Материалы для подготовки к коллоквиуму по дискретной математике
Теоремы

ПМИ 2016
Орлов Никита, Рубачев Иван, Ткачев Андрей, Евсеев Борис

12 декабря 2016 г.

---

4. Задача Муавра (решение уравнения $xi_1 + \ldots + x_m = k$)

Утверждение. *Число решений уравнения $x_1 + x_2 + \ldots + x_k = n$ 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. □

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 $A \to B$.

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

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. $\square$

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 $x_1 \to x_2 \to \ldots \to x_m$. Докажем, что существует вершина x_i такая, что $x_i \to x_m$ и $x_{i+1} \to x_1$.

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 $x_1 \ldots x_{m-1}$, так как в противном случае существует некая вершина x_k вне цепи и данная цепь не является самой длинной. Тогда в A лежат не меньше, чем половина вершин в графе, то есть $|A| \geq \frac{n}{2}$, аналогично $|B| \geq \frac{n}{2}$.

Поскольку всего в графе n вершин, пересечение множеств A и B непусто, то есть найдётся вершина x_j с номером j такая, что она соединена с x_1 и x_m. Тогда рассмотрим цепь $x_{j+1} \to x_{j+2} \to \ldots \to x_m \to x_j \to x_{j-1} \to \ldots \to x_2 \to x_1 \to x_{j+1}$, 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 найденый цикл является гамильтоновым. $\square$

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:*

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

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 $x_i a \equiv x_j \bmod N$.

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

Перемножим все сравнения $x_i \cdot a \equiv x_j \bmod N$, получим

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

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

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

$\square$

24. Мультипликативность функции Эйлера. Формула для функции Эйлера

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

Доказательство. □