ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

2006 МАТЕМАТИКА № 9 (532)

УДК 511.328

*И.А. АЛЛАКОВ*

# ОБ УСЛОВИЯХ РАЗРЕШИМОСТИ СИСТЕМЫ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ В ПРОСТЫХ ЧИСЛАХ

Рассмотрим систему линейных уравнений

$$b_i = a_{i1}p_1 + a_{i2}p_2 + \cdots + a_{im}p_m, \quad i = 1, 2, \ldots, s, \tag{1}$$

где $b_1, b_2, \ldots, b_s$ — натуральные числа, $a_{i1}, a_{i2}, \ldots, a_{im}$ — целые коэффициенты, а $p_1, p_2, \ldots, p_m$ — неизвестные простые числа. В [1] при $m \geq 2s+1$, где изучалась разрешимость этой системы при некоторых дополнительных условиях, получена асимптотическая формула для числа решений системы (1). А при $s < m \leq 2s$ до сих пор не только не получена асимптотическая формула, но даже не установлено существование решений для произвольного набора натуральных чисел $b_1, b_2, \ldots, b_s$.

В [2] для системы (1) при $s = 2$, $m = 3$ оценивалось количество пар $(b_1, b_2)$, $1 \leq b_1, b_2 \leq X$, для которых система (1) неразрешима в простых числах, т. е. количество элементов в множестве $E_2(X) = \{(b_1, b_2) \mid 1 \leq b_1, b_2 \leq X,\ b_i = a_{i1}p_1 + a_{i2}p_2 + a_{i3}p_3,\ i = 1, 2\}$. При этом для достаточно больших $X$ получена степенная оценка

$$\operatorname{card} E_2(X) \leq X^{2-\varepsilon}, \tag{2}$$

где $\varepsilon$ — абсолютная, эффективно вычисляемая, положительная малая постоянная.

Полагая $s = n$, $m = n+1$, из (1) получим систему уравнений

$$b_i = a_{i1}p_1 + a_{i2}p_2 + \cdots + a_{i,n+1}p_{n+1}, \quad i = 1, 2, \ldots, n, \tag{3}$$

состоящую из $n$ уравнений с $n+1$ простыми переменными. Для удобства обозначим

$$A_{i_1 i_2 \ldots i_n} = \begin{bmatrix} a_{1i_1} & a_{1i_2} & \cdots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \cdots & a_{2i_n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{ni_1} & a_{ni_2} & \cdots & a_{ni_n} \end{bmatrix}, \quad \Delta_{i_1 i_2 \ldots i_n} = \det(A_{i_1 i_2 \ldots i_n}),$$

где $1 \leq i_1, i_2, \ldots, i_n \leq n+1$; $\Delta_{i_1 i_2 \ldots i_{n-1} b}$ — определитель матрицы $A_{i_1 i_2 \ldots i_{n-1} b}$, полученной из матрицы $A_{i_1 i_2 \ldots i_n}$ заменой $i_n$-го столбца столбцом свободных членов $b_i$ системы (3). Используем также обозначения $\Delta_i = \Delta_{12\ldots i-1, i+1, \ldots n+1}$, $\Delta_{ik}^b$ — определитель $n$-порядка, полученный из $\Delta_i$ заменой элементов $k$-го столбца столбцом свободных членов $b_i$ системы (3).

Для того чтобы избежать тривиальности и вырожденности, налагаем на коэффициенты $a_{ij}$ условия

$$\Delta_1 \Delta_2 \ldots \Delta_{n+1} \neq 0, \quad (\Delta_1, \Delta_2, \ldots, \Delta_{n+1}) = 1. \tag{4}$$

Как обычно, разрешимость системы (1) зависит от следующих двух условий (см. [2]; [3], гл. 5).

А) Для любого простого $p$ системе уравнений

$$a_{i1}l_1 + a_{i2}l_2 + \cdots + a_{i,n+1}l_{n+1} \equiv b_i \pmod p, \quad i = 1, 2, \ldots, n, \tag{5}$$

удовлетворяют некоторые целые числа $l_1, l_2, \ldots, l_{n+1}$ с условием $1 \leq l_1, l_2, \ldots, l_{n+1} \leq p-1$.

B) Для некоторых положительных вещественных чисел $y_1, y_2, \dots, y_{n+1}$ справедливы равенства

$$a_{i1}y_1 + a_{i2}y_2 + \dots + a_{i,n+1}y_{n+1} = b_i, \quad i = 1, 2, \dots, n.$$

Для любого достаточно большого $X$ через $U(X)$ обозначим множество векторов $\overline{b} = (b_1, b_2, \dots, b_n)$, которые удовлетворяют условиям A), B) и $1 \le b_1, b_2, \dots, b_n \le X$. Пусть

$$B = \max\{3|a_{ij}|\}, \quad 1 \le i \le n, \quad 1 \le j \le n+1.$$

Условия A) и B) являются необходимыми при оценке сингулярного ряда и сингулярного интеграла, возникающих в задаче о разрешимости системы уравнений (3) в простых числах. Поэтому при исследовании разрешимости системы (3) в простых числах рассматриваются только те $\overline{b} = (b_1, b_2, \dots, b_n)$, которые содержатся в $U(X)$ (см. [2], [3]). В связи с этим возникает вопрос: какова мощность множества $U(X)$?

В данной работе показано, что множество $U(X)$ содержит достаточно много элементов, а именно доказана

**Теорема.** *Если для некоторых положительных вещественных чисел $y_1, y_2, \dots, y_{n+1}$ выполняются неравенства*

$$a_{i1}y_1 + a_{i2}y_2 + \dots + a_{i,n+1}y_{n+1} > 0, \quad i = 1, 2, \dots, n, \tag{6}$$

*то справедлива оценка*

$$\operatorname{card} U(X) \gg X^n (B^{2(n-1)^2(2n-1)+n} \ln\ln B)^{-1}.$$

Для сравнения отметим, что ранее при $n = 2$ в [2] была получена оценка

$$\operatorname{card} U(X) \gg X^2 (B^2 \ln\ln B)^{-2}. \tag{7}$$

О численных уточнениях значений констант в оценках (2) и (7) см. [4], [5].

Для доказательства приведем леммы. Пусть $a_{ij}$ ($i = \overline{1,n}$; $j = \overline{1,n+1}$) удовлетворяют условиям теоремы. Для любого целого $q \ge 1$ через $\sum_{(q)}$ обозначим суммирование по всем $l_1, l_2, \dots, l_{n+1}$, удовлетворяющим условиям $1 \le l_j \le q$, $(l_j, q) = 1$, $\sum\limits_{1 \le j \le n+1} a_{ij}l_j \equiv b_i \pmod q$, $i = \overline{1,n}$.

Положим

$$N(q) = \sum\nolimits_{(q)} 1. \tag{8}$$

Следующая лемма дает критерий для проверки выполнения условий (5).

**Лемма 1.** *Для любого простого $p > n+1$ равенство $N(p) = 0$ выполняется тогда и только тогда, когда существует такое $i$, $1 \le i \le n+1$, что $\Delta_{j_1 j_2 \cdots j_n} \equiv 0 \pmod p$ всякий раз, когда $j_1, j_2, \dots, j_n \in \{1, 2, \dots, n+1, b\} \setminus \{i\}$.*

**Доказательство.** В случае $n = 2$ лемма совпадает с утверждением 3.1 работы [2]. Рассмотрим случай $n > 2$. В силу (4), не уменьшая общности, можем предполагать, что $\Delta_{n+1} \not\equiv 0 \pmod p$, где $p > n+1$ — фиксированное простое число.

Для удобства сначала рассмотрим случай $n = 3$. Покажем, что $N(p) = 0$ тогда и только тогда, когда существуют такие $i$, $1 \le i \le 4$, что $\Delta_{j_1 j_2 j_3} \equiv 0 \pmod p$ всякий раз, когда $j_1, j_2, j_3 \in \{1, 2, 3, 4, b\} \setminus \{i\}$. Иначе говоря, $N(p) = 0$ тогда и только тогда, когда выполняется хотя бы одно из следующих условий:

$$\begin{aligned}
&i = 1; \quad j_1, j_2, j_3 \in \{2, 3, 4, b\}, \quad \Delta_{234} \equiv \Delta_{23b} \equiv \Delta_{24b} \equiv \Delta_{34b} \equiv 0 \pmod p,\\
&i = 2; \quad j_1, j_2, j_3 \in \{1, 3, 4, b\}, \quad \Delta_{134} \equiv \Delta_{13b} \equiv \Delta_{14b} \equiv \Delta_{34b} \equiv 0 \pmod p,\\
&i = 3; \quad j_1, j_2, j_3 \in \{1, 2, 4, b\}, \quad \Delta_{124} \equiv \Delta_{12b} \equiv \Delta_{14b} \equiv \Delta_{24b} \equiv 0 \pmod p,\\
&i = 4; \quad j_1, j_2, j_3 \in \{1, 2, 3, b\}, \quad \Delta_{123} \equiv \Delta_{12b} \equiv \Delta_{13b} \equiv \Delta_{23b} \equiv 0 \pmod p.
\end{aligned}$$

В силу условий (4) можем предполагать, что $\Delta_{123} \not\equiv 0 \pmod p$, где $p \geq 5$ — фиксированное простое число. Система сравнений

$$\sum_{1 \leq j \leq 4} a_{ij} l_j \equiv b_i \pmod p, \quad i = 1, 2, 3,$$

эквивалентна

$$\begin{aligned}
\Delta_{123} l_1 &\equiv \Delta_{b23} - \Delta_{423} l_4 \equiv \Delta_{23b} - \Delta_{234} l_4 \pmod p, \\
\Delta_{123} l_2 &\equiv \Delta_{1b3} - \Delta_{143} l_4 \equiv -\Delta_{13b} + \Delta_{134} l_4 \pmod p, \\
\Delta_{123} l_3 &\equiv \Delta_{12b} - \Delta_{124} l_4 \equiv \Delta_{12b} - \Delta_{124} l_4 \pmod p.
\end{aligned}$$

Так как $\Delta_{123} \equiv -\Delta_{231} \pmod p$, то

$$\begin{aligned}
\Delta_{213} l_1 &= \Delta_{234} l_4 - \Delta_{23b} \pmod p, \\
\Delta_{123} l_2 &= \Delta_{134} l_4 - \Delta_{13b} \pmod p, \\
\Delta_{213} l_3 &= \Delta_{124} l_4 - \Delta_{12b} \pmod p.
\end{aligned}$$

Следовательно, $N(p) = 0$, если полином

$$P(z) = (\Delta_{234} z - \Delta_{23b})(\Delta_{134} z - \Delta_{13b})(\Delta_{123} z - \Delta_{12b}) z$$

является нулевым полиномом над областью целостности $Z_p(z)$. Поскольку $p \geq 5$ и $\deg P(z) = 4$, то все коэффициенты этого полинома должны делиться на $p$, а для этого необходимо выполнение одного из следующих сравнений: $\Delta_{234} \equiv \Delta_{23b} \equiv 0 \pmod p$, $\Delta_{134} \equiv \Delta_{13b} \equiv 0 \pmod p$, $\Delta_{124} \equiv \Delta_{12b} \equiv 0 \pmod p$. Пусть $\Delta_{234} \equiv \Delta_{23b} \equiv 0 \pmod p$. Остальные случаи рассматриваются аналогично. Так как по предположению $\Delta_{123} \not\equiv 0 \pmod p$, то $p \not| (a_{1i}, a_{2i}, a_{3i})$, $i = 1, 2, 3$. Поэтому из $\Delta_{234} \equiv 0 \pmod p$ и $\Delta_{23b} \equiv 0 \pmod p$ следует $\Delta_{24b} \equiv \Delta_{34b} \equiv 0 \pmod p$.

Действительно, имеем

$$\begin{aligned}
\Delta_{234} &= a_{14} A_{14} + a_{24} A_{24} + a_{34} A_{34} \equiv 0 \pmod p, \\
\Delta_{23b} &= b_1 A_{14} + b_2 A_{24} + b_3 A_{34} \equiv 0 \pmod p, \\
\Delta_{24b} &= b_1 (a_{22} a_{34} - a_{24} a_{32}) - b_2 (a_{12} a_{34} - a_{14} a_{32}) + b_3 (a_{12} a_{24} - a_{14} a_{22}),
\end{aligned}$$

$A_{i4}$ — алгебраическое дополнение элемента $a_{i4}$. Можно считать, что хотя бы одно из $A_{14}$, $A_{24}$, $A_{34}$ отлично от нуля (иначе было бы $\Delta_{123} = 0$). Пусть $A_{14} \neq 0$, тогда

$$a_{14} \equiv (-a_{24} A_{24} - a_{34} A_{34}) A_{14}^{-1} \pmod p, \quad b_1 \equiv (-b_2 A_{24} - b_3 A_{34}) A_{14}^{-1} \pmod p$$

и $\Delta_{24b} \equiv -b_2 a_{34} (a_{22} A_{24} + a_{12} A_{14} + a_{32} A_{34}) + b_3 a_{24} (a_{32} A_{34} + a_{12} A_{14} + a_{22} A_{24}) \equiv 0 \pmod p$. Аналогично $\Delta_{34b} \equiv b_1 (a_{23} a_{34} - a_{24} a_{33}) - b_2 (a_{13} a_{34} - a_{14} a_{33}) + b_3 (a_{13} a_{24} - a_{14} a_{23}) \equiv -b_2 a_{34} (a_{23} A_{24} + a_{13} A_{14} + a_{33} A_{34}) + b_3 a_{24} (a_{13} A_{14} + a_{33} A_{34} + a_{23} A_{24}) \equiv 0 \pmod p$. Так как $\Delta_{123} \not\equiv 0 \pmod p$, а следовательно, $p \not| (a_{1i}, a_{2i}, a_{3i})$, то из $\Delta_{ij_1j_2} \equiv \Delta_{ik_1k_2} \equiv 0 \pmod p$ следует $\Delta_{j_1k_1k_2} \equiv \Delta_{j_1j_2k_1} \equiv \Delta_{j_2k_1k_2} \equiv \Delta_{j_1j_2k_2} \equiv 0 \pmod p$. Таким образом, в случае $n = 3$ лемма доказана.

Пусть теперь $n > 3$. В этом случае система сравнений

$$\sum_{1 \leq j \leq n+1} a_{ij} l_j \equiv b_i \pmod p, \quad i = 1, 2, \ldots, n,$$

эквивалентна системе

$$\begin{aligned}
\Delta_{n+1} l_1 &\equiv \Delta^b_{n+1,1} - \Delta^{n+1}_{n+1,1} l_{n+1} \pmod p, \\
\Delta_{n+1} l_2 &\equiv \Delta^b_{n+1,2} - \Delta^{n+1}_{n+1,2} l_{n+1} \pmod p, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\Delta_{n+1} l_n &\equiv \Delta^b_{n+1,n} - \Delta^{n+1}_{n+1,n} l_{n+1} \pmod p.
\end{aligned}$$

Следовательно, $N(p) = 0$, если полином

$$P(z) = \prod_{j=1}^{n} (\Delta^{b}_{n+1,j} - \Delta^{n+1}_{n+1,j} z) z$$

является нулевым полиномом над областью целостности $Z_p[z]$, т. е. $P(l) \equiv 0 \pmod p$ для всех $l$, т. к. $\deg P(z) = n + 1 < p$, то это может случиться тогда и только тогда, когда

$$\Delta^{b}_{n+1,j} \equiv \Delta^{n+1}_{n+1,j} \equiv 0 \pmod p$$

хотя бы для одного $j = 1, 2, \ldots, n$. В силу $\Delta_{n+1} \not\equiv 0 \pmod p$ это означает, что

$$\Delta_{j_1 j_2 \ldots j_{n-1}, n+1} \equiv \Delta_{j_1 j_2 \ldots j_{n-1} b} \equiv 0 \pmod p \quad \text{и} \quad \Delta_{j_1 j_2 \ldots j_{n-2}, n+1, b} \equiv 0 \pmod p$$

для всех $j_1, j_2, \ldots, j_{n-1} \in \{1, 2, \ldots, n\}$. Поскольку $\Delta_{n+1} \not\equiv 0 \pmod p$, то $p \not| (a_{1i}, a_{2i}, \ldots, a_{ni})$ при $i = 1, 2, \ldots, n$ и тогда из

$$\Delta_{i j_1 j_2 \ldots j_{n-1}} \equiv \Delta_{i k_1 k_2 \ldots k_{n-1}} \equiv 0 \pmod p$$

следует

$$\Delta_{j k_1 k_2 \ldots k_{n-1}} \equiv \ldots \equiv \Delta_{j_{n-1} k_1 k_2 \ldots k_{n-1}} \equiv 0 \pmod p. \tag{9}$$

В (9) входят все определители $n$-го порядка, которые можно образовать, используя столбцы с номерами $j_1, j_2, \ldots, j_{n-1}$, $k_1, k_2, \ldots, k_{n-1}$. Таким образом, лемма 1 доказана.

**Лемма 2.** *Пусть* $(b_1, b_2, \ldots, b_n)$ *— фиксированное значение* $\overline{b}$ *в кубе* $[1, m]^n$*, для которого* $N(p) > 0$ *при всех* $p$*. Тогда существуют не менее чем* $N_1$,

$$N_1 \gg X^n (m^n B^{2(n-1)^2(2n-1)})^{-1}, \tag{10}$$

*значений* $(z_1, z_2, \ldots, z_n)$*, удовлетворяющих условиям*

$$1 \le z_i \le X, \quad z_i \equiv b_i \pmod m, \quad \sum_{j=1}^{n+1} a_{ij} y_j = z_i, \quad i = \overline{1, n},$$

*где* $y_1, y_2, \ldots, y_{n+1}$ *— некоторые положительные действительные числа.*

**Доказательство.** Решая систему уравнений

$$\sum_{j=1}^{n} a_{ij} y_j = z_i, \quad i = \overline{1, n},$$

относительно $y_2, y_3, \ldots, y_{n+1}$, находим

$$\begin{aligned} y_2 &= \frac{1}{\Delta_1}(-\Delta^1_{12} y_1 + \Delta^z_{12}), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ y_{n+1} &= \frac{1}{\Delta_1}(-\Delta^1_{1,n+1} y_1 + \Delta^z_{1,n+1}). \end{aligned} \tag{11}$$

Если необходимо, переобозначив индексы $j$ коэффициентов $a_{ij}$, можем предположить, что

$$-\Delta^1_{12} > 0, \ldots, -\Delta^1_{1,n+1} > 0.$$

Если $\Delta_1 > 0$, то система (11) разрешима в положительных вещественных числах $y_j$, а это означает, что условие B) выполняется для любого вещественного $b_1, b_2, \ldots, b_n$. Поэтому в этом случае (10) очевидно выполняется.

Теперь рассмотрим случай $\Delta_1 < 0$. В этом случае система (11) будет иметь положительные решения $y_1, y_2, \ldots, y_{n+1}$, если

$$\Delta^z_{12} < 0, \Delta^z_{13} < 0, \ldots, \Delta^z_{1,n+1} < 0.$$

Обозначив $x_i = \frac{z_i}{z_1}$, $i = 2, 3, \ldots, n$, последние условия можно записать в виде системы линейных неравенств относительно $x_2, x_3, \ldots, x_n > 0$:

$$\begin{aligned}
&z_1 A_{11} + z_2 A_{21} + \cdots + z_n A_{n1} < 0,\\
&z_1 A_{12} + z_2 A_{22} + \cdots + z_n A_{n2} < 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&z_1 A_{1n} + z_2 A_{2n} + \cdots + z_n A_{nn} < 0
\end{aligned}$$

или

$$\begin{aligned}
&A_{21} x_2 + \cdots + A_{n1} x_n < -A_{11},\\
&A_{22} x_2 + \cdots + A_{n2} x_n < -A_{12},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&A_{2n} x_2 + \cdots + A_{nn} x_n < -A_{1n}.
\end{aligned}$$

Условия (6) теоремы гарантируют, что множество решений однородных неравенств непусто и, следовательно, можем считать, что $U_1 < x_2, \ldots, x_n < U_2$, где $0 \le U_1 < a(n, B)$, и

$$\frac{1}{a^2(n,B)} < U_2 - U_1 < a(n,B), \quad a(n,B) = [(n-1)!]^n B^{(n-1)^2}. \tag{12}$$

Пусть $z_1 \equiv b_1 \pmod m$ — фиксированное число, тогда $A_i$ — количество $z_i$, удовлетворяющих условиям

$$1 \le z_i \le X, \quad z_i \equiv b_i \pmod m, \quad U_1 < z_i z_1^{-1} < U_2, \quad i = \overline{1,n}, \tag{13}$$

можно записать в виде

$$A_i = \min\{z_i (U_2 - U_1) m^{-1}, (X - z_1 U_1) m^{-1}\} + O(1). \tag{14}$$

Действительно, из (13) находим $U_1 z_1 < z_i < U_2 z_1$, $z_i = b_i + mt$, $m^{-1}(U_1 z_1 - b_i) < t < (U_2 z_1 - b_i) m^{-1}$. Отсюда количество $t$ и, следовательно, количество $z_i$, удовлетворяющих условиям (13), равно

$$\left[\frac{U_2 z_1}{m} - \frac{U_1 z_1}{m}\right] - \varepsilon_2 = \left[\frac{1}{m}(U_2 - U_1) z_1\right] - \varepsilon_2. \tag{15}$$

С другой стороны, $z_i \le X$, $z_i \equiv b_i \pmod m$, поэтому $t \le m^{-1}(X - b_i)$ и количество $z_i$, удовлетворяющих условиям (13), равно

$$\left[\frac{X - b_i}{m} - \frac{U_1 z_1 - b_i}{m}\right] - \varepsilon_3 = \left[\frac{1}{m}(X - U_1 z_1)\right] - \varepsilon_3, \tag{16}$$

где $\varepsilon_2$и $\varepsilon_3$ равно единице или нулю в зависимости от того, является ли $m^{-1}(U_2 - U_1) z_1$ и $m^{-1}(X - U_1 z_1)$ целым или нет. Из (15) и (16) следует (14).

В силу (12) при $z_1 \le X(2U_1)^{-1}$ ($z_1 \le X/2a(n,B)^2$) из (14) находим

$$A_i \gg \min\{z_1 B^{-2(n-1)^2} m^{-1}; X(2m)^{-1}\} - O(1) \gg z_1 (B^{2(n-1)^2} m)^{-1} - O(1), \quad \text{если} \quad X > 2 z_1 B^{-2(n-1)^2}.$$

Собирая такие оценки для всех $i = 2, 3, \ldots, n$, получим

$$A = A_2 A_3 \ldots A_n \gg [z_1 (B^{2(n-1)^2} m)^{-1} - O(1)]^{n-1}.$$

Теперь суммируя по всем $z_1$, удовлетворяющим условиям $z_1 \equiv b_1 \pmod m$ и $1 \le z_1 \le X/2a(n,B)^2$, убедимся, что

$$N_1 \gg \sum_{z_1} \{z_1 (B^{2(n-1)^2} m)^{-1} - O(1)\}^{n-1}.$$

Разлагая выражение, стоящее под суммой, по формуле бинома Ньютона, а затем суммируя по $z_1$ каждый член отдельно, находим

$$N_1 \gg (mB^{2(n-1)^2})^{-n+1} \sum_{\substack{z_1 \le X/2a(n,B)^2 \\ z_1 \equiv b_1 \pmod m}} z_1^{n-1} \gg \frac{m^{n-1}}{(mB^{2(n-1)^2})^{n-1}} \sum_{t \le \frac{X-b_1}{2a(n,B)^2 m}} t^{n-1} \gg$$
$$\gg \frac{1}{B^{2(n-1)^2}} \left(\frac{X-b_1}{2a(n,B)^2 m}\right)^n \gg \frac{X^n}{m^n B^{2(n-1)^3+2n(n-1)^2}} \gg \frac{X^n}{B^{2(n-1)^2(2n-1)} m^n}.$$

Таким образом, лемма 2 доказана.

**Доказательство теоремы.** По определению $U(X)$ количество векторов $\overline{b} = (b_1, b_2, \dots, b_n) \in U(X)$ определяется двумя условиями A) и B). Сначала рассмотрим условие A). В силу (8) достаточно определить количество $\overline{b}$, для которых выполняется $N(p) > 0$ для всех $p$. Пусть $p_1, p_2, \dots, p_s$ — все простые числа, не превосходящие $n+1$. Тогда $N(p_i) > 0$ $(i = 1, 2, \dots, s)$, если $b_1, b_2, \dots, b_n$ лежат в некотором подходяще выбранном классе вычетов по модулю $m_1 = p_1 p_2 \dots p_s$, например, когда $b_i \equiv a_{i1} + \dots + a_{i,n+1} \pmod{m_1}$, $i = 1, 2, \dots, n$ $((l_1, l_2, \dots, l_{n+1}) \equiv (1, 1, \dots, 1))$.

Для $p > n+1$, применяем лемму 1. Сначала, если $p \not\backslash \Delta_1 \Delta_2 \dots \Delta_{n+1}$, то независимо от значений $b_1, b_2, \dots, b_n$ лемма 1 означает, что $N(p) > 0$. Во-вторых, ввиду (4) можем полагать, что $q_1^{(1)}, q_2^{(1)}, \dots, q_{u_1}^{(1)}$ — это те простые числа, бо́льшие $n+1$, которые делят точно один из определителей $\Delta_j$, $j = 1, 2, \dots, n+1$; $q_1^{(2)}, q_2^{(2)}, \dots, q_{u_2}^{(2)}$ — те делители, которые делят точно два из них, и т. д., $q_1^{(n)}, q_2^{(n)}, \dots, q_{u_n}^{(n)}$ — те делители, которые делят точно $n$ из них.

Рассмотрим $q = q_1^{(1)}$ и пусть $q \backslash \Delta_{n+1}$, $q \not\backslash \Delta_1 \Delta_2 \dots \Delta_n$. В силу (9), если $q \backslash \Delta^b_{n+1,n}$, то $q \backslash \Delta^b_{1,n+1}$, $q \backslash \Delta^b_{2,n+1}, \dots, q \backslash \Delta^b_{n,n+1}$. Поэтому $N(p) = 0$ тогда и только тогда, когда $q \backslash \Delta^b_{n+1,n}$. Сравнению $\Delta^b_{n+1,n} \equiv 0 \pmod q$ удовлетворяют точно $q^{n-1}$ значений $\overline{b} = (b_1, b_2, \dots, b_n)$. Действительно, фиксируем $b_3, b_4, \dots, b_n$, тогда существуют $q$ пар $(b_1, b_2)$, которые удовлетворяют указанному сравнению. Учитывая, что $1 \le b_3, b_4, \dots, b_n \le q$ получим $q^{n-2} q = q^{n-1}$ значений $\overline{b}$. Поэтому для каждого оставшегося $q^n - q^{n-1} = \varphi(q^n)$ значений $\overline{b} = (b_1, b_2, \dots, b_n)$ имеем $q \not\backslash \Delta^b_{n+1,n}$ и, следовательно, $N(p) > 0$.

Пусть теперь $q = q_1^{(2)}$ и $q \backslash (\Delta_{n+1}, \Delta_n)$, $q \not\backslash \Delta_1 \Delta_2 \dots \Delta_{n-1}$. Следовательно, $q \backslash \Delta^b_{n+1,n}$.

Так как $q \not\backslash \Delta_1 \Delta_2 \dots \Delta_{n-1}$, то можем полагать, что $q \not\backslash (a_{1j}, a_{2j}, \dots, a_{nj})$ $(j = n, n+1)$. При $j = n$ имеем $\{1, 2, \dots, n, n+1, b\} \setminus \{n\} = \{1, 2, \dots, n-1, n+1, b\}$. Если

$$\Delta_{12\dots n-1,n+1} \equiv \Delta_{12\dots n-1,b} \equiv \Delta_{23\dots n-1,n+1,b} \equiv \Delta_{13\dots n-1,n+1,b} \equiv \dots \equiv \Delta_{123\dots n-2,n+1,b} \equiv 0 \pmod q,$$

то $N(q) = 0$. Согласно условию $\Delta_n = \Delta_{12\dots n-1,n+2} \equiv 0$ и $\Delta^b_{n,n+1} = \Delta_{12\dots n-1,b} \equiv 0 \pmod q$. Поэтому

$$(N(q) = 0) \Leftrightarrow (\Delta_{23\dots n-1,n+1,b} \equiv \Delta_{13\dots n-1,n+1,b} \equiv \dots \equiv \Delta_{123\dots n-2,n+1,b} \equiv 0 \pmod q).$$

Каждое из этих сравнений имеет $q^{n-1}$ решений относительно $b_1, b_2, \dots, b_n$ по модулю $q$. Следовательно, количество решений этой системы не больше $q^{n-1}$. Аналогично при $j = n+1$ получим систему, состоящую из $n-1$ сравнений

$$\Delta_{23\dots n-1,n,b} \equiv 0,\ \Delta_{134\dots n-1,n,b} \equiv 0,\ \dots,\ \Delta_{12\dots n-2,n,b} \equiv 0 \pmod q.$$

Количество решений этой системы не больше $q^{n-1}$. Следовательно, $N(q) > 0$ для не менее чем $q^n - 2q^{n-1}$ значений $\overline{b} = (b_1, b_2, \dots, b_n)$ по модулю $q$.

Аналогично находим, что $N(q) > 0$ для

$$\begin{aligned}
&q = q_1^{(3)}, \quad q^n - 3q^{n-1} \quad (j = n-1, n, n+1), \\
&q = q_1^{(4)}, \quad q^n - 4q^{n-1} \quad (j = n-2, n-1, n, n+1), \\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
&q = q_1^{(n)}, \quad q^n - nq^{n-1} \quad (j = 2, 3, \dots, n, n+1)
\end{aligned}$$

соответственно значений $\overline{b} = (b_1, b_2, \dots, b_n)$ по модулю $q$.

Пусть $m = m_1 q_1^{(1)} \dots q_{u_1}^{(1)} q_1^{(2)} \dots q_{u_2}^{(2)} \dots q_1^{(n)} \dots q_{u_n}^{(n)}$. Из сказанного выше заключаем, что существуют по крайней мере

$$\prod_{j_1=1}^{u_1} (q_{j_1}^{(1)})^{n-1} \varphi(q_{j_1}^{(1)}) \prod_{j_2=1}^{u_2} ((q_{j_2}^{(2)})^n - 2(q_{j_2}^{(2)})^{n-1}) \dots \prod_{j_n=1}^{u_n} ((q_{j_n}^{(n)})^n - n(q_{j_n}^{(n)})^{n-1}) \tag{17}$$

значений $\overline{b} = (b_1, b_2, \dots, b_n)$ по модулю $m$, для которых $N(p) > 0$ для всех простых $p$.

Теперь рассмотрим условие B). Пусть $(b_1, b_2, \dots, b_n)$ — фиксированное значение $\overline{b}$ в кубе $[1, m]^n$, для которого $N(p) > 0$ при всех $p$. Тогда в силу (17) и (10) из определения $U(X)$ получим

$$\operatorname{card} U(X) \gg N_1 \left(\frac{m}{n}\right)^n \prod_{j_1=1}^{u_1} \varphi(q_{j_1}^{(1)})(q_{j_1}^{(1)})^{-1} \prod_{j_2=1}^{u_2} (1 - 2/q_{j_2}^{(2)}) \dots \prod_{j_n=1}^{u_n} (1 - n/q_{j_n}^{(n)}).$$

Учитывая, что $1 - nq_j^{-1} \geq n^{-1}(1 - q_j^{-1})$ для любого $n \geq 1$, имеем

$$\operatorname{card} U(X) \gg N_1 \left(\frac{m}{m_1}\right)^n \prod_{j_1=1}^{u_1} \varphi(q_{j_1}^{(1)})(q_{j_1}^{(1)})^{-1} \prod_{j_2=1}^{u_2} \frac{1}{2}\left(1 - \frac{1}{q_{j_2}^{(2)}}\right) \dots$$

$$\dots \prod_{j_n=1}^{u_n} \frac{1}{n}\left(1 - \frac{1}{q_{j_n}^{(n)}}\right) \gg N_1 \left(\frac{m}{m_1}\right)^n \left(\ln\ln \frac{m}{m_1}\right)^{-1}.$$

Так как $m_1 = p_1 p_2 \dots p_s \leq (n+1)^s \leq (n+1)^{(n+1)/\ln(n+1)}$, $m \leq m_1 |\Delta_1 \Delta_2 \dots \Delta_{n+1}| \ll B^{n(n+1)}$, то $\operatorname{card} U(X) \gg X^n (B^{2(n-1)^2(2n-1)+n} \ln\ln B)^{-1}$, что и требовалось доказать.

В заключение автор выражает благодарность за полезные обсуждения профессорам А.Ф. Лаврику и М.И. Исраилову.

## Литература

1. Wu Fang. *On the solutions of the systems of linear equations with prime variables* // Acta Math. Sinica. – 1957. – V. 7. – P. 102–121.
2. Liu M.C., Tsang K.M. *On pairs of linear equations in three prime variables and application to Goldbach's problem* // J. reine angew. Math. – 1989. – V. 399. – P. 109–136.
3. Хуа-Ло-Ген. *Метод тригонометрических сумм и его применения в теории чисел.* – М.: Мир, 1964. – 188 с.
4. Аллаков И.А. *О разрешимости пары линейных уравнений с тремя простыми переменными* // Узб. матем. журн. – 1993. – № 1. – С. 26–34.
5. Allakov I.A., Israilov M.I. *About simultaneous representation of two natural numbers by sum of three primes* // Lect. of The Third Internat. Workshop of Comput. Algebra in Scien. Comput. Springer. CASC – 2000. – P. 13–20.

*Термезский государственный университет*

*Поступила*
21.02.2003