Университет «Туран-Астана»

Нуспеков Е. Л., Таукенова Л.Ж., Абдибекова Л.М., Жумабаев Е.Н.

ДИСКРЕТНАЯ МАТЕМАТИКА

Учебное пособие

Нур-Султан, 2022

УДК 519.6
ББК 22.176 Я73 Д48
ISBN 978-601-7616-77-9

Ренцензия:
Адамов А.А Евразийский национальный университет им. Л.Н. Гумилева, заведующий кафедрой математического и компьютерного моделирования, к.т.н. профессор.
Жузбаев С.С Профессор кафедры информационных систем Евразийского национального университета имени Л. Н. Гумилева, к.ф-м.н.

Нуспеков Е.Л. Таукенова Л.Ж., Абдибекова Л.М., Жумабаев Е.Н. Дискретная математика: Учебник / Нур-Султан: Университет Туран-Астана, стр. 2022-116.

Предлагаемый учебник призван помочь вам в освоении глав «Дискретная математика».

Для освоения этой главы учащимся даются теоретические обзоры, случайные события, повторение тестов, случайные величины, статистическое распределение выборки, статистические оценки параметров распределения, элементы корреляционной теории, статистическая проверка статистических гипотез. Были выданы и представлены задания по каждой теме, а также индивидуальные задания для каждого ученика. 25 инструкций. Номер инструкции соответствует номеру студента в списке.

Дается теоретическая информация, теоретические вопросы должны быть усвоены на лекциях и в учебниках.

УДК 519.6
ББК 22.176 Я73 Д48
ISBN 978-601-7616-77-9

Тезисы лекций

Темы 1, 2. Элементы теории множеств

Цель:

1. Введение основных понятий теории множеств.
2. Указание способов задания множеств.
3. Рассмотрение основных теоретико-множественных операций и их свойств.

План:

1. Множества. Подмножества. Способы задания множеств.
2. Операции над множествами и их свойства.

1. Множества. Подмножества. Способы задания множеств

Современная научная трактовка математических понятий строится на базе теоретико-множественных идей. С проникновением в математику теоретико-множественной концепции (конец XIX в.) начинается период современной математики.

Понятие множества - одно из основных и наиболее важных понятий современной математики. Этому понятию невозможно дать строгое определение. (Для этого необходим определенный набор терминов, известных ранее). Для понятия “ множества “ это невозможно, т. к. оно является наиболее широким и ни в каких других не содержится.

Основатель теории множеств немецкий математик Георг Кантор (1845-1918) так определял понятие множества: «Множество М есть любое собрание определенных и различимых между собой объектов нашей интуицией, мыслимое как единое, целое».

Произвольные множества обозначаются заглавными латинскими буквами A, B, C… Предметы (объекты), составляющие данное множество, называют его элементами, обозначаются малыми латинскими буквами: a, b, c, …, x…

То, что некоторое множество состоит из элементов x, y, z, мы будем записывать при помощи фигурных скобок: M= {x, y, z…}

Запись: a □M означает, что a является элементом множества (a принадлежит M) “□“ - знак принадлежности.

Если множество содержит конечное число элементов, то говорят, что оно конечно, в противном случае, множество называется бесконечным (т.е. невозможно явно перечислить его элементы).

Язык теории множеств применяется в самых различных областях математики.

Определение 1. Множество A называется **подмножеством** множества B, если всякий элемент A является одновременно и элементом множества B, т.е. из x□A следует x□ B. Символически: A □ B - знак нестрогого включения (A содержится в B, A подмножество B, A включено в B).

Пример. A= {1,2} B= {1,2, {1,3}} A□B

Определение 2. Множество, которое не содержит ни одного элемента, называется **пустым** и обозначается символом□. Обычно все множества, с которыми имеют дело в конкретной математической области, являются подмножествами некоторого фиксированного множества U, которое называется универсальным**.** (это понятие относительно: оно выбирается для какого-нибудь определенного раздела). В стереометрии: множество всех точек пространства. В алгебре: для числовых множеств - множество С; в элементарной алгебре – R.

Определение 3. Два множества называются **равными**, если они состоят из одних и тех же элементов. Запись: A=B.

Заметим, что два множества A и B равны, если всякий элемент из A принадлежит B и обратно, т.е. если одновременно выполняются два условия:
1) A□B 2) B□A
На этом замечании и основывается доказательство равенства двух множеств.

Собственные подмножества.

Из определения подмножества видно, что □ множество является подмножеством самого себя, т. е. M□M. Пустое множество □ также будем называть подмножеством любого множества M: □□M. Эти подмножества называются несобственными. Прочие подмножества называются собственными множествами M. Для собственных подмножеств иногда пишут вместо□знак□ (знак строгого включения).

Пример. A = {a, b, c}
A имеет 2 несобственных подмножества: □, A и 6 собственных подмножеств: {a}, {b}, {c}, {a, b}, {b,c}, {a,c}.

Способы задания множеств

1) Множество может быть задано перечислением всех его элементов (применим лишь к конечным множествам, но не ко всем).

$A=\{x_1, x_2, \square, x_n\}$

2) Универсальный способ: указание *характеристического свойства* его элементов:

а) указывают хорошо известное множество M, подмножеством которого является A;

б) указывают характеристическое свойство P(x), которым обладают те и только те элементы M, которые входят в A.

2. Операции над множествами.

Задать бинарную операцию над множествами, значит указать способ построения по двум данным множествам A и B нового третьего множества.

Определение 1. **Объединением** множеств A и B называется множество, обозначаемое A□B, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из множеств A или B.

Символически: A□B= {x□x□A или x□B} (правило построения □ двух множеств называется операцией объединения).

Пример. A= {1,2,3} B= {2,3,4}; A□B= {1,2,3,4}

Для наглядности изображения удобно использовать диаграммы Эйлера-Венна.

Определение 2. **Пересечением** множеств A и B называется множество, обозначаемое A ∩ B, состоящее из тех и только тех элементов, которые принадлежат множеству A и множеству B одновременно.

Символически: A ∩ B = {x | x□A и x□B}

Правило построения пересечения множеств называется операцией пересечения.

A = {1, 2, 3} B = {1, 2, 3} A ∩ B = {2, 3}

Свойства операций □, □:

1. Коммутативность: A □ B = B□A; A □ B = B□A
2. Ассоциативность: (A □ B) □ C = A □ (B □ C);
   (A □ B) □ C = A □ (B □ C).
3. Дистрибутивность: A □ (B □ C) = (A □ B) □ (A □ C)
   A □ (B □ C) = (A □ B) □ (A □ C).
4. Идемпотентность: A □A = A; A □A = A
5. A □□ = A; A □□ = □;
   A □U = U; A□U = A.

Проиллюстрируем с помощью диаграмм свойство 3.

Определение 3. **Разностью** множеств A и B называется множество, обозначаемое A \ B, состоящее из всех тех и только тех элементов множества A, которые не принадлежат B.

Символически: A \ B = {x | x□A и x□B}.

Правило построения разности называется операцией вычитания.

A = {1, 2, 3} B = {2, 3, 4}

A \ B = {1} B \ A = {4}

Этот пример показывает, что операция вычитания является некоммуникативной.

Определение 4. Случай, когда B□A заслуживает особого внимания.

Если B□A, то разность A \ B = $\overline{B}_{\text{а}}$ называется дополнением множества B до множества A.

B = {1, 3, 5} A = {1, 2,3,4,5} $\overline{B}_{\text{а}}$ = {2, 4} $\overline{A}_{\text{в}}$ = □

Часто в качестве множества A рассматривают универсальное множество U и тогда пишут $\overline{B}_{\text{и}} = \bar{B}$

Свойства операций \, □

6. A \ □ = A; □ \ A = □
7. □ = U; $\overline{U}$ = □
8. A □ $\overline{A}$ = □; A □ $\overline{A}$ = U
9. Законы де Моргана: $\overline{A \cup B} = \overline{A} \square \overline{B}$; $\overline{A \cap B} = \overline{A} \square \overline{B}$
10. Закон инволюции (двойного отрицания): $\overline{\overline{A}} = A$.

Контрольные вопросы:

1. Дайте канторовское определение множества, приведите примеры.
2. Какое множество называется пустым, универсальным?
3. Какие два множества называются равными?
4. Что называется подмножеством? Укажите собственные подмножества.
5. Какие способы задания множеств вы знаете?
6. Какие теоретико-множественные операции вы знаете? Дайте определения.
7. Сформулируйте свойства операций над множествами.

Темы 3,4. <u>Прямое (декартово) произведение. Отображения</u>

Цель:

1. Введение понятия декартова произведения.
2. Введение понятия отображения, области значений отображения.
3. Формирование умения определять типы отображений, находить композицию отображений.

План:

1. Прямое (декартово) произведение множеств.
2. Отображения, типы отображений, композиция отображений.

1. Прямое (декартово) произведение множеств

Мы познакомились с четырьмя операциями над множествами. Рассмотрим ещё одну операцию – операцию прямого умножения множеств.

Пусть даны множества A и B. Рассмотрим совокупность всех упорядоченных пар вида <a,b>, где aЄA, bЄB. Понятие упорядоченной пары означает, что ‹a, b› ≠ ‹b, a›, если исключить случай a = b.

Допустить существование ‹a, b› с таким свойством: ‹a, b› = ‹c, d› ↔ a = c, b = d очевидно, не труднее, чем допустить существование множеств, и поэтому принимаем понятие упорядоченной пары как первичное, не определяя его. (в геометрии: любая точка плоскости однозначно определяется

последовательностью двух чисел ‹x, y›, называемых координатами точки: первое число x является абсциссой, второе y – ординатой.)

Определение 1. Множество всех упорядоченных пар вида ‹x, y›, где xЄA, y Є **B**, называется **прямым (декартовым) произведением** множеств (по имени математика и философа Декарта). Запись: A□B = {‹x, y› | x Є A ^ y Є B} Очевидно, что для любых двух множеств A и B, взятых в указанном порядке, существует, и только одно, их прямое произведение: A□B=Ø <=> A=Ø νB = Ø.

Если A и B – конечные множества, то A□B – конечно, так как мы можем просто перечислить всевозможные комбинации элементов x из A и y из B.

Пример. A= {-2,0,5} B= {3,5}, A□B= {(-2,3), (-2,5), (0,3), (0,5), (5,3), (5,5)} т. е. A□B содержит 6 элементов. Рассмотрим простую геометрическую интерпретацию понятия декартово произведение.

Геометрическая модель множества A□B.

Найдем B□A= {(3,-2), (3,0), (3,5), (5,-2), (5,0), (5,5)}, т. е. A□B ≠ B□A

Этот пример показывает, что операция прямого умножения множеств не коммутативна.

Условимся число элементов конечного множества обозначить через |A|, тогда |A□B|=6.

Если A – конечное множество из n различных элементов a_1, … a_n , B – из m различных элементов b_1, ... b_m , то A□B содержит m*n различных элементов

$$(a_1,b_1),(a_1,b_2), \dots , (a_n,b_m), \dots , (a_n,b_m) \Rightarrow \quad |A□B|=|A|□|B|$$

Если множества A и B равны, то декартово произведение A «самого на себя» называется прямым или декартовым квадратом и обозначается A□A=A^2 (используя символику обычной алгебры).

Упорядоченной тройкой называется множество, состоящее из трех элементов, взятых в определенном порядке.

Введем понятие прямого произведения трех множеств следующим образом: A□B□C = {‹x, y, z› | x Є A, y Є B, z Є C}

Множество точек на плоскости можно теперь представить, как прямое произведение R□R=R^2 (множество действительных чисел), а множество точек пространства R□R□R=R^3.

Пусть имеем n множеств A_1, A_2, ..., An (не обязательно различных). Обобщением понятия упорядоченной пары является понятие кортежа (упорядоченного набора) n элементов; обозначается ‹a_1, a_2, ..., a_n› и называется кортежем длины n.

Эту упорядоченную систему обозначим через ‹a_1, a_2, ..., a_n›, где a_i Є A_i (i=1, ..., n) (сокращенно «эпка»).

Определение 2. Множество всех упорядоченных эпок (кортежей) (a_1, a_2, ..., a_n), a_i Є A_i (i=1, ..., n) называется **прямым произведением n множеств** и обозначается $A_1 \square A_2 \square . \square A_n$, такимобразом$A_1 \square A_2 \square ... \square A_n$= {‹$a_1$,□, an› | a_1ЄA_1, ..., a_nЄA_n}.

Если все A_i равны между собой, то прямое произведение n-множеств. $A \square A \square \ldots \square A = A^n$ называется n-степенью множества А.

Имеет место следующее утверждение: если А-конечное множество и число его элементов равно m, то есть |A| = m, то число элементов множества A^n равно m^n. Доказательство:

$$|A^n| = |A \square ... \square A| = |A|^n = m^n$$

Как и операции объединение, пересечение, вычитание, дополнение, операция прямого умножения позволяет строить из данных множеств новые множества. Однако этим не исчерпывается роль операции умножения в математике. Дело в том, что через понятие прямого произведения двух множеств, оказывается, легко определить такие фундаментальные математические понятия, как понятие отношения (соответствия), отображения, алгебраической операции.

Отображения

Одним из центральных понятий математики является понятие отображения (или функции). Внимательное рассмотрение показывает, что в понятии функции существенно не только её изменение с изменением аргумента, сколько сам закон соответствия, в силу которого по каждому значению аргумента однозначно определяется соответствующие ему значения функции.

Определение 3. Пусть А и В – два множества произвольной природы. Говорят, что задано ***отображение*** (функция) f множества А во множество В, если □элементу x□A поставлен в соответствие однозначно определённый (т. е. единственный) элемент y □ B.

Запись: f: A□B

x□y = f (x), y – называется образом элемента x,

x – прообразом y.

Через f обозначают то отображение (правило), по которому это соответствие устанавливается. С помощью диаграмм Венна это изображается так:

Таким образом, отображение (функцию) можно задать, указав три множества: А, В и множество всех упорядоченных пар <x, y> из A□B, таких, что y = f (x).

Определение 3′. Отображением (функцией) называется тройка

<A, B, S>, где S = {<x, y>□A□B, y = f (x)}.
Множество A – называется областью определения отображения,
B – областью значений,
S – графиком данного отображения.

Типы отображений

Определение 4. Отображение f: A□B называется ***инъективным*** (или взаимно – однозначным), если двум различным элементам A соответствуют два различных образа: $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ □ $x_1, x_2 \in A$.

Определение 5. Отображение f: A□B называют ***сюръективным*** (или отображением «на»), если □ y□Bсоответствует по крайней мере одному элементу x□A, т. е. □ элемент y является образом некоторого элемента x□A (f (A) = B).

При отображении «в», с одной стороны, некоторые элементы из B могут вовсе не иметь прообразов (в отображении «на» этого нет), с другой стороны, могут быть элементы, имеющие несколько (даже бесконечно много) прообразов. Если нет ни того, ни другого, то отображение называется взаимно – однозначным «на».

Определение 6. Отображение f: A□B называется **биекцией**, если f – инъекция и сюръекция одновременно.

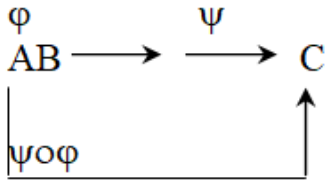
Отображение f называется *биективным,* если □b□B является образом единственного элемента множества A□b□B□ a (!) □A.

Определение 7. Пусть даны отображения □: A□B, □: B□C.

Отображение f: A□C, определяемое формулой f (x) = □ (□ (x)) называется ***суперпозицией (или композицией)*** отображений □, □ и обозначается □□□□.

Суперпозиция иногда называется произведением.

1) Операция суперпозиции отображений ассоциативна:
пусть □: A□B; □: B□C; f: A□C f□ (□□□) = (f□□) □□
2) Коммутативностью не обладает, т. е. □f, □: f□□□□□f



Контрольные вопросы:

1. Как определяется упорядоченная пара?
2. Что называется прямым (декартовым) произведением множеств?
3. Как определяется декартов квадрат?

4. Что называется отображением множеств?
5. Какие типы отображений вы знаете?
6. Сформулируйте определение композиции (суперпозиции) отображений.

Темы 5,6 Бинарные отношения. Фактор-множество

Цель:

1. Введение понятия бинарного отношения и свойств бинарных отношений.
2. Введение понятий отношений эквивалентности и порядка.
3.. Введение понятия фактор-множества.

План:

1.Бинарные отношения. Основные свойства бинарных отношений
2.Отношение эквивалентности и разбиение на классы.
3.Отношение порядка. Фактор-множество.

1.Бинарные отношения. Основные свойства бинарных отношений

В математике часто приходится изучать различные отношения между элементами того или иного множества. Эти отношения могут связывать различные пары элементов множества, различные тройки и так далее (например, два натуральных числа могут быть или не быть взаимно простыми, то есть их НОД=1). Остановимся на отношениях, связывающих различные пары элементов некоторого множества А, так называемых бинарных отношениях.

Определение 1. Для любых двух множеств А и В всякое подмножество $\alpha \in A \square B$ называется **бинарным отношением** между элементами множеств А и В.

ЕслиА=В, то $\alpha \in A^2$ называется бинарным отношением, заданным на множестве А.

Если упорядоченная пара <а, в>$\in \alpha$, то говорят, что а и в связаны отношением α, или, что а находится в отношении α с в и пишут аα в.

Пример. а<в, а $\leq \cdot$в, т. М $\in$прямой а.

Как множество, α может быть задано либо пересечением своих элементов, либо указанием характеристического свойства, которым обладают только пары из α.

Определение 2. Множество всех первых координат элементов бинарного отношения α называют **областью определения** α и обозначают Дот α = Дα = {а | аαв}, а множество всех вторых координат элементов отношения α называют областью значений и обозначают Imα = Iα = {в | аαв}.

Особенно важен для многочленных применений случай, когда А – множество действительных чисел => R^2 – обычная плоскость. Произвольные бинарные отношения рассматриваются как подмножество точек плоскости. Это дает наглядную геометрическую характеристику соответствующего отношения.

Пример. Множество упорядоченных пар, для которых выполняется отношение **x <y**, представляется множеством точек плоскости, лежащих выше прямой **y=x**.

Свойства бинарных отношений на множестве

Определение 3. Бинарное отношение ρ на множестве А называют:

а) *рефлексивным*, если любой элемент множества А находится в отношении ρ сам с собой.

ρ - рефлексивно $\square \forall a \in A \;\; a \rho a$.

Примеры: =, ⋮, ∝, ||.

б)*симметричным,* если вместе с каждой своей парой <а, в> отношение ρ содержит и пару <в, а>.

ρ - симметрично $\square \forall$ а, в$\in$А аρв=>вρа.

Примеры: =, ||, ⊥, ∞.

в) *транзитивным,* если вместе с любыми парами <а, в> и <в, с> оно содержит и пару <а, с>.

ρ - транзитивно $\square \forall$ а, в, с$\in$А аρв $\wedge$ вρс => аρс.

Примеры:<, ⊂, ⋮, ⫤, ∝, ||.

г) *антирефлексивным*, если ни один элемент множества А не находится в этом отношении ρ сам с собой.

ρ - антирефлексивно $\square \forall$ а$\in$А аρа.

д) *антисимметричным*, если в нем одновременно не могут содержаться никакие пары <а, в> и <в, а> с различными а и в.

ρ - антисимметрично $\square \forall$ а,в$\in$А аρв $\wedge$вρа => а = в или аρв$\wedge$а$\neq$в => вρа.

Примеры: ⋮, ≤.

е) *связным*, если при любых различных **а** и **в** принадлежащих множеству **А** оно содержит либо пару <а, в>, либо <в, а>.

ρ - связно $\square \forall$ а,в$\in$А а$\neq$в => аρв $\vee$ вρа.

Примеры:<, ≤.

2.Отношение эквивалентности и разбиение на классы

Особую роль играют бинарные отношения, обладающие одновременно первыми тремя свойствами.

Определение 4. Бинарное отношение ρ, заданное на множестве А, называется **отношением эквивалентности**, если оно рефлексивно, симметрично и транзитивно. Обозначается ~.

Примеры: $=, \|\|, \infty$,

Некоторый общий способ задания отношения эквивалентности на произвольном множестве связан с понятием разбиения на классы.

Определение 5. Будем говорить, что дано **разбиение множества А на подмножества (классы)** A_i, если

1) все эти подмножества непусты: $A_i \neq \emptyset \quad \forall_i \in I$;
2) любые два различных подмножества не пересекаются: $A_i \neq A_j \Rightarrow A_i \cap A_j = \emptyset \quad \forall_{i,j} \in I$;
3) объединение всех подмножеств есть множество А: $UA_i = A, \ _i \in I$.

Пусть ρ - бинарное отношение на А. Множество $\{x \mid a \rho x\} = \bar{a}^{\rho}$ называется классом, порожденным элементом а, который обозначается $<x, y> \in \rho$ □ $x, y \in \bar{a}^{\rho}$. Следовательно ρ - это отношение принадлежности двух элементов множества одновременно одному и тому же классу.

Предложение. Отношение ρ - является отношением эквивалентности.

Отношение эквивалентности ρ определяет разбиение множества А на классы эквивалентности: $\bar{a}^{\rho} = \{x \mid a \rho x\}$.

(1) $\bar{a}^{\rho} \neq \emptyset$, так как $a \in \bar{a}^{\rho}$ (в силу рефлективности) $a \rho a$.

(2) $\bar{a}^{\rho} \cap \bar{в}^{\rho} \neq \emptyset \Rightarrow \bar{a}^{\rho} = \bar{в}^{\rho}$

а) $\exists x \in \bar{\mathbf{a}}^{\rho}$ **и** $\mathbf{x} \in \bar{в}^{\rho} \Rightarrow \mathbf{x} \rho \mathbf{a} \wedge \mathbf{x} \rho \mathbf{в} \Rightarrow \mathbf{a} \rho \mathbf{в};$

покажем, что $\bar{a} \subset \bar{в}$

б) $y \in \bar{a} \Rightarrow y \rho a$ и $a \rho в \Rightarrow y \rho в \Rightarrow y \in \bar{в}$;

аналогично, $\bar{в} \subset \bar{a} \Rightarrow \bar{a} = \bar{в}$

(3) $U \bar{a}^{\rho} = A$

а)_при $\forall \ a \in A \qquad \bar{a}^{\rho} \subset A \Rightarrow U \bar{a}^{\rho} \subset A$

б) обратно, $A \subset U \bar{a}^{\rho}$, так как если $a \in A$, то $a \in \bar{a}^{\rho} \Rightarrow a \in U \bar{a}^{\rho}$.

Итак, имеем $<x, y> \in \rho <=> x, y \in \bar{a}^{\rho}$.

Вывод: ρ - бинарное отношение эквивалентности, порождающее разбиение на классы эквивалентности, которые удовлетворяют двум условиям:

1) любые два элемента одного класса эквивалентны друг другу;
2) элементы из разных классов не эквивалентны друг другу.

$a \rho в$ □ $\bar{a}^{\rho} = \bar{в}^{\rho}$

Примеры. А – множество треугольников, $\infty \equiv \rho$.

Определение 6. Пусть ρ - отношение эквивалентности на множестве А, тогда множество всех классов эквивалентности по отношению ρ называются фактор-множеством множества А по отношению ρ и обозначается A/ρ.

Контрольные вопросы:

1.Что называется бинарным отношением множеств?

2. Какие свойства бинарных отношений вы знаете?

3. Приведите примеры бинарных отношений.

4. Дайте определение отношения эквивалентности и разбиения на классы.

5. Что называется отношением порядка?
6. Как определяется фактор-множества?

Темы 7, 8. Элементы комбинаторики. Размещения

Цель:

1. Введение понятия комбинаторика.
2. Рассмотрение основных правил комбинаторики.
3. Введение понятия размещения.

План:

1. Комбинаторика как раздел дискретной математики.
2. Правила суммы и произведения.
3. Размещения с повторениями и без повторений.

1.Комбинаторика как раздел дискретной математики

Комбинаторикой называется область математики, в которой изучаются вопросы о том, сколько разных комбинаций с заданным условием, можно составить из заданных объектов

Во многих практических случаях возникает необходимость подсчитывать количество возможных комбинаций объектов, удовлетворяющих определённым условиям. Такие задачи называются комбинаторными.

Комбинаторика возникла в 16 в. Первоначально комбинаторные задачи касались в основном азартных игр. (Именно проблемы азартных игр явились движущей силой в развитии комбинаторики и развивающейся вместе с ней теории вероятности).

За последние годы комбинаторика переживает период бурного развития, связанного с общим повышения интереса к проблемам дискретной математики.

Комбинаторные задачи используются в теории вероятностей, математической логике, теории чисел, вычислительной технике, кибернетике, экономике, лингвистике и т. д.

Комбинаторика – один из разделов дискретной математики, который приобрёл важное значение в связи с использованием его в теории вероятностей, математической логике, теории чисел, комбинаторике, вычислительной технике.

2.Правила суммы и произведения

Большинство задач решается с помощью двух основных правил – правило суммы и правило произведения.

Пример. Если на первой полке книжного шкафа стоит 30 различных книг, а на другой – 40 различных книг, то выбрать одну из стоящих на этих полках книг можно 40+30=70 способами.

Обобщением этого примера является следующее утверждение, называемое правилом суммы.

Правило суммы. Если объект А можно выбрать m способами, а объект В – n способами, то выбор «Либо А, либо В» можно сделать m+n способами (любой выбор объекта А отличен от любого выбора элемента В).

Пример. Существует 3 кандидата на место командира и 2 кандидата на место бортмеханика. Сколькими способами можно сформировать экипаж корабля, состоящий из командира и борт инженера?

Решение: Командира корабля можно выбрать 3 способами, после выбора командира ещё 2 способами можно выбрать бортинженера, поэтому общее число способов, которыми можно составить экипаж, находится произведением 3*2=6

Экипажи $К_1$, $Б_1$

Такая схема называется деревом.

Обобщением этого примера является следующее утверждение, называемое правилом произведения.

Правило произведения. Если объект А можно выбрать m способами и если после каждого такого выбора объект В можно выбрать n способами, то выбор упорядоченной пары (А, В) можно сделать mn способами.

Задача 1. Из города А в город Б ведут 2 дороги, из А в Г - 4 дороги, из Б в В 3 дороги, из Г в В – 5 дорог.

а) Сколько различных дорог ведёт из А в В через Б?

б) Сколько вообще разных дорог из А в В?

Решение:

а) по правилу произведения 2*3=6

б) 1 случай: через Б: 6 дорог

2 случай: через Г: 4*5=20 дорог

По правилу суммы получим 20+6=26 дорог

Задача 2. Сколькими способами из 28 костей домино можно выбрать 2 кости так, чтобы их можно было приложить друг к другу?

Решение: выберем 1 кость – 28 способов (в семи случаях эта кость будет «дублем» (числа на половинках одинаковы), а в 21 случае – на половинках разные числа.

1 случай: вторую кость можно выбрать 6 способами – по правилу произведения: 7*6=42 способа

2 случай: 2 кость можно выбрать 12 способами (по 6 на каждую половинку), и по правилу произведения имеем: 21*12=252 способа.

По правилу суммы получаем: 42+252=294 способа выбора пары.

3.Размещения с повторениями и без повторений

Пусть дано множество $\{a_1,\ldots,a_n\}$, состоящее из n разных элементов.

Определение 1. **Выборкой** объема К называется множество $\{a_{i1},\ldots,a_{ik}\}$, содержащее k элементов исходного. Элементы выборки могут быть как разными, так и одинаковыми.

Определение 2 Выборки, у которых порядок существенен, а элементы могут быть одинаковыми, называется **размещением с повторением**.

Обозначаются: A_n^k

Теорема. $A_n^k=n^k$

Доказательство: из правила произведения: на $1^{ом}$ месте могут быть n элементов, на $2^{ом}$-также n элементов…, на $k_{ом}$-n элементов: $n.n\ldots n=n^k$, т.е. каждый из k предметов можно разместить n способами.

Определение 3. Выборки, у которых все элементы разные, а порядок по-прежнему существенен, называется размещениями **(без повторений).** Обозначаются: A_n^k

Теорема. $A_n^k=n(n-1)\ldots(n-$

Произведение всех натур, чисел от1 до n дополнительно обозначаются n! т. е. $n! =1.2\ldots n$

По определению считают: $A_n^0=1$; $A_n^k=0$, если $k> n$

Контрольные вопросы:

1. Что изучает комбинаторика?
2. Какие основные правила комбинаторики вы знаете?
3. Как определяется размещения с повторениями?
4. Как определяется размещения без повторений?
5. Запишите формулы для их нахождения.

Темы 9, 10. Перестановки и сочетания.

Цель:

1. Введение понятия перестановок с повторениями и без повторений.
2. Введение понятия сочетания с повторениями и без повторений.

План:

1. Перестановки с повторениями и без повторений.
2. Сочетания с повторениями и без повторений.

1. Перестановки с повторениями и без повторений

Определение 1. Размещения без повторения при k=n называется **перестановками.** (Такие выборки различаются только порядком элементов).

Обозначается: P_n

$P_n=n!$

Теорема.

Доказательство: $Pn=A_n^n= n (n-1) \ldots (n-(к-1)) =n!$

О! принято считать=1.

Пример. Буквы азбуки Морзе образуются как последовательность точек и тире. Сколько различных букв можно образовать, если использовать коды, содержание 5 символов?

Решение: исходное множество состоит из 2х элементов: точка, тире. Используется 5 символов, поэтому выборка содержит 5 элементов, которые могут повторяться. Следовательно, число различных выборов каждая из которых представляет какую-нибудь букву, равно $2^5=32=A_2^5$

Пример. Сколькими способами в футбольной команде из 11 человек можно выбрать капитана и вратаря?

Решение: капитаном может стать любой из 11 футболистов. После его выбора на роль его заместителя могут претендовать 10 оставшихся человек. Таким образом, имеем $11*10=110=A_{11}^2$ разных вариантов выбора.

Пример. Сколькими способами можно выложить в ряд красный, чёрный, синий и зелёные шарики?

Решение. На 1 место можно положить любой из 4^x шариков, на 2ое – любой из 3^x оставшихся, на $3^{ье}$ – любой из 2^x оставшийся, а на $4^{ое}$ – последний оставшийся шарик.

$$4! =24=P_4$$

2. Сочетания с повторениями и без повторений

Рассмотрим такие выборки из множества A= { a_1, a_2 ,…, $a_к$ }, в которые элемент a_1 входит n_1 раз, a_2 - n_2 раз, …., $a_к$ - $n_к$ раз. Тогда общий объем выборки равен: m= $n_1 + n_2 + \ldots + n_k$.

Набор натуральных чисел (n_1 ,…, n_k) будем называть **составом выборки**.

Определение 2. Число различных выборок одного состава называется числом **перестановок** из m элементов **с заданным числом повторений**. $n_1,\ldots,n_k$.

Пример. Это число вычисляется по формуле: $P_m(n_1,\ldots,n_k)=\frac{m!}{n_1!\cdot\ldots\cdot n_k!}$

Доказательство: действительно, если бы все **m** элементов были различны, то число перестановок было бы равно **m!** Поскольку элемент a_1 входит n_1 раз, то перестановка этого элемента не дает новых перестановок => имеем $\frac{m!}{n_1!}$ различных перестановок (во столько раз будет меньше вариантов), и т. д.

Задача. Сколько различных слов можно образовать из букв слова «МАТАМАТИКА»

$$C_{10}^{3}=\frac{10!}{3!7!}=120.$$

Определение 3. Выборки, у которых все элементы разные, а порядок несущественен, называется **сочетаниями (без повторений)** из**n** элементов по**k**. (Такие выборки отличаются только составом элементов, но не порядком). C_n^k

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

Доказательство: из каждого сочетания можно сделать**k!** перестановок, а число этих сочетаний C_n^k и по правилу произведения

$$k!\cdot C_n^k=A_n^k$$

Задача. В стране 20 городов, каждые два из которых соединены авиалинией. Сколько авиалиний в этой стране?

Решение. Каждая авиалиния соединяет 2 города. В качестве одного города можно взять любой из 20 городов (город А), а в качестве второго – любой из 19 оставшихся (город В). Перемножив эти числа, получаем 20·19=380. Однако при этом подсчете каждая авиалиния учтена дважды (первый раз, когда в качестве одного города был выбран город А, а второй- город В, а второй раз - наоборот). Так образованное число авиалиний 380:2=190= C_{20}^2

Определение 4.Число различных составов выборки объема n, образованной из **k** групп одинаковых элементов называется **сочетаниями (с повторениями)** из **n**элементов по**k** , и равно: $\overline{C}_n^k=\frac{(n+k-1)}{k!(n-1)!}$

Задача. Для несения почетного караула из 10 человек могут быть приглашены офицеры: сухопутных войск, авиации, погранвойск, артиллерии, офицеры морского флота и ракетных войск.
Сколькими способами можно избрать состав почетного караула?

$$\overline{C}_6^{10}=\frac{15!}{10!3!}=3003$$

Контрольные вопросы:

1. Дайте определение перестановкам с повторениями и без повторений.
2. Дайте определение сочетаниям с повторениями и без повторений.
3. Запишите формулы для их нахождения.

Темы 11, 12. Отношение делимости, НОК, НОД.

Цель:

1. Рассмотрение отношения делимости в кольце Z.
2. Введение понятий НОД и НОК, связь между ними.
3. Формирование умений и навыков при решении практических задач.

План:

1. Отношение делимости, его простейшие свойства.
2. НОД. Алгоритм Евклида. НОК.
3. Простые числа.

Исторически теория чисел возникла как непосредственное развитие арифметики. В настоящее время в теорию чисел включают значительно более широкий круг вопросов, выходящих за рамки изучения натуральных чисел.

Современную теорию чисел можно в основном разбить на следующие разделы:

I. *Элементарная теория чисел.*
(теория сравнений; неопределенные уравнения; вопросы теории чисел, являющиеся непосредственным развитием теории делимости; вопросы о представимости чисел в определенной форме).

II. *Алгебраическая теория чисел*.
Изучаются различные классы алгебраических чисел.

III. *Аналитическая теория чисел* – те вопросы теории чисел, при изучении которых применяются методы математического анализа.

IV. *Геометрическая теория чисел* – проблемы, которые могут быть сформулированы в геометрической форме и к решению которых применяются геометрические соображения.

Мы будем изучать некоторые вопросы элементарной теории чисел.

Теория чисел занимается изучением свойств целых чисел $Z=\{Z,+,\cdot,0,1\}$.

1.Отношение делимости, его простейшие свойства

Определение 1. Целое число a делится на целое число b, если существует такое целое число q, что a=b*q.

Число a называется делимым, b – делителем, q – частным.

Обратным к отношению $a \vdots b$ является отношение «b делит a», которое обозначается b/a. отношение делимости $a \vdots b$ (эта запись содержит в себе предположение, что $b \neq 0$) является бинарным отношением в Z.

Свойства отношения делимости.

1⁰Рефлексивность. $\forall a \in Z$ имеем $a \vdots a$ (так как a=a*1, $1 \in$ Z) .

2⁰ Транзитивность. [illegible]

([illegible] $q \in Z, q_1 \in Z$).

3⁰Любое число делится на 1: $a \vdots 1$ для $\forall a \in Z$ (a=1*a).

4⁰ Если $a \vdots b$, то $(\pm a) \vdots (\pm b)$, (то есть при любом сочетании знаков).

[illegible], где $q, -q \in Z$.

5⁰ $a \vdots c \wedge b \vdots c \Rightarrow (a+b) \vdots c$

($a = c*q_1$, $b = c*q_2 \Rightarrow a+b = c*(q_1+q_2) = c*q$, $q \in Z$)

6⁰ $a, b \in Z, a \neq 0$

$a \vdots b \Leftrightarrow |a| \vdots |b|$, где $q \in Z$ (в силу ассоциативности, коммутативности).

7⁰ (Следует из 5⁰, 6⁰) $a \vdots b_1, a \vdots b_2, \ldots, a \vdots b_n \Rightarrow a \vdots (b_1 + b_2 + \ldots + b_n)$, $b_1, \ldots b_n \in Z$.

8⁰ Если $a \neq 0$, то не существует такое q, что $0*q = a$.

(От противоположного: если бы существовало q от деления $a \neq 0$ на 0, то $a = q*0$, но $q*0 = 0 \Rightarrow a = 0$, что противоречит условию). Коротко говоря, на нуль делить нельзя.

9⁰ $a_1 \vdots b, a_2 \vdots b, \ldots, a_n \vdots b \Rightarrow (a_1 + a_2 + \ldots + a_n) \vdots b$

($a_1 = b*q_1, a_2 = b*q_2, \ldots, a_n = b*q_n \Rightarrow a_1 + a_2 + \ldots + a_n = b*(q_1 + q_2 + \ldots + q_n) = b*q$, $q_n \in Z$).

10⁰ (Следствие 9⁰) $a \vdots b, n \in Z, n \neq 0 \Rightarrow an \vdots b$

(частный случай, когда $a_1 = a_2 = \ldots = a_n = a$).

11⁰ $a \vdots b \Rightarrow |a| \geq |b|$, $a = b*q$, потому что $|a| = |b|*|q| \geq |b|$.

12⁰ (Следствие 11^0) $a \vdots b \wedge b \vdots a \Rightarrow a = \pm b$ либо $a = -b$.

$a \vdots b \Leftrightarrow |a| \vdots |b| \Leftrightarrow |a| = |b| \Leftrightarrow a = \pm b$ или $a = -b$.

Теорема о делении с остатком.

Для $\forall a, b \in Z, b \neq 0$, существуют и притом единственные $q, r \in Z$, такие, что $a = bq + r$, $0 \leq r < |b|$.

Доказательство.

I. Существование q и r.

а) $a \in Z; b > 0$.

Рассмотрим множество всех чисел, кратных b и расположим его в порядке возрастания: …, b*(-2),
b*(-1), b*0, b*1, b*2, …

Пусть bq – наибольшее кратное числа b , не превышающее a. Тогда $a \geq bq$, но $a < b(q+1)$, т.е. $bq \leq a < b(q+1)$, откуда $0 \leq a - bq < b$.

Положив $a - bq = r$, получим $a = bq + r$, $0 \leq r < b$.

б) $a \in Z; b < 0$

Т.к. b<0, то –b>0 и согласно сл. а) деление a на –b возможно, а это означает существование таких целых чисел q и r, что $a = (-b)q + r$, $0 \leq r < |-b|$ или $a = b(-q) + r$ $0 \leq r < |b|$

II. Единственность q и r.

Пусть $a = bq + r$ $0 \leq r < |b|$

$a = bq' + r'$ $0 \leq r' < |b|$

Т.е. $\exists$ два неполных частных q и q' и два остатка r и r' ($q \neq q'$) $\Rightarrow bq + r = bq' + r' \Rightarrow b(q - q') = r' - r$ …(*)

Т.к. $\begin{matrix}0\le r'<|b|\\ 0\le r<|b|\end{matrix}\Rightarrow |r'-r|<|b|$

С другой стороны, $|g-g'|>0\Rightarrow$ [illegible] $g\neq g'$ – противоречие, $\Rightarrow g=g'\Rightarrow r=r'$

Следствие:

Если $b\neq 0$, то b является делителем $a \Leftrightarrow$ остаток от деления a на b равен 0.

Определение 2. Число q называется **полным** или **неполным частным** в зависимости от того, равно ли r нулю или нет; r – остаток от деления.

2. НОД. Алгоритм Евклида. НОК

Определение 3. Всякое целое число $\delta\neq 0$, делящее одновременно целые a_1, ... , a_n над общим делителем этих чисел.

Определение 4. Общий делитель d целых чисел a_1, ... , a_n называется наибольшим общим делителем, если он делится на всякий общий делитель этих чисел, т. е.

1) $d/a_1,\dots d/a_n$

2) $\delta/a_1,\dots\delta/a_n\Rightarrow\delta/c$.

Предложение. НОД чисел a_1, ... , a_n определен однозначно с точностью до знака (т.е. если d – НОД чисел a_1, ... , a_n, то – d – тоже НОД этих чисел).

Доказательство: пусть d_1, d_2 - НОД чисел a_1, ... , $a_n \Rightarrow^{опр.1} d_1 \vdots d_2$ и $d_2 \vdots d_1$ (т. к. НОД делится на $\forall$ общий делитель этих чисел) $\Rightarrow^{св.12^\circ} d_1 = d_2$ или $d_1 = -d_2$.

В дальнейшем условимся рассматривать только положительные значения НОД и обозначать $d = (a_1, \dots, a_n)$.

Для нахождения НОД существует алгоритм, который был дан Евклидом. Описав способ нахождения НОД, мы доказываем тем самым существование НОД.

Алгоритм Евклида базируется на следующих леммах:

Лемма 1. Если $a \vdots b$, то $(a, b) = b$

Доказательство: 1) b/a и $b/b \Rightarrow b$ - общий делитель a и b.

2) пусть c - общий делитель a и b.

c/a, $c/b \Rightarrow c/b \Rightarrow^{опр.2} (a, b) = b$.

Лемма 2. Если $a = bq + r$, то $(a, b) = (b, r)$ $\quad r \neq 0$

Доказательство: пусть $(a, b) = d$, тогда

1) из d/a и d/b, $r = a - bq \Rightarrow^{св.7^\circ}$

2) δ/b и $\delta/r \Rightarrow \delta/a$, δ - общий делитель a и $b \Rightarrow$

$\Rightarrow \delta/d \Rightarrow d = (b, r)$.

$(a, b) = (b, r)$.

Алгоритм Евклида

Пусть a и b - положительные числа, $a>b>0$. Разделим a на b, по теореме о делении с остатком: $a=bq_0+r$, $0\le r_1<b$.

1°. $r_1=0$, т. е. $a \vdots b \Rightarrow^{п.1} d=b$.

2°. $r_1\neq 0$, то получаем ряд равенств:

$b=r_1 q_1+r_2$; $0<r_2<r_1$ (если $r_2=0$, то процесс заканчивается).

$r_1=r_2 q_2+r_3$ $\qquad 0<r_3<r_2$

- -

(I) $r_{n-2}=r_{n-1} q_{n-1}+r_n$ $\qquad 0<r_n<r_{n-1}$

$r_{n-1}=r_n q_n$

Процесс заканчивается, когда мы получаем $r_{n+1}=0$.

Последнее неизбежно, т. к. остатки, получаемые в процессе деления неотрицательны и убывают; следовательно, на каком-то шаге получим деление без остатка.

В силу леммы 2: $(a, b)=(b, r_1)=(r_1, r_2)=\ldots=(r_{n-1}, r_n)=r_n$.

Вывод: (a, b) двух чисел равен последнему неравному нулю остатку в процессе алгоритма Евклида.

Пример. Найти (185, 55) = 5.

Задача отыскания НОД конечного множества чисел $a_1, \ldots, a_n$ сводится к нахождению НОД для двух чисел.

Теорема 1. Если $(a_1, a_2)=d_2$; $(d_2, a_3)=d_3$, … , $(d_{n-1}, a_n)=d_n$, то $(a_1, \ldots, a_n)=d_n$. (Доказать самостоятельно).

Свойства НОД.

1°. Пусть $k\neq 0$, $k\in Z$.

$(ak, bk)=(a, b)\,k$

Применим алгоритм Евклида $\qquad ak=bk\,q_0+r_1 k$

$bk=r_1 k\,q_1+r_2 k$

- - - - - - - - - - - -

$r_{n-2}\,k=r_{n-1}k\,q_{n-1}+r_n k$

$r_{n-1}k=r_n k\,q_n$

$\Rightarrow (ak, bk)=r_n k=(a, b)\,k$.

2°. Пусть δ - любой общий делитель a и b, $\left(\frac{a}{\delta}; \frac{b}{\delta}\right)=\frac{(a,b)}{\delta}$

$(a, b)=\left(\frac{a}{\delta}\delta; \frac{b}{\delta}\delta\right)=\left(\frac{a}{\delta}; \frac{b}{\delta}\right)\delta \Rightarrow$ св.2°

Свойства НОК

Определение 5. Целое число $M\neq 0$ называется ОК чисел $a_1, \ldots, a_n$, если оно делится на $\forall$ из данных чисел.

Среди совокупности ОК чисел особую роль играет одно число, называемое НОК.

Определение 6.Целое число m называется **НОК** чисел a_1, ... , a_n, если

1) m - ОК(a_1, ... , a_n)

2) $\forall$ ОК этих чисел $\vdots m$, т.е. $a_1 \,/\, M$, $a_2 \,/\, M$, … , $a_n \,/\, M \Rightarrow M \vdots m$ ($m \,/\, M$).

Возникает вопрос о рациональном способе нахождения НОК. Один из практических способов – использование теоремы, которая устанавливает связь НОК и НОД.

Теорема. НОК двух чисел равно их произведение, деленное на НОД этих чисел.

$$[a,b]=\frac{a\cdot b}{(a,b)}.$$

Доказательство: пусть M =ОК$(a,b) \Rightarrow M = ak, k \in Z$.

M – кратно и $b \Rightarrow \frac{ak}{b} \in Z$.

Пусть $(a,b)=d \Rightarrow a = a_1 d,\ b = b_1 d$

$\frac{a}{b}\frac{k}{b_1}\frac{q}{d}\frac{d}{k}\frac{k}{b_1}\frac{q}{k} \in z$, $(a,b_1)=1 \Rightarrow k \vdots b_1$, т. е. $k = b_1 t = \frac{b}{d} t$, где $t \in Z \Rightarrow$

$\Rightarrow M = \frac{ab}{d} t.$

НОК получим при $t = 1.\ m = \frac{ab}{d};$ или $M = mt.$

Вывод:совокупность общих кратных двух чисел совпадает с совокупностью кратных их общего наименьшего кратного.

Простые числа

Всякое целое число, больше 1, имеет не менее 2-х делителей, именно 1 и само себя.

Определение 1. Натуральное число **p>1** называется **простым**, если p не имеет натуральных делителей, отличных от 1 и p.

Определение 2. Натуральное число **a>1** называется **составным**, если a имеет, по крайней мере, один натуральный делитель, отличный от **1** и **a**.

1 не является ни простым, ни составным (т.к. имеет всего один натуральный делитель).

Первые простые числа в натуральном ряду: 2**, 3, 5, 7, 11, 13, …**

Простые числа – это элементы, при помощи, умножения которых строятся натуральные числа (>1); поэтому одной из важнейших задач теории чисел является изучение свойств простых чисел.

Свойства простых чисел:

1. $p \vdots n,\ n \in N,\ n \neq 1 \Rightarrow p=n$

Доказательство: пусть $p \neq n \Rightarrow$ p имело бы 3 делителя 1, p, n, что невозможно, т.к. p- простое.

2.p_1, p_2 – различные простые числа $\Rightarrow p_2$ не $\vdots p_1$

Доказательство: p_2 – простое $\Rightarrow p_2$ имеет делитель 1 и p_2, но $p_2 \neq p_1 \Rightarrow p_2$

не $\vdots p_1$

3. $n \in N$, p – простое $\Rightarrow n \vdots p$ или (n, p)= 1

Доказательство: пусть (p, n)= d $\Rightarrow \frac{d}{p}$ p- простое число $\Rightarrow$ d= 1 или d = p, d = 1 $\Rightarrow$ (d, n) $\Rightarrow$ 1; d = p $\Rightarrow n \vdots d$, т.е. $n \vdots p$

4. $ab \vdots p \Rightarrow a \vdots p \vee b \vdots p$

Доказательство: если $a \vdots p$ – то утверждение теоремы справедливо, если a не $\vdots p \Rightarrow$ (a, p) = 1 $\wedge$ $ab \vdots p \Rightarrow b \vdots p$

5. Если произведение нескольких сомножителей $\vdots p$, то, по крайней мере, один из сомножителей $\vdots p$. (обобщение свойства 4)

Теорема 1. Для $\forall$ натурального числа **a>1** наименьший отличный от единицы делитель есть число простое.

Доказательство: пусть q – наименьший $\neq 1$ делитель натурального числа a>1; если бы q было составным, то оно имело бы некоторый делитель q_1, с условием $1 < q_1 < q$, но $a \vdots q$ и $\vdots q \Rightarrow a \vdots q_1$, а это противоречит предположению относительно q.

Теорема 2. Наименьший отличный от единицы делитель составного числа **a**(простой по теореме 1) не превосходит $\sqrt{}$**a.**

Доказательство: пусть q – это делитель $\Rightarrow a = q * a_1$, $a_1 \geq q$, откуда, перемножая и сокращая на a_1, получим $a \geq q^2$, $q \leq \sqrt{a}$.

Эта теорема дает критерий, позволяющий судить, является ли натуральное число a простым или составным.

Последовательность простых чисел неограниченна. Этот результат был получен еще Евклидом и помещен в 9 веке в книге его “Начал” в качестве 20-ой теории.

Теорема (Евклида). Множество простых чисел бесконечно.

Доказательство: предполагается, что множество простых чисел конечно и состоит из чисел 2, 3, . . ., p_r (*), где pr– последнее самое большое простое число.

Рассмотрим **$N = 2*3 \ldots p_r + 1$,** N> 1 $\Rightarrow$N- либо простое, либо составное

а) если N- простое; $N > p_i$, где $p_i \in \{2,3,\ldots p\}$ т.е. > любого простого числа (т.к. других простых не существует) $\Rightarrow$N- не может быть простым;

б) если N-составное; $N \vdots 2$, $N \vdots 3$, . . . , $N \vdots p \Rightarrow$ не $\vdots$ ни на одно простое число, т.е. не имеет делителей, отличных от 1 и N $\Rightarrow$ не составное.

$N \neq 1$, ни простое, ни составное – противоречие. ▲

Простые числа, хотя их и бесконечно много, составляют не большую часть всех натуральных чисел.

Контрольные вопросы:

1. Сформулируйте теорему о делении с остатком.
2. Дайте 2 формулировки теоремы Безу.
3. Что называется НОД двух чисел?

4. Перечислите свойства НОД.
5. В чём состоит алгоритм Евклида, как он применяется при нахождении НОД двух чисел?
6. Что называется НОК двух чисел?
7. Какие числа называются простыми, составными?
8. Какая формула связывает НОК и НОД двух чисел?
9. Конечно ли множество простых чисел?

Темы 13, 14. Сравнения в кольце Z

Цель:

1. Рассмотрение отношения сравнения в кольце Z.
2. Введение понятий полной и приведенной систем вычетов.
3. Доказательство теорем Эйлера и Ферма.
4. Формирование умений и навыков при решении практических задач.

План:

1. Отношение сравнения, свойства сравнений.
2. Полная и приведённая системы вычетов.
3. Функция Эйлера. Теоремы Эйлера и Ферма.
4. Сравнения первой степени с одним неизвестным.

1 Отношение сравнения, свойства сравнений

Пусть m – фиксированное натуральное число. Все целые числа по отношению к числу m разбиваются на m классов, если отнести к одному классу числа, дающие один и тот же остаток при делении на m. Числа, относящиеся к одному классу, называется сравнимыми, а теория, изучающая свойства классов, теорией сравнений.

Определение 1. Пусть m – натуральное число. Целые числа a и b называется **сравнимыми по mod m**, если их разность $a - b \vdots m$.

Запись $a \equiv b \pmod m$. Читается «a сравнимо с b по mod m».

Сравнение представляет собой соотношение между 3 числами: a, b и m, причем m играет своего рода эталона сравнения – называется модулем.

Определение 2. Целые числа a и b называется **сравнимыми по modm**, если остаток от деления этих чисел на m равны.

Предложение. Определения 1 – 2 равносильны.

Следствия.

1. $a \vdots m \Rightarrow a \equiv 0 \pmod m$
   Всякое число, кратное m, сравнимо с нулем по mod m.
2. $a = mg + r \Rightarrow a \equiv r \pmod{}$
   $0 \le r < m$

Всякое целое всегда сравнимо с остатком k, получающимся при делении его на m.

Свойства сравнений.

1^0. рефлексивность: $a \equiv a \pmod m$ $a \in Z$

$a - a = 0 \ m$

2^0. симметричность: $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

$a - b \vdots m \Rightarrow b - a \vdots m$

3^0. транзитивность: $a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

$a - b \vdots m \wedge b - c \vdots m \Rightarrow (a - c) + (b - c) = a - c \vdots m$

Вывод. Отношение сравнения на множестве Z по mod m является отношением эквивалентности => Z разбивается на непересекающийся между собой классы эквивалентности.

Эти классы – называются классами вычетов по модулю m или просто классами по mod m.

При этом числа из одного класса попарно сравнимы между собой, а числа из различных классов не сравнимы между собой => класс по mod m состоит из чисел, дающих один и тот же остаток при делении на m.

4^0.Сравнения по одному и тому же модулю можно почленно складывать (вычитать)

$a_1 \equiv b_1 \pmod m$

$a_2 \equiv b_2 \pmod m$

$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m$

$a_1 - b_1 \vdots m$

$\Rightarrow (a_1 \pm a_2) - (b_1 \pm b_2) = (a_1 - b_1) \pm (a_2 - b_2) \ m \ a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m$

$a_2 - b_2 \vdots m$

Следствия.

1.Любое слагаемое из одной части сравнения можно перенести в другую с противоположным знаком.

$a + b \equiv c \pmod m \Rightarrow a \equiv c - b \pmod m$

$-b \equiv -b \pmod m$

$a \equiv c - b \pmod m$

2. К любой части сравнения можно прибавить (отнять) число, кратное модулю.

$a \equiv b \pmod m \Rightarrow a \equiv b - mk \ (\dots m)$

$0 \equiv mk \ (\dots m)$

5^0 Сравнения по одному и тому же mod можно почленно перемножить.

$a_1 \equiv b_1 \pmod m$

$a_2 \equiv b_2 \ (\dots m)$

$a_1 a_2 \equiv b_1 b_2 \ (\dots m)$

$a_1 a_2 - b_1 b_2 = a_1 a_2 - b_1 b_2 + a_1 b_2 - b_1 b_2 = a_1 (a_2 - b_2) + b_2 (a_1 - b_1) \ m$

Следствия.

1)Обе части сравнения можно умножить на одно и то же число

$a \equiv b \ (\dots m) \Rightarrow ac \equiv bc \pmod m \Rightarrow a - b = mg \Rightarrow ac - bc \equiv m \ (gc)$

2) Обе части сравнения можно вознести в одну и ту же натуральную степень.

$a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$

6^0 Обе части сравнения можно сократить на множитель, взаимно простой с модулем.

$ac \equiv bc \pmod m \wedge (c, m) = 1 \Rightarrow a \equiv b \pmod m \Rightarrow ac - bc \ m \Rightarrow c(a - b) \ m \wedge (c, m) = 1 \Rightarrow a - b \ m$

7^0 Обе части сравнения и модуль можно умножить на одно и то же число.

$a \equiv b \pmod m, r \pmod m \in Z \Rightarrow ak \equiv bk \pmod{mr}$

$a - b = mg \Rightarrow ak - bk = (mr)g \ k \in Z$

8^0 Если $ak \equiv bk \pmod{mk} \Rightarrow a \equiv b \pmod m$ где r, m – произв. нат. ч.

Доказательство- самостоятельно.

$9^0 a \equiv b \pmod m \wedge md \Rightarrow a \equiv b \pmod m \Rightarrow a - bm$ и $md \Rightarrow a - bd$

$10^0 a \equiv b \pmod m \Rightarrow$ множество общих делителей a и m совпадает с множеством общих делителей b и m. В частности, (a, m) = (b, m)

$a - b \ \ m \Rightarrow a - b = mg$ и $b = a - mg$, т.е. общий делитель чисел, a и m является общим делителем чисел b и m и наоборот.

Поскольку пара a и m и пара b и m имеют одни и те же общие делители, то и (a, m) = (b, m).

Другими словами, если одна часть сравнения и модуль делятся на какое – либо число, то и другая часть сравнения должна на то же число

$a \equiv b \pmod m$

11^0 $a \equiv b \pmod{m1}$

$a \equiv b \pmod{m2}$

$a \equiv b \pmod{m_k}$ где $m \equiv [m_1, \ldots, m_k]$

12^0 Пусть f(x) – многочлен с целыми коэффициентами, $a \equiv b \pmod m \Rightarrow f(a) \equiv f(b) \pmod m$

Доказательство:

Пусть $f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$

$a \equiv b \pmod m \Rightarrow a^k \equiv b^k \pmod m$ $\quad k = 0, \ldots, n$

Умножая обе части на cn-k

$C_{n-k}a^k \equiv C_{n-k}b^k \pmod m$ $\quad k = 0, n$

Складывая полученные сравнения, получим $f(a) \equiv f(b) \pmod m$

2. Полная и приведенная системы вычетов

Определение 3. Полной системой вычетов по modm называется сисТемы чисел взятых по одному из $\forall$ класса по этому модулю.

Например: по mod 6 : 12,-13,2,63,-2,5

Поскольку в ПСВ число вычетов должно равняться числу классов,то $\forall$ класс содержит бесконечное множество вычетов, то можно составить бесчисленное множество различных полных систем вычетов по данному modm.

а) полная сисТемы наименьших неотрицательных вычетов 0,1, …., m-1 (в прим.0,1,2,3,4,5)

б) полная сисТемы абсолютно наименьших вычетов (составляется из наименьших по абсолютной величине) -2,-1,0,1,2,3

СВОЙСТВА

Теорема 1. Любая совокупность m чисел, попарно несравнимых по mod m есть полная системы вычетов по mod m

Теорема 2. Если (a,m)= 1 и x пробегает полную систему вычетов по mod m$\Rightarrow$ то числа вида ax+b тоже пробегают полную систему вычетов по mod m ($a,b \notin Z$)

Все числа одного и того же класса вычетов $\bar{a}$ по modm имеют с модулем m один и тот же НОД, равный (a,m).

В частности, если одно из чисел класса по mod m взаимно просто с m, то и все числа класса взаимно просты с mod m.

Определение 4. Класс вычетов $\bar{a}$ по mod m состоящий из чисел, взаимно простых с mod ,называется **примитивным классом**.

Для $\forall$го модуля примитивные классы существуют; такими будут, в часности классы $\bar{1}$, $\overline{m-1}$

Пример m=6;$\bar{1}$,$\bar{5}$

m=7: $\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}$

Число примитивных классов по mod m обозначается φ(m) и называется функцией Эйлера. Так, обратная функция Эйлера определяет число положительных (целых), не превосходящих m и взаимно простых с m (для m>1) $\varphi(6)=2$; $\varphi(7)=6$

Если mod—простое число p, то все классы, кроме нулевого, примитивны, так что $\varphi(p)=p-1$

Выберем из $\forall$ примитивного класса по mod m по одному числу, получим приведённую систему вычетов по mod m.

***Определение 5*. Приведенной системой вычетов** по некоторому mod m называется системы вычетов, взятых по одному из $\forall$го примитивного класса по этому модулю $\Rightarrow$ приведенную системе вычетов по mod m можно составить из полной системе вычетов по этому модулю, выписав все числа, взаимно простые с mod.

Если в качестве исходной взять полную систему наименьших неотрицательных или абсолютно наименьших вычетов, то указанным способом получим соответственно приведенной систему наименьших неотрицательных или абсолютно наименьших вычетов по mod m.

Теорема 3. $\forall$ совокупность φ(m) чисел (m>1), взаимно простых с mod m, и попарно несравнимых по mod m есть приведенная системы вычетов по mod m: $a_1,\dots a_{\varphi(m)}$ (1)

Теорема 4. Если (a, m) =1 и x прибегает приведенную систему вычетов по mod m, то ax тоже прибегает приведенную систему вычетов по mod m.

Функция Эйлера. Теоремы Эйлера и Ферма

Функция Эйлера $\varphi(a)$ определяется для всех натуральных чисел и представляет собой число чисел ряда 1,..,*a*-1, взаимно простых с*a*.
Найдем формулу для вычисления функции Эйлера.

Теорема.

Если $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ - каноническое разложение числа *a*, то

$$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

Теорема 2.

Пусть *p* – простое число, $\alpha \geq 1, \alpha \in N$, тогда $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Теоремы Эйлера и Ферма являются основой всей теории сравнений и находят широкое применение как в теоретических исследованиях, так и в арифметических приложениях.

Пример. $\varphi(200) = \varphi(2^3 \cdot 5^2) = 200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) =$

<u>Теорема Эйлера.</u>

Если (a,m)=1 $a^{\varphi(m)} \equiv 1 \pmod m$, $a \geq 1$ (I)

Доказательство: Рассмотрим мультипликационную группу классов вычетов, взаимно простых с modm: Gm.

Эта коммутативная группа содержит $\varphi(m)$ элементов. Применим к ней теорему Лагранжа, вернее следствие из этой теоремы.

Порядок $\forall$ элемента a конечной коммутативности группы G является делителем порядка этой группы, т.е. если конечная коммутативность группы состоит из κ элементов, то для $\forall$ элемента a этой группы выполниться равенство:

$$a^\kappa = \ell$$

Мы получили, что для $\forall$ класса $\bar{a} \in Gm$ выполняется равенство $\bar{a}^{\varphi(m)} = \bar{1}$ или (на языке сравнений) $a^{\varphi(m)} \equiv 1 \pmod m$

Особенно простой вид теорема Эйлера принимает в случае, если m=*p* – простое число. В этом случае φ(*p*)=*p*-1, а потому получаем

<u>Теорема Ферма</u>. Если *p* - простое число, и a - целое, неделящееся на *p, то*

(a,*p*)=1, то $a^{p-1} \equiv 1 \pmod p$ (II)

Другая формулировка теоремы Ферма: (Следствие)

Если p – простое число, то для $\forall$ целого a имеет место $a^p \equiv a \pmod p$

Действительно,

а) если (*a*,*p*)=1 умножим обе части сравнения (II) на a, получим $a^p \equiv a \pmod p$

б) если (*a*,*p*)≠1, то $a^p - a = a(a^{p-1}-1)$ также ⋮ на *p,* т.е. $a^p \equiv a \pmod p$

.Сравнение 1-ой степени с одним неизвестным

Любое сравнение 1 степени с 1 неизвестным можно привести к виду:

$ax \equiv b \pmod m$ (I)

$a \not\equiv 0 \pmod m$

Исследуем, в каких случаях сравнение будет иметь единственное решение, несколько решений или не иметь решений вообще.

Теорема 1. Если (a, m) = 1, то сравнение (1) имеет решение и притом единственное.

Доказательство: сравнение (1) имеет несколько решений, сколько вычетов полной системы вычетов ему удовлетворяет по mod m,

т.к. (a,m)=1 $\Rightarrow ax_1, ax_2, \ldots ax_n$ - также полная системы вычетов по этому модулю $\Rightarrow$ при одном и только одном значении x_i, взятым из полной системы вычетов, число ax_i будет сравнимо с b по mod m

$ax_i \equiv b \pmod m \Rightarrow$ сравнение (1) имеет единственное решение: $x \equiv x_i \pmod m$

Теорема 2. Если (a,m)=d>1 и b не $\vdots$ d, то сравнение (1) не имеет решений.

Доказательство:

пусть $x \equiv c \pmod m$ – решение сравнений (1) $\Rightarrow ac \equiv b \pmod m \Leftrightarrow ac - b \equiv mt(\ldots)$ $(t \in z) \Rightarrow ac - mt = b \wedge (a,m) = d \Rightarrow b \vdots d$

$\vdots d$

Полученное противоречие доказывает теорему.

Теорема 3. Если (a,m)=d>1и b$\vdots$d, то сравнение (1) имеет d различных решений, которые образуют класс вычетов по $\mod \frac{m}{d} = m_1$

Доказательство: т.к. a, b и m$\vdots$d, положим $a=a_1d$, $b=b_1d$, $m=m_1d \Rightarrow$ сравнение

$a_1x \equiv b_1(\ldots m_1)$ (2)

Где $(a_1, m_1)=1$, а значит (2) имеет единственное решение по мод m_1:

$x \equiv x_0 (\ldots m_1)$ или $x = x_0 + m_1t$ (любое $t \in z$), где x_0 - наименьший неотрицательный вычет по мод. m_1 или …… $x_0 - 2m_1, x_0 - m_1, x_0, x_0 + m_1, x_0 + 2m_1 \ldots x_0 + (d-1)m_1 \ldots x_0 + dm_1$ (3)

Все эти вычеты и только они удовлетворяют сравнение (2), а, значит и равносильны ему сравнение (1). По модулю $m_1 = \frac{m}{d}$ все эти числа принадлежат одному классу; по мод. $m = m_1d$ они будут принадлежать различным классам, вычетам которых являются: $x_0, x_0 - m_1, x_0 + 2m_1 \ldots x_0 + (d-1)m_1 \Rightarrow$ сравнение (1) имеет d различных решений по мод. m:

$x \equiv x_0 (\ldots m), x \equiv x_0, x_0 + m_1 (\ldots m),$

$x \equiv x_0 + 2\ m_1(\dots\ m), \dots, x \equiv x_0 + (d-1)\ m_1(\dots\ m)$, где x_0 частное решение.

Литература:

Контрольные вопросы:

1. Какие числа называются сравнимыми по модулю.
2. Какие свойства сравнений вы знаете?
3. Как определяется функция Эйлера? Дайте формулу для её нахождения.
4. Сформулируйте теоремы Эйлера и Ферма.
5. Что называется полной и приведённой сисТемыми вычетов.
6. Как определяется сравнение 1 степени с одним неизвестным?

Темы 15, 16. <u>Диофантовы уравнения.</u>

Цель:

1.Дать предысторию вопроса.

2.Рассмотреть неопределённые уравнения первой степени с одним неизвестным.

3.Формирование умений и навыков при решении практических задач.

План:

1. Диофантовы уравнения-предыстория вопроса.
2. Два этапа решения диофантовых уравнений.

Диофантовы уравнения-предыстория вопроса

Диофант представляет одну из наиболее трудных загадок в истории науки. Точные годы его жизни неизвестны. Промежуток времени, когда мог жить Диофант, составляет 500 лет, хотя имеются косвенные данные о том, что Диофант жил в 3 веке в Александрии- центра научной мысли эллистического мира. Выдающийся исследователь в области собственно теории чисел, Диофант не только поставил проблему решения неопределенных уравнений в рациональных числах, но и дал некоторые общие методы их решения. При этом надо иметь в виду, что в античной математике общие методы никогда не излагались в «чистом виде», отдельно от решаемых задач (т.е. нет общего абстрактного описания этих методов). Его арифметика алгебраических кривых состоит в нахождении рациональных точек алгебраических кривых (например, кривых 2-го порядка – рациональные решения одного алгебраического уравнения от 2-х переменных).

В “Арифметике” Диофанта происходит окончательный отказ от геометрической алгебры. Но это вовсе не означало, что алгебра вернулась к тому состоянию, которое было у неё в Вавилоне. В “Арифметике” алгебра обрела новый язык, гораздо более оперативный и удобный, чем язык геометрии.

Именно здесь родилась буквенная алгебра (ввел алгебраические символы для первых шести положительных и отрицательных степеней неизвестных,

для обозначений вычитания и равенства), расширил числовую область для поля рациональных чисел.

Диофант был последним великим математиком античности. Античная наука и культура погасли вместе с гибелью всего античного общества.

Его методы были поняты и применены для решения новых задач Виетом и Ферма. Проблемой решения неопределенных уравнений в целых числах занимались также Эйлер, Лагранж и Лежандр (и которой продолжают заниматься и теперь).

Область математики, выросшая из задач решения неопределенных уравнений, получила название диофантова анализа (теперь чаще называют диофантовой геометрией).

Определение1. **Неопределенными уравнениями** 1-ой степени с с 2-мя неизвестными с целыми коэффициентами называются уравнения вида

$$ax + by = c, \qquad (1)$$ где $a,b,c \in Z$, $a \neq 0$, $b \neq 0$

Уравнения с несколькими неизвестными, как правило, имеет бесконечное множество решений, поэтому такие уравнения называются неопределенными.

В случае, если c=0, то (1) называется неоднородным (или с правой частью). Уравнение (2) с теми же значениями параметров a и b называется однородным, соответствующим данному неоднородному (1).

Одним из возможных случаев является решение уравнения (1) в области R: уравнение (1) является уравнением прямой $\Rightarrow$ совокупность решений уравнений (1) в R изображается прямой, если $\forall$ - му решению <x,y> можно поставить в соответствии точку M (x,y)$\Rightarrow$ этот случай относится к аналитической геометрии.

В области Q: уравнение (1) решается очень просто: полагая x=t (t-параметр, принимается всевозможные рацион. значения), из уравнения находится $У = \frac{c - at}{b} \in Q \Rightarrow$ все решения в рацион. числах имеют вид (3) x=t; $У = \frac{c - at}{b}$

Наиболее интересным и естественным случаем является решение уравнения (1) в целых числах, которые решаются в теории чисел.

Определение 2. **Решением в целых числах** неопределенных уравнений (1) называется пара (x_0, y_0) целых чисел, удовлетворяющих этому уравнению (т.е числа, которые при подстановке в уравнение дают верное числовое равенство $ax_0+by_0=c$).

Всякое отдельное решение (x_0, y_0) уравнения (1) называется частным; общее решение состоит из всевозможных частных (совокупность всех частных).

Итак, задача – найти все целочисленные решения уравнения (1). Соотношения (3) не могут дать в общем случае

решение этой задачи, т.к. при целочисленных значениях параметра t значения У=$\frac{c-at}{b}$ не обязательно будут целыми.

Теорема 1. Неопределенное уравнение (1) первой степени с 2-мя неизвестными с целыми коэффициентами не имеет решений в целых числах, если правая часть не делится (a, b) =d

(a,b) =d >1 $\wedge \overline{c \vdots d} \Rightarrow$ не имеет решений.

Доказательство: пусть (x_0,y_0) - решение уравнения (1) $\Rightarrow$ должно выполнятся числовое равенство $ax_0+by_0=c \Rightarrow$ т.к. (a,b)=d$\Rightarrow$

$c \vdots d$, что противоположит условию.

Если (a,b)=d>1 и $c \vdots d \Rightarrow$ сократив обе части уравнения (1) на d мы получим равносильное уравнение $a_1x+b_1y=c_1$,где (a_1,b_1)=1, т.е этот случай сводится к уравнению: ax+by=c, где (a,b)=1

Итак, если

1^0 (a,b)=d>1 и $\overline{c \vdots d} \Rightarrow$

2^0 (a,b)=d>1 и $c \vdots d \Rightarrow$

3^0 (a,b)=1 (ax+by=c) (*)

2. Два этапа решения диофантовых уравнений

Процесс нахождения целочисленного решения распадается на 2 этапа:

I. Доказательство того, что уравнение (1) имеет частное решение и указание способов получения этого решения.

I. Нахождение общего решения.

I этап. Нахождение **ч**астных решений.

Отыскание целочисленного решения тесно связано с решением сравнений.

Теорема 2. Если (x_0, y_0) – целочисленное решение уравнения (1), $a \neq 0$, $b \neq 0$, то x_0- решение уравнения $ax \equiv c(\mathrm{mod}\, b)$.

Обратно, если x_0 – решение сравнения (4), то существует $y_0 \in Z$, что (x_0, y_0) – решение неопределенного уравнения (1).

Доказательство: 1) пусть (x_0, y_0) – одно из целочисленных решений уравнения ax+by=c $\Rightarrow$ $ax_0 - c = -by_0 \vdots b \Rightarrow ax_0 \equiv c(\mathrm{mod} b) \Rightarrow x_0$ – решение срав. (4).

2) пусть x_0 – решение сравнения (4) $\Rightarrow$ [illegible], где y_0 [illegible] - целочисленное решение уравнения ax+by=c.

В частности, из полученных выше утверждений о сравнениях 1 степени получаем:

Следствие 1:

Если (a,b)=d, то неопределенное целочисленное решение ax+by=c, имеет целочисленное решение $\Leftrightarrow c \vdots d$

Нахождение частного решения с помощью линейного представления НОД:

Рассмотрим ax+by=1.

Обозначим x_0, y_0 – его решениями. Если (a,b)=1 $\Rightarrow \exists\, x, y \in Z$, что выполняется ax+by=1, частное решение неопределенного уравнения (*) примет вид (x_0c, y_0c).

II этап: нахождение общего решения.

Теорема 3. Если неопределенное уравнение (*) с целыми коэффициентами, где (a, b)=1, имеет частное целочисленное решение (x_0, y_0), то общее решение этого уравнения имеет вид

(**) $\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases} t \in Z$

Доказательство: 1) покажем, сначала, что при $\forall$ целом $t \in Z$ формулы (**) дают некоторое решение неопределенного уравнения (*),

Пусть t – какое-либо целое число $\Rightarrow$

$x' = x_0 + bt, t \in Z$

$y' = y_0 - at$

Непосредственная проверка показывает, что, $a(x_0+bt)$ +

$+b(y_0-at) = ax_0+by_0=c$, т.к. (x_0, y_0) – одно из решений уравнения (*).

2. Обратно, $\forall$ решение неопределенного уравнения (*) может быть записано в виде формулы (**), т.е. эти исчерпываются все целочисленные решения уравнения (*).

Пусть (x_1, y_1) – произвольное решение уравнения (*), тогда

$ax_1+by_1=c$ и $ax_0+by_0=c$,

$a(x_0-x_1) +b(y_0-y_1) =0$

$a(x_0-x_1) =-b(y_0-y_1)$

$\vdots a$ и (a, b) =1

 , $t \in Z$

Подставляем найденное значение y_1 в (5), получим $a(x_0-x_1)=-bat \Rightarrow$

$x_1=x_0+bt$, теорема доказана.

Контрольные вопросы:

1. Дайте определение неопределённого уравнения первой степени с двумя неизвестными.
2. Какие диофантовы уравнения называются однородными и неоднородными?
3. Что называется частным решением неопределённого уравнения?
4. Укажите 2 этапа решения диофантовых уравнений.

Темы 17, 18. <u>Алгебра высказываний.</u>

Цель:

1. Дать сведения из истории математической логики.
2. Введение основных понятий математической логики.
3. Формирование умений и навыков при решении практических

задач.

План:

1. Высказывание. Примеры.
2. Операции над высказываниями.
3. Задание функций алгебры высказываний таблицами.

Введение

Термин "логика" происходит от греческого слова □□□□□ (логос), что означает "мысль", "разум". Логика (или формальная логика) как наука изучает мышление (как и психология, физиология, кибернетика, педагогика и т.д., которые изучают какие-нибудь стороны сложного процесса мышления.

Логика есть наука о законах и формах правильного мышления. Классическая (формальная) логика возникла в глубокой древности, в трудах древнегреческого философа Аристотеля (384 - 322 г. до н.э.) и его последователей. (Он впервые разработал теорию дедукции, т.е. теорию логического вывода).

1 Высказывание. Примеры.

В каждой математической теории изучаются различные утверждения, касающиеся объектов этой теории. При помощи тех или иных рассуждений устанавливается справедливость (истинность) одних утверждений об этих объектах и неверность (ложность) других. В любой теории выделяется класс утверждений, который по законам этой теории является либо истинным, либо ложным. Такие утверждения называют постоянными высказываниями (или просто высказываниям).

Определение. **Высказыванием** называется любое повествовательное предложение, которое является либо истинным, либо ложным (но не тем или другим одновременно).

Высказывания могут быть выражены с помощью слов, а также маТемытических и других знаков.

Пример: 1) “2+5=1” - *и*

2) “14:3” - *л*

Не всякое предложение является высказыванием. Например, восклицательное и вопросительное предложения высказываниями не являются. Не являются высказываниями и определения, которые фиксируют принятое использование терминов.

Высказывание, которое можно разложить на части, будем называть сложным, а неразложимое далее высказывание – простым (элементарным)

Обозначаются высказывания большими латинскими буквами А.В.С, а их значения (*и* или *л*) соответственно 1 или 0.

Логические операции

Все утверждения какой–либо математической теории строятся из некоторых исходных утверждений данной теории с помощью ряда стандартных логических операций.

Каждая из этих операций одному или нескольким утверждениям ставит в соответствие новое утверждение с определенным значением истинности, благодаря чему мы сможем образовывать новые, более сложные высказывания.

Определение2. **Конъюнкцией** 2-х высказываний А и В называется такое третье высказывание А^В, кот. <=> А и В – *и*.

В обычной речи этой операции соответствует союз «*и*» (читается «А» и «В»). Таблица истинности:

А	В	А^В
И	И	И
И	Л	Л
Л	И	Л
Л	Л	Л

Пример:

1) «8:2 и на 4».
2) «Число 12 четное и простое».

Определение 3. **Дизъюнкцией** 2-х высказываний А и В называется такое третье высказывание, которое *л* <=> оба высказывания А и В – *л*. Обозначается – v.

В обычной речи соответствует союз «или». Читается «А или В».

Таблица истинности:

А	В	АvВ
И	И	И
И	Л	И
Л	И	И
Л	Л	Л

Пример: «точка А лежит на прямой или на плоскости».

Определение 4. **Импликацией** 2-х высказываний А и В называют такое третье высказывание А→В, которое *л* <=> А-*и*, В-*л*.

Читается «Из А следует В», «если А, то В», А называется посылкой, В-заключением. «А влечет за собой В»

Таблица истинности:

А	В	А→В
И	И	И
И	Л	Л
Л	И	И
Л	Л	Л

Такой связкой мы пользуемся чаще всего, когда формулируем какую-либо теорему.

Пример: «Если число 48 кратно 8, то оно кратно 4». $A \equiv u$; $B \equiv u \Rightarrow A \rightarrow B \equiv u$.

Определение 5. **Эквивалентностью** двух высказываний А и В называют такое третье высказывание, которое *и* <=> оба высказывания принимают одинаковые значения (либо *и*, либо оба – *л*).

Читается: «А тогда и только тогда, когда В». «Для того, чтобы А, необходимо и достаточно, чтобы В». «В том и только в том случае».

Таблица истинности:

А	В	А↔В
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

Пример: «Для того, чтобы число $\vdots 3$ <=> чтобы сумма цифр этого числа $\vdots 3$»

Формулировка этой теоремы заключает в себе 2 импликации:

1) А→В (условие и заключение меняются местами)
2) В→А

***Определение 6*.** **Отрицанием** высказывания А называется такое высказывание $\overline{A}$, которое *л*, когда А-*и*, и истинно, когда А-*л*.

Обозначается $\overline{A}$. Читается: «не А». «Неверно, что А».

Пример: Например, ”2<3”.

$\overline{"2 < 3"}$ - “неверно, что $2 \geq 3$” или: “2 не <3”.

Таблица истинности:

А	$\overline{A}$
И	Л
Л	И

Если операции $\wedge u \vee$ таковы, что могут соединять между собой совершенно независимые друг от друга высказывания, то при импликации высказываний значения истинности одного может влиять на истинность другого. Импликация «Если данный Δ равнобедренный, то все его стороны равны», значение истинности второго высказывания зависит от истинности первого.

1) Если Δ - равносторонний, то В- истинное высказывание.
2) Если Δ - не равносторонний, то В- ложное высказывание.

Контрольные вопросы:

1. Что называется высказыванием? Дайте примеры высказываний.
2. Какие логические операции вы знаете. Какими таблицами истинности они определяются?

3. Всегда ли логические операции применяют к связанным друг с другом высказываниям по смыслу?
4. Какие из данных логических операций являются бинарными?

Темы 19, 20. Формулы. Равносильность формул. Классы формул.

Цель:
1. Введение понятия формулы алгебры высказываний.
2. Изучение основных законов булевой алгебры.
3. Рассмотрение классов логических формул.
4. Формирование умений и навыков при решении практических задач.

План:
1. Формулы алгебры высказываний, их равносильность.
2. Основные равносильности (законы булевой алгебры)
3. Классификация логических формул.

1. Формулы алгебры высказываний, их равносильность

При помощи операций $\wedge, \vee, \rightarrow, \leftarrow$ мы можем образовывать новые сложные высказывания.

Определение 1. Всякое сложное высказывание, составленное из некоторых исходных элементарных операций, мы будем называть **формулой** алгебры высказываний.

Если мы зададим значения всех переменных элемент. Высказываний, то сама формула примет определенное значение. Таким образом, каждая формула определяет некоторую функцию, аргументами которой является переменные элементарные высказывания.

Определение 2. Две формулы F_1 и F_2 называются **равносильными (эквивалентными)**, если при любых значениях переменных высказываний, входящих в них, эти формулы принимают одинаковые значения (и или *л*).

Обозначать: $F_1 = F_2$, $F_1 <=> F_2$

Любое сложное высказывание (формула) определяет функцию, аргументы которой принимают значения *и* или *л* (независимо друг от друга), а значение самой функции также принадлежит множеству {*и, л*}. Такие функции называют булевыми функциями.

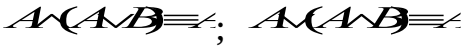
Пр. $F(x,y) = (x \wedge y) \rightarrow y$

2. Законы булевой алгебры. (Основные равносильности)

Пусть A, B, C – булевы функции некоторого фиксированного числа переменных.

1. Коммутативность: $A \wedge B = B \wedge A$; $A \vee B = B \vee A$
2. Ассоциативность: $A \wedge (B \wedge C) = (A \wedge B) \wedge C$; $(A \vee B) \vee C = A \vee (B \vee C)$

3. Дистрибутивность:  ;

4. Законы де Моргана: $\overline{A \wedge B} \equiv \overline{A} \vee \overline{B}$; $\overline{A \vee B} \equiv \overline{A} \wedge \overline{B}$
5. Закон двойного отрицания (инволюции): $\overline{\overline{A}} \equiv A$
6. Законы поглощения:  ;
7. Законы идемпотентности: $A \vee A \equiv A$; $A \wedge A \equiv A$
8. Закон исключенного третьего: $A \vee \overline{A} \equiv и$;
9. Закон противоречия: $A \wedge \overline{A} \equiv л$;
10. $A \wedge и \equiv A$; $A \vee и \equiv и$;
$A \wedge л \equiv л$; $A \vee л \equiv A$;
11. $A \to B \equiv \overline{A} \vee B$
12. 

Основные равносильности позволяют производить над формулами преобразования, приводящее их к более простому или более удобному виду.

При упрощении записи можно опускать скобки, считая, что $\wedge$ (т.е. логическое умножение) предшествует $\vee$ (т.е. логическому сложению), а $\wedge и \vee$ предшествует $\to, \leftrightarrow$. (или, говорят еще «Связывает сильнее»).

3.Классификация логических формул

В формулах можно произвести некоторые сокращения или упрощения, приняв во внимание тот факт, что некоторые части формулы могут принимать при любых значениях переменных высказываний постоянные значения либо *и*, либо *л*, а поскольку истинные или ложные формулы ведут себя в некоторых случаях как единицы или нули, то их можно соответственно отбросить, пользуясь форм.

Естественно, возникает вопрос о выделении тождественно-истинных, тождественно ложных формул.

Определение 3. Формула называется **тождественно -истинной (общезначимой)** или **(тавтологией**), если при всех значениях, входящих в нее переменных высказываний она принимает значение *и*.

Пример: $x \vee \overline{x} \equiv и$; 

Определение 4. Формула называется **тождественно- ложной (или противоречием)**, если при всех значениях, входящих в нее переменных высказываний она принимает значение *л*.

Пример: $x \wedge \overline{x} \equiv л$

Определение 5. Формула называется **выполнимой**, она принимает значение и при некоторых значениях, входящих в нее переменных высказываний.

Пример: $X \vee \overline{y}$; $x \to \overline{x}$

Значение формулы F при конкретном наборе значений входящих в нее элементарных высказываний обозначается: I(F)

Теорема 1: Пусть F-некоторая формула.

Тогда 1. если F-тавтология $\Rightarrow \overline{F}$ -противоречие.

2. если F- противоречие $\Rightarrow \overline{F}$ - тавтология.

Доказательство: очевидно из определений.

Теорема 2: Если формулы F и F$\rightarrow$Q-тавтологии, то формула Q-тавтология.

*Доказательство:*от противного.

Пусть I(Q)$\equiv$*л,* I(Q)$\equiv$*и (по усл.)*$\Rightarrow$ I(F$\rightarrow$Q)=*л*, противоречит предложению, что F$\rightarrow$Q- тавтология.

Заключение:

При рассмотрении логических связок нас интересует только логические значения, (или значения истинности высказываний, а не их содержание. Поэтому любое из введенных высказываний можно рассматривать как определение некоторой операции на двухэлементном множестве {0,1}.

0^0=0 0^1=1^0=0 1^1=1

Контрольные вопросы:

1. Что называется формулой алгебры высказываний?
2. Какие формулы алгебры высказываний называются равносильными?
3. Сформулируйте основные законы булевой алгебры.
4. Какие основные аристотелевские законы вы знаете?
5. Дайте определение основных классов логических формул. Приведите примеры.
6. Сформулируйте связь между основными классами логических формул.

Темы 21, 22. <u>Тавтологии алгебры высказываний. Нормальные формы.</u>

Цель:

1. Рассмотрение проблемы разрешимости и закона двойственности.
2. Введение понятия тавтологии и правил их получения.
3. Введение понятий ДНФ, КНФ, СДНФ, СКНФ.
4. Формирование умений и навыков при нахождении нормальных форм и представление формул алгебры высказываний СДНФ, СКНФ.
5. Формирование умений и навыков при определении тавтологий алгебры высказываний.

План:

1. Закон двойственности.
2. Проблема разрешимости.
3. Основные тавтологии. Правила получения тавтологий.
4. Нормальные формы: ДНФ, КНФ.
5. Совершенные нормальные формы: СДНФ, СКНФ.

Закон двойственности

Будем рассматривать формулы, содержащие только операции $\vee, \wedge, -$, (всякая формула может быть приведена преобразованиями равносильности к такому виду).

Определение. Операция $\wedge$ называется **двойственной** к операции $\vee$ и наоборот. Две **формулы** F и F^* называются **двойственными**, если одна получается из другой заменой каждой операции на двойственную.

Пример: $F=(X \vee \overline{Y}) \wedge Z$; $F^*=(X \wedge \overline{Y}) \vee Z$.

Из равносильности (законов де Моргана) легко вывести следующее положение:

$$(1) \quad \overline{F}\ (X_1,\ldots,X_n) \equiv F^*(\overline{X}_1,\ldots,\overline{X}_n).$$

Из этого соотношения вытекает закон двойственности:

Закон двойственности: Если формулы F и F_1 равносильны, то и двойственные им формулы F^* и F^*_1 также равносильны.

$$(2) \quad F \equiv F_1 \Rightarrow \quad F^* \equiv F^*_1 \qquad\qquad F^*(X_1,\ldots,X_n) \equiv \overline{F}^*(\overline{X}_1,\ldots,\overline{X}_n).$$

Пример: $F=A \vee B \quad \Rightarrow \quad F^*=A \wedge B \quad \Rightarrow \overline{F}(\overline{X}_1,\ldots,\overline{X}_n)=\overline{\overline{A} \vee \overline{B}}$

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

$F \equiv F_1 \Rightarrow F(\overline{X}_1,\ldots,\overline{X}_n) \equiv F_1(\overline{X}_1,\ldots,\overline{X}_n)$

(1) $X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)$ (2) $X \vee (Y \wedge Z) \equiv (X \vee Y) \wedge (X \vee Z)$

Если применять к формуле F дистрибутивный закон (1) и получим формулу F_1, то переход от двойственной формулы F^* к двойственной формуле F^*_1 осуществляется применением (2) дистрибутивного закона (дистрибутивные преобразования).

Переход от F^* к F^*_1 будем называть преобразованием, двойственным преобразованию, переводящему F в F_1.

$F \to F_1 \Rightarrow F^* \to F^*_1$

Тавтологии

Тавтологии представляют собой схемы построения истинных высказываний, независимо от содержания и истинности составляющих высказываний. Для определения истинных определенных высказываний необходимо обладать специальными знаниями, вывод об истинных других делаем, исходя не из их содержания, а из их формульной структуры.

Основное значение тавтологии состоит в том, что некоторые из них представляют правильные способы умозаключения, т.е. такие, которые от истинных посылок всегда приводит к истинным выводам.

Именно такие знания и обогащают их истинными сведениями.

Любая тавтология алгебры высказываний вида $F \to ØG$ составляет некоторой общей схеме логического умозаключения.

Пример: Рассмотрим тавтологию:

$((\overline{x} \to y) \Lambda (\overline{x} \to \overline{y})) \to x$

Схема логического умозаключения, описываемая данной тавтологией, часто используется в математических доказательствах.

Основные тавтологии

Рассмотрим тавтологии, выражающие свойства логических операций, и те, на которых основаны некоторые схемы математических доказательств.

1.1. закон исключение третьего

$$\models X \vee \bar{X}$$

1.2. закон отрицания противоречия

$$\models X \wedge \bar{X}$$

1.3. закон двойного отрицания

$$\bar{\bar{X}} \equiv X$$

1.4. закон тождества: $X \to X$

1.5. закон контрапозиции

$$(X \to Y) \equiv (\bar{Y} \to \bar{X})$$

1.6. закон силлогизма (правило ценного заключения)

$$((X \to Y) \wedge (Y \to Z)) \to (X \to Z)$$

1.7. закон противоположности

$$(X \equiv Y) \equiv (\bar{X} \equiv \bar{Y})$$

1.8. правило добавления антецедента («истина из чего угодно»)

$$X \to (Y \to X)$$

1.9. правило «из ложного что угодно»

$$\bar{X} \to (X \to Y)$$

1.10. правило «modus ponens»

$$(X \wedge (X \to Y)) \to Y$$

1.11 правило «modus tollens»

$$(\bar{Y} \wedge (X \to Y)) \to \bar{X}$$

1.12. правило перестановки посылок

$$(X \to (Y \to Z)) \equiv (Y \to (X \to Z))$$

1.13. правило объединения (и разъединения) посылок

$$(X \to (Y \to Z)) \equiv ((X \wedge Y) \to Z)$$

1.14. правило разбора случаев

$$((X \to Z) \wedge (Y \to Z) \equiv ((X \vee Y) \to Z$$

1.15. правило приведение к абсурду

$$((X \to Y) \wedge (X \to \bar{Y}) \to \bar{X}$$

$$(X \to (Y \wedge \bar{Y})) \to \bar{X}$$

Следующие тавтологии выражают свойства логических операций.

I. Свойства конъюнкции и дизъюнкции.

2.1. закон идемпотентности

$$\models P \wedge P \equiv P,\ P \vee P \equiv P$$

2.2. закон упрощения

$$\models (P \wedge Q) \to P;\ P \to (P \to Q)$$

2.3. закон коммутативности

$$\models P \wedge Q \equiv Q \wedge P;\ P \vee Q \equiv Q \vee P$$

2.4. законы ассоциативности:

$$\models (P \vee Q) \vee R \equiv P \vee (Q \vee R);$$

2.5. законы дистрибутивности:

$$P \wedge (Q \vee P) \equiv (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge P) \equiv (P \vee Q) \wedge (P \vee R)$$

2.6. законы поглощения.

$$P \wedge (P \vee Q) \equiv P;\ P \vee (P \wedge Q) \equiv P$$

2.7. законы де Моргана:

$$\models \overline{P \wedge Q} \equiv \overline{P} \vee \overline{Q};\ \overline{P \vee Q} \equiv \overline{P} \wedge \overline{Q}$$

Свойства импликации и эквивалентности

3.1. $(P \to (Q \to P)) \to ((P \to Q) \to (P \to R))$
3.2. $P \to (Q \to (P \wedge Q))$
3.3. $(P \to R) \to ((Q \to R) \to ((P \vee Q) \to R))$
3.4. $(P \to Q) \to ((P \to \overline{Q}) \to \overline{R}$
3.5. $(Q \to (P \to Q)) \to \overline{P}$
3.6. $(P \wedge (P \vee Q)) \to Q$
3.7. $(P \to Q) \to ((P \vee R) \to (Q \vee R))$
3.8. $(P \to Q) \to ((P \wedge R) \to (Q \wedge R))$
3.9. $(P \to Q) \to ((Q \to R) \to (P \to R))$
3.10. $(P \to Q) \vee (Q \to P)$
3.11. $(Q \to P) \to ((Q \to \overline{P}) \to Q)$
3.12. $((P \to Q) \wedge (R \to Q)) \equiv ((P \vee R) \to Q$
3.13. $(((P \to Q) \wedge (P \to R)) \equiv (P \to (Q \wedge R))$
3.14. $P \equiv P$
3.15. $(P \equiv Q) \equiv (Q \equiv P)$
3.16. $((P \equiv Q) \wedge (Q \equiv R)) \to (P \equiv R)$

Основные правила получения тавтологии

Рассмотрим правила, которые позволяют получать новые тавтологии

Теорема 1. (правило заключения) правило «modus ponens»

Если формулы F и $F \to$ не являются тавтологиями, то формула H также тавтология.

$\models F \wedge \models F \to H \equiv \models H$

Теорема 2. (правило подстановки)

Если формула F, содержащая переменная X, является тавтологией, то подстановка в формуле F вместо переменной X любой формулы H снова приводит к тавтологии.

$\models F \equiv S^{H} F^{x}$

Пример:

$\models X \to (У \to X)$ подставим формулу $(x_1 \wedge \overline{x_2})$ вместо X, получим тавтологию $\models (x_1 \wedge \overline{x_1}) \to (У \to (x_1 \wedge \overline{x_2}))$

Замечания. Правило подстановки позволяет рассмотреть $\equiv$ из тавтологии, приведенных выше, не как отдельно взятую тавтологию, а как схему образования тавтологии.

Например, тавтология 3.2. представляет бесконечное множество тавтологий вида $\models F_1 \to (F_2 \to (F_1 \wedge F_2))$, где F_1, F_2 – произвольные формулы алгебры высказываний.

Помимо этих основных правил существуют и другим, которым мы будим называть вторичными.

Проблема разрешимости

Мы рассматривали способы позволяющие выяснить, является ли формула F тождественно-истинной, тождественно-ложной или выполнимой и тогда этот вопрос автоматически решается для $\overline{F}$.

Если $\overline{F}$ оказалась тождественно-истинной $\Rightarrow$F -тождественно-ложная (не выполнимая).

Если $\overline{F}$ не является тождественно-истинной $\Rightarrow$F- не тождественно-ложная $\Rightarrow$ будет выполнимой.

Постановленная задача носит название **«проблемы разрешимости»**.

(Она ставится не только для алгебры высказываний, но и для других логических систем).

Для алгебры высказываний эта проблема легко решается.

1. Пусть F (X_1…, Xn) – формула для алгебры высказываний, содержащая элементарные высказывания X_1…, Xn.

Эта формула определяет некоторую функцию переменных X_1…, Xn, которые могут принять два значения.

Число всевозможных комбинаций значения переменных X_1…, Xn конечно и равно в точности 2^n: для любых комбинаций значений переменных выясняется её значение (например, таблично).

Изложенный способ дает принципиальное решение проблемы разрешимости, но предполагает большое число испытаний.

2.Существует другой способ, основанный на приведении формул к так называемой «нормальной форме».

Определение1. Назовем **элементарным произведением** ($\wedge$) (соответственно **элементарной суммой** ($\vee$)) произведение (сумму) переменных и их отрицаний.

$$X \wedge \overline{Y} \wedge Z \qquad X \vee \overline{Y} \vee Z$$

элементарное произведение — элементарная сумма

Теорема 1.*Чтобы элементарная сумма была тождественно-истинной,* $\Leftrightarrow$ *в ней хотя бы одна пара слагаемых, из которой одно есть некоторое переменное, а другое – его отрицание.*

$Y \vee Z \vee X \vee \overline{X} \equiv$и , где $X \vee \overline{X} \equiv$и.

Теорема 2.*Чтобы элементарное произведение было тождественно-ложным,* $\Leftrightarrow$ *в нем содержалась хотя бы одна пара множителей, из которых один является отрицанием другого.*

$Y \wedge Z \wedge X \wedge \overline{X} \equiv$и , где $X \wedge \overline{X} \equiv$л.

Нормальные формы для формул алгебры высказываний

Для каждой формулы алгебры высказываний можно указать равносильную ей формулу, содержащую из логических связок лишь отрицание, конъюнкцию и дизъюнкцию (для чего $\to, \leftrightarrow$ выразить через $\vee, \wedge$).

Выразить данную формулу через $\bar{}, \vee, \wedge$ возможно несколькими способами.

Пример: 

Среди всевозможных выражений данной формулы через $\vee, \wedge,$ некоторые играют важную роль, как в алгебре высказываний, так и в ее приложениях.

Определение 2. **Конъюнктивным одночленом** от переменных $X_1 \ldots, X_n$ называется конъюнкция этих переменных или их отрицаний.

Пример:  - элементарное произведение.

Определение 3. **Дизъюнктивным одночленом** от переменных $X_1 \ldots, X_n$ называется дизъюнкция этих переменных или их отрицаний.

Пример:  - элементарные суммы.

Определение 4. **Конъюнктивной нормальной формой** (КНФ) называется конъюнкция дизъюнктивных одночленов (или произведение элементарных сумм)

Пример: 

Определение 5. **Дизъюнктивной нормальной формой** (ДНФ) называется дизъюнкция конъюнктивных одночленов (или сумма элементарных произведений)

Пример: 

Всякая формула обладает как дизъюнктивной, так и конъюнктивной нормальными формами. От одной формы к другой можно перейти, используя законы де Моргана и дистрибутивные свойства. Очевидно, что у данной формулы F существует неограниченно много как дизъюнктивных, так и конъюнктивных нормальных форм (одни из них более громоздкие и сложные, другие более простые)

Пример: Найти КНФ и ДНФ:

и т. д. Среди множества ДНФ и КНФ существует единственная уникальная форма (для данной формулы): СДНФ и СКНФ.

Определение 6. **Одночлен** (конъюнктивный или дизъюнктивный) от переменных $X_1 \ldots, X_n$ называется **совершенным**, если в него входит либо сама переменная, либо ее отрицание.

Определение 7. Нормальная форма (дизъюнктивная или конъюнктивная) называется **совершенной**, если в нее входят лишь совершенные одночлены (конъюнктивные или дизъюнктивные) от этих переменных.

Пример. СКНФ от переменных X_1, X_2:

Контрольные вопросы:

1. Какие операции называются двойственными?
2. Какие две формулы называются двойственными?
3. Что представляют собой тавтологии?
4. Какие основные тавтологии вы знаете?
5. Сформулируйте основные правила получения тавтологий.
1. В чем суть проблемы разрешимости?
2. Что называется элементарным произведением, элементарной суммой?
3. Что называется дизъюнктивным и конъюнктивным одночленами?
4. Что называется дизъюнктивной и конъюнктивной нормальными формами?
5. Как определяется совершенный одночлен?
6. Какая нормальная форма называется совершенной?

Темы 23,24. Логическое следование

Цель:

1. Введение понятия логического следования.
2. Рассмотрение признаков логического следования.
3. Рассмотрение правил логических умозаключений.
4. Формирование умений и навыков при построении буквенной формы силлогизма и определение её правильности.
5. Построение исчисления высказываний в виде формальной аксиоматической теории.
6. Рассмотрение правила вывода ИВ.
7. Доказательство закона, исключенного третьего.
8. Использование теоремы дедукции и её следствий.
9. Рассмотрение теоремы о выводимости тавтологий.
10. Формирование умений и навыков при применении теоремы дедукции и правила вывода

План:

1. Логическое следствие.
2. Признаки логического следствия.
3. Правила логических умозаключений.

4. Прямая и обратная теоремы.
5. Силлогизмы.
6. Символы, формулы и аксиомы исчисления высказываний.
7. Правило вывода ИВ.
8. Теорема дедукции, её следствия.
9. Теорема о выводимости тавтологий.

Раздел алгебры высказываний, изучающий закономерности логического исследования, логического умозаключения, является ее сердцевиной. Знание этих закономерностей нужен прежде всего самой математической науке. С помощью таких знаний происходит доказательство математических теорем и, следовательно, развитие математики. Это значение важно и для других наук, для систематизации научного знания вообще, да и в повседневной жизни оно служит инструментом рассуждений, обоснований и доказательств.

Понятие логического следствия. Когда говорят, что из одного или нескольких предложений $A_1, A_2 \ldots A_m$ следует предложение В, то подразумевают следующее: всякий раз, когда окажутся истинными все предложения $A_1, A_2 \ldots A_m$, истинным и будет предложение В. Вот примеры таких следований: «Если летом я поеду работать в студенческий стройотряд (утверждение А), то у меня будут заработанные деньги (утверждение В)». «Если у меня будут заработанные деньги (утверждение В), то я куплю магнитофон (утверждение С)». «Если днем я не приготовлю уроки на завтра (утверждение A^1), и если вечером я пойду в кино (утверждение A^2), то завтра я буду не готов к занятиям (утверждение Д)». Установление справедливости приведенных суждений не относятся к компетенции математической логики, а осуществляется на основе анализа их содержания и смысла.

Задача математической логики (в частности, алгебры высказываний) в вопросах логического следования состоит в том, что указать такие формы высказываний $A_1, A_2 \ldots A_m$, В, когда последнее высказывание непременно было бы следствием mпервых, независимо от конкретного содержания всех этих высказываний. Формы высказываний выражаются, как нам известно, формулами алгебры высказываний. Итак, теория логического следования (в рамках алгебры высказывания), должна изучать закономерности образования формул $F_1, F_2, \ldots F_m, H$ таких, что первые m из них связаны с последней отношением логического суждения.

Вернемся к двум первым суждениям, приведенным в начале пункта: $A \to B$ и $B \to C$. Вынесем относительно них следующее умозаключение: «Если $A \to B$ и $B \to C$, то $A \to C$». Формулировка данного суждения без использования маТемытической символики будет, конечно, неуклюжа. Поэтому сформулируем его так: Если высказывание $A \to B$ верно и высказывание $B \to C$ верно, то верно и высказывание $A \to C$». Нет никаких сомнений в том, что высказанное суждение справедливо. Более того, мы

осознаем его справедливость, даже не интересуясь содержанием простейших высказываний A, B, C. Значит высказывание, имеющее форму $X \to Z$, и следует из двух высказываний, имеющих формы $X \to Y$ и $Y \to Z$, независимо от того, каковы высказывания X, Y, Z.

Перейдем теперь к точному определению понятия логического следствия и к изучению свойств этого понятия.

Определение 6.1. Формула H (X) называется логическим следствием формул F (X), …., F_m $(X_1,\dots,X_n)$, если формула H $(X_1,\dots,X_n)$ превращается в истинное высказывание при всякой такой подстановке вместо всех ее пропозициональных переменных $X_1,\dots,X_n$ конкретных высказываний, при которой в истинное высказывание превращаются все формулы F_1 $(X_1,\dots,X_n)$, …., F_m $(X_1,\dots,X_n)$. То, что формулы H является логическим следствием формул F_1, …, F_b, записывается так: F_1, …,F_b=H. Формула F_1, …, F_b называются посылками для логического следствия H.

Таким образом, F_1, …, F_b=H, если для любых высказываний $A_1,A_2\dots,A_m$ из λ ($F_1(A_1,A_2\dots,A_m)$)=1,…, λ (F_b ($A_1,A_2\dots,A_m$))=1 следует λ (H ($A_1,A_2\dots,A_m$))=1. Наконец, можно и так сказать о логическом следствии. Составим таблицы истинности для формул F_1, …, F=H. Предположим: если в какой-то стране таблицы все формулы F, …, F принимают значение 1, то в этой строке непременно и формуле H принимает значение 1. Это и будет означать, что H является логическим следствием формул F, …, F.

Признаки логического следствия. То, что некоторая формула является логическим следствием каких-то формул, можно выразить также, сказав, что подходящая формула является тавтологией. В этом существо признаков, о которых пойдет речь в настоящем пункте, чем еще раз подчеркивается важное значение тавтологий.

Теорема. (признак логического следствия). Формула H будет логическим следствием формулы F тогда и только тогда, когда формула $F \to H$ является таврологией: $F=H \Leftrightarrow =F \to H$.

Следующая теорема дает признаки того, что формула является логическим следствием двух или большего количества формул.

Теорема. Для любых формул F, …, F, H ($m \geq 2$) следующие утверждения равносильны:

а) F_1, …, F=H

б) $F_1 \wedge F_2$ …, F=H

в) = ($F_1 \wedge F_2$ …, F) $\to$ H

Теорема. Две формулы алгебры высказываний равносильны тогда и только тогда, когда каждая из них является логическим следствием другой:

$F \cong H \Leftrightarrow$ F=Hи H=F

Правила логических умозаключений. Теперь можем рассмотреть примеры структур правильного мышления, то есть ответить на вопрос, что из чего следует.

Правило 1. (modusponens)

$$\frac{F, F \to G}{G}$$

Это правило означает: от утверждения об истинности посылки F с помощью другой посылки $F \to G$ переходят к утверждению об истинности следствия G. Данное правило называют также правилом заключения или отделения (от посылки $F \to G$ с помощью посылки F отделяется заключение G).

Правило 2. (modus tollens)

$$\frac{F \to G, \neg G}{\neg F}$$

Оно называется modustollens: от отрицания истинности посылки G с помощью $F \to G$ переходят к отрицанию истинности F.

Таким образом, рассмотренные правила вывода 6.8 и 6.9 позволяют в истинной импликации $F \to G$ из истинности посылки F делать вывод об истинности следствия G, а из ложности следствия G- о ложности посылки F.

Правило 3. (введения конъюнкции)

$$\frac{F, G}{F \wedge G}.$$

Из тавтологий теоремы 3.2, б приходим к таким правилам вывода.

Правило 4. (удаления конъюнкции)

$$\frac{F \wedge G}{F} \quad u \quad \frac{F \wedge G}{G}$$

Правило 5. (введения дизъюнкции)

$$\frac{F}{F \vee G} \quad u \quad \frac{G}{F \vee G}.$$

Смысл названий этих правил виден из характера их действий.

Из тавтологии теоремы 3.1, д получаем правило контрапозиции.

Правило 6. (контрапозиции)

$$\frac{F \to G}{\neg G \to \neg F}$$

Из тавтологии теоремы 3.1, е вытекает правило цепного заключения (или правило силлогизма).

Правило 7. (цепного заключения)

$$\frac{F \to G, G \to H}{F \to H}$$

Из тавтологии теоремы 3.1, и следует правило перестановки посылок.

Правило 8. (перестановки посылки)

$$\frac{F \to (G \to H)}{G \to (F \to H)}$$

Наконец, из тавтологии теорем 3.1, и получаем следующие правила.

Правило 9. (объединения и разъединения посылок)

$$\frac{F \to (G \to H)}{(F \wedge G) \to H} \quad u$$

Аристотель впервые строго обосновал один из первых разделов логики-учение о суждениях и силлогизмах.

Аристотель и его ученики ввели понятие силлогизма, т.е. рассуждения, в котором из 2-х суждений выводится третье.

Остановился на силлогистике, чтобы на простых примерах пояснить, что представляет собой логический вывод и какие выводы следует считать правильные, а какие нет.

Пример 1. "Все птицы-животные",
"Все воробьи-птицы», следовательно, "Все воробьи-животные"

Первые два предложения называются *посылками*, третье - *заключением*.

Здесь все три предложения истинны, причем истинность заключения следует по определенной схеме из истинности посылок.

Схема выглядит так:

"Все В суть С" *Силлогизм*

"Все А суть В" *правильной формы*, следовательно, "Все А суть С".

Поэтому вывод по такой схеме считается логически правильным.

Пример 2. «Все квадраты – ромбы».

«Некоторые ромбы имеют острый угол». следовательно, «Некоторые квадраты имеют острый угол».

Первые 2 утверждения – правильные, а вывод – ложный, т.к. он содержит логическую ошибку.

Вывод был сделан по схеме:

«Все А суть В»

«Некоторые В суть С»

Следовательно, «Некоторые А суть С».

Это схема из истинных посылок дает ложное заключение, а правильными считаются лишь те схемы логических выводов, которые *всегда* из истинных посылок приводят к истинным заключениям.

Логические выводы делаются по некоторой определенной схеме, аристотелевские силлогизмы представляют собой лишь малую часть таких схем. (С более общими подходами познакомимся позднее).

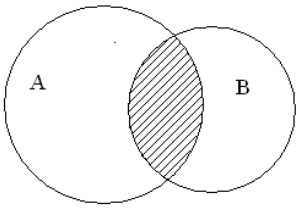
Для проверки правильности силлогизма используем метод, основанный на теории множеств (поскольку суждения, из которых строятся силлогизмы являются на самом деле высказываниями о множествах).

Утверждая, что «Все А суть В», мы говорим, что множество А - подмножество множества В, т.е $A \subset B$.

1. **«Все А суть В»** $\Leftrightarrow$ **$A \subset B$.**

   $A \subset B$

2. **«Некоторые А суть В»** $\Leftrightarrow$ **$A \cap B \neq \varnothing$.**

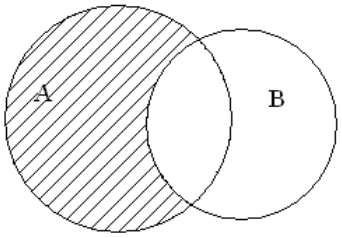


$A \cap B \neq \varnothing$

3. «Ни одно A не является B» $\Leftrightarrow$ **$A \cap B = \varnothing$.**

$A \cap B = \varnothing$

4. «Некоторые A не являются B» $\Leftrightarrow$ **$A \backslash B \neq \varnothing$.**

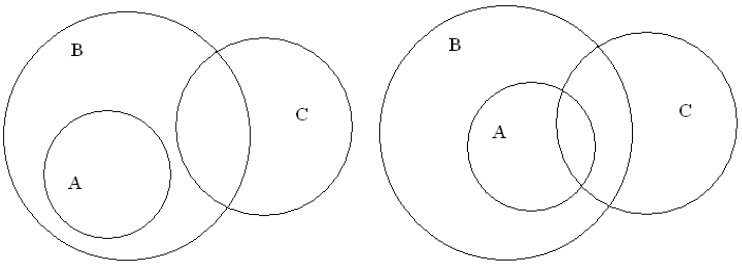


$A \backslash B \neq \varnothing$

Логические высказывания, подобно множествам, удобно изображать с помощью диаграмм Венна.

Пример 1. $A \subset B \wedge B \subset C \Rightarrow A \subset C$.

Пример 2. $A \subset B \wedge B \cap C \neq \varnothing \Rightarrow A \cap C \neq \varnothing$.



вывод - ложный.

Исчисление высказываний

Один из возможных способов формализации логики высказываний - построение **исчисления высказываний** в виде формальной

аксиоматической теории. Описание всякого исчисления содержит описание употребляемых символов, формул исчисления и определение истинных формул. Рассмотрим следующую систему.

1. Символы исчисления высказываний:

-символы переменных с индексами и без них: X, Y ..., X_i…;

- два логических символа: ¯ и v;
- правая и левая скобки "(" и ")".

2. Формулы исчисления высказываний:

а) все переменные;

б) если A, B - формулы, то ($\overline{A}$) и (AvB) - тоже формулы.

Согласно этому определению, если A, B, C - формулы, то Av $\overline{B}$ v C - не формула (поскольку отсутствуют необходимые скобки), а $\overline{(A \vee B)}$ - формула, $\overline{(A \vee (\overline{B}))}$ - формула, $((A \vee \overline{B}) \vee C)$ - также формула. Однако для сокращения и упрощения записи будем опускать внешние скобки в формулах, а также пары скобок, без которых можно восстановить порядок действий.

Символы ¯ и v интерпретируются, конечно, в логике высказываний как операции (или функции) отрицания и дизъюнкции. Однако для удобства нетрудно ввести и другие логические операции:

A &B $\equiv (\overline{A} \vee \overline{B})$

A$\rightarrow$B$\equiv \overline{A} \vee B$

Будем использовать эти знаки, но не как элементы аксиоматической системы, а как **сокращения.**

3. Аксиомы исчисления высказываний (A, B, C - любые формулы):

A1. $A \vee A \rightarrow A$

A2. $A \rightarrow A \vee B$

A3. $A \vee B \rightarrow B \vee A$

A4. $(A \rightarrow B) \rightarrow ((C \vee A) \rightarrow (C \vee B))$

Каждую из этих аксиом можно записать через основные логические символы исчисления. Например, аксиома A3 выглядит так: $(\overline{A} \vee B) \vee (B \vee A)$

Выражения A1-A4 представляют собственно не сами аксиомы, - они называются схемами аксиом, так как вместо. A, B, Св них могут быть подставлены любые формулы.

4. Единственное правило вывода - силлогизм **modusponens**(сокращенно, m.p.), который записывается обычно в виде, $\frac{A, (A \rightarrow B)}{B}$ где над чертой записаны посылки, а под чертой -заключение.

В форме вывода в аксиоматической теории это правило должно выглядеть записанным в строку: $A, A \rightarrow B \vdash B$

Чтобы показать, как работает системы, проведем подробно, с комментариями, доказательство закона, **исключенного третьего**.

1. $\vdash A \rightarrow A \vee B$ -аксиома A2

2. $\vdash A \rightarrow A \vee A$ -из 1; подстановка A. вместо B

3. $\succ A \vee A \to A$ -аксиома А1

4.  -аксиома А4

5  -из 4; подстановке AvA вместо А, А вместо В, $\bar{A}$ вместо С (учитывая, что p→qесть сокращение $\bar{p} \vee q$; подробнее этот переход рассмотрен ниже)

6.  -из 3 и 5 в силу m.p.

7. $\succ A \to A$ т.е. $\bar{A} \vee A$-из 2 и 6 в силу m.p.

8.  -аксиома А3

9.  -из 8; подстановка $\bar{A}$ вместо А и А вместо В

10. $\succ A \vee \bar{A}$ -из 7 и 9 в силу m.p.

Последняя формула означает, что из двух противоположных: высказываний А и $\bar{A}$ хотя бы одно истинно, поскольку их дизъюнкция тождественно истинна.

Представим детально переход от формулы 4 к формуле 5:

Формула 4 

↓ ↓ ↓ ↓ ↓ ↓

подстановка $A \vee A$ A $\bar{A}$ $A \vee A$ $\bar{A}$ A

результат 

подстановки $< \bar{p} \vee q >< \bar{p} \vee q >$

замена дизъюнкций на импликации $A \to A \vee A$ $A \to A$

< p → q > < p → q >

формула 5 

Для исчисления высказываний кроме общих свойств 1-4 выводимости выполнено также свойство

5. Если $\Gamma \succ A \to B$ и $\Gamma \succ A$, то $\Gamma \succ B$

Действительно, если C_1..., C_m-вывод формулы А из системы Г (т.е. последняя в цепочке формула C_m совпадает с А), а D_l..., Dn -вывод формулы А→В из Г (аналогично, D_n совпадаете А→В), то последовательность C_1..., Cm, Dl…, Dn представляет собой вывод формулы В из системы Г. Последняя формула в этой последовательности является следствием предыдущих как раз в силу правила modusponens (обе посылки C_mD_n встречаются в этой последовательности).

Важное свойство в формальном исчислении высказываний составляет

Теорема о дедукции. Если для формул А , В и системы Г выполнено Г, $A \succ B$, то выполнено $\Gamma \succ A \to B$.

Использование теоремы о дедукции позволяет утверждать истинность условного высказывания "если А, то В".

Следствия теоремы о дедукции.

Следствие 1. (правило силлогизма).  .

Следствие 2. 

Следствие 3. Если $\Gamma, A \succ B$ и $\Gamma, \bar{A} \succ B$, то $\Gamma \succ B$ (если из системы Г с добавлением формулы А выводится формула В и с добавлением формулы $\bar{A}$ также выводится формула В, то В выводится просто из системы Г , т.е. формулуА можно не использовать в выводе).

Основной содержательный результат формализации логики высказываний в виде исчисления высказываний формулируется как соотношение между выводимостью формул в исчислении и истинностью логических формул в логике высказываний.

Теорема (о выводимости тавтологий). Формула А исчисления высказываний выводима (из пустой системы гипотез, т.е. только из аксиом) тогда и только тогда, когда она тождественно истинна (тавтология) в логике высказываний (т.е. представляет тождественно равную 1 булеву функцию).

Доказательство теоремы мы проводить не будем; заметим, только, что аксиомы исчисления высказываний - тождественно истинные формулы (это нетрудно проверить, построив таблицы истинности соответствующих функций двух и трех переменных), а правило modusponens из тождественно истинных формул порождает тождественно истинную формулу в силу свойств операции импликации. Поэтому всякая выводимая в исчислении формула тождественно истинна, или, другими словами, выводимы только тождественно-истинные формулы.

Свойство аксиоматической теории, состоящее в том, что выполняется обратное утверждение, т.е. что всякая тождественно истинная формула выводима, называется **полнотой** аксиоматической теории. - Предыдущая теорема утверждает, что исчисление высказываний в предложенной форме полно.

Другое важное требование к аксиоматике: ни для какой формулы ТА не должны быть выводимы обе формулы Аи $\bar{A}$. Аксиоматическая теория с таким свойством называется **непротиворечивой.** Нетрудно показать, что исчисление высказываний непротиворечиво. В самом деле, согласно теореме о выводимости тавтологий, всякая выводимая формула А - это тавтология. Отрицание этой формулы $\bar{A}$ не является тавтологией (подумайте, какую функцию выражает формула $\bar{A}$): следовательно, она не выводима.

Еще один естественный вопрос - о независимости системы аксиом, т.е. о возможности или невозможности вывести одну из аксиом из остальных. Можно доказать, что для рассмотренной нами формы исчисления высказываний выполнено условие независимости.

В заключение заметим, что логику высказываний можно формализовать и другими системами, с использованием других систем аксиом. В том числе для удобства системы аксиом может не быть независимой, подобно тому, как в качестве основной полной системы булевых функций мы рассматривали систему из трех функций (¯, v, &), хотя одну из двух последних можно устранить, поскольку она выражается суперпозицией остальных двух.

Например, одна из часто применяемых систем содержит вместо упомянутых четырех следующие три аксиомы:

В1 $A \to (B \to A)$

В2 $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

В3. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$

Остальное: символы, правила построения формул и правило вывода (m.p.) - те же, что и в рассмотренном выше исчислении.

Контрольные вопросы:

1.Как определяется логическое следование?
2. Укажите признаки логического следования.
3. Какие правила логических умозаключений вы знаете?
4. Как определяются прямые и обратные теоремы?
5. Сформулируйте основные утверждения, составляющие силлогизмы.
6. Назовите символы и формулы ИВ.
7. Какие аксиомы ИВ вы знаете?
8. Укажите правило вывода.
9. Сформулируйте теорему о дедукции и её следствия.
10. Сформулируйте теорему о выводимости тавтологий.

Темы 25, 26. <u>Логика предикатов</u>

Цель:

1. Введение понятия предиката.
2. Рассмотрение классов предикатов и свойств, отражающих их взаимосвязь.
3. Введение кванторных операций над предикатами.

4.Формирование умений и навыков при применении операций над предикатами.

План:

- Предикаты.
- Классификация предикатов.
- Кванторы.

Предикаты. Основные понятия.

Предикаты вслед за высказываниями являются следующим важным предметом, исследуемым математической логикой. Понятие предиката обобщает понятие высказывания, а теория предикатов представляет собой более тонкий инструмент, по сравнению с теорией высказываний, для изучения закономерностей процессов умозаключения и логического следования, составляющих предмет математической логики.

В математике часто приходится иметь дело с предложениями, которые хотя и содержат определенное утверждение, но ложность или истинность их зависит от значения их неизвестной переменной.

Например: 1) «x+2=5» , $x \in Z$

2) «n-простое число»

3) «река x впадает в озеро Байкал»

Каждое из этих предложений становится высказыванием (истинным или ложным) при замене переменной каким-либо конкретным значением.

Пример. Если множество, которому принадлежит x, в предложении не выделено, то его нужно указать отдельно.

Определение 1. Предложение, содержащее nпеременных $x_1…, x_n$, обращающееся в высказывание при подстановке вместо переменных любых конкретных элементов из множеств $M_1…, M_n$, называется n-местным предикатом, определенным на множествах $M_1…, M_n$.

Обозначается $P(x_1…, x_n)$.

Переменные $x_1…, x_n$ называют *предметными*, а элементы множеств $M_1…, M_n$, которые эти переменные пробегают, - *конкретными предметами*.

Всякий n-местный предикат $P(x_1…, x_n)$, определенный на множествах $M_1…, M_n$, представляет собой функцию n аргументов, заданную на указанных множествах и принимающую значение в двухэлементном множестве {0,1}. Поэтому предикат называют также функцией-высказыванием.

Классификация предикатов

Определение 2. Предикат $P(x_1…,x_n)$, заданный на множествах $M_1,…,M_n$, называется:

1) тождественно истинным, если при любой подстановке вместо переменных $x_1…, x_n$ любых конкретных предметов $a_1…, a_n$ из множеств $M_1…, M_n$ соответственно он превращается в истинное высказывание $P(a_1…, a_n)$;

2) тождественно ложным, если при любой подстановке вместо переменных $x_1…, x_n$ любых конкретных предметов $a_1…, a_n$ из множеств $M_1…, M_n$ соответственно он превращается в ложное высказывание $P(a_1…, a_n)$;

3) выполнимым (опровержимым), если существует по меньшей мере один набор конкретных предметов a_1, a_n из множеств $M_1…, M_n$ соответственно, при подстановке которого вместо соответствующих предметных переменных в предикат $P(x_1…, x_n)$ последний превращается в истинное (ложное) высказывание $P(a_1…, a_n)$.

Примеры.

1) Одноместный предикат «$\sin^2x+\cos^2x=1$», определенный на множестве R-тождественно - истинный.

2) Двуместный предикат «$x^2+y^2<0$»-определенный на R- тождественно-ложный.

3) «Река x впадает в озеро Байкал» - одноместный предикат - выполнимый, так как существуют реки (Баргузин), которые превращают в истинное высказывание и опровержимый, так как «Ангара» превращает в ложное высказывание.

Свойства, отражающие взаимосвязь между предикатами различных типов.

1) Каждый тождественно-истинный предикат является выполнимым, но обратное неверно;

2) Каждый тождественно-ложный предикат является опровержимым, но обратное неверно;

3) Каждыйне тождественно-истинный предикат будет опровержимым (но, вообще говоря, не будет тождественно-ложным);

4) Каждый не тождественно-ложный предикат будет выполнимым (но, вообще говоря, не будет тождественно-истинным).

Определение: **Множеством истинности предиката** P $(x_1,\ldots,x_n)$, заданного на множествах $M_1,\ldots,M_n$, называется совокупность всех упорядоченных n-ок $(a_1,\ldots,a_n)$, в которой $a_1 \in M_1$, …, $a_n \in M_n$, таких, что данный предикат обращается в истинное высказывание P $(x_1,\ldots,x_n)$. Обозначается P^+.

Множество P^+ истинности n-местного предиката P $(x_1\ldots, x_n)$ представляет собой парное отношение между элементами множеств $M_1\ldots$, M_n. Если предикат P(x) одноместный, заданный на множестве M, то его множество истинности P^+ является подмножеством множества M: $P^+ \subseteq M$.

Примеры:

1) Множеством истинности двухместного предиката S (x,y): «$x^2+y^2=9$», заданного на множестве R, есть множество всех таких пар действительных чисел, которые являются координатами точек плоскости, образующими окружность с центром в начале координат и R=3.

2) A (x): «$|x| > 2$»-одноместный предикат над R.

В терминах множества истинности легко выразить понятия, связанные с классификацией предикатов.

n-местный предикат P $(x_1\ldots, x_n)$, заданный на множествах $M_1\ldots$, M_n будет:

I. тождественно-истинным $\Leftrightarrow$ 

II. тождественно-ложным $\Leftrightarrow P^+ = \varnothing$

III. выполнимым $\Leftrightarrow P^+ \neq \varnothing$

IV. опровержимым $\Leftrightarrow$ 

Кванторные операции над предикатами

Специфика природы предикатов позволяет ввести над ними такие операции, которые не имеют аналогов среди операций над высказываниями ( ).

Это-две кванторные операции над предикатами (или операции квантификации): *квантор общности* и *квантор существования.*

Чтобы получить из одноместного предиката высказывание, нужно подставить вместо его переменной одно из значений, а из области задания предиката.

Но есть еще один способ для такого превращения – это применение к предикату операций связывания квантором общности и квантором существования.

Каждая из этих операций ставит в соответствие одноместному предикату некоторое высказывание, истинное или ложное, в зависимости от исходного предиката (то есть одноместный предикат превращается в нуль местный).

Определение: Операцией связывания квантором общности называется правило, по которому каждому одноместному предикату P (x), определенному на множестве M, сопоставляется высказывание, обозначаемое $(\forall x)(P(x))$. (читается: «для всех x выполнено P (x)»), которое истинно $\Leftrightarrow$ предикат P (x) тождественно истинно и ложно в противном случае, то есть

Пример. $P(x) \equiv$ "$1 \le x$" - тождественно-истинный предикат

$P(x) \equiv$ "x делится на 3" на N –опровержимый предикат

$\Rightarrow$ операция связывания квантором общности, примененная к ним, дает в первом случае истинное высказывание, во втором - ложное.

Вывод: если данный предикат истинный для всех элементов множества M, то навешивание квантора общности $(\forall x \in M)$: p (x) превращает его в истинное высказывание.

При этом переменная x становится «связанной», поскольку перестает быть переменной в обычном смысле (обозначается - от первой буквы «All»-«все»).

Определение: Операцией связывания квантором существования называется правило, по которому каждому одноместному предикату P (x), определенному на множестве M, сопоставляется высказывание, обозначаемое ($\exists$ x)(P(x)) (читается: «существует x, для которого выполнено P(x)»), которое ложно $\Leftrightarrow$ предикат P(x)- тождественно-ложен и истинно в противном случае, то есть

(Символ $\exists$ происходит от первой буквы «Exist»-«существовать»)

Пример: P (x): «x=x+1» - тождественно-ложный предикат

$P(x) \equiv$ "$x^2 > 0$" - выполнимый предикат

$\Rightarrow$ применение операции навешивания квантора существования дает в первом случае ложное высказывание, во втором – истинное высказывание.

(**Вывод:** если данный предикат P(x) истинен хотя бы для одного элемента $x \in M$, то навешивание квантора существования $(\exists x \in M): P(x)$ превращает его в истинное высказывание). Здесь x также «связанная переменная».

Особенность этих операций.

а) логические операции $\wedge, \vee, \rightarrow$ ставили в соответствие одному или нескольким предикатам новый предикат, то операции квантификации – сопоставляют предикату (одноместному) высказывание.

б) если одноместный предикат P(x) задан на конечном множестве M, то

$$M = \{a_1 \ldots, a_k\}$$

Высказывание $(\forall x)(P(x))$ эквивалентно конъюнкции

$P(a_1) \wedge \ldots \wedge P(a_k)$

Высказывание $(\exists x)(P(x))$ эквивалентно дизъюнкции

$P(a_1) \vee \ldots \vee P(a_k)$

Литература: [6], стр 122,128, 134 [17]; стр 254.

Контрольные вопросы:

1. Дайте определение предиката.
2. Какие классы предикатов вы знаете?
3. Укажите связь между предикатами разных типов.
4. Как определяется множество истинности предиката?
5. Какие кванторные операции вы знаете?
6. Укажите особенность этих операций.
7. Дайте понятие связанной и несвязанной переменной.

Темы 27, 28. <u>Аксиоматическое построение теорий</u>

Цель:

1. Введение понятия формальной аксиоматической теории.
2. Введение понятий аксиом и правил вывода.
3. Рассмотрение аксиоматики Пеано.
4. Формирование умений и навыков при доказательстве методом полной математической индукции.

План:

1. Процесс аксиоматизации.
2. Аксиомы и правила вывода.
3. Аксиоматическое построение арифметики Пеано.
4. Метод полной математической индукции.

Представление некоторой содержательной теории в виде формальной (оно называется формализацией) позволяет выявить общие свойства, полезные аналогии и ответить на ряд общих вопросов. Формализация процесса правильных рассуждений достигается с помощью **аксиоматизации.**

Формальная аксиоматическая теория Т (синонимы: формальная системы, исчисление) задается следующим образом.

(1) Некоторый алфавит А символов, называемых **символами** теории. Слова в алфавите А называются **выражениями** теории Т.

(2) Выделено некоторое подмножество выражений, называемых **формулами** теории Т (правильно построенные выражения).

(3) Выделено некоторое множество формул, называемых **аксиомами** теории Т.

На содержательном, т. е неформальном уровне - аксиомы суть формулы, по определению считающиеся истинными.

(4) Имеется конечное множество **правил вывода** R_1..., Rm, каждое из которых есть отношение между формулами. Если A_1…, A_k, В - формулы и выполнено отношение R_i (A_1…, A_k, В), то В называется **непосредственным следствием** формул A_1…, A_k, полученным по правилу R_i.

Однократное применение какого-либо правила вывода представляет формализованный элементарный шаг правильного рассуждения.

Выводом в теории Т называется всякая цепочка (последовательность, или кортеж) формул B_1,B_2,…,B_n такая, что для i=1,2,…,n формула B_i есть либо аксиома теории Т, либо непосредственное следствие каких-либо предыдущих формул этой последовательности. Вывод есть последовательное проведение элементарных шагов, составляющее доказательное рассуждение.

Формула С называется **теоремой** теории Т, если существует вывод, в котором последней формулой является С. Этот вывод называется выводом формулы С (он не единственный в теории Т). Понятно, что все формулы в выводе С, кроме аксиом, являются также теоремами теории. Таким образом, **теоремы в аксиоматической теории - это формулы, которые могут быть выведены из аксиом по принятым правилам.**

В более общем смысле, можно рассматривать вывод не только из аксиом. Пусть для множества формул Г = {B_1…, Bn} существует последовательность формул A_1..., A_mтакая, что для любого i=1…, m формула A_i–либо аксиома теории, либо формула из Г (т.е. одна из B_i), либо непосредственное следствие предыдущих формул. Тогда A_m называется **следствием системы формул** Г: обозначается Г ├ A_m, или B_1…, Bn ├ A_m. Последовательность A_1..., A_m называется выводом формулы A_mиз системы Г. Формулы системы Г называются **посылками**, или **гипотезами**, а формула A_m– **выводимой из системы гипотез** Г.

Частный случай, когда Г = Ø, т.е. А есть следствие только аксиом, и есть теорема: обозначение ├ А. Вывод теоремы называют также её доказательством.

Можно сказать, что множество всех следствий некоторой системы формул и, в частности, теорем теории Т есть результат порождающего процесса. Для порождающей процедуры характерно, что это последовательность действий, когда при каждом шаге возможны, вообще говоря, различные продолжения, которые могут приводить к различным результатам.

Отметим, что отношение “быть выводимой из системы гипотез Г” между заключительной формулой B_n и множеством гипотез можно рассматривать как транзитивное замыкание отношения “быть непосредственным следствием”.

Рассмотрим теперь некоторые свойства выводимости из системы гипотез; напомним, что для формальной системы обоснование должно использовать формальные определения понятий, а естественность этих свойств означает, что они содержательно отражают реальные свойства аксиоматических построений. Пусть Г – произвольное множество формул, А, В, С – некоторые формулы.

1. Г, А ├ А. Это значит, что если в числе посылок кроме Г присутствует также некоторая формула А, то А есть следствие пары <Г, А>. в этом случае систему Г можно не использовать – вывод состоит из одной формулы А.
2. Если Г ├ А, то Г, В ├ А. Смысл этого выражения состоит в том, что добавление к посылкам Г любой формулы В не изменяет выводимости А – можно не изменять и вывод формулы А.
3. Если (Г ├ А) & (Г ├ В) & (А, В ├ С), то Г ├ С. Это значит, что если из системы Г выводятся А и В, а из них С, то С есть следствие системы Г. Действительно, пусть A_1..., A_m, А- вывод формулы А из Г, B_1…, Bn, В вывод из Г, C_1…, C_k, С- вывод С из (А, В). тогда A_1..., A_m, А, B_1…, Bn, В, C_1…, C_k, С есть вывод С из Г.
4. Если (Г, А ├ В) & (Г ├ А), то (Г ├ В). Это правило удаления выводимой гипотезы: в выводе, содержащем А в качестве одной из посылок, можно заменить каждое вхождение формулы А на цепочку представляющую ее вывод из системы Г.

Формальная системы потому и называется формальной, что она оперирует с формальными, абстрактными объектами: символами, словами и их последовательностями. Реальное содержание имеют интерпретации формальных систем, которые для одной и той же системы могут быть различны. Мы уже видели, что алгебра множеств и алгебра логики описываются одинаково (изоморфны).

Метод математической индукции

Неполная индукция приводит часто к ошибочным результатам. Метод полной индукции имеет лишь ограниченное применение. Многие интересные математические утверждения охватывают бесконечное число частных случаев, а провести проверку для бесконечного числа случаев человек не может.

Во многих случаях выход из такого рода затруднений заключается в обращении к особому методу рассуждений, называемому методом математической индукции. Доказательства этим методом опираются на следующую аксиому.

Принцип (аксиома) математической индукции.

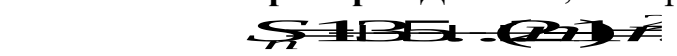
Утверждение, зависящее от натурального числа n, справедливо для любого n, если выполнены два условия:

а) утверждение справедливо при n=1;

б) при любом натуральном значении k из справедливости утверждения для n=k вытекает его справедливость и для n=k+1.

Приведем примеры доказательств методом математической индукции.

Пример 1. Доказать, что при любых $n \in N$ справедливо



Решение.

а) $S_1 = 1 = 1^2$, следовательно, утверждение верно при n=1.

б) Пусть k – любое натуральное число и пусть утверждение справедливо для n=k, то есть

 .

Докажем, что тогда утверждение справедливо и для следующего натурального числа n=k+1, то есть докажем, что

 .

В самом деле,

 .

Тем самым по принципу матемитической индукции утверждение доказано для любого натурального значения n.

Контрольные вопросы:

1. Как задаётся формальная аксиоматическая теория?
2. Как определяется аксиомы и правила вывода?
3. Укажите систему аксиом Пеано.
4. В чем заключается метод полной матемитической индукции.

Темы 29, 30. **Элементы теории алгоритмов**

Цель:

1. Введение понятия алгоритма, его общих типичных черт.
2. Рассмотрение вычисления простейших числовых функций.
3. Введение определения машины Тьюринга.
4. Формирование умений и навыков при применении машин Тьюринга к словам.

План:

1.Понятие алгоритма.

2.Вычислимые функции.

3.Машины Тьюринга.

1.Понятие алгоритма

Проанализировав примеры алгоритмов, выявим общие типичные черты и особенности.

1) Любой алгоритм предполагает наличие начальных или исходных данных, в результате применения приводит к получению определённого искомого результата.

2) Применение каждого алгоритма осуществляется путем выполнения дискретной цепочки, последовательности некоторых элементарных действий, которые называются шагами, а процесс их выполнения называется алгоритмическим процессом, следовательно, так образовывается отличительное свойство дискретности.

3) Существенной чертой алгоритма является его массовый характер, т.е. возможность применить его к обширному классу начальных данных, следовательно, любой алгоритм призван решить ту или иную массовую проблему, т.е. решать класс однотонных задач.

4) Непременное условие для алгоритма его детерминированность (определённость) (т.е. результат получится в любом случае, независимо от того, кем он выполняется)

Предписание алгоритма настолько точны, отчетливы, что выполнение тех или иных алгоритмов может быть поручено машине.

Под алгоритмом понимается чёткая системы инструкций, определяющая дискретный детерминированный процесс, ведущей от варьируемых начальных данных к искомому результату. (если таковой существует). Другими словами, под алгоритмом понимают чёткую систему инструкций о выполнении в определённом порядке некоторых действий для решения всех задач какого-то данного класса.

Термин «алгоритм» происходит от имени великого среднеазиатского учёного Мухаммеда аль - Хорезми (IX в).

2.Вычислимые функции

Рассмотрим функцию f от одного или нескольких аргументов, заданные на множестве $N=\{0,1,2,\ldots,n,\ldots\}$ всех натуральных чисел или некоторых подмножествах (частные функции) и принимающие значение во множестве N.

Определение 1. Функция $f(x_1,x_2)$ называется вычислимой, если $\exists$ алгоритм, позволяющий вычислить её значение для всех наборов аргументов, для какой она определена, и работающий вечно, если функция для данного набора значений аргумента неопределенна.

Пусть $M \le N^n$

Определение 2. Множество M называется разрешимым, если имеется алгоритм для выяснения того, принадлежит или не принадлежит произвольной элемент к этому множеству.

Функция X_M называется характеристической функцией множества M, если она задана на множестве M и принимает значения в двух элементарном множестве {0,1} определяется следующим образом:

Отсюда ясно, что множество M разрешимо его характеристическая функция X_M вычислима.

Определение 3. Множество $M \subseteq N$ называется (рекурсивно, или эффективно, или алгоритмически) перечислимым если M либо пустым, либо есть область значения некоторой вычислимой функции, или, другими словами, если $\exists$ алгоритм для последовательного нахождения (перечисления) всех его элементов.

Пример. Рассмотрим множество M= {1,4, 9…} квадратов натуральных чисел. Оно перечислимо для получения его элементов нужно последовательно брать числа 1,2, 3…и возводить их в квадрат.

Другими словами, M есть область значений вычислимой функции $f(x)=x^2$: $M=\{1^2,2^2,...\}$

Более того, это множество является также разрешённым: для проверки того, принадлежит или нет некоторое число данному множеству, нужно разложить его на простые множители, что позволит выяснить, является ли оно точным квадратом.

Оказывается, любое разрешённое множество перечислимо, но обратное утверждение неверно.

3.**Машины Тьюринга**

Введение понятия машины Тьюринга явилось одной из первых и весьма удачных попыток дать точный математический эквивалент для общего интуитивного представления об алгоритме. Это понятие названо по имени английского математика, сформулировавшего его в 1937г., за 9 лет до появления первой ЭВМ.

Определение машины Тьюринга

Машина Тьюринга есть математическая (воображаемая) машина; т.е. такой же математический объект, как функция, производная, интеграл, группа и т.д.

Как и другие математические понятия, она отражает объективную реальность, моделирует некие реальные процессы. Тьюринг предпринял попытку смоделировать действия математика (или другого человека), осуществляющего некую умственную созидательную деятельность.

Машину Тьюринга удобно представлять в виде автоматически работающего устройства.

В каждый дискретный момент времени устройство, находясь в некотором состоянии, обозревает содержимое одной ячейки протягиваемой через устройство ленты и делает шаг, заключающийся в том, что устройство переходит в новое состояние, изменяет содержимое обозреваемой ячейки, справа и слева. Причём шаг осуществляется на основании предписанной команды. Совокупность всех команд представляет собой программу машины Тьюринга.

Описание машины Тьюринга. Машина Тьюринга располагает конечным числом знаков (символов, букв), образующих так называемый внешний алфавит $A=\{a_0, a_1 \dots a_n\}$

В любую ячейку обозреваемой ленты в любой дискретный момент времени может быть записан только один символ из алфавита А.

Ради единообразия удобно считать, что среди букв внешнего алфавита А имеется «пустая буква» и именно она записана в пустую ячейку ленты. Условия, что «пустой буквой» или символом пустой ячейки является буква a_0. Лента предполагается неограниченной в обе стороны, но в каждый момент времени на ней записано конечное число непустых букв.

В любой момент времени машина Тьюринга способна находиться в одном состоянии из конечного числа внутренних состояний, совокупность которых $Q=\{q_0, q_1 \dots q_n\}$ Среди состояний выделяются два начальное q_1 и заключительное, или состояние остановки, q_0. Находясь в состоянии q_1, машина начинает работать. Попав в состояние q_0 машина останавливается.

Работа машины Тьюринга определяется программой (функциональной схемой). Программа состоит из команд. Каждая команда

T (I, j) (I =1, 2…m; j=0, 1…. n) представляет собой выражение одного из следующих видов.

$$q_i a_j \rightarrow q_k a_e C$$

$$q_i a_j \rightarrow q_k a_e L$$

$$q_i a_j \rightarrow q_k a_e R$$

В выражении 1 вида символ С будем часто опускать.

$a \le k \le m$; $a \le l \le n$

Работа машины Тьюринга. Находясь в какой либо момент времени в не заключительном состоянии (т.е. отличная от q_0), машина совершает шаг, как полностью определяется её текущем состоянием q_1 и символом a_j воспринимаемом ею в данный момент на ленте. При этом содержание шага регламентировано соответствующей командой T(I , j): $q_i a_j \rightarrow q_k a_e X$, где $X \in \{C, L, R\}$

Шаг заключается в том, что

1) содержимое a_j обозреваемой на ленте ячейки стирается, и на его место записывается символ a_l (который может совмещаться с a_j)

2) машина переходит в новое состояние q_k (может совпадать с предыдущем состоянием q_i)

3) машина переходит к обозрению следующий правой ячейки от той, которая обозревалась только что, если Х=П, или к обозрению следующий левой ячейки, если Х=Л, или же продолжает обозревать ту же ячейку, если Х=С.

Контрольные вопросы:

1. Дайте понятие алгоритма.
2. Какая функция называется вычислимой?
3. Какое множество называется разрешимым?
4. Дайте описание машины Тьюринга.

Список литературы

1.Новиков Ф.А. Дискретная математика (для программистов) – Санкт-Петербург: «Питер», 2001. – 304с.
2.Ежов И.И., Скороход А.В., Ядренко М. И. Элементы комбинаторики, М.:Наука, 1977. 320с.
3.Акимов О.Е. Дискретная математика: логика, группы, графы. – М.: Лаб. Баз. Знаний 2003. 376с.
4. Новиков П.С. Элементы математической логики. -М., 1973. –400с.
5. Гиндикин С. Г. Алгебра логики в задачах.- М., 1979. –288с.
6. Игошин В. И. Математическая логика и теория алгоритмов.- Изд-во Саратовского университета. , 1991. – 256с.
7. Игошин В.И. Задачник-практикум по математической логике.М.,1986 159с.
8. Бухштаб А.А. Теория чисел. М., Просвещение, 1966. –256с.
9. Грибанов В.У. Сборник упражнений по теории чисел. М., Просвещение, 1964. 141с.
10.Виленкин Н.Я. Комбинаторика. - М.: Наука, 1969. – 328с.
11.Липский П. Комбинаторика в информатике. – М.: Наука, 1973. –198с.
12.Яблонский С.В. Введение в дискретную математику. – М.: Наука, 1986. 223с.
13.Лавров И. А., Максимова Л. Л. Задачи по теории множеств, математической логике и теории алгоритмов.- М., 1975. –240с.
14.Столл Р. Множества, логика, аксиоматические теории.- М., Просвещение, 1968. –265с.
15. Шнеперман Л.Б. Сборник задач по алгебре и теории чисел. Минск,Вышэйшая школа, 1982. 223
16. Виноградов И.М. Основы теории чисел. М., Наука, 1965. –172с.
17. Ершов Ю.Л., Палютин Е.А. Математическая логика. М., Наука, 1979. – 320с.
18. А.С. Джумадильдаев. Дискретная математика, Алматы, 2000.