Сибирский математический журнал
Июль—август, 2009. Том 50, № 4

УДК 512.543.14

ЭКОНОМНАЯ ОТДЕЛИМОСТЬ В СВОБОДНЫХ ГРУППАХ

Н. В. Бускин

Аннотация. Пусть F_n — свободная группа ранга n с базисом X. В [1, проблема 15.35] О. В. Богопольский выдвинул гипотезу, что любой элемент $w \in F_n$ длины $|w| \geq 2$ относительно X может быть отделен подгруппой $H \leq F_n$ индекса $\leq C \ln |w|$ с некоторой константой C. Доказывается истинность гипотезы при условии $w \notin [F_n, F_n]$, где $[F_n, F_n]$ — коммутант группы F_n, и отделимость подгруппой индекса $\leq \frac{|w|}{2} + 2$ в общем случае.

Ключевые слова: отделимость подгруппами.

§ 1. Введение

Пусть G — группа. Говорят, что элемент $g \in G$ *отделяется подгруппой* $H \leq G$, если $w \notin H$. Пусть $F_n = F(x_1, \dots, x_n)$ — свободная группа ранга n. О. В. Богопольский выдвинул следующую гипотезу.

Гипотеза [1, проблема 15.35]. *Элемент $w \in F_n$ длины $|w| \geq 2$ отделяется некоторой подгруппой индекса $\leq C \ln |w|$, где константа C зависит только от n.*

Есть и другие варианты этой проблемы. Сравнительно недавно появились работы, посвященные экономной отделимости *нормальными* подгруппами. Из результатов работы [2] следует, что элемент w свободной группы F_n, $n \geq 2$, отделяется нормальной подгруппой индекса $O(|w|^3)$.

В работе И. Ривина [3] утверждается, что если элемент w лежит в $\gamma_k F_n \setminus \gamma_{k+1} F_n$, то w отделяется нормальной подгруппой индекса $O(\ln^k |w|)$. При этом в [4] доказано, что $k = O(\sqrt{|w|})$.

В настоящей работе исследуется экономная отделимость произвольными подгруппами конечного индекса, причем методы исследования отличаются от методов, использованных в работах [2, 3].

Оценка, полученная здесь, гораздо слабее предложенной в гипотезе, но тем не менее является оригинальным результатом, составляющим основное содержание настоящей работы.

Теорема. *Элемент $w \in F_n$, $w \neq 1$, отделяется подгруппой индекса $i \leq \frac{|w|}{2} + 2$.*

Доказательство этой теоремы будет дано в § 2. В процессе доказательства мы будем предполагать, что читатель знаком с заданием подгрупп группы F_n как фундаментальных групп размеченных графов, накрывающих букет n окружностей (см., например, [5]).

Работа выполнена при поддержке гранта АВЦП Минобразования России «Развитие научного потенциала высшей школы» (проект 2.1.1.419).

Докажем утверждение гипотезы в предположении, что $w \notin [F_n, F_n]$. Рассмотрим для начала пример, когда длина w нечетна. В группе F_n имеется подгруппа индекса 2, состоящая в точности из всех элементов $w \in F_n$, имеющих четную длину, и называемая *подгруппой четных слов*. Таким образом, любой элемент нечетной длины отделяется подгруппой четных слов.

Рассмотрим общий случай. Так как $w \notin [F_n, F_n]$, для одного из порождающих $a \in \{x_1, \dots, x_n\}$ суммарная степень $\sigma_a(w)$ этого порождающего в слове $w = w(x_1, \dots, x_n)$ отлична от нуля. Пусть $\varphi : F_n \to \mathbb{Z}$ — гомоморфизм такой, что $\varphi(a) = 1$ и $\varphi(x_j) = 0$ для любого порождающего $x_j \neq a$.

Определим функцию $d : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, считая, что $d(t)$ равно наименьшему целому положительному числу, не делящему t. Например, $d(1) = 2$, $d(2) = 3$, $d(2k+1) = 2$, где k — произвольное целое число.

Пусть $\psi : \mathbb{Z} \to \mathbb{Z}_{d(\sigma_a(w))}$ — канонический гомоморфизм. Тогда образ w относительно $\psi \circ \varphi$ нетривиален. Значит, w отделяется нормальной подгруппой $H = \operatorname{Ker} \psi \circ \varphi$ индекса $d(\sigma_a(w))$ в F_n. Так как $|\sigma_a(w)| \leq |w|$, достаточно доказать, что функция $d(t)$ оценивается сверху логарифмом $C \ln |t|$.

Для этого достаточно доказать существование констант $C_1 > 0$, $C_2 > 0$ таких, что $d(t) \leq C_1 \ln |t| + C_2$, $t \in \mathbb{Z} \setminus \{0\}$. Действительно, если это будет доказано, то можно подобрать константу C такую, что $d(\sigma_a(w)) \leq C_1 \ln |\sigma_a(w)| + C_2 \leq C \ln |w|$ для любого w такого, что $\sigma_a(w) \neq 0$ и $|w| \geq 2$. Здесь нам понадобятся следующие результаты, известные из анализа и элементарной теории чисел.

Лемма 1. *Для любого $k \in \mathbb{N}$ выполняется $\left(\frac{k}{e}\right)^k \leq k!$.*

Как несложно видеть, эта лемма является следствием формулы Стирлинга.

Лемма 2. *Пусть $\pi(m)$ — число простых чисел, не превосходящих m, где $m \geq 2$. Существует константа $c > 0$ такая, что $c\frac{m}{\ln m} < \pi(m)$.*

Утверждение этой леммы есть часть двойного неравенства, доказанного Чебышёвым: $c_1 \frac{m}{\ln m} < \pi(m) < c_2 \frac{m}{\ln m}$ (см., например, [6]).

Докажем требуемое неравенство для $d(t)$. Пусть $p_1, \dots, p_k$ — все простые числа, не превосходящие $m = d(t) - 1$. Тогда так как эти простые числа строго меньше $d(t)$, то $p_1, p_2, \dots, p_k | t$, а значит, $p_1 p_2 \dots p_k | t$, откуда вытекает, что $k! \leq p_1 p_2 \dots p_k \leq |t|$. Из этого неравенства и леммы 1 следует, что $\left(\frac{k}{e}\right)^k \leq |t|$. Логарифмируя, получаем

$$k(\ln k - 1) \leq \ln |t|. \tag{$*$}$$

Из леммы 2 вытекает, что $c\frac{m}{\ln m} < k$. Подставляя $c\frac{m}{\ln m}$ вместо k в неравенство $(*)$ (левая часть $(*)$ — строго возрастающая функция k), получаем, что $c\frac{m}{\ln m}(\ln c + \ln m - \ln(\ln m) - 1) \leq \ln |t|$. При больших m левая часть последнего неравенства имеет порядок cm, значит, для любого $\varepsilon \in (0, c)$ найдется $N(\varepsilon) \in \mathbb{N}$ такой, что при всех $m \geq N(\varepsilon)$ выполнено $(c - \varepsilon)m \leq \ln |t|$. Тем самым для любого m выполняется $(c - \varepsilon)m \leq \ln |t| + (c - \varepsilon)N(\varepsilon)$, что влечет требуемое неравенство для $d(t)$.

§ 2. Доказательство теоремы

Будем доказывать теорему для случая $n = 2$, $F_2 = F(a, b)$. Все рассуждения легко переносятся на общий случай. Пусть $B(a, b)$ — букет двух окружностей, размеченных буквами a и b. Будем работать в категории графов, размеченных буквами a и b, имеющих выделенную вершину и определяющих конечнолистные накрытия графа $B(a, b)$.

Во-первых, можно считать, что w принадлежит подгруппе четных слов (в противном случае для данного w утверждение теоремы очевидно) и, следовательно, имеет четную длину. Пусть $|w| = 2(i-1)$ для подходящего i. Докажем, что существует подгруппа индекса $\leq i{+}1$, не содержащая w, или, что равносильно, существует размеченный граф Γ, определяющий $\leq i+1$-листное накрытие букета $B(a,b)$, такой, что путь с меткой w, начинающийся в базисной вершине графа Γ, не замкнут. Далее любой размеченный граф, определяющий конечнолистное накрытие букета $B(a,b)$, будем называть иногда *графом-накрытием*.

Как обычно, обозначим для графа Γ через $v(\Gamma)$, $e(\Gamma)$ множества его вершин и ребер. Для графа с разметкой будем называть *c-ребром* любое его ребро, имеющее метку c или c^{-1}. Для ребра графа e обозначаем через $\bar{e}$ то же ребро, проходимое в обратном направлении, аналогично для пути γ определяется путь $\bar{\gamma}$. Для произвольной петли (т. е. ребра, у которого начало и конец совпадают) e введем естественные обозначения: $e^k = e \dots e$ (k раз) при $k > 0$ и $e^k = \bar{e} \dots \bar{e}$ ($|k|$ раз) при $k < 0$. Путь с меткой w будем обозначать через γ_w независимо от того, в каком графе он рассматривается (для размеченных графов, соответствующих накрытиям, путь с началом в фиксированной вершине однозначно определяется своей меткой). Условимся называть *прямым* ребро, не являющееся петлей.

Опишем в общих чертах процесс поиска графа, определяющего $\leq i+1$-листное накрытие для $B(a,b)$, такого, что путь с меткой w, начинающийся в базисной вершине этого графа, не замкнут. Сначала введем необходимые в дальнейшем операции I и II, которые позволяют получать из графов-накрытий новые графы-накрытия.

Пусть дан граф-накрытие Γ и $e \in e(\Gamma)$ — некоторое его c-ребро, $c \in \{a,b\}$.

Операция I. Введем новую вершину v, разбивающую ребро e на два c-ребра и приклеим в вершине v d-петлю, где $d \in \{a,b\} \setminus \{c\}$ (рис. 1).

Рис. 1.

Рис. 2.

Операция II$_k$. Пусть $e \in e(\Gamma)$ — c-петля, началом и концом которой является вершина v. Удалим эту петлю и приклеим к вершине v цикл C (отождествляя v и некоторую вершину C), состоящий из k штук c-ребер. К каждой вершине цикла C, кроме v, приклеим d-петлю, $d \in \{a,b\} \setminus \{c\}$, так, что вновь полученный граф будет снова определять накрытие (рис. 2).

Можно сказать, что операция II$_k$ заключается в k-кратном применении операции I.

Процесс поиска начинается с некоторого стартового графа Γ_1, определяющего накрытие листности $\leq i$. Если Γ_1 не подходит (γ_w замкнут в Γ_1), то рассматриваем графы, получающиеся из Γ_1 с помощью операции I. Операция I, примененная к произвольному ребру графа Γ_1, увеличивает число его вершин на 1. Если все графы, полученные с помощью операции I, не подходят (т. е. γ_w замкнут во всех этих графах, это важно!), то для некоторого $s > 1$ с помощью операции II_s из графа Γ_1 будет получен либо граф-накрытие Γ' с числом вершин $\leq i+1$ такой, что путь γ_w не замкнут в Γ', либо граф-накрытие $\Gamma_2 \neq \Gamma_1$ с числом вершин $\leq i$.

Если реализуется вторая возможность, то рассматриваем графы-накрытия, получаемые уже из Γ_2 с помощью операции I: если среди них нет подходящего, то, как и на предыдущем шаге, из графа Γ_2 с помощью операции II будет получен требуемый граф Γ' либо граф $\Gamma_3 \notin \{\Gamma_1, \Gamma_2\}$ с числом вершин $\leq i$. Так шаг за шагом построим последовательность графов-накрытий $\Gamma_1, \Gamma_2, \dots, \Gamma_k$ с условием $|v(\Gamma_j)| \leq i$ для $j = 1, \dots, k$. Ясно, что такой процесс поиска конечен и для некоторого k либо Γ_k будет искомым, либо искомый граф содержится среди графов с числом вершин $\leq i+1$, получающихся из Γ_k с помощью операций I и II.

Приступим к более подробному описанию нашего алгоритма. Пусть в приведенной записи w начинается с буквы a, т. е. $w = a^t b^s \dots$, где $t \neq 0$. Положим $h(t) = |t| + 1$, если $|t| \leq 2$, иначе $h(t) = \left[\frac{|t|}{2}\right] + 1$. Ясно, что $h(t)$ не делит t.

Стартовый граф. Рассмотрим граф Γ_1, у которого все a-ребра составляют цикл длины $h(t)$, а b-ребра суть петли с началом в вершинах этого цикла (рис. 3, пример для $|t| = 8$), x — отмеченная вершина.

Рис. 3.

Стрелка показывает направление, в котором γ_w обходит цикл C_1, образованный a-ребрами графа Γ_1. Ориентации ребер не фиксированы, поэтому рис. 3 отражает оба случая $t = \pm 8$. Вершина v_1 графа Γ_1 является концом пути γ_{a^t} с началом в x (первый слог w). Так как $h(t)$ не делит t, то $v_1 \neq x$. Граф Γ_1 определяет $h(t)$-листное накрытие букета $B(a,b)$ и, таким образом, соответствует некоторой подгруппе индекса $h(t)$. Если слово w имеет слоговую длину 1, т. е. $w = a^t$, то $h(t) \leq \frac{|w|}{2} + 2$ и граф Γ_1 будет искомым.

Будем считать теперь, что слоговая длина w не меньше 2. В этом случае также верно неравенство $h(t) \leq \frac{|w|}{2} + 2 = i+1$. На самом деле в случае слоговой длины 2 путь γ_w также не замкнут, случай слоговой длины 3 сопряжением (или применением описанной конструкции к единственному b-слогу b^s) сводится к случаю слоговой длины 2 или 1, так что по-настоящему интересным является случай слоговой длины ≥ 4.

Если путь γ_w не замкнут в графе Γ_1, то все доказано.

Допустим, что путь γ_w замкнут. Предположим, что для некоторого ребра e_a с меткой a суммарное число вхождений ребер $e_a, \bar{e}_a$ в путь γ_w равно 1 (т. е. в пути γ_w встречается ровно одно из двух ориентированных ребер $e_a, \bar{e}_a$ и ровно один раз). Пусть для определенности в путь γ_w входит ребро e_a. Начало и конец ребра e_a обозначим через p и q. Тогда $\gamma_w = \gamma_1 e_a \gamma_2$, подпути γ_1 и γ_2 не содержат вхождений $e_a, \bar{e}_a$. Применим к ребру e_a операцию I, новую вершину обозначим через v (рис. 4).

Рис. 4.

Ясно, что новый граф Γ' соответствует подгруппе индекса $\leq i+1$. Из равенства $\gamma_w = \gamma_1 e_a \gamma_2$ для слова w имеем приведенное представление $w = w_1 a w_2$, где подслова w_1, w_2 суть метки подпутей γ_1, γ_2 соответственно. В графе Γ' концы путей с метками $w_1 a$ и w_2^{-1}, начинающихся в вершине x, не совпадают (это вершины v и q), значит, путь γ_w не может быть замкнутым в этом графе. Таким образом, мы нашли подгруппу индекса $\leq i+1$, не содержащую w.

Точно так же можно отделить слово w подгруппой индекса $\leq i+1$, если для некоторой b-петли суммарное число вхождений этой петли в путь γ_w равно 1. Если путь γ_w замкнут в графе Γ_1 и любое ребро из Γ_1 входит в γ_w без учета ориентации по крайней мере дважды, то мы переходим к следующему шагу алгоритма.

Шаг алгоритма. Предположим, что для некоторого $k \geq 1$ уже построен граф Γ_k с отмеченными вершинами $v_1, \ldots, v_k$ с условием $|v(\Gamma_k)| \leq i$, имеющий вид, как на рис. 5.

Рис. 5.

Вершина v_j, где $j = 1, \ldots, k$, является концом подпути α_j пути γ_w, соответствующего первым j слогам слова w. Индекс c в символе e_c — это одна из букв a, b; $d \in \{a, b\} \setminus \{c\}$. При $k = 1$ есть единственный цикл C_1 и мы имеем граф Γ_1. Цикл C_j, $1 \leq j \leq k$, в этом графе соответствует j-му слогу $c^{\pm s_j}$, $c \in \{a, b\}$, слова w: он состоит из $h(s_j)$ c-ребер, где s_j — длина j-го слога w. Для простоты изображена конкретная ситуация, когда первые k слогов имеют длину 8.

Сделаем необходимое для дальнейшего замечание: если l_j, $1 \leq j \leq k$, — число различных пар прямых ребер $\{e, \bar{e}\}$ из цикла C_j графа Γ_k таких, что e или $\bar{e}$ входит в подпуть β_j пути γ_w, соответствующий j-му слогу слова w и начинающийся в вершине $v_{j-1} (v_0 = x)$, то

(A) $|C_j| = h(s_j) \leq l_j + 1$.

Эти неравенства легко проверяются (достаточно проверить неравенство для $j = 1$, остальные получаются аналогично).

Если путь γ_w не замкнут в Γ_k, то мы нашли требуемый граф. Если γ_w замкнут, то, так как вершина v_k — это конец пути α_k, соответствующего первым k слогам слова w, петля e_c обязана входить в путь γ_w. Далее, если есть ребро e графа Γ_k такое, что суммарное число вхождений ребер $e, \bar{e}$ в γ_w равно 1 (т. е. в γ_w входит только одно из ребер $e, \bar{e}$ и ровно 1 раз), то операция I, примененная к этому ребру, даст граф с числом вершин $\leq i+1$ такой, что путь γ_w не будет замкнутым в этом графе.

Пусть теперь путь γ_w замкнут в любом графе, полученном из Γ_k с помощью операции I. В частности, выполнено следующее условие.

(B) *Для каждого ребра e графа Γ_k, входящего в путь γ_w, суммарное число вхождений ребер $e, \bar{e}$ в γ_w не меньше* 2.

Отсюда, кстати, следует, что $2k \leq 2(l_1 + \cdots + l_k) \leq |\gamma_w| = |w|$. Как сказано в наброске алгоритма в начале доказательства теоремы, наша цель — с помощью операции II построить либо Γ', который будет искомым, либо Γ_{k+1}. Для понимания того, какая из этих возможностей реализуется, важно знать число вхождений петель $e_c, \bar{e}_c$ в путь γ_w в графе Γ_k и расположение этих вхождений.

Выделим первое вхождение петли e_c в путь γ_w. Здесь есть несколько случаев (суммарное число вхождений $e_c, \bar{e}_c$, конечно же, не менее 2):

1a) $\gamma_w = \gamma_1 e_c^{\pm 2} \gamma_2$, подпути γ_1 и γ_2 не содержат вхождений петли e_c и обратной к ней;

1b) $\gamma_w = \gamma_1 e_c^s \gamma_2, s \in \mathbb{Z}, |s| > 2$, условия на γ_1 и γ_2 те же, что и в п. 1a;

2a) $\gamma_w = \gamma_1 e_c^{\pm 1} \gamma_2$, здесь подпуть γ_1 не содержит вхождений петли e_c и обратной к ней, а для подпути γ_2 суммарное число вхождений этих ребер равно по меньшей мере 1, при этом γ_2 не начинается с $e_c, \bar{e}_c$;

2b) $\gamma_w = \gamma_1 e_c^{\pm 2} \gamma_2$, условия на γ_1, γ_2 те же, что и в п. 2a;

2c) $\gamma_w = \gamma_1 e_c^s \gamma_2, |s| > 2$, условия на γ_1, γ_2 те же, что и в п. 2a.

Покажем, что в первой группе случаев 1a, 1b можно построить граф Γ', во второй группе 2a, 2b, 2c построим Γ_{k+1}.

Рассмотрим случай 1a. Пусть для определенности $\gamma_w = \gamma_1 e_c e_c \gamma_2$. В этом случае из условия (B) и определения чисел l_j следует, что $2l_1 + \dots + 2l_k + 2 \leq |\gamma_w| = |w| = 2(i-1)$ (слагаемое 2 возникает как вклад подпути $e_c e_c$ в длину пути γ_w), откуда получаем $l_1 + \dots + l_k + 1 \leq i - 1$. Применим к петле e_c операцию $\mathrm{II}_{h(2)}, h(2) = 3$ (рис. 6).

Рис. 6.

Новый цикл обозначим через C_{k+1}. Число вершин полученного графа равно $|C_1| + (|C_2| - 1) + \dots + (|C_k| - 1) + (|C_{k+1}| - 1) \leq_{(A)} (l_1 + 1) + l_2 + \dots + l_k + 2 \leq (i-1) + 2 = i + 1$. Для слова w имеем $w = w_1 c^2 w_2$, подслова w_1, w_2 суть метки подпутей γ_1 и γ_2 в графе Γ и в полученном графе концы путей с метками $w_1 c^2$ и w_2^{-1} не совпадают (это вершины v_{k+1} и v_k). Значит, γ_w не будет замкнутым в построенном графе. Таким образом, найдена подгруппа индекса $i + 1$, не содержащая w.

Рассмотрим случай 1b. Для удобства считаем $s > 0$. Как и ранее, из условия (B) имеем $2l_1 + \dots + 2l_k + s \leq |w| = 2(i-1)$, откуда $l_1 + \dots + l_k + \left[\frac{s}{2}\right] \leq i - 1$. Применим к петле e_c операцию $\mathrm{II}_{h(s)}$, $h(s) = \left[\frac{s}{2}\right] + 1$. Новый цикл обозначим через C_{k+1}. Число вершин в полученном графе равно

$$|C_1| + (|C_2| - 1) + \dots + (|C_k| - 1) + (|C_{k+1}| - 1) \leq (l_1 + 1) + l_2 + \dots + l_k + \left[\frac{s}{2}\right] \leq i.$$

Как и ранее, из равенства $\gamma_w = \gamma_1 e_c^s \gamma_2$ имеем приведенную запись $w = w_1 c^s w_2$. Так как $h(s)$ не делит s, в новом графе пути с метками $w_1 c^s$ и w_2^{-1} с началом в x имеют несовпадающие концы v_{k+1}, v_k, следовательно, путь γ_w с началом в вершине x не будет замкнутым. Значит, найдется подгруппа индекса $\leq i$, не содержащая w.

Разберем теперь вторую группу случаев.

Случай 2a. Так как суммарное число вхождений $e_c, \bar{e}_c$ в γ_w не менее 2, получаем $2l_1 + \dots + 2l_k + 2 \leq |w| = 2(i-1)$. Применим к петле e_c операцию $\mathrm{II}_{h(1)}$, $h(1) = 2$. Конец подпути α_{k+1} пути γ_w (метка этого подпути равна $w_1 c^{\pm 1}$) является вершиной нового цикла C_{k+1}, отличной от v_k. Обозначим ее через v_{k+1} (рис. 7).

Число вершин построенного графа Γ равно $|C_1| + (|C_2| - 1) + \dots + (|C_k| - 1) + (|C_{k+1}| - 1) \leq (l_1 + 1) + l_2 + \dots + l_k + 1 \leq i$. Положим $\Gamma_{k+1} = \Gamma$.

Рис. 7.

Рассмотрим случай 2b. Так как в этом случае петля e_c входит в γ_w по меньшей мере три раза, имеем очевидное неравенство $2l_1 + \dots + 2l_k + 3 \leq 2(i-1)$. Поскольку левая часть неравенства — нечетное число, на самом деле верно даже более сильное неравенство $2l_1 + \dots + 2l_k + 4 \leq 2(i-1)$. Применим к петле e_c операцию $\mathrm{II}_{h(2)}, h(2) = 3$, как и в случае 1a. Новый цикл обозначим через C_{k+1}. Число вершин полученного графа $|C_1| + (|C_2| - 1) + \dots + (|C_{k+1}| - 1) \leq (l_1 + 1) + l_2 + \dots + l_k + 2 \leq i$. Обозначим этот граф через Γ_{k+1}.

Рассмотрим случай 2c. Применим к петле e_c операцию $\mathrm{II}_{h(s)}$, как и в случае 1b. Новый цикл обозначим через C_{k+1}. Число вершин полученного графа $\leq i$. Таким образом, и в этом случае мы можем построить граф Γ_{k+1}.

Доказательство завершено.

ЛИТЕРАТУРА

1. *Коуровская тетрадь*. Нерешенные вопросы теории групп / составители В. Д. Мазуров, Е. И. Хухро. 15-е изд. Новосибирск: Ин-т математики СО РАН, 2002.
2. *Khalid Bou-Rabee.* Quantifying residual finiteness. Technical Report arXiv:0807.0862v2 [math.GR], arxiv.org, 2008.
3. *Rivin I.* Geodesics with one self-intersection, and other stories. Technical Report arXiv:0901.2543v3 [math.GT], arxiv.org, 2009.
4. *Malestein J., Putman A.* On the self-intersections of curves deep in the lower central series of a surface group. arXiv, math.GT, Jan 2009. 12 pages, 2 figures.
5. *Богопольский О. В.* Введение в теорию групп. М.; Ижевск: Институт компьютерных исследований, 2002.
6. *Айерленд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987.

Статья поступила 21апреля 2009 г.

Бускин Николай Владиславович
Новосибирский гос. университет, механико-математический факультет,
ул. Пирогова, 2, Новосибирск 630090
buskin1983@mail.ru