

Материалы для подготовки к коллоквиуму по дискретной математике Теоремы

ПМИ 2016

Орлов Никита, Рубачев Иван, Ткачев Андрей, Евсеев Борис

11 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 « $\varphi(n)$ верно для всех $n \leq k$ », 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 « $\varphi(n)$ истинно для всех $n \leq k$ » верно при всех k , а значит $\varphi(n)$ - верно для всех n .

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

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 $\binom{S}{3}$ раза (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

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 хотябы 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

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

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 предыдущего числа на предыдущее, а предпоследнее делится на последнее нацело, то есть:

$$a = x_0q_1 + x_1,$$

$$b = x_1q_2 + x_2,$$

$$x_2 = x_3q_3 + x_4,$$

$$\dots$$

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

$$\dots$$

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

$$x_{n-1} = x_nq_n.$$

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

Доказательство. Поймем, что такие $r_1, r_2, r_3, r_4, \dots, r_n$ - существуют, причем единственно: всегда можно найти остаток m (причем единственным образом) при делении r_k на r_{k+1} , если $r_{k+1} \neq 0$, причем $a > b > r_k > r_{k+1} > m$, 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: $x_0 = aq_0 + bp_0$, $x_1 = aq_1 + bp_1$, $x_2 = aq_2 + bp_2$, $x_3 = aq_3 + bp_3$: $(a, b) = x_n = as + bt$*

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