

# Материалы для подготовки к коллоквиуму по дискретной математике Теоремы

ПМИ 2016

Орлов Никита, Рубачев Иван, Ткачев Андрей, Евсеев Борис

12 декабря 2016 г.

## 2. Бином Ньютона. Формула для биномиальных коэффициентов

Число сочетаний из  $n$  по  $k$  равно:

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

*Доказательство.* На первое место можно поставить любой из  $n$  элементов, на второе любой из  $n-1$  оставшихся, ..., на  $k$ -е любой из  $n-k+1$ . Тогда по правилу произведения существует  $n(n-1)(n-2)\cdots(n-k+1)$  упорядоченных наборов. Но порядок нам не важен, поэтому существует  $\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$  неупорядоченных наборов.  $\square$

Формула бинома Ньютона имеет вид:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \dots + \binom{n}{k}a^{n-k}b^k + \dots + \binom{n}{n}b^n = \sum_{k=0}^n \binom{n}{k}a^{n-k}b^k$$

*Доказательство.* Раскрытие скобок даст все возможные комбинации  $a$  и  $b$  длины  $n$ . Так как умножение коммутативно, то элементы с одинаковым количеством  $b$  можно сгруппировать. Тогда перед  $a^{n-k}b^k$  будет стоять коэффициент  $c$ . Количество слогаемых, в которых  $b$  встречается ровно  $k$  раз равно  $\binom{n}{k}$ . Тогда  $c = \binom{n}{k}$ , а значит:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k}a^{n-k}b^k$$

$\square$

## 6. Формулы для суммы степеней вершин в неориентированном и в ориентированном графе

**Определение.** Сумма степеней всех вершин в неориентированном графе равна удвоенному числу ребер. 
$$\sum_{v \in V(G)} \deg(v) = 2 \cdot |E(G)|$$

*Доказательство.* Пусть в графе степень каждой вершины равна 0 (в графе нет ребер). При добавлении ребра, связывающего любые две вершины, сумма всех степеней увеличивается на 2 единицы. Таким образом, сумма всех степеней вершин четна и равна удвоенному числу ребер.  $\square$

**Определение.** Число исходящих степеней вершин равно числу входящих, равно числу ребер.

*Доказательство.* Первая часть утверждения очевидна. Каждое ребро выходит из одной вершины и входит в другую, поэтому каждое ребро дает одинаковый вклад в суммы исходящих и входящих степеней вершин. Для доказательства второй части утверждения докажем что число ребер равно числу исходящих степеней вершин. Исходящая степень вершины равна числу ребер, которые из нее выходят. Ребро не может выходить более чем из одной вершины, поэтому сумма исходящих степеней вершин равна числу ребер. По транзитивности отношения «= $\Rightarrow$ » число ребер равно также и сумме исходящих вершин.  $\square$

## 10. Деревья – это в точности минимально связные графы

*Доказательство.*

[ $\Rightarrow$ ] Докажем индукцией по числу вершин. База: для  $n = 2$  существует лишь одно дерево, для которого утверждение очевидно. Предположим это для некоторого дерева  $G_n$  на  $n$  вершинах, в котором  $n - 1$  ребро. Шаг для  $n + 1$ : добавляя одну вершину  $u$ , нужно связать её с графом  $G_n$ , то есть соединить с некоторыми вершинами. Если бы мы соединили её с двумя вершинами  $v_1$  и  $v_2$ , то у нас в графе  $G_{n+1}$  получился бы цикл, так как в  $G_n$  уже существовал путь  $v_1, a_1, a_2, \dots, a_k, v_2$ , а значит в  $G_{n+1}$  существует цикл  $v_1, a_1, a_2, \dots, a_k, v_2, u, v_1$ , а значит  $G_{n+1}$  – не дерево. Значит, при добавлении вершины мы можем добавить не более одного ребра (а для сохранения связности ещё и более 0), значит  $G_{n+1}$  должен содержать  $n - 1 + 1 = n$  рёбер, что означает, что предположение индукции выполнено и для  $n + 1$ .

[ $\Leftarrow$ ] Для начала докажем что в связном графе не может меньше чем  $n - 1$  ребро по индукции. База: для  $n = 2$  граф на 2-ух вершинах, все очевидно. Шаг для  $n + 1$ : если для  $n$  вершин утверждение верно, то для  $n + 1$  вершины оно тоже будет верно, так как нужно связать добавленную вершину как минимум с одним ребром (то есть ребер станет не менее чем  $n - 1 + 1 = n$ ). Пусть у нас есть связный граф на  $n$  вершинах, с  $n - 1$  ребрами и в этом графе есть циклы. Из некоторого цикла удалим ребро соединявшее вершины  $u$  и  $v$ , при этом граф останется связным, но в нем будет уже  $n - 2$  ребра – получили противоречие. Значит в таком минимально связном графе нет циклов, то есть этот граф – дерево.  $\square$

## 14. Равносильность свойств ориентированных графов...

**Формулировка.** Следующие свойства ориентированных графов равносильны:

1. Каждая компонента сильной связности состоит из одной вершины.
2. Вершины графа можно занумеровать так, чтобы каждое ребро вело из вершины с меньшим номером в вершину с большим номером.
3. В графе нет циклов длины больше 1.

*Доказательство.* Рассмотрим вершины занумерованные таким образом. Из того, что номера все время возрастают следует отсутствие циклов в графе, так как в вершину с меньшим номером нельзя попасть из вершины с большим номером  $\square$

## 18. Признаки делимости на 3, 9 и 11

Число  $x$  делится на 3 (на 9) тогда и только тогда, когда сумма его цифр делится на 3 (на 9)

*Доказательство.* Пусть  $x = \overline{a_n a_{n-1} \dots a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10 a_1 + a_0$ . Так как  $10 \equiv 1 \pmod{3}$ , то:

$$x \equiv \sum_{i=0}^n a_i \pmod{3}$$

Для делимости на 9 доказательство аналогично.  $\square$

Число  $x$  делится на 11, тогда и только тогда, когда:

$$11 \mid \left( \sum_{2 \nmid i}^n a_i - \sum_{2 \mid i}^n a_i \right)$$

*Доказательство.*  $10 \equiv -1 \pmod{11}$ , значит  $10^n \equiv (-1)^n \pmod{11}$ . Тогда:

$$x \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \dots + (-1) a_1 + a_0 \equiv \sum_{2 \nmid i}^n a_i - \sum_{2 \mid i}^n a_i \pmod{11}$$

$\square$

## 22. Основная теорема арифметики

**Лемма.** Если простое число  $p$  делит без остатка произведение двух целых чисел  $x \cdot y$ , то  $p$  делит  $x$  или  $y$ .

*Доказательство.* Пусть  $x \cdot y$  делятся на  $p$ , но  $x$  не делится на  $p$ , тогда  $x$  и  $p$  – взаимнопростые, следовательно, найдутся такие целые числа  $u$  и  $v$ , что:

$$x \cdot u + p \cdot v = 1$$

Умножая обе части на  $y$  получаем:

$$(x \cdot y) \cdot u + p \cdot v \cdot y = y$$

Здесь оба слагаемых в левой части делятся на  $p$ , значит и  $y$  делится на  $p$ .  $\square$

**Теорема.** Каждое натуральное число  $n > 1$  представляется в виде  $n = p_1 \cdot \dots \cdot p_k$ , где  $p_1, \dots, p_k$  – простые числа, причём такое представление единственно с точностью до порядка следования сомножителей.

*Доказательство.*

**Существование.** Пусть  $n$  – наименьшее целое число не разложимое в произведение простых чисел. Оно не может быть единицей по формулировке теоремы. Оно не может быть и простым, потому что любое простое число является произведением одного простого числа – себя. Если  $n$  составное, то оно – произведение двух меньших натуральных чисел. Каждое из них можно разложить в произведение простых чисел, значит  $n$  тоже является произведением простых чисел. Противоречие.

**Единственность.** Пусть  $n$  – наименьшее натуральное число, разложимое в произведение простых чисел двумя разными способами. Если оба разложения пустые – они одинаковы. В противном случае, пусть  $p$  – любой из сомножителей в любом из двух разложений. Если  $p$  входит и в другое разложение, мы можем сократить оба разложения на  $p$  и получить два разных разложения числа  $\frac{n}{p}$ , что невозможно. А если  $p$  не входит в другое разложение, то одно из произведений делится на  $p$ , а другое – не делится (как следствие из леммы), что противоречит условию.  $\square$

## 26. Критерий того, что бинарное отношение записывается с помощью функции полезности

**Формулировка.** Пусть множество  $A$  конечно, тогда соотношение:

$$xPy \iff u(x) > u(y)$$

Выполняется для некоторой функции  $u(x)$  в том и только в том случае, когда  $P$  – отношение слабого порядка.

*Доказательство.*

[ $\Rightarrow$ ] Докажем это утверждение в одну сторону. Пусть выполняется данное соотношение. Для того чтобы доказать, что  $P$  – отношение слабого порядка, необходимо проверить его антирефлексивность, транзитивность и транзитивность его дополнения.

**Антирефлексивность.** Пусть  $x \in A$ . Тогда  $u(x)$  не больше  $u(x)$ , то есть  $x\bar{P}x$ . Значит отношение  $P$  антирефлексивно.

**Транзитивность.** Пусть  $x, y, z \in A$ , таковы, что  $xPy$  и  $yPz$ . Это значит, что  $u(x) > u(y)$  и  $u(y) > u(z)$ . Следовательно,  $u(x) > u(z)$ , или  $xPz$ , значит  $P$  транзитивно.

**Транзитивность дополнения.** Пусть  $x, y, z \in A$  таковы, что  $x\bar{P}y$  и  $y\bar{P}z$ . В силу соотношения из формулировки  $u(x) \leq u(y)$  и  $u(y) \leq u(z)$ , отсюда  $x\bar{P}z$ , то есть  $\bar{P}$  транзитивно.

[ $\Leftarrow$ ] Пусть  $P$  – слабый порядок. Определим значение  $u(x)$ , как число элементов во множестве  $\{y | xPy\}$ , то есть число альтернатив, которые менее предпочтительны, чем  $x$ . Докажем, что при этом  $xPy \iff u(x) > u(y)$ .

Пусть  $xPy$ . Поскольку отношение  $P$  транзитивно, то для любого  $z$ , такого, что  $yPz$ , верно и  $xPz$ . Поэтому из  $x$  выходят дуги как минимум в те же вершины, что и из  $y$ , значит  $u(x) \geq u(y)$ . Кроме того  $P$  антирефлексивно, поэтому из  $y$  не ведет дуга в  $y$ , а из  $x$  в  $y$  ведет. Значит,  $u(x) > u(y)$ .

Обратно, пусть  $u(x) > u(y)$ , т.е. из  $x$  выходит больше дуг, чем из  $y$ . Значит, существует такой элемент  $z$ , что  $xPz$ , но  $y\bar{P}z$ . Если  $x\bar{P}y$ , то отношение  $\bar{P}$  не транзитивно, что противоречит условию, значит  $(x, y) \in P$ .  $\square$

### 30. Биекция между двоичными словами, подмножествами конечного множества и характеристическими функциями

**Определение.** *Характеристической функцией множества  $X \subset U$  называют функцию  $\chi_X$ , которая равна 1 на элементах  $X$  и 0 на остальных элементах  $U$ .*

Составим двоичное слово следующим образом: если  $i$  элемент лежит в  $X$ , то на  $i$ -м месте ставим 1, иначе 0. Биекция между характеристической функцией и подмножеством очевидна – значения характеристической функции однозначно задают подмножество.