Süleyman Demirel University
Engineering Faculty

Department of Natural Sciences, Mathematics and Informatics

А.С.Джумадильдаев

Элементы дискретной математики

Учебное пособие. Часть 1.

Almaty – 2004

Süleyman Demirel University
Engineering Faculty

Department of Natural Sciences, Mathematics and Informatics

А.С.Джумадильдаев

Элементы дискретной математики

Учебное пособие. Часть 1.

Almaty – 2004

ББК 22.176я73
Д42

Книга содержит конспект лекций, прочитанных на первом курсе в Университете им. Сулеймана Демиреля и в Казахстанско-Британском Техническом Университете 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 недели. В ней будут обсуждены следующие темы:

- Алгебраические структуры
- Логика высказываний и булевые функции
- Элементы теории графов.

Рекомендовано к печати Ученым Советом Университета имени Сулеймана Демиреля.

Джумадильдаев А.С.
Д42 Элементы дискретной математики: Учебное пособие, Часть 1 – Алматы, 2004, 92 с.

ISBN 9965-9150-9-1

ББК 22.176я73

Д $\frac{1602120000}{00(15)-04}$

ISBN 9965-9150-9-1

Оглавление

1 Множества **3**
- 1.1 Множества, подмножества и элементы . . . 3
- 1.2 Парадокс Рассела . . . 5
- 1.3 Булеан. Диаграммы Венна . . . 5
- 1.4 Тождества алгебры множеств . . . 6
- 1.5 Задачи . . . 8

2 Отношения и функции **12**
- 2.1 Декартово произведение и отношения . . . 12
- 2.2 Отношение эквивалентности . . . 14
- 2.3 Отношение порядка . . . 16
- 2.4 Операции над отношениями . . . 16
- 2.5 Функции . . . 18
- 2.6 Задачи . . . 20

3 Комбинаторика и теория чисел **25**
- 3.1 Принципы счета . . . 25
- 3.2 Принцип Дирихле . . . 26
  - 3.2.1 Задачи . . . 28
- 3.3 Формула включения - исключения . . . 29
  - 3.3.1 Задачи . . . 32
- 3.4 Биномиальные коэффициенты . . . 33
  - 3.4.1 Задачи . . . 35
- 3.5 Функции на конечных множествах . . . 36
- 3.6 Математическая индукция . . . 38
  - 3.6.1 Задачи . . . 39
- 3.7 Числа Фиббоначчи . . . 41
  - 3.7.1 Задачи . . . 42
- 3.8 Реккурентные соотношения . . . 43
  - 3.8.1 Задачи . . . 46
- 3.9 Производящие функции . . . 46
  - 3.9.1 Задачи . . . 52
- 3.10 Целые числа и делимость . . . 53

3.10.1 Задачи 55
3.11 Сравнения 58
3.12 Цепные дроби 60
3.12.1 Задачи 64
3.13 Мультипликативные функции 64
3.13.1 Задачи 67
3.14 Решение уравнении в целых числах 69
3.14.1 Задачи 69
3.15 Компьютеры и простые числа 72
3.15.1 Компьютерные тесты на простоту чисел 72
3.15.2 Крипосистема с открытым ключом 76

4 Темы для самостоятельных работ 79
4.1 Задачи 79
4.2 Литература 90

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:

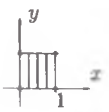
"неделя"={ понедельник, вторник, среда четверг, пятница, суббота, воскресенье}.

Пример. Множество "Гражданс 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



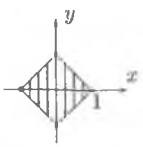
или в виде множества решении неравенств

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

или, еще проще, в виде решении неравенств

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

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

- $A \cup A = A$, $A \cap A = A$ (идемпотентность)
- $A \cup B = B \cup A$, $A \cap B = B \cap A$ (коммутативность)
- $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ (ассоциативность)

- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (дистрибутивность)
- $A \cup \emptyset = A$, $A \cap U = A$, $A \cup U = U$, $A \cap \emptyset = \emptyset$ (нейтральность)
- $\bar{\bar{A}} = A$(инволютивность)
- $A \cup \bar{A} = U$, $A \cap \bar{A} = \emptyset$ $U = \emptyset$, $\emptyset = U$ (дополнение)
- $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$, $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$ (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

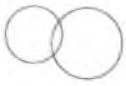
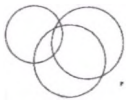
$$x \in X \Rightarrow x \in Y$$

и

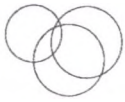
$$y \in Y \Rightarrow y \in X.$$

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

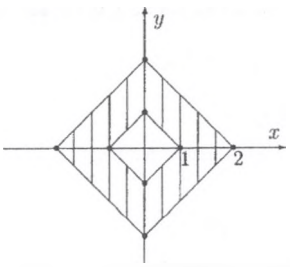
- $\bar{A}, \bar{B}, \bar{C}$
- $A \setminus B, B \setminus C, C \setminus E$,
- $A \cup B, B \cap C, A \cap B$,
- $A \oplus B, A \oplus C, B \oplus C$.

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. $R = A \times A$

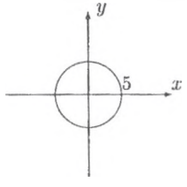
Пустое отношение. $R = \emptyset \subset A \times A$

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

$$\text{яйцо} \quad R \quad \text{корова}$$

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

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 значений,

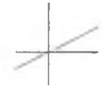
$$Im(R) = \{b \mid (a,b) \in R, \text{ для некоторого } a \in A\}.$$

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 отношений $R \subseteq A \times A$:

- 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 элемеитов. 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

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

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

2.3 Отношение порядка

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

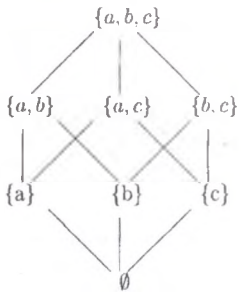
Пример. Отношение $a \prec b$ определенное по правилу $a|b$ задает порядок на множестве $\mathbf{N}$.

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 отиосительно 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 (объединение, 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: $f : A \to B$, $A \xrightarrow{f} B, f : x \mapsto f(x)$.

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. $f : \mathbf{R} \to \mathbf{R}$, $x \mapsto x^2$, – не инъективна и не сюръективна.
Пример. $f : \mathbf{R} \to \mathbf{R}^+$, $x \mapsto x^2$. – сюръективна, но не инъективна.
Пример. $f : \mathbf{Z} \to \mathbf{Z}$, $x \mapsto 2x$, – инъективна, но не сюръективна.
Пример. $f : \mathbf{R} \to \mathbf{R}$, $x \mapsto 2x$ – 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 $a) n = 1; \quad b) n = 2; \quad c) n = 3$?

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_R, $M_{\overline{R} \cup S}$, $M_{\overline{R \cap S}}$.

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.

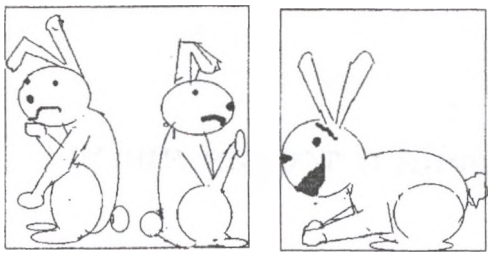


Рис. 3.1: Как бы ни сажали трех зайцев в две клетки всегда найдется клетка, в которой содержится по крайней мере два зайца.

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 способами, 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 один из оставшихся чисел.

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 действитель-

ных чисел между 0 и 100. Рассмотрим последовательность 11 чисел $\sqrt{a_1}, \ldots, \sqrt{}$
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. Тогд
$0 < |\sqrt{x} - \sqrt{y}| < 1$.

3.2.1 Задачи

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

Указание. Сколько дней в году?

2. На кафедре высшей математики работают 13 преподавателей. Докажит
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 крайне
мере два слова начинающие из одинаковых букв. Доказать.

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

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

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

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

7. Найти последовательность четырех различных действительных чисел, к
торые не содержат убывающую или возрастающую подпоследовательность дл
ны 3.

8. Найти последовательность девяти различных действительных чисел, к
торые не содержат убывающую или возрастающую подпоследовательность дл
ны 4.

9. Доказать, что в задаче P. Erdös, G.Szekeres заменить $n^2 + 1$ на n^2 нельз
Постройте последовательность различных действительных чисел длины n^2
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

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

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

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

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

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

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

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

Поскольку множество $A_1 \cup \cdots \cup A_k$ состоит из чисел, которые имеют хотя бы один делитель вида p_i для некоторого $1 \le i \le k$, 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 $0 < i_1 < \cdots < i_s \le n$,

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

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

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

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

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

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

Поэтому

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

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 информатику. 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

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

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 $B \setminus \{a_n\} \subseteq A \setminus \{a_n\}$ и $|B \setminus \{a_n\}| = k-1$. 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

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.

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

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

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

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

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

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

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

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

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

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 крайне 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 $|A| = |B|$ по нятия эквивалентные. Другими словами, все три понятия инъективность, сюръ ективность 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.

3.6 Математическая индукция

Математическая индукция. Пусть $P(n)$ – некоторое утверждение зависящ 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. $\sum_{i=1}^{n} i^2 = n(n + 1)(2n + 1)/6$.
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 по
ным квадратом.

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

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

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 любог
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, кот
рое в литровой банке, но бабушка не позволяла его трогать. И внучек задума
обмануть бабушку. Он решил съедать каждый день по 0.1 литра из самой луч
шей банки и доливать ее водой (тщательно перемещав). Через сколько дне
бабушка обнаружит обман, если варенье останется прежним на вид при раз
бавлении его водой наполовину ?

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

Ответ. 7 дней.

13. Вычислить сторону правильного 2^n-угольника, вписанного в круг рад
уса 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 любым
двумя из которых не превосходит единицы. Доказать, что все эти точки можн
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.

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

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

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

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

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

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 $f_n = a f_{n-1} + b f_{n-2}$ 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 им ет вид $f_n = cq_1^n + dq_2^n$ для некоторых констант c, d. Допустим, что заданы на чальные 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 данны Таким образом в случае $q_1 \neq q_2$, наше реккурентное соотношение имеет решен 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 ви упражнения.

Пример. (Числа Фиббоначчи) Решить уравнение $f_n = f_{n-1} + f_{n-2}$ с грани ными 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 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 $\sqrt{37} - 6 < 0.1$

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

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

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

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

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

Теорема. Отображение $\Gamma\to\mathbf{C}[[x]],\quad a\mapsto G(a)$ является гомоморфизм 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, получ ной из последовательностей b_n, c_n путем сложения: $a_n=b_n+c_n$, получается порождающих функции $G(a)$ и $G(b)$ также путем сложения:

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

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

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

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

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

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

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,

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

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,

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

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

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

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

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 $\binom{n}{0},\binom{n}{1},\binom{n}{2},\ldots,\binom{n}{n}$.

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

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

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

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 $n \leq \alpha < n$
- $\lceil \alpha \rceil$– верхняя целая часть числа $\alpha \in \mathbf{R}$, т.е., такое $n \in \mathbf{Z}$, что $n-1 < \alpha \leq$

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

Алгоритм Евклида. Пусть $a, b \in \mathbf{Z}, b \neq 0$. Алгоритм Евклида состоит в 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 $a = 7228, b = 3$ 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,

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

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 $2^{k-1}PH_n$ 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 $3^{k-1}PS_n$ 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 $2, 3, 5, 7$. 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

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

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 $d = НОД(a, m)$. 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 сравнений первой степени. Система сравнений

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

сводится к системе вида

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

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

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

где $i = 1, 2, \ldots, n$. Тогда

$$x = m_2m_3 \cdots m_nx_1b_1 + m_1m_3 \cdots m_nx_2b_2 + \cdots + m_1m_2 \cdots m_{n-1}x_nb_n$$

решение системы сравнении

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

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 21

3.12 Цепные дроби

Как построить цепную дробь ? Пусть $a, b \in \mathbf{Z}, b > 0$. Применим алгори 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	...	s	...
q_s		q_0	q_1	q_2	...	q_s	...
P_s	1	$P_0 = q_0$	$P_1 = P_0q_1 + 1$	$P_2 = P_1q_2 + P_0$	...	$P_s = P_{s-1}q_s + P_{s-2}$	...
Q_s	0	$Q_0 = 1$	$Q_1 = q_1$	$Q_2 = Q_1q_2 + Q_0$	...	$Q_s = Q_{s-1}q_s + Q_{s-2}$	...

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

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

Имеем,

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

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 $P_i = q_0, Q_0 = 1, P_1 = q_0q_1 + 1, Q_1 = q_1$. 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 $d = \text{НОД}(P_s, Q_s)$, то d – делитель числа $(-1)^s$, поэтому $d = 1$.

Пример. $\text{НОД}(19,1) = 1, \text{НОД}(153,8) = 1, \text{НОД}(631,33) = 1, \text{НОД}(784,41) = 1, \text{НОД}(1415,74) = 1, \text{НОД}(3614,189) = 1$.

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 $\text{НОК}(a,b) = 1$.

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 $\theta(p^\alpha) = 2^k$, 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

$$\sum_{d|a} \theta(a) = \prod_{i=1}^{k} (1 + \theta(p_i) + \cdots + \theta(p_i^{\alpha_i})).$$

Доказательство. Раскроем скобки правой части. Получаем сумму слагаемых вида

$$\theta(p_1^{\beta_1}) \cdots \theta(p_k^{\beta_k}) = \theta(p_1^{\beta_1} \cdots p_k^{\beta_k}).$$

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 $\mu(n) = 0$, если n делится на квадрат простого числа, $\mu(n) = (1)^k$, если n – произведение k различных простых чисел.

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 $a \in \mathbf{Z}$,

$$a^p - a \equiv 0 (mod p)$$

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. Пусть $n(n)$–функция Мебиуса:

$$\mu(n) = \begin{cases} 0, & \text{если } n \text{ делится на квадрат простого числа,} \\ (-1)^k, & \text{если } n - \text{произведение } k \text{ различных простых чисел.} \end{cases}$$

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.

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 $\phi(n) = 1792$ и n имеет вид $n = 2^\alpha 5^\beta 13^\gamma$.

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 $\delta_{k-1} = P_{k-1}/Q_{k-1}$. Тогда $x = Q_{k-1}, y = (-1)^k P_{k-1}$ – решение уравнения $ax + by = 1$.

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

- $53x - 17y = 25$
- $47x + 105y = 4$
- $18x + 33y = 112$
- $11x + 16y = 156$

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 и простые числа

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 ля 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 последним 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, 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 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.

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 напоминаем, что символ Якоби $\left(\frac{a}{n}\right) \in \{1, -1\}$ для $a \in \mathbf{Z}, НОД(a,n) = 1$ 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 ,
$\left(\frac{a}{n}\right) = 0$, если $НОД(a,b) \neq 1$,
$\left(\frac{a}{1}\right) = 1$, 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 совниваться 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 Крипосистема 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 $D(y) = y^d (mod\, N)$, которая 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.

Этот метод шифровки носит название криптосистемы с открытым ключом. Идея построения односторонней функции с секретом, лежащей на основе таких криптосистем высказали ы 1975 году Диффи и Хэллмэн.

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:

$$\frac{4288266240}{19} = 225698223 + \frac{1}{6 + \frac{1}{3}}.$$

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: $x = 134217728$.

Глава 4

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 30 баллов и темы должны быть разработаны на не ниже чем 15 баллов.

Желаю успехов !

4.1 Задачи

1. *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.

2. *Счастливые билеты.* (4)

Билет содержит 6 цифр. Билет называется счастливым, если сумма первых трех цифр совпадает с суммой последних трех. Сколько существуют счастливых билетов ?

3. *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)

$$\lambda_n^i = (-1)^{n+i}\, \tilde{s}_{n+1}^{i+1},$$

где $\tilde{s}_n^i, 1 \le i \le n$, – 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 $yx = xy - x$.

4. *Неассоциативная расстановка скобок.* (10)

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.

5. *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.

6. *Тождество Абеля.* (10)

Доказать, что для любых x, y, z,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x(x-kz)^{k-1}(y+kz)^{n-k},$$

7. *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	

?

8. *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 $1/t$.

9. *Теорема Вильсона* (4)

Доказать, что если p простое, то $(p-1)! + 1$ делится на p.

10. *Число Рамануджана*(8)

Доказать, что $a^{1729} \equiv a (mod\, 1729)$ для всех $a \in \mathbf{Z}$.

11. *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.

12. *Рассеянные аксакалы и галоши.* (10)

Несколько усложненная предыдущая задача. В мечеть нельзя заходить в обуви. Аксакалы после намаза вышли из мечети и надели галоши. Одноногих аксакалов нет. Аксакалы различают левые и правые галоши. Сколькими способами может возникнуть такое событие, если количество аксакалов – n.

(Для тех кто знает что такое вероятность). Найти вероятность того, что никто из аксакалов не наденет свои галоши.

13. *Тождества Ли* (8)

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

$$[a, b] = -[b, a],$$

$$[[a, b], c] + [[b, c], a] + [[c, a], b] = 0.$$

14. *Тождества Йордана.* (10)

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

$$\{a,b\} = \{b,a\},$$

$$\{\{a,a\},\{b,a\}\} = \{\{\{a,a\},b\},a\}.$$

15. *Тождества для q-коммутаторов.* (15)

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

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

$$[a,b] = a \circ_q b - b \circ_q a.$$

16. *Тождества Тортки* (15)

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

17. *Функции Аккермана.* (5)

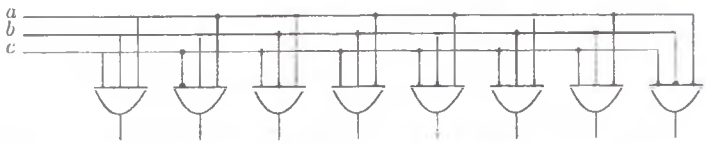
Функции Аккермана - функция от двух неотрицательных целочисленных аргументов, определенная следующей рекурсивной процедурой

- 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 $A(1,3)$.

18. *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.

19. *Системa 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.

20. *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

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

21. *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 $0, 1$.

- 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?

22. *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

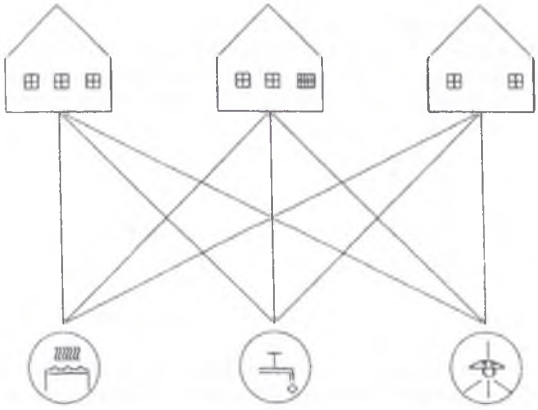
$$\partial^3(f^4) + (f\partial)^3(f) = 25f(\partial(f))^3 + 40f^2\partial(f)\partial^2(f) + 5f^3\partial^3(f) \equiv 0(mod 5).$$

23. *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 ?

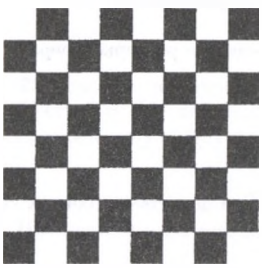
24. *Газ, вода и электричество* (5)

Нужно провести газ, воду и электричество в три дома так, чтобы их линии не пересекались. Можно ли это сделать?



25. *Путешествие коня.* (5)

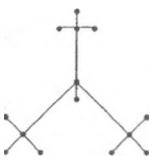
Может ли конь обойти шахматное поле, побывав в каждой клетке ровно по одному разу? Другая формулировка: является ли граф с вершинами в шахматных клетках и ребрами, порожденными всевозможными движениями коня, гамильтоновым ?



26. *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:

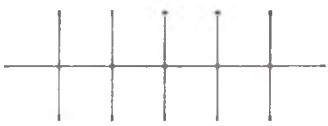
бутан



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

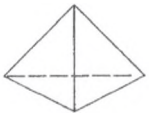
n	1	2	3	4	5	6	7	8	9	10	11	12	13
Количество деревьев	1	1	1	2	3	5	9	18	35	75	159	357	799

Попробуйте повторить некоторые из этих вычислении. Например, для $n = 6, 7$. Постройте соответствующие деревья.

27. *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:

$M =$  , $f(\text{куб}, q) = \frac{q^2(q^6+17q^2+16)}{24}$,

$M =$  , $f(\text{тетраэдр}, q) = \frac{q^2(q^2+11)}{12}$,

$$f(\text{октаэдр}, q) = \frac{q^2(q^4+3q^2+12q+8)}{24}.$$

28. *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: голько теперь разрешается сажать радикалы CH_3 H и OH в вершинах атомов углерода.

4.2 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. Рукщин, *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.

Аскар Серкулович Джумадильдаев

ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ.
Учебное пособие. Часть 1

Askar S.Dzhumadil'daev

ELEMENTS OF DISCRETE MATHEMATICS
Textbook, Part 1.

Редактор Гаджиев Ф.А.

Подписано в печать 12.10.2004

Формат 60 x 84 1/16. Бумага тип. Ризограф.
Усл.печ.5,6 л. Уч.-изд. 5,9 л. Тираж 250.

Заказ №820.

Цена договорная

Издание Казахской головной архитектурно-строительной академии
Издательский дом КазГАСА «Строительство и архитектура»
480043, г.Алматы, ул. К.Рыскулбекова, 28