k = n$ в натуральных числах: $x_i = y_i + 1, i = 1, \ldots, k$. Мы знаем, что уравнение $y_1 + \cdots + y_k = m$ имеет $\binom{m+k-1}{k-1}$ решении в неотрицательных целых числах. Поэтому уравнение $x_1 + \cdots + x_k = n$ имеет $\binom{n-k+k-1}{k-1}$ решении в натуральных числах.

Ответ. $\binom{n-1}{k-1}$.

3.9.1 Задачи

1. Функция $(x+1)^n$ является производящей функцией для $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}, 0, 0, \ldots$.

2. ($n \in \mathbf{Z}^+$) Функция $(x+1)^{-n}$ является производящей функцией для $\binom{-n}{0}, \binom{-n}{1}, \binom{-n}{2}, \ldots$.
Пример. Найти производящую функцию для последовательности $0, 1, 4, 9, 16, \ldots$.
Ответ: $\frac{x+1}{(1-x)^3}$.

3. Найти коэффициент при x^5 в $(1 - 2x)^{-7}$.

4. Найти коэффициент при x^8 в $\frac{1}{(x-3)(x-2)^2}$.

5. Найти коэффициент при x^{15} в $(x^2 + x^3 + x^4 + \cdots)^4$.

6. Пусть $n, m, k \in \mathbf{Z}^+$. Доказать, что $\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$.
Указание. $(x + 1)^{m+n} = (x + 1)^m(x + 1)^n$.

7. Сколько существуют однородных полиномов степени n с k неизвестными, т.е., полиномов $x_1^{\alpha_1} \cdots x_k^{\alpha_k}$, таких, что $\alpha_1 + \ldots + \alpha_k = n, \alpha_1, \ldots, \alpha_k \in \mathbf{Z}^+$?

Ответ: $\binom{n+k-1}{k}$

8. Пусть $p_0(n)$ – количество упорядоченных разбиении числа n. Например, $p_0(3) = 4$, поскольку $3 = 1+1+1, 3 = 1+2, 3 = 2+1, 3 = 3$. Найти $p_0(n)$.

Ответ: $p_0(n) = 2^{n-1}$.

9. Пусть p_n – количество разбиении числа n. Например,

$$p_1 = 1: \quad 1 = 1;$$

$$p_2 = 2: \quad 2 = 2, 2 = 1+1;$$

$$p_3 = 3: \quad 3 = 3, 3 = 2+1, 3 = 1+1+1;$$

$$p_4 = 5: \quad 4 = 4, 4 = 3+1, 4 = 2+2, 4 = 2+1+1, 4 = 1+1+1+1;$$

$$p_5 = 7: \quad 5 = 5, 5 = 4+1, 5 = 3+2, 5 = 3+1+1, 5 = 2+2+1,$$

$$5 = 2+1+1+1, 5 = 1+1+1+1+1.$$

Доказать, что

$$G(p) = \prod_{i \geq 1} (1 - x^i)^{-1}.$$

3.10 Целые числа и делимость

Внизу мы полагаем, что $a, b, c, q, r \in \mathbf{Z}$.

Делитель (обозначение $d|a$) d – делитель числа a, если $a = dq$, для некоторого $q \in \mathbf{Z}$.

Кратное. a кратное b, если $b|a$.

a делится на b, если $b|a$.

Наибольший общий делитель чисел a, b (обозначение НОД(a, b)):

$$d_1|a, d_1|b \Rightarrow d_1|\text{НОД}(a, b)$$

Пример. НОД$(18, 30) = 6$.

Наименьшее общее кратное (обозначение НОК(a, b)):

$$a|c, b|c \Rightarrow \text{НОК}(a, b)|c$$

Пример. НОК$(18, 30) = 90$.

Числа

- $\mathbf{N}$ – множество натуральных чисел $\{1, 2, 3, \ldots\}$
- $\mathbf{Z}$ – множество целых чисел $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- $\mathbf{Z}^+$ – множество целых неотрицательных чисел $\{0, 1, 2, \ldots\}$
- $\mathbf{Q}$ – множество рациональных чисел $\{p/q : p, q \in \mathbf{Z}, q \neq 0\}$

- $\mathbf{R}$ – множество действительных чисел
- $\mathbf{C}$ – множество комплексных чисел
- $\lfloor \alpha \rfloor$ – нижняя целая часть числа $\alpha \in \mathbf{R}$, т.е., такое $n \in \mathbf{Z}$, что $n \leq \alpha < n+1$.
- $\lceil \alpha \rceil$– верхняя целая часть числа $\alpha \in \mathbf{R}$, т.е., такое $n \in \mathbf{Z}$, что $n-1 < \alpha \leq n$.

Каноническое разложение числа $n \in \mathbf{N}$– представление n в виде произведения степеней различных простых делителей: $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $p_1 < p_2 < \cdots < p_k$.

Алгоритм Евклида. Пусть $a, b \in \mathbf{Z}, b \neq 0$. Алгоритм Евклида состоит в том чтобы повторять многократно процесс деления с остатком. Допустим, что

$$a = bq_0 + r_1, 0 < r_1 < b,$$

$$b = r_1 q_1 + r_2, 0 < r_2 < r_1,$$

$$r_1 = r_2 q_2 + r_3, 0 < r_3 < r_2,$$

$$\vdots$$

$$r_{k-1} = r_k q_k$$

для некоторого k. Тогда

$$\text{НОД}(a, b) = r_k.$$

Пример. Найдем наибольший общий делитель чисел $a = 7228, b = 378$. Имеем

$$7228 = 378 \times 19 + 46,$$

$$378 = 46 \times 8 + 10,$$

$$46 = 10 \times 4 + 6,$$

$$10 = 6 \times 1 + 4,$$

$$6 = 4 \times 1 + 2,$$

$$4 = 2 \times 2 + 0.$$

Другими словами,

$$\begin{array}{rl} 7228 & |\underline{378} \\ \underline{-7182} & \;19 \end{array} \quad \begin{array}{rl} 378 & |\underline{46} \\ \underline{-368} & \;8 \end{array} \quad \begin{array}{rl} 46 & |\underline{10} \\ \underline{-40} & \;4 \end{array} \quad \begin{array}{rl} 10 & |\underline{6} \\ \underline{-6} & \;1 \end{array} \quad \begin{array}{rl} 6 & |\underline{4} \\ \underline{-4} & \;1 \end{array} \quad \begin{array}{rl} 4 & |\underline{2} \\ \underline{-4} & \;2 \\ 0 & \end{array}$$

Поэтому

$$\text{НОД}(7228, 378) = 2.$$

Простое число. Число $n > 1$ называется простым, если у него нет делителей кроме 1 и n.

Пример. 7 – простое число.

Составное число – не простое число.

Пример. 6 – составное число.

Теорема Евклида. Простых чисел бесконечно много.

Доказательство. Если $p_1 < \ldots < p_n$ – различные простые числа, то эти числа не являются делителями числа $p_1 \cdots p_n + 1$. Поэтому он имеет простой делитель $> p_n$.

Основная теорема арифметики. Любое $n \in \mathbf{N}$ можно представить в виде $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, где $p_1 < \cdots < p_k$ – простые числа и $\alpha_1, \ldots, \alpha_k \in \mathbf{N}$. Такое разложение единственно: если $n = q_1^{\beta_1} \cdots q_r^{\beta_r}$, где $q_1 < \cdots < q_r$ – простые числа и $\beta_1, \ldots, \beta_r \in \mathbf{N}$, то $k = r$ и $\alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k$.

Каноническое разложение. Разложение $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, где $p_1 < \cdots < p_k$ – простые числа и $\alpha_1, \ldots, \alpha_k \in \mathbf{N}$, называется каноническим разложением.

Пример. $5040 = 2^4 \times 3^2 \times 5^1 \times 7^1$ – каноническое разложение числа 5040.

Совершенное число. Натуральное число называется совершенным, если его удвоение равно сумме всех своих делителей.

Пример. $6, 28$ – совершенные числа, поскольку $12 = 1 + 2 + 3 + 6$ и $56 = 1 + 2 + 4 + 7 + 14 + 28$.

3.10.1 Задачи

1. Доказать, что для любых целых $r_1, \ldots, r_n$

$$b|a_1, \ldots, b|a_n \Rightarrow b|r_1 a_1 + \cdots r_n a_n.$$

2. Доказать, что для любого целого n число $n^5 - n$ оканчивается нулем.

3. Доказать, что гармоническое число $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ не может быть целым числом.

Решение. Пусть k – наибольшее целое с условием $2^k \leq n$ и P – произведение всех нечетных простых чисел, не превосходящих n. Число $2^{k-1} P H_n$ представится суммою, все слагаемые которой, кроме $2^{k-1} P \frac{1}{2^k}$, суть целые числа.

4. Докажите, что сумма $\frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n+1}$, где $n > 0$, не может быть целым числом.

Решение. Пусть $S_n = \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n+1}$. Пусть k – наибольшее целое с условием $3^k \leq 2n + 1$ и P – произведение всех взаимно простых с 6 чисел, не превосходящих $2n+1$. Число $3^{k-1} P S_n$ представится суммою, все слагаемые которой, кроме $3^{k-1} P \frac{1}{3^k}$, суть целые числа.

5. Пусть $n \in \mathbf{N}$. Доказать, что все коэффициенты разложения бинома Ньютона $(a + b)^n$ будут нечетными тогда и только тогда, когда n имеет вид $2^k - 1$.

6. Пусть p – простое число. Доказать, что показатель максимальной степени числа p, на которую делится $n!$ равна $\sum_{k>0}\lfloor\frac{n}{p^k}\rfloor$

7. Сколькими нулями оканчивается число 100! ?

Указание. Пусть 100! оканчивается с s нулями. Это значит, что 100! делится на 10^s, причем s – максимальное число с таким свойством. Пусть $100! = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}\cdots$ – каноническое разложение. Заметим, что

$$\alpha_3 = \sum_{i\geq 1}\lfloor 100/5^i\rfloor = 20 + 4 = 24,$$

и

$$\alpha_1 = \sum_{i\geq 1}\lfloor 100/2^i\rfloor = 50 + 25 + 12 + 6 + 3 + 1 > 24 = \alpha_3,$$

Поскольку $10^s = 2^s 5^s$, мы получаем, что $s = 24$.

Ответ. 100! оканчивается с 24 нулями.

8. (вопрос студенки 1 курса Жулдуз Арыкбаевой) Сколько цифр имеет 100! ?

Ответ. 100! имеет $\lceil\log_{10} 100!\rceil = 158$ цифр.

9. Найти каноническое разложение числа 20! .

Решение. Заметим, что простыми делителями числа 20! являются $2, 3, 5, 7, 11, 13, 17, 19$. Поэтому каноническое разложение числа 20! имеет вид

$$20 = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}11^{\alpha_5}13^{\alpha_6}17^{\alpha_7}19^{\alpha_8}.$$

Заметим, что

$$\alpha_1 = \lfloor 20/2\rfloor + \lfloor 20/4\rfloor + \lfloor 20/8\rfloor + \lfloor 20/16\rfloor = 10 + 5 + 2 + 1 = 18,$$

$$\alpha_2 = \lfloor 20/3\rfloor + \lfloor 20/9\rfloor = 6 + 2 = 8,$$

$$\alpha_3 = \lfloor 20/5\rfloor = 4,$$

$$\alpha_4 = \lfloor 20/7\rfloor = 2,$$

$$\alpha_5 = \lfloor 20/11\rfloor = 1,$$

$$\alpha_6 = \lfloor 20/13\rfloor = 1,$$

$$\alpha_7 = \lfloor 20/17\rfloor = 1,$$

$$\alpha_8 = \lfloor 20/19\rfloor = 1.$$

Ответ. $20! = 2^{18}\cdot 3^8\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 18$.

10. Найти наибольший общий делитель и наименьшее общее кратное чисел 65 и 520; 1139 и 1288; 162 и 56; 543 и 831.

11. Доказать, что если n нечетное, то $a^n + b^n$ делится на $a + b$.

Доказательство. $a^n + b^n = (a + b)\sum_{i=0}^{n-1} a^i b^{n-i-1}$.

12. Пусть $n \in \mathbf{N}$. Доказать, что $a^n - b^n$ делится на $a - b$.

Доказательство. $a^n - b^n = (a-b)\sum_{i=0}^{n-1} a^i b^{n-i}$.

13. (Мерсенн) Если число $2^n - 1$ простое, то n – тоже простое.

Доказательство. Допустим, что n не простое и $n = ab, a > 1, b > 1$. Тогда $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$ делится на $2^a - 1$. Поскольку $2^n - 1 > 2^a - 1 > 1$, мы получаем, что $2^n - 1$ не простое. Полученное противоречие показывает, что n простое, если $2^n - 1$ простое.

14. (Ферма) Если число $2^n + 1$ простое, то n – степень двойки.

Доказательство. Допустим, что n не является степенью 2. Это означает, что n можно представить в виде $n = 2^s a$, где a – нечетное и $a > 1$. Тогда $2^n + 1 = 2^{ab} + 1 = (2^a)^b + 1$ делится на $2^a + 1$. Поскольку $2^n + 1 > 2^a + 1 > 1$, мы получаем, что $2^n + 1$ не простое. Противоречие.

15. (Евклид) Если число $2^{k+1} - 1$ является простым, то число $2^k(2^{k+1} - 1)$ является совершенным.

Доказательство. Поскольку $2^{k+1} - 1$ – простое, число $N = 2^k(2^{k+1} - 1)$ имеет следующее множество простых делителей

$$D(N) = \{2^i, 2^i(2^{k+1} - 1) \mid 0 \leq i \leq k\}.$$

Тогда

$$\sum_{d|N} = \sum_{i=0}^{k} 2^i + \sum_{i \geq 0} 2^i(2^{k+1} - 1) = (\sum_{i=0}^{k} 2^i)(2^{k+1} - 1 + 1) = (2^{k+1} - 1)2^{k+1} = 2N.$$

Это значит, что число N совершенное.

16. (Эйлер) Каждое четное совершенное число имеет вид $2^k(2^{k+1}-1)$, где $2^{k+1}-1$ является простым числом.

17. Остап Бендер раздавал слонов 28 членам и 37 не членам профсоюза, причем всем членам профсоюза досталось поровну, и всем не членам – тоже поровну. Оказалось, что у Остапа был единственный способ раздать слонов таким образом. Какое наибольшее количество слонов у него могло быть ?

3.11 Сравнения

Сравнение. Пусть $a, b \in \mathbf{Z}$. Запись вида $a \equiv b(mod\, m)$ означает, что число $a - b$ делится на m. В таких случаях говорят, что числа a и b сравнимы по модулю m.

Пример. $63 \equiv 18(mod 15)$.

Классы вычетов. Отношение $a \equiv b(mod\, m)$ является отношением эквивалентности. Соответствующие классы эквивалентности называются классами вычетов. Всего имеются m классов вычетов по модулю m.

Пример. Классы вычетов по модулю $m = 5$:

$$\bar{0} = \{0, \pm 5, \pm 10 \pm 15, \cdots\},$$

$$\bar{1} = \{1, 6, 11, \cdots, -4, -9, \cdots\},$$
$$\bar{2} = \{2, 7, 17, \cdots, -3, -8, \cdots\},$$
$$\bar{3} = \{3, 8, 13, \cdots, -2, -7, \cdots\},$$
$$\bar{4} = \{4, 9, 14, \cdots, -1, -6, -11, \cdots\}.$$

Сравнения первой степени. Решение сравнения $ax \equiv b(mod\, m)$ – класс вычетов по модулю m, один элемент которого удовлетворяет сравнению. Очевидно, что тогда любой элемент этого класса удовлетворяет сравнению.

Пусть $d = \text{НОД}(a, m)$. Сравнение $ax \equiv b(mod\, m)$ разрешимо тогда и только тогда, когда $d|b$. В этом случае оно имеет d решений.

Решение сравнения $ax \equiv b(mod\, m)$ эквивалентно решению уравнения $ax+my = b$ в целых числах. Способ решения таких уравнении с помощью цепных дробей рассматривается в пункте 3.14. При небольших m это сравнение решается подбором.

Система сравнении первой степени. Система сравнений

$$\begin{cases} a_1x \equiv b_1(mod\, m_1), \\ a_2x \equiv b_2(mod\, m_2), \\ \qquad\vdots \\ a_nx \equiv b_n(mod\, m_n) \end{cases}$$

сводится к системе вида

$$\begin{cases} x \equiv b_1(mod\, m_1), \\ x \equiv b_2(mod\, m_2), \\ \qquad\vdots \\ x \equiv b_n(mod\, m_n). \end{cases}$$

Чтобы решить последний достаточно уметь решать систему

$$\begin{cases} x \equiv b_1(mod\, m_1), \\ x \equiv b_2(mod\, m_2). \end{cases}$$

Из первого сравнения получим $x = b_1 + m_1t$. Подставим это во второе сравнение. Получаем $m_1t = b_2 - b_1(mod\, m_2)$. Критерием разрешимости этого сравнения является условие $\text{НОД}(m_1, m_2)|b_2 - b_1$. В этом случае имеем одно решение по модулю $m_2/\text{НОД}(m_1, m_2)$:

$$t \equiv t_0(mod\, \frac{m_2}{\text{НОД}(m_1, m_2)}).$$

Поэтому

$$x = b_1 + m_1(t_0 + \frac{m_2}{\text{НОД}(m_1, m_2)}t) = b_0 + \frac{m_1m_2}{\text{НОД}(m_1, m_2)}t = b_0 + \text{НОК}(m_1, m_2)t$$

является решением нашей системы из двух сравнении. Итак система из двух сравнении в случае разрешимости имеет единственное решение по модулю $\text{НОК}(m_1, m_2)$.

В общем случае если система сравнении имеет решение, то она имеет единственное решение по модулю $\text{НОК}(m_1, \ldots, m_n)$.

Китайская теорема об остатках. Допустим, что целые числа $m_1, m_2, \ldots, m_n$ попарно взаимно просты. Пусть x_i – решение сравнения

$$m_1 \cdots m_{i-1} x_i m_{i+1} \cdots m_n \equiv 1 (mod\, m_i),$$

где $i = 1, 2, \ldots, n$. Тогда

$$x = m_2 m_3 \cdots m_n x_1 b_1 + m_1 m_3 \cdots m_n x_2 b_2 + \cdots + m_1 m_2 \cdots m_{n-1} x_n b_n$$

решение системы сравнении

$$\begin{cases} x \equiv b_1 (mod\, m_1), \\ x \equiv b_2 (mod\, m_2), \\ \quad \vdots \\ x \equiv b_n (mod\, m_n) \end{cases}$$

Это решение единственно по модулю произведения $m_1 m_2 \cdots m_n$.

Пример. Решить системы сравнений китайским способом

$$\begin{cases} x \equiv 2 (mod\, 5) \\ x \equiv 3 (mod\, 6) \\ x \equiv 4 (mod\, 7) \end{cases}$$

Решение. $m_1 = 5, m_2 = 6, m_3 = 7$. Имеем

$$x_1 \times 6 \times 7 \equiv 1 (mod\, 5) \Rightarrow x_1 \equiv 3 (mod\, 5),$$

$$x_2 \times 5 \times 7 \equiv 1 (mod\, 6) \Rightarrow x_2 \equiv -1 (mod\, 6),$$

$$x_3 \times 5 \times 6 \equiv 1 (mod\, 7) \Rightarrow x_3 \equiv 4 (mod\, 7).$$

Поэтому

$$x = 6 \times 7 \times 3 \times 2 + 5 \times 7 \times (-1) \times 3 + 5 \times 6 \times 4 \times 4 = 627$$

решение нашей системы сравнении. Это решение единственно по модулю 210.

3.12 Цепные дроби

Как построить цепную дробь ? Пусть $a, b \in \mathbf{Z}, b > 0$. Применим алгоритм Евклида:

$$a = bq_0 + r_1, 0 < r_1 < b,$$

$$b = r_1 q_1 + r_2, 0 < r_2 < r_1,$$

$$r_1 = r_2 q_2 + r_3, 0 < r_3 < r_2,$$

$$\vdots$$

$$r_{k-1} = r_k q_k$$

для некоторого k. Тогда цепная дробь соответствующая $\frac{a}{b}$ равна

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}$$

Краткая запись:

$$a/b = [q_0, q_1, \ldots, q_k].$$

Пример. Найдем цепную дробь для $a = 3614/189$. Имеем

$$3614 = 189 \times 19 + 23,$$

$$189 = 23 \times 8 + 5,$$
$$23 = 5 \times 4 + 3,$$
$$5 = 3 \times 1 + 2,$$
$$3 = 2 \times 1 + 1,$$
$$2 = 1 \times 2 + 0.$$

Тогда

$$\frac{3614}{189} = 19 + \cfrac{1}{8 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}}$$

или кратко

$$3614/189 = [19, 8, 4, 1, 1, 2].$$

Подходящие дроби рационального числа $a/b = [q_0, q_1, \ldots, q_k]$ задаются так

$$\delta_0 = \frac{q_0}{1},$$

$$\delta_1 = q_0 + \frac{1}{q_1},$$

$$\vdots$$

$$\delta_k = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}.$$

Тогда

$$\delta_0 = \frac{P_0}{Q_0}, \delta_1 = \frac{P_1}{Q_1}, \cdots \delta_s = \frac{P_s}{Q_s}, \cdots, \delta_k = \frac{P_k}{Q_k}.$$

Способ вычисления P_s, Q_s дается по следующим реккурентным формулам.

Теорема. $P_0 = q_0, \quad Q_0 = 1,$

$$P_s = P_{s-1}q_s + P_{s-2}, \quad Q_s = Q_{s-1}q_s + Q_{s-2}, \quad s = 1, 2, \ldots, k.$$

Доказательство. Для $s = 0, 1$ утверждение очевидно. Допустим, что утверждение верно для s. Поскольку

$$[q_0, q_1, \ldots, q_{s+1}] = [q_0, q_1, \ldots, q_{s-1}, q_s + \frac{1}{q_{s+1}}],$$

положив

$$q'_s = q_s + q_{s+1}^{-1},$$

$(s+1)$-ую подходящую дробь δ_{s+1} можно записать в виде s-ой подходящей дроби:

$$\delta_{s+1} = [q_0, q_1, \ldots, q_{s-1}, q'_s].$$

Правда, здесь q'_s не обязан быть целым. Но наши вычисления формальны, они не требуют целочисленности q'_s. По предположению индукции для $\delta_{s+1} = P_{s+1}/Q_{s+1}$ как s-ой подходящей дроби имеем,

$$P_{s+1} = P_{s-1}q'_s + P_{s-2} = P_{s-1}(q_s + q_{s+1}^{-1}) + P_{s-2},$$

$$Q_{s+1} = Q_{s-1}q'_s + Q_{s-2} = Q_{s-1}(q_s + q_{s+1}^{-1}) + Q_{s-2}.$$

Поэтому

$$\frac{P_{s+1}}{Q_{s+1}} = \frac{P_{s-1}(q_s + q_{s+1}^{-1}) + P_{s-2}}{Q_{s-1}(q_s + q_{s+1}^{-1}) + Q_{s-2}} =$$

$$\frac{P_{s-1}q_s + P_{s-2} + P_{s-1}q_{s+1}^{-1}}{Q_{s-1}q_s + Q_{s-2} + + q_{s+1}^{-1}Q_{s-1}} =$$

$$\frac{P_s + P_{s-1}q_{s+1}^{-1}}{Q_s + Q_{s-1}q_{s+1}^{-1}} =$$

$$\frac{P_s q_{s+1} + P_{s-1}}{Q_s q_{s+1} + Q_{s-1}}.$$

Итак, индуктивный переход возможен. Теорема доказана.

Итак, числители P_s и знаменатели Q_s можно вычислить по схеме

s		0	1	2	$\cdots$	s	$\cdots$	k
q_s		q_0	q_1	q_2	$\cdots$	q_s	$\cdots$	q_k
P_s	1	$P_0 = q_0$	$P_1 = P_0q_1 + 1$	$P_2 = P_1q_2 + P_0$	$\cdots$	$P_s = P_{s-1}q_s + P_{s-2}$	$\cdots$	P_k
Q_s	0	$Q_0 = 1$	$Q_1 = q_1$	$Q_2 = Q_1q_2 + Q_0$	$\cdots$	$Q_s = Q_{s-1}q_s + Q_{s-2}$	$\cdots$	Q_k

Пример. Найти подходящие дроби для 3614/189. Напомним, что

$$3614/189 = [19, 8, 4, 1, 1, 2].$$

Имеем,

s		0	1	2	3	4	5
q_s		19	8	4	1	1	2
P_s	1	$P_0 = 19$	$P_1 = 19 \times 8 + 1 = 153$	$P_2 = 153 \times 4 + 19 = 631$	$P_3 = 631 \times 1 + 153 = 784$	$P_4 = 784 \times 1 + 631 = 1415$	$P_5 = 1415 \times 2 + 784 = 3614$
Q_s	0	$Q_0 = 1$	$Q_1 = 8$	$Q_2 = 8 \times 4 + 1 = 33$	$Q_3 = 33 \times 1 + 8 = 41$	$Q_4 = 41 \times 1 + 33 = 74$	$Q_5 = 74 \times 2 + 41 = 189$

Поэтому

$$\delta_0 = \frac{19}{1}, \quad P_0 = 19, Q_0 = 1,$$

$$\delta_1 = \frac{153}{8}, \quad P_1 = 153, Q_1 = 8,$$

$$\delta_2 = \frac{631}{33}, \quad P_2 = 631, Q_2 = 33,$$

$$\delta_3 = \frac{784}{41}, \quad P_3 = 784, Q_3 = 41,$$

$$\delta_4 = \frac{1415}{74}, \quad P_4 = 1415, Q_4 = 74,$$

$$\delta_5 = \frac{3614}{189}, \quad P_5 = 3614, Q_5 = 189.$$

Свойства подходящих дробей. Внизу полагается, что $s = 0, 1, 2, \ldots, k$ и все примеры внизу относятся к числу $a/b = 3614/189$.

1. $P_s, Q_s \in \mathbf{Z}$, причем $Q_s \in \mathbf{N}$ для всех s и $Q_1 < Q_2 < \cdots < Q_k$.

Пример. Знаменатели начиная с первого члена образуют возрастающую последовательность: $1 < 33 < 41 < 74 < 189$

2. $P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s$.

Доказательство. Будем рассуждать индукцией по $s = 1, 2, \ldots, k$. Пусть $s = 1$. Имеем $P_0 = q_0, Q_0 = 1, P_1 = q_0q_1 + 1, Q_1 = q_1$. Тогда

$$P_0Q_1 - P_1Q_0 = q_0q_1 - (q_0q_1 + 1) \times 1 = -1.$$

Допустим, что утверждение верно для s. Тогда $P_{s+1} = P_sq_s + P_{s-1}, Q_{s+1} = Q_sq_s + Q_{s-1}$, и

$$P_sQ_{s+1} - P_{s+1}Q_s = P_s(Q_sq_s + Q_{s-1}) - (P_sq_s + P_{s-1})Q_s = P_sQ_{s-1} - P_{s-1}Q_s.$$

Значит по предположению индукции

$$P_sQ_{s+1} - P_{s+1}Q_s = -(-1)^s.$$

Итак, индукционный переход возможен. Утверждение доказано полностью.

Пример.

$$P_0Q_1 - P_1Q_0 = 19 \times 8 - 153 \times 1 = -1,$$

$$P_1Q_2 - P_2Q_1 = 153 \times 33 - 631 \times 8 = 1,$$
$$P_2Q_3 - P_3Q_2 = 631 \times 41 - 784 \times 33 = -1,$$
$$P_3Q_4 - P_4Q_3 = 784 \times 74 - 1415 \times 41 = 1,$$
$$P_4Q_5 - P_5Q_4 = 1415 \times 3614 - 3614 \times 74 = -1.$$

3. НОД$(P_s, Q_s) = 1$

Доказательство. Следует из предыдущего свойства: если $d =$ НОД(P_s, Q_s), то d – делитель числа $(-1)^s$, поэтому $d = 1$.

Пример. НОД$(19, 1) = 1,$НОД$(153, 8) = 1,$НОД$(631, 33) = 1,$НОД$(784, 41) = 1,$НОД$(1415, 74) = 1,$НОД$(3614, 189) = 1.$

4. $|\delta_s - \delta_{s-1}| = \frac{1}{Q_{s-1}Q_s}$.

Доказательство. Утверждение следует из формулы пункта 2 :

$$\delta_s - \delta_{s-1} = \frac{P_sQ_{s-1} - P_{s-1}Q_s}{Q_{s-1}Q_s} = \frac{(-1)^{s-1}}{Q_{s-1}Q_s}.$$

5.

$$\delta_1 > \delta_3 > \delta_5 > \cdots > \delta_{2p+1} > \cdots > a/b$$
$$\delta_0 < \delta_2 < \delta_4 < \cdots < \delta_{2p} < \cdots < a/b$$

Пример. $\delta_1 = 153/8 > \delta_3 = 784/41 > \delta_5 = 3614/184 > a/b, \quad \delta_0 = 19 < \delta_2 = 631/33 < \delta_4 = 1415/74 < a/b$

3.12.1 Задачи

1. Разложить в цепную дробь и найти все подходящие дроби разложения: $\frac{105}{38}$; $\frac{245}{83}$; $\frac{37}{81}$; $2,71828$; $3,14159$.

2. Преобразовать в обыкновенную дробь следующие цепные дроби $[2, 3, 1, 4]$; $[2, 1, 1, 2, 1, 6, 2, 5]$.

3. Преобразовать цепную дробь в обыкновенную

$$1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{5}}}}$$

3.13 Мультипликативные функции

Мультипликативная функция это функция $\theta : \mathbf{N} \to \mathbf{C}$ с условием $\theta(ab) = \theta(a)\theta(b)$, для любых $a, b \in \mathbf{N}$ таких, что НОД$(a, b) = 1$.

Предложение. Пусть θ – мультипликативная функция и $\theta(a_0) \neq 0$ для некоторого $a_0 \in \mathbf{N}$. Тогда $\theta(1) = 1$ и $\theta(a)$ полностью определяется своими значениями в степенях простых чисел.

Доказательство. Поскольку

$$\theta(a_0) = \theta(a_0 1) = \theta(a_0)\theta(1), \quad \theta(a_0) \neq 0,$$

имеем

$$\theta(1) = 1.$$

Если $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ и $p_1 < \cdots < p_k$, то ввиду мультипликативности θ,

$$\theta(a) = \theta(p_1^{\alpha_1}) \cdots \theta(p_k^{\alpha_k}).$$

Таким образом, если мы знаем значения $\theta(p_i^{\alpha_i})$, где p_i – простые числа и $\alpha_i \in \mathbf{N}$, то числа $\theta(a)$ вычисляются однозначно для любых $a \in \mathbf{N}$.

Пример. Положим $\theta(1) = 1$ и $\theta(p^\alpha) = 2$, если $\alpha \in \mathbf{N}$. Тогда

$$\theta(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \theta(p_1^{\alpha_1}) \cdots \theta(p_k^{\alpha_k}) = 2^k.$$

Иными словами функция θ , определенная по правилу

$$\theta(a) = 2^k,$$

если a имеет k различных простых делителей, является мультипликативной.

Лемма. Пусть θ_1 и θ_2 – мультипликативные функции и θ – функция определенная по правилу $\theta(a) = \theta_1(a)\theta_2(a)$. Тогда θ – мультипликативна.

Доказательство. Имеем

$$\theta(1) = \theta(1)\theta(1) = 1.$$

Если НОД$(a, b) = 1$, то

$$\theta(ab) = \theta_1(ab)\theta_2(ab) =$$

$$\theta_1(a)\theta_1(b)\theta_2(a)\theta_2(b) = \theta_1(a)\theta_2(a)\theta_1(b)\theta_2(b) =$$

$$\theta(a)\theta(b).$$

Предложение. Пусть θ – мультипликативная функция и $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ – каноническое разложение числа a. Тогда

$$\sum_{d|a} \theta(d) = \prod_{i=1}^{k} (1 + \theta(p_i) + \cdots + \theta(p_i^{\alpha_i})).$$

Доказательство. Раскроем скобки правой части. Получаем сумму слагаемых вида

$$\theta(p_1^{\beta_1}) \cdots \theta(p_k^{\beta_k}) = \theta(p_1^{\beta_1} \cdots p_k^{\beta_k})$$

и 1. Поскольку всякий делитель числа a имеет вид $p_1^{\beta_1} \cdots p_k^{\beta_k}$, в левой части стоят такая же сумма.

Количество делителей числа n

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1),$$

где $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$– каноническое разложение.

Пример. $\tau(60) = 12$.

Функция Мебиуса $\mu(n)$ определяется так:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат простого числа}, \\ (-1)^k, & \text{если } n \text{ – произведение } k \text{ различных простых чисел}. \end{cases}$$

Докажите, что функция Мебиуса – мультипликативна.

Пример. $\mu(60) = 0, \quad \mu(30) = -1, \quad \mu(35) = 1$.

Предложение. Пусть θ – мультипликативная функция и $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$– каноническое разложение. Тогда

$$\sum_{d|a} \mu(d)\theta(d) = (1 - \theta(p_1)) \cdots (1 - \theta(p_k)).$$

Доказательство. Произведение двух мультипликативных функции $\theta_1(a) = \theta(a)\mu(a)$ также является мультипликативной. Поэтому

$$\theta_1(p) = -\theta(p), \quad \theta_1(p^\alpha) = 0, \alpha > 1.$$

Осталось применить предыдущее предложение.

Следствие.

$\sum_{d|a} \mu(d) = \begin{cases} 0, & \text{если } a > 1, \\ 1, & \text{если } a = 1 \end{cases}$

Доказательство. Возьмем в качестве мультипликативной функции θ функцию, заданную по правилу $\theta(a) = 1$, для всех $a \in \mathbf{N}$.

Следствие.

$\sum_{d|a} \frac{\mu(d)}{d} = \begin{cases} (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}), & \text{если } a > 1, \\ 1, & \text{если } a = 1. \end{cases}$

Доказательство. Возьмем в качестве мультипликативной функции θ функцию, определенную по правилу $\theta(a) = \frac{1}{a}$, для всех $a \in \mathbf{N}$.

Функция Эйлера $\phi(n)$ – количество натуральных чисел, меньших чем n и взаимно простых с n. Имеет место формула

$$\phi(n) = n \prod_{i \geq 1} (1 - \frac{1}{p_i}),$$

где p_i – простые делители числа n.

Пример. $\phi(60) = 60(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 240$.

Теорема Эйлера.

$$\text{НОД}(a, n) = 1 \Rightarrow a^{\phi(n)} - 1 \equiv 0 (mod\, a).$$

Доказательство. Назовем a обратимым по модулю n, если $au \equiv 1(mod\, n)$. Если a, b обратимы по модулю n, то ab обратимы по модулю n:

$$au \equiv 1(mod\, n), bv \equiv 1(mod\, n) \Rightarrow (ab)(uv) \equiv 1(mod\, n).$$

Если a обратим по модулю n, то

$$au \equiv av(mod\, n) \Rightarrow u \equiv v(mod\, n).$$

Пусть $a_1, \ldots, a_{\phi(n)}$ – представители всех обратимых классов вычетов по модулю n. Если их всех умножить на число a, то получатся представители всех обратимых классов вычетов.

Перемножим все обратимые вычеты двумя способами:

$$a_1 \cdots a_{\phi(n)} \equiv (aa_1) \cdots (aa_{\phi(n)} = a^{\phi(n)} a_1 \cdots a_{\phi(n)}.$$

Поскольку $a_1 \cdots a_{\phi(n)}$ также обратим по модулю n, мы получаем, что

$$a^{\phi(n)} \equiv 1(mod\, n).$$

Малая теорема Ферма Для любого простого p и для любых $a \in \mathbf{Z}$,

$$a^p - a \equiv 0(modp)$$

Доказательство. Заметим, что $\phi(p) = p - 1$. Утверждение следует из теоремы Эйлера.

Пример. Для любого целого числа a числа a^5 и a оканчиваются одинаковыми цифрами.

3.13.1 Задачи

1. Пусть $\tau(n)$– количество делителей числа $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Доказать, что

$$\tau(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1).$$

2. Найти $\tau(5600), \tau(116424)$.

3. Найдите все натуральные числа меньшие 300, имеющие ровно 15 делителей.

4. Если $\theta(a)$ – мультипликативная функция, то

$$\sum_{d|a} \mu(d)\theta(d) = \prod_{i=1}^{k} (1 - \theta(p_i)),$$

где $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$– каноническое разложение числа n и $\mu(n)$ – функция Мебиуса.

5. Найти $\mu(n)$ для всех $n = 1, 2, \ldots, 100$.

6. Пусть θ – мультипликативная функция и $\theta_1 = \sum_{d|a} \theta(d)$. Доказать, что θ_1 также мультипликативна.

Обратно, пусть θ определена на $\mathbf{N}$ и функция $\psi(a) = \sum_{d|a} \theta(a)$ – мультипликативна. Доказать, что θ также мультипликативна.

7. Пусть $\phi(n)$ – количество целых чисел между 1 и n взаимно простых с n (Функция Эйлера). Доказать, что

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}), \tag{3.3}$$

где $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$– каноническое разложение числа n.

8. Для $n = 1, 2, \ldots, 50$

- построить множества взаимно простых чисел меньших чем n и вычислить $\phi(n)$.
- вычислить $\phi(n)$ с помощью формулы 3.3
- вычислить $\phi(n)$ используя мультипликативность функции $\phi(n)$.

9. Пусть $n \in \mathbf{Z}^+$ и F– функция определенная на множестве делителей числа n. Пусть

$$G(n) = \sum_{d|n} F(d).$$

Тогда

$$F(n) = \sum_{d|n} \mu(d) G(\frac{n}{d}).$$

10. Найти n, если

- $\phi(11^n) = 13310$
- $\phi(7^n) = 705894$

11. Найти n, если $\phi(n) = 2496$ и n имеет вид $n = 2^\alpha 5^\beta 13^\gamma$.
Ответ: $n = 6760$.

12. Проверить формулу $\sum_{d|n} \phi(d) = n$ на примерах $n = 100, 1240$.

13. Доказать, что

- $\phi(4n) = 2\phi(2n)$
- $\phi(4n + 2) = \phi(2n + 1)$

14. Пользуясь формулами Эйлера и Ферма, найти остаток от деления: 3^{78} на 11 ; 4^{93} на 13; 46^{921} на 21.

15. Найти последнюю цифру в десятичном представлении чисел: 9^{100}; 13^{219}; 17^{300}; 243^{402}; 473^{2004}.

3.14 Решение уравнении в целых числах.

Способ нахождения частного решения уравнения $ax + by = 1$

Разложим a/b в цепную дробь:

$$a/b = [q_0, q_1, \ldots, q_k].$$

Пусть δ_{k-1} – $(k-1)$-ая подходящая дробь и $\delta_{k-1} = P_{k-1}/Q_{k-1}$.

Теорема. Пусть НОД$(a, b) = 1$. Уравнение $ax + by = 1$ имеет следующее целочисленное решение:

$$x_0 = (-1)^{k-1}Q_{k-1}, y_0 = (-1)^k P_{k-1}.$$

Доказательство следует из соотношения $P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s$, приведенного в пункте 3.12. При $s = k$ получаем, что

$$(-1)^k P_{k-1}Q_k + (-1)^{k-1}P_kQ_{k-1} = 1.$$

Поскольку $P_k = a, Q_k = b$, это означает, что

$$a(-1)^{k-1}Q_{k-1} + b(-1)^k P_{k-1} = 1.$$

Другими словами,

$$ax_0 + by_0 = 1.$$

Пример. Уравнение $3614x+189y = 1$ имеет частное решение $x = 74, y = -1415$, поскольку, как мы установили выше, $k = 5$ и $\delta_4 = 1415/74$.

Общее решение уравнения $ax + by = c$.

Пусть $d =$ НОД(a, b). Уравнение $ax+by = c$ имеет целочисленное решение в том и только в том, случае когда c делится на d.

Пусть (x_0, y_0) – частное решение уравнения $ax + by = c$. Тогда общее решение этого уравнения имеет вид

$$x = x_0 - \frac{b}{d}t,$$
$$y = y_0 + \frac{a}{d}t,$$

где $t \in \mathbf{Z}$.

Пример. Найти общее решение уравнения $3614x+189y = 1$. Как было установлено выше это уравнение имеет частное решение $x_0 = 74, y_0 = -1415$. Мы знаем, что числа 3614 и 189 взаимно просты: $d = 1$. Поэтому общее решение имеет вид

$$x = 74 - 189t, y = -1415 + 3614t.$$

Пример. Решить уравнение $12x + 15y = 4$ в целых числах.

Уравнение решения не имеет, поскольку $c = 4$ не делится на наибольший общий делитель $d = 3$.

Пример. Решить уравнение $12x + 15y = 6$ в целых числах.

Уравнение имеет частное решение $x_0 = -2, y_0 = 2$ и $d = 3$. Поэтому общее решение имеет вид

$$x = -2 - 5t, y = 2 + 4t, \quad t \in \mathbf{Z}.$$

3.14.1 Задачи

1. Имеют ли решения в целых числах следующие уравнения ?

- $30x + 64y = 7$
- $12x + 86y = 16$

2. Решить сравнения в целых числах

- $7x \equiv 5(mod 31)$
- $6x \equiv 17(mod 29)$
- $-7x \equiv 21(mod 14)$

3. Решить уравнения в целых числах

- $53x - 17y = 25$
- $47x + 105y = 4$
- $18x + 33y = 112$
- $11x + 16y = 156$
- $35x + 16y = 2$

4. Докажите, что число внутренних целых точек отрезка с целыми концами $A(x_1, y_1), B(x_2, y_2)$ равно $d - 1$, где $d = (y_1 - y_2, x_1 - x_2)$.

5. Через сколько целых точек проходят стороны треугольника с вершинами $A(2, 3)$, $B(7, 8)$, $C(13, 5)$.

6. Найдите наименьшее натуральное число, кратное 7 и дающее остаток 1 при делении его на 2,3,4,5,6.

7. Припишите справа к числу 79 такое двузначное число, чтобы полученное четырехзначное число при делении на 11 и 13 дало бы соответственно остатки 3 и 5.

8. Требуется проложить трассу газопровода на участке длиной 450 м. В распоряжении строителей имеются трубы размеров длиной 9 м и 13 м. Сколько труб того и другого размера надо взять, чтобы проложить трассу ? Трубы резать не следует, число сварных швов должно быть минимальным.

Решение. Пусть x, y – числа труб длин x и y соответственно. Тогда

$$9x + 13y = 450.$$

Построим цепную дробь для 13/9 и построим с ее помощью решение частное уравнения $9x + 13y = 1$. Имеем

$$\begin{array}{rrr} & & 9 \;\; |\underline{13} \\ & & \underline{-0} \;\; 0 \\ & 13 & |\underline{9} \\ & \underline{-9} & 1 \\ 9 & |\underline{4} & \\ \underline{-8} & 2 & \\ 4 \;\; |\underline{1} & & \\ \underline{-4} \;\; 4 & & \\ 0 & & \end{array}$$

Итак, НОД$(9, 13) = 1$ и

$$9/13 = [0, 1, 2, 4].$$

Имеем

$$\delta_0 = 0, \delta_1 = 1, \delta_2 = 2/3.$$

Итак, $k = 3, P_{k-1} = 2, Q_{k-1} = 3$. Поэтому

$$x_0 = 3, y_0 = -2$$

– частное решение уравнения $9x+13y = 1$. Значит $x_1 = 3 \cdot 450 = 1350, y_1 = -2 \cdot 450 = -900$ частные решения уравнения $9x + 13y = 450$. Итак, общее решение уравнения $9x + 13y = 450$ имеет вид

$$x = 1350 - 13t, \quad y = -900 + 9t, \quad t \in \mathbf{Z}.$$

Найдем такие $t \in \mathbf{Z}$, что x, y будут неотрицательными:

$$\begin{cases} 1350 - 13t \geq 0 \\ -900 + 9t \geq 0 \end{cases}$$

Решение этой системы неравенств:

$$103\frac{11}{13} \geq t \geq 100.$$

Значит целыми решениями этой системы неравенств будут:

$$t = 100, 101, 102, 103.$$

Составим таблицу

t	100	101	102	103
x	50	37	24	11
y	0	9	18	27
$x + y$	50	46	42	38

.

Число швов равно $x + y$. Мы видим, что минимальное число швов получается при $x + y = 38$. Значит $x = 11, y = 27$.

Ответ. 11 труб длины 9 и 27 труб длины 13.

3.15 Компьютеры, простые числа и криптосистемы

3.15.1 Компьютерные тесты на простоту чисел

Напомним, что число n называется составным, если $n = a \cdot b$ для некоторых $a, b \in \mathbf{N}$. В противном случае n называется простым.

Имеются две основные проблемы касательно простоты n.

Проблема 1. Является ли n простым?

Проблема 2. Как разложить n в произведение простых сомножителей ?

Теоретически эти две проблемы эквивалентны. На практике при больших n эти задачи превращаются в очень сложные и совершенно разные проблемы, которых нельзя решить без помощи супермощных компьютеров.

Прежде чем рассказать об алгоритмах проверки простоты на компьютерах приведем несколько примеров. Математически они явно куръезны, но они иллюстрируют возникающиеся трудности.

Число

$$10^{100} + 267 = 1\underbrace{00\ldots00}_{97\text{ нулей}}267$$

является первым простым числом с 101 цифрами. На компьютерах это можно проверить в несколько секунд. Если число 200-значное, то типичное простые числа этого порядка требуют для проверки несколько минут.

Вероятно[1], что число

$$\frac{10^{1031}-1}{9} = \underbrace{111\ldots11}_{1031\text{ цифр}}$$

является простым. Чтобы разобраться с такими числами требуются несколько недель.

Для чисел некоторых специальных типов можно пойти дальше. Например, Д. Словинский с помощью компьютера CRAY-1 доказал, что 25962-значное число Мерсенна

$$2^{86243} - 1 = 536\ldots207$$

является простым. Это потребовало несколько часов машинного времени. Напомним, что число Мерсенна определяется как число вида $2^n - 1$.

Выше в разделе 3.10.1 (см.задачу Мерсенна) мы доказали, что простота n является необходимым условием для простоты числа $2^n - 1$. Это условие не является достаточным. Например,

$$p_1 = 2^2 - 1 = 3, p_2 = 2^3 - 1 = 7, p_3 = 2^5 - 1 = 31, p_4 = 2^7 - 1 = 127$$

действительно являются простыми, но число $2^{11}-1 = 2047 = 23 \cdot 89$ – нет. Вот список первых семи простых чисел Мерсенна (первые четыре простых числа приведены

[1]После выхода из печати первого варианта книги школьник 10 класса средней школы N 16 г. Алматы Арман Кудайбергенов сообщил о том, что это утверждение точное. Его программа, написанная в системе MAPLE приведено в секции 3.15.2.

выше)

$$p_5 = 2^{13} - 1 = 8191, p_6 = 2^{17} - 1 = 131071, p_7 = 2^{19} - 1 = 524287.$$

В 1998 году, 2 февраля, Роланд Кларксон, 19-летний студент Калифорнийского Государственного университета объявил об открытии 37-го числа Мерсенна. Им оказался число $2^{3021377} - 1$.

В 2004 году 15 мая, Джош Финдлей (Josh Findley) открыл 41-ое число Мерсенна $2^{24036583} - 1$. Число имеет больше 7 миллионов цифр и является наибольшим простым числом известным в настоящий момент (10 октября 2004). Джош проверял этот факт около двух недель на своем компьютере 2.4 GHz Pentium 4. Он был терпелив и ловил удачу около 5 лет. Новизна и простота числа были перепроверены Тони Раих (Tony Reix) в течение 5 дней. Он использовал операционную систему Линух на компьютере 16 Itanium II 1.3 GHz CPUs. Вторая проверка была сделана канадцем Джефф Гилхрист (Jeff Gilchrist). Проверка потребовала 11 дней.

Проблема разложения числа на простые сомножители гораздо сложнее. Существующие методы расправляются с числами порядка 40 или 50 цифр в несколько часов. Известно, например, что число

$$2^{293} - 1 = 159 \ldots 791$$

является составным, но найти хотя бы один его сомножитель очень непросто. Последнее достижение в этой области: 13 сентября 2004 года Давид Симкох (David Symcox) нашел 53-цифровой сомножитель для числа Мерсенна $2^{971} - 1$. Это было наименьшее число Мерсенна, для которого сомножители не были известны.

Удивительно, что не зная сомножителей можно узнать является ли заданное число простым или нет. Такие факты обычно устанавливаются с помощью следующей теоремы или их разновидностями.

Теорема Ферма (Пьер Ферма, 1601-1655, работал юристом в Тулузском парламенте. На досуге занимался математикой.)

$$n \text{ простое} \Rightarrow a^n \equiv a (mod\, n), \quad \forall a \in \mathbf{Z}.$$

Заметим, что для данных a и n легко проверить выполнена ли заключение теоремы Ферма (по крайней мере на компьютере). Это верно даже если a и n очень большие. Например, для чисел порядка 10^{100}. Для этого не нужно начинать вычислять непосредственно a^n: даже для $a = 3, n \approx 10^{100}$ это число становится насколько большим, что его невозможно вычислить даже на компьютере. Вместо этого достаточно вычислять остатки a^n от деления на n. Это можно легко сделать, например, последовательными возведениями в квадрат и умножениями по модулю n. Этот метод приведен в следующей секции.

Чтобы заключить, что n составное, достаточно найти хотя бы одного $a \in \mathbf{Z}$ не удовлетворяющего условию $a^n \equiv a (mod\, n)$. Для этого не нужно находить делителей числа n.

Чтобы доказать простоту n необходимо обращение теоремы Ферма. Здесь возникают две проблемы.

1. Первая проблема состоит в том, что непосредственное обращение теоремы Ферма, в котором импликация $\Rightarrow$ заменяется на $\Leftarrow$ неверно. Число Рамануджана $1729 = 7 \cdot 13 \cdot 19$ составное, но

$$a^{1729} \equiv a(mod\, 1729), \quad \forall a \in \mathbf{Z}.$$

Составные числа обладающие этим свойством называются числами Кармайкла. Вероятно, таких чисел бесконечно много.

Список первых 10 чисел Кармайкла:

Числа Кармайкла	канонические разложения
561	$3 \cdot 11 \cdot 17$
1105	$5 \cdot 13 \cdot 17$
1729	$7 \cdot 13 \cdot 19$
2465	$5 \cdot 17 \cdot 29$
2821	$7 \cdot 13 \cdot 31$
6601	$7 \cdot 32 \cdot 41$
8911	$7 \cdot 19 \cdot 67$
41041	$7 \cdot 11 \cdot 13 \cdot 41$
825265	$5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
413631505	$5 \cdot 7 \cdot 17 \cdot 73 \cdot 89 \cdot 107$

2. Вторая проблема состоит в том, что даже, если непосредственное обращение теоремы Ферма верно, это дает не так уж много, поскольку проверка условия $a^n - a \equiv 0(mod\, n)$ для всех целых $a(mod\, n)$ почти необозрима, даже для n средних размеров.

Как решать эти проблемы ?

Первая проблема решается использованием более утонченных версии теоремы Ферма, которые допускает обращение. Мы приведем два примера. Первое – алгебраическое обобщение теоремы Ферма.

Теорема. n – простое $\Rightarrow (a+b)^n = a^n + b^n(mod\, n), \quad \forall a, b \in \mathbf{Z}$.

Пусть n – нечетное. Прежде чем дать теоретико-числовое обобщение теоремы Ферма мы напомним, что символ Якоби $\left(\frac{a}{n}\right) \in \{1, -1\}$ для $a \in \mathbf{Z}, \text{НОД}(a, n) = 1$ определяется так

$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}(mod\, n)$, если n – простое ,
$\left(\frac{a}{n}\right) \equiv \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right)$, если $n = p_1 \cdots p_r$, где p_i – простые числа ,
$\left(\frac{a}{b}\right) = 0$, если $\text{НОД}(a, b) \neq 1$,
$\left(\frac{a}{1}\right) = 1$, для всех $a \in \mathbf{Z}$.

Символ Якоби изучается в теории Гаусса. Теория базируется на квадратичном законе взаимности. Мы не будем приводить этот закон, но отметим одно следствие: используя закон взаимности можно эффективно вычислить $\left(\frac{a}{b}\right)$, даже если разложение n на простые сомножители неизвестно.

Из определения символа Якоби вытекает следующее формулировка теоремы Ферма.

Теорема.

$$n\text{– простое } \Rightarrow a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(mod\, n) \text{ для любого } a \in \mathbf{Z} \text{ такого, что НОД}(a,n) = 1.$$

Даже для больших a и n с помощью компьютера можно легко проверить выполнено ли условие $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(mod\, n)$.

В 1976 году Д.Н. Лехмер доказал, что обращение этой теоремы верно.

Теорема. Если n нечетное составное число, то $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right)(mod\, n)$, по крайней мере для половины всех $a \in \{1, 2, \ldots, n-1\}$, взаимно простых с n.

Таким образом, решение проблемы 1 можно считать удовлетворительным.

Проблема 2 все еще остается: нет вычислительно осуществимых проверок для всех $a(mod\, n)$. Первый предлагаемый метод, чтобы решить эту проблему — вероятностный метод. Он состоит в следующем. Выберем 100 случайных значении из множества $\{1, 2, \ldots, n-1\}$ и проверим для них условие

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) = \pm 1(mod\, n).$$

Если это не верно хотя бы для одного a, то конечно, n – составное. С другой стороны, если это верно для всех выбранных наугад 100 чисел a, то n имеет большую вероятность чтобы быть простой.

Чтобы убедиться в этом, предположим, что n – не простое. По теореме Лехмера для всякого фиксированного a вероятность вышеприведенного сравнения $\leq 1/2$, поэтому вероятность выполнения сравнения для всех 100 чисел

$$\leq (1/2)^{100} < 0.\underbrace{00000000000000000000000000001}_{30 \text{ цифр}}.$$

Поэтому очень трудно совневаться в простоте n.

Этот метод в основном был предложен Р. Соловеем и В. Штрассеном. Как видим, в математическом смысле он неспособен давать строгие доказательства простоты. С другой стороны он очень быстр и может быть применен прежде чем использовать другие методы пожирающие много времени.

Следующий метод решения проблемы 2 является футуристическим, поскольку он зависит от недоказанной гипотезы – от обобщенной гипотезы Римана. Это утверждение касается распеделению нулей некоторых комплексных функции. Исходя из этой гипотезы Г.Л. Миллер в 1976 году доказал, что в вышеприведенном тесте можно рассматривать только такие a, что

$$a < 70(\log n)^2, \quad a\text{– простое.}$$

Если для всех таких a выполнено условие $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)(mod\, n)$, то используя обобщенную гипотезу Римана можно доказать, что n простое. Этот метод имеет два недостатка. Первое, грубые оценки показывают, что для чисел имеющие около 100 цифр, метод работает примерно 500 раз медленнее чем обсуждаемые методы,хотя для достаточно больших n он работает быстрее. Второй недостаток метода: он основан на недоказанном утверждении – на гипотезе Римана.

3.15.2 Простые числа, состоящие из одних единиц

Число, состоящая из одинаковых цифр делится на эту цифру. Поэтому такое число является простым в том и только в том случае, когда эта цифра равна 1. Пусть a_n число, состоящая из n единиц.

Нижеприведенная программа, написанная в системе MAPLE позволяет вычислять простые числа вида a_n.

```
units:=proc(s)
local n,k; n:=1; k:=1;
while k<s do
n:=n*10+1;
k:=k+1;
if isprime(k) and isprime(n) then print(‘n‘=n, ‘length‘=k)
end if
end do;
print(‘finish‘)
end proc
```

Обращение к этой процедуре дает такой результат. Число состоящее из $k \leq 1200$ единиц – простое только в следующих пяти случаях:

$$k = 2, 19, 23, 317, 1031.$$

Существуют бесконечно много составных чисел, состоящие из одних единиц. Этот факт вытекает из следующей теоремы.

Теорема. Для любого натурального n, взаимно простого с 10, существует число, состоящее из не более чем n единиц, которое делится на n.

Доказательство. Допустим, что ни одно из n чисел $a_1, a_2, \ldots, a_n$ не делится на n. Поскольку остатки чисел $a_1, a_2, \ldots, a_n$ от деления на n лежат в $(n-1)$-элементном множестве $\{1, 2, \ldots, n-1\}$, по принципу Дирихле найдутся по крайней мере два числа a_k и a_s, $s < k$, такие, что их разность

$$a_k - a_s = a_{k-s} \cdot 10^s$$

делится на n. Так как числа 10 и n взаимно просты, это означает, что число a_{k-s} делится на n.

Неизвестно, существуют ли бесконечно много простых чисел вида a_n.

3.15.3 Бинарный метод возведение в степень.

Дадим способ вычисления a^N по модулю m. Он понадобится в криптосистемах с открытым ключом, об чем будет идти речь в следующей секции.

Любое натуральное число a можно представить в в виде

$$a = \sum_{i=0}^{k} a_i n^i,$$

где

$$0 \le a_i < n, \quad i \ge 0,$$

причем такое представление единственно. Последовательность $(a_k \cdots a_1 a_0)_n$ или кратко $a_k \cdots a_1 a_0$ называется n-адичной записью числа a.

Пример. Пусть $a = 3602$. Тогда $a = 3 \cdot 10^3 + 6 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0$. Поэтому 3602 – десятичная запись числа a.

Пример. Пусть $a = 3602$. Тогда $a = 1 \cdot 5^5 + 3 \cdot 5^3 + 4 \cdot 5^2 + 2$ и 103402 – 5-ичная запись числа a.

Пример. Пусть $a = 3602$. Тогда $a = 1 \cdot 2^{11} + 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^4 + 1 \cdot 2^1$ и 111000010010 – двоичная запись числа a.

Как найти n-адичную запись числа a? Повторим алгоритм деления с остатком:

$$a = nq_0 + r_0, \quad 0 \le r_0 < n,$$

$$q_0 = nq_1 + r_1, \quad 0 \le r_1 < n,$$
$$q_1 = nq_2 + r_2, \quad 0 \le r_2 < n,$$
$$\vdots$$
$$q_{k-2} = nq_{k-1} + r_{k-1}, \quad 0 \le r_{k-1} < n,$$
$$q_{k-1} = nq_k.$$

Тогда $r_{k-1} r_{k-2} \cdots r_1 r_0$ и есть n-адичная запись числа a.

Пример.

$$3602 = 2 \cdot 1801 + 0, \quad r_0 = 0,$$
$$1801 = 2 \cdot 900 + 1, \quad r_1 = 1,$$
$$900 = 2 \cdot 450 + 0, \quad r_2 = 0,$$
$$450 = 2 \cdot 225 + 0, \quad r_3 = 0,$$
$$225 = 2 \cdot 112 + 1, \quad r_4 = 1,$$
$$112 = 2 \cdot 56 + 0, \quad r_5 = 0,$$
$$56 = 2 \cdot 28 + 0, \quad r_6 = 0,$$
$$28 = 2 \cdot 14 + 0, \quad r_7 = 0,$$
$$14 = 2 \cdot 7 + 0, \quad r_8 = 0,$$
$$7 = 2 \cdot 3 + 1, \quad r_9 = 1,$$
$$3 = 2 \cdot 1 + 1, \quad r_{10} = 1,$$
$$1 = 2 \cdot 0 + 1, \quad r_{11} = 1.$$

Итак, двоичная запись числа 3602 есть 111000010010.

Запишем N в двоичной системе счисления: $N = \sum_{i=0}^{k} N_i 2^i$. Заменим в последовательности $N_k \cdots N_1 N_0$ каждую цифру 1 на пару букв SM_a и каждую цифру 0 на S после этого вычеркнем пару букв SM_a слева. Получившаяся последовательность

букв будем интерпретировать как способ вычисления a^k, полагая S как "возведение в степень 2 и взять остаток по модулю m" и M_a как " умножение на a и взять остаток по модулю m."

Пример. Вычислить 165^5 по модулю $N = 221$.

Решение. Двоичная представление числа 5 равно 101. Ему соответствует последовательность $SM_{165}SSM_{165}$. Выбросив левую SM_{165}, получаем последовательность SSM_{165}. Тогда

$$165^5 = ((165)^2)^2 \cdot 165.$$

В $\mathbf{Z}_{221}$ имеем

$$165^2 = 42, \qquad 42^2 = 217, \qquad 217 \cdot 165 = 3.$$

Ответ. $165^5 \equiv 3 (mod\, 221)$.

3.15.4 Криптосистема с открытым ключом

Мы видим, как древняя наука о простых числах остается очень привлекательной и для суперсовременных технологии. Она нужна не только для того, чтобы испытывать мощности новых компьютеров. Приведем в заключение еще одно применение обсуждаемого круга вопросов в построении криптосистем с открытым ключом.

Предположим, что отправителю нужно отправить сообщение (целое число x такое, что $0 < X < N$) получателю. Для этого получатель делает общедоступными два числа: N и e (открытый ключ), которые подчинены двум условиям:

- $N = pq$, где p и q – большие простые числа, которые B держит в секрете.
- число $e \in \mathbf{N}$ берется взаимно простым с $\phi(N) = (p-1)(q-1)$.

Отправитель передает вместо x число $E(x) = x^e (mod\, N)$. Это и есть зашифрованное сообщение, которое отправляется получателю.

Чтобы восстановить исходное сообщение, получатель поступает так:

- находит $d \in \mathbf{N}$ такое, что $1 \leq d \leq N-1$ и $ed \equiv 1 (mod\, \phi(N))$. Это сравнение разрешимо единственным образом, поскольку e взаимно прост с $\phi(N)$). Для решения сравнения $ed \equiv 1 (mod\, \phi(N))$ получатель должен вычислить $\phi(N)$, что для него не составит труда, так как $\phi(N) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.
- далее, имея в распоряжение число $y = E(x)$, получатель вычисляет $D(y) = y^d (mod\, N)$, которое и есть исходное число . Действительно, по теореме Эйлера,

$$y^d \equiv x^{ed} \equiv x^{\phi(N)k+1} \equiv (x^{\phi(N)})^k x \equiv x (mod\, N).$$

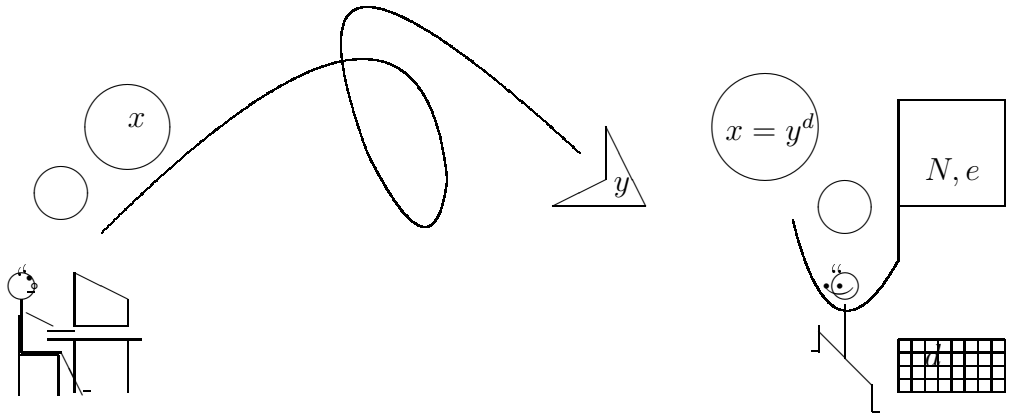
Что же получаем в итоге ? Отправителю нет необходимости знать сомножители p и q, т.е., ему не нужно знать метод дешифровки. Получатель по полученному сообщению легко восстанавливает исходный текст. Туго придется злоумышленнику, который хочет раскрыть исходное сообщение. Он вынужден находить сомножители p и q, а эта задача, как мы отмечали выше имеет большую вычислительную

сложность. Итак, при шифровке с открытым ключом сообщение отправителя в принципе может быть раскрыто, но не сразу. Если есть срок актуальности сообщения и раскрытие может произойти после этого срока, то отправителю и получателю выгодно пользоваться этим методом.

Полученная криптосистема носит название *криптосистемы с открытым ключом.*

Функция $f : X \to Y$ называется односторонней функцией, если $f(x)$ легко вычисляется при любом $x \in X$, в то время как $f^{-1}(y)$ не поддается вычислению почти для всех $y \in Y$. Односторонняя функция называется *односторонней функции с секретом* (иногда она называется функцией с закрытыми дверьми), если обратная функция также легко вычислима, но узнать ее сразу по f невозможно: до тех пор, пока вам не сообщат, что функция обратная f существует и не покажут, f воспринимается как односторонняя функция.

Идею построения односторонней функции с секретом, лежащей на основе криптосистем с открытым ключом высказали в 1975 году Уитфилд Диффи и Мартин Хэллмэн - два инженера-электрика из Станфордского университета, а также Рольф Меркль, бывший в то время студентом Калифорнийского университета. Эту идею впервые воплотили в жизнь Райвсет, Шамир и Адельман в 1978. Метод шифровки и расшифровки, о которых мы рассказывали выше в этой секции и есть их достижение. Ныне этот метод широко известен под названием RSA-метода (по первым буквам имен авторов).



RSA-шифровальная схема

Сообщите всем желающим N и e (*открытый ключ*).
Храните в тайне p, q, d (*закрытый ключ*)

Здесь $N = pq$, НОД$(e, \phi(N)) = 1, ed \equiv 1 (mod\, \phi(N))$ и p, q – простые числа.

Шифровка: $y \equiv x^e (mod\, N)$.
Дешифровка: $x \equiv y^d (mod\, N)$.

Пример. Допустим, что $N = 4294967297$ и $e = 19$. Допустим, что получено сообщение $y = 2$. Найти исходное сообщение x.

Прежде чем приступать к решению задачи, скажем несколько слов откуда взяты числа N и e и почему $\phi(N)$ и e взаимно просты. Будем думать, что злоумышленник не посещает наши лекции и не читает нашу книжку.

Заметим, что пятое число Ферма

$$N = 2^{2^5} + 1 = 4294967297$$

не является простым:

$$4294967297 = 641 \cdot 6700417.$$

Поэтому,

$$\phi(2^{2^5} + 1) = (641 - 1)(6700417 - 1) = 4288266240.$$

Ясно, что $\phi(N)$ делится на большую степень числа 2, именно на 2^{14}. Нетрудно проверить, что $\phi(N)/2^{14}$ разлагается в произведение трех простых чисел

$$\phi(N)/2^{14} = 3 \cdot 5 \cdot 17449.$$

Итак,

$$\phi(N) = 4288266240 = 2^{14} \cdot 3 \cdot 5 \cdot 17449$$

– каноническое разложение. В частности, числа $\phi(N)$ и e взаимно просты.

Решение. Представим $\phi(N)/e$ в виде цепной дроби:

$$\frac{4288266240}{19} = 225698223 + \frac{1}{6 + \dfrac{1}{3}}.$$

Поэтому

$$\delta_0 = 225698223,$$

$$\delta_1 = 225698223 + \frac{1}{6} = \frac{1354189339}{6},$$

и

$$k = 2, P_1 = 1354189339, Q_1 = 6.$$

Значит,

$$19 \cdot 1354189339 - 6 \cdot 4288266240 = 1.$$

Другими словами, в качестве d, обратного к 19 по модулю $\phi(N)$ можем взять

$$d = 1354189339.$$

Заметим, что $d = d_1 \cdot d_2$, где

$$d_1 = 8689, d_2 = 155851.$$

Имеем

$$2^{d_2} \equiv 2048 (mod\, N),$$

$$2048^{d_1} \equiv 134217728 (mod\, N).$$

Следовательно,

$$x = 2^d = 134217728(mod\, N).$$

Ответ: $x = 134217728$.

Пример. Студент получил сообщение $y = 3$ зашифрованное с помощью открытых ключей $N = 221, e = 5$. Расшифровать это сообщение.

Решение. Имеем

$$N = 221 = 13 \cdot 17.$$

Поэтому

$$\phi(221) = (13 - 1)(17 - 1) = 192.$$

Заметим, что

$$192 = 2^6 \cdot 3.$$

Напомним, китайскую теорему об остатках. Она утверждает, что если

$$M = m_1 \cdots m_n,$$

$$M_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_n,$$

и x_i – решение сравнения

$$x_i M_i \equiv 1(mod\, m_i),$$

то

$$x = \sum_{i=1}^{n} x_i b_i$$

– решение системы сравнении

$$x \equiv b_i(mod\, m_i), \quad i = 1, \ldots, n.$$

Применим эту теорему для нахождения $d = e^{-1}$ – обратного к e по модулю $\phi(N)$.

Заметим, что

$$5^{-1} \equiv 2(mod\, 3),$$

$$5^{-1} \equiv 13(mod\, 64),$$

поэтому систему сравнении

$$ed \equiv 1(mod\, 64),$$
$$ed \equiv 1(mod\, 3).$$

можно переписать так

$$d \equiv 13(mod\, 64),$$
$$d \equiv 2(mod\, 3).$$

Теперь все готово к применению китайской теоремы об остатках:

$$m_1 = 64,\ m_2 = 3,\ M = 64 \cdot 3 = 192,\ M_1 = 3,\ M_2 = 64,$$

и сперва мы должны решить сравнения

$$3x_1 \equiv 1(mod\, 64), 64x_2 \equiv 1(mod\, 3).$$

Очевидно, что

$$x_1 \equiv -21 (mod\, 64).$$

Поскольку $64 \equiv 1 (mod\, 3)$, то

$$x_2 \equiv 1 (mod\, 3).$$

Поэтому

$$x = -21 \cdot 13 \cdot 3 + 1 \cdot 2 \cdot 64 = -691 \equiv 77 (mod\, 192),$$

Итак,

$$d = 77.$$

Двоичная запись числа 77 равно 1001101, поскольку

$$77 = 64 + 8 + 4 + 1 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^0.$$

Поэтому числу 77 соответствует последовательность $SM_3SSSM_3SM_3SSM_3$. Вычеркнем левую часть SM_3, получим последовательность $SSSM_3SM_3SSM_3$. Итак,

$$3^{77} = ((((((3^2)^2)^2 \cdot 3)^2 \cdot 3)^2)^2) \cdot 3.$$

Выполним в $\mathbf{Z}_{221}$ эти операции

$$3^2 = 9,\ 9^2 = 81,\ 81^2 = 152,\ 152 \cdot 3 = 14,\ 14^2 = 196,\ 196 \cdot 3 = 146,$$

$$146^2 = 100,\ 100^2 = 55,\ 55 \cdot 3 = 165.$$

Итак,

$$3^{77} \equiv 165 (mod\, 221),$$

и расшифрованное сообщение

$$x = 165.$$

Проверка: как было показано выше в примере $165^5 \equiv 3 (mod\, 221)$.
Ответ: $x = 165$.

3.15.5 Электронная подпись

?????

Глава 4

Алгебраические структуры

4.1 Расстановки скобок

Допустим, что на множестве A задана бинарная операция. Иначе говоря, любым двум элементам $a, b \in A$ сопоставлен однозначно определенный элемент из A, которого будем обозначать через ab и называть произведением элементов a и b. Итак, задана функция: $A \times A \to A, \quad (a, b) \mapsto ab$.

В этой секции нас интересует вопрос:

Сколькими способами можно расставить скобки между буквами $a_1, a_2, \ldots, a_k$ (переставлять буквы запрещено) так, чтобы однозначно можно было вычислить их произведение ?

Обозначим через α_n количество способов расстановок скобок на n буквах. Положим, по определению,

$$\alpha_1 = 1.$$

Пример. $\alpha_2 = 1, \alpha_3 = 2, \alpha_4 = 5$. Действительно, имеются только следующие расстановки скобок:

$$n = 2, \quad (a_1 a_2),$$

$$n = 3, \quad (a_1 a_2)a_3, a_1(a_2 a_3),$$

$$n = 4, \quad ((a_1 a_2)a_3)a_4,\ (a_1(a_2 a_3))a_4,\ (a_1 a_2)(a_3 a_4),\ a_1((a_2 a_3)a_4),\ a_1(a_2(a_3 a_4)).$$

Теорема.

$$\alpha_{n+1} = \frac{1}{n+1}\binom{2n}{n}, \quad n \geq 0.$$

Это число называется числом *Каталана.*

Доказательство. Допустим, что α_k известны для всех $k = 1, 2, \ldots, n-1$. Тогда мы умеем расставлять скобки на множестве $\{a_1, \ldots, a_k\}$ (таких способов – α_k) и на множестве $\{a_{k+1}, \ldots, a_n\}$ (таких способов – α_{n-k}). Поэтому по правилу произведения имеются $\alpha_k \alpha_{n-k}$ таких способов расстановок скобок. Поскольку k пробегает все значения $1, 2, \ldots, n-1$, по правилу суммы получаем, что

$$\alpha_n = \sum_{i=1}^{n-1} \alpha_i \alpha_{n-i}, \quad n > 1. \tag{4.1}$$

Напомним, что по определению,

$$\alpha_1 = 1.$$

Пусть

$$G(\alpha) = \sum_{i \geq 1} \alpha_i x^i$$

– производящая функция для последовательности α_n. Из формулы (4.1) следует, что

$$G(\alpha)G(\alpha) =$$

$$(\sum_{i \geq 1} \alpha_i x^i)(\sum_{j \geq 1} \alpha_j x^j) = \sum_{i,j \geq 1} \alpha_i \alpha_j x^{i+j}$$

$$= \sum_{n \geq 2} (\sum_{i=1}^{n-1} \alpha_i \alpha_{n-i}) x^n = \sum_{n \geq 2} \alpha_n x^n = \sum_{n \geq 1} \alpha_n x^n - \alpha_1 x =$$

$$G(\alpha) - x.$$

Итак, мы получили квадратное уравнение

$$G(\alpha)^2 - G(\alpha) + x = 0.$$

Это уравнение имеет два решения

$$G(\alpha) = \frac{1 \pm \sqrt{1 - 4x}}{2}. \tag{4.2}$$

Вычислим $(1 - 4x)^{1/2}$ с помощью формулы

$$(1 + t)^m = \sum_{i \geq 1} \binom{m}{i} t^i.$$

Напомним, что здесь m необязательно целое и биномиальный коэффициент $\binom{m}{i}$, где $i \in \mathbf{Z}^+$, понимается так

$$\binom{m}{i} = \frac{m(m-1)\cdots(m-i+1)}{i!}.$$

Сначала разберемся какой знак следует брать в формуле (4.2). Так как функция $G(x)$ не имеет свободных членов, и свободный член ряда $(1 - 4x)^{1/2}$ равен 1, чтобы свободные члены сократились, очевидно, здесь следует брать знак минус. Итак,

$$G(\alpha) = \frac{1 - \sqrt{1 - 4x}}{2} = \sum_{i \geq 1} -\frac{1}{2} \binom{1/2}{i} (-4x)^i.$$

Введем в рассмотрение двойные факториалы:

$$(2i - 1)!! = 1 \cdot 3 \cdot 5 \cdots (2i - 1)$$

$$(2i)!! = 2 \cdot 4 \cdots (2i)$$

– соответственно, произведения всех нечетных чисел от 1 до $2i-1$ и четных чисел от 2 до $2i$.

Имеем,

$$(-1)^{i+1}\binom{1/2}{i}\frac{4^i}{2} = (-1)^{i+1}\frac{1/2(1/2-1)\cdots(1/2-i+1))}{i!}\frac{4^i}{2} =$$

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

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

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

$$\frac{(2i-1)!!(2(i-1))!!}{(i-1)!i!} =$$

$$\frac{1}{i}\binom{2(i-1)}{i-1}.$$

Таким образом,

$$G(\alpha) = \sum_{n\geq 1}\frac{1}{n}\binom{2(n-1)}{n-1}x^n.$$

В частности,

$$\alpha_n = \frac{1}{n}\binom{2(n-1)}{n-1}, \quad n\geq 1,$$

что и требовалось доказать.

4.1.1 Коммутативные расстановки скобок

???

4.1.2 Ассоциативные расстановки скобок

???

4.1.3 Задачи

4.2 Группа

Чтобы определить группу нужно задать четыре вещи:

- множество G
- умножение $\circ$ (бинарное операция)
- единица e (0-арная операция)

- $f : G \to G, \quad a \mapsto f(a)$ (унарная операция)

Умножение – бинарная операция на G. Единица – некоторый выделенный элемент множества G. Единицу иногда называют нейтральным элементом. Четверка $(G, \circ, e, f)$ (или кратко G) называется группой, если выполнены следующие условия

$$a \circ (b \circ c) = (a \circ b) \circ c, \forall a, b, c \in G \text{ (ассоциативность)}$$

$$a \circ e = e \circ a = a, \quad \forall a \in G \text{ (единица)}$$

$$a \circ f(a) = e, \quad \forall a \in A.$$

Последнее условие обычно переписывается так:

$$\forall a \in G \quad \exists b \in G, \quad \text{такой, что } a \circ b = e.$$

Элемент $f(a)$ называется обратным элементом и обычно обозначается так: a^{-1} или $-a$.

Абелева группа – группа с тождеством $a \circ b = b \circ a$ для всех $a, b \in G$.

Пример. Пусть $G = \mathbf{Z}, a \circ b = a + b, e = 0$. Тройка $(\mathbf{Z}, +, 0)$ (или кратко $\mathbf{Z}$) образует абелеву группу.

Пример. Z относительно умножения $a \cdot b$ не образует группу $(\mathbf{Z}, \cdot, 1)$

Пример. Множество невырожденных матриц $GL_n = \{X \in Mat_n | det\, X \neq 0\}$ относительно умножения матриц и единицы $E = (\delta_{i,j})$ (единичная матрица) образует неабелеву группу.

Пример. Пусть X – конечное множество и $\mathcal{F}(X, X)$ – множество взаимно-однозначных функции на множестве X. Пусть $id \in \mathcal{F}(X, X)$ тождественная функция:

$$id(x) = x, \qquad \forall x \in X.$$

Напомним, что композиция функции $f \cdot g$ определяется по правилу

$$f \cdot g(x) = f(g(x)), \qquad f, g \in \mathcal{F}(X, X).$$

Тогда множество $A = \mathcal{F}(X, X)$ образует группу относительно следующих операции:

- операции композиции
- единицы $e = id$
- и относительно операции взятия обратной функции.

Перестановка – взаимно-однозначная функция на множестве из элементов. Как правило, в качестве этого множества берут множество чисел от 1 до n.

Множество перестановок $G = S_n$ относительно операции умножения перестановок $a \circ b$ и относительно элемента

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

образует группу.

Определения. Подмножество $H \subseteq G$ называется подгруппой группы G, если $a \circ b \in H$ для любых $a, b \in H$. Обозначение: $H \leq G$.

Подгруппа $H \leq G$ называется нормальным делителем, если $a \circ h \circ a^{-1} in H$ для любых $a \in G$ и $h \in H$. Обозначение: $H \trianglelefteq G$.

Пусть G и F– группы относительно умножении $\circ$ и $\star$. Функция $\alpha : G \to F$ называется гомоморфизмом, если

$$\alpha(a \circ b) = \alpha(a) \star \alpha(b), \qquad \forall a, b \in G.$$

Ядро гомоморфизма определяется как:

$$Ker\,\alpha = \{a \in G | \alpha(a) = e\}.$$

где e единица в группе F.

Предложение. Пусть G и H группы и $\alpha : G \to F$ – гомоморфизм групп. Тогда $Ker\,\alpha$ – нормальный делитель группы G.

Доказательство. Справедливы импликации

$$a, b \in Ker\,\alpha \Rightarrow \alpha(a) = e, \alpha(b) = e \Rightarrow$$

$$\alpha(a \circ b) = \alpha(a) \star \alpha(b) = e \star e = e \Rightarrow a \circ b \in Ker\,G.$$

Другими словами, $Ker\,\alpha$ – подгруппа группы G. Далее,

$$a \in Ker\,\alpha, b \in G \Rightarrow \alpha(a) = e \Rightarrow \alpha(b \circ a \circ b^{-1}) = \alpha(b) \star \alpha(a) \star \alpha(b)^{-1} =$$

$$\alpha(b) \star e \star \alpha(b)^{-1} = \alpha(b) \star \alpha(b)^{-1} = e \Rightarrow b \circ a \circ b^{-1} \in Ker\,G.$$

Итак, $Ker\,\alpha$ – нормальный делитель группы G.

Определение. Инъективный гомоморфизм называется вложением (или мономорфизмом). Сюръективный гомоморфизм называется наложением (или эпиморфизмом).

Теорема(Кэли). Для любой группы G порядка n существует вложение $G \to S_n$.

Доказательство. Для любого $a \in G$ определим функцию $L_a : G \to G$ по правилу

$$L_a(b) = a \circ b.$$

Тогда

$$L_{a \circ b}(c) = (a \circ b) \circ c = a \circ (b \circ c) = a \circ L_b(c) = L_a(L_b(c)).$$

Иными словами,

$$L_{a \circ b} = L_a \cdot L_b,$$

где $\cdot$ обозначает композицию функций. Заметим, что

$$L_a = id \Rightarrow L_a(b) = b, \quad \forall b \in G \Rightarrow a \circ b = b \Rightarrow a = e.$$

Итак, отображение

$$G \to \mathcal{F}(G, G), \quad a \mapsto L_a$$

задает инъективный гомоморфизм группы G в группу функции $\mathcal{F}(G, G)$.

Другими словами, любая конечная группа изоморфна подгруппе группы перестановок. Заметим, что тут условие конечности группы несущественна.

Порядок элемента $a \in G$ это такое число m, что $a^m = e$, но $a^{m-1} \neq e$.

Порядок группы – количество ее элементов .

Циклическая группа – группа порожденная одним элементом.

Предложение. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Доказательство.

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = (a \circ (b \circ b^{-1})) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e.$$

Класс смежности (левый класс смежности) относительно подгруппы $H \leq G$ – подмножество группы G вида $a \circ H = \{a \circ h | h \in H\}$.

Правый класс смежности относительно подгруппы $H \leq G$ – подмножество группы G вида $H \circ a = \{h \circ a \,|\, h \in h\}$.

Легко видеть, что если $H \trianglelefteq G$ – нормальный делитель, то правые и левые смежные классы совпадают.

Пример. Пусть

$$S_3 = \left\{ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \right.$$

$$\left. a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, a_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, a_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

– группа перестановок на трех элементах. Группа S_3 имеет подгруппу порядка 2

$$H = \{e, a_1\}.$$

Относительно этой подгруппы смежные классы таковы:

Левые смежные классы	Правые смежные классы
$e \circ H = \{e, a_1\}$	$H \circ e = \{e, a_1\}$
$a_2 \circ H = \{a_2, a_5\}$	$H \circ a_2 = \{a_2, a_4\}$
$a_3 \circ H = \{a_3, a_4\}$	$H \circ a_3 = \{a_3, a_5\}$

Мы видим, что левые и правые смежные классы разные, поэтому H не является нормальным делителем в S_3.

Пример. Группа S_4 имеет подгруппу

$$H = \left\{ e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, b_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, b_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, b_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}.$$

Левые и правые смежные классы относительно H одинаковы:

??????

Поэтому H – нормальный делитель в S_4.

Теорема (Лагранж). Пусть G конечная группа и $H \leq G$ – ее подгруппа. Тогда порядок подгруппы $|H|$ является делителем порядка группы $|G|$.

Доказательство. Определим отношение R в группе G по правилу aRb, если $a \circ b^{-1} \in H$. Тогда R отношение эквивалентности. Действительно,

$$aRa, \text{ поскольку } a \circ a^{-1} = e \in H$$

(рефлексивность),

$$aRb \Rightarrow a \circ b^{-1} \in H \Rightarrow (a \circ b^{-1})^{-1} \in H \Rightarrow b \circ a^{-1} \in H \Rightarrow bRa$$

(симметричность),

$$aRb, bRc \Rightarrow a \circ b^{-1} \in H, b \circ c^{-1} \in H \Rightarrow a \circ c^{-1} = (a \circ b^{-1}) \circ (b \circ c^{-1}) \in H \Rightarrow aRc$$

(транзитивность).

Класс эквивалентности относительно этого отношения эквивалентности, как мы определяли выше, называется правым классом смежности. Пусть $H \circ g_1, \ldots, H \circ g_k$ – непересекающиеся классы смежности. Группу G можно представить в виде объединения непересекающихся классов смежности:

$$G = \cup_{i=1}^{k} H \circ g_i.$$

Заметим, что

$$|H \circ g| = |H|,$$

для любого $g \in G$. Действительно,

$$h \circ g = h_1 \circ g, \quad h, h_1 \in H \Rightarrow h = (h_1 \circ g) \circ g^{-1} = h_1.$$

Таким образом,

$$|G| = \sum_{i=1}^{k} |H \circ g_i| = |H|k,$$

и

$$|G|/|H| \in \mathbf{Z}.$$

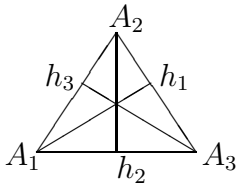
Следствие. Любая группа порядка p, где p – простое число, является циклической.

Доказательство. Пусть $a \in G$ произвольный элемент отличный от e. Рассмотрим подгруппу, порожденную элементом a. По теореме Лагранжа ее порядок является делителем p. Поскольку $a \neq e$, этот порядок больше 1. Значит, порядок элемента a равен p. Другими словами, группа G порождается одним элементом. Это означает, что G – циклическая.

Замечание. Утверждение, обратное к теореме Лагранжа не верно. Если d – делитель порядка G, то это не значит, что G имеет подгруппу порядка d. Например, знакопеременная группа A_4 порядка 12 не имеет подгруппы порядка 6.

Пример. Группа симметрии правильного треугольника.

Занумеруем вершины правильного треугольника цифрами $1, 2, 3$. Пусть h_1, h_2, h_3 – высоты опущенные из вершин $1, 2, 3$.



Симметрия многоугольника – взаимно-однозначное отображение вершин многоугольника в себя сохраняющее многоугольник.

Правильный треугольник имеет шесть симметрии:

$$\phi_1 = \text{ тождественное преобразование,}$$

$$\phi_2 = \text{ поворот вокруг центра против часовой стрелки на угол } 2\pi/3$$

$$\phi_3 = \text{ поворот вокруг центра против часовой стрелки на угол } 4/pi/3,$$

$$\theta_1 = \text{ отражение относительно высоты } h_1,$$

$$\theta_2 = \text{ отражение относительно высоты } h_2,$$

$$\theta_3 = \text{ отражение относительно высоты } h_3.$$

Пусть G – множество симметрии правильного треугольника. Зададим на множестве G бинарную операцию – композицию функции.

Проверим например, что

$$\phi_2 \circ \theta_1 = \theta_2.$$

Имеем,

$$\phi_2 \circ \theta_1(A_1) = \phi_2(\theta_1(A_1)) = \phi_2(A_1) = A_3,$$
$$\phi_2 \circ \theta_1(A_2) = \phi_2(\theta_1(A_2)) = \phi_2(A_3) = A_2,$$
$$\phi_2 \circ \theta_1(A_3) = \phi_2(\theta_1(A_3)) = \phi_2(A_2) = A_1,$$

Поскольку

$$\theta_2(A_1) = A_3,$$
$$\theta_2(A_2) = A_2,$$
$$\theta_2(A_3) = A_1,$$

это означает, что $\phi_2 \circ \theta_1 = \theta_2$. Аналогичным образом можно вычислить все попарные произведения элементов множества G. Полученная таблица умножении называется таблицей Кэли.

Мы знаем, что композиция функции – ассоциативная операция. Тождественное преобразование соответствует единице. Взаимно-однозначные функции имеют обратные функции относительно композиции. Таким образом, множество симметрии G относительно операции композиции и единицы $e = \phi_1$ образует группу.

Таблица Кэли для группы симметрии правильного треугольника

$\circ$	ϕ_1	ϕ_2	ϕ_3	θ_1	θ_2	θ_3
ϕ_1	ϕ_1	ϕ_2	ϕ_3	θ_1	θ_2	θ_3
ϕ_2	ϕ_2	ϕ_3	ϕ_1	θ_2	θ_3	θ_1
ϕ_3	ϕ_3	ϕ_1	ϕ_2	θ_3	θ_1	θ_2
θ_1	θ_1	θ_3	θ_2	ϕ_1	ϕ_3	ϕ_2
θ_2	θ_2	θ_1	θ_3	ϕ_2	ϕ_1	ϕ_3
θ_3	θ_3	θ_2	θ_1	ϕ_3	ϕ_2	ϕ_1

Пример. Группа симметрии квадрата.

Группа симметрии правильного n-угольника называется группой диэдра и обозначается через D_n. Можно показать, что D_n имеет $2n$ элементов и группа порождается двумя элементами a, b и образующими соотношениями

$$a^n = e, b^2 = e, bab = a^{n-1}.$$

Продемонстируем это наблюдение на примере квадрата $n = 4$.

Квадрат $A_1A_2A_3A_4$ имеет четыре вращении против часовой стрелки:

a_1 – поворот вокруг центра на 0;

a_2 – поворот вокруг центра на $\pi/2$;

a_3 – поворот вокруг центра на π;

a_4 – поворот вокруг центра на $3\pi/2$;

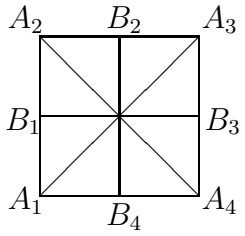
и четыре отражения:

b_1 – отражение относительно середин сторон B_1B_3;

b_2 – отражение относительно диагонали A_2A_4;

b_3 – отражение относительно середин сторон B_2B_4;

b_4 – отражение относительно диагонали A_3A_1;



Можно написать таблицу умножении в терминах этих поворотов и отражении. Мы поступим несколько иначе. Построим группу с помощью образующих и определяющих соотношении.

Возьмем в качестве образующих два элемента $a = a_1, b = b_1$. Тогда все симметрии квадрата можно получить из этих двух элементов с помощью операции умножения. Например, $a_3 = a^3$.

Имеют места следующие соотношения

$$a^4 = e, \quad b^2 = e, \quad b \circ a \circ b = a^3.$$

Проверим, например, последнее соотношение. С одной стороны имеем

$$(b \circ a \circ b)(A_1) = (b \circ a)(b(A_1)) = (b \circ a)(A_2)) = b(a(A_2)) = b(A_1) = A_2,$$

$$(b \circ a \circ b)(A_2) = (b \circ a)(b(A_2)) = (b \circ a)(A_1)) = b(a(A_1)) = b(A_4) = A_3,$$

$$(b \circ a \circ b)(A_3) = (b \circ a)(b(A_3)) = (b \circ a)(A_4)) = b(a(A_4)) = b(A_3) = A_4,$$

$$(b \circ a \circ b)(A_4) = (b \circ a)(b(A_4)) = (b \circ a)(A_3)) = b(a(A_3)) = b(A_2) = A_1.$$

С другой стороны a^3 – поворот на угол $-\pi/2$, т.е.,

$$a^3(A_1) = A_2, \quad a^3(A_2) = A_3, \quad a^3(A_3) = A_4, \quad a^3(A_4) = A_1.$$

Итак, мы проверили, что $b \circ a \circ b = a^3$.

Мы получаем, что $G = \{e, a, a^2, a^3, b, a \circ b, a^2 \circ b, a^3 \circ b\}$. Напишем таблицу умножения. Для упрощения обозначении опустим знаки умножения и вместо $a^i \circ b$ будем писать $a^i b$.

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Прямое произведение двух групп — группа заданная на множестве $G_1 \times G_2$ (декартово произведение) относительно операции умножения

$$(a_1, a_2) \circ (b_1, b_2) = (a_1 \circ_1 b_1, a_2 \circ_2 b_2),$$

где $\circ_1$ и $\circ_2$ – умножения в группах G_1 и G_2.

Пример. Группа Клейна $G = \{a, b \,|\, a^2 = e, b^2 = e, ab = ba\}$ имеет ровно четыре элемента e, a, b, ab. Любое слово построенное из двух букв с помощью наших определяющих соотношении сводится к одному из этих четырех элементов. Например, чему равны слова $abba$ и $bababbaa$? Ответ прост:

$$abba = aea = a^2 = e,$$

$$bababbaa = babaee = baba = baab = beb = bb = e.$$

Таблица умножения в группе Клейна

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Эта группа изоморфна прямому произведению двух циклических групп

$$G \cong \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Изоморфизм $f : G \to \mathbf{Z}_2 \times \mathbf{Z}_2$ можно задать так:

$$f(e) = (0,0),\ f(a) = (0,1),\ f(b) = (1,0),\ f(ab) = (1,1).$$

Здесь $\mathbf{Z}_2 = \{0, 1\}$ понимается как группа вычетов по модулю 2 относительно сложения.

4.2.1 Задачи

1. Проверьте образуют ли следующие множества группу относительно соответствующих операции

- $\mathbf{Z}$ относительно умножения
- $\mathbf{Z}$ относительно вычитания
- $\mathbf{Q}$ относительно сложения
- $\mathbf{Q}$ относительно умножения
- $\mathbf{Q} \setminus \{0\}$ относительно умножения
- $\mathbf{R}$ относительно операции $\circ$ такой, что $a \circ b = a + b + 2$.
- $\mathbf{R} \setminus \{-1\}$ относительно операции $\circ$ определенной по правилу $a \circ b = a + b + ab$.
- множество нечетных чисел относительно умножения

2. Доказать, что группа симметрии правильного треугольника изоморфна группе перестановок S_3.

3. Пусть $G = \mathbf{R} \setminus \{0, -1\}$. Определим шесть функции $f_i : G \to G, i = 1, 2, 3, 4, 5, 6$, определенным по правилам

$$f_1(x) = x, \quad f_2(x) = 1 - x, \quad f_3(x) = \frac{1}{x},$$

$$f_4(x) = \frac{1}{1-x}, \quad f_5(x) = 1 - \frac{1}{x}, \quad f_6(x) = \frac{x}{x-1}.$$

Доказать, что G относительно операции композиции образует группу. Постройте таблицу умножения. Докажите, что полученная группа изоморфна группе перестановок S_3.

4. Доказать, что группа с тождеством $a^2 = e$ абелева.

5. Доказать, что множество $\mathbf{Z}_n^* = \{i \in \mathbf{Z} | 0 < i < n, \text{НОД}(i, n) = 1\}$ образуют группу. Найти ее порядок.

6. Построить таблицу умножения группы $\mathbf{Z}_{30}^*$.

7. Классифицировать все группы порядка не более чем 7.

8. Построить таблицу умножения группы симметрии правильного треугольника.

9. Построить таблицу умножения группы симметрии квадрата.

10. Построить таблицу умножения группы симметрии прямоугольника с разными сторонами.

11. Найти знак перестановок

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix}$

12. Умножить перестановки $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$

13. Пусть $\mathbf{Z}[i] = \{a + bi | a, b \in \mathbf{Z}\}$ – множество Гауссовых чисел. Является ли группа $\mathbf{Z}[i]$ циклической ?

14. Нарисовать таблицу умножения и найти порядок всех элементов в группе $\{\pm 1, \pm i, \pm j, \pm k\}$, где $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$. Эта группа называется группой кватернионов.

15. Построить таблицу умножения порожденной двумя элементами a, b и с порождающими соотношениями $a^4 = e, b^2 = a^2, \quad bab^{-1} = a^{-1}$. Доказать, что эта группа изоморфна группе кватернионов.

16. Пусть G – группа порожденная матрицами $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ относительно умножения матриц. Показать, что неабелева группа порядка 8 . Является ли эта группа изоморфной группе симметрии квадрата или группе кватернионов Q?

17. Показать, что группа диэдра D_n (группа симметрии правильного n-угольника) изоморфна группе порожденной матрицами $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}$ относительно умножения матриц, где комплексные $\eta = e^{\frac{2\pi i}{n}}$ – корни степени n из 1.

18. Найти группы симметрии многочленов

- $(x_1 + x_2)(x_3 + x_4)$
- $(x_1 - x_2)(x_3 - x_4)$
- $(x_1 - x_2)^2 + (x_2 - x_3)^2 + (x_3 - x_4)^2 + (x_4 - x_5)^2$.

19. Построить таблицу умножения порожденной двумя элементами a, b и с порождающими соотношениями $a^3 = b^2 = e, \quad ab = ba^2$.

20. Пусть G – группа и $Z(G) = \{a \in G | ab = ba, \forall b \in G\}$ – ее центр. Доказать, что $Z(G)$ является абелевой подгруппой группы G.

21. Доказать, что любая подгруппа индекса 2 является нормальным делителем.

22. Доказать, что группа перестановок S_4 имеет два нормальных делителя:

- знакопеременная подгруппа A_4 и
- подгруппа, изоморфная группе Клейна
$\{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\}$

23. Доказать, что четные перестановки образуют группу.

24. Найти порядок знакопеременной группы.

4.3 Кольца и поля

Чтобы определить кольцо нужно задать пять вещей:

- множество K
- сложение $+$ (бинарная операция)
- нуль 0 (0-арная операция)
- $f : K \to K$ (унарная операция)
- умножение $\circ$ (бинарная операция)

Пятерка $(K, +, \circ, 0, f)$ (или кратко K) называется кольцом, если выполнены следующие условия:

- $(K, +, 0, f)$ – абелева группа
- $a \circ (b + c) = a \circ b + a \circ c$ (дистрибутивность справа)
- $(a + b) \circ c = a \circ c + b \circ c$ (дистрибутивность слева)

Обычно $f(a)$ называется обратным элементом (относительно аддитивной операции $+$) и обозначается так: $-a$. Если выполнено условие ассоциативности умножения

$$a \circ (b \circ c) = (a \circ b) \circ c, \qquad \forall a, b, c \in K,$$

то кольцо называется ассоциативным. Если выполнено условие существование единицы относительно умножения

$$a \circ e = e \circ a = a, \qquad \forall a \in K,$$

то кольцо называется кольцом с единицей. Если выполнено условие коммутативности умножения

$$a \circ b = b \circ a, \qquad \forall a, b \in K,$$

то кольцо называется коммутативным. Во многих учебниках условия ассоциативности, коммутативности и существование единицы автоматически предполагаются.

Пример. $(\mathbf{Z}, +, \cdot, 0, 1)$ ассоциативное коммутативное кольцо с единицей.

Пример. $(Mat_n, +, \circ, 0, 1)$ образует ассоциативное, но некоммутативное кольцо с единицей. Здесь $X \circ Y$ – обычное умножение матриц, 0 – нулевая матрица и 1 – единичная матрица.

Поле. Ассоциативное коммутативное кольцо с единицей $(K, +, \cdot, 0, 1)$ (или кратко K, когда ясно о каком сложении, умножении и о каких нейтральных элементах 0, 1 идет речь) называется полем, если выполнено условие существование обратного элемента

$$\forall a \in G \quad \exists b \in G, \quad \text{такой, что} \;\; a \cdot b = 1.$$

Пример. Относительно обычных операции сложения, умножения и чисел 0, 1 следующие числовые множества образуют поле: $(\mathbf{Q}, +, \cdot, 0, 1)$, $(\mathbf{R}, +, \cdot, 0, 1)$, $(\mathbf{C}, +, \cdot, 0, 1)$. Относительно сложения и умножения по модулю 2 множество $\mathbf{Z}_2 = \{0, 1\}$ образует поле. Это пример конечного поля.

4.3.1 Задачи

1. Показать, что $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbf{Q}\}$ образует коммутативное кольцо, более того поле, относительно операции умножения и сложения чисел.

2. Пусть $P(X)$ – булеан множества X. Доказать, что $(P(X), \oplus, \cap)$ – кольцо относительно операции симметрической разности $\oplus$ и пересечения $\cap$. Построить таблицы для $\oplus$ и $\cap$ где $X = \{a, b, c\}$.

3. Показать, что отображение $f : P(X) \to \mathbf{Z}_2, \quad f(\emptyset) = \bar{0}, f(X) = \bar{1}$, задает изоморфизм колец, если $|X| = 1$.

4. Показать, что отображение $f : \mathbf{Z}_{24} \to \mathbf{Z}_4, \quad f(x(mod\,24)) = x(mod\,4)$, является гомоморфизмом колец.

5. Построить изоморфизм колец $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$

6. Пусть $(R, +, \cdot)$ – кольцо. Определим новые операции $\oplus$ и $\circ$ на R по правилам

$$r \oplus s = r + s + 1, \quad r \circ s = r \cdot s + r + s.$$

- Доказать, что $(R, \oplus, \circ)$ – кольцо.
- Найти мультипликативные и аддитивные единицы $(R, \oplus, \circ)$.
- Доказать, что кольца $(R, \oplus, \circ)$ и $(R, +, \cdot)$ изоморфны.

7. Разделить многочлен $x^3 + 2x^2 + x + 2$ на многочлен $x^2 + 2$ в кольце $\mathbf{Z}_3[x]$.

8. Найти наибольший общий делитель многочленов $x^4 + x^3 + 3x - 9$ и $2x^3 - x^2 + 6x - 3$ в $\mathbf{Q}[x]$.
Ответ: $-\frac{9}{4}x^2 - \frac{27}{4}$.

9. Доказать, что $\mathbf{Z}_n$ – поле тогда и только тогда, когда n – простое.

10. Проверить, что кольцо Гауссовых чисел $\mathbf{Q}[\sqrt{-3}]$ не обладает свойством однозначности разложения на простые сомножители. Например,

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

4.4 Логика высказывании

Высказывание – предложение, относительно которого имеет смысл говорить, истинно оно или ложно.

Пример. "$\sin^2 x + cos^2 x = 1$" – высказывание, причем истинное высказывание.

Пример. "Есть ли жизнь на Марсе ?" – не высказывание.

Пример. "Алматы - столица Казахстана" – высказывание, именно ложное высказывание.

Пример. "Сделай домашнее задание" – не высказывание.

Операции над высказываниями.

Внизу в таблицах истинности вместо слов "Истина" и "Ложь" будем писать кратно "И" и "Л" или "1" и "0."

Отрицание высказывания $\bar{p}$; оно истинно, если p ложно и наоборот, $\bar{p}$ ложно, если p истинно. Таблица истинности:

p	$\bar{p}$
0	1
1	0

Отрицание формализует частицу "не".

Конъюнкция высказывании $p\&q$ – истинно тогда и только тогда, когда p и q истинны. Таблица истинности:

p	q	$p\&q$
1	1	1
1	0	0
0	1	0
0	0	0

Конъюнкция формализует союз "и".

Дизъюнкция высказывании $p \vee q$ – истинно тогда и только тогда, когда хотя бы одно из высказывании p, q истинно. Таблица истинности :

p	q	$p \vee q$
1	1	1
0	1	1
1	0	1
0	0	0

Дизъюнкция формализует союз "или".

Импликация высказывании $p \to q$ – ложно, тогда и только тогда, когда высказывание q ложно, но p истинно. Таблица истинности :

p	q	$p \to q$
1	1	1
0	1	1
1	0	0
0	0	1

Импликация формализует союз "если, то ". Поэтому импликацию иногда называют условным высказыванием.

С условным высказыванием $p \to q$ связаны еще три типа высказывании:

- $q \to p$ конверсия высказывания $p \to q$
- $\bar{p} \to \bar{q}$ инверсия высказывания $p \to q$
- $\bar{q} \to \bar{r}$ контрапозиция высказывания $p \to q$

Пример. Пусть p и q следующие высказывания:
p = "играет в футбол"
q = "он популярен".
Тогда
$p \to q$="Если он играет в футбол, то он популярен".
Для этой импликации имеем:

конверсия:	Если он популярен, то он играет в футбол
инверсия:	Если он не играет в футбол, то он не популярен
контрапозиция:	Если он не популярен, то он не играет в футбол.

4.5 Булевы функции.

Булевы функции(или функции алгебры логики) – функции аргументы и значения которых принимают значения 0 и 1.

Логические высказывания можно представить себе как булеву функцию, если под 1 понимать истину и под 0 – ложь.

Таблица истинности. Булеву функцию $f(p_1, \ldots, p_k)$ от k аргументов можно задать с помощью таблицы

p_1	p_2	$\cdots$	p_{k-1}	p_k	$f(p_1, \ldots, p_k)$
0	0	$\cdots$	0	0	$f(0, 0, \ldots, 0, 0)$
0	0	$\cdots$	0	1	$f(0, 0, \ldots, 0, 1)$
0	0	$\cdots$	1	0	$f(0, 0, \ldots, 1, 0)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
1	1	$\cdots$	1	1	$f(1, 1, \ldots, 1, 1)$

(строки пробегают всевозможные варианты 0 и 1; количество строк – 2^k). Эта таблица называется таблицей истинности функции $f(p_1, \ldots, p_k)$

Теорема . Существуют 2^{2^n} различных булевых функции с n аргументами.

Доказательство. При построении таблиц истинности мы убедились, что любую булеву функцию от n аргументов можно представить себе как функцию на множестве из 2^n элементов (2^n строк длины n) со значениями в множестве из двух элементов $\{0,1\}$. Мы знаем, что $|\mathcal{F}(A,B)| = m^n$, где $|A| = n, |B| = m$, и $\mathcal{F}(A,B) = \{f : A \to B\}$ – множество функции из A в B. Поэтому множество булевых функции от n аргументов имеет порядок 2^{2^n}.

Тавтология. Булева функция называется тавтологией, если она принимает значение 1 при любых значениях аргументов.

Пример. $p \vee \bar{p}$ – тавтология.

Пример. "Быть или не быть" – тавтология.

Пример. "Если он умен и богат, то он богат " – тавтология

Противоречие. Булева функция называется противоречием, если она принимает значение 0 при любых значениях аргументов.

Пример. $p \wedge \bar{p}$ – противоречие.

Пример. "Он двигается в направлении Алматы и двигается в противоположном направлении " – противоречие.

Логические операции

Имеется две 0-арных булевых функции

- тождественный нуль 0.
- тождественная единица 1.

Существуют 4 унарных булевых функции. Из них два имеют несущественные переменные. Существенные 1-арные булевы функции:

- тождественная функция p
- отрицание $\bar{p}$

Существуют 16 бинарных булевых функции. Из них 9 имеют несущественные переменные. Существенные бинарные булевы функции задаются так:

p	q	$\&$	$\vee$	$\oplus$	$\equiv$	$\to$	$\uparrow$	$\downarrow$
0	0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	1	0	0	1	0
1	1	1	1	0	1	1	0	0

Как отмечали выше некоторые функции имеют специальные названия

- $p\&q$ – конъюнкция (или логическое умножение); читается " p и q "
- $p \vee q$ – дизъюнкция (или логическая сумма); читается " p или q"
- $p \oplus q$ – сумма по модулю 2 (или арифметическая сумма); читается "p плюс q"
- $p \equiv q$ – эквивалентность; читается "p эквивалентно q"
- $p \to q$ – импликация; читается "из p следует q" или "p влечет q"

- $p \uparrow q$ – штрих Шеффера ($\overline{p \wedge q}$); читается " не p и q"
- $p \downarrow q$ – стрелка Пирса ($\overline{p \vee q}$); читается "не p или q"

Эквивалентность формул. Формулы $f(p_1, p_2, \ldots, p_k)$, $g(p_1, p_2, \ldots, p_k)$ эквивалентны , если совпадают их таблицы истинности.

Тождества исчисления высказывании.

- $p \vee p \equiv p, \quad p \wedge p \equiv p$ (идемпотентность)
- $p \vee q \equiv q \vee p, \quad p \wedge q \equiv q \wedge p$ (коммутативность)
- $(p \vee q) \vee r \equiv p \vee (q \vee r), \quad (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ (ассоциативность)
- $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r), \quad (p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ (дистрибутивность)
- $p \vee F \equiv p, \quad p \wedge F \equiv F,$
  $p \vee T \equiv T, \quad p \wedge T \equiv p$ (нейтральность)
- $\bar{\bar{p}} \equiv p$(инволютивность)
- $p \vee \bar{p} \equiv T, \quad p \wedge \bar{p} \equiv F$
  $\bar{T} \equiv F, \quad \bar{F} \equiv T$ (дополнение)
- $\overline{(p \vee q)} \equiv \bar{p} \wedge \bar{q}, \quad \overline{(p \wedge q)} \equiv \bar{p} \vee \bar{q}$ (Де Морган)

Умозаключение состоит из предпосылкок (гипотез) и заключения (вывода). Умозаключение правильно, если заключение истинно , всякий раз когда истинны его гипотезы. Обозначение:

$$P_1, P_2, \cdots, P_k \vdash Q$$

или

$$\begin{array}{c} P_1 \\ P_2 \\ \vdots \\ P_k \\ \hline Q \end{array}$$

где $P_1, P_2, \ldots, P_k$ – предпосылки и Q – заключение.

Пример. Если p влечет q и q влечет r, то p влечет r. Другими словами, следующее умозаключение верно

$$p \to q, q \to r \vdash p \to r \text{ Закон силлогизма.}$$

Для этого мы должны проверить, что следующее высказывание является тавтологией:

$$(p \to q) \wedge (q \to r) \to) p \to r)$$

Проверим этот факт построив таблицу истинности

Элементарная дизъюнкция $x^\delta = x^{\delta_1} \vee x^{\delta_2} \vee \cdots \vee x_k^{\delta_k}$, где $\delta_1, \ldots \delta_k = 0, 1$ и $x_i^1 = x_i, x_i^0 = \bar{x}$.

Элементарная конъюнкция $x^\delta = x^{\delta_1} \wedge x^{\delta_2} \wedge \cdots \wedge x_k^{\delta_k}$, где $\delta_1, \ldots \delta_k = 0, 1$ и $x_i^1 = x_i, x_i^0 = \bar{x}$.

Дизъюнктивная нормальная форма (ДНФ) – дизъюнкция элементарных конъюнкции.

Пример ДНФ. $(p \wedge \bar{q}) \vee (p \wedge \bar{q} \wedge r)$

Конъюнктивная нормальная форма (КНФ) – конъюнкция элементарных дизъюнкции.

Пример КНФ. $(\bar{p} \vee q) \wedge (\bar{p} \vee \bar{q}) \wedge (\bar{p} \vee \bar{r})$

Совершенная дизъюнктивная нормальная форма (СДНФ) – дизъюнктивная нормальная форма, в которой нет двух одинаковых элементарных конъюнкции и каждая элементарная конъюнкция, входящая в нее, максимальна. Элементарной конъюнкция от переменных $(p_1, p_2, \ldots, p_n)$ называется максимальной, если каждая переменная p_i из набора $(p_1, p_2, \ldots, p_n)$ входит ровно один раз в виде p_i или в виде $\bar{p}_i$.

Пример. $(p_1 \wedge \bar{p}_2 \wedge p_3) \vee (\bar{p}_1 \wedge p_2 \wedge p_3)$ – СДНФ.

Пример. $(p_1 \wedge \bar{p}_2 \wedge p_3) \vee (\bar{p}_1 \wedge p_2 \wedge p_3) \vee (p_1 \bar{p}_2 \wedge p_3)$ не является СДНФ.

Совершенная конъюнктивная нормальная форма (СКНФ) – конъюнктивная нормальная форма, в которой нет двух одинаковых дизъюнкции и каждая входящая в ней элементарная дизъюнкция максимальна. Элементарная дизъюнкция от переменных $(p_1, p_2, \ldots, p_n)$ называется максимальной, если каждая переменная p_i из набора $(p_1, p_2, \ldots, p_n)$ входит ровно один раз в виде p_i или в виде $\bar{p}_i$.

Пример. $(p_1 \vee p_2 \vee \bar{p}_3) \wedge (\bar{p}_1 \vee p_2 \vee p_3) \wedge (p_1 \vee p_2 \vee \bar{p}_3)$ – СКНФ.

Пример. $(p_1 \vee p_2 \vee \bar{p}_3) \wedge (\bar{p}_1 \vee p_2 \vee p_3) \wedge (p_1 \vee p_2)$ – не является СКНФ.

Теорема Шеннона (дизъюнктивная формулировка.) Любая булева функция $f(p_1, \ldots, p_n)$ представима в виде

$$f(p_1, \ldots, p_k, p_{k+1}, \ldots, p_n) = \vee_\delta \, \&_{i=1}^k p_i^{\delta_i} \& f(\delta_1, \ldots, \delta_k, p_{k+1}, \ldots, p_n),$$

где $\delta_i = 0, 1; i = 1, 2, \ldots, k$,

$$p_i^{\delta_i} = \begin{cases} p_i & \text{при } \delta_i = 1, \\ \bar{p}_i & \text{при } \delta_i = 0 \end{cases}.$$

Здесь дизъюнкция проводится по всем наборам $\delta = (\delta_1, \ldots, \delta_k)$.

В предельном случае $n = k$ мы получаем, что любая ненулевая булева функция представима в виде СДНФ:

Любая ненулевая булева функция $f(p_1, p_2, \ldots, p_n)$ представима в виде

$$f(p_1, p_2, \ldots, p_n) = \vee_\delta \, \&_{i=1}^k p_i^{\delta_i}.$$

Здесь дизъюнкция проводится по всем наборам $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$, на которых $f(\delta_1, \delta_2, \ldots, \delta_n) = 1$.

Теорема Шеннона(конъюнктивная формулировка.) Любая булева функция $f(p_1, \ldots, p_n)$ представима в виде

$$f(p_1, \ldots, p_k, p_{k+1}, \ldots, p_n) = \wedge_\delta \, (\vee_{i=1}^k p_i^{\bar{\delta}_i} \vee f(\delta_1, \ldots, \delta_k, p_{k+1}, \ldots, p_n)),$$

где $\delta_i = 0, 1; i = 1, 2, \ldots, k$,

$$p_i^{\delta_i} = \{ \begin{array}{ll} p_i & \text{при } \delta_i = 1, \\ \bar{p}_i & \text{при } \delta_i = 0 \end{array} .$$

Здесь конъюнкция проводится по всем наборам $\delta = (\delta_1, \ldots, \delta_k)$.

В предельном случае $n = k$ мы получаем, что любая ненулевая булева функция представима в виде СКНФ:

Любая ненулевая булева функция $f(p_1, p_2, \ldots, p_n)$ представима в виде

$$f(p_1, p_2, \ldots, p_k) = \wedge_\delta \, (\vee_{i=1}^k p_i^{\bar{\delta}_i}).$$

Здесь конъюнкция проводится по всем наборам $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$, на которых $f(\delta_1, \delta_2, \ldots, \delta_n) = 0$.

Функциональная полнота.

???

Метод Карно

Пример.

4.5.1 Задачи

1. Составить таблицы для логических операции, формализующих союз:

- "но"
- "хотя бы"

2. Как с помощью логических операции записать высказывания:

- p достаточное условие для q,
- p необходимое условие для q,
- p, только если q,
- p необходимое и достаточное условие для q.

3. Пусть p означает "Сегодня холодно" и q означает "идет дождь". Что означают следующие высказывания ?

- $\bar{p}$
- $p \wedge q$
- $p \vee q$
- $q \vee \bar{p}$

4. Пусть p означает "Студент читает "Жас Алаш", q означает "Студент читает "Экспресс-К" " и r означает "Студент читает "Егемен Қазақстан"". Напишите следующие предложения в символической форме:

- Студент читает "Жас Алаш", "Экспресс-К", но не читает "Егемен Қазақстан"".
- Утверждение "Студент читает "Жас Алаш" и "Экспресс-К" " не верно.
- Утверждение "Студент читает "Егемен Казахстан" или "Экспресс-К", но не читает "Жас Алаш" " не верно.

5. Построить таблицу истинности для $\bar{p} \wedge q$

6. Доказать, что высказывание $p \vee \overline{p \wedge q}$ является тавтологией.

7. Доказать, что высказывания $\overline{p \wedge q}$ и $\bar{p} \vee \bar{q}$ логически эквивалентны.

8. Перепишите следующие условные предложения без использования условии:

- Если холодно, то он надевает шапку
- Если растет продуктивность, то издержки падают

9. Напишите отрицание следующих предложении:

- Если она работает, то она получает зарплату
- Он плавает если и только если вода теплая
- Если идет снег, то он не водит автомобиль

10. Верны ли следующие рассуждения:

- $p \to q, \bar{p} \vdash \bar{q}$
- $p \to q, \bar{q} \vdash \bar{p}$
- $p \to \bar{q}, r \to q, r \to \bar{p}$

11. Правильны ли следующие рассуждения ?

- Если две стороны треугольника равны, то противоположные углы также равны. Две стороны треугольника не равны. Следовательно, противоположные углы не равны.
- Если 7 меньше чем 4 то 7 не простое. 7 больше чем 4. Следовательно, 7 простое.

12. Проверить общезначимость формулы с помощью алгоритма Квайна

$$(((p \wedge q) \to r) \wedge (p \to q)) \to (p \to r)$$

13. Проверить общезначимость формулы с помощью алгоритма редукции

$$((p \wedge q) \to r) \to (p \to (q \to r))$$

14. Доказать выводимость формул в исчислении высказывании

- $p \to q, q \to r \vdash p \to r$
- $p \to (q \to r) \vdash q \to (p \to r)$
- $p \to (q \to r) \vdash (p \wedge q) \to r$
- $p \to q \vdash (p \wedge r) \to (q \wedge r)$
- $p \to q \vdash (p \vee r) \to (q \vee r)$
- $\bar{p} \vdash p \to r$

15. Выводимы ли следующие формулы в исчислении высказывании ?

- $(p \vee q) \to (p \wedge q)$
- $((p \to q) \to q) \to p$
- $((p \to q) \to q) \to q$
- $\overline{p \vee \bar{p}} \to (p \vee \bar{p})$
- $p \to \overline{p \to \bar{p}}$
- $(p \to q) \to (q \to p)$

16. Сколько существуют различных двуместных логических операции ?

17. Сколько существуют различных коммутативных двуместных логических операции ?

18. Пусть $M_n(r)$ – число булевых функции с r несущественными переменными. Доказать, что

$$M_n(r) = \binom{n}{r} \sum_{k=0}^{n-r} (-1)^k \binom{n-r}{k} 2^{2^{n-r-k}}, \quad r = 0, 1, \ldots, n-1.$$

Указание. Пусть A_i – множество булевых функции $f(x_1, \ldots, x_n)$ с несущественной переменной x_i. Тогда множество $A_{i_1} \cap \cdots A_{i_k}$ можно представить как множество булевых функции с 2^{n-k} аргументами. Поэтому согласно теореме о количестве булевых функции

$$|A_{i_1} \cap \cdots \cap A_{i_k}| = 2^{2^{n-k}}.$$

Заметье, что r несущественных переменных можно выбрать с $\binom{n}{r}$ способами и примените теорему включения и исключения.

4.6 Булева алгебра

Булева алгебра определяется множеством и пятью операциями. Пусть A – множество и заданы две бинарные операции $(a,b) \mapsto a+b, \quad (a,b) \mapsto a \cdot b$, одна унарная операция $a \mapsto \bar{a}$ и две нуль-арные операции $0, 1$. Они удовлетворяют следующим законам

$$x+y=y+x, \quad x \cdot y = y \cdot x \text{ (коммутативность)}$$

$$x+(y+z)=(x+y)+z, \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z \text{ (ассоциативность)}$$

$$x \cdot (x+y) = x, \quad x+(x \cdot y) = x \text{ (поглошение)}$$

$$x+(y \cdot z) = (x+y) \cdot (x+z), \quad x \cdot (y+z) = x \cdot y + x \cdot z \text{ (дистрибутивность)}$$

$$x \cdot 0 = 0, x+0=x, \quad x \cdot 1 = x, x+1=1 \text{ (универсальные границы)}$$

$$x \cdot \bar{x} = 0, \quad x+\bar{x}=1 \text{ (дополнение)}$$

Тогда A называется Булевой алгеброй.

Следствие 1.

$$x+x=x, \qquad x \cdot x = x \text{ (законы де Моргана)}$$

Доказательство. Подставим в аксиому поглощения $y = x \cdot x$. Имеем,

$$x(x+x \cdot x) = x,$$

$$x+x \cdot x = x.$$

Поэтому

$$x \cdot x = x.$$

Другое утверждение $x+x=x$ а также следующие следствия доказываются аналогичным образом.

Следствие 2.

$$\overline{x \cdot y} = \bar{x} + \bar{y}, \qquad \overline{x+y} = \bar{x} \cdot \bar{y} \text{ (идемпотентность)}$$

Следствие 3.

$$\overline{\bar{x}} = x \text{ (инволютивность)}$$

Теорема (Принцип двойственности) Любая общезначимая теорема о булевых алгебрах, в формулировке которой участвуют только операции "$+$", "$\cdot$" и "$\bar{a}$" остается общезначимой, если в ее формулировке всюду заменить "$+$" на "$\cdot$" и наоборот.

Доказательство. Все аксиомы булевой алгебры при такой замене остаются в силе. Поскольку все утверждения булевых алгебр вытекают только из таких аксиом, то любое такое доказательство при вышеуказанной замене превращаются в доказательство двойственного утверждения.

Пример. Пусть $P(A)$ булеан множества A. Наделим множество $P(A)$ двумя бинарными операциями $\vee, \wedge$, унарной операцией – дополнение и в качестве 0 возьмем пустое множество $\emptyset$ и в качестве 1 возьмем A. Тогда $(P(A), \vee, \wedge, \bar{}, 0, 1)$ будет булевой алгеброй.

Пример. Пусть $D(n)$ множество делителей числа n. Определим умножение и сложение ?? по правилам ??? . Пусть ???? . Тогда является булевой алгеброй.

4.7 Решетки

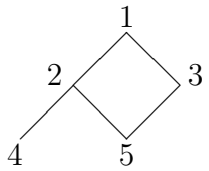
В этом пункте множество натуральных чисел $\mathbf{N}$ упорядочивается относительно порядка "делимость": $a \prec b \Leftrightarrow a|b$.

1. Пусть D_m – множество делителей числа m. Доказать, что D_m относительно операции $a + b = a \vee b = \text{НОК}(a, b), a \star b = a \wedge b = \text{НОД}(a, b)$ превращается в ограниченную дистрибутивную решетку.

2. Написать символ $\prec, \succ$ или $\|$ (не сравнимы) между следующими парами чисел 2 8; 18 24; 9 3; 5 15.

3. Являются ли следующие подмножества $\mathbf{N}$ линейно упорядоченными $\{24, 2, 6\}$; $\{3, 15, 5\}$; $\mathbf{N}$; $\{2, 8, 32, 4\}$; $\{7\}$; $\{15, 5, 30\}$?

4. Пусть $A = \{1, 2, 3, 4, 5\}$– множество с диаграммой Хассе



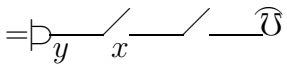
- Расставить знаки $\prec, \succ$ или $\|$ между парами элементов 1 5; 2 3; 4 1; 3 4
- Найти максимальные и минимальные элементы множества A. Имеет ли A первый и последний элемент ?
- Пусть $L(A)$– множество всех линейно упорядоченных подмножеств множества A с 2 или более элементами, упорядоченное по включению. Нарисовать диаграмму Хассе для $L(A)$.

5. Пусть D_m – множество делителей числа m. Доказать, что решетка D_m относительно операции $a+b = \text{НОК}(a, b), \quad a \star b = \text{НОД}(a, b)$, является Булевой алгеброй, если m не делится на квадрат простого числа. Найти атомы D_m.

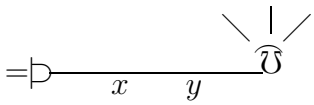
4.8 Переключательные схемы

В 1938 году Клод Шеннон заметил связь между электрическими цепями и булевыми функциями.

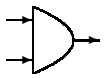
Коньюнкцию $p \wedge q$ можно представить себе в виде последовательного соединения переключателей p и q.



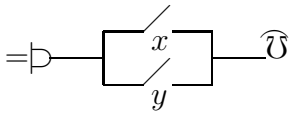
Чтобы загорелась лампочка необходимо замкнуть оба переключателя:



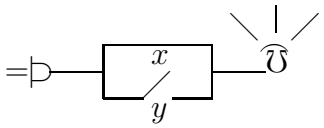
Такое расположение переключателей называется логическим элементом p и q или *схемой логического умножения.* Этот логический элемент обозначается так:



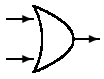
Дизъюнкцию $p \wedge q$ можно представить себе в виде последовательного соединения переключателей p и q.



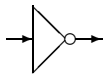
Чтобы загорелась лампочка достаточно замкнуть хотя бы один из переключателей:



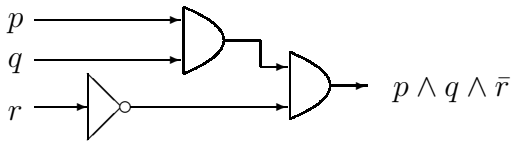
Такое расположение переключателей называется логическим элементом p или q или *схемой логического сложения.* Этот логический элемент обозначается так:



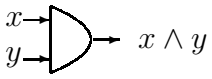
Рассмотрим переключательную схему с одним переключателем p обладающая таким свойством, что лампочка загорается тогда и только тогда, когда он разомкнут. Эта схема соответствует отрицанию $\bar{p}$ и называется логическим элементом *не* или *конвертором.* Обозначение:

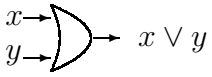


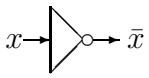
Пример. Переключательная схема для выражения $p \wedge q \wedge \bar{r}$



Пример. ???







4.8.1 Задачи

1. Полусумматор

2. Построить схему трехклавишного переключателя. Свет должен быть включен, если замкнуты по крайней мере два переключателя.

Ответ: $pqr + p\bar{q}\bar{r} + \bar{p}q\bar{r} + \bar{p}\bar{q}r$

Глава 5

Графы

5.1 Основные определения

Чтобы задать граф G нужно задать множество *вершин* $V = V(G)$ и множество *ребер* $E = E(G)$, такой, что $E \subseteq V \times V$. Если $e = (u, v)$ – ребро, то вершины u и v называется конечными точками или вершинами ребра e. В таких случаях говорят, что u и v *связаны* и, что вершины u и v *инцидентны* с ребром e и наоборот, ребро e *инцидентно* с вершинами u и v и иногда обозначают $e = uv$.

??? Петля. Мультиграф. Простой граф ????

Чтобы задать ориентировнанный граф, кроме множества вершин и ребер нужно задать ориентацию ребер. Если $e = \overrightarrow{uv}$ – ориентированное ребро:

то говорят, что u – *начало* и v – *конец* ребра e.

Маршрут – последовательность вершин и ребер $v_0e_0v_1e_1 \dots v_{s-1}e_{s-1}v_s$ такой, что $e_i = (v_{i-1}, v_i)$ – ребро с вершинами v_{i-1} и v_i. Обычно вместо обозначения $v_0e_0v_1e_1 \dots v_{s-1}e_{s-1}v_s$ пишут кратко $v_0v_1 \dots v_{s-1}v_s$.

Цикл – маршрут, у которых начальная и конечная вершины совпадают.

Цепь – маршрут, в котором все ребра разные.

Простая цепь – цепь не содержащая повторяющихся вершин, т.е. цепь не пересекающая себя.

Матрица инцидентности $(a_{i,j})$ – матрица порядка $n \times m$, где $n = |V|$ и $m = |E|$. Строки индексируются элементами множества вершин V и столбцы – элементами множества ребер E.

$$a_{i,j} = \begin{cases} 1 & \text{если вершина } v_i \text{ инцидентна ребру } e_j \\ 0 & \text{в противном случае.} \end{cases}$$

Матрица смежности $(b_{i,j})$ – матрица порядка $n \times n$, где $n = |V|$. Строки и столбцы индексируются элементами множества вершин V.

$$b_{i,j} = \begin{cases} s & \text{если вершина } v_i \text{ связана с вершиной } v_j \text{ с помощью } s \text{ ребер} \\ 0 & \text{в противном случае.} \end{cases}$$

Если G – ориентированный граф, то матрицу смежности определяется так: ??

$$b_{i,j} = \begin{cases} 1??? & \text{если } v_i \text{ начальная и } v_j \text{ конечная вершина некоторого ребра} \\ 0 & \text{в противном случае.} \end{cases}$$

??

Алгоритм Варшалла. Транзитивное замыкание отношения. ??

Пусть $G = (V, E)$ – ориентированный граф. Пусть $W = (w_{i,j})$ – матрица смежности:

$$w_{i,j} = \begin{cases} 1, & \text{если из вершины } v_i \text{ в } v_j \text{ направлено ребро} \\ 0, & \text{в противном случае} \end{cases}$$

Внизу все сложения понимаются в логическом смысле. Обратим внимание на различие: $1+1 = 1$ в логическом сложении и $1+1 = 0$ в арифметическом сложении.

Алгоритм Варшалла построения матрицы достижимости W^*.

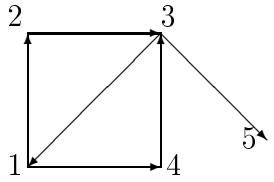
Возьмем первую столбец матрицы $W_1 = W$ и сложим первую строку во все строки матрицы W_1, у которых на первом месте стоят 1. Полученную матрицу обозначим через W_2.

Возьмем второй столбец матрицы W_2 и сложим вторую строку матрицы W_2 во все строки, у которых на втором месте стоят 1. Обозначим полученную матрицу W_3. И т.д. На n-ом шаге получим матрицу W_n. Это и есть матрица достижимости W^* в графе G.

Иногда W^* можно получить и раньше не дожидаясь n-ого шага. Начиная с некоторого шага матрицы начинают повторяться: $W_i = W_{i+1} = \cdots$. Тогда $W^* = W_i$.

Смысл матрицы W^* таков. Если $W^* = (w^*_{i,j})$ и $w^*_{i,j} = 1$, то существует путь из вершины v_i в вершину v_j. Если $w^*_{i,j} = 0$, то такого пути нет.

Пример. Найти матрицу достижимости графа



Решение. Имеем

$$W = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Поэтому

$$W_0 = W = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

В первом столбце только третья строка имеет 1. Добавим этой строке первую строку. Имеем,

$$W_1 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

На втором столбце матрицы только первая и третья строка имеет 1. Добавим этим строкам вторую строку. Имеем

$$W_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

На третьем столбце все строки кроме пятой имеют 1. Добавим этим строкам третью строку. Получаем, что

$$W_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

и

$$W_i = W_3,$$

для всех $i > 3$. Итак,

$$W^* = W_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Другими словами, из любой вершины, кроме вершины 5 можно попасть в любую другую вершину.

5.1.1 Деревья

Дерево – связный граф без цикла.

Лес – граф все компоненты связности которого являются деревьями.

Теорема. Следующие условия эквивалентны:

- Граф – дерево
- Граф является связным и не имеет простых циклов.
- Граф является связным и число его ребер ровно на единицу меньше чем числа вершин.

- Любые две различные вершины графа можно соединить единственной (и притом простой) цепью.
- Граф не содержит циклов, но, добавляя к нему любое новое ребро, получаем ровно один (с точностью до направления обхода и начальной вершины обхода) и притом простой цикл проходящий через добавляемое ребро.

Остовное дерево графа – любой его подграф, содержащий все вершины графа и являющийся деревом.

Цикломатическое число графа $G = (V, E)$ есть число $\nu(G) = |E| - |V| + 1$

Поскольку количество ребер на единицу меньше чем количество вершин, любое остовное дерево графа $G = (V, E)$ имеет $|V| - 1$ ребер. Поэтому остовное дерево получается в результате удаления из графа ровно $\nu(G)$ ребер.

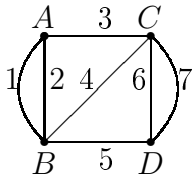
5.2 Электрические цепи и графы

В теории электрических цепей обычно применяются следующая терминология.

Узел – вершина степени не меньше 3. Вместо терминов "ребро" и "цикл" часто используются слова "ветвь" и "контур".

Основным примером графа, на котором иллюстрируются утверждения этого параграфа является

Пример.

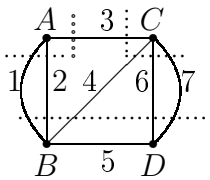


Количество ребер $e = 7$. Количество вершин $v = 4$

Сечение – система ребер, удаление которых разбивают граф на две несвязные части, каждая из которых является связным подграфом. При этом присоединение любой из удаленных ветвей должно приводит к связному графу.

Пример. Ребра, инцидентные любой вершине образуют сечение.

Пример. Следующие ребра образуют сечения: $1, 2, 3$; $3, 6, 7$; $1, 2, 4, 6, 7$.



Заметим, что число сечении могут превысить число вершин.

Контур графа – цикл

Законы Киркгофа:

- Алгебраическая сумма токов ребер сечения равна нулю:

$$\sum \pm i_k = 0.$$

- Алгебраическая сумма напряжении ребер контура равна нулю:

$$\sum \pm u_k = 0.$$

Для графа без петель G с вершинами $v_1, \ldots, v_n$ определим матрицу смежности $A = (a_{i,j})$ и матрицу (матрица Кирхгофа) $D = (d_{i,j})$ по правилам

$$a_{i,j} = \text{ количество ребер соединяющих вершины } v_i \text{ и } v_j, \text{ если } i \neq j,$$

$$\begin{array}{ll} d_{i,i} = & deg\, v_i, \\ d_{i,j} = & -a_{i,j}, \text{ если } i \neq j \end{array}.$$

Теорема. Алгебраические дополнения всех элементов матрицы Кирхгофа равны между собой.

Доказательство. Пусть D – матрица Кирхгофа и $D_{i,j}$ – его (i,j)-алгебраическое дополнение. Пусть $D = (\alpha_{i,j})$. Тогда

$$\sum_{j=1}^{n} \alpha_{i,j} = 0, \qquad i = 1, 2, \ldots, n,$$

$$\sum_{i=1}^{n} \alpha_{i,j} = 0, \qquad i = 1, 2, \ldots, n.$$

Другими словами,

$$B \cdot \mathbf{1} = 0,$$

$$\mathbf{1}^t \cdot B = 0,$$

где $\mathbf{1}$ – столбец длины n, состоящий из 1.

Поэтому, $det\, D = 0$, и $rank\, D \leq n-1$. Если $rank\, D < n-1$, то $D_{i,j} = 0$, для всех $1 \leq i, j \leq n$.

Рассмотрим теперь случай $rank\, D = n-1$. Пусть D^{adj} – присоединенная матрица:

$$D^{adj} = \begin{pmatrix} D_{11} & D_{21} & \cdots & D_{n1} \\ D_{12} & D_{22} & \cdots & D_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ D_{1n} & D_{2n} & \cdots & D_{nn} \end{pmatrix}$$

Следующее свойство матриц хорошо известно:

$$D\, D^{adj} = D^{adj}\, D = (det\, D)E.$$

Поэтому

$$D\, D^{adj} = (det\, D)E = 0.$$

Поскольку $D\, D^{adj} = 0$, любой столбец X матрицы D^{adj} удовлетворяет системе $DX = 0$. Ранг этой системы линейных уравнении равна $n-1$. Поэтому фундаментальная система решении уравнения одномерна и порождается вектором $\mathbf{1}$. Значит

столбец соответствующий любому другому решению системы $DX = 0$ пропорционален **1**. Итак,

$$D_{i1} = D_{i2} = \cdots = D_{in}, \qquad i = 1, 2, \ldots, n.$$

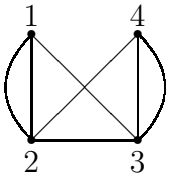
Аналогично,

$$D_{1i} = D_{2i} = \cdots = D_{ni}, \qquad i = 1, 2, \ldots, n.$$

Поэтому все элементы присоединенной матрицы D^{adj} одинаковы, что и требовалось доказать.

Теорема. Пусть D – матрица Кирхгофа и $D_{i,j}$ – его (i,j)-алгебраическое дополнение. Тогда количество остовных деревьев графа G равно $D_{i,j}$ для любых i, j.

Пример. Матрица Кирхгофа для графа



выглядит так

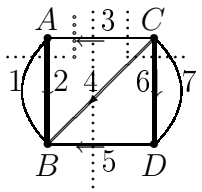
$$D = \begin{pmatrix} 3 & -2 & -1 & 0 \\ -2 & 4 & -1 & -1 \\ -1 & -1 & 4 & -2 \\ 0 & -1 & -2 & 3 \end{pmatrix}$$

Тогда

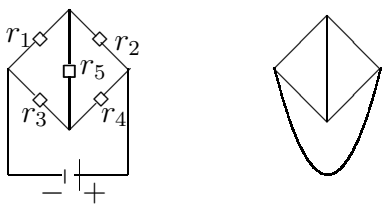
$$|D_{1,1}| = \begin{vmatrix} 4 & -1 & -1 \\ -1 & 4 & -2 \\ -1 & -2 & 3 \end{vmatrix} = 21$$

Итак, граф имеет 21 остовных деревьев. Перечислите их.

Пример.



Пример. Количество остовных деревьев равна



5.3 Эйлеровы графы

Цикл называется Эйлеровым, если он проходит все ребра ровно по одному разу. Аналогично, путь, начало и конец которых не совпадают, называется Эйлеровым, если он проходит все ребра ровно по одному разу. Граф Эйлеров, если существует Эйлеров путь или цикл. Другими словами, граф Эйлеров, если его можно нарисовать одним росчерком пера не т.е., отрывая перо от бумаги.

Напомним, что вершина графа называется четной, если она имеет четную степень. Аналогично, вершина нечетна, если ее степень нечетна. Напомним также, что по теореме о рукопожатиях множество нечетных вершин имеет четное количество элементов.

Теорема. Конечный связный граф G имеет Эйлеров цикл, если и только если число нечетных вершин равно нулю.

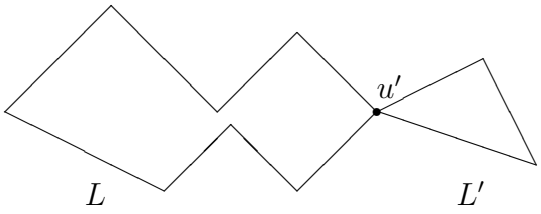
Доказательство. Допустим, что существует Эйлеров цикл. Это означает, что сколько ребер входят в вершину, столько и выходят. Другими словами, степень любой вершины четна.

Обратно, допустим, что степень любой вершины четна.

Покажем сначала, что в графе существует цикл, в котором все ребра различны. Пусть $v_1e_1v_2e_2\cdots v_{k-1}e_{k-1}v_k$ – некоторый путь, где ребро e_i начинается с вершины v_i и кончается на вершине v_{i+1} и все ребра $e_1,\ldots,e_k$ различны. Допустим, что длина пути k максимальна и что $v_k \neq v_1$. Тогда с вершиной v_k инцидентна нечетное количество ребер из множества $\{e_1,\ldots,e_{k-1}\}$. Поскольку степень вершины v_k четна, существует ребро e_k, отличное от $e_1,\ldots,e_{k-1}$, которое из нее выходит. Если другая вершина ребра e_k, обозначим ее через v_{k+1}, не совпадает совпадает с вершиной v_1, то получаем путь длины большей чем k. Поэтому $v_k = v_1$ и мы получаем цикл $v_1e_1v_2e_2\cdots v_{k-1}e_{k-1}v_ke_kv_1$.

Допустим, что цикл $L = v_1e_1v_2e_2\cdots v_{k-1}e_{k-1}v_ke_kv_1$ имеет максимальную длину и все ребра $e_1, e_2, \ldots, e_k$ различны. Докажем, что все ребра графа появляется в этом списке.

Предположим, что это не так: $E \neq \{e_1,\ldots,e_k\}$, где E – множество ребер графа G. Пусть F – граф, полученный из G путем удаления ребер $e_1,\ldots,e_k$. Граф H может быть не связным, но каждая вершина графа имеет четную степень, поскольку путь L имеет четное количество ребер инцидентных с каждой ее вершиной. Поскольку G связна, существует ребро e' графа H, которое имеет одну вершину u' лежащую в пути L. Построим путь L' в графе H, начинающуюся из вершины u'. Поскольку все вершины графа H имеют четную степень, мы можем построить цикл L' в графе H, в котором все ребра пути L' различны.



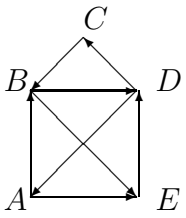
Другими словами, путь L может быть продолжен с помощью пути L'. Это противоречит максимальности k, длины пути L. Итак, L – Эйлеров путь.

Теорема. Граф G имеет Эйлеров путь, если и только если число нечетных вершин равно 2. При этом любой Эйлеров путь начинается с одной нечетной вершины и кончается на другой нечетной вершине.

Доказательство. Пусть $v_1e_1v_2e_2\dots v_{k-1}e_{k-2}v_k$ – Эйлеров путь и $v_1 \neq v_k$. Степени всех внутренних вершин $v_i, 1 < i < k$, четные, поскольку каждому входящему ребру e_{i-1} соответствует другое выходящее ребро e_i. Степени начальной вершины v_1 нечетна, поскольку одно ребро e_1 выходит но к нему не соответствует ни одного входящего ребра. Аналогично, в конечной вершину v_k одно ребро e_{k-1} входит но ни одно ребро не выходит, поэтому степень $deg\, v_k$ нечетна. Итак, если граф имеет Эйлеров путь, то вершины всех внутренних вершин четны и степени двух конечных вершин нечетны.

Обратно, если граф имеет ровно два нечетных вершин, то любой максимальный путь с началом в одной нечетной вершине кончается в другой нечетной вершине и обходит все ребра. Доказательство повторяет рассуждения приведенные выше в доказательстве теоремы об Эйлеровых циклах.

Пример. Открытый конверт можно нарисовать одним росчерком пера. Один из таких путей $ABDCBEDAE$ показан внизу. Можно начать из вершины A, следовать по направлению стрелок и попасть в вершину E.

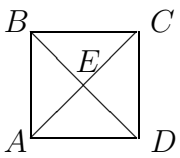


Заметим, что

$$deg\, A = 3, deg\, B = 4, deg\, C = 2, deg\, D = 4, deg\, E = 3.$$

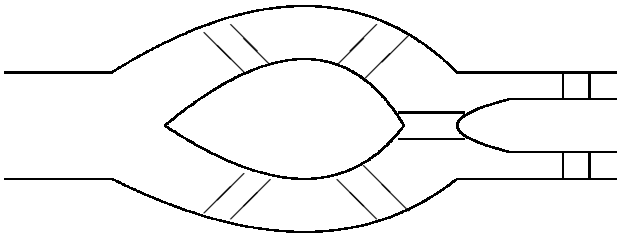
Две вершины A и E имеют нечетную степень. Поэтому любой Эйлеров путь начинается в одной и кончается в другой из этих вершин.

Пример. Закрытый конверт уже невозможно нарисовать одним росчерком пера, поскольку он имеет четыре нечетных вершин.



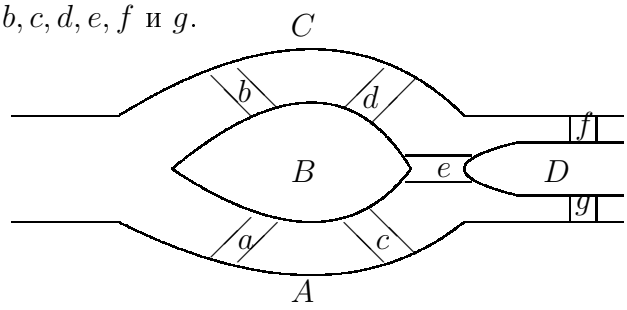
$$deg\, A = deg\, B = deg\, C = deg\, C = 3, \qquad deg\, E = 4.$$

Пример. (Путешествие по Кенигсбергским мостам) В реке имеются два острова. Берега соединены с островами семью мостами. Можно ли пройти по всем мостам не проходя дважды по одному и тому же мосту ?

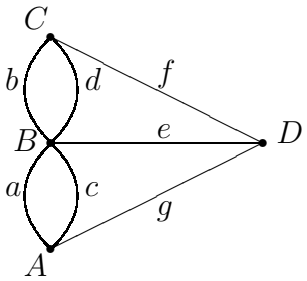


Ответ: Нет.

Чтобы увидеть это обозначим берега через A и C, острова через B, D и мосты через a, b, c, d, e, f и g.



Тогда граф с вершинами, соответствующими суше и ребрами, соответствующим мостам имеет $4 > 2$ нечетных вершин.



$deg\, A = 3,\ deg\, B = 5,\ deg\, C = 3,\ deg\, D = 3.$

Поэтому граф не является Эйлеровым. Это означает, что как бы ни путешествовал человек по всем мостам обязательно найдется мост по которому он будет проходить по крайней мере два раза.

5.4 Гамильтоновы графы

?????

5.5 Планарные графы

Планарный граф – граф, изоморфный графу, у которого ребра не пересекаются.

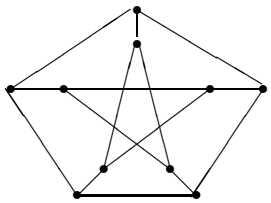
Пример. $K_{2,2}$, $K_{2,3}$ – планарные графы:

Гомеоморфность (стягиваемость ??) графа

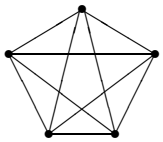
Теорема (Куратовский) Граф не является планарными тогда и только тогда, когда он содержит подграф, гомеоморфный графам K_5 или $K_{3,3}$.

Пример. Граф Петерсена – не планарный.

Доказательство. Напомним определение графа Петерсена



С помощью стягивания вершин внешнего пятиугольника с соответствующими вершинами внутренней пятиугольной звезды граф Петерсена можно свести к полному графу K_5 :



Следовательно, по теореме Куратовского граф Петерсена не является планарным.

Теорема (Эйлер) Пусть G – планарный граф с v вершинами, e ребрами и f гранями. Тогда

$$e - v + f = 2.$$

Граф называется *правильным,* если степени всех вершин одинаковы и каждая грань является многоугольником, с одинаковым количество сторон у каждой грани.

Теорема. Существует ровно пять правильных графов. Правильные многогранники соответствующие правильным графам приведены в рисунках **??** и **??**.

Доказательство. Пусть $k = deg\, v$, для любого $v \in V$. Допустим, что каждая грань является выпуклым n-угольником. Подсчитаем удвоенное количество ребер $2e$ графа двумя способами.

Первый способ. По теореме о рукопожатиях

$$kv = 2e.$$

Поэтому

$$e = kv/2.$$

Второй способ. Количество граней $-f$. Каждая грань имеет n ребер. Каждое ребро является стороной двух граней. Следовательно

$$fn = 2e.$$

Таким образом,

$$f = 2e/n = kv/n.$$

Значит, по теореме Эйлера

$$v - kv/2 + kv/n = 2.$$

Итак,

$$2vn - kvn + 2kv = 4n,$$

и

$$v(2n - kn + 2k) = 4n.$$

Поскольку $v, n \in \mathbf{Z}$, должно быть

$$2n + 2k - kn \geq 0.$$

Другими словами,

$$(n-2)(k-2) < 4.$$

Произведения двух целых положительных чисел < 4 могут принимать значения $1, 2, 3$. Таким образом, для целых чисел n, k возможны следующие пять случаев:

$$n-2 = 1, k-2 = 1,$$

$$n-2 = 1, k-2 = 2,$$

$$n-2 = 1, k-2 = 3,$$

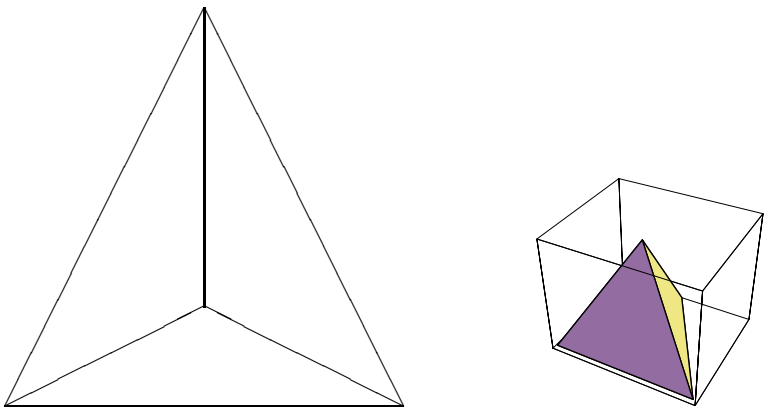
$$n-2 = 2, k-2 = 1,$$

$$n-2 = 3, k-2 = 1.$$

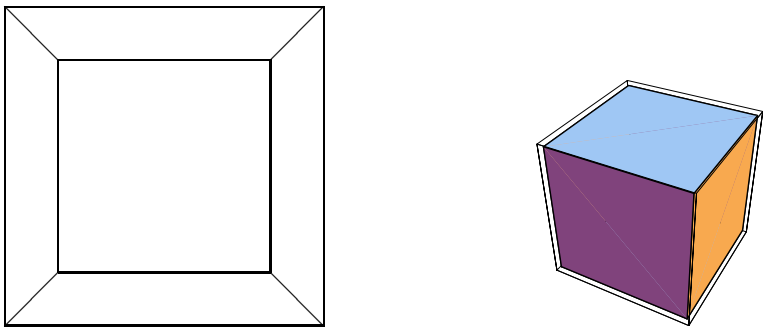
Итак, получаем следующие возможности

k	n	v	e	f	Тип
3	3	4	6	4	Тетраэдр
3	4	8	12	6	Куб
3	5	20	30	12	Додекаэдр
4	3	6	12	8	Октаэдр
5	3	12	30	20	Икосаэдр

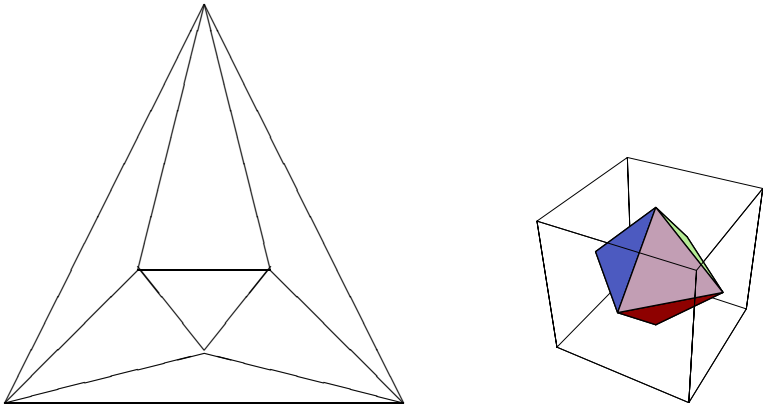
Как показаны в нижеприводимых рисунках все эти возможности реализуемы.



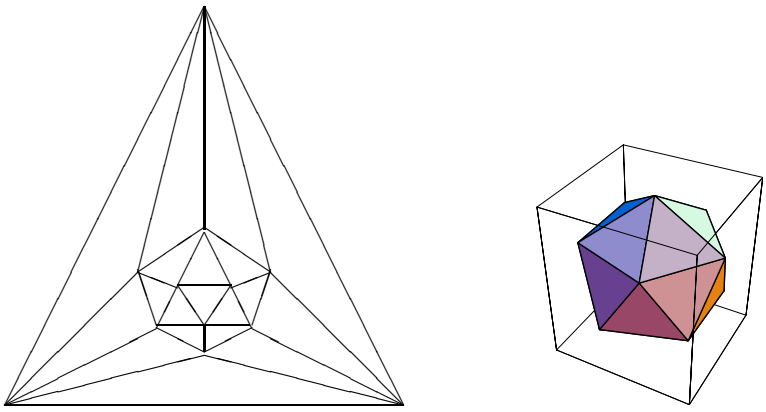
Тетраэдр и его граф



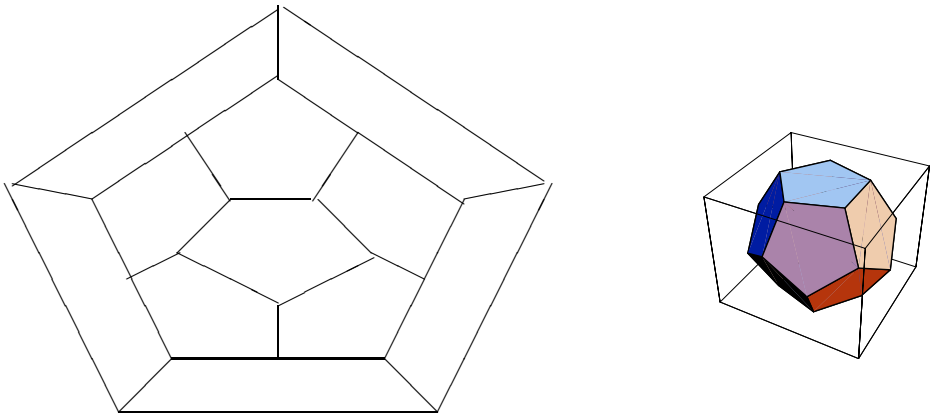
Куб и его граф



Октаэдр и его граф



Икосаэдр и его граф



Додекаэдр и его граф

Теорема о классификации правильных графов полностью доказана.

Двойственные граф строится так. Пусть $G = (V, E)$ – планарный граф. Построим новый граф $G*$ с множеством вершин $V*$, таким что существуют взаимнооднозначное соответствие между $V*$ и множеством граней графа G. Вершины $u, v \in V^*$ соединены ребром, если и только если соответствующие грани в G имеют общую границу.

Пример. Граф, двойственный графу октаэдра изоморфен графу куба

Пример. Граф, двойственный графу додекаэдра изоморфен графу икосаэдра.

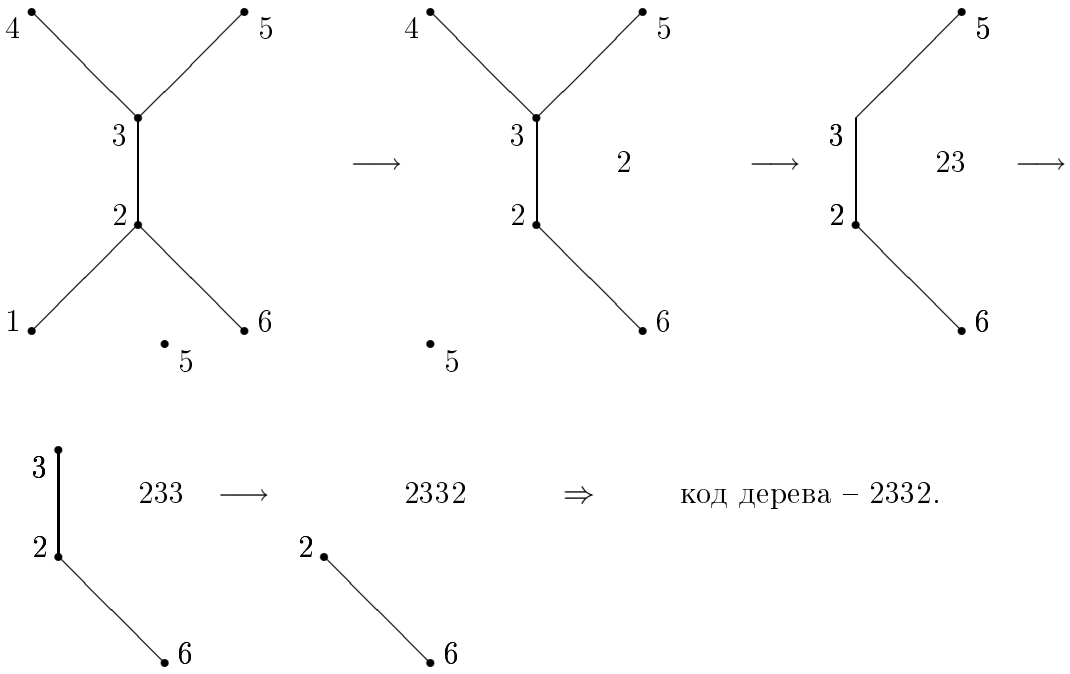
5.5.1 Кодировка деревьев

Деревья с множеством вершин занумерованными элементами множества $\{1, 2, \ldots, n\}$ можно закодировать с помощью $n = 2$ элементов $i_1 i_2 \ldots i_{n-2}$, где $i_1, \ldots, i_{n-2} \in \{1, 2, \ldots, n\}$. Такие коды, они называются кодами Прюффера, строятся по следующему алгоритму.

Алгоритм построения кода Прюффера.

Пусть T – дерево с множеством вершин занумерованные элементами множества $\{1, 2, \ldots, n\}$ Находим вершину с наименьшим номером и с наименьшей степенью. Пусть это будет вершина v_{i_1} и с этой вершиной связана вершина v_{i_2}. Убираем вершину v_{i_1} и инцидентную с ней ребро $v_{i_1} v_{i_2}$. Напишем номер i_2 вершины v_{i_2}. С полученным графом поступаем точно также и повторяем эту процедуру до тех пор, пока не останется одно ребро. Полученная последовательность $n - 2$ чисел $i_1 i_2 \ldots i_{n-2}$ и есть код Прюффера.

Пример.



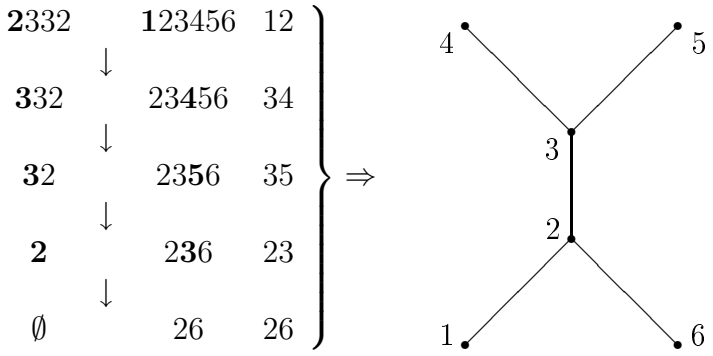
Алгоритм построения дерева по коду Прюффера.

Пусть $i_1 i_2 \dots i_{n-2}$ – набор чисел произвольным образом выбранные из множества $\{1, 2, \dots, n\}$. Чтобы построить дерево T так, чтобы его код был равен $i_1 i_2 \dots i_{n-2}$ нужно поступать следующим образом.

Написать три колонки. В первый первую колонку включить лист $i_1 i_2 \dots i_{n-2}$и во вторую $12 \dots n$. Взять наименьшее число со второго листа, который не лежит в первом. Пусть это будет число j_1. Убрать i_1 с первого листа и написать полученный лист в первую колонку. Убрать j_1 со второго листа и написать полученный лист на вторую колонку. Написать в третью колонку $i_1 j_1$. Повторить ту же процедуру с полученными листами в первой и во второй колонках и написать в третью колонку $i_2 j_2$, где j_2 – наименьшее число не содержащее в первой листе. Повторить эту процедуру до тех пор пока в первой колонке не останется пустое множество и во второй лист из двух чисел. Последний лист из двух чисел из второй колонки включить в третью колонку.

Тогда все пары написанные в третьей колонке дадут нам множество ребер дерева вершины которого занумерованы элементами множества $\{1, 2, \dots, n\}$.

Пример.



5.5.2 Алгоритм Дейкстры

Пусть задан граф с весом $G = (V, E, f)$. Здесь весом называется некоторая функция $f : E \to \mathbf{R}_+$ с положительными значениями. Для любого $e \in E$ назовем $f(e)$ весом ребра. Вес пути $x = v_1 e_1 v_2 e_2 \dots v_k e_k v_{k+1}$ определяется по формуле

$$|x| = f(e_1) + \dots + f(e_k).$$

Требуется построить путь с минимальным весом из вершины v_1 к вершине v_k.

Дадим алгоритм построения таких путей. Алгоритм носит имя Е.В.Дейкстры.

На каждом шаге s будем строить множество вершин $V_1^{(s)}$ и $V_2^{(s)}$ м каждая вершина v будет иметь вес $\lambda^{(s)}(v)$. При этом

$$V_1^{(s)} \subset V_1^{(s+1)} = V_1^{(s)} \cup \{v_{i_s}\}, \quad V_2^{(s+1)} = V_2^{(s)} \setminus \{v_{i_s}\} \subset V_2^{(s)}, \qquad s = 1, 2, \dots,$$

и веса вершин $v \in V_1^{(s)}$ дальше менятся не будут ($\lambda^{(s')}(v) = \lambda^{(s)}(v)$, для всех $s' > s$. Для таких $v_{i_s} \in V_1^{(s)}$ положим

$$\lambda(v_{i_s}) = \lambda^{(s)}(v_{i_s}).$$

В то время веса вершин $v \in V_1^{(s)}$ могут меняться с ростом s. Поэтому вершины $v \in V_1^{(s)}$ называются постоянными а вершины $v \in V_2^{(s)}$ – временными. Кроме этого каждой вершине $v \in V_1^{(s)}$ сопоставляется некоторая вершина u, которую будем называть вершиной предыдущей к вершине v. Способы построения весов и предыдущих вершин приводятся внизу.

В начальный момент

$$V_1^{(1)} = \{v_1\}, \quad V_2 = V \setminus V_1 = \{v_2, \dots, v_k\},$$

и

$$v_1 = v_1(0, 0),$$

$$v_i = v_i(\infty, 0\}, \quad i \neq 1.$$

Допустим, что на s-ом шаге мы знаем, что

$$V_1^{(s-1)} = \{v_1 = v_{i_1}, v_{i_2}, \ldots, v_{i_{s-1}}\}, V_1^{(s)} = V_1^{(s-1)} \cup \{v_{i_s}\},$$

$$V_2 = V \setminus V_1,$$

причем v_{i_s} – последняя вершина.

Для вершины $v \in V$ обозначим через $x(v)$ ее предыдущая вершина

Пусть v_j – временная вершина, смежная с v_{i_s} и ей приписаны вес и предыдущая вершина $(\lambda^{(s)}(v_j), x(v_j))$.

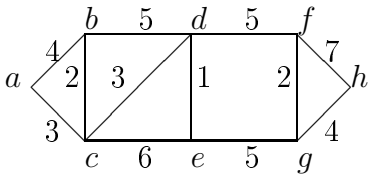
Изменим вес $\lambda^{(s+1)}(v_j)$ на $(\lambda^{(s)}(v_{i_s}) + f(v_{i_s}, v_j)$ и изменим предыдущую вершину $x(v_j)$ на v_{i_s}, если $\lambda^{(s)}(v_j) > \lambda^{(s)}(v_{i_s}) + f(v_{i_s}, v_j)$ и оставим $(\lambda^{(s)}(v_j), x(v_j))$ без изменения в противном случае. Проделаем эту процедуру со всеми временными вершинами, смежными с v_{i_s}. Выберем среди них одну вершину, пусть это будет $v_{i_{s+1}}$, такой что $\lambda^{(s+1)}(v_j)$ минимален. Включим такую вершину в множество постоянных вершин и исключим ее из множества временных вершин. Тогда

$$V_1^{(s+1)} = V_1^{(s)} \cup \{v_{i_{s+1}}\}, \quad V_2^{(s+1)} = V_2^{(s)} \setminus \{v_{s+1}\}.$$

Продолжим эту процедуру до $s = n$, где $n = |V|$ – количество вершин графа G. Тогда

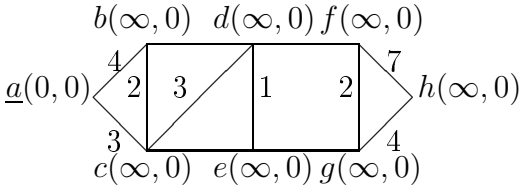
$$V_1 = V_1^{(n)}.$$

Пример. Найти минимальное расстояние между вершинами a и h.



Решение. Применим алгоритм Дейкстры.

Шаг 1. Положим $u^{(1)} := a$ и присваеваем ей вес $(0, 0)$. Всем остальным вершинам присваеваем веса $(\infty, 0)$.



Итак,

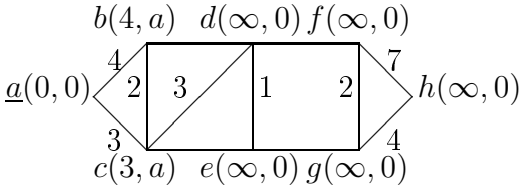
$$V_1^{(1)} = \{a\}, \quad V_2^{(1)} = \{b, c, d, e, f, g, h\},$$

$$\lambda(a) = \lambda^{(1)}(a) = 0,$$

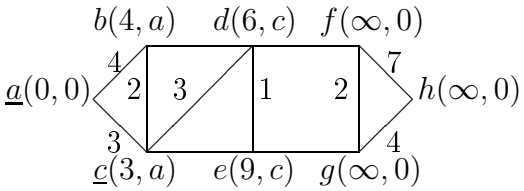
$$\lambda^{(1)}(b) = \infty, \lambda^{(1)}(c) = \infty, \lambda^{(1)}(d) = \infty,$$

$$\lambda^{(1)}(e) = \infty, \lambda^{(1)}(f) = \infty, \lambda^{(1)}(g) = \infty, \lambda^{(1)}(h) = \infty.$$

Шаг 2. Присваеваем вершинам b и c, смежным с вершиной $u^{(1)} = a$ веса $(4, a)$ и $(3, a)$ (расстояния до $u^{(1)}$)



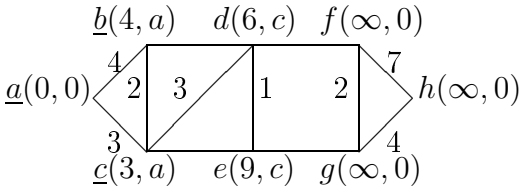
Берем вершину c в качестве $u^{(2)}$, поскольку расстояние вершины c до вершины $u^{(1)}$ меньше чем расстояние вершины b до вершины $u^{(1)}$.



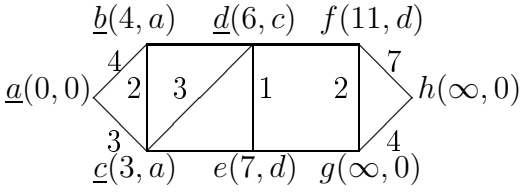
Итак,

$$V_1^{(2)} = \{a, c\}, \quad V_2^{(2)} = \{b, d, e, f, g, h\},$$
$$\lambda(a) = 0, \lambda(c) = \lambda^{(1)}(c) = 3,$$
$$\lambda^{(2)}(b) = 4, \lambda^{(2)}(d) = 6,$$
$$\lambda^{(2)}(e) = 9, \lambda^{(2)}(f) = \infty, \lambda^{(2)}(g) = \infty, \lambda^{(2)}(h) = \infty.$$

Шаг 3. Вершины b, d и e лежат в $V_2^{(2)}$ и смежны с вершиной $u^{(2)} = c$. Вычислим веса этих вершин относительно $u^{(2)}$. Меняем веса вершин d и e на $(6, c)$ и $(9, c)$, поскольку $6 < \infty$ и $9 < \infty$. Вес веса b оставляем неизменным, так как $\lambda^{(2)}(b) = 4 < 3 + 2 = \lambda(c) + f(u^{(2)}, b)$.



Берем вершину b в качестве $u^{(3)}$, так как веса вершин d и e больше чем веса вершины b.

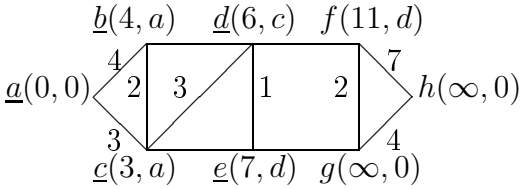


Итак,

$$V_1^{(3)} = \{a, c, b\}, \quad V_2^{(3)} = \{d, e, f, g, h\},$$

$$\lambda(a) = 0, \lambda(c) = 3, \lambda(b) = \lambda^{(1)}(b) = 4,$$
$$\lambda^{(3)}(d) = 6, \lambda^{(3)}(e) = 9, \lambda^{(3)}(f) = \infty, \lambda^{(3)}(g) = \infty, \lambda^{(3)}(h) = \infty.$$

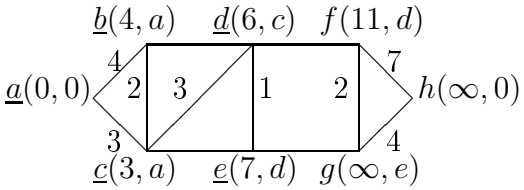
Шаг 4. Вычисляем расстояния от вершины $u^{(3)} = b$ до вершины d смежной с $u^{(3)}$.



Вес вершины d оставляем неизменной, поскольку $\lambda^{(3)}(d) = 6 < 4 + 5 = \lambda(b) + f(u^{(3)}, d)$. Берем d в качестве $u^{(4)}$. Итак,

$$V_1^{(4)} = \{a, c, b, d\}, \quad V_2^{(4)} = \{e, f, g, h\},$$
$$\lambda(a) = 0, \lambda(c) = 3, \lambda(b) = 4, \lambda(d) = \lambda^{(3)}(d) = 6,$$
$$\lambda^{(4)}(e) = 9, \lambda^{(4)}(f) = \infty, \lambda^{(4)}(g) = \infty, \lambda^{(4)}(h) = \infty.$$

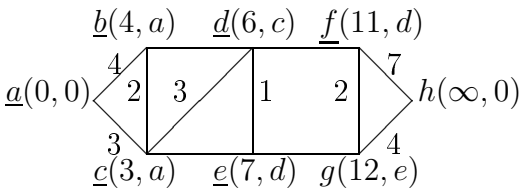
Шаг 4. Только вершины e и f смежны с вершиной $u^{(4)} = d$ и лежат в V_2. Легко видеть, что относительно $u^{(4)}$ эти вершины имеют веса $(7, d)$ и $(11, d)$.



Поэтому $u^{(5)} = e$ и

$$V_1^{(5)} = \{a, c, b, d, e\}, \quad V_2^{(4)} = \{f, g, h\},$$
$$\lambda(a) = 0, \lambda(c) = 3, \lambda(b) = 4, \lambda(d) = 6, \lambda(e) = \lambda^{(4)}(e) = 7,$$
$$\lambda^{(5)}(f) = \infty, \lambda^{(5)}(g) = \infty, \lambda^{(5)}(h) = \infty.$$

Шаг 5. Имеется только одна вершина в V_2, смежная с вершиной $u^{(5)} = e$. Эта вершина g. Легко видеть, что g имеет вес $(12, e)$.

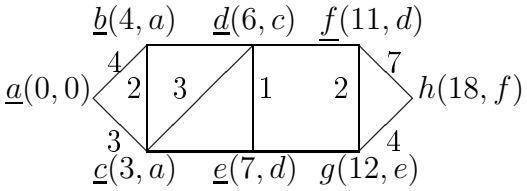


Поэтому $u^{(6)} = f$ и

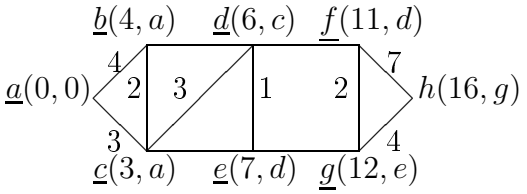
$$V_1^{(6)} = \{a, c, b, d, e, f\}, \quad V_2^{(6)} = \{g, h\},$$

$$\lambda(a)=0,\lambda(c)=3,\lambda(b)=4,\lambda(d)=6,\lambda(e)=7,\lambda(f)=\lambda^{(5)}(f)=11,$$
$$\lambda^{(6)}(g)=12,\lambda^{(6)}(h)=\infty.$$

Шаг 7. Имеются две вершины g и h в V_2 смежная с $u^{(6)}=f$. Очевидно, относительно $u^{(6)}$ эти вершины имеют веса $g(12,e)$ и $h(18,f)$.



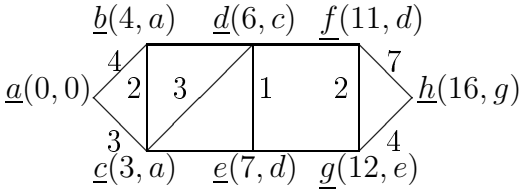
Сравнивая веса вершин g и h видим, что в качестве $u^{(7)}$ мы должны взять g.



Итак, $u^{(7)}=g$ и

$$V_1^{(7)}=\{a,c,b,d,e,f,g\},\quad V_2^{(7)}=\{h\},$$
$$\lambda(a)=0,\lambda(c)=3,\lambda(b)=4,\lambda(d)=6,\lambda(e)=7,\lambda(f)=11,\lambda(g)=\lambda^{(6)}(g)=12,$$
$$\lambda^{(6)}(h)=\infty.$$

Шаг 8. Осталось только одна вершина в V_2, именно h, смежная с $u^{(7)}=g$. Она имеет вес $h(16,g)$.



Итак, минимальное расстояние между вершинами a и h равно 16 и путь $acdegh$ – минимален.

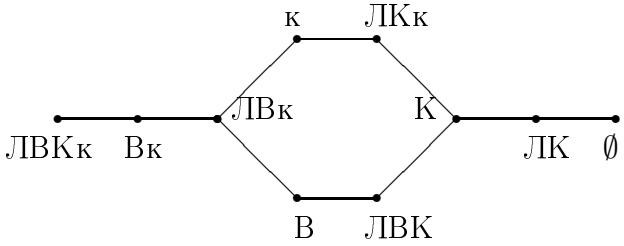
5.5.3 Задачи

1. Лодочник хочет переправить козу, волка и капусту на другой берег. Лодка кроме лодочника может брать только одного пассажира. Как лодочник переправится вместе со своими спутниками на другой берег? Нарисовать граф перемещении.

Решение. Вершины графа состояния соответствуют тем членам команды (лодочник, коза, капуста и волк), которые находятся на левом берегу. Цель – переплыть со всей командой на правый берег. При этом используются следующие сокращения: Л – лодочник, К – коза, В – волк, к – капуста.

В начальном состоянии на левом берегу находятся вся команда (состояние ЛВКк). В конечном состоянии на левом берегу должно находится пустое множество (состояние $\emptyset$). Итак, нам необходимо выяснить имеются ли в графе пути от вершины ЛВКк к вершине $\emptyset$.

Граф перемещения лодочника с козой, капустой и с волком:



Итак мы видим, что имеются два способа переправы.

Первый способ. Путь по верхней части графа { ЛВКк, Вк, ЛВк, к, ЛКк, К, ЛК, $\emptyset$} означает следующие движения лодочника.

1. (Состояние Вк) Переправляется с козой на правый берег. В левом берегу остается волк и капуста.

2. (Состояние ЛВк) Оставляет козу на правом берегу и возвращается в левый берег один.

3. (Состояние к) Берет волка и переправляется на правый берег.

4. (Состояние ЛКк) Оставляет волка на правом берегу, берет козу и переправляется в левый берег.

5. (Состояние К) Оставляет козу в левом берегу, берет капусту и с капустой переправляется на правый берег.

6. (Состояние ЛК) Оставляет капусту на правом берегу с волком и лодочник переправляется один на левый берег.

7. (Состояние $\emptyset$) Забирает козу и переправляется на правый берег.

Второй способ. Путь по нижним ребрам графа { ЛВКк, Вк, ЛВк, В, ЛВК, К, ЛК, $\emptyset$} означает следующие движения лодочника. Все как выше, за исключениями пунктов 3 и 4. Вместо них должны быть:

3. (Состояние В) Берет капусту и переправляется на правый берег.

4. (Состояние ЛКк) Оставляет капусту на правом берегу, берет козу и переправляется в левый берег.

2. ("Задача о трех ревнивых мужьях") Три супружеские пары подошли к реке, где они нашли маленькую лодку, которая не может поднять более двух человек одновременно. Переправа осложняется тем, что все мужья ревнивы и ни один из них не может допустить, чтобы его жена оставалась без него в компании, где есть какой-нибудь другой мужчина. Начертить граф допустимых перемещении.

3. Сосуд емкостью 8 литров наполнен водой. Разрешается переливать воду, используя пустые сосуды с емкостями 3 и 5 литров.

- Нарисовать граф состоянии (x, y, z), где x, y и z количества воды в литрах в трех сосудах (3, 4 и 5 литров соответственно).
- Показать, что воду можно разделить по 4 литра. Другими словами, состояние $(0, 4, 4)$ достижимо.
- Показать, что состояния $(1, 1, 6), (1, 2, 5), (2, 1, 5), (1, 3, 4), (1, 4, 3), (2, 2, 4)$, $(2, 3,), (2, 4, 2)$ не достижимы.

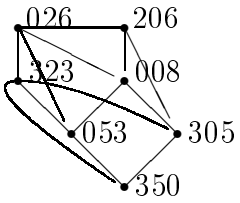
Указание. Обозначим состояние системы через (x, y, z), где x, y и z – количества литров воды в сосудах с 3, 5 и 8 литрами соответственно. Заметим, что уравнение $x + y + z = 8$ с условиями $0 \leq x \leq 3, 0 \leq y \leq 5, 0 \leq z \leq 8$, имеет 24 решении:

$$\{\{0, 0, 8\}, \{0, 1, 7\}, \{0, 2, 6\}, \{0, 3, 5\}, \{0, 4, 4\}, \{0, 5, 3\}, \{1, 0, 7\}, \{1, 1, 6\},$$

$$\{1, 2, 5\}, \{1, 3, 4\}, \{1, 4, 3\}, \{1, 5, 2\}, \{2, 0, 6\}, \{2, 1, 5\}, \{2, 2, 4\}, \{2, 3, 3\},$$

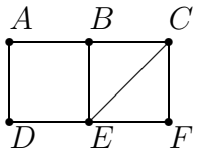
$$\{2, 4, 2\}, \{2, 5, 1\}, \{3, 0, 5\}, \{3, 1, 4\}, \{3, 2, 3\}, \{3, 3, 2\}, \{3, 4, 1\}, \{3, 5, 0\}\}.$$

Поэтому граф состоянии имеет 24 вершины. Например, часть графа имеет вид:

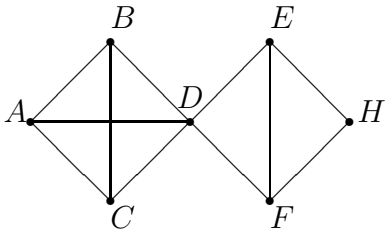


4. Пусть G – граф:

a)



b)

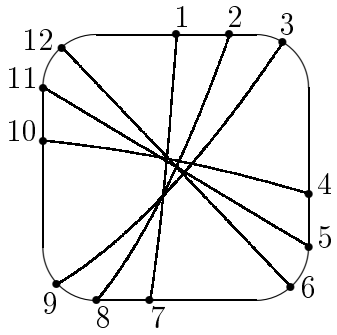


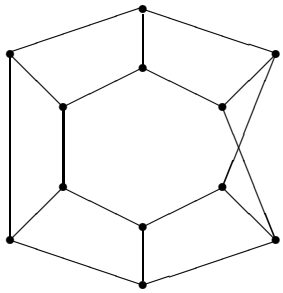
Найти

- множество вершин $V(G)$, множество ребер $E(G)$, степени вершин и проверить теорему о рукопожатиях
- найти все простые цепи от A до F

- все цепи от A до F
- дистанция от A до F
- диаметр графа G
- все циклы которые содержат вершину A
- все циклы в G.

5. Построить изоморфизм графов





6. i) Доказать, что для всякого дерева количество ребер на единицу меньше чем количество вершин.

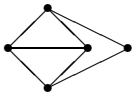
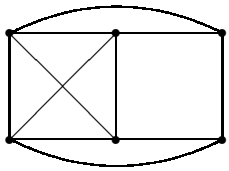
ii) Доказать, что связной граф, у которого количество ребер на единицу меньше чем количество вершин, является деревом.

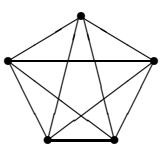
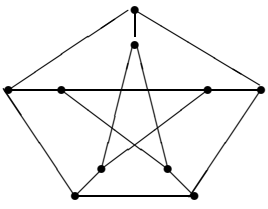
7. Доказать, что для всякого графа $G = (V, E)$ с k компонентами выполнено неравенство

$$|V| - k \leq |E| \leq (|V| - k)(|V| - k + 1)/2$$

Пример. Линейный граф $L(G)$ графа G имеет вершину, соответствующую каждому ребру графа G и две вершины $L(A)$ соединены ребром, если и только если соответствующие ребра графа A имеют общую вершину.

Тогда

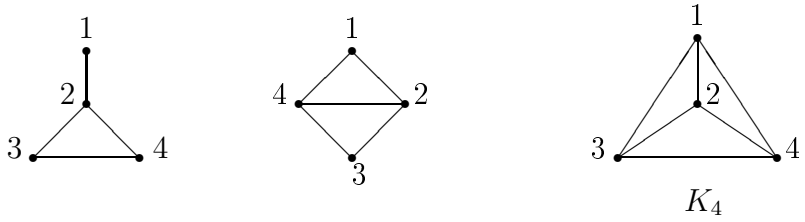
$G =$  $\Rightarrow$ $L(G) =$ 

$G =$  $\Rightarrow$ $\overline{L(G)} =$ 

Граф Петерсена

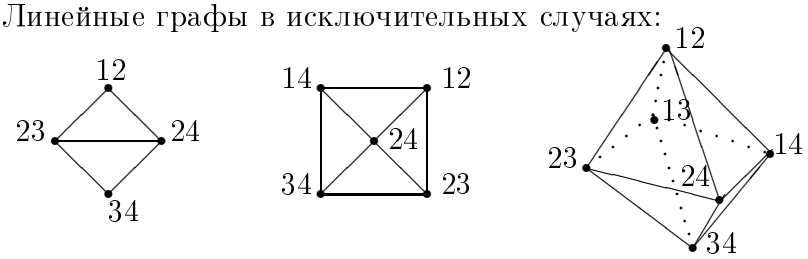
Автоморфизм графа G индуцирует автоморфизм $L(G)$, но последний граф может иметь дополнительные автоморфизмы.

Теорема. Пусть G – связный граф по крайней мере с тремя вершинами, тогда $Aut\,L(G) \cong Aut\,G$ если только граф G не является одним из следующих графов:



K_4

Линейные графы в исключительных случаях:

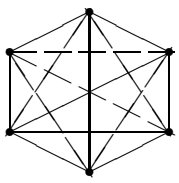


$L(K_4) =$ октаэдр

В каждом из исключительных случаев $Aut\,L(G)$ больше чем $Aut\,G$; например, $L(K_4)$ – октаэдр, но не все его симметрии индуцируются автоморфизмами K_4.

Дополнением графа G называется граф $\bar{G}$ с теми же вершинами, что и граф G и ребрами, которые соединяют две вершины графа $\bar{G}$ в том и только в том случае, если эти графы не соединены ребром в графе G. Граф называется *самодополнительной*, если $\bar{G} \cong G$.

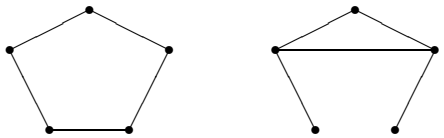
Пример. На следующем рисунке изображен граф (сплошные линии) и его дополнение (прерывистые линии)



Легко видеть, что граф и его дополнение, наложенное на одно и то же множество вершин образует полный граф с максимальным числом ребер $p(p-1)/2$, возможным у графа с p вершинами.

Если граф самодополнителен, то числа ребер графа и его дополнения одинаковы. Следовательно, $p(p-1)/2$ должно быть четным. Это возможно только при $p \equiv 0, 1 (mod\,4)$.

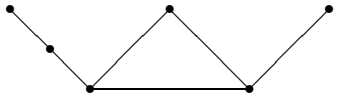
8. Доказать, что существуют ровно два самодополнительных графов с 5 вершинами:



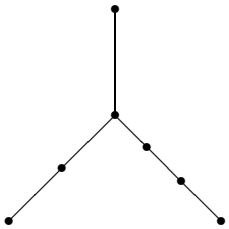
9. Сколько существуют самодополнительных графов с 6 и 7 вершинами ?

10. Граф называется *асимметрическим,* если других автоморфизмов, кроме тождественного автоморфизма нет: $Aut\,G =< e >$.

- Доказать, что асимметрических графов с числом вершин не более чем пяти, нет.
- Проверить, что следующий граф ассимметричен:

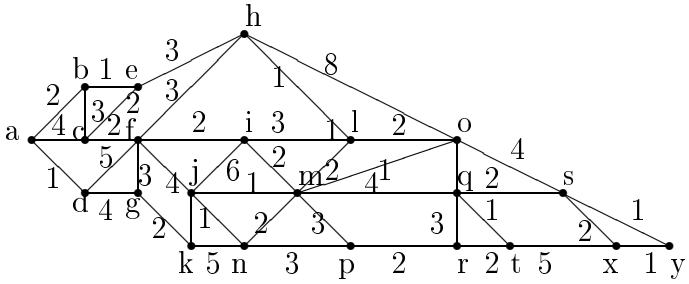


- Доказать, что всякий асимметрический граф с шестью вершинами изоморфен этому графу.
- Доказать, что асимметрических деревьев с числом вершин ≤ 6 нет
- Проверьте, что следующее дерево асимметричен



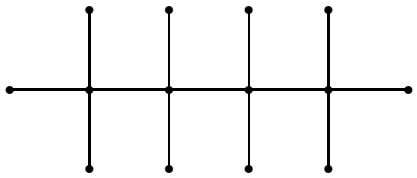
- Доказать, что других асимметрических деревьев с семью вершинами, нет.

11. Найти минимальное расстояние между вершинами a и x

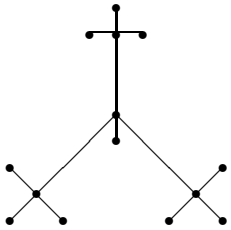


5.6 Графы и углеводороды

В этой секции приводятся применения теории графов в классификации предельных (насыщенных) углеводородов. Молекулы углеводорода состоят из атомов углерода (валентность 4) и атомов водорода (валентность 1) и они могут быть представлены в виде графа. Например, молекулы бутана и 2-метилпропана (изобутан) оба содержат четыре атомов углерода и десять атомов водорода:



бутан

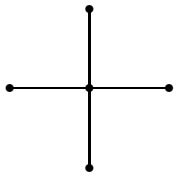


2-метилпропан

Такие неизоморфные структуры графов с одним и тем же количеством атомов углерода и водорода задают изомеры углеводорода. Выше показаны примеры изомеров C_4H_{10}.

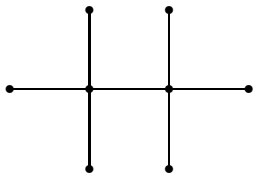
1. Доказать, что других изомеров C_4H_{10} нет.

2. Доказать, что C_1H_4 имеет ровно один изомер (метан)



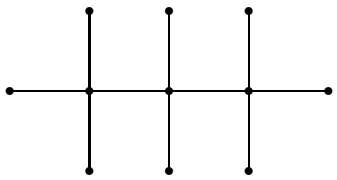
метан

3. Доказать, что C_2H_6 имеет ровно один изомер (этан)



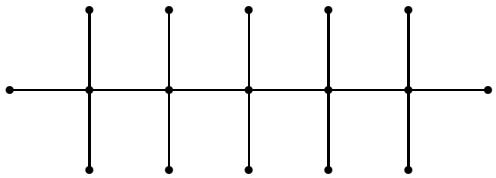
этан

4. Доказать, что C_3H_8 имеет ровно один изомер (пропан)

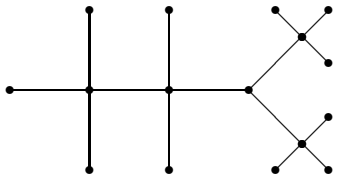


пропан

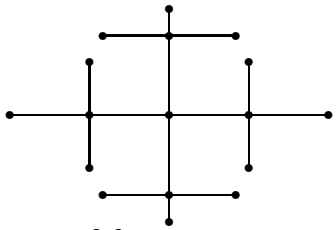
5. Доказать, что C_5H_{12} (пентан) имеет ровно три изомера



пентан

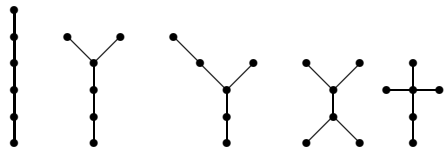


2-метилбутан



2,2-диметилпропан

6. Доказать, что C_6H_{12} (гексан) имеют ровно 5 изомеров. Они соответствуют следующим деревьям



Здесь для упрощения рисунков приведены лишь вершины соответствующие атомам углерода. Добавив к этому дереву водородные связи (легко убедиться, что число таких связей всегда будет $2n + 2$) так, чтобы степени всех его вершин равнялись четырем, получим полное изображение структуры соединения. Последовательное дерево соответствует прямой цепи углеводорода, в другие деревья - его изомерам.

7. Доказать, что всякая молекула углеводорода вида C_nH_{2n+2} (они называются парафином или алканами) имеют структуру дерева.

8. Доказать, что молекула углеводорода вида C_nH_{2n} (они называются алкенами) не имеют структуру дерева.

Глава 6

Темы для самостоятельных работ

Кто хочет получить оценку "отлично автоматом" может разработать одну из предложенных ниже тем. Для этого следует написать контрольные работы за два модуля на не ниже чем 60 баллов и темы должны быть разработаны на не ниже чем 20 баллов.

Желаю успехов !

6.1 Задачи

1. *Счастливые билеты.* (4)

Билет содержит 6 цифр. Билет называется счастливым, если сумма первых трех цифр совпадает с суммой последних трех. Сколько существуют счастливых билетов ?

2. *Красивые билеты.* (5)

Билет содержит 6 цифр. Билет называется красивым, если произведение первых трех цифр совпадает с произведением последних трех и все цифры разные. Например, билет с номером 643189 красив. Доказать, что существует ровно 144 красивых билетов.

Билет называется суперкрасивым, если он красив и счастлив. Доказать, что суперкрасивых билетов не существуют.

3. *Транзитивные отношения* (15)

Сколько существуют транзитивных отношении на множестве из n элементов ? Поэкспериментируйте на компьютере.

4. *Антисимметрические отношения* (7)

Сколько существуют антисимметрических отношении на множестве из n элементов ? Попробуйте вычислить это число для небольших n на компьютере.

5. *Отношения порядка* (15)

Сколько существуют отношении порядка на множестве из n элементов ? Быть может Вам поможет некоторый компьютерный эксперимент.

6. *Монотонные функции* (4)

Функция $f : A \to A$, где $A = \{1, 2, \ldots, n\}$, называется монотонной, если из условия $i < j$ следует, что $f(i) \leq f(j)$. Найти количество монотонных функции.

7. *Уравнение на множестве* $\{1, 2\}$ (3)

Сколько решении имеет уравнение $x_1 + \cdots + x_k = n$, где $x_i \in \{1, 2\}, i = 1, 2, \ldots, k, \quad k = 0, 1, 2, \ldots$?

8. *Еще одна формула для определителя* (5)

Пусть $A = (a_{i,j})$ – квадратная матрица порядка n. Наряду с известными формулами

$$\det A = \sum_{i=1}^{n} a_{i,j}\Delta_{i,j} = \sum_{j=1}^{n} a_{i,j}\Delta_{i,j},$$

где $\Delta_{i,j} = (-1)^{i+j} det\, A_{i,j}$ – алгебраическое дополнение, имеет место следующие "усложнения" этих формул.

Допустим, что все компоненты матрицы $A = (a_{i,j}) \in Mat_n$, $n \geq 3$, отличны от нуля. Тогда для любого $1 \leq j \leq n$,

$$det\, A = \sum_{i=1}^{n} \lambda_{i,j} a_{i,j} \Delta_{i,j},$$

и для любого $1 \leq i \leq n$,

$$det\, A = \sum_{j=1}^{n} \bar{\lambda}_{i,j} a_{i,j} \Delta_{i,j},$$

где

$$\lambda_{i,j} = (\prod_{s \neq i} a_{s,j})(\sum_{r=1}^{n} a_{1,r}^{-1} \cdots a_{i-1,r}^{-1} a_{i+1,r}^{-1} \cdots a_{n,r}^{-1}),$$

$$\bar{\lambda}_{i,j} = (\prod_{s \neq j} a_{i,s})(\sum_{r=1}^{n} a_{r,1}^{-1} \cdots a_{r,j-1}^{-1} a_{r,j+1}^{-1} \cdots a_{r,n}^{-1}).$$

Доказать.

9. *Ортогональные матрицы третьего порядка* (5)

Несмотря на сложность предыдущая формула для определителей имеет любопытное применение при изучении Адамаровых обратных матриц. Напомним, что Адамарова обратная $A^{(-1)}$ определяется для квадратных матриц с ненулевыми компонентами: если $A = (a_{i,j}), a_{i,j} \neq 0$, то $A^{(-1)} = (a_{i,j}^{-1})$.

Пусть A – любая ортогональная матрица порядка 3 с ненулевыми компонентами, т.е., $AA^t = E, a_{i,j} \neq 0$. Доказать, что матрица $A^{(-1)}$ вырождена.

10. *Мультиномиальные коэффициенты* (3)
Доказать формулу

$$(x_1 + \cdots x_k)^n = \sum_{i_1,\ldots,i_k} \binom{n}{i_1,\ldots,i_k} x^{i_1} \cdots x_k^{i_k},$$

где

$$\binom{n}{i_1,\ldots,i_k} = \frac{n!}{i_1! \cdots i_k!}$$

– мультиномиальные коэффициенты.

11. *Некоммутативный бином Ньютона* (15)
Допустим, что переменные x, y удовлетворяют условию

$$[x, y] = x$$

или

$$yx = x(y - 1).$$

Надо найти формулу для $(x + y)^n$.
Именно, докажите, что

$$(x + y)^n = \sum_{i=0}^{n} \lambda_n^i S_i(x, y),$$

где

$$S_0(x, y) = 1,$$

$$S_i(x, y) = \sum_{j=0}^{i-1} \binom{i}{j} x^i (y + 1) \cdots (y + i - j) + x^j$$

и

$$\lambda_0^0 = 1, \quad \lambda_n^i = \lambda_{n-1}^{i-1} - (i + 1)\lambda_{n-1}^i, i = 0, 1, \ldots, n.$$

Другими словами, (для тех, кто знает что такое число Стрилинга)

$$\lambda_n^i = (-1)^{n+i}\ \bar{s}_{n+1}^{i+1},$$

где $\bar{s}_n^i, 1 \leq i \leq n$, – числа Стирлинга второго рода.
При выводе формулы (коммутативной) Ньютона мы пользуемся законами ассоциативности и коммутативности. Например,

$$(x + y)^2 = (x + y)(x + y) = xx + xy + yx + yy =$$

$$(\text{тождество коммутативности}) = x^2 + 2xy + y^2.$$

В общем случае

$$(x+y)^2 = x^2 + 2xy + y^2 - [x,y],$$

где $[x,y] = xy - yx$ – коммутатор. Поэтому

$$(x+y)^2 = x^2 + 2xy + y^2 - x = S_0(x,y) - 3S_1(x,y) + S_2(x,y),$$

где

$$S_0(x,y) = 1, S_1(x,y) = y + 1 + x, S_2(x,y) = (y+1)(y+2) + 2x(y+1) + x^2.$$

При выводе формулы для суммы квадратов тождество ассоциативности не нужен. При выводе формулы для суммы кубов мы должны пользоваться законом ассоциативности, хотя бы для того чтобы определить что такое куб:

$$(xx)x = x(xx),$$

поэтому мы можем положить $x^3 = (xx)x = x(xx)$ не заботясь о том, где расположена скобка. Нас интересуют формулы для степеней суммы $(x+\ y)^n$ при этом разрешается расставлять скобки где хотим, но переставлять элементы мы должны с большой осторожностью, используя формулу $yx = xy - x$.

12. *Неассоциативная расстановка скобок.* (7)

Сколькими способами можно расставить скобки на n буквах? Например, имеется 5 способов расстановки скобок для 4 букв:

$$a(a(aa)), \quad (aa)(aa), \quad ((aa)a)a, \quad (a(aa))a, \quad a((aa)a).$$

Поскольку закона ассоциативности нет, все эти элементы различны. Надо доказать, что имеется

$$\frac{1}{n}\binom{2(n-1)}{n-1}$$

путей неассоциативных расстановок скобок. Такие числа называются числами Каталана. Имеется очень много других интерпретации чисел Каталана.

13. *Бинарные деревья* (7)

Найти количество бинарных корневых деревьев с n вершинами.

14. *Коммутативная расстановка скобок.* (20)

Предыдущая задача при условии закона коммутативности

$$ab = ba, \forall a, b.$$

Пусть c_n-количество коммутативных расстановок скобок на n буквах. Например, $c_4 = 2$, поскольку имеется только 2 способа коммутативных расстановок скобок на 4 буквах

$$a(a(aa)), \quad (aa)(aa).$$

Остальные 4-х буквенные элементы с помощью закона коммутативности сводится к этим двум елементам:

$$((aa)a)a = a((aa)a) = a(a(aa)),$$

$$(a(aa))a = a(a(aa)),$$

$$a((aa)a) = a(a(aa)).$$

Постройте коммутативные расстановки скобок для $n \leq 10$ и убедиться, что

n	1	2	3	4	5	6	7	8	9	10
c_n	1	1	1	2	3	6	11	23	46	98

Попробуйте найти асимптотику для c_n. Точной формулы для c_n аналогичной формуле Каталана неизвестно.

15. *Тождество Абеля.* (10)
Доказать, что для любых x, y, z,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x(x-kz)^{k-1}(y+kz)^{n-k},$$

16. *Игра в 15* (5)
Доска размером 4×4 заполнена 15 фишками, занумерованными числами $1, 2, \ldots, 15$. Вынимать фишки запрещено. Разрешается двигаться в свободную клетку как показано в следующем примере

15	2	3	14
8	6	7	10
9		11	12
13	5	4	1

$\Rightarrow$

15	2	3	14
8	6	7	10
9	5	11	12
13		4	1

$\Rightarrow$

15	2	3	14
8	6	7	10
9	5	11	12
	13	4	1

Можно ли в положении

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

с помощью таких движении поменять местами фишки с номерами 14 и 15 :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

$\Rightarrow$

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

?

17. *Формула Альперна.* (10)
Доказать, что

$$\frac{d^n}{dt^n}\{t^{n-1}f(\frac{1}{t})\} = \frac{(-1)^n}{t^{n+1}}f^{(n)}(\frac{1}{t}),$$

где $f^{(n)}(1/t)$– n-ая производная функции f в точке $1/t$.

18. *Теорема Вильсона* (4)
Доказать, что если p простое, то $(p-1)!+1$ делится на p.

19. *Двузначные числа, которые делятся на квадрат* (5)
Найти минимальное число k обладающее следующим свойством. Любое множество из k элементов, состоящее из целых чисел между 0 и 9 содержит два элемента такое, что двузначное число составленное ими имеет нулевую функцию Мебиуса.

20. *Число Раманудджана* (5)
Доказать, что $a^{1729} \equiv a(mod\,1729)$ для всех $a \in \mathbf{Z}$.

21. *Уравнение* $x!+1=y^2$ (15)
Решить уравнение $x!+1=y^2$ в целых числах. Это уравнение имеет решения $(x,y)=(4,5),(5,11),(7,71)$. Неизвестно существуют ли другие целочисленные решения.
Следующая задача касается этой темы и ее решение не является сложным.

22. *Уравнение* $x!+a=y^2$. (3)
Пусть a – натуральное число. Уравнение $x!+a=y^2$, где a не является квадратом, имеет конечное число целочисленных решении. Уравнение $x!-a=y^2$ имеет конечное число целочисленных решении при любом a.

23. *Рассеянный гардеробщик.* (5)
Джентельмены сдали в гардероб свои шляпы. Когда головные уборы были возвращены, они заметили, что гардеробщик все перепутал и никто не получил свою шляпу обратно. Сколькими способами он это может сделать, если количество джентельменов – n.
(Для тех кто знает что такое вероятность) Найти вероятность такого события.

24. *Тождества Ли* (3)
Пусть A – ассоциативное кольцо с умножением $\circ$. Другими словами в A выполнено тождество

$$a \circ (b \circ c) = (a \circ b) \circ c, \quad \forall a,b,c \in A.$$

Введем в A новое умножение обозначаемое квадратной скобкой $[\,,\,]$ по правилу

$$[a,b] = a \circ b - b \circ a.$$

Это умножение называется умножением Ли или коммутатором Ли в честь норвежского математика Софуса Ли. Докажите что новое кольцо удовлетворяет тождествам

$$[a,b] = -[b,a],$$
$$[[a,b],c] + [[b,c],a] + [[c,a],b] = 0.$$

25. *Тождества Йордана.* (4)

Пусть A– ассоциативное кольцо с умножением $\circ$. Введем в A новое умножение обозначаемое фигурной скобкой $\{a,b\}$, и определяемое по правилу

$$\{a,b\} = a \circ b + b \circ a.$$

Это умножение называется Йордановым умножением в честь немецкого математика Йордана. Такие умножения возникли в квантовой физике. Докажите, что новое умножение удовлетворяет тождествам

$$\{a,b\} = \{b,a\},$$
$$\{\{a,a\},\{b,a\}\} = \{\{\{a,a\},b\},a\}.$$

26. *Тождества для q-коммутаторов.* (10)

Пусть A – ассоциативное алгебра над полем комплексным чисел $\mathbf{C}$ с умножением $\circ$ и $q \in \mathbf{C}$. Наделим A новым умножением $\circ_q$ (назовем его q-коммутатором) определяемым по правилу

$$a \circ_q b = a \circ b + q\, b \circ a.$$

Доказать, что $\circ_q$ удовлетворяет тождеству

$$(q-1)^2(a,c,b) + q\,[c,[a,b]] = 0,$$

где положены

$$(a,b,c) = a \circ_q (b \circ_q c) - (a \circ_q b) \circ_q c,$$
$$[a,b] = a \circ_q b - b \circ_q a.$$

27. *Тождества Торткен* (5)

Пусть $A = \mathbf{C}[x]$– алгебра многочленов относительно умножения

$$a \circ b = \partial(ab).$$

Здесь $\partial = \frac{\partial}{\partial x}$ – обычное дифференцирование и ab – обычное умножение многочленов. Например, $\partial(x^5) = 5x^4$ и $x^3 \circ x^5 = 5x^7$. Доказать, что выполнено тождество

$$(a \circ b) \circ (c \circ d) - (a \circ d) \circ (b \circ c) = (a,b,c) \circ d - (a,d,c) \circ b,$$

где положено $(a,b,c) = a \circ (b \circ c) - (a \circ b) \circ c$.

28. *Произведения сумм квадратов* (4)

Произведение суммы двух квадратов есть сумма квадратов:

$$a = x^2 + y^2, b = z^2 + t^2 \Rightarrow ab = (x^2 + y^2)(z^2 + t^2) = (xz)^2 + (yz)^2 + (xt)^2 + (yt)^2$$

$$= (xz)^2 + 2xyzt + (yt)^2 + (xt)^2 - 2xyzt + (yz)^2 =$$

$$(xz + yt)^2 + (xt - yz)^2.$$

Другими словами, множество

$$A = \{x^2 + y^2 \,|\, x, y \in \mathbf{Z}\}$$

замкнуто относительно умножения:

$$a, b \in A \Rightarrow ab \in A.$$

А. Кэли рассматривает обобщение этого вопроса. Для каких k множество

$$A = \{x_1^2 + \cdots + x_k^2 \,|\, x_1, \ldots, x_k \in \mathbf{Z}\}$$

замкнуто относительно умножения ?

Докажите, что утверждение верно :

- для четырех квадратов;
- для восьми квадратов.

Верно ли это утверждение для суммы трех квадратов? Двух кубов ?

29. *Произведения попарных разностей* (15)

(A. Cayley, *Report of the British Association for the Advancement of Science,* (1875), p.10, =*Mathematical Papers,* v.9, 1896, 426.) Кэли изучает вопрос представимости произведении попарных разностей в виде суммы и разности квадратов попарных разностей. Среди прочих от отмечает следующий любопытный факт.

$$2(a-b)(b-c)(c-d)(d-a) = (b-c)^2(a-d)^2 - (c-a)^2(b-d)^2 + (a-b)^2(c-d)^2$$

Доказать.

A. Cayley, *On a relation between certain products of differences,* Quaterly J. Pure Appl. Math.m v. 15, 1878, pp. 174, 175.

Еще один любопытный факт на тему произведении разностей.

$$S[a,b,c]\ S[d,c] + S[b,d,c]\ S[a,c] + S[d,a,c]\ S[b,c] = 0,$$

где

$$S[a,b,c] = (a-b)(b-c)(c-a),$$

$$S[a,b] = (a-b)(b-a).$$

Докажите.

Составьте программу на Basic, C или Pascal или на каком-либо другом языке программирования и проверьте эти соотношения. Было бы интересно найти другие соотношения такого плана с помошью компьютера.

Проверьте например вручную и затем на компьютере следующее соотношение для произведении разностей от пяти элементов

$$\begin{gathered}3S[a,b,c]\ S[d,e]+3S[b,c,d]\ S[e,a]+3S[c,d,e]\ S[a,b]\\ +3S[d,e,a]\ S[b,c]+3S[e,a,b]\ S[c,d]\\ -S[a,b,d]\ S[c,e]-S[b,c,e]\ S[d,a]-S[c,d,a]\ S[e,b]\\ -S[d,e,b]\ S[a,c]-S[e,a,c]\ S[b,d]\\ =10\ S[a,b,c,d,e],\end{gathered}$$

where

$$S[a,b,c,d,e]=(a-b)(b-c)(c-d)(d-e)(e-a).$$

Кэли не приводит доказательства. Мне неизвестно простое доказательство этого факта. Для меня гораздо более интересен вопрос: Существует ли аналогичная формула для произведении попарных разностей от шести элементов?

30. *Вариации на тему произведении попарных разностей* (7)

Пусть A – ассоциативное коммутативное кольцо и $\mathcal{F}^k(A,A)$ – множество функции от k аргументов $A\times\cdots\times A\to A$.

Определим произведение $\mathcal{F}^k(A,A)\times\mathcal{F}^l(A,A)\to\mathcal{F}^{k+l}(A,A)$ по правилу

$$\psi\smile\phi(a_1,\dots,a_{k+l})=\sum_{\sigma\in Sym_{k,l-1}} sgn\,\sigma\,\psi(a_{\sigma(1)},\dots,a_{\sigma(k)})\phi(a_{\sigma(k+1)},\dots,a_{\sigma(k+l-1)},a_{k+l}),$$

где

$$Sym_{k,l}=\{\sigma\in Sym_{k+l}\,|\,\sigma(1)<\ldots<\sigma(k),\ \sigma(k+1)<\cdots<\sigma(k+l)\}.$$

Пусть

$$s_k(a_1,\dots,a_k)=(a_1-a_2)(a_2-a_3)\cdots(a_{k-1}-a_k)(a_k-a_1).$$

Доказать, что

$$\begin{gathered}s_{2i}\smile s_l=2\binom{[l/2]+i-1}{i}s_{2i+l},\\ s_{2i+1}\smile s_l=0,\quad\forall 0<i,1<l.\end{gathered}$$

$$\sum_{i=1}^{2k+1}(-1)^i s_{2k}(a_1,\dots,\hat{a_i},\dots,a_{2k+1})=-2(a_1-a_2)(a_2-a_3)\cdots(a_{2k}-a_{2k+1}),$$

$$\sum_{i=1}^{2k+1}(-1)^i a_i s_{2k}(a_1,\dots,\hat{a_i},\dots,a_{2k+1})=-(a_1-a_2)(a_2-a_3)\cdots(a_{2k}-a_{2k+1})(a_{2k+1}+a_1),$$

$$\sum_{i=1}^{2k+1}(-1)^i a_i^2 s_{2k}(a_1,\dots,\hat{a_i},\dots,a_{2k+1}) = -2a_1a_{2k+1}(a_1-a_2)\cdots(a_{2k}-a_{2k+1}).$$

В общем случае,

$$\sum_{i=1}^{2k+1}(-1)^i a_i^r s_{2k}(a_1,\dots,\hat{a_i},\dots,a_{2k+1})$$

делится на

$$(a_1-a_2)\cdots(a_{2k}-a_{2k+1})$$

для всех r.

$$\sum_{i=1}^{2k}(-1)^i s_{2k-1}(a_1,\dots,\hat{a_i},\dots,a_{2k}) = 0,$$

$$\sum_{i=1}^{2k}(-1)^i a_i s_{2k-1}(a_1,\dots,\hat{a_i},\dots,a_{2k}) = 0,$$

$$\sum_{i=1}^{2k}(-1)^i a_i^2 s_{2k-1}(a_1,\dots,\hat{a_i},\dots,a_{2k+1}) = 0,$$

$$\sum_{i=1}^{2k}(-1)^i a_i^3 s_{2k-1}(a_1,\dots,\hat{a_i},\dots,a_{2k+1}) = (\sum_{i=1}^{2k-1}(-1)^i a_i a_{i+1} + a_{2k}a_1)s_{2k}(a_1,\dots,a_{2k}).$$

В общем случае,

$$\sum_{i=1}^{2k}(-1)^i a_i^r s_{2k-1}(a_1,\dots,\hat{a_i},\dots,a_{2k})$$

делится на

$$s_{2k}(a_1,\dots,a_{2k})$$

для всех r.

Частные случаи:

$$\sum_{i=1}^{4}(-1)^i a_i^3 s_3(a_1,\dots,\hat{a_i},\dots,a_4) = \prod_{1\le i<j\le 4}(a_i-a_j),$$

$$\sum_{i=1}^{4}(-1)^i a_i^4 s_3(a_1,\dots,\hat{a_i},\dots,a_4) = (\sum_{i=1}^{4} a_i)\prod_{1\le i<j\le 4}(a_i-a_j),$$

$$\sum_{i=1}^{4}(-1)^i a_i^5 s_3(a_1,\dots,\hat{a_i},\dots,a_4) = (\sum_{1\le i<j\le 4} a_i a_j)\prod_{1\le i<j\le 4}(a_i-a_j).$$

31. *Функции Аккермана.* (3)

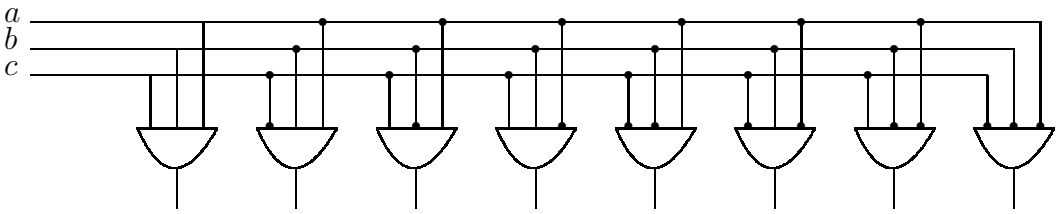
Функции Аккермана - функция от двух неотрицательных целочисленных аргументов, определенная следующей рекурсивной процедурой

- Если $m = 0$, то $A(m, n) = n + 1$.
- Если $m \neq 0$ но $n = 0$, то $A(m, n) = A(m - 1, 1)$
- Если $m \neq 0$ и $n \neq 0$, то $A(m, n) = A(m - 1, A(m, n - 1))$.

Вычислить $A(1, 3)$.

32. *Упрощение одноступенной схемы для перекодирования* (5)

Восемь трехразрядных двоичных чисел имеют вид (a, b, c), где $a, b, c \in \{0, 1\}$. Каждый из восьми разрядов кода 1-из-8 доставляется в точности одной из восьми совершенных конъюнкций, которые принимают значение 1 в точности для одной комбинации a, b, c, как показано в следующем одноступенном устроиство для перекодирования



Требуется построить пирамидальную схему эквивалентную ей используя три отрицания и двенадцать двуместных конъюнкции.

33. *Система электронного голосования* (3)

Комитет из трех человек хочет применить электронную схему для тайного голосования простым большинством голосов. Построить такую схему, чтобы каждый член, голосующий "за" нажимал кнопку и не нажимал ее, если он голосует против, и чтобы в случае , если большинство членов комитета проголосует "за" загоралась сигнальная лампочка.

34. *Числа Фиббоначчи* (3)

Числа Фиббоначчи определяется реккурентной формулой

$$F_0 = 0, \quad F_1 = 1,$$

$$F_n = F_{n-1} + F_{n-2}, \quad n > 1.$$

Доказать, что

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

35. *Фиббоначчиева система счисления* (8)

Доказать, что для любого натурального числа $a \in \mathbf{N}$

- существует представление в виде линейной комбинации с помощью чисел Фиббоначчи $a = \lambda_1 F_n + \lambda_2 F_{n-1} + \cdots + \lambda_{n-1} F_2$ и чисел $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ принимающих значения $0, 1$, таких, что $\lambda_i \lambda_{i+1} = 0$, для всех $i \geq 1$.

- Такое представление единственно. Коэффициенты $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ называются фиббоначчиевыми цифрами числа a и последовательность $\lambda(a) = \lambda_1 \lambda_1 \cdots \lambda_{n-1}$ называется фиббоначиевой записью числа a. Например, $\lambda(19) = 101001$ так как $19 = F_7 + F_5 + F_2$.

- Всякая ли запись с помощью нулей и единиц может быть принять в качестве фиббоначчиевой записи?

36. *Открытие английского геолога* (10)

В 1816 г. английский геолог Фарей расположил в неубывающем порядке все правильные числа со знаменателями, не большими N, и получил, то что сейчас называют последовательностью Фарея f_N. Например, f_3 – это $\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$.

- Доказать, что в ряде f_N при $N > 1$ нет двух соседних дробей с одинаковыми знаменателями.

- Пусть $\frac{a}{b}$ и $\frac{c}{d}$ – соседние члены ряда f_N. Доказать, что $ad - bc = 1$.

- Пусть $\frac{1}{b}$ и $\frac{c}{d}$ – соседние дроби Фарея. Доказать, что дроби $\frac{a+c}{b+d}$ и $\frac{a+b}{c+d}$ несократимы.

- Доказать, что количество элементов последовательности f_N равно $\sum_{i=1}^{N} \phi(i) + 1$.

- Пусть $\frac{a}{b} \leq \alpha \leq \frac{c}{d}$, $\frac{a}{b}$ и $\frac{c}{d}$ – соседние числа в ряде Фарея f_N. Тогда справедливы хотя бы одно из трех неравенств:

$$|\alpha - \frac{a}{b}| < \frac{1}{\sqrt{5} b^2}, \qquad |\alpha - \frac{c}{d}| < \frac{1}{\sqrt{5} d^2}, \qquad |\alpha - \frac{a+c}{b+d}| < \frac{1}{\sqrt{5}(b+d)^2}.$$

37. *Степень дифференцирования в характеристике p* (15)

Пусть $\partial = \frac{\partial}{\partial x}$ – дифференцирование алгебры многочленов $\mathbf{C}[x]$. Доказать, что для любого $f = f(x) \in \mathbf{C}[x]$

$$\partial^{p-2}(f^{p-1}) + (f\partial)^{p-2}(f) \equiv 0 (mod\, p).$$

Проверим это для небольших p. Пусть $p = 3$. Тогда по правилу Лейбница

$$\partial(f^2) = 2f\partial(f) \Rightarrow \partial(f^2) + f\partial(f) = 3f\partial(f) \equiv 0 (mod 3)$$

Пусть $p = 5$. Тогда по правилу Лейбница

$$\partial^3(f^4) = \partial^2(4f^3\partial(f)) = \partial(12f^2(\partial(f))^2 + 4f^3\partial^2(f))$$

$$= 24f(\partial(f))^3 + 24f^2\partial(f)\partial^2(f) \quad + 12f^2\partial(f)\partial^2(f) + 4f^3\partial^3(f)$$
$$= 24f(\partial(f))^3 + 36f^2\partial(f)\partial^2(f) + 4f^3\partial^3(f)$$

$$(f\partial)^3(f) = (f\partial)^2(f\partial(f)) = f\partial(f^2\partial^2(f) + f(\partial(f))^2) = 2f^2\partial(f)\partial^2(f) + f^3\partial^3(f)$$
$$+f(\partial(f))^3 + 2f^2\partial(f)\partial^2(f)$$

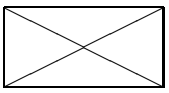
$$= f(\partial(f))^3 + 4f^2\partial(f)\partial^2(f) + f^3\partial^3(f)$$

и

$$\partial^3(f^4) + (f\partial)^3(f) = 25f(\partial(f))^3 + 40f^2\partial(f)\partial^2(f) + 5f^3\partial^3(f) \equiv 0(mod5).$$

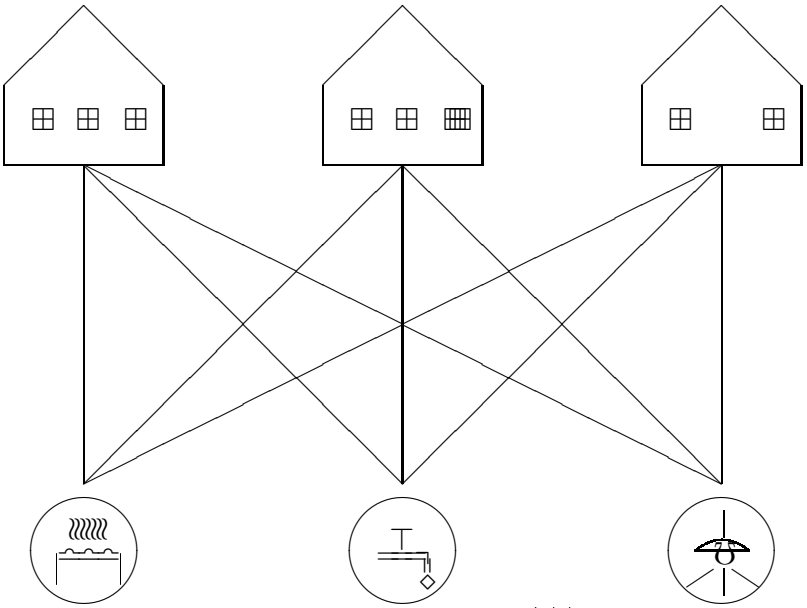
Тому, кто решит эту задачу приз в 300$

38. *Открытые и закрытые конверты* (3)

Можно ли единым росчерком пера не поднимая перо от бумаги нарисовать открытый конверт  ? А что, если конверт закрыть  ? Можно ли его нарисовать единым росчерком пера ?

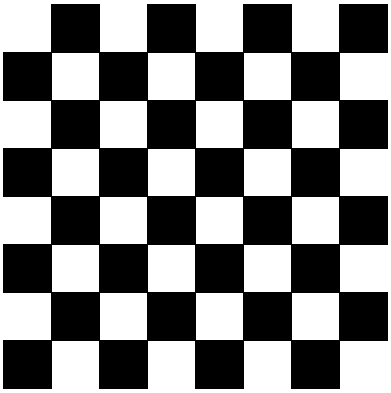
39. *Газ, вода и электричество* (5)

Нужно провести газ, воду и электричество в три дома так, чтобы их линии не пересекались. Можно ли это сделать?



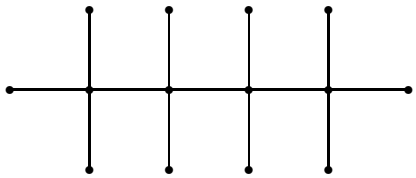
40. *Путешествие коня* (5)

Может ли конь обойти шахматное поле, побывав в каждой клетке ровно по одному разу? Другая формулировка: является ли граф с вершинами в шахматных клетках и ребрами, порожденными всевозможными движениями коня, гамильтоновым ?

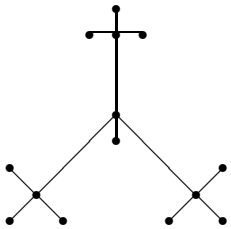


41. *Структуры углеводородов парафинового ряда* (15)

Молекулы углеводорода состоят из атомов углерода (валентность 4) и атомов водорода (валентность 1) и они могут быть представлены в виде графа. Например, молекулы бутана и 2-метилпропана (изобутан) оба содержат четыре атомов углерода и десять атомов водорода:



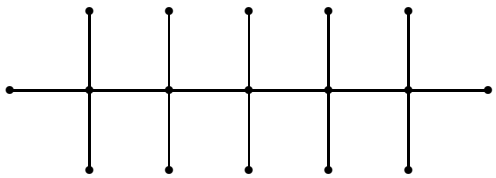
бутан



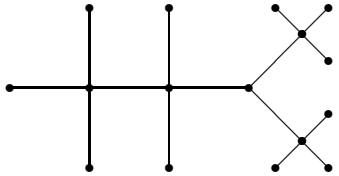
2-метилпропан

Такие неизоморфные структуры графов с одним и тем же количеством атомов углерода и водорода задают изомеры углеводорода. Выше показаны примеры изомеров C_4H_{10}. Доказать, что других изомеров C_4H_{10} нет.

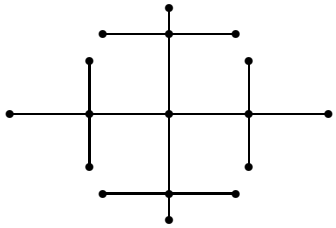
Доказать, что C_5H_{12} имеет ровно три изомера



пентан



2-метилбутан



2,2-диметилпропан

Подсчет числа всевозможных изомеров для парафинового ряда C_nH_{2n+2}, как и для ряда других органических соединений, основан на сложных методах комбинаторного анализа и в значительной мере стимулировала его развитие. Количества различных деревьев связанных с C_nH_{2n+2} при небольших n приведены ниже

n	1	2	3	4	5	6	7	8	9	10	11	12	13
Количество деревьев	1	1	1	2	3	5	9	18	35	75	159	357	799

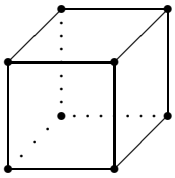
Попробуйте повторить некоторые из этих вычислении. Например, для $n = 6, 7$. Постройте соответствующие деревья.

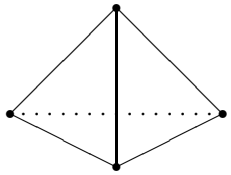
42. *Шахматы* 5×5. *Существует ли гамильтонов цикл для хода коня*
????

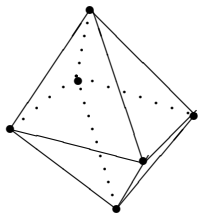
43. *Разбиение квадрата на меньшие квадраты*
???

44. *Молекулы на многогранниках* (15)

Пусть атомы q различных сортов располагаются всевозможными способами в вершинах правильного многогранника M. "Молекулы" получающиеся друг из друга поворотом вокруг некоторой оси, не различаются. Пусть $f(M, q)$ – число различных "молекул". Получить формулы:

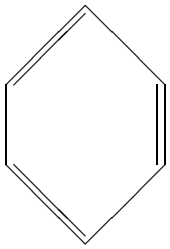
$M =$  , $f(\text{куб}, q) = \frac{q^2(q^6+17q^2+16)}{24}$,

$M =$  , $f(\text{тетраэдр}, q) = \frac{q^2(q^2+11)}{12}$,

$M =$  , $f(\text{октаэдр}, q) = \frac{q^2(q^4+3q^2+12q+8)}{24}$

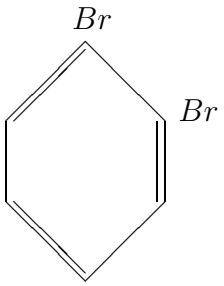
45. *Химические формулы на бензоловом кольце* (4)

Сколько различных химических формул можно получить прикрепляя радикалы CH_3 или H в вершинах бензолового кольца



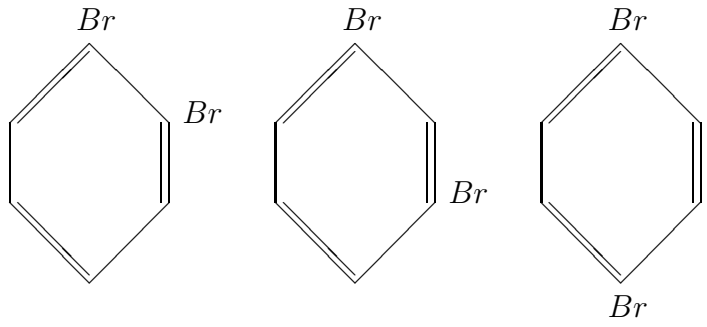
Тот же вопрос: только теперь разрешается сажать радикалы CH_3 H, OH или брома Br в вершинах атомов углерода.

Пример. Существует ровно один однозамещенный бромбензол



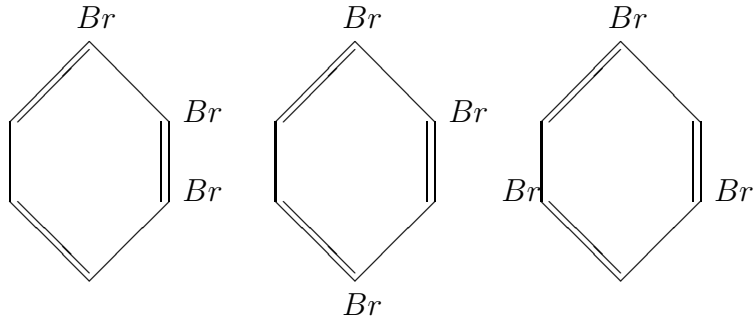
моно-бромбензол

Для двабромозамещенного бензола существуют 3 изомерных соединения:



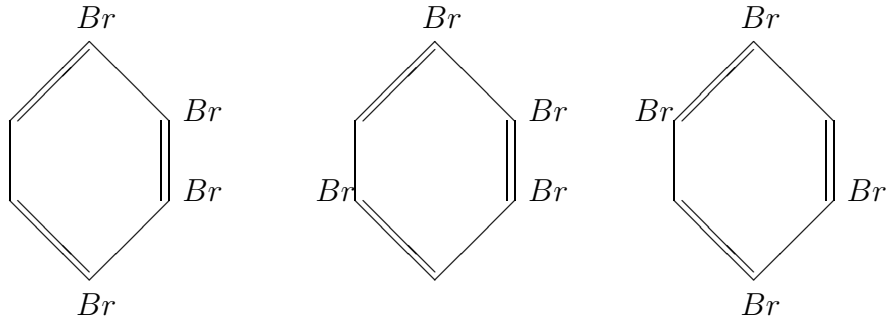
орто-бромбензол (1,2-дибромбензол) мета-бромбензол (1,3-дибромбензол) пара-бромбензол (1,4-дибромбензол)

Для трибромозамещенного бензола существуют 3 изомера:



1,2,3-бромбензол 1,2,4-бромбензол 1,3,5-бромбензол

Для четырехзамещенных бензолов существуют 3 изомера:



1,2,3,4-тетрабромбензол 1,2,3,5-тетрабромбензол 1,2,4,6-тетрабромбензол

Формулу для количества изомеров можно получить из теоремы Бернсайда. Пусть G – конечная группа и G действует на множестве M. Другими словами пусть задана функция

$$\alpha : G \times M \to M$$

такая, что

$$\alpha(g \circ h, m) = \alpha(g, \alpha(h, m)), \quad \forall g, h \in G, \forall m \in M,$$
$$\alpha(e, m) = m, \quad \forall m \in M.$$

Для упрощения записи вместо $\alpha(g, m)$ будем писать $g(m)$. Пусть

$$Fix\, g = \{m \in M | gm = m\}$$

– фиксатор элемента $g \in G$. Введем бинарное отношение на множестве M по правилу mRn, если $m = g(n)$ для некоторого $g \in G$. Проверьте, что R будет отношением эквивалентности.

Тогда количество классов эквивалентности можно вычислить по формуле

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix\, g|.$$

В этом и состоит теорема Бернсайда. Широкое применение теоремы Бернсайда при изучении химических формул было сделано известным математиком и педагогом Пойа.

6.2 Литература

1. *Алгебра и теория чисел,* под ред. Виленкина, Москва "Просвещение", 1984.

2. Н.Е. Воробьев, *Числа Фиббоначчи,* Москва, "Наука", 1992.

3. И.М. Виноградов. *Основы теории чисел,* Москва "Наука", 10-ое изд., 1981.

4. В.А. Горбатов, *Основы дискретной математики,* Москва "Высшая школа", 1986.

5. О. П. Кузнецов, Г.М. Адельсон-Вельский, *Дискретная математика для инженера,* Москва, "Энергия", 1980.

6. Г.И. Москинова *Дискретная математика (математика для менеджера в примерах и задачах),* Москва, "Логос", 2003.

7. Ф.А. Новиков, *Дискретная математика для программистов*, Санкт-Петербург, 2000.

8. С.В. Судоплатов, Е.В. Овчинникова, *Элементы дискретной математики,* Москва, Новосибирск, 2002.

9. В.П. Сигорский, *Математический аппарат инженера,* Киев, "Техніка", 1975.

10. С.Е. Рукшин, *Теория чисел в задачах,* Алматы, 2001.

11. С.В. Яблонский, *Введение в дискретную математику,* Москва, "Наука", 1979.

12. R. Grimaldi, *Discrete and combinatorial mathematics*, fourth ed., Addison-Wesley, 1999.

13. B. Kolman, R. C. Busby, *Discrete mathematical structures for computer science,* Prentice-Hall Int., 1984.

14. J. Matousek, J. Nesetril, *Invitation to discrete mathematics,* Clarendon Press, Oxford, 1999.

15. K. Rosen, *Discrete mathematics and its applications,* thrid ed., McGraw-Hill, 1995.