ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
Областное государственное автономное профессиональное образовательное учреждение
«СТАРООСКОЛЬСКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»
(ОГАПОУ СПК)

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ЕН.02 ДИСКРЕТНАЯ МАТЕМАТИКА

для студентов специальности 09.02.05 Прикладная информатика
(по отраслям)

Старый Оскол

Методические рекомендации по выполнению практических работ по учебной дисциплине «Дискретная математика» разработаны в соответствии с Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности 09.02.05 Прикладная информатика (по отраслям) среднего профессионального образования (далее СПО) и предназначены для студентов второго курса очной формы обучения.

Разработчик:
Анисимова В.И., преподаватель математики ОГАПОУ СПК

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4
КАРТА ПРАКТИЧЕСКИХ РАБОТ 5
СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ 6
Практическая работа №1 «способы задания множеств. Отношения между множествами. Операции над множествами» 6
ПРАКТИЧЕСКАЯ РАБОТА №2 «ПОДСТАНОВКИ. МЕТОД МАТЕМАТИЧЕСКОЙ ИНДУКЦИИ» 16
ПРАКТИЧЕСКАЯ РАБОТА №3 «ЛОГИЧЕСКИЕ ОПЕРАЦИИ НАД ВЫСКАЗЫВАНИЯМИ. ТАБЛИЦЫ ИСТИННОСТИ. ЗАКОНЫ АЛГЕБРЫ ЛОГИКИ. ЛОГИЧЕСКИЕ ОПЕРАЦИИ НАД ПРЕДИКАТАМИ» 24
ПРАКТИЧЕСКАЯ РАБОТА №4 «ВИДЫ ГРАФОВ. ГРАФЫ ЧИСЛОВЫХ МНОЖЕСТВ, ХАРАКТЕРИСТИКИ ГРАФОВ» 36
ПРАКТИЧЕСКАЯ РАБОТА №5 «ПОЛНАЯ И ПРИВЕДЕННАЯ СИСТЕМЫ ВЫЧЕТОВ. ВЫБОР МОДУЛЯ ДЛЯ КОНТРОЛЯ. КОДИРОВАНИЕ ИНФОРМАЦИИ» 40
КРИТЕРИИ ОЦЕНКИ РАБОТ 48
ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ 49

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Практическое занятие - это форма организации учебного процесса, предполагающая выполнение обучающимися по заданию и под руководством преподавателя одной или нескольких практических работ.

Дидактическая цель практических работ - формирование у обучающихся профессиональных умений, а также практических умений, необходимых для изучения последующих учебных дисциплин, а также подготовка к применению этих умений в профессиональной деятельности.

Так, на практических занятиях по дискретной математике у обучающихся формируется умение решать задачи, которое в дальнейшем должно быть использовано для решения профессиональных задач по специальным дисциплинам.

В ходе практических работ обучающиеся овладевают умениями пользоваться информационными источниками, работать с нормативными документами и инструктивными материалами, справочниками, выполнять чертежи, схемы, таблицы, решать разного рода задачи, делать вычисления.

Задачи, которые решаются в ходе практических занятий по дискретной математике:

1) расширение и закрепление теоретических знаний по математике, полученных в ходе лекционных занятий;

2) формирование у обучающихся практических умений и навыков, необходимых для успешного решения задач по математике;

3) развитие у обучающихся потребности в самообразовании и совершенствовании знаний и умений в процессе изучения математики;

4) формирование творческого отношения и исследовательского подхода в процессе изучения математики;

5) формирование профессионально-значимых качеств будущего специалиста и навыков приложения полученных знаний в профессиональной сфере.

КАРТА ПРАКТИЧЕСКИХ РАБОТ

Тема курса	Практическая работа
Тема 1.1. Элементы теории множеств	Практическая работа №1 «Способы задания множеств. Отношения между множествами. Операции над множествами»
Тема 1.2. Элементы теории отображений и алгебры подстановок	Практическая работа №2 «Подстановки. Метод математической индукции»
Тема 1.3. Алгебра логики	Практическая работа №3 «Логические операции над высказываниями. Таблицы истинности. Законы алгебры логики. Логические операции над предикатами»
Тема 1.4. Основы теории графов	Практическая работа №4 «Виды графов. Графы числовых множеств, характеристики графов»
Тема 1.5. Основы алгебры вычетов и их приложение к простейшим криптографическим шифрам	Практическая работа №5 «Полная и приведенная системы вычетов. Выбор модуля для контроля. Кодирование информации»

СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1
«Способы задания множеств. Отношения между множествами. Операции над множествами»

Цель: формирование навыков выполнения операций над векторами и вычисления модуля и скалярного произведения векторов.

Теоретические сведения

Понятие ***множества*** является фундаментальным неопределимым понятием, одно из основных, если не основное, понятий математики. Оно не имеет точного определения, и его следует отнести к аксиоматическим понятиям. Как правило, термин **множество** объясняется с помощью примеров, а потом указываются правила его использования в математических применениях. Последнее можно сделать на разных уровнях строгости. Детальное и строгое изложение теории **множеств** требовало бы скрупулезного анализа логики математических рассуждений, а это – специальная самостоятельная тема, которая относится к *области основ математики*. Для наших целей достаточно выбрать уровень так называемой *интуитивной теории множеств*.

Интуитивно под ***множеством*** понимается совокупность определенных, вполне различимых объектов, рассматриваемых как единое целое. Можно говорить о множестве граней многоугольника, множестве точек на прямой, множестве натуральных чисел, множестве рациональных чисел, множестве операторов языка программирования, множестве языков программирования и т.д. Из этих примеров видно, что ***множество*** – это совокупность определенных различаемых объектов таких, что для любого объекта можно установить, принадлежит этот объект данному множеству или нет. Вполне очевидно, что множество, которое подчиняется такому ограничению, может содержать объекты почти любой природы. Например, множество жителей города Старый Оскол; множество студентов СПК; множество автобусных маршрутов нашего города; множество станций московского метро; множество правых ботинок; множество символов кодов компьютера; множество идентификаторов в программе и т.д. Следует подчеркнуть, что о множестве можно вести речь только тогда, когда элементы множества различимы между собой. Например, нельзя говорить о множестве капель в стакане воды, т.к. невозможно четко и ясно указать каждую отдельную каплю.

Множества, все элементы которого являются числами, называются числовыми множествами. Множества, элементами которого являются другие множества, называются классом или семейством.

Отдельные объекты, из которых состоит множество, называют ***элементами*** множества. Например, 5 – элемент множества натуральных чисел, G – элемент множества букв латинского алфавита.

Таким образом, когда мы говорим о множестве, то объединяем некоторые объекты в одно целое, а именно в множество, элементами которого они являются.

Основатель теории множеств **Георг Кантор** определил формулировку интуитивного понятия множества следующими словами: «*Произвольная совокупность определенных предметов нашей интуиции или интеллекта, которые можно отличить один от другого и которые представляются как единое целое, называется* ***множеством****. Предметы, которые входят в состав множества, называются его* ***элементами***».

Существенным пунктом канторовского понятия множества является то, что совокупность предметов рассматривается как один предмет («представляется как единое целое»). Основное внимание тут переносится с отдельных предметов на совокупности предметов, которые в свою очередь, можно рассматривать как предметы.

Что касается «предметов нашей интуиции или интеллекта», то эта формулировка дает значительную свободу прежде всего тем, что никак не ограничивает природу предметов, составляющих множество. Множество может состоять, например, из людей, простых чисел, точек пространства, планет Вселенной и т.д. Заметим, что канторовская формулировка множества дает возможность рассматривать множества, элементы которых по определенной причине точно задать невозможно.

Смысл выражений: «которые можно отличить один от другого» и «определенные предметы» заключается в следующем. В первом случае для любых двух предметов, которые рассматриваются как элементы данного множества, должна существовать возможность выяснить, различные эти предметы или одинаковые. Во втором случае, если задано некоторое множество и какой-нибудь предмет, то можно определить, является ли этот предмет элементом данного множества. Отсюда следует, что всякое множество полностью определяется своими элементами. Это канторовское требование формулируется как **интуитивный принцип объемности или аксиома экстенсиональности**, согласно которому два множества (A и B) равны тогда и только тогда, когда они состоят из одних и тех же элементов (обозначают A=B).

Таким образом, два множества равны, если каждый элемент одного из них является элементом другого и наоборот.

Общим обозначением множества служит пара фигурных скобок {…}, внутри которых перечисляются элементы множества. Для обозначения конкретных множеств используют различные прописные буквы (M, X, A,…), или прописные с индексами (M_1, M_2, …). Для обозначения элементов множества в общем случае используют различные строчные буквы, или строчные буквы с индексами. Для указания того, что некоторый элемент a является элементом множества A, используется символ принадлежности множеству $\in$[1]. Запись $a \in A$ означает, что элемент a принадлежит множеству A, а запись $a \notin A$ означает, что элемент a не принадлежит множеству A. Записью $a_1, a_2, \dots a_n \in A$ пользуются в качестве сокращения для записи $a_1 \in A$, $a_2 \in A$, $a_3 \in A$, $\dots a_n \in A$.

Множества бывают ***конечными*** и ***бесконечными***. Множество называют ***конечным***, если число его элементов конечно, т.е. если существует натуральное число N, являющееся числом элементов множества. Множество называют ***бесконечным***, если оно содержит бесконечное число элементов.

Величина, определяющая число элементов множества, называется **кардинальным числом множества** или **степенью множества,** и обозначается |A| или card(A).

Способы задания множества

Существует два основных способа задания множества: перечисление и описание.

Например, множество отличников группы можно задать, перечислив студентов, которые учатся на “отлично”. Например: {Иванов, Сидоров, Петров,…}.

Для сокращения записи $A=\{a_1, a_2, \dots a_n\}$ иногда пишут $A=\{a_i\}_1^n$, или вводят множество индексов $I=\{1,2,\dots n\}$ и пишут $A=\{a_i\}$, $i \in I$. Такой способ удобен при рассмотрении конечных множеств, содержащих небольшое число элементов.

Описательный способ задания множества состоит в том, что указывается характерное свойство, которым обладают все элементы множества. Под свойством предмета x будем понимать такое повествовательное предложение, в котором нечто утверждается относительно предмета x и которое можно характеризовать как истинное или ложное по отношению к x (характеристический предикат).

Например, свойствами являются:

- 5 делит x;
- $x^2 > 0$.

Выражения:

- существует такой x, что $5x < 0$;

[1] Символ $\in$ происходит от греческой буквы ε

- для всех x, y xy=yx

не являются свойствами, потому что их нельзя характеризовать как истинные или ложные относительно x.

Если обозначить P(x) некоторое свойство, тогда P(a) будет означать тоже самое свойство, но с заменой x на a. Задание множества в терминах свойств достигается с помощью **интуитивного принципа абстракции или аксиомы свертки**: всякое свойство P(x) определяет некоторое множество A с помощью условия: элементами множества A являются те и только те предметы a, которые имеют свойства P.

В силу принципа абстракции всякое свойство P(x) определяет единственное множество, которое обозначают {a|P(a)} и читают так: «множество всех тех предметов a, что P(a)»

Так, если C – множество студентов группы, то множество O отличников этой группы запишется в виде:

$$O = \{s \in C \mid s - \text{отличник группы}\}.$$

«Множество O состоит из элементов s множества C, обладающих тем свойством, что s является отличником группы».

В тех случаях, когда не вызывает сомнений из какого множества берутся элементы s, указание о принадлежности s множеству C можно опустить. При этом множество O запишется в виде:

$$O = \{s \mid s - \text{отличник группы}\}.$$

Примеры:

A={x|x – четное} – множество целых четных чисел;

B={x|x^2-1=0} – множество {-1, 1}.

Пусть N множество целых чисел. Тогда {n∈N| $0 < n \le 7$} есть множество {1,2,3,4,5,6,7}.

Важным понятием теории множеств является понятие ***пустого множества***. Пусть A – некоторое множество, а P(x) имеет вид x ≠ x, тогда множество {a|P(a)} = {a|a ≠ a}, очевидно, не имеет элементов. Из принципа объемности следует, что может существовать только одно множество, которое не имеет элементов. Это множество и называется **пустым множеством**.

Иначе ***пустым множеством*** называют множество, не содержащее ни одного элемента. Пустое множество обозначается символом ∅.

Например, {n∈N| n^2+2n+5=0}=∅.

Пустое множество условно относится к конечным множествам.

Множество, содержащее только один элемент, называется **синглетоном**.

Задание множества называют ***неизбыточным***, если каждый элемент входит в данное множество в единственном экземпляре, и ***избыточным***, если хотя бы один элемент входит в его состав более чем в одном экземпляре (мультимножества).

Равенство множеств

Как уже отмечалось, два множества называются равными, если они состоят из одних и тех же элементов, т.е. представляют собой одно и тоже множество. Символ равенства множеств обладает свойствами:

- A=A – рефлексивность;
- если A=B, то B=A – симметричность;
- если A=B и B=C, то A=C – транзитивность.

Из определения равенства множеств вытекает:

1. порядок элементов в множестве несуществен. Например, множества {1,2,3,4} и {3,4,1,2} представляют собой одно и тоже множество;

2. в множестве не должно быть неразличимых элементов. Поэтому в множестве не должно быть одинаковых элементов. Например, запись множества A={6,7,8,6,9} следует рассматривать как A={6,7,8,9}[1].

Но, множество, которое состоит из элементов некоторого множества A так, что эти элементы могут входить в состав этого множества в любом количестве экземпляров, называют ***мультимножеством*** множества A. С точки зрения теории множеств, множество и мультимножество – это один и тот же объект и они могут между собой не различаться. Однако часто, особенно когда речь идет о представлении множества в памяти ЭВМ, возникает потребность отличать множество от мультимножества.

Подмножество

Множество A является ***подмножеством*** множества B, если любой элемент множества A принадлежит и множеству B.

Например, множество студентов группы является подмножеством студентов отделения; множество четных целых чисел может рассматриваться как подмножество множества натуральных чисел.

Для определения подмножества в теории множеств используются символы:

- $\forall$ - символ, называемый квантором всеобщности. Запись $\forall$x означает: “ любой x”, “каков бы ни был x”, “для всех x”, “для всякого x”; и т.п.
- $\exists$ - символ, называемый квантором существования. Запись $\exists$x означает: “существует такой x, что”;
- $\rightarrow$ (или $\Rightarrow$) символ следствия (импликации), означающий “влечет за собой”; “если… то”;
- $\Leftrightarrow$ - символ эквивалентности, означающий “тогда и только тогда”, “то же самое”.

Тогда определение подмножества, которое может быть сформулировано в виде: для любого x утверждение “x принадлежит A“ влечет за собой утверждение “x принадлежит B” запишется так:

$$\forall x[x \in A \Rightarrow x \in B]$$

Более краткой записью выражение “A является подмножеством B” будет запись

$$A \subseteq B \qquad \text{(Читается “B содержит A”).}$$

Используемый здесь символ $\subseteq$ означает включение.

Если множество B содержит и другие элементы кроме элементов из A, то используют символ строгого включения $\subset$ и обозначается это $A \subset B$. В этом случае A называется собственным подмножеством множества B

Связь между символами дается выражениями:

$$A \subset B \Leftrightarrow A \subseteq B \text{ и } A \neq B$$

Свойства подмножеств:

- $A \subseteq A$ – рефлексивность; ($A \not\subset A$ – иррефлексивность)
- $[A \subseteq B$ и $B \subseteq C] \rightarrow A \subseteq C$ – транзитивность. 1.5

Следует отметить важное свойство, что для любого множества A пустое множество $\varnothing \subseteq A$.

Если $A \subseteq B$ и $B \subseteq A$, то множества A и B эквивалентны: A=B, т.е. все эле-менты A являются элементами B, а все элементы B являются элементами A.

Т.е. $A=B \Leftrightarrow (A \subseteq B$ и $B \subseteq A)$.

[1] Однако в этой ситуации возникают следующие проблемы. Если мы рассмотрим первоначальное определение A и выбросим одно из чисел 6 из множества, то мы, очевидно, будем иметь $6 \in A$ и $6 \notin A$. Возникает противоречие. Поэтому следует рассматривать повторение символов в определении множеств как упоминание одного и того же символа, а его дублирование как недосмотр. Удаление повторяющихся элементов образует основу для некоторых дальнейших математических рассуждений.

Подмножества разделяются на два вида: **собственные** подмножества и **несобственные** подмножества множества. Само множество A и пустое множество называются несобственными, а все остальные – собственными.

Множество всех подмножеств данного множества A называют ***булеаном*** или ***степенью множества*** A и обозначают β(A).

Формально $\beta(A)=\{B \mid B\subseteq A\}$. В частности заметим, что поскольку $\varnothing \subseteq A$ и $A \subseteq A$, то $\varnothing \in \beta(A)$; $A \in \beta(A)$. Мощность булеана (кардинальное число булеана) $|\beta(A)| = 2^{|A|}$, или $|\beta(A)|=2^n$, где $n=|A|$ - мощность множества A.

Пример. Пусть A={a,b,c}. Тогда β(A)={ ∅, {a}, {b}, {c}, {a,b}, {a,c}, {b,c}, A}. Кроме того, заметим, что множество A имеет 2 несобственных подмножества (∅ и A={a,b,c}) и 6 собственных подмножеств ({a}, {b}, {c}, {a,b}, {a,c}, {b,c}).

Операции над множествами

Над множествами можно производить действия, которые во многом напоминают действия сложения и умножения в элементарной алгебре. Если a и b некоторые числа, то законы элементарной алгебры можно записать как:

1. $a+b = b+a$; $a\cdot b=b\cdot a$ - коммутативный (переместительный) закон;
2. $\left.\begin{array}{l}(a+b)+c=a+(b+c)\\(a\cdot b)\cdot c=a\cdot(b\cdot c)\end{array}\right\}$ - ассоциативный (сочетательный) закон;
3. $(a+b)\cdot c=a\cdot c+b\cdot c$ - дистрибутивный (распределительный) закон.

Заметим, что в ассоциативном и коммутативном законах можно заменить действие сложения умножением, а действие умножения – сложением. При этом получим другой закон, который будет справедлив, как и первый. Однако в дистрибутивном законе подобной симметрии нет. Если в этом законе заменить сложение умножением, а умножение сложением, то придем к абсурду

$$(a\cdot b)+c=(a+c)\cdot(b+c).$$

Всегда ли это так? Оказывается, существуют алгебры, и именно алгебра множеств, в которой все три закона симметричны относительно действий “сложения” и “умножения”.

Объединение множеств

Объединением множеств A и B называют множество, состоящее из всех тех и только тех элементов, которые принадлежат хотя бы одному из множеств A и B. Объединение множеств A и B обозначается символом $\cup$, т.е. $A\cup B$.

Определение объединения множеств можно записать как

$$A\cup B=\{x \mid x\in A \text{ или } x\in B\}$$

Объединение множеств иногда называют суммой множеств и обозначают A+B. Однако свойства объединения множеств несколько отличаются от свойств суммы при обычном арифметическом понимании. Поэтому термином сумма пользоваться не рекомендуется.

Примеры.

1. Пусть A={4,5,8,12,16,21}; B={1,2,5,7,12,17,21,30}. Тогда $A\cup B$={1,2,4,5,7,8,12,16,17, 21,30}.
2. Пусть A={a,b,c,d}; B={a,d,e,f,g}. Тогда $A\cup B$={a,b,c,d,e,f,g}.

Если множества A и B представить в виде точек, ограниченных окружностями A и B соответственно, то объединение множеств $A\cup B$ представляет собой закрашенную область, ограниченную обоими кругами, как это показано на рис. 1.1.

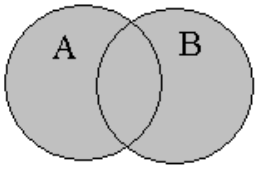


Рис. 1.1

Понятие объединения множеств можно распространить и на большее число множеств. Пусть $M=\{X_1, X_2,\ldots X_n\}$ – совокупность n множеств $X_1, X_2, \ldots X_n$, называемую системой множеств. Объединение этих множеств представляет собой множество, состоящее из всех тех и только тех элементов, которые принадлежат хотя бы одному из множеств системы M.

$$\bigcup_{i=1}^{n} X_i = \bigcup_{X \in M} X = X_1 \cup X_2 \cup X_3 \cup .... \cup X_n$$

Для объединения множеств справедливы коммутативный и ассоциативный законы:

$$A \cup B = B \cup A;$$

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

Вполне очевидно, что $A \cup \varnothing = A$.

Пересечение множеств

Пересечением множеств A и B называют множество, состоящее только их тех и только тех элементов, которые принадлежат как множеству A, так и множеству B. Пересечение множеств обозначается символом $\cap$, т.е. $A \cap B$. Определение пересечения может быть записано как

$$A \cap B = \{x \mid x \in A \text{ и } x \in B\}$$

Пересечение множеств иногда называют произведением множеств, что некорректно.

Примеры.

1. Если A={4,5,8,12,16,21}; B={1,2,5,7,12,17,21,30}, то $A \cap B$ ={5,12,21}.
2. Если A={a,b,c,d}; B={a,d,e,f,g}, то $A \cap B$={a,d}.

Если A – множество левого круга, B – множество правого круга, то пересечение множеств $A \cap B$ представляет собой закрашенную область, являющуюся общей частью обоих кругов, как это показано на рис. 1.2.

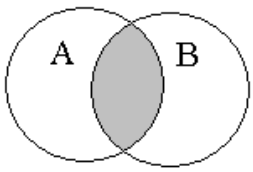


Рис. 1.2

Множества A и B называются непересекающимися, если они не имеют общих элементов, т.е. $A \cap B = \varnothing$.

Пример. Пусть A={3,4,5}, B={2,6,7}. Тогда $A \cap B = \varnothing$.

Множества A и B находятся в общем положении, если выполняются три условия:

- Существует элемент множества A, не принадлежавший множеству B;
- Существует элемент множества B, не принадлежавший множеству A;
- Существует элемент, принадлежащий как множеству A, так и множеству B.

Пересечение распространяется и на большее количество множеств. Пусть имеем систему множеств M={X_1, X_2,…. X_n}. Множество

$$\bigcap_{X \in M} X = \bigcap_{i=1}^{n} X_i = X_1 \cap X_2 \cap X_3 .... \cap X_n$$

представляет собой множество, элементы которого принадлежат каждому из множеств системы M.

Пересечение множеств обладает свойством коммутативности

$$A \cap B = B \cap A$$

и ассоциативности

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

Кроме того имеет место соотношение: $A \cap \varnothing = \varnothing$.

Разность множеств

Разностью множеств A и B называют множество, состоящее из тех и только тех элементов, которые принадлежат только множеству A и не принадлежат множеству B. Разность множеств[1] A и B обозначается A\B. Формально определение разности множеств A и B можно записать в виде:

$$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}.$$

[1] Разность множеств A и B называют также дополнением B до A.

Примеры.

1. Пусть имеем A={4,5,8,12,16,21}; B={1,2,5,7,12,17,21,30}. Тогда A\B={4,8,16}, а B\A={1,2,7,17,30}.
2. A={a,b,c,d}; B={a,d,e,f,g}. В этом случае получаем: A\B={b,c} и B\A={e,f,g}.

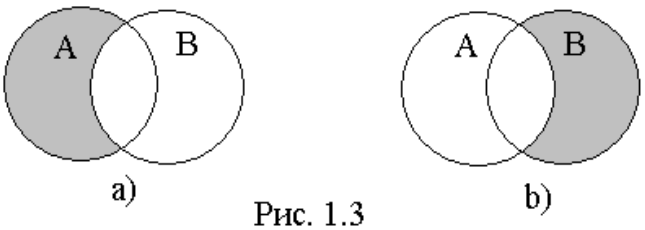


Рис. 1.3

Если как и ранее множества A и B изобразить в виде точек кругов A и B соответственно, то разность множеств будет представляться так, как это показано на рис. 1.3, где a) соответствует разности A\B, b)- разности B\A.

Симметрическая разность

Симметрической разностью множеств A и B называют множество, состоящее из объединения множеств разностей A\B и B\A. Симметрическая разность множеств A и B обозначается символом ⊕ (или символом Δ). Таким образом, по определению

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

Нетрудно убедиться, что $A \oplus B = (A \cup B) \setminus (A \cap B)$.

Примеры.

1. Имеем: A={4,5,8,12,16,21}; B={1,2,5,7,12,17,21,30}. Тогда A ⊕ B={1,2,4,7,8,16, 17,30}.
2. A={a,b,c,d}; B={a,d,e,f,g}. В этом случае получаем A ⊕ B={b,c,e,f,g}.

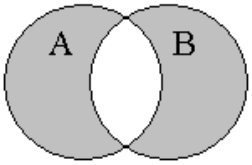


Рис. 1.4

Графически симметричная разность множеств A и B может быть представлена как показано на рис. 1.4. Закрашенные области соответствуют симметрической разности множеств A и B.

Универсальное множество

Если в некотором рассмотрении участвуют только подмножества некоторого фиксированного множеств I, то это самое большое множество называют ***универсальным*** (***или полным***) ***множеством, или - универсум***.

В различных конкретных случаях роль универсального множества играют различные множества. Так, при рассмотрении студентов института универсальным (полным) множеством является вся совокупность студентов. Отдельные группы (факультеты) можно рассматривать как подмножества. В некоторых случаях универсальным множеством может являться и отдельная группа, в которой имеют место свои подмножества (отличники; студенты, проживающие в общежитии; юноши; девушки и т.п.).

Вполне очевидно, что для универсального множества справедливы следующие соотношения:

$$\boxed{A \cap I = A} \quad \text{и} \quad \boxed{A \cup I = I}$$

Универсальное множество удобно изображать графически в виде множества точек прямоугольника. Различные области внутри прямоугольника будут означать различные подмножества универсального множества. Изображение множества в виде областей в прямоугольнике, представляющем универсальное множество, называют диаграммой Эйлера-Венна.

Дополнение множества

Множество $\overline{A}$, определяемое из соотношения

$$\overline{A} = I \setminus A$$

называют ***дополнением множества*** A (до универсального множества I)

Графически дополнение множества A может быть представлено как показано на рис. 1.5.

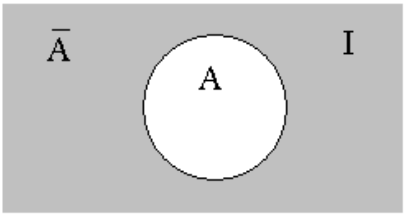
Формальное определение дополнения множества A может быть записано как

$$\overline{A} = \{x \mid x \in I \quad \text{и} \quad x \notin A\}$$

Из определения дополнения множества следует, что A и $\overline{A}$ не имеют общих элементов, т.е.

$$A \bigcap \overline{A} = \varnothing$$

Кроме того, $A \bigcup \overline{A} = I$



Из симметрии формул 1.22 и 1.23 следует, что не только $\overline{A}$ является дополнением A, но и A является дополнением $\overline{A}$. Но дополнение $\overline{A}$ есть $\overline{\overline{A}}$. Таким образом $\overline{\overline{A}} = A$

Рис. 1.5

С помощью операции дополнения удобно представить разность множеств:

$$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\} = \{x \mid x \in A \text{ и } x \in \overline{B}\}, \text{ т.е } A \setminus B = A \bigcap \overline{B}$$

Прямое произведение множеств

Прямым произведением множеств A и B называют множество, обозначаемое $A \times B$ и состоящее из всех тех и только тех упорядоченных пар, первая компонента которых принадлежит множеству A, а вторая – множеству B. Таким образом, элементами прямого произведения множеств являются двухэлементные кортежи вида (x,y).

Данное определение может быть записано в виде:

$$A \times B = \{(x, y) \mid x \in A, y \in B\}$$

Пример.

Пусть A={1,2,4}; B={1,2}

Тогда A×B={(1,1), (1,2), (2,1), (2,2), (4,1), (4,2)}.

Пример.

Пусть даны множества A={a, b, c, d, e, f, g, h} и B = {1, 2, 3, 4, 5, 6, 7, 8}

Тогда $A \times B$ есть множество обозначений шахматной доски.

Мощность произведения конечных множеств равна произведению мощностей этих множеств, т.е. $|A \times B| = |A| \cdot |B|$.

Операция прямого произведения легко распространяется и на большее число множеств.

Задания

1. Для следующих пар множеств проверьте наличие соотношений $A \subset B$, $B \subset A$, $A = B$, $A \in B$, $B \in A$.

   а) A={a,b,c,d}, B={a,c,d}

   б) A=∅, B={a,b,c}

   в) A=∅, B=∅

   г) A=∅, B={∅}

   д) A={a,b,c}, B={b,c, a}

   е) A={{a},a,∅}, B={ a}

   ж) A={{a},a,∅}, B=∅

з) $A=\{\{a,b\},\{c,d\},c,d\}$, $B=\{\{a,b\},c\}$

2. Даны множества $A=\{1,2,3,4,5,6,7\}$, $B=\{3,4,5,6,7,8,9\}$, $C=\{-3,-2,-1,0,1,2,3,4\}$, $D=\{2,3,4,5,6\}$. Определите мощность заданных множеств. Задайте списками множества и определите их мощность:
   а) $A\cap B\cap C\cap D$
   б) $A\cup B\cup C\cup D$
   в) $(A\cup B)\cap(C\cup D)$
   г) $(A\cap B)\cup(C\cap D)$
   д) $(A\setminus B)\cup(B\setminus A)$
   е) $\overline{D}_A\cup(C\setminus B)$
3. Даны множества: $A=(-\infty;\ \ 4]$, $B=[2;\ \ 11]$, $C=(6;\ \ 10)$. Найдите $(\overline{A}\setminus B)\cap C$.
4. Даны множества. Задайте эти множества перечислением элементов.
   а) $X=\{a/a\in Z$ и $|a|<6\}$
   б) $Y=\{a/a\in Z$ и $a^2\le 4\}$
   в) $A=\{x/5x-6-x^2=0\}$
   г) $B=\{x/(x-1)(2x+1)(x+3)=0\}$
   д) $C=\{a/5-a^2=0\}$
   е) $D=\{y/6y+y^2=0\}$
   ж) $E=\{x/5x-6-x^2<0\}$
   з) $F=\{x/x^2+1=0\}$
   и) $I=\{x/x^2+1\ge 0\}$
   к) $K=\{x/1<x<5,\ x\in N\}$
   л) $L=\{x/x=(-1)^n,\ n\in N\}$
   м) $M=\{x/x=1+3(-1)^n,\ n\in N\}$
5. Задайте множества характеристическим свойством:
   а) A - множество всех действительных чисел, не больших 5;
   б) B - множество всех действительных чисел, больших 2 и меньших 5;
   в) C - множество всех отрицательных рациональных чисел;
   г) D - множество всех неотрицательных действительных чисел;
   д) E - множество всех отрицательных целых чисел;
   е) F - множество всех цифр.
6. Даны множества $X=\{-5,-4,-3,-2,-1,0,1\}$, $Y=\{-3,-2,-1,2,3,4\}$, $Z=\{-7,-6,5,6,7\}$. Задайте списками множества:
   а) $X\cup Y\cup Z$
   б) $(X\cap Z)\cup Y$
   в) $Z\cup(X|Y)$
   г) $X\cap Y\cap Z$
   д) $Z\cup(X\cap Y)$
   е) $(X\cup Z)\cap(Y\cup Z)$
7. Пусть R – множество букв современного русского алфавита,
   A – подмножество R, состоящее из букв, составляющих слово <u>*аксиома*</u>,
   B – подмножество R, состоящее из букв, составляющих слово <u>*скорость*</u>,
   C – подмножество R, состоящее из букв, составляющих слово <u>*паспорт*</u>.
   Задайте способом перечисления следующие множества и найдите их мощность:
   а) $A\cup B$ б) $B\cap C$ в) $C\setminus A$ г) $A\cap B\cap C$
8. Составьте множества: A – множество букв своего полного имени; B – множество букв своего отчества, C – множество букв своей фамилии. Для полученных множеств найдите:
   а) $A\cup B$; б) $A\cap B$; в) $C\setminus A$; г) $A\setminus C$; д) $A\cap B\cap C$

9. Из 40 студентов 30 умеют плавать, 27 умеют играть в шахматы и только пятеро не умеют ни того, ни другого. Сколько студентов умеют плавать и играть в шахматы?
10. 20 мальчиков поехали на пикник. При этом 5 из них обгорели, 8 были сильно покусаны комарами, а 10 остались всем довольны. Сколько обгоревших мальчиков не было покусано комарами? Сколько покусанных комарами мальчиков также и обгорели?
11. В штучном отделе магазина посетители обычно покупают либо один торт, либо одну коробку конфет, либо один торт и одну коробку конфет, В один из дней было продано 57 тортов и 36 коробок конфет. Сколько было покупателей, если 12 человек купили и торт, и коробку конфет?
12. Из 35 сотрудников фирмы «Толмач», каждый из которых владеет хотя бы одним иностранным языком, 25 человек знают английский язык, 15 человек – греческий язык, 20 человек – французский язык, 15 человек знают английский и французский языки, 6 – греческий и французский языки и 10 – греческий и английский языки. Сколько сотрудников фирмы знают: а) все 3 языка? б) только греческий и французский языки (т.е. знают греческий и французский языки, но не знают английского языка)?
13. Среди абитуриентов, выдержавших приемные экзамены в вуз, оценку «отлично» получили: по русскому языку – 48 абитуриентов, по математике –37, по физике – 42, по русскому языку или математике – 75, по русскому языку или физике – 76, по математике или физике – 66, по всем трем предметам – 4. Сколько абитуриентов получили хотя бы одну пятерку? Сколько среди них получивших только одну пятерку?
14. Каждый из студентов 3 курса в летние каникулы ровно два раза был в театре, при этом спектакли А, В и С видели соответственно 25, 12 и 23 студента. Сколько студентов на 3 курсе? Сколько из них видели спектакли А и В, А и С, В и С?
15. В течение недели в кинотеатре демонстрировались фильмы А, *B* и *C*. Из 40 студентов, каждый из которых просмотрел либо все три фильма, либо один из трех, фильм А видели 13, фильм В – 16, фильм С – 19. Найти, сколько студентов просмотрели все три фильма.
16. Преподаватель решил узнать, кто из 40 студентов читал книги А, В и С. Результаты опроса оказались таковы: книгу А читало 25 человек, книгу В – 22, книгу С – также 22. Книгу А или В читали 33 студента, А или С – 32, В или С – 31; все три книги прочли 10 студентов. Сколько студентов прочли только по одной книге? Сколько студентов не читали ни одной из этих трех книг?
17. В спортивном лагере 65% студентов умеют играть в футбол, 70% – в волейбол и 75% – в баскетбол. Каково наименьшее число студентов, умеющих играть и в футбол, и в волейбол, и в баскетбол?
18. Исследуется текст из 100 предложений. В каждом из 100 предложений имеется либо местоимение «***я***», либо местоимение «***ты***», либо оба местоимения. Всего в тексте встретилось 60 местоимений «***я***» и 50 местоимений «***ты***». Сколько предложений содержат и местоимение «***я***» и местоимение «***ты***»? Сколько предложений содержат местоимение «***я***» и не содержат местоимения «***ты***»?
19. Найдите декартово произведение множеств *A* и *B*, *B* и *A*, если $A=\{1,2,3,4,5,6,7\}$, $B=\{3,4,5,6,7,8,9\}$,
20. Изобразите в прямоугольной системе координат множество $A\times B$, если $A=(2;\ \ 6]$, $B=(-\infty;\ \ 1]$.
21. Напишите первые пять элементов занумерованного счетного множества, *n-й* элемент которого задан формулой $a_n=\dfrac{n+1}{n^2}$.

Контрольные вопросы

1. Что такое множество, конечное и бесконечное множество, мощность множества, подмножество?
2. Какие способы задания множеств вам известны?
3. Как определить мощность множества?

4. Как сравнить множества?
5. Какие операции над множествами вам известны?
6. Расскажите правила выполнения операций над множествами.

Практическая работа №2
«Подстановки. Метод математической индукции»

Цель: формирование навыков выполнения операций с подстановками и использования метода математической индукции.

Теоретические сведения

Подстановки

Всякое взаимно однозначное отображение множества А первых n натуральных чисел на себя называется подстановкой n-й степени, причем, очевидно, всякая подстановка А может быть записана при помощи двух перестановок, подписанных одна под другой

$$A = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \alpha_{i_1} & \alpha_{i_2} & \dots & \alpha_{i_n} \end{pmatrix} \qquad (1)$$

Через α_i здесь обозначается то число, в которое при подстановке А переходит число i , $i = 1, 2, \dots, n$.

Запишем одну под другой две перестановки из n символов, беря полученные две строки в скобки; например, n=5:

$$\begin{pmatrix} 3\ 5\ 1\ 4\ 2 \\ 5\ 2\ 3\ 4\ 1 \end{pmatrix} \qquad (2)$$

Мы скажем, что число 3 переходит в число 5, число 5 переходит в 2, число 1 переходит в 3, число 4 переходит в 4(или остаётся на месте), и, наконец, число 2 переходит в 1. Таким образом, две перестановки, записанные друг под другом в виде (2), определяют некоторое взаимно однозначное отображение множества из первых пяти натуральных чисел на себя, т. е. отображение, которое каждому из натуральных чисел 1, 2, 3, 4, 5 ставит в соответствие одно из этих же натуральных чисел, причем разным числам ставятся в соответствие различные же числа.

Ясно, что то взаимно однозначное отображение множества их первых пяти натуральных чисел, которые мы получили при помощи (2), можно было получить, записывая одну под другой и некоторые другие пары перестановок из пяти символов. Эти записи получаются из (2) путем нескольких транспозиций (перестановок) столбиков; таковы, например,

$$\begin{pmatrix} 3\ 5\ 1\ 4\ 2 \\ 5\ 2\ 3\ 4\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1\ 5\ 2\ 4\ 3 \\ 3\ 2\ 1\ 4\ 5 \end{pmatrix}, \quad \begin{pmatrix} 2\ 5\ 1\ 4\ 3 \\ 1\ 2\ 3\ 4\ 5 \end{pmatrix}. \qquad (3)$$

Во всех этих записях 3 переходит в 5, 5 в 2 и т. д.

Подстановка А обладает многими различными записями вида (1). Так, (2) и (3) являются различными записями одной и той же подстановки 5-й степени.

Канонический вид подстановки

В частности, всякая подстановка n-й степени А может быть записана в каноническом виде

$$\begin{pmatrix} 1 & 2 & \dots & 3 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \qquad (4)$$

т. е. с натуральным расположением чисел в верхней строке. При такой записи различные подстановки отличаются друг от друга перестановками, стоящими в нижней строке.

Примером подстановки n-й степени служит тождественная подстановка

$$E = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

при котором на месте остаются все символы.

Замечание. Следует заметить, что верхняя и нижняя строки в записи (1) подстановки А играют разные роли и, переставив их, мы, вообще говоря, получаем другую подстановку.

Цикловая структура подстановки

Подстановка вида

$$i_1 \to i_2,\ \ i_2 \to i_3,\ \ \ldots,\ \ i_{m-1} \to i_m,\ \ i_m \to i_1.$$

(При этом все числа i_1, i_2, …, i_m - различны)

называется циклом длины m.

Для циклов вводят специальное обозначение:

$$\begin{pmatrix} i_1\ i_2 \ldots\ i_{m-1}\ i_m \\ i_2\ i_3 \ldots\ i_m \quad\ i_1 \end{pmatrix} = (i_1,\ \ i_2,\ \ \ldots\ \ i_{m-1},\ \ i_m)$$

Задание 1. Цикл (2 3 4 1) действует следующим образом

$$2 \to 3 \to 4 \to 1 \to 2$$

Циклы, не содержащие общих элементов, называются **независимыми** (непересекающимися).

Теорема. Каждую подстановку можно разложить в произведение независимых циклов. Это разложение единственно с точностью до порядка циклов.

Алгоритм составления цикла:

1.Берем подстановку, смотрим, во что переходит первый элемент.

2.Полученный элемент пишем за первым элементом и находим его образ под действием подстановки.

3. Как только образ совпадает с элементом, с которого началось построение цикла, закрываем цикл.

4. Дальше берем любой элемент, не входящий в уже выписанные циклы и начинаем построение нового цикла.

Задание 2.

Разложить подстановку

$$\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 3\ 4\ 5\ 2\ 1\ 8\ 7\ 6 \end{pmatrix}$$

в произведение независимых циклов.

Решение.

Так как $1 \to 3 \to 5 \to 1$, то получаем цикл (135). Цепочка 2→4→2 дает транспозицию (24). Так же 6→8→6 дает транспозицию (68). 7 остается на месте.

Ответ: $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 3\ 4\ 5\ 2\ 1\ 8\ 7\ 6 \end{pmatrix} = (135)(68)(24)(7)$

Знак подстановки

Говорят, что в данной строке элементы i и j составляют инверсию, если i > j, но i стоит в этой строке раньше.

(5 3 4 1 2) – число 5 образует 4 инверсии. Общее число инверсий в строке равно 8.

Знак подстановки

$$\begin{pmatrix} 1 & 2 & \ldots & 3 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}$$

равен $(-1)^a$, где a – число инверсий в строке (α_1, α_2, …, α_n)

Задание 3.

Определить знак подстановки

$$\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 3\ 4\ 5\ 2\ 1\ 8\ 7\ 6 \end{pmatrix}$$

Решение.

Число инверсий в строке (3 4 5 2 1 8 7 6) равно 2+2+2+1+0+2+1=10, так как $(-1)^{10}=1$, то данная подстановка является четной.

Знак подстановки можно определить и другим способом. Для этого надо разложить подстановку в произведение независимых циклов.

$$b = (k_1-1)+(k_2-1)+\ldots+(k_l-1)=k_1+k_2+\ldots+k_l-S, \qquad (5)$$

где k_1 , k_2 , …, k_l – длины циклов.

Тогда знак равен $(-1)^b$

Пусть дана подстановка n-й степени и пусть s есть число независимых циклов в её разложении плюс число символом, оставляемых ею на месте. Разность n – s называется декрементом этой подстановки. Декремент равен числу действительно перемещаемых символов, уменьшенному на число независимых циклов, входящих в разложение подстановки и равносилен b в формуле (5).

Замечание. Четность подстановки совпадает с четностью декремента этой подстановки.

Задание 4.

Определите знак подстановки

$$\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 3\ 4\ 5\ 2\ 1\ 8\ 7\ 6 \end{pmatrix} = (135)(68)(24)(7)$$

с помощью разложения подстановки в произведение независимых циклов.

Решение.

Данная подстановка раскладывается следующим образом в произведение независимых циклов.

$b = 3+2+2+1–4 = 4$, $(-1)^4 = 1$. Это четная подстановка.

Умножение подстановок

Произведением первой подстановки на вторую называют последовательное выполнение двух подстановок n-й степени, приводящее к некоторой вполне определенной третьей подстановке n-й степени.

так, если даны подстановки четвертой степени

$$A = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 4\ 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 3\ 4\ 2 \end{pmatrix},$$

то

$$AB = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 1\ 2\ 3 \end{pmatrix}.$$

Действительно, при подстановке A символ 1 переходит в 3, но при B символ 3 переходит в 4, поэтому при AB символ 1 переходит в 4, и т. д.

Можно перемножить лишь подстановки одинаковой степени. Умножение подстановки n-й степени при $n \geq 3$некоммутативно. Действительно, для рассмотренных выше подстановок A и B произведение BA имеет вид

$$BA = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 4\ 2\ 1 \end{pmatrix}$$

т. е. подстановка BA отлична от подстановки AB. Такие примеры можно подобрать для всех n при $n \geq 3$, хотя для некоторых пар подстановок закон коммутативности случайно может выполняться.

Умножение подстановок ассоциативно, т. е. можно говорить о произведении любого конечного числа подстановок n-й степени, взятых (ввиду некоммутативности) в определенном порядке. В самом деле, пусть даны подстановки A, B и C и пусть символ i_1, $1 \leq i_1 \leq n$, переходит при подстановке A в символ i_2, i_2 при подстановке B переходит в символ i_3, а последний при подстановке C – в символ i_4. Тогда при подстановке AB символ i_1 переходит в i_3, при подстановке BC символ i_2 переходит в i_4, а поэтому как при (AB)C, так и при A(BC) символ i_1, будет переходить в символ i_4.

Очевидно, что произведение любой подстановки A на тождественную подстановку E, а также произведение E на A, равно A:

$$AE=EA=A$$

Назовем, наконец, обратной для подстановки A такую подстановку A^{-1} той же степени, что

$$AA^{-1} = A^{-1}A = E$$

Легко видеть, что обратной подстановкой для подстановки

$$A = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$$

служит подстановка

$$A^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

получающаяся из А переменой мест верхней и нижней строк.

Задание 5.

Найти подстановку, обратную данной

$$A = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,3\,5\,6\,1 \end{pmatrix}$$

Решение.

Подстановка A^{-1}, обратная подстановке А будет иметь вид

$$A^{-1} = \begin{pmatrix} 2\,4\,3\,5\,6\,1 \\ 1\,2\,3\,4\,5\,6 \end{pmatrix}$$

приведем её к каноническому виду.

$$A^{-1} = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 6\,1\,3\,2\,4\,5 \end{pmatrix}$$

Задание 6.

Найти порядок указанного элемента в группе S_n, n=5

$$S_5 = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix}$$

Решение:

$$S^2 = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} \times \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,2\,4\,5 \end{pmatrix}$$

$$S^3 = S^2 \times S \quad = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,2\,4\,5 \end{pmatrix} \times \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,3\,5\,4 \end{pmatrix}$$

$$S^4 = S^3 \times S \quad = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,3\,5\,4 \end{pmatrix} \times \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,4\,5 \end{pmatrix}$$

$$S^5 = S^4 \times S \quad = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,4\,5 \end{pmatrix} \times \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,2\,5\,4 \end{pmatrix}$$

$$S^6 = S^5 \times S \quad = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,1\,2\,5\,4 \end{pmatrix} \times \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,5\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 1\,2\,3\,4\,5 \end{pmatrix}$$

Наконец, получили тождественную подстановку Е

Ответ: 6

Метод математической индукции

При изучении явлений в любой области знаний (математика, история, физика, медицина, астрономия, экономика и т.д.) основным этапом является установление определенных закономерностей, связывающих отдельные элементы изучаемого явления. Подмечается определенная связь между элементами изучаемого явления, справедливого для многих частных случаев, и распространяется на все случаи вообще, устанавливается общий закон, раскрывающий сущность данного явления.

Все утверждения можно разделить на общие и частные. Например, утверждение «Во всяком параллелограмме диагонали делятся в точке пересечения пополам» является общим, так как относится ко всему множеству параллелограммов. В то же время утверждение «В параллелограмме ABCD диагонали делятся в точке пересечения пополам» является частным, так как относится к конкретному параллелограмму ABCD.

По своему первоначальному смыслу слово «индукция» применяется к рассуждениям, при помощи которых получают общие выводы, опираясь на ряд частных утверждений. Простейшим методом рассуждений такого рода является полная индукция.

Вот пример подобного рассуждения.

Пусть требуется установить, что каждое натуральное четное число n в пределах 4‹n‹20 представимо в виде суммы двух простых чисел. Для этого возьмем все такие числа и выпишем соответствующие разложения:

4=2+2; 6=3+3; 8=3+5; 10=7+3; 12=7+5; 14=7+7; 16=11+5; 18=13+5; 20=13+7.

Эти девять равенств показывают, что каждое из интересующих нас чисел действительно представляется в виде суммы двух простых чисел.

Таким образом, полная индукция заключается в том, что общее утверждение доказывается по отдельности в каждом из конечного числа возможных случаев.

Метод полного перебора конечного числа случаев, исчерпывающих все возможности, называется **полной индукцией**. Этот метод имеет крайне ограниченную область применения в математике, так как обычно математические утверждения касаются бесконечного множества объектов (например, натуральных чисел, простых чисел, квадратов и т.п.) и перебрать их невозможно.

Иногда общий результат удается предугадать после рассмотрения не всех, а достаточно большого числа частных случаев (так называемая неполная индукция). Результат, полученный неполной индукцией, остается, однако, лишь гипотезой, пока он не доказан точным математическим рассуждением, охватывающим все частные случаи. Неполная индукция в математике не считается законным методом строгого доказательства, но является мощным методом открытия новых истин.

Пусть, например, требуется найти сумму первых n последовательных нечетных чисел. Рассмотрим частные случаи:

$1=1=1^2$

$1+3=4=2^2$

$1+3+5=9=3^2$

$1+3+5+7=16=4^2$

$1+3+5+7+9=25=5^2$.

После рассмотрения этих нескольких частных случаев напрашивается следующий общий вывод:

$1+3+5+\ldots+(2n-1)=n^2$, т.е. сумма n последовательных нечетных чисел равна n^2.

Разумеется, сделанное наблюдение еще не может являться доказательством данной формулы. Часто неполная индукция приводит к ошибочным результатам.

Во многих случаях выход из такого рода затруднений заключается в обращении к *методу математической индукции.* Этот метод рассуждений, который позволяет **заменить неосуществимый бесконечный перебор** доказательством того, что если утверждение истинно в одном случае, то оно окажется истинным и в следующем за ним случае. Этот метод – это рассуждение от n к n+1.

Метод математической индукции заключается в следующем.

Пусть нужно доказать справедливость некоторого утверждения для любого натурального числа n (например, нужно доказать, что сумма n последовательных нечетных чисел равна n^2). Непосредственная проверка этого утверждения для каждого значения n невозможна, поскольку множество натуральных чисел бесконечно. Чтобы это доказать, проверяют сначала его справедливость для n=1. Затем доказывают, что при любом натуральном значении k из справедливости рассматриваемого утверждения при n =k вытекает его справедливость и при n= k+1. Тогда утверждение считается доказанным для всех n.

В основе метода математической индукции (ММИ) лежит **принцип математической индукции**: утверждение $P(n)$ (где n - натуральное число) справедливо при $\forall n \in N$, если:

- Утверждение $P(n)$ справедливо при n=1.
- Для $\forall k \in N$ из справедливости $P(k)$ следует справедливость $P(k+1)$.

Доказательство с помощью метода математической индукции проводится в два этапа:

1. **База индукции (базис индукции).** Проверяется истинность утверждения при n=1 (или любом другом подходящем значении n)
2. **Индуктивный переход (шаг индукции).** Считая, что справедливо утверждение $P(k)$ при $n=k$, проверяется истинность утверждения $P(k+1)$ при $n=k+1$.

Метод математической индукции **применяется в разных типах задач**:

- Доказательство делимости и кратности
- Доказательство равенств и тождеств
- Задачи с последовательностями
- Доказательство неравенств
- Нахождение суммы и произведения

Примеры

Задание 1.

Доказать, что 1+3+5+…+(2n-1)=n^2.

Решение:1) Имеем n=1=1^2. Следовательно, утверждение верно при n=1, т.е. A(1) истинно.

2) Докажем, что A(k) =>A(k+1).

Пусть k – любое натуральное число и пусть утверждение справедливо для n= k, т.е. 1+3+5+…+(2 k -1)=k^2.

Докажем, что тогда утверждение справедливо и для следующего числа n= k+1, т.е. что 1+3+5+…+(2 k +1)=$(k+1)^2$. В самом деле, 1+3+5+…+(2 k -1)+ (2 k +1)= k^2+2 k+1=$(k+1)^2$.

Итак, A(k) =>A(k+1). На основании принципа математической индукции заключаем, что предложение A(n) истинно для любого n∈N.

Задание 2.

Доказать, что при любом n справедливо утверждение: 1^2+2^2+3^2+…+n^2= n(n+1)(2 n+1)/6.

Решение:1) Пусть n=1, тогда 1^2=1(1+1)(2+1)/6=1. Значит, при n=1 утверждение верно.

2) Предположим, что при n= k верно 1^2+2^2+3^2+…+k^2= k (k +1)(2 k +1)/6.

3) Рассмотрим данное утверждение при n= k+1:

1^2+2^2+3^2+…+k^2+$(k+1)^2$= k (k +1)(2 k +1)/6+$(k+1)^2$=(k (k +1)(2 k +1)+6$(k+1)^2$)/6=

=(k +1) (k(2 k +1)+6(k +1))/6=(k +1)(2k^2+7 k+6)/6=(k +1) (k +2) (2k +3)/6.

Из приведенного доказательства видно, что утверждение верно при n= k+1, следовательно, равенство верно при любом натуральном n.

Задание 3.

Доказать, что при любом n справедливо утверждение: 1^3+2^3+3^3+…+n^3= $n^2(n+1)^2$/4.

Решение:1)Пусть n=1. Тогда X_1 =$1^2(1+1)^2$/4.

2) Предположим, что равенство верно при n= k: X_k=$k^2(k+1)^2/4$.

3) Докажем истинность этого утверждения при n= k+1, т.е. X_{k+1}=$(k+1)^2(k+2)^2/4$.

X_{k+1}= 1^3+2^3+3^3+…+k^3 + $(k+1)^3$= $k^2(k+1)^2$/4+$(k+1)^3$=

$= \frac{(k+1)^2\left(k^2+4(k+1)\right)}{4} = (k+1)^2(k+2)^2/4.$

Из приведенного доказательства видно, что утверждение верно при n= k+1, следовательно, равенство верно при любом натуральном n.

Задание 4.

Доказать, что при любом целом неотрицательном n число 2n^3-3n^2+ n делится на 6.

Решение: 1) Пусть n=1. Тогда X_1=$2\cdot 1^3 - 3\cdot 1^2 + 1$=0 делится на 6.

2) Предположим, что при n= k X_k=$2\cdot k^3 - 3\cdot k^2 + k$ делится на 6, т.е. X_k= 6m, где m – целое число.

3) Докажем истинность этого утверждения при n= k+1.

X_{k+1}= $2\cdot(k+1)^3 - 3\cdot(k+1)^2 + (k+1)$=2$k^3$+6$k^2$+6 k+2-3$k^2$-6 k-3+ k+1=

=$2\cdot k^3 - 3\cdot k^2 + k$+6$k^2$= 6m+6$k^2$ =6(m+k^2) кратно 6.

В силу метода математической индукции утверждение доказано.

Задание 5.

Доказать, что разность одинаковых четных степеней двух целых чисел делится на сумму оснований, т.е. (x^{2n}-y^{2n}) делится на x+y при любом натуральном n (x+y не равно 0).

Решение: 1) При n=1 утверждение задачи верно, т.е. (x^2-y^2) делится на x+y. Значит, при n=1 утверждение верно.

2) Предположим, что при n= k (x^{2k}-y^{2k}) делится на x+y, т.е. (x^{2k}-y^{2k})=(x+y)c.

3) Докажем, что это утверждение верно при n= k+1.

x^{2k+2}-y^{2k+2}= (x^2-y^2) x^{2k}+$x^{2k}y^2$-y^{2k+2}=(x^2-y^2) x^{2k}+y^2(x^{2k}-y^{2k})= (x-y)(x+y) x^{2k}+(x+y)cy^2=

=(x+y)((x-y) x^{2k}+cy^2). Утверждение верно при любом n.

В силу метода математической индукции утверждение доказано.

Задание 6.

Доказать, что сумма каждой строки таблицы

1

2,3,4

3.4,5,6,7

……

равна квадрату нечетного числа, номер которого в строке равен номеру строки от начала таблицы.

Решение: Общий член последовательности, т.е. n-я строка, может быть записан так:

n, n+1, n+2, …, (n+(n-1)·2). Значит, последний член в этой строке равен 3n-2. Надо доказать, что сумма чисел этой строки равна S(n)=$(2n-1)^2$.

Решение: 1) Для n=1 формула верна.

2) Предположим, что формула верна для некоторого натурального значения n= k, т.е. S(k)= k+(k+1)+(k+2)+…+(3 k-2)= $(2k-1)^2$.

3) Докажем, что она верна при n= k+1.

S(k+1)= (k+1)+(k+2)+…+(3 k-2)+(3k-1)+ 3k +(3k+1) = k +(k+1)+(k+2)+…+(3 k-2)+(3k-1)+

+3k +(3k+1) – k= S(k)+ (3k-1)+ 3k +(3k+1) – $(2k-1)^2$=$(2k-1)^2$+8k=$(2k+1)^2$.

В силу метода математической индукции утверждение доказано.

Задание 7.

Доказать, что при любом натуральном n>3 справедливо неравенство

1/1!+1/2!+1/3!+…+1/ n!<(2n-1)/n.

Решение: 1) При n=4 имеем 1+17/24<1+3/4, т.е. для n=4 неравенство верно.

2) Предположим, что неравенство верно при n= k, т.е. 1/1!+1/2!+1/3!+…+1/ k!<(2 k - 1)/ k.

3) Докажем, что оно верно и для n= k+1.

1/1!+1/2!+1/3!+…+1/ k!+ 1/ (k+1)!<(2k -1)/ k+1/ (k+1)!=2-1/ k+1/(k+1)!=2(k+1)/ (k+1)-1/(k+1)+1/(k+1)- 1/k+1/(k+1)!=(2(k+1)-1)/ (k+1)+(1/ (k+1)!-1/(k (k+1)))< (2(k+1)-1)/ (k+1), т.к. 1/ (k+1)!- 1/(k (k+1))<0.

В силу метода математической индукции неравенство доказано.

Задание 8.

Доказать, что при любом натуральном n>2 справедливо неравенство

1+(1/2^2)+(1/3^2)+…+(1/n^2)<1,7-(1/ n).

Решение: 1) При n=3 имеем 1+(1/2^2)+(1/3^2)=245/180<246/180=1,7-(1/3).

2) Предположим, что неравенство верно при n= k, т.е. 1+(1/2^2)+(1/3^2)+…+(1/k^2)<1,7-(1/ k).

3) Докажем, что для n= k+1 верно неравенство

1+(1/2^2)+(1/3^2)+…+(1/k^2)+ (1/$(k+1)^2$)<1,7-(1/ k)+ (1/$(k+1)^2$).

Докажем, что 1,7-(1/ k)+ (1/$(k+1)^2$)< 1,7-(1/ (k+1)):

(1/$(k+1)^2$)+ (1/ (k+1))< 1/ k;

(k+2)/$(k+1)^2$< 1/ k;

k (k+2)< $(k+1)^2$;

$k^2+2k < k^2+ 2k +1$.

Последнее очевидно, а поэтому $1,7-(1/ k)+ (1/(k+1)^2)< 1,7-(1/ (k+1))$.

В силу метода математической индукции неравенство доказано.

Задание 9.

Каждый человек в мире пожал какое-то количество рук. Доказать, что число людей, пожавших нечетное число рук, - четно.

Решение.

Пронумеруем все рукопожатия в мире от первого (его необязательно должны были совершить Адам и Ева) до произвольного натурального n. Очевидно, что при n=1 утверждение справедливо. Предположим, что оно верно при каком-то n= k, т.е. количество людей, участвовавших в рукопожатиях с номерами от 1 до k и сделавших нечетное количество рукопожатий, четно.

Докажем, что это утверждение верно при k. Возможны три варианта осуществления (k+1) рукопожатия:

друг другу пожимают руки: а) два особых человека; б) два неособых человека; в) один особый и один неособый человек.

В каждом из этих трех случаев количество особых людей либо уменьшается на два, либо увеличивается на два, либо не изменяется, т.е. остается четным.

Утверждение доказано.

Задание 10.

Чему равна сумма первых n членов последовательности 1,3,5,7,9,11,13,…?

Решение.

Составим суммы одного, двух, трех и т.д. первых членов данной последовательности:

$S_1=1=1^2$; $S_2=1+3=4=2^2$; $S_3=1+3+5=9=3^2$; $S_4=1+3+5+7=16=4^2$; $S_5=1+3+5+7+9=25=5^2$.

На основе этих наблюдений можно высказать предположение, что

$S_n=1+3+5+7+9+\ldots+(2n-1) =n^2$ (1)

Верно ли это предположение при любом натуральном n?

Предположим, что формула (1) верна для n= k, где k-натуральное, т.е.

$S_k=1+3+5+7+9+\ldots+(2k-1) =k^2$ (2)

Докажем ее справедливость и для числа, следующего за k, для числа n= k+1:

$S_{k+1}=1+3+5+7+9+\ldots+(2k-1)+ (2k+1)=(k+1)^2$ (3)

Заменим на основе равенства (2) $S_k=1+3+5+7+9+\ldots+(2k-1)$ на k^2:

$S_{k+1}=S_k+(2k+1)= k^2+2k+1=(k+1)^2$.

Доказано.

При доказательстве гипотезы методом математической индукции очень важно выполнение всех его составляющих.

Рассмотрим следующие примеры.

При отсутствии первого шага (*базиса индукции*) можно «доказать», что числа вида 2n-1 являются четными при любом натуральном n.

Пусть утверждение справедливо для n= k, т.е. 2k -1 является четным числом.

Проверим верность утверждения при n= k+1: 2(k+1)-1=2 k+2-1=(2k-1)+2.

По предположению индукции 2k -1 четное число, следовательно, число (2k-1)+2 тоже четное.

Отсутствие первого шага приводит к ошибке.

В поисках формулы, дающей только простые числа, знаменитый математик XVIII века Л.Эйлер подверг испытанию трехчлен $P(n)=n^2+n+41$. Этот трехчлен давал простые числа при всех значениях n от 1 до 39:

P(1)=12+1+41=43;

P(2)=22+2+41=47;

P(3)=32+3+41=53;

……

P(39)=392+39+41=1601;

P(40)=402+40+41=1641=41^2.

Отсутствие второго шага (*индукционного шага*) приводит к неверному результату.

Само доказательство гипотезы методом математической индукции состоит из следующих частей:

Проверяют справедливость гипотезы для наименьшего из натуральных чисел, при котором гипотеза имеет смысл (базис);

Сделав предположение, что гипотеза верна для некоторого значения k, стремятся доказать справедливость ее для k+1.

Если такое доказательство удалось довести до конца, то, на основании принципа математической индукции можно утверждать, что высказанная гипотеза справедлива при любом натуральном n.

Метод математической индукции не дает никаких указаний, как построить гипотезу. Вопрос о том, как возникает гипотеза, принадлежит к той области, в которой нет никаких общих правил, здесь делает свое дело эксперимент, аналогия, конструктивная индукция.

Задания

1. Разложить подстановку

$$\begin{pmatrix} 1\ 2\ 3\ 5\ 4\ 6\ 7\ 8 \\ 3\ 5\ 4\ 2\ 8\ 1\ 7\ 6 \end{pmatrix}$$

в произведение независимых циклов.

2. Определить знак подстановки

$$\begin{pmatrix} 1\ 2\ 3\ 5\ 4\ 6\ 7\ 8 \\ 3\ 5\ 4\ 2\ 8\ 1\ 7\ 6 \end{pmatrix}$$

3.Найти подстановку, обратную данной

$$A = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 4\ 2\ 5\ 3\ 1\ 6 \end{pmatrix}$$

4.Найти порядок указанного элемента в группе S_n, n=5

$$S_5 = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 2\ 1\ 4\ 5 \end{pmatrix}$$

5.Применяя метод математической индукции, доказать, что для любого натурального *n* справедливы следующие равенства:

а) $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ **;**

б) $1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$ **.**

Контрольные вопросы

1. Что такое подстановка?
2. Как определить знак подстановки?
3. Как найти подстановку, обратную данной?
4. В чем суть метода математической индукции?

Практическая работа №3
«Логические операции над высказываниями. Таблицы истинности. Законы алгебры логики. Логические операции над предикатами»

Цель: формирование навыков выполнения логических операций и составления таблиц истинности.

Теоретические сведения

Исследования в алгебре логики тесно связаны с изучением ***высказываний*** (хотя высказывание — предмет изучения формальной логики). ***Высказывание*** — это языковое образование, в отношении которого имеет смысл говорить о его истинности или ложности.

Простым высказыванием называют повествовательное предложение, относительно которого имеет смысл говорить, ***истинно*** оно или ***ложно***.

С помощью высказываний устанавливаются свойства, взаимосвязи между объектами. Высказывание истинно, если оно адекватно отображает эту связь, в противном случае оно ложно.

Примеры высказываний:

1. Сегодня светит солнце.
2. Трава растет.

Каждое из этих высказываний характеризует свойства или состояние конкретного объекта (в пермом предложении - погоды, во втором - окружающего мира). Каждое из этих высказываний несет значение ***«истина»*** или ***«ложь»***.

В математической логике не рассматривается конкретное содержание высказывания, важно только, ***истинно*** оно или ***ложно***. Поэтому высказывание можно представить некоторой ***переменной величиной***, значением которой может быть только ***0*** или ***1***. Если высказывание ***истинно***, то его значение равно ***1***, если ***ложно - 0***.

Простые высказывания назвали ***логическими переменными***, а ***сложные - логическими функциями***. Значения логической функции также только ***0*** или ***1***. Для простоты записи высказывания обозначаются латинскими буквами ***A, B, C***.

Однако определение истинности высказывания далеко не простой вопрос. Например, высказывание «Число 1 +22 = 4294 967297 — простое», принадлежащее Ферма (1601-1665), долгое время считалось истинным, пока в 1732 году Эйлер (1707-1783) не доказал, что оно ложно. В целом, обоснование истинности или ложности простых высказываний решается вне алгебры логики. Например, истинность или ложность высказывания «Сумма углов треугольника равна 180°» устанавливается геометрией, причем в геометрии Евклида это высказывание является истинным, а в геометрии Лобачевского — ложным.

В булевой алгебре простым высказываниям ставятся в соответствие логические переменные, значение которых равно ***1***, если высказывание ***истинно***, и ***0***, если высказывание ***ложно***. Обозначаются логические переменные, ***большими буквами латинского алфавита***.

Существуют разные варианты обозначения истинности и ложности логических переменных:

Истина	И	True	T	1
Ложь	Л	False	F	0

Сложные (составные) высказывания представляют собой набор простых высказываний (по крайней мере двух) связанных ***логическими операциями***.

С помощью логических переменных и символов логических операций любое высказывание можно ***формализовать***, то есть заменить ***логической формулой (логическим выражением)***.

Логическое выражение - это символическая запись высказывания, состоящая из ***логических величин (констант или переменных)***, объединенных ***логическими операциями (связками)***.

Связки ***"НЕ", "И", "ИЛИ"*** заменяются логическими операциями ***инверсия***, ***конъюнкция***, ***дизъюнкция***. Это основные логические операции, при помощи которых можно записать любое логическое выражение.

Введем перечисленные логические операции.

Конъюнкция - логическое умножение (от латинского conjunctio - союз, связь):

- в естественном языке соответствует союзу ***«И»***;
- в алгебре высказываний обозначение ***«&»***;
- в языках программирования обозначение ***«And».***

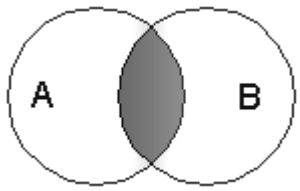
Конъюнкция - это логическая операция, ставящая в соответствие каждым двум простым (или исходным) высказываниям составное высказывание, являющееся истинным тогда и только тогда, когда оба исходных высказывания истинны. Если хотя бы одно из составляющих высказываний ложно, то и полученное из них с помощью союза ***«И»*** сложное высказывание также считается ложным.

В алгебре множеств ***конъюнкции*** соответствует операция ***пересечения*** множеств, т.е. множеству получившемуся в результате умножения множеств ***A*** и ***B*** соответствует множество, состоящее из элементов, принадлежащих одновременно двум множествам.

Таблица истинности

A	B	A&B
1	1	1
1	0	0
0	1	0
0	0	0

Диаграмма Эйлера-Венна



Итак, если два высказывания соединены союзом ***"И"***, то полученное сложное высказывание истинно тогда и только тогда, когда истинны оба исходных высказывания.

Дизъюнкция - логическое сложение (от латинского disjunctio - ***разобщение, различие***):

- в естественном языке соответствует союзу ***«ИЛИ»***;
- в алгебре высказываний обозначение ***«V»*** или ***«+»***;
- в языках программирования обозначение ***«Or».***

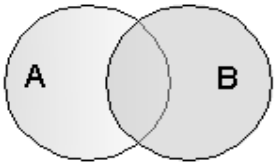
Дизъюнкция - это логическая операция, которая каждым двум простым (или исходным) высказываниям ставит в соответствие составное высказывание, являющееся ложным тогда и только тогда, когда оба исходных высказывания ложны и истинным, когда хотя бы одно из двух образующих его высказываний истинно.

В алгебре множеств ***дизъюнкции*** соответствует операция ***объединения*** множеств, т.е. множеству, получившемуся в результате сложения множеств ***A*** и ***B*** соответствует множество, состоящее из элементов, принадлежащих либо множеству ***A***, либо множеству ***B***.

Таблица истинности

A	B	A + B
1	1	1
1	0	1
0	1	1
0	0	0

Диаграмма Эйлера-Венна



Итак, если два высказывания соединены союзом ***"ИЛИ"***, то полученное сложное высказывание истинно, когда истинно хотя бы одно из составляющих высказываний.

Рассмотренные выше операции были двуместными (бинарными), т.е. выполнялись над двумя операндами (высказываниями). В алгебре логики определена и широко используется и одноместная (унарная) операция ***отрицание.***

Инверсия - отрицание (от латинского disjunctio - ***разобщение, различие***):

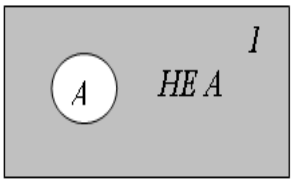
- в естественном языке соответствует словам ***«неверно, что...»*** и частице ***«не»***;
- в алгебре высказываний обозначение ***«¬»*** или ***«-»***;
- в языках программирования обозначение ***«Not».***

Отрицание - логическая операция, которая с помощью связки ***«не»*** каждому исходному высказыванию ставит в соответствие составное высказывание, заключающееся в том, что исходное высказывание отрицается.

В алгебре множеств ***логическому отрицанию*** соответствует операция ***дополнения*** до универсального множества, т.е. множеству, получившемуся в результате отрицания множества ***A*** соответствует множество, дополняющее его до универсального множества.

Таблица истинности	**Диаграмма Эйлера-Венна**

A	**¬ A**
0	1
1	0



Итак, если исходное выражение истинно, то результат ***отрицания*** будет ложным, и наоборот, если исходное выражение ложно, то результат ***отрицания*** будет истинным.

Логическое следование (импликация):

Высказывание, составленное из двух высказываний при помощи связки ***«если ..., то ...»***, называется ***логическим следованием, импликацией*** (импликация от латинского implico - ***тесно связываю***). **A => B "Из A следует B"**

A	**B**	**A=>B**
1	1	1
1	0	0
0	1	1
0	0	1

Итак, новое высказывание, полученное с помощью импликации, является ложным тогда и только тогда, когда условие (посылка ***A***) - истинно, а следствие (заключение ***B***) - ложно и истинно во всех остальных случаях.

Пример. Дано сложное высказывание: «Если выглянет солнце, то станет тепло». Требуется записать его в виде логической формулы. Обозначим через ***A*** простое высказывание «выглянет солнце», а через ***B*** - «станет тепло». Тогда логической формулой этого сложного высказывания будет импликация: **A -> B**.

Эквивалентность (логическое тождество):

Высказывание, составленное из двух высказываний при помощи связки ***«тогда и только тогда, когда»***, называется ***эквивалентностью*** (эквивалентность - ***логическое тождество, равнозначность, взаимная обусловленность.***) **A <=> B "A равносильно B"**

A	**B**	**A<=>B**

1	1	1
1	0	0
0	1	0
0	0	1

Итак, новое высказывание, полученное с использованием эквивалентности, является истинным тогда и только тогда, когда оба исходных высказывания одновременно истинны или одновременно ложны.

В алгебре логики логические связки и соответствующие им логические операции имеют специальные названия и обозначаются следующим образом:

Логическая связка	**Название логической операции**	**Обозначения**
не	Отрицание, инверсия	□□□□
и, а, но	Конъюнкция, логическое умножение	**&, • ,** □
или	Дизъюнкция, логическое сложение	**V, +**
если ..., то	Импликация, следование	□□□
тогда и только тогда, когда	эквивалентность, эквиваленция, равнозначность	□□□□□□□□□□□

Построение таблиц истинности и логических функций

Логическая функция - это функция, в которой переменные принимают только два значения: ***логическая единица*** или ***логический ноль***. Истинность или ложность сложных суждений представляет собой функцию истинности или ложности простых. Эту функцию называют ***булевой функцией суждений f (a, b)***.

Любая логическая функция может быть задана с помощью таблицы истинности, в левой части которой записывается набор аргументов, а в правой части - соответствующие значения логической функции. При построении таблицы истинности необходимо учитывать порядок выполнения логических операций.

Порядок выполнения логических операций в сложном логическом выражении:

1. инверсия;
2. конъюнкция;
3. дизъюнкция;
4. импликация;
5. эквивалентность.

Для изменения указанного порядка выполнения операций используются скобки.

Алгоритм построения таблиц истинности для сложных выражений:

1. Определить количество строк:

количество строк = 2^n + строка для заголовка,

n - количество простых высказываний.

2. Определить количество столбцов:

количество столбцов = количество переменных + количество логических операций;

- определить количество переменных (простых выражений);
- определить количество логических операций и последовательность их выполнения.

3. Заполнить столбцы результатами выполнения логических операций в обозначенной последовательности с учетом таблиц истинности основных логических операций.

Пример: Составить таблицу истинности логического выражения: ***D=¬ A & (B □ C)***.

Решение:

1. Определить количество строк:

на входе три простых высказывания: ***A, B, C*** поэтому n=3 и количество строк равно 2^3 +1 = 9.

2. Определить количество столбцов:

- простые выражения (переменные): A, B, C;
- промежуточные результаты (логические операции):
- ¬ ***A*** - инверсия (обозначим через ***E***);
- ***B □ C*** - операция дизъюнкции (обозначим через ***F***);

а также искомое окончательное значение арифметического выражения: ***D = ¬ A & (B □ C)***. т.е. ***D = E & F*** - это операция конъюнкции.

3. Заполнить столбцы с учетом таблиц истинности логических операций.

A	**B**	**C**	**E**	**F**	**E & F**
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	1	0	1	0
1	1	0	0	1	0
1	1	1	0	1	0

Построение логической функции по ее таблице истинности

Попробуем решить обратную задачу. Пусть дана таблица истинности для некоторой логической функции ***Z(X,Y)***:

X	**Y**	**Z**
0	0	1
0	1	0
1	0	1
1	1	0

Составить логическую функцию для заданной таблицы истинности.

Правила построения логической функции по ее таблице истинности:

1. Выделить в таблице истинности те строки, в которых значение функции равно ***1***.

2. Выписать искомую формулу в виде дизъюнкции нескольких логических элементов. Число этих элементов равно числу выделенных строк.

3. Каждый логический элемент в этой дизъюнкции записать в виде конъюнкции аргументов функции.

4. Если значение какого-либо аргумента функции в соответствующей строке таблице равно ***0***, то этот аргумент взять с отрицанием.

Решение.

1. В первой и третьей строках таблицы истинности значение функции равно ***1***.

2. Так как строки две, получаем ***дизъюнкцию*** двух элементов: ***( ) V ( )***.

3. Каждый логический элемент в этой дизъюнкции запишим в виде ***конъюнкции*** аргументов функции ***X*** и ***Y***: ***(X & Y) V (X & Y)***.

4. Берем аргумент с отрицанием если его значение в соответствующей строке таблицы равно ***0*** и получаем искомую функцию: ***Z (X, Y) =(¬ X & ¬Y) V (X & ¬Y)***.

Законы логики и правила преобразования логических выражений

1. Закон двойного отрицания (двойное отрицание исключает отрицание):

$A = \overline{\overline{A}}$.

2. ***Переместительный (коммутативный) закон:***

- для логического сложения: ***A □ B = B □ A***;
- для логического умножения: ***A & B = B & A***.

Результат операции над высказываниями не зависит от того, в каком порядке берутся эти высказывания.

3. ***Сочетательный (ассоциативный) закон:***

- для логического сложения: ***(A □ B) □ C = A □ (B □ C)***;
- для логического умножения: ***(A & B) & C = A & (B & C)***.

При одинаковых знаках скобки можно ставить произвольно или вообще опускать.

4. ***Распределительный (дистрибутивный) закон:***

- для логического сложения: ***(A □ B) & C = (A & C) □ (B & C)***;
- для логического умножения: ***(A & B) □ C = (A □ C) & (B □ C)***.

Закон определяет правило выноса общего высказывания за скобку.

5. ***Закон общей инверсии (законы де Моргана):***

- для логического сложения: $\overline{A \vee B} = \overline{A} \,\&\, \overline{B}$;
- для логического умножения: $\overline{A \,\&\, B} = \overline{A} \,\square\, \overline{B}$

6. ***Закон идемпотентности*** (от латинских слов idem — тот же самый и potens — сильный; дословно — равносильный):

- для логического сложения: ***A □ A = A***;
- для логического умножения: ***A & A = A*** .

Закон означает отсутствие показателей степени.

7. ***Законы исключения констант***:

- для логического сложения: ***A □ 1 = 1, A □ 0 = A***;
- для логического умножения: ***A & 1 = A, A & 0 = 0***.

8. ***Закон противоречия***:

- $A \,\&\, \overline{A} = 0$.

Невозможно, чтобы противоречащие высказывания были одновременно истинными.

9. ***Закон исключения третьего***:

- $A \,\square\, \overline{A} = 1$.

Из двух противоречащих высказываний об одном и том же предмете одно всегда истинно, а второе — ложно, третьего не дано.

10. ***Закон поглощения:***

- для логического сложения: ***A*** □ ***(A & B)*** = ***A***;
- для логического умножения: ***A & (A*** □ ***B) = A***.

Знание законов логики позволяет проверять правильность рассуждений и доказательств. Основываясь на законах, можно выполнять упрощение сложных логических выражений. Такой процесс замены сложной логической функции более простой, но равносильной ей, называется минимизацией функции.

Некоторые преобразования логических формул похожи на преобразования формул в обычной алгебре (вынесение общего множителя за скобки, использование переместительного и сочетательного законов и т.п.), другие - основаны на свойствах, которыми не обладают операции обычной алгебры (использование распределительного закона для конъюнкции, законов поглощения, склеивания, де Моргана и др.).

Нарушения законов логики приводят к логическим ошибкам и вытекающим из них противоречиям.

Упрощение формул

Задание 1. Упростить выражения $\overline{AB}+\overline{B}$, $\overline{\overline{B}C+C}$, $\overline{\overline{A}C}+B\overline{C}$ так, чтобы в полученных формулах не содержалось отрицания сложных высказываний.

Решение:

$$X=\overline{AB}+\overline{B}=\overline{A}+\overline{B}+\overline{B}=\overline{A}+\overline{B};$$

$$Y=\overline{\overline{B}C+C}=\left(B+\overline{C}\right)\overline{C}=\overline{C};$$

$$\overline{\overline{A}C}+B\overline{C}=A+\overline{C}+B\overline{C}=A+\overline{C}.$$

Рассмотрим несколько задач, которые решаются построением таблиц истинности сложных высказываний.

Задание2. Составить таблицу истинности высказывания $\overline{A\wedge\overline{B}\vee\overline{A}}$

Решение.

Данное высказывание состоит из двух операндов А и В. Для его вычисления необходимо сначала вычислить отрицание А, то есть $\bar{A}$, затем $\overline{B}$, далее выполнить логическое умножение $A\wedge\overline{B}$, затем сложение $A\wedge\overline{B}\vee\overline{A}$ и, наконец, отрицание $\overline{A\wedge\overline{B}\vee\overline{A}}$. Таким образом, в таблице истинности будет 7 столбцов и 5 строк.

A	B	$\bar{A}$	$\overline{B}$	$A\wedge\overline{B}$	$A\wedge\overline{B}\vee\overline{A}$	$\overline{A\wedge\overline{B}\vee\overline{A}}$

Заполняем ячейки, соответствующие значению всем возможным сочетаниям значений высказываний А и В.

A	B	$\bar{A}$	$\overline{B}$	$A\wedge\overline{B}$	$A\wedge\overline{B}\vee\overline{A}$	$\overline{A\wedge\overline{B}\vee\overline{A}}$
0	0					
0	1					
1	0					
1	1					

Далее заполняем третий и четвертый столбцы таблицы, соответственно, отрицая высказывания А и В.

A	B	$\bar{A}$	$\bar{B}$	$A \wedge \bar{B}$	$A \wedge \bar{B} \vee \bar{A}$	$\overline{A \wedge \bar{B} \vee \bar{A}}$
0	0	1	1			
0	1	1	0			
1	0	0	1			
1	1	0	0			

При заполнении пятого столбца таблицы будьте внимательны. Операндами высказывания являются А и $\bar{B}$, значит, при заполнении пятого столбца смотреть нужно на первый и четвертый столбцы таблицы. Помните, что результат логического умножения имеет значение истина только в том случае, когда истинны оба операнда (единица будет только в четвертой строке пятого столбца).

A	B	$\bar{A}$	$\bar{B}$	$A \wedge \bar{B}$	$A \wedge \bar{B} \vee \bar{A}$	$\overline{A \wedge \bar{B} \vee \bar{A}}$
0	0	1	1	0		
0	1	1	0	0		
1	0	0	1	1		
1	1	0	0	0		

При заполнении шестого столбца таблицы, следует обратить внимание на значения, стоящие в третьем и пятом столбцах, и выполнить операцию логического сложения.

A	B	$\bar{A}$	$\bar{B}$	$A \wedge \bar{B}$	$A \wedge \bar{B} \vee \bar{A}$	$\overline{A \wedge \bar{B} \vee \bar{A}}$
0	0	1	1	0	1	
0	1	1	0	0	1	
1	0	0	1	1	1	
1	1	0	0	0	0	

Для получения результата осталось заполнить последний столбец, где отрицается высказывание, полученное в шестом столбце.

A	B	$\bar{A}$	$\bar{B}$	$A \wedge \bar{B}$	$A \wedge \bar{B} \vee \bar{A}$	$\overline{A \wedge \bar{B} \vee \bar{A}}$
0	0	1	1	0	1	0
0	1	1	0	0	1	0
1	0	0	1	1	1	0
1	1	0	0	0	0	1

Ответ: Таблица истинности сложного высказывания следующая.

A	B	$\overline{A \wedge \bar{B} \vee \bar{A}}$
0	0	0
0	1	0
1	0	0
1	1	1

Задание 3.

Установить эквивалентность двух высказываний:

1) A V B Λ C;
2) (A V B) Λ (A V C).

Решение.

Для установления эквивалентности двух высказываний достаточно сравнить их таблицы истинности. Если таблицы совпадают, то высказывания эквивалентны.

Построим таблицу истинности первого высказывания. В выражении участвуют три высказывания. Для того чтобы рассмотреть все возможные сочетания их значений, будем использовать следующий прием: первые три столбца таблицы заполним двоичным представлением чисел 0, 1, 2, 3,..., 2^3-1, дополняя слева нужное количество нулей. Выражение не содержит скобок, следовательно, воспользуемся тем, что конъюнкция выполняется раньше, чем дизъюнкция. Получим следующую таблицу.

A	B	C	B Λ C	A V B Λ C
0	0	0	0	0

0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Аналогичным образом составим таблицу истинности второго высказывания.

A	B	C	A V B	A V C	(A V B) Λ (A V C)
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	1	1	1
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	1	1

Поскольку таблицы истинности совпадают, то высказывания 1 и 2 эквивалентны.

Ответ: высказывания эквивалентны

Задание 4. Докажите тавтологию *(X Λ Y) -› (X VY)*

Решение.

Для доказательства тавтологии построим следующую таблицу истинности.

X	Y	X Λ Y	X V Y	(X Λ Y) -› (X VY)
0	0	0	0	1
0	1	0	1	1
1	0	0	1	1
1	1	1	1	1

Ответ: тавтология доказана.

Основные законы логики: $A = A$ – закон тождества

$A \& \overline{A} = 0$ – закон непротиворечия

$A \vee \overline{A} = 1$ – закон исключенного третьего

$\overline{\overline{A}} = A$ – закон двойного отрицания

Свойства констант: $\overline{0} = 1$ $\overline{1} = 0$

$A \vee 0 = A$ $A \& 0 = 0$

$A \vee 1 = 1$ $A \& 1 = 1$

Законы идемпотентности: $A \vee A = A$

$A \& A = A$

Законы коммутативности: $A \vee B = B \vee A$

$A \& B = B \& A$

Законы ассоциативности: $A \vee (B \vee C) = (A \vee B) \vee C$

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

Законы дистрибутивности: $A \vee (B \& C) = (A \vee B) \& (A \vee C)$

$A \& (B \vee C) = (A \& B) \vee (A \& C)$

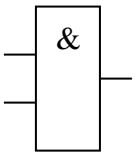
Законы поглощения: $A \vee (A \& B) = A$

$A \& (A \vee B) = A$

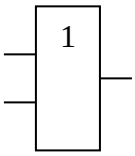
Законы де Моргана: $\overline{A \vee B} = \overline{A} \& \overline{B}$

$\overline{A \& B} = \overline{A} \vee \overline{B}$

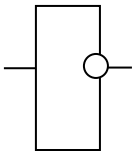
Базовые логические элементы компьютера



Логический элемент **И**
конъюнктор



Логический элемент **ИЛИ**
дизъюнктор



Логический элемент **НЕ**
инвертор

Задания

1. Установите, какие из следующих предложений являются логическими высказываниями, а какие — нет (объясните почему):
   - "Солнце есть спутник Земли";
   - "2+3?4";
   - "сегодня отличная погода";
   - "в романе Л.Н. Толстого "Война и мир" 3 432 536 слов";
   - "Санкт-Петербург расположен на Неве";
   - "музыка Баха слишком сложна";
   - "первая космическая скорость равна 7.8 км/сек";
   - "железо — металл";
   - "если один угол в треугольнике прямой, то треугольник будет тупоугольным";
     "если сумма квадратов двух сторон треугольника равна квадрату третьей, то он прямоугольный".
2. Укажите, какие из высказываний предыдущего задания истинны, какие — ложны, а какие относятся к числу тех, истинность которых трудно или невозможно установить.
3. Составьте таблицы истинности логических выражений:
   - ***A □ (¬B □ C)*** .
   - ***¬ (A □ B) □ (A □ ¬ B)*** .
   - ***(A □ B) □ (C □ B)*** .
4. Записать заданные формулы в виде предложений:

$(A \to B) \vee (C \wedge \overline{B})$;

$(A \to \overline{B}) \leftrightarrow (C \wedge B)$;

$\overline{B} \vee (C \to (B \wedge A))$;

$(A \to B) \vee \overline{(C \wedge B)}$;

$(A \to B) \leftrightarrow (C \vee \overline{B})$;

Если:
A - студент сидит на паре
B - завтра экзамен
C - осенью хорошая погода

5. Составить таблицу истинности для логических функций:

$$((X \wedge Z) \leftrightarrow (\overline{X} \vee \overline{Z})) \rightarrow \overline{(X \leftrightarrow (Y \rightarrow Z))};$$

$$((Y \vee \overline{Z}) \wedge (Y \rightarrow \overline{X}) \wedge (\overline{Y} \leftrightarrow X)) \rightarrow Y;$$

$$\overline{(\overline{Z} \vee (X \leftrightarrow \overline{Y}) \vee (X \rightarrow Y))} \wedge (Y \rightarrow \overline{Z});$$

$$\overline{\overline{X} \vee ((X \leftrightarrow ((Y \rightarrow Z) \wedge (Z \rightarrow \overline{Y}))) \leftrightarrow Y)}.$$

6. Упростить выражения и построить логические схемы для полученных логических функций:

$$((X \leftrightarrow Y) \rightarrow (X \vee Y)) \wedge \overline{X}$$

$$((X \rightarrow Y) \wedge (Y \rightarrow \overline{X})) \rightarrow Y$$

$$(X \rightarrow \overline{Y}) \wedge (\overline{X} \rightarrow (Y \wedge \overline{X}))$$

$$\overline{X} \wedge ((\overline{Y} \rightarrow X) \wedge (X \rightarrow Y))$$

$$(Y \leftrightarrow X) \wedge (X \rightarrow (X \wedge Y))$$

7. Упростить логические выражения, используя законы преобразования логических выражений

1. $((\overline{X} \leftrightarrow Y) \vee Z) \wedge \overline{Y}$;
2. $\overline{((\overline{\overline{X} \wedge Y}) \rightarrow Y)} \rightarrow (X \wedge \overline{Z})$;
3. $\overline{((\overline{X \wedge Y}) \rightarrow Y)} \rightarrow (\overline{X} \wedge Z)$;
4. $(X \wedge Z) \vee (\overline{Y} \leftrightarrow Z)$;
5. $(X \leftrightarrow Y) \wedge (\overline{X} \vee Z)$;
6. $(Z \wedge Y) \vee ((Z \rightarrow \overline{Y}) \wedge \overline{X})$;
7. $((Z \rightarrow Y) \vee \overline{X}) \rightarrow \overline{X}$;
8. $(\overline{Y} \wedge X) \vee (Z \leftrightarrow Y)$;
9. $\overline{X} \wedge \overline{(Y \leftrightarrow Z)}$;
10. $Y \rightarrow (\overline{X} \leftrightarrow Z)$;
11. $\overline{(X \wedge \overline{Y}) \vee (\overline{Z} \rightarrow Y)}$;
12. $(\overline{Y} \wedge \overline{Z}) \vee (X \rightarrow \overline{Z})$;
13. $(Y \leftrightarrow X) \rightarrow (Y \wedge \overline{Z})$;
14. $(X \leftrightarrow Y) \rightarrow (\overline{X} \vee Z)$;
15. $((\overline{Z} \leftrightarrow Y) \vee \overline{X}) \wedge \overline{Y}$;
16. $((\overline{X} \rightarrow Z) \rightarrow Y) \rightarrow X$;
17. $((X \leftrightarrow \overline{Y}) \vee Z) \wedge Y$;
18. $((X \rightarrow Y) \rightarrow Z) \rightarrow \overline{X}$;
19. $(X \leftrightarrow Z) \rightarrow (X \wedge \overline{Y})$;
20. $(\overline{X} \wedge Z) \vee (Y \rightarrow Z)$;
21. $\overline{(X \wedge Y)} \vee \overline{(Z \rightarrow Y)}$;
22. $X \rightarrow (Y \leftrightarrow Z)$;
23. $\overline{X \vee (Y \leftrightarrow \overline{Z})}$;
24. $(X \leftrightarrow Y) \vee (\overline{Y} \wedge Z)$;
25. $(X \vee (Y \rightarrow Z)) \rightarrow X$;
26. $(X \wedge Y) \vee ((X \rightarrow \overline{Y}) \wedge \overline{Z})$;
27. $(X \leftrightarrow Y) \wedge (\overline{Y} \vee Z)$;
28. $(X \wedge Y) \vee (Y \leftrightarrow Z)$;
29. $((X \leftrightarrow \overline{Y}) \vee Z) \wedge Y$;
30. $(X \leftrightarrow Y) \rightarrow (\overline{X} \vee Z)$.

Контрольные вопросы

1. Что такое высказывание?
2. Какие бывают высказывания?
3. Что называют функцией в алгебре логики?
4. Что такое логическая функция?
5. Как построить таблицу истинности по заданной логической функции?
6. Как построить логическую функцию по заданной таблице истинности?
7. Что такое таблица истинности?
8. Какую формулу называют тождественно-истинной (тождественно-ложной)?
9. Какую формулу называют выполнимой (опровержимой)?

Практическая работа №4
«Виды графов. Графы числовых множеств, характеристики графов»

Цель: формирование навыков выполнения операций над векторами и вычисления модуля и скалярного произведения векторов.

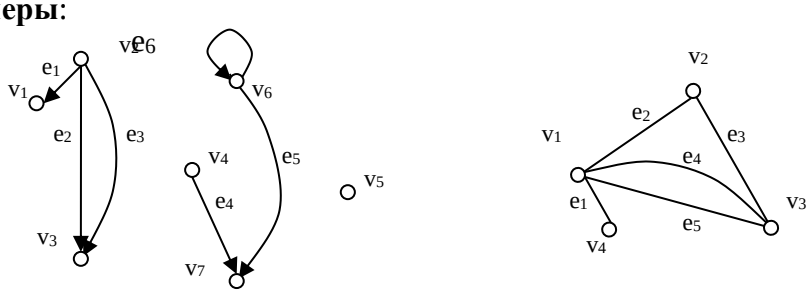
Теоретические сведения

Граф G – это совокупность двух множеств: непустого множества вершин $V = \{v_1, v_2, ..., v_n\}$ и множества ребер (дуг) $E = \{e_1, e_2, ..., e_n\}$. Таким образом, $G = (V, E)$, $V \neq \varnothing$, $E \subset V \times V$.

Если (v_1, v_2) – упорядоченная пара (т. е. дуга), то v_1 называется началом, а v_2 – концом дуги e. Если $\{v_1, v_2\}$ – неупорядоченная пара, то ребро e называется неориентированным. Всякому графу G можно поставить в соответствие соотнесенный неориентированный граф G с теми же множествами V и E и инцидентностями, но все пары неупорядоченные. Такой граф называется ассоциированным. Вершина, не инцидентная ни одному ребру, называется изолированной. Вершина, инцидентная ровно одному ребру, и само это ребро называются концевыми или висячими. Ребро с совпадающими концами называется петлей. Две вершины, инцидентные одному и тому же ребру, называются смежными. Два ребра, инцидентные одной и той же вершине, называются смежными. Ребра, которым поставлена в соответствие одна и та же пара вершин, называются кратными или параллельными.

Граф, содержащий кратные ребра, называется **мультиграфом**. Неориентированное ребро графа эквивалентно двум противоположно направленным дугам, соединяющим те же самые вершины. Граф с кратными ребрами и петлями называется **псевдографом**.

Примеры:



а) ориентированный граф б) неориентированный граф

Рис. 1

На рис. 1 изображены: ориентированный псевдограф, имеющий 7 вершин и 6 дуг, и неориентированный мультиграф, имеющий 4 вершины и 5 ребер. Проиллюстрируем некоторые введенные понятия.

Для орграфа (рис. 1*а*): v_1, v_2, v_3, v_4, v_5, v_6 , v_7 – вершины (узлы); v_5 – изолированная вершина; v_1, v_4 – концевые (висячие) вершины; v_2 и v_3, v_2 и v_1 – пары соседних вершин; e_1, e_2, e_3, e_4, e_5, e_6 – ориентированные ребра (дуги); e_2 и e_3 – параллельные (кратные) дуги; e_2 и e_1 – смежные дуги; e_6 –петля для орграфа.

Для графа (рис. 1*б*): v_1, v_2, v_3, v_4 – вершины; v_4 – концевая (висячая) вершина; v_2 и v_3, v_2 и v_1 – пары соседних вершин; e_1, e_2, e_3, e_4, e_5 – ребра (дуги); e_4 и e_5 – параллельные (кратные) ребра; e_2 и e_3 – смежные ребра; петель нет.

Способы задания графов

1. Перечисление (список) ребер графа с указанием их концов и добавлением списка изолированных вершин.

2. Матрица смежности $A = (a_{ij})$ определяется одинаково для ориентированного и неориентированного графов. Это квадратная матрица порядка n, где n – число вершин, у которой

$$a_{ij} = \begin{cases} 1, если\ (v_i, v_j) \in E, \\ 0, если\ (v_i, e_j) \notin E. \end{cases}$$

Матрицей инцидентности $B = (b_{ij})$ ориентированного графа называется матрица ($n \times m$), где n – число вершин, m – число ребер, у которой

$$b_{ij} = \begin{cases} 1, \text{если вершина } v_i \text{ является концом дуги } e_j; \\ -1, \text{если вершина } v_i \text{ является началом дуги } e_j; \\ 0, \text{если вершина } v_i \text{ не инцидентна дуге } e_j. \end{cases}$$

Для неориентированного графа матрица инцидентности B задается следующим образом:

$$b_{ij} = \begin{cases} 1, \text{если вершина } v_i \text{ инцидентна ребру } e_j; \\ 0, \text{если вершина } v_i \text{ не инцидентна ребру } e_j. \end{cases}$$

Петле соответствует элемент, равный 2.

Пример.

Матрицы смежности и инцидентности графа, изображенного на рис. 1*а*, имеют вид (рис. 2):

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Рис. 2

3. Для наглядности граф представляют в виде геометрического объекта: вершинам соответствуют различные выделенные точки в пространстве (на плоскости), ребрам – отрезки кривых, связывающие вершины.

Рассмотрим некоторые разновидности графов.

Неориентированный граф $G = (V, E)$ – **двудольный,** если множество его вершин V можно разбить на два такие подмножества V_1 и V_2, что каждое ребро имеет один конец в V_1, а другой в V_2. Если же каждая из вершин класса V_1 связана ребром с каждой вершиной класса V_2, то граф называется полным двудольным и обозначается $K_{m,n}$, где $m = |V_1|$, $n = |V_2|$. На рис. 3*а* изображен двудольный граф, на рис. 3*б* и 3*в* – полные двудольные графы $K_{3,2}$ и $K_{3,3}$.

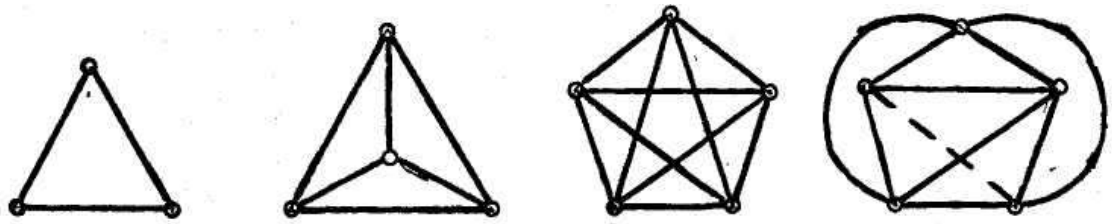
Пример.

а б в

Рис. 3

Полным графом называется граф без кратных ребер (и иногда без петель), в котором любые две вершины соединены ребром (ориентированным или неориентированным). Полный неориентированный граф с n вершинами обозначается K_n. Очевидно, граф K_n содержит $n(n - 1)/2$ ребер.

На рис. 4*а*, 4*б* и 4*в* изображены графы K_3, K_4, K_5, соответственно. На рис. 4*г* также изображен полный граф.



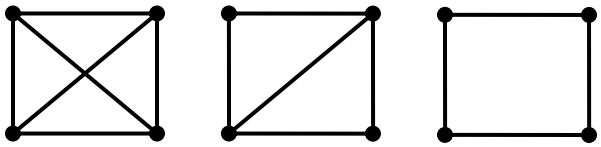
а б в г

Рис. 4

Подграфы

Граф $G' = (V', E')$ называется подграфом графа $G = (V, E)$, обозначение: $G' \subseteq G$, если $V' \subseteq V$, $E' \subseteq E$ и для множеств V' и E' сохраняются инциденции графа G. При этом, очевидно, каждое ребро из E' входит в подграф G' вместе со своими концами. Подграф называется **собственным**, если он отличен от самого графа.

Пример. Графы на рис. 5*б* и 5*в* являются подграфами графа на рис. 5*а*.



а б в

Рис. 5

Изоморфизм графов

Два графа $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ изоморфны, если между их вершинами существует взаимно однозначное соответствие φ: $V_1 \to V_2$ такое, что для любой пары вершин u, v из V_1 ребро $(u, v) \in E_1 \leftrightarrow$ ребро $(\varphi(u), \varphi(v)) \in E_2$.

Пример. Графы, изображенные на рис. 6, являются изоморфными.

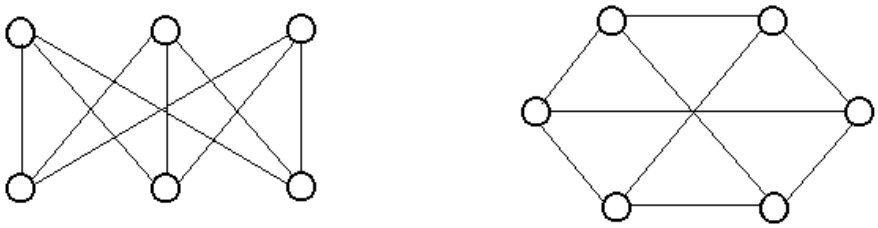


Рис. 6

Изоморфные графы отличаются только нумерацией вершин. Матрицы смежности двух изоморфных графов могут быть получены одна из другой перестановкой строк и столбцов. Чтобы узнать, являются ли два графа изоморфными, нужно произвести все возможные перестановки строк и столбцов матрицы смежности одного из графов. Если после какой-нибудь перестановки получится матрица смежности второго графа, то эти графы изоморфны. Чтобы убедиться, что графы неизоморфны, надо выполнить все $n!$ возможных перестановок строк и столбцов.

Степени вершин графа

Степенью вершины v графа G называется число $\delta(v)$ ребер графа G, инцидентных вершине v. Вершина графа, имеющая степень 0, называется **изолированной,** а степень 1 – **висячей**.

В случае неориентированного псевдографа считается, что вклад каждой петли, инцидентной некоторой вершине v, в $\delta(v)$ равен 2 (тогда как вклад любого другого ребра, инцидентного вершине v, равен 1).

Полустепенью исхода (захода) вершины v орграфа D называется число $\delta^+(v)$ ($\delta^-(v)$) дуг орграфа D, исходящих из вершины v (входящих в вершину v).

В случае ориентированного псевдографа вклад каждой петли, инцидентной некоторой вершине v, в $\delta(v)$ равен 1, как в $\delta^+(v)$, так и в $\delta^-(v)$.

Пример.

В графе G (рис. 1*б*) степень вершины v_1 равна четырем, т. е. $\delta(v_1) = 4$; вершина v_4 – висячая, так как $\delta(v_4) = 1$. В ориентированном псевдографе (рис. 1*а*) степень вершины v_6 равна трем, т. е. $\delta(v_6) = \delta^+(v_6) + (\delta^-(v_6) = 2 + 1 = 3$; вершина v_1 – висячая, так как $\delta(v_1) = 1$, вершина v_5 – изолированная, так как $\delta(v_5) = 0$.

Задания

1. Даны реализации графов (рис. 7). Какие это графы? Описать их основные характеристики. Привести примеры элементов графов.

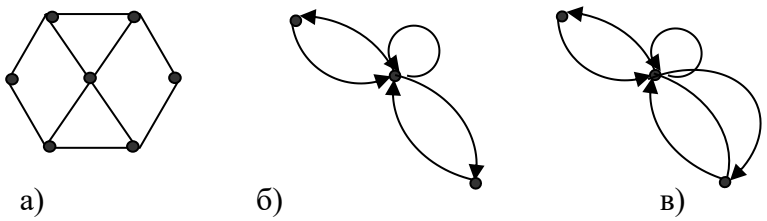


Рис. 7

2. Записать матрицы смежности и инцидентности для неориентированного графа (рис. 7*а*).

3. Записать матрицы смежности и инцидентности для ориентированного графа (рис. 7*б*).

4. Изобразить ассоциированный граф для заданного графа (рис. 7*б*).

5. Изобразить все попарно неизоморфные 4-вершинные графы без петель и кратных ребер. Записать для них матрицы смежности и инцидентности.

6. Построить все попарно неизоморфные 5-вершинные графы, не имеющие петель, кратных ребер и изолированных вершин.

7. Какое из двух утверждений верно: а) ориентированный граф является частным случаем неориентированного графа; б) неориентированный граф является частным случаем ориентированного графа.

8. Перечислить все возможные способы задания графов.

9. Всегда ли матрица смежности симметрична относительно главной диагонали?

10. Как по матрице смежности определить число ребер неориентированного графа?

11. Как по матрице инцидентности, не рисуя граф, определить его матрицу смежности?

12. Может ли матрица $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ быть матрицей смежности неориентированного графа?

13. Какие из следующих утверждений являются правильными: а) если матрица смежности несимметричная, то граф ориентированный; б) если граф неориентированный, то матрица смежности симметричная; в) если диагональные элементы матрицы смежности – нули, то граф неориентированный?

14. Записать матрицы смежности и инцидентности для ориентированного графа (рис. 7*в*).

15. Изобразить все попарно неизоморфные ориентированные псевдографы, содержащие: а) 2 вершины и 2 дуги; б) 3 вершины и 4 дуги; в) 4 вершины и 3 дуги.

16. Изобразить ассоциированный граф для заданного графа (рис. 7*в*).

17. Чему равны степени вершин для ориентированного и неориентированного графов?

18. Определить степени вершин орграфа (рис. 1*а*). Есть ли в заданном графе изолированные и висячие вершины?

19. Определить степени вершин в заданных графах (рис. 7).

20. Даны реализации графов (рис. 7). Какие это графы? Привести примеры смежных вершин и смежных ребер.

Контрольные вопросы

1. Что называется графом? Ориентированным графом? Приведите примеры.
2. Перечислите и сформулируйте основные понятия, связанные с неориентированными графами.
3. Перечислите основные понятия, связанные с орграфами.
4. Какие два графа называются изоморфными?
5. Что называется маршрутом, циклом, путем и цепью графа?
6. Сформулируйте понятие связности графа.
7. Дайте определение эйлерова графа.
8. Какой граф называют гамильтоновым?
9. Дайте понятие дерева и перечислите его свойства.
10. Перечислите операции над графами.
11. Перечислите способы задания графов.
12. В чем состоит аналитический способ задания графа?
13. В чем состоит геометрический способ задания графа?
14. В чем состоит матричный способ задания графа?
15. Какая матрица называется матрицей смежности графа?
16. Какая матрица называется матрицей инцидентности графа?

Практическая работа №5
«Полная и приведенная системы вычетов. Выбор модуля для контроля. Кодирование информации»

Цель: формирование вычислительных навыков работы с вычетами и кодированием информации.

Теоретические сведения

Будем рассматривать целые числа в связи с остатками от деления на натуральное число m, называемое *модулем*.

$$a \equiv b(mod\ m) \qquad (1)$$

где $a = b + km$ для некоторого целого k.

Иногда b называют вычетом a по модулю m, a – конгруэнтным b по модулю m.

Формулу (1) также можно интерпретировать следующим образом: если два числа имеют одинаковые остатки от деления на m, то они сравнимы по модулю m (например, $8 \equiv 5(\mathrm{mod}\,3)$).

В отличие от (1) операция $c\ mod\ t$ означает остаток от деления $\frac{c}{t} \in [0, m-1]$ (например, $5 \mathrm{mod} 3 = 2$). Эта операция называется приведением по модулю.

Далее приведены свойства функции сравнения:

1. Сравнения по одинаковому модулю можно почленно складывать: $a_1 \equiv b_1(\mathrm{mod}\,m), a_2 \equiv b_2(\mathrm{mod}\,m) \Rightarrow a_1 + a_2 \equiv (b_1 + b_2)(\mathrm{mod}\,m)$.
2. Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, изменив его знак на обратный: $a + b \equiv c(\mathrm{mod}\,m) \Rightarrow a \equiv (c - b)(\mathrm{mod}\,m)$.
3. К любой части сравнения можно прибавить любое число, кратное модулю: $a \equiv b(\mathrm{mod}\,m) \Rightarrow a + mk \equiv b(\mathrm{mod}\,m)$.

4. Сравнения по одинаковому модулю можно почленно перемножать: $a_1 \equiv b_1 (\bmod m), a_2 \equiv b_2 (\bmod m) \Rightarrow a_1 a_2 \equiv (b_1 b_2)(\bmod m)$.

5. Обе части сравнения можно возвести в одну и ту же степень.

6. Как следствие из вышеперечисленных свойств, получаем: $a_0 \equiv b_0 (\bmod m)$, $a_1 \equiv b_1 (\bmod m), \ldots, a_n \equiv b_n (\bmod m)$,

$$x \equiv y (\bmod m) \Rightarrow \; a_0 x^n + a_1 x^{n-1} + \ldots + a_n = (b_0 y^n + b_1 y^{n-1} + \ldots + b_n)(\bmod m)$$

7. Обе части сравнения можно разделить на их общий делитель, взаимно простой с модулем.

8. Обе части сравнения и его модуль можно умножить на одно и то же целое число или разделить на их общий делитель.

9. Если сравнение $a \equiv b$ имеет место по нескольким разным модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.

10. Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.

11. Если одна часть сравнения и модуль делятся на некоторое число, то и другая часть сравнения должна делиться на то же число.

12. К обеим частям сравнения можно прибавить одно и тоже число; обе части сравнения можно умножить на одно и тоже число.

Свойство операции приведения по модулю:

$(a \Diamond b) \; mod \; m \; = \; [(a \; mod \; m) \Diamond (b \; mod \; m)] \; mod \; m$, где $\Diamond \; = \; \{+, -, *\}$.

Пример 1.

Проверим *7*-ое свойство функции сравнения: $24 \equiv 6 (\bmod 9)$, общие делители *24* и *6* – *2,3.* Взаимно простое с *9* – это *2*: $НОД(2,9) = 1$. Тогда делим на *2* обе части сравнения: $12 \equiv 3 (\bmod 9)$, иначе было бы неверно: $8 \overline{\equiv} 2 (\bmod 9)$.

Пример 2.

Проверим свойство операции приведения:

$$(24-5) \bmod 9 = \{19 \bmod 9 = 1\} = ((24 \bmod 9) - (5 \bmod 9)) \bmod 9 = (6-5) \bmod 9 = 1 \bmod 9$$

Найдем $a^8 \; mod \; n$ при помощи свойства операции приведения по модулю:

$$a^8 \; mod \; n \; = \; (a^4 \; mod \; n \cdot a^4 \; mod \; n) \; mod \; n \; =$$

$$= \; [(a^2 \; mod \; n \cdot a^2 \; mod \; n) \; mod \; n \cdot (a^2 \; mod \; n \cdot a^2 \; mod \; n) \; mod \; n] \; mod \; n \; =$$

$$= \; [(a^2 \; mod \; n)^2 \; mod \; n]^2 \; mod \; n$$

Такой прием называется цепочкой разложения, в основе которой лежит двоичное представление числа.

Числа, сравнимые по модулю m, образуют класс вычетов по модулю m. Все числа из одного и того же класса имеют один и тот же остаток r от деления на m. Любое число a из класса вычетов называется вычетом по модулю m.

Всего имеется m классов вычетов по модулю m (если классы обозначать как $\bar{a}$): $\bar{0}, \bar{1}, \ldots, \overline{m-1}$.

Свойства классов вычетов:

1. $a \equiv b (\bmod m) \Leftrightarrow \bar{a} = \bar{b}$.

2. $a \overline{\equiv} b (\bmod m) \Leftrightarrow \bar{a} \cap \bar{b} = \varnothing$.

3. Любые m чисел попарно не сравнимые по модулю m образуют полную систему вычетов.

4. Если $НОД(a, m) = 1$ и x «пробегает» полную систему вычетов по модулю m, то $ax + b$, где b – любое число, также пробегает полную систему вычетов по модулю m.

Полная система вычетов – это совокупность вычетов, взятых по одному из каждого класса эквивалентности.

Приведенная система вычетов по модулю m – это совокупность всех вычетов из полной системы, взаимно простых с модулем m.

Пример 3.

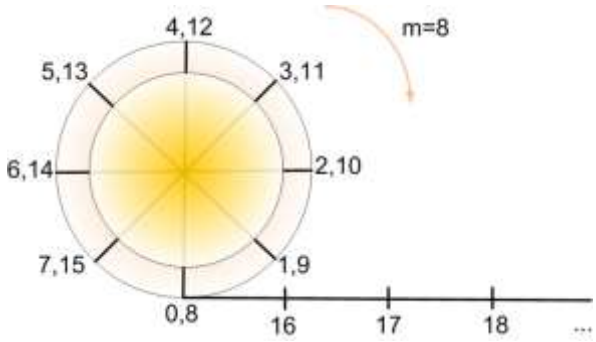


Рис. 1. Иллюстрация к образованию классов вычетов по модулю *8*

На рис. 1 изображен процесс «наматывания» цепочки целых чисел на колечко с $m = 8$ делениями, при этом на одно деление автоматически попадают сравнимые между собой числа.

Существуют *8* классов вычетов по модулю $m = 8$. В каждом классе находятся числа, дающие при делении на m одинаковые остатки:

Члены класса	0,8,16, …	1,9,17, …	2,10,15, …	3,11,19, …	4,12,20, …	5,13,21, …	6,14,22, …	7,15,23, …
Название класса	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$

Например, одна из полных систем вычетов по модулю 8: 1200, 33, 42, 3, 12, 629, 22, 807.

Приведенная система вычетов: 0, 1, 3, 5, 7.

Количество классов вычетов в приведенной системе вычетов минус один обозначают как $\varphi(m)$ и называют функцией Эйлера (или представляет собой количество чисел ряда $1,2,...,m-1$ взаимно простых с m). Например, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$, $\varphi(8)=4$. Кроме того, $\varphi(1)=1$

Свойства функции Эйлера:

1. Если p – простое, то $\varphi(p)=p-1$.
2. Если p – простое, то $\varphi(p^k)=p^k-p^{k-1}$.
3. Мультипликативность функции Эйлера: если $НОД(a,b)=1 \Rightarrow \varphi(ab)=\varphi(a)\cdot\varphi(b)$.

Следствие из этого свойства: $\varphi(a)=a\prod_{t\ \text{делит}\ a}\left(1-\frac{1}{t}\right)$.

Пример 4.

Дано $a=15$. Найдем простые все числа $t<a$, на которые делится a без остатка: *3, 5*. Тогда $\varphi(15)=15\cdot\left[\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\right]=8$. Посчитаем для проверки количество классов в приведенной системе вычетов: *1, 2, 4, 7, 8, 11, 13, 14*. Оно равно *8*.

Теорема Эйлера. Пусть $m>1$, $НОД(a,m)=1$, $\varphi(m)$ – функция Эйлера. Тогда: $a^{\varphi(m)}\equiv 1(\bmod m)$.

Например, $m=6, a=11$, $\varphi(6)=2 \Rightarrow 11^2=121\equiv 1(\bmod 6)$.

Теорема Ферма (малая теорема Ферма или малая теорема Эйлера). Если $НОД(a,p)=1$, p – простое, то $a^{p-1}\equiv 1(\bmod p)$

Следствие из теоремы Ферма: $a^p \equiv a(\mathrm{mod}\ p)$, где *не обязательно* $НОД(a, p) = 1$, но p – простое.

Пример 5.

Девятая степень однозначного числа оканчивается цифрой 7. Найти это число.

$a^9 \equiv 7(\mathrm{mod}\,10)$. Понятно, что $НОД(7{,}10) = 1$, $НОД(a{,}10) = 1$, $\varphi(10) = 4$.

По теореме Эйлера: $a^4 \equiv 1(\mathrm{mod}\,10)$, возведем в квадрат обе части сравнения: $a^8 \equiv 1(\mathrm{mod}\,10)$. Почленно поделим $a^9 \equiv 7(\mathrm{mod}\,10)$ на $a^8 \equiv 1(\mathrm{mod}\,10)$: $a \equiv 7(\mathrm{mod}\,10) \Rightarrow a = 7$.

Пример 6.

Доказать, что $1^{18} + 2^{18} + ... + 6^{18} \equiv 6(\mathrm{mod}\,7)$.

$НОД(1{,}7) = 1, НОД(2{,}7) = 1, ..., НОД(6{,}7) = 1$. $p = 7$ – простое. По теореме Ферма: $a^{7-1} \equiv 1(\mathrm{mod}\,7)$, где $a = 1{,}2{,}...{,}6$. Получаем систем:

$1^6 \equiv 1(\mathrm{mod}\,7)$

$2^6 \equiv 1(\mathrm{mod}\,7)$

...

$6^6 \equiv 1(\mathrm{mod}\,7)$

Возводим каждое сравнение почленно в третью степень и складываем: $1^{18} + 2^{18} + ... + 6^{18} \equiv 6(\mathrm{mod}\,7)$.

Пример 7.

Найти остаток от деления 7^{402} на 101.

$p = 101$ – простое, $НОД(7{,}101) = 1 \Rightarrow$ по теореме Ферма $7^{100} \equiv 1(\mathrm{mod}\,101)$. Возведем данное сравнение в 4-ую степень и умножим на $7^2 \equiv 49(\mathrm{mod}\,101)$: $7^{402} \equiv 49(\mathrm{mod}\,101) \Rightarrow$ остаток равен 49.

Пример 8.

Найти две последние цифры числа 243^{402}.

Две последние цифры числа – это остаток от деления на *100*.

$243(\mathrm{mod}\,100) = (200 + 43)(\mathrm{mod}\,100) = 43(\mathrm{mod}\,100)$, значит:

$243^{402}(\mathrm{mod}\,100) = 43^{402}(\mathrm{mod}\,100)$. Так как $НОД(43{,}100) = 1$, по теореме Эйлера $43^{\varphi(100)} \equiv 1(\mathrm{mod}\,100)$. $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2)$, *2* и *5* простые числа, значит: $\varphi(100) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 40$. Тогда: $43^{40} \equiv 1(\mathrm{mod}\,100)$; возведем в *100* степень и умножим на $43^2 \equiv 49(\mathrm{mod}\,100)$: $43^{402} \equiv 49(\mathrm{mod}\,100)$.

Значит, последние две цифры *4* и *9*.

Пример 9.

Показать, что $73^{12} - 1$ делится на *105*.

Решение.

$105 = 3 \cdot 5 \cdot 7$, $НОД(73{,}3) = НОД(73{,}5) = НОД(73{,}7) = 1$. По теореме Ферма:

$73^2 \equiv 1(\mathrm{mod}\,3) \overset{10\,св-во}{=} 1(\mathrm{mod}\,105)$

$73^4 \equiv 1(\mathrm{mod}\,5) \overset{10\,св-во}{=} 1(\mathrm{mod}\,105)$.

$73^6 \equiv 1(\mathrm{mod}\,7) \overset{10\,св-во}{=} 1(\mathrm{mod}\,105)$

Умножим эти сравнения и вычтем $1 \equiv 1(\mathrm{mod}\,105)$: $73^{12} - 1 \equiv 1 - 1(\mathrm{mod}\,105) = 0(\mathrm{mod}\,105)$.

Пример 10.

Найти вычет числа $2^{5432675}$ по $\mathrm{mod}13$.

Разделим степень на $p-1=13-1$ с остатком $k=q(p-1)+r=452722\cdot 12+11$; $a^k(\mathrm{mod}\ p)=a^{q(p-1)+r}(\mathrm{mod}\ p)=\left(a^{p-1}\right)^q a^r(\mathrm{mod}\ p)=\left(a^{p-1}\right)^q(\mathrm{mod}\ p)\cdot a^r(\mathrm{mod}\ p)$. По теореме Ферма (так как p – простое): $a^{p-1}\equiv 1(\mathrm{mod}\ p)$.

Тогда $a^k(\mathrm{mod}\ p)=a^{q(p-1)+r}(\mathrm{mod}\ p)=\left(a^{p-1}\right)^q a^r(\mathrm{mod}\ p)$. Значит, $2^{5432675}(\mathrm{mod}13)\equiv 2^{11}(\mathrm{mod}13)=7(\mathrm{mod}13)$.

Рассмотрим сравнение:

$ax\equiv b(\mathrm{mod}\ m)$ (2)

Под решением любого сравнения понимается класс вычетов по модулю m, один элемент которого (а значит и все) удовлетворяют данному сравнению. Решить сравнение – значит найти все x, которые удовлетворяют данному сравнению, при этом весь класс вычетов по модулю m считается за одно решение.

Пример 11.

Сравнение 5-ой степени: $x^5+x+1\equiv 0(\mathrm{mod}\ 7)$.

Класс вычетов для $m=7:\overline{0,6}$. Данному сравнению удовлетворяют: $x_1=2, x_2=4$, так как $35\equiv 0(\mathrm{mod}\ 7)$ и $1029\equiv 0(\mathrm{mod}\ 7)$. Таким образом у данного сравнения есть два решения: $35\equiv 0(\mathrm{mod}\ 7)$ и $x_2\equiv 4(\mathrm{mod}\ 7)$.

Естественно, метод перебора затруднителен. В случае сравнения первой степени если $НОД(\mathrm{a,m})=1$ решение означает отыскание целых u,v таких, что: $au+mv=1$, то есть $au\equiv 1(\mathrm{mod}\ m)$. u – это обратный к a по модулю m элемент.

Умножим (2) на u: $aux\overset{12св-во}{\equiv}bu(\mathrm{mod}\ m)$. С учетом $au\equiv 1(\mathrm{mod}\ m)$ получаем:.

$x\equiv bu(\mathrm{mod}\ m)$ (3)

Значит, сравнение первой степени имеет одно решение по модулю m.

Если же $НОД(\mathrm{a,m})=d$, то для решения сравнения (2) необходимо, чтобы d делил b без остатка. При этом сравнение будет иметь d решений: $x_1, x_1+m,\ldots,x_1+(d-1)m$.

Пример 12.

Решить уравнение $111x=75(\mathrm{mod}\ 321)$.

$НОД(a,m)=НОД(111,321)=3$. Поэтому по свойству 11,7,8 функции сравнение: $37x=25(\mathrm{mod}\ 107)$. Далее для решения сравнения можно использовать два подхода:

1. Алгоритм Евклида (применяется при небольших m для нахождения u: $au\equiv 1(\mathrm{mod}\ m)$).
2. Способ Эйлера.

Рассмотрим алгоритм Евклида для нахождения наибольшего общего делителя $НОД(\mathrm{a,b})$.

Выполним следующие деления с остатком:

$a=bq_1+r_1, 0\le r_1<b$

$b=r_1q_2+r_2, 0\le r_2<r_1$

$r_1=r_2q_3+r_3, 0\le r_3<r_2$

....

$r_{n-2}=r_{n-1}q_n+r_n, 0\le r_n<r_{n-1}$

$n_{n-1}=r_nq_{n+1}$.

Тогда $НОД(\mathrm{a,b})=НОД(b,\mathrm{r}_1)=НОД(r_1,\mathrm{r}_2)=\ldots=r_n$. То есть $НОД(\mathrm{a,b})$ равен последнему отличному от нуля остатку в алгоритме Евклида.

Пример 13.

Найдем $НОД(1234,54)$.

Решение.

$1234 = 54 \cdot 22 + 46$

$54 = 46 \cdot 1 + 8$

$46 = 8 \cdot 5 + 6$

$8 = 6 \cdot 1 + 2$

$6 = 2 \cdot 3 + 0$

Значит, $НОД(1234,54) = 2$.

Если мы хотим найти линейное разложение НОД'а: $r_n = au + bv$, то надо остатки r_i выражать друг через друга:

$$r_n = 2 = 8 - 6 = 8 - (46 - 8 \cdot 5) = (54 - 46) - (46 - (54 - 46) \cdot 5) =$$
$$= (\underline{54} - [\overline{1234} - \underline{54} \cdot 22]) - ([\overline{1234} - \underline{54} \cdot 22] - (\underline{54} - [\overline{1234} - \underline{54} \cdot 22]) \cdot 5) =$$
$$= -7 \cdot 1234 + 160 \cdot 54 \bullet$$

Пример 14.

Решим уравнение $111x \equiv 75 (\mathrm{mod}\, 322)$.

$НОД(111,322) = 1$.

Найдем линейное разложение НОД'а: $au + mv = 1$:

$322 = 111 \cdot 2 + 100$

$111 = 100 \cdot 1 + 11$

$100 = 11 \cdot 9 + 1$

$11 = 1 \cdot 11$

$$r_n = 1 = 100 - 11 \cdot 9 = 100 - (111 - 100) \cdot 9 =$$
$$= [\overline{322} - \underline{111} \cdot 2] - (\underline{111} - [\overline{322} - \underline{111} \cdot 2]) \cdot 9 =$$
$$= 10 \cdot 322 - 29 \cdot 111$$

Значит, $v = 10, u = -29$. По формуле (3): $x \equiv 75 \cdot (-32) (\mathrm{mod}\, 322) = -2175 (\mathrm{mod}\, 322) = 79 (\mathrm{mod}\, 322)$. Проверим, действительно ли так: $111 \cdot 79 \mathrm{mod} 322 = 79$.

Пример 15.

Решим уравнение $111x \equiv 75 (\mathrm{mod}\, 321)$.

Решение.

$НОД(111,321) = 3$. Получаем: $37x = 25 (\mathrm{mod}\, 107)$. Найдем линейное разложение НОД'а: $au + mv = 1$:

$107 = 37 \cdot 2 + 33$

$37 = 33 \cdot 1 + 4$

$33 = 4 \cdot 8 + 1$

$4 = 4 \cdot 1$

$$r_n = 1 = 33 - 4 \cdot 8 = 33 - [37 - 33] \cdot 8 = (\overline{107} - \underline{37} \cdot 2) - [\underline{37} - (\overline{107} - \underline{37} \cdot 2)] \cdot 8 =$$
$$= 9 \cdot 107 - 26 \cdot 37$$

Значит, $u = -26, v = 9$.

Получается, что $x_1 \equiv -26 \cdot 25 (\mathrm{mod}\, 107) = 99 (\mathrm{mod}\, 107)$.

Исходное решение: $x_1 \equiv 99 (\mathrm{mod}\, 321), x_2 \equiv (99 + 107) (\mathrm{mod}\, 321) = 206 (\mathrm{mod}\, 321),$
$x_3 \equiv (99 + 2 \cdot 107) (\mathrm{mod}\, 321) = 313 (\mathrm{mod}\, 321)$

Теорема 1.

Пусть $m > 1$, $НОД(\mathrm{a,m}) = 1$. Тогда сравнение (2) имеет решение (3), где $u = a^{\varphi(m)-1}$.

Пример 16.

Решить сравнение $7x \equiv 3(\mathrm{mod}\,10)$.

$НОД(7,10)=1$, $\varphi(10)=4$.

Значит: $x = 3\cdot 7^3(\mathrm{mod}\,10) = 1029(\mathrm{mod}\,10) = 9(\mathrm{mod}\,10)$.

Отрицательным моментом этого метода является то, что необходимо возводить a в степень.

Число a, взаимно простое с модулем m ($НОД(a,m)=1$), принадлежит показателю n, если n такое наименьшее натуральное число, что выполняется сравнение: $a^n \equiv 1(\mathrm{mod}\,m)$.

Свойства данного числа a:

1. Числа $a^0, a^1, ..., a^{n-1}$ попарно не сравнимы по модулю n.
2. $a^t \equiv a^{t'}(\mathrm{mod}\,m) \Leftrightarrow t \equiv t'(\mathrm{mod}\,n)$.
3. n делит $\varphi(m)$ без остатка.

Число, принадлежащее показателю $\varphi(m)$, называется первообразным корнем.

4. По любому простому модулю p существует первообразный корень.
5. Пусть $c=\varphi(m)$, $q_1, q_2, ..., q_k$ – различные простые делители числа c. Число a, взаимно простое с модулем m, будет первообразным корнем тогда и только тогда, когда не выполнено ни одно из следующих сравнений: $a^{c/q_1} \equiv 1(\mathrm{mod}\,m)$, $a^{c/q_2} \equiv 1(\mathrm{mod}\,m)$,…, $a^{c/q_k} \equiv 1(\mathrm{mod}\,m)$.

Теорема 2.

Если p – нечетное простое число, то по модулям вида p^k и $2\cdot p^k$ ($k \ge 1$) существуют первообразные корни.

Пример 17.

$m=7$, $c=\varphi(7)=7-1=6$. Простые делители c: *2* и *3*. Значит, первообразный корень a не должен удовлетворять сравнениям: $a^3 \equiv 1(\mathrm{mod}\,7)$ и $a^2 \equiv 1(\mathrm{mod}\,7)$. Числа, взаимно простые с m: $\overline{1, m-1}$.

Проверим их:

$2^3(\mathrm{mod}\,7)=1$ –

$3^3(\mathrm{mod}\,7)=6$

$3^2(\mathrm{mod}\,7)=2$

$4^3(\mathrm{mod}\,7)=1$ –

$5^3(\mathrm{mod}\,7)=6$

$5^2(\mathrm{mod}\,7)=4$

Значит, первообразными корнями по модулю $m=7$ являются *3* и *5*.

Проверим выполнение сравнения: $a^{\varphi(m)} \equiv 1(\mathrm{mod}\,m)$. $3^6 \equiv 1(\mathrm{mod}\,7)$, $5^6 \equiv 1(\mathrm{mod}\,7)$ – верно.

Таким образом, *вычетом числа a по модулю m* называется остаток от деления a на m

Из определения видно, что вычеты связаны с делением с остатком.

Разделить натуральное число *a* на натуральное число *b* с остатком означает унайти неотрицательные числа два числа q и г, причем г < b такие, что выполняется равенство

a = q·b + г

Так для чисел 187 и 12 соответствуют два числа 15 и 7, такие, что 187= 15·12+7. Это равенство часто записывается в виде 187:12 = 15(ост. 7).

Напишем названия компонентов деления с остатком:

a – делимое, b- делитель, q- частное, r – остаток.

Рассмотрим еще примеры:

a = - 12, *b* = 8 ® -12 = (- 2) · 8 + 4, q= -2, r=4

a = - 324, *b* = - 15 ® — 324 = 22 · (- 15) + 6 q=22, r=6

a = 4, b=10 ® 4=0·10+4 q=0, r=4

a = 12, b = 4 ® 12=4·3+0 q=4, r=0

Число *a* делится нацело на *b,* если остаток *r* = 0 или, *a* = *qb*. .Причем отношение «делиться на цело» обозначается .

Теорема. Если *a* и *b* делятся на с, то при любых целых *k* и j сумма *ka* + *jb* делится на*c.*

Задание

1. Найти такое число *d ' 1*, на которое делятся числа *6n* + *5* и 9л + 2. При каком значении *n.* это деление возможно?
2. Для степени y=2n (n–натуральное число) установить классы сравнимости. Установить зависимость последней цифры этой степени от ее показателя.
3. Найти остаток от деления 7^{402} на 73.

Контрольные вопросы

1. Что такое вычет?
2. Что такое модуль?
3. Как найти НОД?
4. Как найти НОК?

КРИТЕРИИ ОЦЕНКИ РАБОТ

Оценка «отлично» выставляется, если

- практическая работа выполнена полностью; в логических рассуждениях и обосновании решения нет пробелов и ошибок;
- в решении нет математических ошибок (допустимы некоторые неточности, описки, которая не является следствием незнания или непонимания учебного материала).

Отметка «хорошо» ставится, если

- работа выполнена полностью, но обоснования шагов решения недостаточны (если умение обосновывать рассуждения не являлось специальным объектом проверки);
- допущена одна ошибка или есть два – три недочёта в выкладках, рисунках, чертежах или графиках (если эти виды работ не являлись специальным объектом проверки).

Отметка «удовлетворительно» ставится, если:

- допущено не более двух ошибок или более двух – трех недочетов в выкладках, чертежах или графиках, но обучающийся обладает обязательными умениями по проверяемой теме.

Отметка «неудовлетворительно» ставится, если:

- допущены существенные ошибки, показавшие, что обучающийся не обладает в полной мере обязательными умениями по данной теме.

Преподаватель может повысить отметку за оригинальный ответ на вопрос или оригинальное решение задачи, которые свидетельствуют о высоком уровне математической подготовки обучающегося; за решение более сложной задачи или ответ на более сложный вопрос, предложенные обучающемуся дополнительно после выполнения им каких-либо других заданий.

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

Основные источники

1. Богомолов Н.В. Практические занятия по математике: учеб. Пособие для бакалавров / Н.В. Богомолов. – 11-е изд. – М.: Юрайт, 2012. – 495с.
2. Дадаян А.А. Математика / А.А. Дадаян. – 3-е изд. – М.: Форум; Инфра-М, 2012. – 544 с.
3. Дадаян А.А. Сборник задач по математике / А.А. Дадаян. – М.: Форум; Инфра-М, 2012. – 352 с.
4. Пехлецкий И.Д. Математика: учебник для студ. учреждений сред проф. образования / И.Д. Пехлецкий. – 11-е изд., перераб. и доп. – М.: Академия. 2014. – 320 с.
5. Спирина М. С. Дискретная математика: учебник для студентов среднего профессионального образования / М.С. Спирина, П.А. Спирин. – 5-е изд., стер. – М.: Академия, 2015. – 368 с.
6. Стойлова Л.П. Теоретические основы начального курса математики: учеб. пособие для студ. учреждений сред. проф. образования / Л.П. Стойлова. – М.: Академия, 2014. – 272с.

Дополнительные источники

1. Аматова Г.М. Математика. Упражнения и задачи: учебное пособие для студентов высш. пед. учебных заведений / Г.М. Аматова, М.А. Аматов. – М.: Академия, 2013. – 332с.
2. Аматова Г.М. Математика: в 2 кн. Кн. 1: учебное пособие для студентов высш. пед. учебных заведений / Г.М. Аматова, М.А. Аматов. – М.: Академия, 2013. – 256с.
3. Аматова Г.М. Математика: в 2 кн. Кн. 2: учебное пособие для студентов высш. пед. учебных заведений / Г.М. Аматова, М.А. Аматов. – М.: Академия, 2013. – 240с.
4. Дадаян А.А. Математика для педагогических училищ, /А.А. Дадаян. – М.: Форум; Инфра-М, 2011. – 512 с.
5. Иванов Б.Н. Дискретная математика. Алгоритмы и программы: учебное пособие / Б.Н. Иванов. – М. : Лаборатория Базовых Знаний, 2012.
6. Новиков Ф. А. Дискретная математика для программистов: Учебное пособие для вузов по спец. "Информатика и вычислительная техника" / Ф.А. Новиков. – 2-е изд. – СПб.: Питер, 2013. – 364 с.

Интернет-ресурсы

1. http://www.ru.wikipedia.org Свободная универсальная энциклопедия, написанная на русском языке.
2. http://www.Allmath.ru - это математический портал, на котором вы найдете любой материал по математическим дисциплинам.
3. http://www.math.ru/ На сайте вы найдёте книги, видео-лекции, занимательные математические факты, различные по уровню и тематике задачи,

отдельные истории из жизни учёных — всё то, что поможет окунуться в удивительный и увлекательный мир математики.

4. http://www.bymath.net Этот сайт – средняя математическая интернет-школа, в которой вы можете учиться, не выходя из дому. В отличие от других сайтов здесь содержатся все необходимые материалы по элементарной математике в полном объёме.
5. http://free-math.ru/ Любите математику! Интересуйтесь математикой! Уважайте математику! Мы собираем для Вас только самое полезное и интересное. Учитесь с нами!
6. www. window. edu. ru Единое окно доступа к образовательным ресурсам Российской Федерации.
7. http://www.school.edu.ru/catalog.asp Каталог образовательный ресурсов на федеральном «Российском общеобразовательном портале».