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 следущие 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 следущие условия:*

- *1. Утверждение истинно для $n = 1$*
- *2. Если утверждение истинно для всех $n \leqslant k$, 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 дальньейших 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 $\psi(k) \Leftrightarrow$ «$\varphi(n)$ истинно для всех $n \leqslant k$».

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 опеределению $\psi(n)$.

Предположение. Пусть верно $\psi(k)$.

Шаг. Мы предположили, что для $\varphi(n)$ выполняются гипотезы сильной индукции, а значит, если «$\varphi(n)$ верно для всех $n \leqslant k$», 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 $n \leqslant k+1 \Rightarrow \psi(k+1)$.

Согласно принципу мат. индукции $\psi(k)$ - верно для всех положительных k, занчит утверждение «$\varphi(n)$ истинно для всех $n \leqslant k$» верно при всех k, а значит $\varphi(n)$ - верно для всех n.

Таким образом, из принципа мат. индукции следует принцип полной мат. индукциию. □

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 $\dfrac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \dfrac{n!}{k!(n-k)!}$ неупорядоченных наборов. □

Формула бинома Ньютона имеет вид:

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

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:

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

□

3. Основные свойства треугольника Паскаля

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

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

Доказательство. Рассмотрим произвольный элемент $x \in \left|\bigcup_{i=1}^{n} A_i\right|$, входящий в ровно S множеств $A_{q_1}, \ldots A_{q_S}$ 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 $A_{q_1}, \ldots A_{q_S}$).
- Во второй сумме $\sum_{i<j} |A_i \cap A_j|$ элемент x посчитан ровно $\binom{S}{2}$ раз (количесво попарных пересечений $A_i \cap A_j$, таких, что $A_i, A_j \in A_{q_1}, \ldots A_{q_S}$).
- 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 $i, j \in q_1, \ldots q_S$).

  ...
- В S-ой сумме $\sum_{i_1<i_2<\ldots<i_S} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_S}|$ x будет посчитан $\binom{S}{S} = 1$ раз (x войдет только в слагаемое $|A_1 \cap A_2 \cap \ldots \cap A_n|$).
- 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 $S - \binom{S}{2} + \binom{S}{3} - \ldots + (-1)^{S+1}\binom{S}{S}$ раз. Покажем, что эта сумма в точности равна 1. Воспользуемся биномом Ньютона:

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

$$\Updownarrow$$

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

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. □

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. □

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 «=» число ребер равно также и сумме исходящих вершин. □

7. Нижняя оценка числа связных компонент в неориентированном графе

Теорема 1. *Число компонент связности в графе не меньше, чем разность количества вершин и ребер*

Доказательство. Докажем по индукции по вершинам.

База индукции. При $n = 1$ граф состоит из одной вершины, которая является единственной компонентой связности в графе. Разность количества вершин и ребер равно 1, база доказана.

Шаг индукции. Пусть для всех графов на n вершинах выполняется эта оценка, добавим еще одну вершину и рассмотрим случай связи, при котором сумма количества компонент связности и количество ребер наименьшая: выберем такой граф на n вершинах (C - количество компонент связности в этом графе, E - количество ребер в этом графе), чтобы в нем эта сумма была наименьшей и добавим к нему еще одну вершину. Заметим, что если связать новую вершину хотя бы одним ребром с k уже существовавшими компонентами связности, то количество ребер увеличится, как минимум, на k, а компонент связности станет на$k-1$меньше, чем в графе наn вершинах. (Если не связывать, то станет на одну больше, так как будет еще одна компонента связности, если связать компоненты связности, то они станут одной компонентой связности, то есть количество уменьшится на единицу.) Так как нужна наименьшая сумма, то нужно использовать, как можно меньше ребер: будем соединять вершину 1 ребром с каждой из k существовавших компонентов связности - ребер станет на k больше, а количество компонентов связности уменьшится на $k - 1$, то есть сумма компонентов связности и ребер нового графа будет такой: $(C + 1 - k) + (E + k) = C + E + 1$. Но $C + E + 1 \geq V + 1$ из $C + E \geq V$. Значит для $n + 1$ оценка верна. □

10. Деревья – это в точности минимально связные графы

Доказательство.

[⇒] 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 $v_1, a_1, a_2, \ldots, a_k, v_2$, а значит в G_{n+1} существует цикл $v_1, a_1, a_2, \ldots, a_k, v_2, u, v_1$, 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. □

11. Деревья - это в точности связные графы с $n-1$ ребром

Доказательство. Докажем в обе стороны.

$\Rightarrow$. Докажем по индукции по вершинам.

База индукции. Для $n=2$ существует в точности одно дерево, для которого утверждение очевидно.

Шаг индукции. Пусть есть дерево на n вершинах, в котором в точности $n-1$ ребро. Если мы добавим в него вершину, нам необходимо будет ее связать с графом. Если мы проведем из нее больше одного ребра мы получим цикл, так как между проведенными вершинами существовал единственный путь. Добавлением двух ребер мы замкнули цикл, а значит мы не можем добавить больше одного ребра. Тогда получается, мы можем добавить в точности одно ребро, а значит и число ребер увеличилось на один, а значит и утверждение доказано.

$\Leftarrow$. См. пункт 10.

□

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: $u_0 \to u_1 \to ...u_n \to u_0$, $u_i \in V$. Поймем, что если удалить любое ребро принадлежащее цикул, связность не нарушится. Покажем в частности, что можно удалит 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. □

Пусть теперь $G = (V, E)$ - связный граф, для которого нужно доказать существование остовног 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 - цикличен, то снова удалим ребро не нарушая связности, иначе остановимся и порадуемся; индуктивно будем повторять описанные операции, на каждой иттерации 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 цилов, т.е. дерево $\Rightarrow G'$ по определению - остовное дерево графа G. □

15. Критерий существования эйлерова цикла в орграфе

Теорема 2. *Орграф содержит эйлеров цикл тогда и только тогда, когда он сильно связен и у любой вершины входящая степень равна степени исходящей.*

Доказательство. $\Rightarrow$. Пусть эйлеров цикл есть. Тогда он проходит через все вершины и по нему можно пройти от любой вершины до любой другой, а значит, он сильно связен.

Возьмем произвольную вершину v в графе и пусть она встречается в цикле k раз. Тогда, идя по циклу, мы придем в нее k раз и уйдем из нее k раз. При этом, так как цикл эйлеров, мы должны пройти все ребра, а значит мы должны выйти и войти в вершину одинаковое количество раз. Значит, входящая и исходящая степени равны.

$\Leftarrow$. Будем рассматривать пути, которые не проходят дважды по одному ребру. (Таков, например, путь, состоящий из одного ребра) Выберем среди них самый длинный путь $a_1 \to a_2 \dots a_n$ и покажем, что он является искомым циклом, то есть что $a_1 = a_n$ и что он содержит все рёбра. Если он самый длинный, то добавить к нему ребро $an \to a_{n+1}$ уже нельзя, то есть все выходящие из an рёбра уже использованы (иначе мы нашли бы длиннее). Это возможно, лишь если $a_1 = a_n$. Почему? В самом деле, если вершина a_n встречалась только внутри пути(то есть не являлась началом пути) (пусть она входит k раз внутри пути и ещё раз в конце пути), то мы использовали $k+1$ входящих рёбер и k выходящих, и больше выходящих нет(путь самый длинный). Это противоречит равенству входящей и исходящей степени. Если во всех вершинах цикла использованы все рёбра, то из вершин этого цикла нельзя попасть вне цикла, то есть использованы все вершины (мы предполагаем, что граф связен или сильно связен) и, следовательно, все рёбра. Если из какой-то вершины a_i выходит ребро $a_i \to v$, то путь можно удлинить до $a_i \to a_{i+1} \to \dots \to a_n = a_1 \to a_2 \to \dots \to a_i \to v$, вопреки нашему выбору (самого длинного пути). Если в какую-то вершину a_i входит ребро $v \to a_i$, добавим v в начало, тем самым удлинив путь, что опять же противоречит нашему выбору самого длинного пути. $\square$

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

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

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

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

$$ax - 1 \equiv 0\ (mod\ N)$$

$$\Downarrow$$

$$N|(ax-1)$$

$$\Downarrow$$

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

Пусть $(a,\ N) = b$ ($1 \leqslant b$, 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 $|b| \leqslant 1$, но тогда $b = 1 \Rightarrow (a,\ N) = 1$.

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

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. □

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

$$11 \Big| \Big(\sum_{2|i}^{n} a_i - \sum_{2\nmid i}^{n} a_i \Big)$$

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

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

□

19. Малая теорема Ферма и лемма Вильсона

Теорема 3. *Пусть p - простое и a, такое, что оно не делится на p. Тогда утверждается, что*

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Доказательство. Сперва докажем следующую лемму: Умножение остатков $1, 2, 3, \dots, p-1$ на a даст те же остатки, но в другом порядке. *Доказательство от противного.* Пусть нашлись каких-то два числа ax и ay, дающих одинаковый остаток при делении на p (x и y — остатки). Тогда $a(x-y)$ делится на p, что невозможно. Тогда нет совпадающих остатков. Так как произведений, как и остатков, $p-1$, то лемма верна.

Рассмотрим произведения $a, 2a, 3a, \dots, (p-1)a$. Тогда

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv a^{p-1}(p-1)! \ (mod\ p)$$

С другой стороны, по лемме это эквивалентно $(p-1)!$ по модулю p. Тогда $a^{p-1} \equiv 1 \ (mod\ p)$, что и требовалось доказать. □

21. Корректность алгоритма Евклида и расширенного алгоритма Евклида.

Алгорим Евклида. *Пусть a и b - целые числа одноверемненно 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 $r_1, r_2, r_3, r_4, \cdots r_n$ - 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, rсовпадают. 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 $\{x_i\}$: $(x_0,\ x_1) = (x_1,\ x_2) = (x_2,\ x_3) = \dots = (x_n,\ 0) = x_n$. □

Алгорим Евклида (Расширенный алгоритм Евклида)**.** *Формулы для x_i могут быть переписаны следующим образом:* $x_0 = aq_0 + bp_0,\ x_1 = aq_1 + bp_1,\ x_2 = aq_2 + bp_2\ x_3 = aq_3 + bp_3 \vdots$ $(a,\ b) = x_n = as + bt$

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 определнию: $m \cdot x_{k-1} + x_k = x_{k-2}$, 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 $\exists x,\ y : ax + by = 1$). □