**References**

[1] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Москва 1964.
[2] Б. М. Бредихин, *Дисперсионный метод и бинарные аддитивные проблемы определенного типа*, Uspehi Mat. Nauk 20 (1965), no. 2 (122), pp. 89–130.
[3] Б. М. Бредихин, Ю. В. Линник, *Асимптотика и эргодические свойства решений обобщенного уравнения Гарди-Литтлвуда*, Мат. сб. 71 (113) (1966), pp. 145–161.
[4] Б. В. Левин, А. С. Файнлейб, *Применение некоторых интегральных уравнений к вопросам теории чисел*, Uspehi Mat. Nauk 27 (1967), no. 3 (135), pp. 119–197.
[5] А. О. Гельфонд, Ю. В. Линник, *Элементарные методы в аналитической теории чисел*, Москва 1962.
[6] H. Iwaniec, *On the error term in the linear sieve*, Acta Arith. 19(1971), pp. 29–58.
[7] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Berlin–Heidelberg–New York 1971.
[8] Y. Motohashi, *On the distribution of prime numbers which are of the form* $x^2+y^2+1$, Acta Arith. 16 (1970), pp. 351–363.
[9] H.-E. Richert, *Selberg's sieve with weights*, Proc. Symposia Pure Math. 20 (1971), pp. 287–310.
[10] E. Schering, *Beweis des Dirichletschen Satzes*, Ges. Werke, Bd. II, 1909, pp. 357–365.
[11] G. L. Watson, *Integral quadratic forms*, Cambridge 1960.
[12] H. Weber, *Beweis des Satzes, dass usw.*, Math. Ann. 20 (1882), pp. 301–329.
[13] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplicative Funktionen*, Math. Ann. 143 (1961), pp. 75–102.

*Received on 24. 7. 1971* (193)

ACTA ARITHMETICA
XXI (1972)

# Количественная форма задачи Бореля

Л. П. Постникова (Москва)

Понятие нормального числа в $g$-ичной шкале, т.е. вещественного числа $\alpha$, для которого дробные доли $\{\alpha g^x\}$, $x = 1, 2, \ldots$, равномерно распределены на отрезке $[0, 1]$, было впервые введено Э. Борелем [2], стр. 197–199. Будем говорить, что некоторое число $\alpha$ *явно конструируется*, если указано разложение числа $\alpha$ в $g$-ичную дробь. Э. Борель [2], стр. 198–199, дал набросок явной конструкции нормальных чисел. Таким образом, задача о построении нормальных чисел восходит к Э. Борелю. Начиная с работ Мизеса [8] и Чемпернуона [13], было предложено множество конструкций нормальных чисел и более общих конструкций, библиографические сведения по этому вопросу можно найти в книге А. Г. Постникова [9].

Обозначим через $N_\gamma(P)$ количество дробных долей функции $\alpha g^x$, попадающих на полуинтервал $[0, \gamma)$, $0 < \gamma \leqslant 1$, когда $x$ пробегает значения $x = 1, 2, \ldots, P$. Свойство равномерного распределения означает, что при любом $\gamma$

$$N_\gamma(P) = \gamma P + o(P). \tag{1}$$

Естественно придать проблеме более определенный характер: под этим мы понимаем задачу о построении таких чисел $\alpha$, для которых понижение в остаточном члене формулы (1) имело бы как можно меньший порядок. Инициатором такой постановки вопроса явился Н. М. Коробов; в работе [5] Н. М. Коробов явно сконструировал числа $\alpha$, для которых при любом заданном $\gamma$ выполняется соотношение

$$N_\gamma(P) = \gamma P + O(P^{1/2}). \tag{2}$$

В работах А. Г. Постникова [10] и М. Ф. Куликовой [7] были построены числа $\alpha$, для которых в соотношении (2) остаточный член понижается на некоторую степень логарифма $P$, именно в работе [7] для любого целого $g \geqslant 2$ строится число $\alpha$ такое, что при любом $\varepsilon > 0$

$$N_\gamma(P) = \gamma P + O\left(\frac{P^{1/2}}{(\ln P)^{1/4-\varepsilon}}\right).$$

Это самый сильный результат общего характера в направлении количественной трактовки задачи Бореля.

В работе [6] Н. М. Коробов развил новый арифметический метод в этом вопросе, который использовал для того, чтобы при $g$ равном простому числу, $g = p$, построить число, для которого справедливо соотношение

$$N_\gamma(P) = \gamma P + O(P^{1/3}\ln^{4/3}P).$$

Результат Н. М. Коробова касается оснований частного вида; естественно стремится к тому, чтобы получить степенное понижение относительно стандарта (2) для произвольных оснований $g$. В моей работе [11] метод Н. М. Коробова был распространен на случай бесквадратных $g$. Наибольшая трудность в решении общей задачи состоит в построении для случая оснований равных степени простых чисел, причем таких построений, которые были бы способны к „мультипликативному синтезу". В настоящей работе мы преодолеваем эту трудность посредством построения нормальных периодических систем с помощью относительных полей Галуа. Это дает нам возможность для любого заданного $g \geqslant 2$ построить число $a$, для которого в асимптотической формуле (1) остаточный член имеет порядок $O(P^\omega)$, где $\omega < \frac{1}{2}$, т.е. дает решение задачи в общем случае.

Теорема. *Пусть каноническое разложение натурального числа $g \geqslant 2$ имеет вид*

$$g = g_1 \dots g_s,$$

*где $g_1 = p_1^{\varkappa_1}, \dots, g_s = p_s^{\varkappa_s}$ ($p_1, \dots, p_s$ — различные простые числа). Пусть $g_1$ минимальное из чисел $g_i$ ($i = 1, 2, \dots, s$). Определим число $\varkappa$ из равенства*

$$\varkappa = \begin{cases} 0, & \text{если} \quad s = 1, \\ \dfrac{\ln g_2 \dots g_s}{\ln g_1}, & \text{если} \quad s > 1. \end{cases}$$

*Явно конструируется число $a$ такое, что распрделение дробных долей $ag^x$, $x = 1, 2, \dots, P$ описывается асимптотической формулой*

$$N_\gamma(P) = \gamma P + O\left(P^{\frac{1}{2}-\frac{1}{8\varkappa+6}}(\ln P)^c\right),$$

*где* $c = \dfrac{4\varkappa+4}{4\varkappa+3}$.

Прежде чем приступить к построению понадобится вспомогательная работа.



Пусть $g_i$ какое-либо из чисел $g_1, \dots, g_s$; $g_i = p_i^{\varkappa_i}$. Через $[p_i]$ будем обозначать простое поле характеристики $p_i$; через $[g_i]$ поле, состоящее из $g_i = p_i^{\varkappa_i}$ элементов.

В $g$-ичном представлении вещественного числа $\alpha$, $0 \leqslant \alpha < 1$,

$$\alpha = \frac{A_1}{g} + \frac{A_2}{g^2} + \dots,$$

знаки $A_1, A_2, \dots$ суть целые числа с условием $0 \leqslant A_i \leqslant g-1$, $i = 1, 2, \dots$ Нам будет удобно установить взаимнооднозначное соответствие (кодирование) целых чисел $A$ отрезка $[0, g-1]$ с помощью $s$-компонентных векторов $(a^{(1)}, \dots, a^{(s)})$, где $a^{(i)} \in [g_i]$, $i = 1, 2, \dots, s$. Опишем это соответствие. Прежде всего, напомним следующий элементарный факт (см. например, [3], гл. III, стр. 49, задача 9а).

Лемма 1. *Пусть $g_i$ какое-либо из чисел $g_1, g_2, \dots, g_s$. Обозначим через $N_i = g/g_i$ ($i = 1, 2, \dots, s$). Если форме*

$$N_1A^{(1)} + N_2A^{(2)} + \dots + N_sA^{(s)}$$

*заставим числа $A^{(1)}, A^{(2)}, \dots, A^{(s)}$ пробегать полные системы вычетов соответственно по модулям $g_1, g_2, \dots, g_s$, то получим все элементы полной системы вычетов по модулю $g$ и каждый один раз.*

Первый шаг нашего соответствия заключается в том, что числу $A$, $0 \leqslant A \leqslant g-1$ сопоставляется $s$-компонентный вектор

$$A \leftrightarrow (A^{(1)}, \dots, A^{(s)}),$$

где $A^{(i)}$, $i = 1, 2, \dots, s$, числа с условием $0 \leqslant A^{(i)} \leqslant g_i - 1$.

Зафиксируем для каждого $i = 1, 2, \dots, s$ какой-либо порождающий элемент поля $[g_i]$ над полем $[p_i]\eta_i$

$$[g_i] = [p_i](\eta_i).$$

Любой элемент $a^{(i)} \in [g_i]$ может быть однозначно представлен в виде

$$a^{(i)} = u_0^{(i)} + u_1^{(i)}\eta_i + \dots + u_{\varkappa_i-1}^{(i)}\eta_i^{\varkappa_i-1},$$

где $u_j^{(i)} \in [p_i]$, $j = 0, 1, \dots, \varkappa_i - 1$. Пусть $U_0^{(i)}, U_1^{(i)}, \dots, U_{\varkappa_i-1}^{(i)}$ — целые числа $0 \leqslant U_j^{(i)} \leqslant p_i - 1$, $j = 0, 1, \dots, \varkappa_i - 1$, принадлежащие соответственно к классам вычетов $u_0^{(i)}, u_1^{(i)}, \dots, u_{\varkappa_i-1}^{(i)}$. Элементу $a^{(i)}$ сопоставим число $A^{(i)}$, $0 \leqslant A^{(i)} \leqslant p_i^{\varkappa_i} - 1$

$$A^{(i)} = U_0^{(i)} + U_1^{(i)}p_i + \dots + U_{\varkappa_i-1}^{(i)}p_i^{\varkappa_i-1}.$$

Обратно, дано целое число $A^{(i)}$, $0 \leqslant A^{(i)} \leqslant p_i^{\varkappa_i} - 1$. Представим его в $p_i$-ичной системе счисления

$$A^{(i)} = U_0^{(i)} + U_1^{(i)}p_i + \dots + U_{\varkappa_i-1}^{(i)}p_i$$

где $0 \leqslant U_j^{(i)} \leqslant p_i - 1$; $j = 0, 1, \ldots, \varkappa_i - 1$. Пусть $u_j^{(i)}$ класс вычетов по модулю $p_i$, которому принадлежит $U_j^{(i)}$ $(j = 0, 1, \ldots, \varkappa_i - 1)$. Сопоставим числу $0 \leqslant A^{(i)} \leqslant p_i^{\varkappa_i} - 1$ элемент $a^{(i)} \in [g_i]$

$$a^{(i)} = u_0^{(i)} + u_1^{(i)}\eta_i + \ldots + u_{\varkappa_i - 1}^{(i)}\eta_i^{\varkappa_i - 1}.$$

Теперь мы можем до конца описать соответствие между числами $A$, $0 \leqslant A \leqslant g - 1$ и векторами с компонентами из полей $[g_i], i = 1, 2, \ldots, s$. Пусть

$$A \leftrightarrow (A^{(1)}, \ldots, A^{(s)}),$$

где $0 \leqslant A^{(i)} \leqslant g_i - 1$. Пусть далее числу $A^{(i)}$ соответствует элемент $a^{(i)}$ поля $[g_i]$, $i = 1, 2, \ldots, s$. Нужное нам соответствие задается формулой

$$A \leftrightarrow (a^{(1)}, \ldots, a^{(s)}). \tag{4}$$

Соответствие (4) позволяет упорядочивать по величине векторы

$$(a^{(1)}, \ldots, a^{(s)}),$$

где

$$a^{(i)} \in [g_i], \quad i = 1, 2, \ldots, s.$$

Итак, когда записывается $g$-ичное разложение числа $\alpha$, $0 \leqslant \alpha < 1$,

$$\alpha = 0, A_1 A_2 \ldots$$

под символами $A_j, j = 1, 2, \ldots$, будем понимать векторы

$$(a_j^{(1)}, \ldots, a_j^{(s)}), \quad \text{где} \quad a_j^{(i)} \in [g_i], \quad i = 1, 2, \ldots, s,$$

соответствующие в указанном выше смысле $j$-ому $g$-ичному знаку числа $\alpha$.

Определим сложение векторов $A$ посредством правила сложения соотвествующих компонент. Вектора $A$ образуют по сложению группу.

Заданы два вектора

$$M = (m^{(1)}, \ldots, m^{(s)})$$

и

$$A = (a^{(1)}, \ldots, a^{(s)}).$$

Обозначим через $AM$ вектор

$$AM = (m^{(1)}a^{(1)}, \ldots, m^{(s)}a^{(s)}).$$

Пусть $a^{(i)} \in [g_i]$. Обозначим через

$$\mathrm{Sp}_{[g_i]/[p_i]} a^{(i)} = a^{(i)} + a^{(i)p_i} + \ldots + a^{(i)p_i^{\varkappa_i - 1}}.$$

Это выражение будем называть следом элемента $a^{(i)} \in [g_i]$ в $[p_i]$. Ясно, что

$$\mathrm{Sp}_{[g_i]/[p_i]} a^{(i)} \in [p_i].$$



Далее, ясно, что

$$\mathrm{Sp}_{[g_i]/[p_i]}(a^{(i)} + b^{(i)}) = \mathrm{Sp}_{[g_i]/[p_i]} a^{(i)} + \mathrm{Sp}_{[g_i]/[p_i]} b^{(i)}.$$

Для $a \in [g_i]$ обозначим

$$e_i(a^{(i)}) = \exp\left[2\pi i \frac{\mathrm{Sp}_{[g_i]/[p_i]} a^{(i)}}{p_i}\right].$$

Это выражение есть неглавный характер аддитивной группы поля $[g_i]$ и нетрудно доказать, что

$$\sum_{a^{(i)} \in [g_i]} e_i(a^{(i)}) = 0.$$

Далее, для векторов $A = (a^{(1)}, \ldots, a^{(s)})$, где $a^{(i)} \in [g_i]$ введем функцию

$$e(A) = e_1(a^{(1)}) \ldots e_s(a^{(s)}).$$

Очевидно, что

$$e(A + B) = e(A) \cdot e(B).$$

Лемма 2. *Для векторов $A = (a^{(1)}, \ldots, a^{(s)})$, где $a^{(i)} \in [g_i]$ введем символ*

$$\delta(A) = \begin{cases} 0, & A \neq (0, 0, \ldots, 0), \\ 1, & A = (0, 0, \ldots, 0). \end{cases}$$

*Справедлива формула*

$$\delta(A) = \frac{1}{g} \sum_M e(MA),$$

*где суммирование распространено на все векторы*

$$M = (m^{(1)}, \ldots, m^{(s)}), \quad m^{(i)} \in [g_i], \ i = 1, 2, \ldots, s.$$

Доказательство. В самом деле,

$$\frac{1}{g} \sum_M e(MA) = \prod_{i=1}^{s} \left( \frac{1}{g_i} \sum_{m^{(i)} \in [g_i]} e_i(m^{(i)}a^{(i)}) \right). \tag{5}$$

Если $a^{(i)} = 0$, то $\mathrm{Sp}_{[g_i]/[p_i]} m^{(i)} a^{(i)} = 0$ и мы имеем

$$\frac{1}{g_i} \sum_{m^{(i)} \in [g_i]} e_i(m^{(i)}a^{(i)}) = \frac{1}{g_i} \sum_{m^{(i)} \in [g_i]} 1 = 1.$$

Если $a^{(i)} \neq 0$, то

$$\frac{1}{g_i} \sum_{m^{(i)} \in [g_i]} e_i(m^{(i)}a^{(i)}) = \frac{1}{g_i} \sum_{b^{(i)} \in [g_i]} e_i(b^{(i)}) = 0.$$

Итак, если хотя бы одна из компонент вектора $A$ не равна нулю, то соответствующий множитель в правой части (5) обратится в нуль. Лемма доказана.

Мы будем считать известным понятие нормальной периодической системы $\varrho_k(g)$ (см. работу [4]). Условимся что под знаками $A$ нормальной периодической системы мы будем понимать векторы

$$A = (a^{(1)}, \ldots, a^{(s)}),$$

где $a^{(i)} \in [g_i]$, $i = 1, 2, \ldots, s$. Обозначим через $\varrho'_k(g)$ систему, которая получается из системы $\varrho_k(g)$ отбрасыванием последних $k-1$ знаков.

Риз [12] предложил способ построения нормальных периодических систем на основе теории конечного поля. Мы сейчас дадим модифицированное изложение способа Риза.

Через $[g_i^K]$, $i = 1, 2, \ldots, s$, будем обозначать поле из $g_i^K = p_i^{\varkappa_i K}$ элементов. Пусть $a^{(i)} \in [g_i^K]$. Обозначим

$$\mathrm{Sp}_{[g_i^K]/[g_i]} a^{(i)} = a^{(i)} + a^{(i)g_i} + \ldots + a^{(i)g_i^{K-1}}$$

и будем это выражение называть следом элемента $a^{(i)} \in [g_i^K]$ в $[g_i]$. Этот след есть элемент $[g_i]$. Ясно, что для $a^{(i)}, b^{(i)} \in [g_i^K]$

$$\mathrm{Sp}_{[g_i^K]/[g_i]}(a^{(i)} + b^{(i)}) = \mathrm{Sp}_{[g_i^K]/[g_i]} a^{(i)} + \mathrm{Sp}_{[g_i^K]/[g_i]} b^{(i)}.$$

Далее, следует иметь ввиду, что если $a^{(i)} \in [g_i^K]$ и $n^{(i)} \in [g_i]$, то

$$n^{(i)} \mathrm{Sp}_{[g_i^K]/[g_i]} a^{(i)} = \mathrm{Sp}_{[g_i^K]/[g_i]} n^{(i)} a^{(i)}.$$

Наконец, для элемента $a^{(i)} \in [g_i^K]$

$$\mathrm{Sp}_{[g_i]/[p_i]} \mathrm{Sp}_{[g_i^K]/[g_i]} a^{(i)} = \mathrm{Sp}_{[g_i^K]/[p_i]} a^{(i)} = a^{(i)} + a^{(i)p_i} + \ldots + a^{(i)p_i^{K\varkappa_i - 1}}$$

есть элемент поля $[p_i]$.

Лемма 3. *Пусть $\theta^{(i)}$ порождающий элемент мультипликативной группы поля $[g_i^K]$, $i = 1, 2, \ldots, s$, и $m^{(i)} \neq 0$ элемент поля $[g_i^K]$. Определим*

$$b_l^{(i)} = \mathrm{Sp}_{[g_i^K]/[g_i]} m^{(i)} \theta^{(i)l},$$

*$l = 1, 2, \ldots$ В последовательности*

$$(6) \qquad (b_1^{(i)}, \ldots, b_K^{(i)}), \quad (b_2^{(i)}, \ldots, b_{K+1}^{(i)}), \ldots, (b_{g_i^K-1}^{(i)}, \ldots, b_{g_i^K+K-2}^{(i)})$$

*содержатся все $K$-членные скобки, состоящие из элементов поля $[g_i]$, кроме скобки $(0, 0, \ldots, 0)$, а если дополнить последовательность*

$$b_1^{(i)}, b_2^{(i)}, \ldots, b_{g_i^K+K-2}^{(i)}$$



*нулем, поставив его перед комбинацией $(0, 0, \ldots, 0, 1)$, то получится нормальная периодическая система $\varrho_K(g_i)$.*

Доказательство. Всего различных скобок $(a_1^{(i)}, \ldots, a_K^{(i)})$ $g_i^K$. В последовательности (6) содержится $g_i^K - 1$ скобок. Докажем, что в ней не содержится скобка $(0, 0, \ldots, 0)$. Так как степени $\theta^{(i)}$ дают все элементы $[g_i^K]$, кроме нуля, то $\theta^{(i)}$ является порождающим элементом поля $[g_i^K]$ над $[g_i]$ и удовлетворяет уравнению $K$-ой степени с коэффициентами из $[g_i]$

$$\theta^{(i)K} = a_{K-1}^{(i)} \theta^{(i)K-1} + \ldots + a_0^{(i)}.$$

Отсюда

$$m^{(i)} \theta^{(i)n+k} = m^{(i)} a_{K-1}^{(i)} \theta^{(i)n+K-1} + \ldots + m^{(i)} a_0^{(i)} \theta^{(i)n}.$$

Этому же уравнению удовлетворяют все сопряженные относительно поля $[g_i]$ величины

$$m^{(i)} \theta^{(i)s} = (m^{(i)} \theta^{(i)s})_1, \ldots, (m^{(i)} \theta^{(i)s})_K.$$

Складывая получаем

$$\mathrm{Sp}_{[g_i^K]/[g_i]} m^{(i)} \theta^{(i)n+K} = a_{K-1}^{(i)} \mathrm{Sp}_{[g_i^K]/[g_i]} m^{(i)} \theta^{(i)n+K-1} + \ldots + a_0^{(i)} \mathrm{Sp}_{[g_i^K]/[g_i]} \theta^{(i)n} m^{(i)},$$

т.е.

$$b_{n+K}^{(i)} = a_{K-1}^{(i)} b_{n+K-1}^{(1)} + \ldots + a_0^{(i)} b_n^{(i)}.$$

Если в последовательности (6) была бы комбинация $(0, 0, \ldots, 0)$, то вся бы последовательность (6) состояла бы из нулей, что противоречило невырожденности следа $\mathrm{Sp}_{[g_i^K]/[x_i]} x$.

Теперь нам следует установить, что все элементы строки (6) различны. Предположим, что при $1 \leqslant n \leqslant g_i^K - 1$,

$$\mathrm{Sp}\, m^{(i)} \theta^{(i)n} = \mathrm{Sp}\, m^{(i)} \theta^{(i)},$$
$$\ldots\ldots\ldots\ldots,$$
$$\mathrm{Sp}\, m^{(i)} \theta^{(i)n+K-1} = \mathrm{Sp}\, m^{(i)} \theta^{(i)K},$$

(мы всюду опустили при символе Sp индекс $[g_i^K]/[g_i]$). Тогда

$$m_1^{(i)} (\theta_1^{(i)n} - \theta_1^{(i)}) + \ldots + m_K^{(i)} (\theta_K^{(i)n} - \theta_K^{(i)}) = 0,$$
$$m_1^{(i)} \theta_1^{(i)} (\theta_1^{(i)n} - \theta_1^{(i)}) + \ldots + m_K^{(i)} \theta_K^{(i)} (\theta_K^{(i)n} - \theta_K^{(i)}) = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$m_1^{(i)} \theta_1^{(i)K-1} (\theta_1^{(i)n} - \theta_1^{(i)}) + \ldots + m_K^{(i)} \theta_K^{(i)} (\theta_K^{(i)n} - \theta_K^{(i)}) = 0,$$

здесь $m_1^{(i)}, \ldots, m_K^{(i)}$ набор сопряженных (относительно поля $[g_i]$) величин к $m^{(i)}$, $\theta_1^{(i)}, \ldots, \theta_K^{(i)}$ набор сопряженных (относительно поля $[g_i]$) величин к $\theta^{(i)}$. Коль скоро $1 \leqslant n \leqslant g_i^K - 1$, то

$$\theta_1^{(i)n} - \theta_1^{(i)} \neq 0,$$

и значит, $m_1^{(i)}(\theta_1^{(i)n}-\theta_1^{(i)})\neq 0$, т.е. система уравнений

$$\theta_1^{(i)s}x_1+\ldots+\theta_K^{(i)s}x_K=0,\quad s=1,\ldots,K-1$$

имеет нетривиальное решение. Но тогда

$$\begin{vmatrix} 1 & \ldots & 1 \\ \theta_1^{(i)} & \ldots & \theta_K^{(i)} \\ \ldots & \ldots & \ldots \\ \theta_1^{(i)K-1} & \ldots & \theta_K^{(i)K-1} \end{vmatrix}=0,$$

что противоречит тому, что все сопряженные к $\theta^{(i)}$ различны. Лемма доказана.

Лемма 4. *Пусть $\theta^{(i)}$ порождающий элемент мультипликативной группы поля $[g_i^K]$ и $m^{(i)}\neq 0$ элемент поля $[g_i^K]$. Пусть $a_i$ целое число, $0\leqslant a_i\leqslant g_i^K-1$. Рассмотрим тригонометрическую сумму*

$$S_i=\sum_{x_i=1}^{g_i^K-1}\exp\left[2\pi i\frac{\mathrm{Sp}_{[g_i^K]/[p_i]}m^{(i)}\theta^{(i)x_i}}{p_i}\right]\exp\left[2\pi i\frac{a_ix_i}{g_i^K}\right].$$

*Имеет место оценка*

$$|S_i|\leqslant 7g_i^{K/2}. \tag{7}$$

Доказательство. Будем ради упрощения записи опускать всюду индекс $i$. Мы имеем, обозначая,

$$S'=\sum_{x=1}^{g^K-1}\exp\left[2\pi i\frac{\mathrm{Sp}_{[g^K]/[p]}m\theta^x}{p}\right]\exp\left[2\pi i\frac{ax}{g^K-1}\right],$$

что

$$|S-S'|\leqslant\sum_{x=1}^{g^K-1}|e^{2\pi i\frac{ax}{g^K-1}}-e^{2\pi i\frac{ax}{g^K}}|\leqslant$$

$$\leqslant 2\pi a\sum_{x=1}^{g^K-1}\left(\frac{1}{g^K-1}-\frac{1}{g^K}\right)\leqslant 2\pi(g^K-1)\frac{g^K-1}{(g^K-1)g^K}\leqslant 2\pi<7.$$

Поэтому достаточно доказать, что

$$|S'|\leqslant g^{K/2}. \tag{7'}$$

Доказательство. Если $g^K-1\mid a$, то

$$S'=-1$$

и оценка (7') очевидна. Пусть $g^K-1\nmid a$. Для элемента $y\in[g^K]$ обозначим

$$e^*(y)=\exp\left[2\pi i\frac{\mathrm{Sp}_{[g^K]/[p]}y}{p}\right],$$



$e^*(y)$ неглавный характер аддитивной группы поля $[g^K]$. Далее положим

$$\chi^*(y)=\begin{cases}0, & y=0,\\ e^{2\pi i\frac{a\,\mathrm{ind}\,y}{g^K-1}}, & y\neq 0,\end{cases}$$

где $\mathrm{ind}\,y$ определяется из равенства

$$y=\theta^{\mathrm{ind}\,y},$$

$\chi^*(y)$ характер мультипликативной группы поля $[g^K]$. Мы имеем

$$S'=e^{-2\pi i\frac{\mathrm{ind}\,m}{g^K-1}}\sum_{y\in[g^K]}e^*(y)\chi^*(y).$$

Но для суммы Гаусса мы имеем классическое равенство (см. [1], стр. 29)

$$\Big|\sum_{y\in[g^K]}e^*(y)\chi^*(y)\Big|=g^{K/2},$$

что нам дает

$$|S|=g^{K/2}.$$

Лемма доказана.

В работе Риза [12] устанавливается следующее утверждение

Лемма 5. *Пусть $g_1,\ldots,g_s$ степени различных простых чисел $p_1,\ldots,p_s$. Обозначим для $i=1,2,\ldots,s$*

$$N_i=\frac{g}{g_i}.$$

*Заданы $s$ конечных последовательностей (каждая из $g^K$ знаков), знаки которых берутся соответственно из полей $[g_1],\ldots,[g_s]$*

$$\begin{aligned} u_x^{(1)}&:\underbrace{\varrho_K'(g_1)\ldots\varrho_K'(g_1)}_{N_1^K\text{ раз}},\\ &\ldots\ldots\ldots\ldots\\ u_x^{(s)}&:\underbrace{\varrho_K'(g_s)\ldots\varrho_K'(g_s)}_{N_s^K\text{ раз}}. \end{aligned} \tag{8}$$

*Последовательность векторов*

$$A_x=(u_x^{(1)},\ldots,u_x^{(s)}),$$

$x=0,1,\ldots,g^K-1$ *образует систему* $\varrho_K'(g)$.

В дальнейшем мы будем использовать следующее очевидное свойство последовательностей (8): для $j=1,2,\ldots,s$

$$u_{x+g_i^K}^{(j)}=u_x^{(j)}.$$

Приступим к построению. Мы будем использовать векторный язык: однако, в случае, если $g$ есть степень простого числа, то участвующие в построении векторы однокомпоненты и мы фактически имеем дело с элементами поля $[g]$.

Пусть $\theta^{(i)}$ порождающий элемент мультипликативной группы поля $[g_i]$. Обозначим через $\bar{\varrho}'_K(g_i)$, систему полученную по способу леммы 3 с $m^{(i)}=1$, т.е. зададим знаки $\bar{\varrho}'_K(g_i)$ равенством

$$b_n^{(i)} = \mathrm{Sp}_{[g_i^K]/[g_i]}\theta^{(i)n}.$$

Если $g$ не есть степень простого числа, то построим систему $\varrho'_K(g)$, состоящую из векторов $A_x$, $x=0,1,\ldots,g^K-1$, из систем $\bar{\varrho}'_K(g_i)$, $i=1,2,\ldots,s$, по способу леммы 5.

Пусть $C_1$ и $C_2$ обозначают произвольные положительные постоянные, $C_2 \geqslant C_1+1$ и $\varphi(K)$ любая положительная функция, удовлетворяющая условиям

$$C_1 K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}} \leqslant \varphi(K) \leqslant C_2 K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}}. \tag{9}$$

Напомним, что если $g$ есть степень простого числа, то $\varkappa=0$.

Определим число $\alpha$ с помощью равенства

$$\alpha = 0,\ \underbrace{\bar{\varrho}'_1 \ldots \bar{\varrho}'_1}_{\varphi(1)} \ldots \underbrace{\bar{\varrho}'_K \ldots \bar{\varrho}'_K}_{\varphi(K)} \ldots \tag{10}$$

Напомним, что мы кодируем $g$-ичные знаки вещественных чисел в случае, если $g$ есть степень простого числа с помощью элементов поля $[g]$, а в случае если $g$ состоит из $s$ различных простых чисел с помощью $s$-компонентных векторов.

Именно для числа $\alpha$, определенного равенством (10) мы и будем доказывать выполнение соотношения (3). Обозначимя через $n_K$ количество знаков, предшествующих в разложении (10) первой из систем $\bar{\varrho}'_{K+1}$. Тогда, очевидно, $n_0=0$,

$$n_K = \sum_{\nu=1}^{K} \varphi(\nu) g^\nu.$$

Пусть число $\gamma$ задано своим $g$-ичным разложением

$$\gamma = 0, \Gamma_1 \Gamma_2 \ldots$$

и $N_\gamma(Q,P)$ есть количество выполнений неравенства

$$0 \leqslant \{\alpha g^x\} < \gamma$$

при $x = Q+1, \ldots, Q+P$ $(N_\gamma(0,P) = N_\gamma(P))$. Каждое натуральное число $P$ можно единственным образом представить в виде

$$P = n_{K-1} + rg^K + r', \tag{12}$$



где $0 \leqslant r < \varphi(K)$ и $0 \leqslant r' < g^K$. Следовательно, определив $K$ из условия

$$n_{K-1} \leqslant P < n_K$$

при любом $P$ получаем

$$N_\gamma(P) = \sum_{\nu=1}^{K-1} N_\gamma\left(n_{\nu-1}, \varphi(\nu)g^\nu\right) + N_\gamma(n_{K-1}, rg^K) + N_\gamma(n_{K-1}+rg^K, r'). \tag{13}$$

Покажем, что при произвольном $\nu \geqslant 1$ и любом $r_0$ из интервала $0 < r_0 \leqslant \varphi(\nu)$ выполняется неравенство

$$N_\gamma(n_{\nu-1}, r_0 g^\nu) = \gamma r_0 g^\nu + O\left(\nu^2 g^{\nu\frac{2\varkappa+1}{2\varkappa+2}}\right), \tag{14}$$

где константа в символе „$O$" не зависит от $\nu$. В самом деле, так как

$$\{\alpha g^x\} = 0, A_{x+1} \ldots A_{x+\nu} \ldots,$$

то при любом фиксированном $\nu \geqslant 1$ дробные доли $\{\alpha g^x\}$ лежат внутри интервала $[0,\gamma)$, если выполняется неравенство

$$0, A_{x+1} \ldots A_{x+\nu} < 0, \Gamma_1 \Gamma_2 \ldots \Gamma_\nu,$$

и не попадают в этот интервал, если

$$0, A_{x+1} \ldots A_{x+\nu} > 0, \Gamma_1 \ldots \Gamma_\nu.$$

Отнеся к остаточному члену случаи, когда

$$0, A_{x+1} \ldots A_{x+\nu} = 0, \Gamma_1 \ldots \Gamma_\nu,$$

по построению $\alpha$, т.е. по свойству систем $\varrho'_\nu(g)$ имеем

$$N_\gamma(n_{\nu-1}, r_0 g^\nu) = 0, \Gamma_1 \ldots \Gamma_\nu \cdot r_0 g^\nu + O(r_0).$$

Отсюда, так как

$$\gamma = 0, \Gamma_1 \ldots \Gamma_\nu + O\left(\frac{1}{g^\nu}\right)$$

следует, что

$$N_\gamma(n_{\nu-1}, r_0 g^\nu) = \gamma r_0 g^\nu + O(r_0).$$

Но согласно выбору функции $\varphi(\nu)$

$$r_0 \leqslant \varphi(\nu) = O\left(\nu^2 g^{\nu\frac{2\varkappa+1}{2\varkappa+2}}\right),$$

что и доказывает неравенство (14).

Покажем теперь, что

$$N_\gamma(n_{K-1}+rg^K, r') = \gamma r' + O\left(K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}}\right). \tag{15}$$

Определим вектора $A'_x$ равенством

$$A'_x = A_{n_{K-1}+rg^K+x}.$$

Тогда, согласно выбору $\alpha$ при $1 \leqslant x \leqslant r'$ набор векторов

$$A'_x, \ldots, A'_{x+K-1}$$

представляет $K$ последовательных знаков системы $\bar{e}'_K$. Условимся что выражение

$$\sum_{B_1,\ldots,B_K}$$

означает сумму, распространенную на систему векторов $B_1 \ldots B_K$, для которых выполняется условие

$$0, B_1 \ldots B_K < 0, \Gamma_1 \ldots \Gamma_K.$$

Вспоминая введенный в лемме 2 символ $\delta(A)$ и данное для него представление в виде тригонометрической суммы, имеем

$$(16)\quad N_\gamma(n_{K-1}+rg^K, r') = \sum_{B_1 \ldots B_K} \sum_{x=1}^{r'} \delta(A'_x - B_1) \ldots \delta(A'_{x+K-1} - B_K) + O(1) = 0, \Gamma_1 \ldots \Gamma_K \cdot r' + R + O(1),$$

где

$$(17)\quad R = 1/g^K \sum_{M_1,\ldots,M_K}{}' \sum_{B_1 \ldots B_K} e(-M_1B_1) \ldots e(-M_KB_K) \times \sum_{x=1}^{r'} e(M_1A'_x) \ldots e(M_KA'_{x+K-1}),$$

и в сумме $\sum'$ пропущего слагаемое с $M_1 = M_2 = \ldots = M_K = \bar{0}$. Заметим, что условие

$$0, B_1 \ldots B_K < 0, \Gamma_1 \ldots \Gamma_K$$

равносильно системе условий

$$\begin{aligned} &B_1 = \Gamma_1, \ \ldots, \ B_{\nu-1} = \Gamma_{\nu-1}, \ B_\nu < \Gamma_\nu \\ &B_{\nu+1} \leqslant g-1, \ \ldots, \ B_K \leqslant g-1 \end{aligned} \qquad \nu = 1, 2, \ldots, K,$$

поэтому

$$\begin{aligned} &\Big| \sum_{B_1 \ldots B_K} e(-M_1B_1) \ldots e(-M_KB_K) \Big| = \\ &= \Big| \sum_{\nu=1}^{K} \sum_{B_\nu=0}^{\Gamma_\nu - 1} e(-M_\nu B_\nu) \sum_{B_{\nu+1} \ldots B_K = 0}^{g-1} e(-M_{\nu+1}B_{\nu+1}) \ldots e(-M_KB_K) \Big| = \\ &= \Big| \sum_{\nu=1}^{K} g^{K-\nu} \sum_{B_\nu=0}^{\Gamma_\nu - 1} e(-M_\nu B_\nu)\, \delta(M_{\nu+1}) \ldots \delta(M_K) \Big| \leqslant \\ &\leqslant g^{K+1} \sum_{\nu=1}^{K} \frac{\delta(M_{\nu+1}) \ldots \delta(M_K)}{g^\nu}. \end{aligned}$$



Но тогда

$$|R| \leqslant g \sum_{M_1 \ldots M_K}{}' \sum_{\nu=1}^{K} \frac{\delta(M_{\nu+1}) \ldots \delta(M_K)}{g^\nu} \Big| \sum_{x=1}^{r'} e(M_1A'_x) \ldots e(M_KA'_{x+K-1}) \Big|.$$

Обозначим при фиксированной системе векторов $M_1, \ldots, M_K$, отличной от системы $M_1 = M_2 = \ldots = M_K = \bar{0}$,

$$L_x = M_1A'_x + \ldots + M_KA'_{x+K-1}.$$

Мы имеем

$$e(L_x) = e(M_1A'_x) \ldots e(M_KA'_{x+K-1}).$$

Наша цель состоит в оценке модуля суммы

$$\sum_{x=1}^{r'} e(L_x).$$

Для этой цели применим классическое преобразование

$$(18)\quad \sum_{x=1}^{r'} e(L_x) = \frac{1}{g^K} \sum_{a=0}^{g^K-1} \sum_{x=1}^{g^K} \sum_{y=1}^{r'} e(L_x) e^{2\pi i \frac{a(x-y)}{g^K}} = \frac{r'}{g^K} \sum_{x=1}^{g^K} e(L_x) + \frac{1}{g^K} \sum_{a=0}^{g^K-1} \Big( \sum_{x=1}^{g^K} e(L_x) e^{2\pi i \frac{ax}{g^K}} \Big) \Big( \sum_{y=1}^{r'} e^{-2\pi i \frac{ay}{g^K}} \Big).$$

Таким образом, нам надо рассмотреть сумму

$$S(a) = \sum_{x=1}^{g^K} e(L_x) e^{2\pi i \frac{ax}{g^K}}.$$

Если $M_j = (m_j^{(1)}, \ldots, m_j^{(s)})$, $j = 1, 2, \ldots, K$ и $L_x = (l_x^{(1)}, \ldots, l_x^{(s)})$, то

$$l_x^{(i)} = m_1^{(i)} u_x^{(i)} + m_2^{(i)} u_{x+1}^{(i)} + \ldots + m_K^{(i)} u_{x+K-1}^{(i)},$$

$i = 1, 2, \ldots, s$. Мы имеем

$$S(a) = \sum_{x=0}^{g^{K-1}} e_1(l_x^{(1)}) \ldots e_s(l_x^{(s)}) e^{2\pi i \frac{ax}{g^K}}.$$

Вспомним лемму 1 и представим число $x$ в виде

$$x = \Big(\frac{g}{g_1}\Big)^K x_1 + \ldots + \Big(\frac{g}{g_s}\Big)^K x_s,$$

где $x_1, \ldots, x_s$ пробегают системы вычетов соответственно по модулям $g_1^K, \ldots, g_s^K$. Заметим, что при этом

$$x \equiv x_i (\mathrm{mod}\, g_i^K), \quad i = 1, 2, \ldots, s.$$

Учитывая также замечание к лемме 5, по которому при

$$x' \equiv x'' \pmod{g_i^K}, \quad i = 1, 2, \ldots, s,$$
$$l_{x'}^{(i)} = l_{x''}^{(i)},$$

мы получаем, что

$$S(a) = \prod_{i=1}^{s} \Big( \sum_{x_i=0}^{g_i^K-1} e_i(l_{x_i}^{(i)}) \Big) e^{2\pi i \frac{ax_i}{g_i^K}}.$$

Но по лемме 2 сумма

$$\sum_{x_i=0}^{g_i^K-1} e_i(l_{x_i}^{(i)}) e^{2\pi i \frac{ax_i}{g_i^K}}$$

самое большое одним членом отличается от суммы

$$S_i' = \sum_{x_i=0}^{g_i^K-1} e^{2\pi i \frac{ax_i}{g_i^K}} \exp\left[ 2\pi i \frac{\mathrm{Sp}_{[g_i^K]/[p_i]}(m_1^{(i)} \theta^{(i)^{x_i}} + \ldots + m_K^{(i)} \theta^{(i)^{x_i+K-1}})}{p_i} \right] =$$
$$= \sum_{x_i=0}^{g_i^K-1} e^{2\pi i \frac{ax_i}{g_i^K}} \exp\left[ 2\pi i \frac{\mathrm{Sp}_{[g_i^K]/[p_i]} f^{(i)} \theta^{(i)^{x_i}}}{p_i} \right],$$

где

$$f^{(i)} = m_1^{(i)} + \ldots + m_K^{(i)} \theta^{(i)^{K-1}}.$$

Но по формуле (7) имеем

$$|S_i'| \leqslant \begin{cases} 7 g_i^{K/2}, & \text{не все } m_1^{(i)}, \ldots, m_K^{(i)} \text{ есть нули;} \\ 0, & m_1^{(i)} = m_2^{(i)} = \ldots = m_K^{(i)} = 0;\ a \not\equiv 0 \pmod{g_i^K}; \\ g_i^K, & \text{все } m_1^{(i)}, \ldots, m_K^{(i)} \text{ есть нули } a \equiv 0 \pmod{g_i^K}. \end{cases}$$

Но система сравнений

$$a \equiv 0 \pmod{g_1^K}, \ldots, a \equiv 0 \pmod{g_s^K}$$

эквивалентна одному сравнению

$$a \equiv 0 \pmod{g^K}.$$

Поэтому

$$|S(a)| \leqslant \begin{cases} 8 g_1^{K/2} (g_2 \ldots g_s)^K, & a \equiv 0 \pmod{g^K}, \\ 8^s g^{K/2}, & a \not\equiv 0 \pmod{g^K}. \end{cases}$$

Отсюда и из (18) получаем

$$\sum_{x=1}^{r'} e(L_x) = O(g_1^{K/2} g_2^K \ldots g_s^K).$$



Если $g = g_1$ есть степень простого числа, то

$$\sum_{x=1}^{r'} e(L_x) = O(g_1^{K/2} \ln g_1),$$

и в этом случае, т.е. в случае $\varkappa = 0$, вычисления доводятся до конца, так как в работе Н. М. Коробова [6].

Пусть $\varkappa > 0$. Тогда $g_1 \ldots g_s = g_1^{1+\varkappa}$, $g_1 = g^{1/(1+\varkappa)}$, т.е.

$$g_1^{K/2} (g_2 \ldots g_s)^K = g_1^{(\varkappa+\frac{1}{2})K} = g^{\frac{(\varkappa+\frac{1}{2})K}{1+\varkappa}} = g^{\frac{2\varkappa+1}{2\varkappa+2}K}.$$

Значит,

$$|R| \leqslant \sum_{\nu=1}^{K} \frac{1}{g^{\nu-1}} \sum_{M_1, \ldots, M_\nu=0}^{g-1}{}' g^{\frac{2\varkappa+1}{2\varkappa+2}K} \ll K g^{\frac{2\varkappa+1}{2\varkappa+2}K} \leqslant K^2 g^{\frac{2\varkappa+1}{2\varkappa+2}K}.$$

Отсюда

$$N_\gamma(n_{K-1} + r g^K, r') = 0, \Gamma_1 \ldots \Gamma_K \cdot r' + O(K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}}).$$

Замечаем, что $r' \leqslant g^K$ и

$$0, \Gamma_1 \ldots \Gamma_K = \gamma + O\left(\frac{1}{g^K}\right),$$

получаем, что

$$N_\gamma(n_{K-1} + r g^K, r') = \gamma r' + O(K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}}).$$

Теперь

$$N_\gamma(P) = \gamma \Big( \sum_{\nu=1}^{K-1} \varphi(\nu) g^\nu + r g^K + r' \Big) + O(R_1),$$

где

$$R_1 = \sum_{\nu=1}^{K-1} \nu^2 g^{\nu \frac{2\varkappa+1}{2\varkappa+2}} + K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}} = O(K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}}).$$

Но

$$\sum_{\nu=1}^{K-1} \varphi(\nu) g^\nu + r g^K + r' = n_{K-1} + r g^K + r' = P$$

и, следовательно,

$$N_\gamma(P) = \gamma P + O(K^2 g^{K\frac{2\varkappa+1}{2\varkappa+2}}).$$

Отсюда, так как

$$C_1 (K-1)^2 g^{\left(1+\frac{2\varkappa+1}{2\varkappa+2}\right)(K-1)} \leqslant \varphi(K-1) g^{K-1} \leqslant n_{K-1} \leqslant P,$$

получаем $K = O(\ln P)$ и

$$K^2 P^{\frac{2\varkappa+1}{4\varkappa+3}} \gg K^{\frac{4\varkappa+2}{4\varkappa+3}} K^2 g^{\frac{2\varkappa+1}{2\varkappa+2}K}, \qquad K^2 g^{\frac{2\varkappa+1}{2\varkappa+2}K} \ll K^{\frac{4\varkappa+4}{4\varkappa+3}} P^{\frac{2\varkappa+1}{4\varkappa+3}},$$

т.е.

$$N_\gamma(P) = \gamma P + O\left(P^{\frac{2\varkappa+1}{4\varkappa+3}} (\ln P)^{\frac{4\varkappa+4}{4\varkappa+3}}\right) = \gamma P + O\left(P^{\frac{1}{2}-\frac{1}{8\varkappa+6}} (\ln P)^{i}\right),$$

что и требуется доказать.

### Литература


[1] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Москва 1964.

[2] E. Borel, *Leçons sur la théorie des fonctions*, Paris 1914.

[3] И. М. Виноградов, *Основы теории чисел*, Москва 1965.

[4] Н. М. Коробов, *О некоторых вопросах равномерного распределения*, Изв. АН СССР, серия матем. 14 (1950), стр. 215–238.

[5] — *Числа с ограниченным отношением и их приложения к вопросу диофантовых приближений*, Изв. АН СССР, серия матем. 19 (1955), стр. 361–380.

[6] — *О распределении дробных долей показательной функции*, Вестник МГУ, серия матем. мех. 4 (1966), стр. 42–46.

[7] М. Ф. Куликова, *Построение числа a, для которого дробные доли $\{ag^x\}$ быстро равномерно распределяются*, ДАН СССР, 143, №4 (1962), стр. 782–784.

[8] R. von Mises, *Zahlenfolgen mit kollektiv-ähnlichen Verhalten*, Math. Annalen 108(1933), стр. 757–772.

[9] А. Г. Постников, *Арифметическое моделирование случайных процессов*, Труды Матем. Ин-та АН СССР, вып. 57 (1960).

[10] — *О количестве попаданий дробных долей показательной функции на данный интервал*, Успехи Матем. Наук, 16, вып. 3, (99), стр. 201–205.

[11] Л. П. Постникова, *Конструктивная задача о дробных долях показательной функции*, Сборник Исследования по теории чисел, вып. 4, Саратов 1972.

[12] D. Rees, *Note on the paper by I. J. Good*, J. London Math. Soc. 21 (3) (1946), стр. 169–173.

[13] D. C. Champernowne, *The construction of the scale of ten*, J. London Math. Soc. 8 (1933), стр. 254–260.


*Получено 31. 7. 1971* (182)

ACTA ARITHMETICA
XXI (1972)

# On some problems of W. Sierpiński

by

A. Rotkiewicz (Warszawa)

*Dedicated to the memory of my teacher Professor Wacław Sierpiński*

A composite natural number $n$ is said to be a *pseudoprime* if $n \mid 2^n - 2$.

The most important theorems on pseudoprimes which answer to questions raised by Sierpiński are:

1. Every arithmetical progression $ax+b$ $(x = 1, 2, \ldots)$, where $(a, b) = 1$ contains an infinite number of pseudoprimes (Rotkiewicz [4] and [5]).
2. Let $a, b$ be fixed coprime positive integers. If $D > 0$ is given and $x > x_0(a, D)$, there exists at least one pseudoprime $P$ satisfying: $P \equiv b \pmod a$, $x < P < x\exp\left\{\frac{\log x}{(\log\log x)^D}\right\}$ (Halberstam and Rotkiewicz [1]).
3. There exist infinitely many squarefree pseudoprimes divisible by an arbitrary given prime $p$ (Rotkiewicz [3]).
4. There exist infinitely many arithmetic progressions formed of four pseudoprimes (Rotkiewicz [10]).
5. There exist infinitely many pseudoprimes which are at the same time triangular (Rotkiewicz [6] and [9]).
6. There exist infinitely many pseudoprimes which are at the same time pentagonal (Rotkiewicz [8] and [9]).

In 1965 (during a seminar which the author attended) W. Sierpiński raised the question whether there exist pseudoprimes which are at the same time tetrahedral. (A tetrahedral number is one of the form $\frac{n(n+1)(n+2)}{6}$). The answer to this question is in the affirmative.

Here we shall prove the following

Theorem 1. *If the numbers $8n+1$, $12n+1$ and $24n+1$ are primes and the numbers $12n+1$ and $24n+1$ are of the form $x^2+27y^2$, then the tetrahedral number $T_{24n+1}$ is a pseudoprime number.*