

Материалы для подготовки к коллоквиуму  
по дискретной математике  
Теоремы

ПМИ 2016

Орлов Никита, Рубачев Иван, Ткачев Андрей, Евсеев Борис

13 декабря 2016 г.

---

# 1. Вывод принципа полной математической индукции из принципа математической индукции

**Принцип математической индукции.** Если для утверждения зависящего от положительного натурального  $n$  выполняются следующие условия:

- 1. Утверждение истинно при  $n = 1$
- 2. Когда утверждение истинно при  $n = k$ , оно истинно и при  $n = k + 1$

Тогда утверждение истинно при всех положительных  $n$ .

**Принцип полной математической индукции.** Если для утверждения зависящего от положительного натурального  $n$  выполняются следующие условия:

- 1. Утверждение истинно для  $n = 1$
- 2. Если утверждение истинно для всех  $n \leq k$ , оно также истинно и для  $n = k + 1$

Тогда утверждение истинно при всех положительных  $n$ .

**Утверждение.** Если уместна математическая индукция, то уместна и сильная индукция.

**Доказательство.** В дальнейших рассуждениях будем считать, что  $n$  - натуральное, большее или равное 1, а также обозначим утверждение зависящее от  $n$  за  $\varphi(n)$ .

Предположим, что для  $\varphi(n)$  выполняются условия (1) и (2) для сильной индукции.

Пусть  $\psi(k) \Leftrightarrow \langle \varphi(n) \text{ истинно для всех } n \leq k \rangle$ .

Попытаемся доказать, что утверждение  $\psi(n)$  истинно для всех положительных натуральных  $n$  по индукции. Как следствие, мы получим, что и  $\varphi(n)$  верно для всех положительных  $n$ , т.е. тот же вывод, который должен дать принцип сильной индукции.

**База.** В силу нашего предположения  $\varphi(1)$  истинно (гипотеза (1) сильной индукции верна), но тогда истинно и  $\psi(1)$ , по определению  $\psi(n)$ .

**Предположение.** Пусть верно  $\psi(k)$ .

**Шаг.** Мы предположили, что для  $\varphi(n)$  выполняются гипотезы сильной индукции, а значит, если  $\langle \varphi(n) \text{ верно для всех } n \leq k \rangle$ , то и  $\varphi(k + 1)$  - верно. По предположению индукции -  $\psi(k) \Rightarrow \varphi(k + 1)$  (см. определение  $\psi(n)$  и гипотезу (2) сильной индукции). Получаем, что  $\psi(k + 1)$  - истинно, т.к.  $\varphi(n)$  истинно для всех  $n \leq k + 1 \Rightarrow \psi(k + 1)$ .

Согласно принципу мат. индукции  $\psi(k)$  - верно для всех положительных  $k$ , значит утверждение  $\langle \varphi(n) \text{ истинно для всех } n \leq k \rangle$  верно при всех  $k$ , а значит  $\varphi(n)$  - верно для всех  $n$ .

Таким образом, из принципа мат. индукции следует принцип полной мат. индукции.  $\square$

## 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 слагаемых, в которых  $b$  встречается ровно  $k$  раз равно  $\binom{n}{k}$ . Тогда  $c = \binom{n}{k}$ , а значит:

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

□

## 4. Задача Муавра (решение уравнения $x_1 + \dots + x_m = k$ )

**Утверждение.** Число решений уравнения  $x_1 + x_2 + \dots + x_k = n$  в неотрицательных целых числах равно  $\binom{n+k-1}{k-1}$

*Доказательство.* Воспользуемся методом «шаров и перегородок». Пусть есть  $n$  шаров и  $k-1$  перегородок, тогда какая-то их расстановка однозначно задаёт решение уравнения:  $x_1$  – количество шаров перед первой перегородкой,  $x_2$  – между 1 и 2, и так далее, количество шаров после последней перегородки –  $x_k$ . Тогда число решений равно  $\binom{n+k-1}{k-1}$ .

Докажем справедливость данной формулы. Рассмотрим  $n$  одинаковых объектов, добавим к ним ещё  $k-1$  таких же объектов. Тогда, заменив какие-то  $k-1$  объектов на перегородки, мы получим разбиение множества из  $n$  элементов на  $k$  непересекающихся подмножеств. □

## 5. Доказательство формулы включений и исключений

**Определение** (Формула включений и исключений.). *Формула включений-исключений* — комбинаторная формула, позволяющая определить мощность объединения конечного числа конечных множеств, которые в общем случае могут пересекаться друг с другом.

**Утверждение.** Пусть  $A_1, A_2, \dots, A_n$  — конечные множества. Формула включений-исключений утверждает:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_i |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.$$

*Доказательство.* Рассмотрим произвольный элемент  $x \in \left| \bigcup_{i=1}^n A_i \right|$ , входящий в ровно  $S$  множеств  $A_{q_1}, \dots, A_{q_S}$  и подсчитаем, сколько раз он учитывается в правой части формулы включений-исключений (вернее покажем, что учитывается ровно 1 раз):

- В первой сумме  $\sum_i |A_i|$  элемент  $x$  посчитан ровно  $\binom{S}{1} = S$  раз (В слагаемых  $A_{q_1}, \dots, A_{q_S}$ ).
- Во второй сумме  $\sum_{i < j} |A_i \cap A_j|$  элемент  $x$  посчитан ровно  $\binom{S}{2}$  раз (количество попарных пересечений  $A_i \cap A_j$ , таких, что  $A_i, A_j \in A_{q_1}, \dots, A_{q_S}$ ).

- В третьей сумме  $\sum_{i < j < k} |A_i \cap A_j \cap A_k|$   $x$  будет посчитан  $\binom{S}{3}$  раз (количество пересечений  $A_i \cap A_j \cap A_k$  для которых  $i, j \in q_1, \dots, q_S$ ).
- ...
- В  $S$ -ой сумме  $\sum_{i_1 < i_2 < \dots < i_S} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_S}|$   $x$  будет посчитан  $\binom{S}{S} = 1$  раз ( $x$  войдет только в слагаемое  $|A_1 \cap A_2 \cap \dots \cap A_n|$ ).
- суммы, содержащие  $S + 1$  и более пересечений, не учитывают элемент  $x$ , поскольку  $x$  не входит в пересечение более чем  $S$  множеств.

Таким образом  $x$  оказывается посчитанным ровно  $S - \binom{S}{2} + \binom{S}{3} - \dots + (-1)^{S+1} \binom{S}{S}$  раз. Покажем, что эта сумма в точности равна 1. Воспользуемся биномом Ньютона:

$$0 = (1 - 1)^S = \sum_{k=0}^S \binom{S}{k} \cdot 1^{S-k} \cdot (-1)^k = 1 - \sum_{k=1}^S \binom{S}{k} \cdot 1^{S-k} \cdot (-1)^{k+1}$$

$$\Updownarrow$$

$$1 = \sum_{k=1}^S \binom{S}{k} \cdot (-1)^{k+1} = S - \binom{S}{2} + \binom{S}{3} - \dots + (-1)^{S+1} \binom{S}{S}$$

Таким образом, каждый  $x \in \left| \bigcup_{i=1}^n A_i \right|$  учитывается и левой и правой частью формулы ровно 1 раз, и очевидно, что все прочие  $y \notin \left| \bigcup_{i=1}^n A_i \right|$  не учитываются ни правой, ни левой частями.  $\square$

## 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.

## 8. Критерий двураскрашиваемости графа.

**Утверждение.** Неориентированный граф является 2-раскрашиваемым тогда и только тогда, когда в нём нет циклов нечётной длины.

*Доказательство.*  $\Rightarrow$  Пусть в графе есть цикл нечётной длины. Покрасим какую-то вершину цикла в первый цвет и будем двигаться по нему в одном направлении, крася каждую следующую вершину в противоположный цвет. Тогда, вернувшись в исходную вершину, получим противоречие.

$\Leftarrow$  Пусть циклов нечётной длины нет. Выберем произвольную вершину  $A$  и покрасим её в первый цвет. Для любой другой вершины  $B$  рассмотрим количество рёбер в пути  $A \rightarrow B$ .

Если есть два пути  $A \rightarrow B$  таких, что в одном чётное число рёбер, а в другом – нечётное, то есть цикл с нечётным числом рёбер, который получается, если пройти  $A \rightarrow B$  по первому пути и вернуться  $B \rightarrow A$  по второму.

Следовательно, между любыми двумя вершинами все пути либо чётной, либо нечётной длины. Раскрасить граф можно следующим образом:

- выделим остовное дерево, раскрасим корень в первый цвет
- раскрасим его потомков во второй цвет
- для каждого из потомков раскрасим всех его потомков опять в первый цвет, и.т.д

Полученная раскраска будет корректной, так как в остовном дереве любой путь между вершинами одного цвета имеет чётную длину (по построению), а по доказанному выше путей нечётной длины между такими вершинами нет.  $\square$

## 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.  $\square$

## 12. Эквивалентность определений дерева и графа с простым путём между любыми двумя вершинами.

**Утверждение.** Деревья это в точности графы, в которых для любых двух вершин есть ровно один простой путь с концами в этих вершинах.

*Доказательство.*  $\Rightarrow$

По определению дерева оно является связным графом без циклов. Рассмотрим какие-то две вершины  $a$  и  $b$ . Докажем, что существует ровно один простой путь между ними.

Поскольку дерево по определению связно, путь есть. Докажем его единственность.

Если есть несколько путей, то маршрут из  $a$  в  $b$  по первому пути и обратно по другому пути будет являться циклом – значит, путь только один.

$\Leftarrow$

Рассмотрим две вершины  $a$  и  $b$  данного графа, по условию между ними существует простой путь. Если таких путей несколько, то маршрут из  $a$  в  $b$  по первому пути и обратно по другому пути будет являться циклом. Следовательно, путей не более одного. Если же такого пути нет, то вершина  $b$  не достижима из  $a$ , то есть граф не связен. Следовательно, такой граф является деревом.  $\square$

### 13. Существование остовного дерева

**Определение.** *Частичный граф* исходного графа  $G = (V, E)$  — граф  $G' = (V, E')$ ,  $E' \subseteq E$ .

**Определение.** *Остовное дерево* связного графа  $G = (V, E)$  — всякий его частичный граф, являющийся деревом.

**Лемма.** *Если граф связен, то у него есть остовное дерево.*

*Доказательство.* Для начала докажем вспомогательную лемму:

**Лемма.** *Если граф связен и содержит хотя бы один цикл, то из него можно удалить ребро не нарушая связности.*

*Доказательство леммы.* Пусть  $G = (V, E)$  и цикл в нем:  $u_0 \rightarrow u_1 \rightarrow \dots u_n \rightarrow u_0$ ,  $u_i \in V$ . Поймем, что если удалить любое ребро принадлежащее циклу, связность не нарушится. Покажем в частности, что можно удалить ребро  $(u_0, u_1)$ . Действительно, если есть какой-нибудь путь из  $v \in V$  в  $w \in V$ , проходящий через ребро  $(u_0, u_1)$ , то существует путь проходящий через прочие ребра цикла, ведь в цикле до каждой вершины можно дойти хотя бы двумя разными путями, значит удаление ребра не изменит того факта, что  $v$  соединено путем с  $w$ . Если пути из  $v$  к  $w$  не содержат ребра  $(u_0, u_1)$ , то очевидно, что его удаление на их связи не отразится  $\Rightarrow$  граф без этого ребра останется связанным. Тогда удалим его и получим связный граф.  $\square$

Пусть теперь  $G = (V, E)$  — связный граф, для которого нужно доказать существование остовного дерева. Возможны два сценария:

1. Граф  $G$  — связный граф без циклов.
2. В графе  $G$  есть хотя бы один цикл.

В первом случае  $G$  — дерево по определению, а значит сам является своим остовным деревом.

Во втором случае, по доказанной лемме, мы можем удалить из  $G$  ребро не нарушая связности. Так сделаем же это. Если полученный граф — циклический, то снова удалим ребро не нарушая связности, иначе остановимся и порадуемся; индуктивно будем повторять описанные операции, на каждой итерации имея связный граф; число ребер в графе — конечно, значит процесс не может продолжаться вечно  $\Rightarrow$  в какой-то момент мы не сможем удалить ребро не нарушая связности, что было бы не возможно, если бы в графе остался цикл. В ходе описанных операций мы не добавляли новых ребер и не удаляли вершин  $\Rightarrow$  если  $G' = (V', E')$  — итоговый граф, то  $V' = V$ ,  $E' \subseteq E \Rightarrow G'$  — частичный граф графа  $G$ , связный и без циклов, т.е. дерево  $\Rightarrow G'$  по определению — остовное дерево графа  $G$ .  $\square$

### 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  $\square$

## 16. Критерий Дирака гамильтоновости графа.

**Утверждение.** Критерий Дирака: граф  $G$  на  $n$  вершинах содержит гамильтонов цикл, если каждая вершина графа имеет степень не меньшую, чем  $\frac{n}{2}$ .

*Доказательство.* Рассмотрим самую длинную простую цепь в графе, обозначим её  $x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_m$ . Докажем, что существует вершина  $x_i$  такая, что  $x_i \rightarrow x_m$  и  $x_{i+1} \rightarrow x_1$ .

Выберем из множества вершин этой цепи два подмножества номеров вершин ( $1 \leq i \leq m-1$ ):

- множество вершин из цепи, соединённых с последней вершиной  $x_m$ , то есть  $A = \{i | (x_i, x_m) \in E\}$
- множество вершин из цепи, соединённых со первой вершиной  $x_1$ , то есть  $B = \{i | (x_1, x_{i+1}) \in E\}$

Все соседние с вершиной  $x_m$ , находятся среди  $x_1 \dots x_{m-1}$ , так как в противном случае существует некая вершина  $x_k$  вне цепи и данная цепь не является самой длинной. Так как по условию степень вершины  $x_1 \geq \frac{n}{2}$ , то и  $|A| \geq \frac{n}{2}$ , аналогично  $|B| \geq \frac{n}{2}$ .

Тогда  $|A| + |B| \geq n$ , но по построению элементы данных множеств – это числа  $1 \leq i \leq m-1$ , это означает, что множества пересекаются и у них есть некоторый общий элемент  $j$ . Таким образом, в графе имеются ребра  $x_1 x_{j+1}$  и  $x_m x_j$ . Тогда рассмотрим цепь  $x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_j \rightarrow x_m \rightarrow x_{m-1} \rightarrow \dots \rightarrow x_{j+1} \rightarrow x_1$ , то есть простой цикл на  $m$  вершинах.

Если существует некая вершина вне этой цепи, то данная цепь не является самой длинной. Следовательно, в ней присутствуют все вершины из графа, то есть  $m = n$ , а найденный цикл является гамильтоновым.  $\square$

## 17. Сравнение $ax \equiv 1 \pmod{N}$ имеет решение тогда и только тогда, когда $(a, N) = 1$

**Замечание.** Здесь и далее условимся обозначать НОД( $a, N$ ), как  $(a, N)$ .

**Утверждение.** Сравнение  $ax \equiv 1 \pmod{N}$  имеет решение  $(1) \Leftrightarrow (a, N) = 1$  (2).

*Доказательство.* Докажем следствие  $(1) \Rightarrow (2)$

$$ax - 1 \equiv 0 \pmod{N}$$

$$\Downarrow$$

$$N | (ax - 1)$$

$$\Downarrow$$

$$(ax - 1) = Nk, k \in \mathbb{Z}.$$

Пусть  $(a, N) = b$  ( $1 \leq b$ , т.к. 1 - всегда делитель). Тогда  $a = a' \cdot b$ ,  $N = N' \cdot b \Rightarrow$

$$a'bx - 1 = N'bk$$

$\Downarrow$

$$1 = b(a'x - N'k)$$

По определению  $b|1$ , но тогда  $|b| \leq 1$ , но тогда  $b = 1 \Rightarrow (a, N) = 1$ .

Докажем следствие (2)  $\Rightarrow$  (1): (2)  $\Rightarrow (a, N) = 1$ , тогда по соотношению Безу  $\exists m, k : am + Nk = 1 \Rightarrow am = 1 - Nk \Rightarrow am \equiv 1 \pmod{N}$ , и  $x = m$  - решение сравнения  $ax \equiv 1 \pmod{N}$ .  $\square$

## 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  $x = \overline{a_n a_{n-1} \dots a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10a_1 + a_0$ . 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:

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

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

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

$\square$

## 20. Теорема Эйлера

**Теорема.** Пусть  $N$  - произвольное простое число,  $\varphi(N)$  - функция Эйлера (то есть число остатков от 0 до  $N-1$ ), а число  $a$  - один из этих остатков, взаимно простой с  $N$ . Тогда:

$$a^{\varphi(N)} \equiv 1 \pmod{N}$$

*Доказательство.* Поскольку  $a$  взаимно просто с  $N$  и  $x_i$  взаимно просто с  $N$ , то и  $x_i \cdot a$  также взаимно просто с  $N$ , то есть существует  $x_j$  такой, что  $x_i a \equiv x_j \pmod{N}$ .

Отметим, что все остатки  $x_i \cdot a$  различны по модулю  $N$ . Пусть это не так, тогда  $x_{i_1} a \equiv x_{i_2} a \pmod{N} \Rightarrow a(x_{i_1} - x_{i_2}) = 0$ , то есть  $x_{i_1} \equiv x_{i_2} \pmod{N}$  - это противоречит тому, что все остатки  $x_1 \dots x_{\varphi(N)}$  различны.

Перемножим все сравнения  $x_i \cdot a \equiv x_j \pmod{N}$ , получим

$$x_1 \cdots x_{\varphi(N)} a^{\varphi(N)} \equiv x_1 \cdots x_{\varphi(N)} \pmod{N} \quad x_1 \cdots x_{\varphi(N)} (a^{\varphi(N)} - 1) \equiv 0 \pmod{N}$$

Поскольку каждый из остатков  $x_1 \dots x_{\varphi(N)}$  взаимно прост с  $N$ , можно записать:

$$a^{\varphi(N)} - 1 \equiv 0 \pmod{N}$$

$\square$



## 21. Корректность алгоритма Евклида и расширенного алгоритма Евклида.

**Алгоритм Евклида.** Пусть  $a$  и  $b$  - целые числа одновременно не равные нулю, и последовательность чисел  $x_0 > x_1 > x_2 > x_3 \cdots > x_n > 0$  определена тем, что  $x_0 = a$ ,  $x_1 = b$ , каждое  $x_k$ ,  $k > 1$  — это остаток от деления предпредыдущего числа на предыдущее, а предпоследнее делится на последнее нацело, то есть:

$$a = x_0 q_1 + x_1,$$

$$b = x_1 q_2 + x_2,$$

$$x_2 = x_3 q_3 + x_4,$$

$\dots$

$$x_{k-2} = x_{k-1} q_{k-1} + x_k,$$

$\dots$

$$x_{n-2} = x_{n-1} q_{n-1} + x_n,$$

$$x_{n-1} = x_n q_n.$$

Тогда  $(a, b)$  равен  $x_n$ , последнему ненулевому члену этой последовательности.

*Доказательство.* Поймем, что такие  $x_1, x_2, x_3, x_4, \dots, x_n$  - существуют, причем единственно: всегда можно найти остаток  $m$  (причем единственным образом) при делении  $x_k$  на  $x_{k+1}$ , если  $x_{k+1} \neq 0$ , причем  $a > b > r_k > x_{k+1} > m$ , т.е. каждый следующий член последовательности строго меньше предыдущего, но т.к. числа ее составляющие - целые, то убывать бесконечно она не может, а значит  $\exists x_{n+1} = 0$  - последний член последовательности.

Докажем тогда, что если  $x_n$  - последний не нулевой член последовательности, то  $(a, b) = (x_n, 0) = x_n \neq 0$ . Для этого заметим две вещи:

1.  $r \neq 0 \Rightarrow (r, 0) = |r|$  так как 0 делится на любое целое число, кроме нуля.
2. Пусть  $a = bq + r$ , тогда  $(a, b) = (b, r)$ . Пусть  $k$  — любой общий делитель чисел  $a$  и  $b$ , не обязательно наибольший, тогда  $a = t_1 k$  и  $b = t_2 k$ , где  $t_1$  и  $t_2$  — целые числа из определения.

Тогда  $k$  является также общим делителем чисел  $b$  и  $r$ , так как  $b$  делится на  $k$  по определению, а  $r = a - b \cdot q = (t_1 - t_2 \cdot q) \cdot k$  (выражение в скобках есть целое число, следовательно,  $k$  делит  $r$  без остатка).

Обратное также верно. Любой делитель  $k$  чисел  $b$  и  $r$  так же является делителем  $a$  и  $b$ :  $a = b \cdot q + r = k \cdot (b'q + r') \Rightarrow k|a$ .

Следовательно, все общие делители пар чисел  $a, b$  и  $b, r$  совпадают. Другими словами, нет общего делителя у чисел  $a, b$ , который не был бы также делителем  $b, r$ , и наоборот.

В частности, наибольший общий делитель остается тем же самым. Что и требовалось доказать.

Тогда по построению последовательности  $\{x_i\} : (x_0, x_1) = (x_1, x_2) = (x_2, x_3) = \dots = (x_n, 0) = x_n$ .  $\square$

**Алгоритм Евклида** (Расширенный алгоритм Евклида). *Формулы для  $x_i$  могут быть переписаны следующим образом:*

$$\begin{aligned}x_0 &= aq_0 + bp_0, \\x_1 &= aq_1 + bp_1, \\x_2 &= aq_2 + bp_2, \\x_3 &= aq_3 + bp_3, \\&\vdots \\(a, b) &= x_n = as + bt\end{aligned}$$

*Т.е. НОД( $a, b$ ) можно представить в виде  $ax + by$ , где  $x, y$  - какие-то целые числа.*

*Доказательство.* Докажем по индукции по  $n$ .

*База.*  $x_0 = a + b \cdot 0$ ,  $x_1 = a \cdot 0 + b$ . Т.е.  $q_0 = P_1 = 1$ ,  $p_0 = q_1 = 0$

*Предположение.* Пусть  $x_{k-2} = aq_{k-2} + bp_{k-2}$  и  $x_{k-1} = aq_{k-1} + bp_{k-1}$ .

*Шаг.* Докажем, что  $x_k = aq_k + bp_k$ , где  $q_k, p_k$  - целые. Мы помним, что  $x_k$  - остаток от деления  $x_{k-2}$  на  $x_{k-1}$ , значит по определению:  $m \cdot x_{k-1} + x_k = x_{k-2}$ , где  $m$  - какое-то целое число. Тогда  $x_k = x_{k-2} - m \cdot x_{k-1}$ , по п.и.,  $x_k = aq_{k-2} + bp_{k-2} - m(aq_{k-1} + bp_{k-1}) = a(q_{k-2} - mq_{k-1}) + b(p_{k-2} - mp_{k-1}) = aq_k + bp_k$ .

Таким образом каждое из чисел  $x_i$  представимо в виде линейной комбинации  $a$  и  $b$  (В частности, если  $(a, b) = 1$ , то  $\exists x, y : ax + by = 1$ ).  $\square$

## 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.  $\square$

## 23. Китайская теорема об остатках

**Теорема.** Для любых попарно взаимно-простых  $a_1, a_2, \dots, a_n$  и для любых  $r_1, r_2, \dots, r_n$  таких, что  $0 \leq r_i < a_i$ , существует и единственен с точностью до операции взятия по модулю  $M = \prod_1^n a_i$   $x$  являющийся решением системы (1):

$$\begin{cases} x \equiv r_1 \pmod{a_1} \\ x \equiv r_2 \pmod{a_2} \\ \vdots \\ x \equiv r_n \pmod{a_n} \end{cases}$$

И любой  $x' \equiv x \pmod{\prod_1^n a_i}$  так же является решением этой системы.

(Иная формулировка: Если натуральные числа  $a_1, a_2, \dots, a_n$  попарно взаимно просты, то для любых целых  $r_1, r_2, \dots, r_n$  таких, что  $0 \leq r_i < a_i$  при всех  $i \in \{1, 2, \dots, n\}$ , найдётся число  $N$ , которое при делении на  $a_i$  даёт остаток  $r_i$  при всех  $i \in \{1, 2, \dots, n\}$ . Более того, если найдутся два таких числа  $N_1$  и  $N_2$ , то  $N_1 \equiv N_2 \pmod{a_1 \cdot a_2 \cdot \dots \cdot a_n}$ .)

*Доказательство.* Покажем, что  $x = \sum_{i=1}^n r_i M_i M_i^{-1} \pmod{M}$  (2), где  $M_i = \frac{M}{a_i}$ , а  $M_i^{-1}$  - обратный к  $M_i$  элемент по модулю  $a_i$ , является решением указанной выше системы.

Проверим, что для него выполняется  $i$ -е равенство в системе:

$$x \equiv \sum_{j=1}^n r_j M_j M_j^{-1} \equiv r_i M_i M_i^{-1} \equiv r_i \pmod{a_i}$$

Второе равенство справедливо т.к.  $M_j \equiv \prod_{k \neq j} a_k \equiv 0 \pmod{a_i}$  при всех  $i \neq j$  (т.е. все слагаемые кроме  $j$ -ого делятся на  $a_i$ ), третье т.к.  $M_i^{-1}$  является обратным для  $M_i$  по модулю  $a_i$ . Повторяя рассуждения для всех  $i$ , убедимся, что  $x$ , определенный формулой (2), является решением для (1).

В силу выбранного числа  $M$  все числа  $x' \equiv x \pmod{M}$  будут удовлетворять системе.

Покажем теперь, что среди чисел  $0, 1, \dots, M-1$  (множество  $A$ ) не найдется другого решения кроме найденного нами ранее. Проведем доказательство этого факта от противного. Предположим, что получилось найти хотя бы два решения  $x_1, x_2 \in A$  для некоторого набора остатков  $r$ . Так как множество  $B$  всех допустимых наборов  $(r_1, r_2, \dots, r_n)$  является равномошным множеству  $A$  (количество наборов остатков в  $B$ :  $|B| = a_1 \cdot a_2 \cdot \dots = M = |A|$ ), то для  $\bar{A}_x := A \setminus \{x_1, x_2\}$  и  $\bar{B}_r := B \setminus \{r\}$  выполнено  $|\bar{A}_x| < |\bar{B}_r|$ . Однако по доказанному ранее, для любого набора из  $\bar{B}_r$  существует решение из  $\bar{A}_x$ , следовательно по принципу Дирихле найдутся как минимум 2 набора остатков, которым соответствует одно и то же  $x \in A$ . Для такого  $x$  найдется  $a_i$  такое, что  $x \equiv r_1, x \equiv r_2 \pmod{a_i}$  и  $r_1 \neq r_2$ . Противоречие.  $\square$

## 24. Мультипликативность функции Эйлера. Формула для функции Эйлера

**Утверждение.** Для взаимно простых  $m$  и  $n$  верно, что  $\varphi(mn) = \varphi(m)\varphi(n)$

*Доказательство.*  $\square$

## 25. Доказательство корректности определения классов эквивалентности

**Теорема.** Для любого отношения эквивалентности на множестве  $A$  множество классов эквивалентности образует разбиение множества  $A$ . Обратно, любое разбиение множества  $A$  задает на нем отношение эквивалентности, для которого классы эквивалентности совпадают с элементами разбиения.

*Доказательство.* Докажем прямое следствие.

Каждому  $x \in A$  сопоставим  $[x] = \{y \mid x \sim y\}$  - по-множеству множество всех элементов с которыми  $x$  вступает в отношение  $\sim$ .

Утверждается, что система подмножеств  $[x]$  образует разбиение  $A$ . Действительно, во-первых, каждое подмножество  $[x] \neq \emptyset$ , так как в силу рефлексивности отношения  $\sim$   $x \in [x]$ .

Во-вторых, два различных подмножества  $[x]$  и  $[y]$  не имеют общих элементов. Рассуждая от противного, допустим существование элемента  $z$  такого, что  $z \in [x]$  и  $z \in [y]$ . Тогда  $z \sim x$  и  $z \sim y$ . Поэтому для любого элемента  $t \in [x]$  из  $t \sim x$ ,  $z \sim x$  и  $z \sim y$  в силу симметричности и транзитивности отношения а вытекает  $aPy$  ( $t \sim x$  и  $x \sim z \Rightarrow tPz$ , но  $z \sim y \Rightarrow t \sim y$ ), то есть  $a \in [y]$ . Следовательно,  $[x] \subseteq [y]$ . Аналогично получаем, что  $[y] \subseteq [x]$ . Полученные два включения влекут равенство  $[x] = [y]$ , противоречащее предположению о несовпадении подмножеств  $[x]$  и  $[y]$ . Таким образом,  $[x] \cap [y] = \emptyset$ .

В-третьих, объединение всех подмножеств  $[x]$  (классов эквивалентности) совпадает со множеством  $A$ , ибо для любого элемента  $x \in A$  выполняется условие  $x \in [x]$ .

Итак, система подмножеств эквивалентности  $[x]$ , образует разбиение множества  $A$ .

*Обратное следствие.*

Пусть есть разбиение  $A$  на непересекающиеся множества  $M_0, \dots, M_1$ . Тогда отношение эквивалентности на  $A$  задается так:

$$a \sim b \leftrightarrow (a \in M_i \wedge b \in M_i)$$

Свойства транзитивности, рефлексивности и симметричности очевидны ( Например для транзитивности:  $a \sim b$  и  $b \sim c$ , значит  $(a \in M_i \wedge b \in M_i) \wedge (b \in M_i \wedge c \in M_i) \Leftrightarrow (a \in M_i \wedge c \in M_i) \Leftrightarrow a \sim c$ ). Тогда, два элемента принадлежат одному классу тогда и только тогда, когда они лежат в одном подмножестве  $M_i$ , т.е. классы задаются разбиением.  $\square$

## 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  $(x, y) \in P$ .  $\square$

## 28. Теорема о представлении частичного порядка в виде пересечения линейных

**Теорема 1.** Любой частичный порядок, определенный на множестве из  $n$  элементов, можно представить, как пересечение не более, чем  $n^2$  линейных порядков.

*Доказательство.* Пусть у нас есть частичный порядок  $P$ . Рассмотрим несравнимую пару  $x$  и  $y$ . Образует новый частичный порядок  $P'$ , полученный из  $P$  добавлением сравнимости  $xPy$  и некоторых других для того, чтобы транзитивность сохранилась. Образует еще один частичный порядок  $P''$ , полученный из  $P$  добавлением сравнимости  $yPx$  и некоторых других сравнимостей для сохранения транзитивности. Тогда каждый из этих двух частичных порядков можем достроить до линейного порядка (по теореме Шпильрайна). Назовем их  $Lin_{P'}$  и  $Lin_{P''}$  соответственно.

Теперь оценим количество несравнимых пар. Всего пар в отношении может быть  $n \cdot n = n^2$  штук, однако нас не интересует порядок элементов внутри пар, тогда без учета порядка их не более  $2 \cdot \frac{n^2}{2!} = \frac{n^2}{2}$ . Получаем, что несравнимых пар также не более  $\frac{n^2}{2}$ . Тогда рассмотрим для каждой из них  $Lin_{P'}$  и  $Lin_{P''}$ , таких линейных порядков в сумме не более  $\frac{n^2}{2} = n^2$ . Теперь изучим, что будет, если их пересечь. В действительности, мы получим как раз  $P$ , так как если  $xPy$ , то она принадлежит и  $Lin_{P'}$ , и  $Lin_{P''}$ , иначе она будет принадлежать только одному из них, и тогда при пересечении её уже не будет.

*P.S.* Внимательный читатель скажет, что мы рассмотрели только случай, когда нам нужно получить строгий частичный порядок, однако на самом деле получение нестрогого обходится нам «дешево» и не влияет на нашу оценку, так как её можно осуществить параллельно с другими пересечениями.  $\square$

## 29. Критерий существования функции, обратной к данной. Критерий биекции в терминах обратной функции

**Критерий существования функции, обратной к данной.** Пусть  $f$  - функциональное соответствие  $f : X \rightarrow Y$ . Тогда обратное соответствие:  $f^{-1} = (y, x) | (x, y) \in f \iff f(x) = y$ .

**Замечание.**  $f^{-1}$  - функционально  $\iff f$  - инъективно.

*Доказательство.* Докажем  $\rightarrow$ .

Из того, что  $f^{-1}$  - функционально  $\Rightarrow \forall y \in Y : f^{-1}(y) = x$  и  $f^{-1}(y) = x' \Leftrightarrow x = x' \Rightarrow$  если  $f(x) = f(x') = y$ , то  $f^{-1}(y) = x = x'$ , что и означает инъективность  $f$ .

Докажем  $\leftarrow$ .

Из инъективности  $f \Rightarrow \forall y \in Y : f(x) = y$  и  $f(x') = y \Leftrightarrow x = x' \Rightarrow$  если  $(y, x) \in f^{-1}$  и  $(y, x') \in f^{-1}$ , то  $x = x' \Rightarrow f^{-1}$  - функционально.  $\square$

### Критерий биекции в терминах обратной функции

**Теорема.** Критерием биективности:

1. Если  $f$  - биекция  $A \leftrightarrow B$ , то  $f \circ f^{-1} = id_B$  и  $f^{-1} \circ f = id_A$ .
2. Если  $f$  - функция  $A \rightarrow B$  и существует  $g : B \rightarrow A$ , такая что  $f \circ g = id_B$  и  $g \circ f = id_A$ , то  $f^{-1} = g$  и  $f$  - биекция.

*Доказательство.* Утверждение 1 проверяется непосредственно, по свойствам биекции:  $\forall a \in A : f^{-1} \circ f(a) = a$  и  $\forall b \in B : f \circ f^{-1}(b) = b$ .

Докажем 2, проверив  $f$  на свойства биекции.

*Всюду определенность* Если  $f$  не всюду определена, то  $g \circ f(x) = g(f(x))$  - не всюду определена, а значит не тождественна, что противоречит гипотезе. Значит  $f$  - тотальна.

*Инъективность.* Пусть  $f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow x_1 = x_2$ .

*Сюръективность.* Пусть  $f$  не принимает значение  $b \in B$ , тогда  $f(g(\dots))$  не принимает значение  $b$ , значит  $f \circ g$  - не тождественна, что противоречит условию. Тогда  $\forall b \in B : \exists a \in A : f(a) = b$ .

Таким образом  $f$  - биекция. Тогда очевидно, что  $g = f^{-1}$  (проверяется поэлементно из композиции  $g \circ f = id_A$ ,  $f \circ g = id_B$ :  $(a, b) \in f \Rightarrow (b, a) \in g$  и аналогично, если  $(b, a) \in g$ , то  $(a, b) \in f$ ).  $\square$

## 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.