УДК 511

# О показательных сравнениях

**А. Шинцель**

Эта статья касается рассмотренных в последнее время задач о показательных сравнениях, первая из них изучалась С. Корралез Родриганез и Р. Схофом, вторая — С. П. Тунгом.

Библиография: 4 названия.

Корралез Родриганез и Схоф [1] доказали следующее утверждение.

*Пусть* $\mathbb{K}$ *— алгебраическое числовое поле и* $\alpha, \beta \in \mathbb{K}^*$. *Если для почти всех простых идеалов* $\wp$ *из* $\mathbb{K}$ *и для всех натуральных* $n$ *из* $\alpha^n \equiv 1 \pmod{\wp}$ *следует* $\beta^n \equiv 1 \pmod{\wp}$, *то* $\beta = \alpha^e$, $e \in \mathbb{Z}$ ("почти все" здесь и в дальнейшем понимаются как все за исключением множества с нулевой плотностью Дирихле).

Это утверждение будет обобщено следующим образом.

Теорема 1. *Пусть* $\mathbb{K}$ *— алгебраическое числовое поле,* $\alpha_1, \dots, \alpha_k$; $\beta_1, \dots, \beta_k \in \mathbb{K}^*$. *Если для почти всех простых идеалов* $\wp$ *из* $\mathbb{K}$ *и всех целых* $n_1, \dots, n_k$

$$\text{из} \quad \prod_{i=1}^{k} \alpha_i^{n_i} \equiv 1 \pmod{\wp} \quad \text{следует} \quad \prod_{i=1}^{k} \beta_i^{n_i} \equiv 1 \pmod{\wp}, \tag{1}$$

*то*

$$\alpha_i = \beta_i^e \quad (1 \leqslant i \leqslant k), \quad e \in \mathbb{Z}.$$

Если $\varphi \in \mathbb{Q}(t) \setminus \mathbb{Q}[t]$, то существует арифметическая прогрессия $P$ такая, что $\varphi(n) \notin \mathbb{Z}$ для $n \in P$ (см. [3, лемма к теореме 36, p. 195]). В переписке с автором С. П. Тунг поставил вопрос, выполняется ли подобное утверждение для

$$\frac{f(t)2^{F(t)} + g(t)}{h(t)},$$

и этот вопрос был распространен Ж.-Л. Николя на выражения типа

$$\frac{f(t)a^{F(t)} + g(t)b^{G(t)}}{h(t)}.$$

Ответ дает следующая

Теорема 2. *Пусть* $f, g, h, F, G \in \mathbb{Z}[t]$, $(f, g, h) = 1$, $h \notin \mathbb{Z}$, $a, b \in \mathbb{N}$, *причем* $a^{F(n)} b^{-G(n)}$ *не является постоянной для* $n \in \mathbb{Z}$. *Тогда существует арифметическая прогрессия* $P$ *такая, что для всех* $n \in P$

$$\frac{f(n)a^{F(n)} - g(n)b^{G(n)}}{h(n)} \notin \mathbb{Z}. \tag{2}$$

Теорема 1 является непосредственным следствием следующих двух лемм.

Лемма 1. *Пусть* $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^k$, $n \in \mathbb{N}$. *Если для всех* $\mathbf{x} \in \mathbb{Z}^k$ *из* $\mathbf{ax} \equiv 0 \pmod n$ *следует* $\mathbf{bx} \equiv 0 \pmod n$, *то* $\mathbf{b} \equiv \mathbf{a}e \pmod n$, $e \in \mathbb{Z}$.

Доказательство. Это частный случай леммы 2 из [2].

Лемма 2. *Пусть* $[\mathbb{K} : \mathbb{Q}] < \infty$, $\alpha_1, \ldots, \alpha_k; \beta_1, \ldots, \beta_k \in \mathbb{K}^*$. *Если система сравнений*

$$\alpha_i^x \equiv \beta_i \pmod \wp \quad (1 \leqslant i \leqslant k)$$

*разрешима для почти всех простых идеалов* $\wp$ *из* $\mathbb{K}$, *то соответствующая система уравнений разрешима в целых рациональных числах.*

Доказательство. Это следствие 1 из [4].

Доказательство теоремы 1. Пусть $g$ — первообразный корень по простому идеалу $\wp$ и $\operatorname{ind}_g \alpha$ — индекс $\alpha$ относительно $g$, определенный по $\bmod\ \varphi(\wp)$, где $\varphi$ — функция Эйлера. Если $\operatorname{ord}_\wp \alpha_i = \operatorname{ord}_\wp \beta_i = 0$ $(1 \leqslant i \leqslant k)$, то из (1) следует, что

$$\text{если} \quad \sum_{i=1}^{k} n_i \operatorname{ind}_g \alpha_i \equiv 0 \pmod{\varphi(\wp)},$$
$$\text{то} \quad \sum_{i=1}^{k} n_i \operatorname{ind}_g \beta_i \equiv 0 \pmod{\varphi(\wp)},$$

поэтому по лемме 1

$$\operatorname{ind}_g \beta_i \equiv e_\wp \operatorname{ind}_g \alpha_i \pmod{\varphi(\wp)},$$

где $e_\wp \in \mathbb{Z}$. Таким образом,

$$\beta_i \equiv \alpha_i^{e_\wp} \pmod \wp \quad (1 \leqslant i \leqslant k)$$

и

$$\beta_i = \alpha_i^e \quad (1 \leqslant i \leqslant k), \quad e \in \mathbb{Z},$$

по лемме 2.

Для доказательства теоремы 2 нам потребуются еще три леммы.

Лемма 3. *Пусть $q$ — простое число, $[\mathbb{K}:\mathbb{Q}]<\infty$, $A,B\in\mathbb{K}^*$. Если для почти всех простых идеалов $\wp$ из $\mathbb{K}$ из разрешимости сравнения $x^q\equiv A\pmod{\wp}$ следует разрешимость в $\mathbb{K}$ сравнения $x^q\equiv B\pmod{\wp}$, то*

$$B=A^r\Gamma^q,\quad \text{где}\quad r\in\mathbb{Z},\quad \Gamma\in\mathbb{K}^*. \tag{3}$$

Доказательство. Это частный случай теоремы 1 из [2].

Лемма 4. *Если $h,F,G\in\mathbb{Z}[t]$, $h$ неприводим над $\mathbb{Q}$; $a,b,C\in\mathbb{N}$ и $a^{F(n)}\neq b^{G(n)}$ для некоторого $n\in\mathbb{Z}$, то существует арифметическая прогрессия $P$ такая, что для любого $n\in P$*

$$C\frac{a^{F(n)}-b^{G(n)}}{h(n)}\notin\mathbb{Z}. \tag{4}$$

Доказательство. Рассмотрим сначала случай, когда $a$ и $b$ мультипликативно зависимы. Тогда существуют $c\in\mathbb{N}$ и $\alpha,\beta\in\mathbb{N}\cup\{0\}$ такие, что $c$ не является точной степенью числа из $\mathbb{N}$ и

$$a=c^\alpha,\quad b=c^\beta. \tag{5}$$

Пусть

$$h(v)=0,\quad \mathbb{K}=\mathbb{Q}(v),\quad d=[\mathbb{K}:\mathbb{Q}]. \tag{6}$$

Поскольку $a^{F(n)}\neq b^{G(n)}$ для некоторого $n\in\mathbb{Z}$, то $\alpha F-\beta G\neq 0$. Поэтому существуют целое число $n_1$ и простое $q_1>d$ такие, что

$$\alpha F(n_1)-\beta G(n_1)\not\equiv 0\pmod{q_1}. \tag{7}$$

Положим в лемме 3 $q=q_1$, $A=1$, $B=c$. Равенство (3) не может выполняться, поскольку число $\Gamma$ в (3) должно иметь степень $q_1$ и поэтому в силу (6) $d\geqslant q_1$, что противоречит выбору $q_1$. Следовательно, по лемме 3 существует простой идеал $\wp_1$ первой степени из $\mathbb{K}$, который не делит ни $cCq_1$, ни знаменатель числа $v$ и для которого сравнение $x^{q_1}\equiv c\pmod{\wp_1}$ неразрешимо в $\mathbb{K}$. Мы имеем: $v\equiv m_1\pmod{\wp_1}$, $m_1\in\mathbb{Z}$. Рассмотрим арифметическую прогрессию

$$P_1=\{n\in\mathbb{Z},\ \ n\equiv n_1\pmod{q_1},\ \ n\equiv m_1\pmod{p_1}\},$$

где $p_1$ — простое число, делящееся на $\wp_1$. Если $n\in P_1$ и не выполняется (4), то мы имеем:

$$h(n)\equiv h(v)\equiv 0\pmod{\wp_1},$$

поэтому в силу (5)

$$c^{\alpha F(n)-\beta G(n)} \equiv 1 \pmod{\wp_1},$$

и, ввиду (7),

$$\alpha F(n) - \beta G(n) \not\equiv 0 \pmod{q_1}.$$

Следовательно, для некоторых целых $\xi, \eta$

$$1 = q_1\xi - \bigl(\alpha F(n) - \beta G(n)\bigr)\eta$$

и $c \equiv (c^{\xi})^{q_1}$, что противоречит выбору $\wp_1$.

Рассмотрим теперь случай, когда $a$ и $b$ мультипликативно независимы. Пусть

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{k} p_i^{\beta_i},$$

где $p_i$ — различные простые числа и $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$ $(1 \leqslant i \leqslant k)$. Вектора $[\alpha_1, \ldots, \alpha_k], [\beta_1, \ldots, \beta_k]$ линейно независимы, поэтому, перенумеровывая их компоненты, если это необходимо, мы можем полагать, что

$$D = \alpha_1\beta_2 - \alpha_2\beta_1 \neq 0.$$

Поскольку $a^{F(n)} \neq b^{G(n)}$ для некоторого $n \in \mathbb{Z}$, то без ограничения общности мы можем полагать, что $G \neq 0$. Поэтому существуют целое число $n_2$ и простое $q_2 > d$ такие, что

$$G(n_2) \not\equiv 0 \pmod{q_2}, \quad q_2 \nmid D. \tag{8}$$

Возьмем в лемме 3 $q = q_2$, $A = a$, $B = b$. Равенство (3) не может выполняться с $\Gamma \in \mathbb{Q}$, так как из этого следовало бы, что $q_2 \mid D$, поэтому число $\Gamma$, удовлетворяющее (3), должно иметь степень $q_2$, а тогда, ввиду (6), $d \geqslant q_2$ вопреки выбору $q_2$. Следовательно, по лемме 3 существует простой идеал $\wp_2$ первой степени в $\mathbb{K}$, не делящий ни $Cabq_2$, ни знаменатель числа $v$ такой, что сравнение $x^{q_2} \equiv a \pmod{\wp_2}$ разрешимо в $\mathbb{K}$, но $x^{q_2} \equiv b \pmod{\wp_2}$ неразрешимо. Пусть $v \equiv m_2 \pmod{\wp_2}$, $m_2 \in \mathbb{Z}$. Рассмотрим арифметическую прогрессию

$$P_2 = \{n \in \mathbb{Z}, \quad n \equiv n_2 \pmod{q_2}, \quad n \equiv m_2 \pmod{p_2}\},$$

где $p_2$ — простое число, делящееся на $\wp_2$. Если $n \in P_2$ и не выполняется (4), то

$$h(n) \equiv h(v) \equiv 0 \pmod{\wp_2},$$

поэтому
$$a^{F(n)} \equiv b^{G(n)} \pmod{\wp_2},$$
и в силу (8) $G(n) \not\equiv 0 \pmod{q_2}$. Следовательно, для некоторых целых $\xi$ и $\eta$
$$1 = q_2\xi - G(n)\eta.$$
А поскольку $a \equiv a_2^{q_2} \pmod{\wp_2}$, $a_2 \in \mathbb{K}$, то
$$b = b^{q_2\xi - G(n)\eta} \equiv \left(b^{\xi} a_2^{-F(n)}\right)^{q_2} \pmod{\wp_2},$$
что противоречит выбору $\wp_2$.

Лемма 5. *Пусть* $[\mathbb{K} : \mathbb{Q}] < \infty$, $\alpha_1, \alpha_2, \beta \in \mathbb{K}^*$. *Тогда, если сравнение* $\alpha_1^{x_1}\alpha_2^{x_2} \equiv \beta \pmod{\wp}$ *разрешимо для почти всех простых идеалов* $\wp$ *из* $\mathbb{K}$, *то соответствующее уравнение разрешимо в целых рациональных числах.*

Доказательство. Это частный случай теоремы 2 из [2].

Доказательство теоремы 2. Достаточно рассмотреть случай, когда $h$ неприводим над $\mathbb{Q}$ и примитивен. Случай $h \mid fg$ тривиален, поэтому полагаем, что $h \nmid fg$. Снова определим $v$, $\mathbb{K}$ и $d$ посредством (6). Рассмотрим два случая.

Случай 1.
$$\frac{g(v)}{f(v)} = a^k b^{-l}, \quad k, l \in \mathbb{Z}.$$

Случай 2.
$$\frac{g(v)}{f(v)} \neq a^k b^{-l}, \quad k, l \in \mathbb{Z}.$$

1. В этом случае $h(t) \mid f(t)a^k - g(t)b^l$, и, поскольку многочлен $h$ примитивный, то для всех $n \in \mathbb{Z}$
$$h(n) \mid a^{-\min\{0,k\}} b^{-\min\{0,l\}} \big(f(n)a^k - g(n)b^l\big).$$
Если (2) не выполняется, то
$$h(n) \mid \big(f(n), h(n)\big) a^{-\min\{0,k\}} b^{-\min\{0,l\}} \big(a^{F(n)}b^l - a^k b^{G(n)}\big).$$

Далее $\big(f(n), h(n)\big) \mid R$, где $R$ — результант $f$ и $g$ и, так как $h \nmid f$, то $R \neq 0$. Утверждение теоремы следует из леммы 4, если взять в ней
$$C = a^{k-\min\{0,k\}} b^{l-\min\{0,l\}} |R|$$
и заменить $F$ на $F - k$, а $G$ на $G - l$.

2. В этом случае по лемме 5 существует в $\mathbb{K}$ простой идеал $\wp_0$ первой степени, не делящий знаменатель $v$, такой, что для всех $x, y \in \mathbb{Z}$ выполнено $f(v)a^x - g(v)b^y \not\equiv 0 \pmod{\wp_0}$.

Пусть $v \equiv m_0 \pmod{\wp_0}$ и

$$P_0 = \{n \in \mathbb{Z} : \quad n \equiv m_0 \pmod{p_0}\},$$

где $p_0$ — простое число, делящееся на $\wp_0$. Если $n \in P_0$ и не выполняется (2), то мы имеем:

$$h(n) \equiv h(m_0) \equiv h(v) \equiv 0 \pmod{\wp_0},$$

поэтому

$$f(v)a^{F(n)} - g(v)b^{G(n)} \equiv f(n)a^{F(n)} - g(n)b^{G(n)} \equiv 0 \pmod{\wp_0},$$

что противоречит выбору $\wp_0$.

Замечание. При помощи несколько более сложных рассуждений мы можем доказать следующее обобщение теоремы 2.

*Пусть* $[\mathbb{K} : \mathbb{Q}] < \infty$, $f, g, h \in \mathbb{K}[t]$, $(f, g, h) = 1$, $h \notin \mathbb{K}$, $F, G \in \mathbb{Q}[t]$ — *целозначные многочлены*, $\alpha, \beta \in \mathbb{K}^*$, $\alpha^{F(n)}\beta^{-G(n)}$ *не постоянно при* $n \in \mathbb{Z}$. *Тогда существует арифметическая прогрессия* $P$ *такая, что для любых* $n \in P$

$$\frac{f(n)\alpha^{F(n)} - g(n)\beta^{G(n)}}{h(n)}$$

*не являются целыми в* $\mathbb{K}$.

Instytut Matematyczny
Polskiej Akademii Nauk

Поступило
01.09.94

## Список литературы

[1] *Corralez Rodrigáñez C., Schoof R.* The support problem and its elliptic analogue // J. Number Th. (to appear).
[2] *Schinzel A.* On power residues and exponential congruences // Acta Arith. 1975. V. XXVII. P. 397–420.
[3] *Schinzel A.* Selected topics on polynomials: Ann Arbor, 1982.
[4] *Schinzel A.* Systems of exponential congruences // Demonstratio Math. 1985. V. 18. P. 377–394.