Записки научных
семинаров ПОМИ
Том 322, 2005 г.

Ю. В. Нестеренко

О ПРОБЛЕМЕ ВАРИНГА (ЭЛЕМЕНТАРНЫЕ МЕТОДЫ)

**Посвящается памяти
Юрия Владимировича Линника**

1. Введение

В 1770 г. Ж. Л. Лагранж доказал, что каждое натуральное число есть сумма не более четырех квадратов натуральных чисел. В том же году Е. Варинг высказал предположение, что *каждое натуральное число есть сумма не более* 9 *кубов натуральных чисел, не более* 19 *биквадратов и т.д.*

Первый шаг в решении проблемы Варинга сделал в 1859 г. Ж. Лиувилль, доказавший, что каждое натуральное число есть сумма не более 53 биквадратов. При этом он использовал некоторое тождество для многочленов от 4 переменных. Позднее для той же цели Е. Люка предложил более простое тождество

$$6(x_1^2+x_2^2+x_3^3+x_4^2)^2 = \sum \left((x_i+x_j)^4+(x_i-x_j)^4\right), \qquad (1)$$

в котором суммирование ведется по всем парам целых чисел i, j с условием $1 \le i < j \le 4$.

Впоследствии усилиями многих математиков подобные результаты были установлены для степеней 3, 5, 6, 7, 8, 10, см. [10], гл. 25. При этом в основе доказательств лежали все более сложные тождества, подобные (1). В 1909 г. в работе [13] Д. Гильберт доказал, что

Теорема 1. *При любом целом* $n \ge 1$ *каждое натуральное число допускает представление в виде суммы* n*-х степеней натуральных чисел, количество которых не превосходит некоторой границы, определяемой только показателем* n *и не зависящей от представляемого числа.*

Эта работа выполнена при частичной поддержке Российского Фонда Фундаментальных исследований, грант No. 03-01-00359.

Распространено мнение, что доказательство теоремы Гильберта весьма сложно в техническом отношении и трудно для понимания. В действительности это не так.

Настоящая статья носит методический характер. В ней приводятся два элементарных доказательства теоремы Гильберта. Первое следует идеям самого Гильберта, а второе было предложено Ю. В. Линником в 1943 г. Естественно, оба доказательства имеют отличия от оригинальных, так как впитали в себя ряд упрощений и усовершенствований, предложенных впоследствии различными авторами. Мы не касаемся результатов, полученных аналитическими методами. С ними можно познакомиться, например, по комментариям к русскому переводу трудов Гильберта [13], стр. 540–546, см. также Предисловие Р. С. Вона к книге H. Davenport [21].

2. Доказательство Гильберта

Работа Гильберта завершает целый ряд исследований, естественным образом обобщая и развивая предшествующие идеи. Технические трудности оригинального доказательства были сосредоточены в обосновании необходимого общего тождества (теорема 2). Вывод с его помощью гипотезы Варинга был совершенно элементарен и помещен нами с некоторыми упрощениями в разделе 2.2.

2.1. Тождество Гильберта.

Теорема 2. *Для любых целых $m > 1$ и $r > 1$ существуют положительные рациональные числа b_i и целые отличные от нуля числа a_{ij} такие, что тождественно по r переменным $x_1, \ldots, x_r$ выполняется равенство*

$$\left(x_1^2 + \ldots + x_r^2\right)^m = \sum_{j=1}^{M} b_j \left(a_{1j}x_1 + \ldots + a_{rj}x_r\right)^{2m}, \qquad (2)$$

причем $M = (2m+1)^r$.

Отметим, что Гильберт доказал эту теорему при $r = 5$ и меньшем значении M. Однако для решения проблемы Варинга в его формулировке величина M не имеет значения.

Теорема 2 была сформулирована в работе Гурвица [15] в качестве предположения, и использовалась там для доказательства утверждения, что из справедливости гипотезы Варинга для показателя m следует ее справедливость для показателя $2m$. Впервые теорема 2 была доказана Гильбертом, [13], с использованием для этого кратных интегралов по многомерному шару. Одновременно со статьей Гильберта была опубликована статья Хаусдорфа [12], где давалось иное доказательство теоремы, применявшее кратные несобственные интегралы и ортогональные многочлены Эрмита. Впоследствии оказалось, что доказательство Хаусдорфа может быть проведено без использования интегралов. За три года в работах Е. Стридсберга [18], А. Гурвица [16], Р. Ремака [17], Г. Фробениуса [11] был найден элементарный вариант рассуждений Хаусдорфа. Ниже дается еще одно элементарное доказательство теоремы 2. По существу оно также является переработкой доказательства Хаусдорфа.

Определим последовательность целых чисел c_k равенствами

$$c_{2j} = \frac{(2j)!}{j!}, \quad , c_{2j+1} = 0, \quad j \geq 0.$$

Пусть при некоторых натуральных n и m действительные числа α_h, β_h, $h = 1, \ldots, n$ удовлетворяют условиям

$$\sum_{h=1}^{n} \beta_h \alpha_h^k = c_k, \quad k = 0, 1, \ldots, 2m, \quad \beta_h > 0, \tag{3}$$

Тогда тождественно по переменным $x_1, \ldots, x_r$ выполняются равенства

$$\begin{aligned}
&\sum_{h_1=1}^{n} \cdots \sum_{h_r=1}^{n} \beta_{h_1} \cdots \beta_{h_r} \left(\alpha_{h_1} x_1 + \ldots + \alpha_{h_r} x_r\right)^{2m} \\
&= \sum_{h_1=1}^{n} \cdots \sum_{h_r=1}^{n} \sum_{k_1+\cdots+k_r=2m} \frac{(2m)!}{k_1! \cdots k_r!} \beta_{h_1} \cdots \beta_{h_r} \alpha_{h_1}^{k_1} \cdots \alpha_{h_r}^{k_r} x_1^{k_1} \cdots x_r^{k_r} \\
&= \sum_{k_1+\cdots+k_r=2m} \frac{(2m)!}{k_1! \cdots k_r!} c_{k_1} \cdots c_{k_r} x_1^{k_1} \cdots x_r^{k_r} \\
&= \frac{(2m)!}{m!} \sum_{j_1+\cdots+j_r=m} \frac{m!}{j_1! \cdots j_r!} x_1^{2j_1} \cdots x_r^{2j_r} = \frac{(2m)!}{m!} \left(x_1^2 + \cdots + x_r^2\right)^m .
\end{aligned} \tag{4}$$

Таким образом, теорема 2 будет доказана, если мы установим, что при некотором n система условий (3) относительно неизвестных α_h, β_h разрешима в рациональных числах.

Положим в (3), (4) параметр $n = 2m + 1$. Тогда для доказательства теоремы достаточно установить существование действительных чисел β_k и различных действительных чисел α_k, удовлетворяющих условиям (3). Действительно, при фиксированных различных α_h и $n = 2m+1$ равенства (3) определяют числа β_k единственным образом. При этом числа β_k непрерывно зависят от α_h. Если выбрать рациональные числа $\alpha_h^{'}$ достаточно близкими к α_h, отличными от нуля, и определить для них соответствующие числа $\beta_k^{'}$ с помощью равенств (3), то числа $\beta_k^{'}$ также будут расположены вблизи от чисел β_k. Это означает, что для рациональных чисел $\alpha_k^{'}$, $\beta_k^{'}$ будут выполнены все условия (3), и, следовательно, теорема 1 будет справедлива.

Определим формальные ряды $f_n(x)$ следующим образом

$$f_n(x) = 2^n \sum_{k=0}^{\infty} \frac{(2k+n)!}{k!} x^{-2k-n-1}, \quad n \geq 0.$$

Тогда

$$f_0(x) = \sum_{k=0}^{\infty} c_k x^{-k-1}. \tag{5}$$

Лемма 1. *Справедливы следующие соотношения*

$$f_1(x) = x f_0(x) - 1, \tag{6}$$

$$f_{n+1}(x) = x f_n(x) - 2n f_{n-1}(x), \quad n \geq 1. \tag{7}$$

Доказательство. Оба тождества (6), (7) доказываются сравнением коэффициентов соответствующих рядов. Имеем

$$x f_0(x) - 1 = 2 \sum_{k=1}^{\infty} \frac{(2k-1)!}{(k-1)!} \cdot x^{-2k} = f_1(x),$$

и при $n \geq 1$

$$x f_n(x) - 2n f_{n-1}(x) = x^{-n} 2^{n+1} \sum_{k=1}^{\infty} \frac{(2k+n-1)!}{(k-1)!} \cdot x^{-2k} = f_{n+1}(x). \quad \square$$

Определим последовательность многочленов $Q_n(x)$ при помощи рекуррентного уравнения

$$Q_{n+1}(x) = x Q_n(x) - 2n Q_{n-1}(x), \quad Q_0(x) = 1,\ Q_1(x) = x. \tag{8}$$

Вторую последовательность многочленов $P_n(x)$ определим с помощью того же рекуррентного уравнения, но с начальными данными $P_0(x) = 0$, $P_1(x) = 1$. Из (8) следует, что степень многочлена $Q_n(x)$ равна n, а коэффициент при x^n равен 1. Кроме того $\deg P_n(x) \leq n - 1$.

Лемма 2. *При $n \geq 0$ справедливы тождества*

$$f_n(x) = Q_n(x) f_0(x) - P_n(x), \tag{9}$$

$$P_{n+1}(x) Q_n(x) - P_n(x) Q_{n+1}(x) = 2^n \cdot n!, \tag{10}$$

$$Q'_{n+1}(x) = (n+1) Q_n(x). \tag{11}$$

Доказательство. Три последовательности $f_n(x)$, $P_n(x)$, $Q_n(x)$ удовлетворяют одному и тому же рекуррентному уравнению второго порядка, см. (7), (8). Поэтому для доказательства (9) достаточно проверить эти соотношения при $n = 0, 1$. При $n = 0$ равенство (9) следует из определения многочленов $P_0(x)$ и $Q_0(x)$. А при $n = 1$ оно совпадает с равенством (6).

Прямое вычисление показывает, что $P_1(x) Q_0(x) - P_0(x) Q_1(x) = 1$. Так как обе последовательности $P_n(x)$ и $Q_n(x)$ удовлетворяют рекуррентному уравнению (8), то справедливо тождество

$$P_{n+1}(x) Q_n(x) - P_n(x) Q_{n+1}(x) = 2n(P_n(x) Q_{n-1}(x) - P_{n-1}(x) Q_n(x)),$$

из которого с помощью индукции получается равенство (10).

Для доказательства (11) также воспользуемся индукцией. При $n = 0$ и $n = 1$ равенство (11) проверяется непосредственно. Предположим, что оно справедливо при всех $n < k$, где $k \geq 2$. Дифференцируя равенство

$$Q_{k+1}(x) = x Q_k(x) - 2k Q_{k-1}(x),$$

и пользуясь предположением, находим

$$Q'_{k+1}(x) = Q_k(x) + xk Q_{k-1}(x) - 2k(k-1) Q_{k-2}(x) = (k+1) Q_k(x). \quad \square$$

Лемма 3. *Для $n \geq 1$ полином $Q_n(x)$ имеет n действительных корней $\lambda_1 < \lambda_2 < \ldots < \lambda_n$, причем*

$$\operatorname{sign} Q'_n(\lambda_j) = (-1)^{n-j}, \quad j = 1, \ldots, n.$$

Доказательство. Докажем лемму индукцией по n. При $n = 1$ имеем $Q_1(x) = x$ и утверждение, очевидно, выполняется. Докажем теперь утверждение леммы для многочлена $Q_{n+1}(x)$, считая, что для $Q_n(x)$ оно имеет место. Из равенств (8) и (11) находим

$$Q_{n+1}(\lambda_j) = -2nQ_{n-1}(\lambda_j) = -2Q_n'(\lambda_j).$$

Поэтому $\operatorname{sign} Q_{n+1}(\lambda_j) = (-1)^{n+1-j}$. Отсюда следует, что существуют нули μ_j многочлена $Q_{n+1}(x)$ такие, что

$$\lambda_1 < \mu_2 < \lambda_2 < \ldots < \lambda_{n-1} < \mu_n < \lambda_n.$$

Учитывая, что $\operatorname{sign} Q_{n+1}(\lambda_n) = -1$ и $\operatorname{sign} Q_{n+1}(+\infty) = 1$, заключаем, что многочлен $Q_{n+1}(x)$ имеет нуль $\mu_{n+1} > \lambda_n$. Кроме того, равенства $\operatorname{sign} Q_{n+1}(-\infty) = (-1)^{n+1}$, $\operatorname{sign} Q_{n+1}(\lambda_1) = (-1)^n$ означают существование нуля μ_1 с условием $\mu_1 < \lambda_1$. Итак, многочлен $Q_{n+1}(x)$ имеет $n+1$ различных действительных нулей.

Пользуясь теперь следующими из (11) равенствами

$$Q_{n+1}'(\mu_j) = (n+1)Q_n(\mu_j)$$

и неравенствами

$$\mu_1 < \lambda_1 < \mu_2 < \lambda_2 < \ldots < \lambda_{n-1} < \mu_n < \lambda_n < \mu_{n+1},$$

заключаем, что последовательность $Q_{n+1}'(\mu_j)$ – знакочередующаяся. Учитывая, что $Q_n(\mu_{n+1}) > 0$ и, потому $Q_{n+1}'(\mu_{n+1}) > 0$, находим, что $\operatorname{sign} Q_{n+1}'(\mu_j) = (-1)^{n+1-j}$. $\square$

Завершим теперь доказательство существования действительных чисел α_h, β_h, удовлетворяющих условиям (3) при $n = 2m+1$. Обозначим $\alpha_1, \ldots, \alpha_n$ корни многочлена $Q_n(x)$. Согласно лемме 3 все они действительны и различны. Поскольку $\deg P_n(x) < Q_n(x)$, то рациональная функция $\frac{P_n(x)}{Q_n(x)}$ имеет следующее разложение в сумму простейших дробей

$$\frac{P_n(x)}{Q_n(x)} = \frac{\beta_1}{x-\alpha_1} + \cdots + \frac{\beta_n}{x-\alpha_n}. \tag{12}$$

Из этого равенства и тождеств (10), (11) находим

$$\beta_h = \frac{P_n(\alpha_h)}{Q_n'(\alpha_h)} = \frac{2^{n-1}\cdot(n-1)!}{Q_n'(\alpha_h)Q_{n-1}(\alpha_h)} = \frac{2^{n-1}\cdot n!}{Q_n'(\alpha_h)^2} > 0.$$

Из (12) следует, что разложение функции $\frac{P_n(x)}{Q_n(x)}$ в ряд Тейлора в окрестности точки ∞ имеет вид

$$\frac{P_n(x)}{Q_n(x)} = \sum_{k=0}^{\infty} \left(\sum_{h=1}^{n} \alpha_h \beta_h^k \right) x^{-k-1}. \tag{13}$$

Согласно (9) имеем

$$f_0(x) - \frac{P_n(x)}{Q_n(x)} = \frac{f_n(x)}{Q_n(x)} = O(x^{-2n-1}),$$

так что первые $2n$ коэффициентов разложения (13) совпадают с соответствующими коэффициентами ряда (5) для $f_0(x)$. Таким образом, выполняются равенства

$$\sum_{h=1}^{n} \alpha_h \beta_h^k = c_k, \quad k = 0, 1, \ldots, 2n-1,$$

и, в частности, равенства (3) при $n = 2m+1$. Итак, действительные числа, удовлетворяющие условиям (3) построены. Это завершает доказательство теоремы 2.

Формальный ряд (5), определяющий $f_0(x)$, является вырожденной гипергеометрической функцией. Разложения таких рядов в непрерывные дроби хорошо известны, см. [4, гл. 2]. Дроби $\frac{P_n(x)}{Q_n(x)}$ являются подходящими дробями непрерывной дроби для $f_0(x)$. Рекуррентные уравнения (8) – это уравнения для числителей и знаменателей подходящих дробей, см. [4, формула (2.1.6)]. Равенства (10) – также классические соотношения между числителями и знаменателями соседних подходящих дробей, см. [4, формула (1.1.9)]. Знаменатели подходящих дробей $Q_n(x)$ связаны с классическими многочленами Эрмита $H_n(x)$ соотношением $Q_n(x) = H_n(\frac{x}{2})$, см., например, [5, формула (63.10)].

Тождество (4) впервые появилось в работе Стридсберга [18].

2.2. Доказательство теоремы 1.

В доказательстве будет использоваться тождество теоремы 2 с $r = 5$ и еще одно тождество нечетной степени, получающееся из (2) дифференцированием.

Следствие 1. *Для каждого целого $m > 1$ существуют положительные рациональные числа $c_1, \ldots, c_M$, $M = (2m+1)^5$, и целые* *отличные от нуля числа* $a_{i,j}$, $1 \le i \le 5$, $1 \le j \le M$, *такие, что тождественно по переменным* $x_1, \ldots, x_5$ *выполняется равенство*

$$x_1 \left(x_1^2 + \ldots + x_5^2\right)^{m-1} = \sum_{j=1}^{M} c_j \left(a_{1,j} x_1 + \ldots + a_{5,j} x_5\right)^{2m-1}, \qquad (14)$$

Доказательство. Для доказательства достаточно продифференцировать тождество (2) и положить $c_j = b_j a_{1,j}$. □

Для доказательства теоремы 1 будет установлено следующее

Предложение 1. *Для каждого натурального* n *существуют два целых числа* p *и* q *такие, что*

$$n = p + q, \qquad 0 \le p < q,$$

натуральное число K *и положительные рациональные числа* $r_1, \ldots, r_L$ *со следующими свойствами: для любых* $x, y \in \mathbb{Z}, x > 0$, *с условием*

$$|y| \le x^q \qquad (15)$$

существуют целые неотрицательные числа $u_1, \ldots, u_L$ *такие, что*

$$x^p(Kx^q + y) = \sum_{j=1}^{L} r_j u_j^n.$$

Целые числа вида $x^p(Kx^q + y)$ с условием (15) составляют достаточно плотное множество $\mathfrak{M}$. Каждое большое целое число может быть представлено в виде суммы двух чисел из $\mathfrak{M}$. Именно на этом свойстве и основан следующий далее вывод теоремы 1.

Вывод теоремы 1 из предложения 1. Пусть Q – достаточно большое целое число. Обозначим буквой x наибольшее целое число, такое что

$$K(x^n + x^{n+1}) \le Q,$$

и $z = Q - K(x^n + (x+1)^n)$. Тогда

$$0 \le z < K((x+1)^n + (x+2)^n) - K(x^n + (x+1)^n) = K((x+2)^n - x^n) \le x^n,$$

если Q, а, значит, и x достаточно велико. Существуют целые числа y_1, y_2, такие что

$$z = (x+1)^p y_2 - x^p y_1, \qquad 0 \le y_1 < (x+1)^p.$$

Тогда $0 \le y_1 \le x^{p+1} \le x^q$, $y_2 > 0$ и

$$y_2 = \frac{x^p y_1 + z}{(x+1)^p} \le x^p + \frac{z}{(x+1)^p} \le x^p + \frac{x^n}{(x+1)^p} < x^p + x^q < (x+1)^q.$$

Пары чисел (x, y_1) и $(x+1, y_2)$ удовлетворяют условиям предложения 1. Поэтому существуют целые неотрицательные числа $u_1, \dots, u_L$, $v_1, \dots, v_L$, для которых

$$x^p(Kx^q - y_1) = \sum_{j=1}^{L} r_j u_j^n, \qquad (x+1)^p(K(x+1)^q + y_2) = \sum_{j=1}^{L} r_j v_j^n.$$

Но тогда

$$Q = K(x^n + (x+1)^n) + z$$
$$= x^p(Kx^q - y_1) + (x+1)^p(K(x+1)^q + y_2) = \sum_{j=1}^{L} r_j(u_j^n + v_j^n).$$

Пусть $R_0 > 0$ – наименьший общий знаменатель чисел r_j и $r_j = R_j/R_0$. Из доказанного следует, что каждое достаточно большое целое число, делящееся на R_0, может быть представлено в виде суммы $2(R_1 + \dots + R_L)$ слагаемых, каждое из которых есть n-я степень целого числа. Если N достаточно велико, и $N = R_0 Q + T, 0 \le T < R_0$, то T представимо в виде суммы не более чем R_0 единиц. Но тогда число N представимо в виде суммы n-х степеней целых чисел, состоящей не более чем из $R_0 + 2(R_1 + \dots + R_L)$ слагаемых. Это завершает доказательство теоремы 1. $\square$

Перейдем теперь к доказательству предложения 1. Пусть $n \ge 2$ – фиксированное целое число. Определим три числа $a, A, \varkappa$, зависящие от n, следующим образом. Обозначим буквой a наименьшее общее кратное всех чисел $a_{1,1}, \dots, a_{1,M}$ в тождествах (2), (14), написанных для всех $m \le n/2$. Воспользовавшись представлением

$$a_{1,j}x_1 + \dots + a_{5,j}x_5 = \frac{a_{1,j}}{a}(ax_1 + a'_{2,j}x_2 + \dots + a'_{5,j}x_5),$$

где $a'_{i,j} = a_{i,j}\frac{a}{a_{1,j}}$, и подправив коэффициенты b_j, c_j, можно добиться, чтобы в тождествах (2), (14) при всех $m \le n/2$ выполнялись равенства $a_{1,1} = \dots = a_{1,M} = a$. Обозначим теперь

$$A = \max(|a_{2,j}| + \dots + |a_{5,j}|),$$

где максимум берется по всем $j, 1 \le j \le M$, и по всем тождествам (2), (14), при всех $m \le n/2$. Пусть теперь $\varkappa$ – наименьшее целое число, удовлетворяющее неравенству $\varkappa > \frac{6A^2}{a}$ и делящееся на a.

Определим теперь последовательность $K_0, K_1, \dots$ рекуррентно с помощью равенств

$$K_0 = \varkappa^2, \qquad K_r = \left(\frac{K_{r-1} + a\varkappa}{a}\right)^2.$$

Легко видеть, что все K_r есть целые числа, делящиеся на a^2, причем $K_r \ge \varkappa^2$.

Предложение 1 доказывается по индукции. Соответствующее индуктивное утверждение мы сформулируем в следующем виде.

Предложение 2. *Пусть s, n – целые числа, $0 \le s \le \log_2 n$, целые числа u, v определены условиями*

$$n = v \cdot 2^s + u, \qquad 0 \le u < 2^s.$$

Существуют положительные рациональные числа $d_1, \dots, d_Q, Q \le n^{5s}$ такие, что для любых целых чисел x, y с условием

$$|y| \le \varkappa\sqrt{K_s}x^{2^s} \tag{16}$$

найдутся целые неотрицательные числа $w_1, \dots, w_Q$, с которыми выполняется равенство

$$x^u(K_s x^{2^s} + y)^v = \sum_{i=1}^{Q} d_i w_i^n. \tag{17}$$

Вывод предложения 1 из предложения 2. Пусть g – наибольшее целое число с условием $2^g \le n$. Положим в предложении 2 $s = g$. Тогда $v = 1$ и $u = n - 2^g < 2^g$. Если взять $p = u = n - 2^g$ и $q = 2^g$, то из предложения 2 получается предложение 1. $\square$

Обозначим $\mathfrak{M}_s$ совокупность целых чисел, представимых в виде $x^u(K_s x^{2^s} + y)^v$ с целыми x, y, удовлетворяющими условиям (16). В частности, множество $\mathfrak{M}_0$ состоит из n-х степеней целых чисел. Каждый элемент множества $\mathfrak{M}_s$, как это будет видно из доказательства предложения 2, представим в виде суммы ограниченного числа слагаемых из множества $\mathfrak{M}_{s-1}$ с коэффициентами, принадлежащими фиксированному конечному множеству положительных рациональных чисел. Индукция по s обеспечивает выполнимость нужного утверждения. Такова вкратце схема доказательства предложения 2.

Доказательство. Как уже указывалось, предложение 2 будет доказываться индукцией по s. При $s = 0, (u = 0, v = n)$ утверждение, очевидно, выполняется с $Q = 1$, $d_1 = 1$ и $w_1 = K_0x + y \geq 0$.

Предположим, что $s \geq 1$ и для $s-1$ утверждение справедливо. Пусть также целые числа x, y удовлетворяют условию (16).

Определим некоторым специальным образом целые числа $x_1, \dots, x_5$, причем так, чтобы выполняется равенство

$$K_s x^{2^s} + y = x_1^2 + \cdots + x_5^2.$$

Положим $G = K_{s-1}/a$ и $x_1 = Gx^{2^{s-1}}$. Поскольку $K_s = (G + \varkappa)^2$, имеем

$$K_s - G^2 = 2G\varkappa + \varkappa^2 \geq \varkappa\sqrt{K_s}.$$

Следовательно

$$(K_s - G^2)x^{2^s} + y \geq (K_s - G^2)x^{2^s} - \varkappa\sqrt{K_s}x^{2^s} \geq 0,$$

и по теореме Лагранжа существуют целые неотрицательные числа $x_2, \dots, x_5$, удовлетворяющие равенству

$$(K_s - G^2)x^{2^s} + y = x_2^2 + \cdots + x_5^2.$$

Имеем

$$(K_s - G^2) + \varkappa\sqrt{K_s} = 3G\varkappa + 2\varkappa^2 \leq 6\varkappa G. \tag{18}$$

Здесь использовалось неравенство $G = K_{s-1}/a \geq \varkappa^2/a \geq \varkappa$. Из (18) и (16) следует

$$|x_k| \leq \sqrt{6\varkappa G} \cdot x^{2^{s-1}}, \qquad k \geq 2. \tag{19}$$

Возьмем некоторые целые $m \leq n/2$ и $j, 1 \leq j \leq M$. Выбор в дальнейшем j, m и тождества (2) или (14) будет зависеть от u, v. Если $a_{j,i}$ – коэффициенты соответствующих тождеств (2) и (14) положим

$$y_j = a_{j,2}x_2 + \cdots + a_{j,5}x_5.$$

Тогда

$$|y_j| \leq A \cdot \sqrt{6\varkappa G} \cdot x^{2^{s-1}} < \varkappa\sqrt{K_{s-1}} \cdot x^{2^{s-1}}. \tag{20}$$

Последнее неравенство выполняется, поскольку согласно определению $\varkappa$ имеем

$$6\varkappa GA^2 \le a\varkappa^2 G = \varkappa^2 K_{s-1}.$$

Рассмотрим два случая в зависимости от величины числа u.

1. Допустим, что выполнено неравенство $0 \le u < 2^{s-1}$. Воспользуемся тождеством (2) при $r = 5$, $m = v$ и выбранных ранее значениях x_i. Тогда имеем

$$x^u(K_s x^{2^s} + y)^v = x^u(x_1^2 + \cdots + x_5^2)^v = \sum_{j=1}^{M} b_j \cdot x^u(K_{s-1}x^{2^{s-1}} + y_j)^{2v}.$$

Учитывая, что $n = 2v \cdot 2^{s-1} + u, 0 \le u < 2^{s-1}$, согласно индуктивному предположению находим равенства

$$x^u(K_{s-1}x^{2^{s-1}} + y_j)^{2v} = \sum_{i=1}^{Q'} d'_i w_{j,i}^n$$

с некоторыми целыми неотрицательными $w_{j,i}$ и положительными рациональными числами d'_i, зависящими только от n, u, v. Подставляя найденные представления в равенство (20), получаем нужное утверждение.

2. Допустим, что выполнены неравенства $2^{s-1} \le u < 2^s$. Воспользуемся тождеством (14) при $m = v + 1$ и выбранных ранее значениях x_i. Имеем равенство

$$x^u(K_s x^{2^s} + y)^v = x^u(x_1^2 + \cdots + x_5^2)^v$$
$$= \frac{1}{G}\sum_{j=1}^{M} c_j \cdot x^{u-2^{s-1}}(K_{s-1}x^{2^{s-1}} + y_j)^{2v+1}. \qquad (21)$$

Так как $(2v+1)2^{s-1} + (u - 2^{s-1}) = n, 0 \le u - 2^{s-1} < 2^{s-1}$ и каждое слагаемое в правой части (21) удовлетворяет условиям индуктивного предположения, имеем равенство

$$x^{u-2^{s-1}}(K_{s-1}x^{2^{s-1}} + y_j)^{2v+1} = \sum_{i=1}^{Q'} d'_i w_{j,i}^n$$

с некоторыми целыми неотрицательными $w_{j,i}$ и положительными рациональными числами d'_i, зависящими только от n, u, v. Подставляя найденные представления в равенство (21), получаем нужное утверждение. Это завершает доказательство теоремы 1. $\square$

3. Доказательство Линника

Новое элементарное решение проблемы Варинга предложил в 1943 г. Ю. В. Линник, [6], который в то время уже имел докторскую степень, несмотря на свои 28 лет. Пользуясь простыми соображениями Л. Г. Шнирельмана о плотности последовательностей, Линник свел доказательство теоремы 1 к оценке числа решений некоторого диофантова уравнения, теорема 4 ниже. Необходимое утверждение было доказано им с помощью элементарной интерпретации метода Г. Вейля оценки тригонометрических сумм. Подробное изложение доказательства Линника было дано в 1948 г. А. Я. Хинчиным, [3]. В 1956 г. Хуа Ло-ген внес некоторые усовершенствования, см. [14] и [8], позволившие уточнить и упростить доказательство, и изложил его на языке тригонометрических сумм в виде оценки некоторого тригонометрического интеграла. При этом, впрочем, было добавлено, что интеграл используется лишь “ради удобства; не представляет труда провести доказательство средствами элементарной теории чисел”, см. [8], стр. 20. За прошедшие после этого почти 50 лет никто, насколько нам известно, не удосужился выполнить такую работу. Поэтому мы сочли возможным в год 90-летия со дня рождения Ю. В. Линника опубликовать его доказательство с внесенными Хуа Ло-геном усовершенствованиями на элементарном языке оригинала.

3.1. Плотность последовательности. Леммы Шнирельмана.

Содержание этого раздела хорошо известно и приводится здесь для полноты изложения.

Рассмотрим бесконечную возрастающую последовательность целых чисел

$$a_0 = 0, a_1, a_2, \dots . \tag{A}$$

Символом $A(n)$ будет обозначаться количество положительных членов этой последовательности, не превосходящих n. Величина

$$d(A) = \inf_{n\geq 1} \frac{A(n)}{n}$$

называется *плотностью* последовательности A. Для двух последовательностей A и B указанного выше вида символом $A + B$ будет обозначаться последовательность, состоящая из чисел, каждое из которых представимо в виде $a + b$, $a \in A$, $b \in B$. Следующие две леммы принадлежат Л. Г. Шнирельману, см. [9].

Лемма 4. *Если $d(A) \geq \frac{1}{2}$, то $A + A$ есть натуральный ряд.*

Доказательство. Докажем, что произвольно выбранное натуральное число N принадлежит множеству $A + A$. Если $N \in A$, утверждение справедливо. Далее будем считать, что N не принадлежит A. Обозначим буквой B совокупность $a_1, \dots, a_n$ всех положительных членов последовательности A, удовлетворяющих неравенству $a_i \leq N$. Все они отличны от N. Согласно условию $n = A(N) \geq N/2$. Буквой C обозначим совокупность чисел $N - a_i, 1 \leq i \leq n$. Каждое из множеств B и C содержит не менее $N/2$ элементов и все они принадлежат отрезку $[1, N-1]$. Отсюда следует, что множества B и C имеют нетривиальное пересечение, т.е. найдутся элементы a, b, принадлежащие A, для которых $a = N - b$. $\square$

Лемма 5. *Для любых двух последовательностей A, B справедливо неравенство*

$$d(A + B) \geq d(A) + d(B) - d(A)d(B).$$

Доказательство. Если $d(A) = 0$ или $d(B) = 0$, утверждение, очевидно, выполняется. Будем далее считать, что $\alpha = d(A) > 0$ и $\beta = d(B) > 0$. В частности, это означает, что $a_1 = 1$ и $A(m) \geq \alpha m, B(m) \geq \beta m$ при любом $m \geq 1$. Пусть N – натуральное число и n – наибольшее целое с условием $a_n \leq N$. Тогда $n = A(N)$. Обозначим для каждого $k, 1 \leq k < n$ символом i_k наибольший индекс с условием $a_k + b_{i_k} < a_{k+1}$. Пусть также i_n – наибольший индекс с условием $a_n + b_{i_n} \leq N$. Учитывая, что множество $A + B$ содержит элементы $a_k + b_j$, $1 \leq k < n$, $0 \leq j \leq i_k$, все эти элементы различны и не превосходят N, получаем

$$\begin{gathered}(A + B)(N) \geq n + i_1 + \dots + i_n \\ = A(N) + B(a_2 - a_1 - 1) + \dots + B(a_n - a_{n-1} - 1) \\ + B(N - a_n) \geq A(N) + \beta(a_2 - a_1 - 1 + \dots + a_n - a_{n-1} - 1 + N - a_n) \\ = (1 - \beta)A(N) + \beta N \geq (\alpha + \beta - \alpha\beta)N. \quad \square\end{gathered}$$

Приведем также два очевидных следствия лемм 4 и 5.

Следствие 2. *Для любых последовательностей $A_1, \dots, A_r$ справедливо неравенство*

$$1 - d(A_1 + \dots + A_r) \leq (1 - d(A_1)) \cdots (1 - d(A_r)).$$

Следствие 3. *Если $d(A) > 0$, то для некоторого r последовательность $\underbrace{A + \cdots + A}_{r}$ совпадает с множеством целых неотрицательных чисел.*

3.2. Теоремы о числе решений диофантовых уравнений.

Обозначим при фиксированном целом $n \geq 2$ буквой A последовательность чисел

$$A = \{0, 1, 2^n, 3^n, \ldots\},$$

а буквой B последовательность $B = \underbrace{A + \cdots + A}_{r}$. Последовательность A имеет нулевую плотность. Ниже будет доказано, что при некотором r последовательность B будет иметь положительную плотность, что согласно следствию 3 влечет справедливость теоремы 1.

Пусть N неотрицательное целое число. Тогда согласно принятым ранее обозначениям $B(N)$ есть количество целых $m, 0 \leq m \leq N$, для которых уравнение

$$x_1^n + \ldots + x_r^n = m, \qquad x_j \geq 0, \tag{22}$$

разрешимо в целых числах x_j. Обозначим символом $R(m)$ количество решений уравнения (22). С помощью неравенства Коши–Буняковского получаем

$$\left(\sum_{m=0}^{N} R(m)\right)^2 \leq \sum_{m \leq N, R(m) \neq 0} 1 \cdot \sum_{m=0}^{N} R(m)^2. \tag{23}$$

Сумма $\Sigma_1 = \sum_{m=0}^{N} R(m)$ есть количество решений неравенства

$$x_1^n + \cdots + x_r^n \leq N, \qquad x_j \geq 0. \tag{24}$$

Каждый набор целых чисел $x_1, \ldots, x_r$ с условиями $0 \leq x_j \leq (N/r)^{1/n}$ удовлетворяет неравенству (24), поэтому

$$\Sigma_1 \geq (1 + [(N/r)^{1/n}])^r \geq (N/r)^{r/n}$$

и (23) может быть переписано так

$$\left(\frac{N}{r}\right)^{2r/n} \leq B(N) \cdot \sum_{m=0}^{N} R(m)^2. \tag{25}$$

Сумма $\sum\limits_{m=0}^{N} R(m)^2$ есть количество решений системы

$$\begin{cases} x_1^n + \cdots + x_r^n & = y_1^n + \cdots + y_r^n, \\ x_1^n + \cdots + x_r^n & \le N, \quad x_j \ge 0, y_j \ge 0, \end{cases}$$

и не превосходит количества решений системы

$$\begin{cases} x_1^n + \cdots + x_r^n = y_1^n + \cdots + y_r^n, \\ 0 \le x_j \le N^{1/n}, \quad 0 \le y_j \le N^{1/n}. \end{cases} \tag{26}$$

Теорема 3. *Существует натуральное число $r = r(n)$ такое, что при любом натуральном N количество решений системы (26) не превосходит*

$$cN^{\frac{2r}{n}-1},$$

где c – положительная постоянная, зависящая только от r и n.

Из (25) и оценки теоремы 3 следует неравенство $B(N) \ge c_1 N$ с некоторой положительной постоянной, зависящей только от n и r. Таким образом, плотность последовательности B не меньше $c_1 > 0$.

Итак, для доказательства теоремы 1 достаточно установить теорему 3. В свою очередь, последняя теорема может быть выведена из следующего утверждения.

Теорема 4. *Пусть $P \ge 1$ и многочлен $f(x) = a_0x^n + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$ удовлетворяет условиям*

$$n \ge 2, \quad 0 < |a_0| < \lambda, \quad |a_1| \le \lambda P, \ldots, |a_{n-1}| \le \lambda P^{n-1},$$

где λ – достаточно большая по сравнению с n постоянная. Тогда число решений уравнения

$$\sum_{j=1}^{s} (-1)^j f(x_j) = 0, \qquad s = 8^{n-1},$$

в целых числах x_i с условиями $0 \le x_i \le P$ не превосходит $\lambda^{s-3}P^{s-n}$.

Вывод теоремы 3 из теоремы 4. Выберем многочлен $f(x) = x^n$. Положим также $2r = 8^{n-1} = s$, $P = N^{1/n}$. Согласно теореме 4 количество решений уравнения

$$\sum_{j=1}^{2r} (-1)^j x_j^n = 0, \qquad 0 \le x_j \le N^{1/n},$$

не превосходит $\lambda^{s-3}P^{2r-n} = \lambda^{s-3}N^{\frac{2r}{n}-1}$. $\square$

Остаток этого параграфа посвящен доказательству теоремы 4, которое проводится индукцией по степени многочлена $f(x)$ и сходно с методом Г. Вейля оценки тригонометрических сумм. Заметим, что оригинальное доказательство Линника этой теоремы дает значение $s = 2^{4^n}$, см. [3], стр. 35. Значение $s = 8^{n-1}$ получено Хуа Ло-геном.

3.3. Леммы Хуа Ло-гена.

Лемма 6. *Пусть X, Y – действительные числа, удовлетворяющие неравенствам $1 \le X \le Y$ и a – целое число. Количество решений диофантова уравнения*

$$x_1y_1 + x_2y_2 = a \tag{27}$$

при условиях

$$0 < |x_i| \le X, \qquad |y_i| \le Y, \quad i = 1, 2,$$

не превосходит

$$12X^2Y, \quad \textit{при} \quad a = 0,$$
$$40XY\sum_{d|a}\frac{1}{d}, \quad \textit{при} \quad a \ne 0.$$

В последней сумме d пробегает все положительные делители a.

Доказательство. Рассмотрим сначала случай $a = 0$. Тройку (x_1, x_2, y_2), $x_i \ne 0$ можно выбрать

$$2[X] \cdot 2[X] \cdot (2[Y] + 1) \le 12X^2Y$$

способами. Для каждой такой тройки, ввиду условия $x_1 \ne 0$ существует не более одного y_1, удовлетворяющего равенству $x_1y_1 + x_2y_2 = 0$.

Пусть $a \ne 0$. Оценим число решений с условием $|x_2| \le |x_1|$. Все решения (x_1, x_2, y_1, y_2) разобьем на группы с одинаковым значением $d = (x_1, x_2) \ge 1$.

Фиксируем сначала пару взаимно простых чисел x_1, x_2. Тогда для любых двух решений $(y_1', y_2'), (y_1'', y_2'')$ уравнения (27) имеем

$$y_1'' = y_1' + tx_2, \qquad y_2'' = y_2' + tx_1, \quad t \in \mathbb{Z},$$

и

$$|t| = \frac{|y_2'' - y_2'|}{|x_1|} \le \frac{2Y}{|x_1|}.$$

Поскольку $|x_1| \le X \le Y$, количество значений t не превосходит $2\left[\frac{2Y}{|x_1|}\right] + 1 \le 5\frac{Y}{|x_1|}$. Следовательно, количество решений с условиями $(x_1, x_2) = 1, |x_2| \le |x_1|$ не превосходит

$$5 \sum_{1 \le |x_1| \le X} \sum_{1 \le |x_2| \le |x_1|} \frac{Y}{|x_1|} \le 20XY.$$

Число решений с условием $(x_1, x_2) = 1$ и без ограничения $|x_2| \le |x_1|$ может быть оценено сверху величиной $40XY$, а с условием $(x_1, x_2) = d \ge 1$ – величиной $\frac{40}{d}XY$. Суммируя по всем d, получим нужное неравенство.

Лемма 7. *Количество решений уравнения*

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 = 0, \tag{28}$$

при условиях

$$0 < |x_i| \le X, \quad |y_i| \le Y, \quad 1 \le i \le 4, \quad 1 \le X \le Y,$$

не превосходит $c(XY)^3$, где $c = 6 \cdot 10^4$.

Величина константы c в дальнейшем не имеет значения.

Доказательство. Обозначим буквами $q(a)$ и M количества решений уравнений (27) и (28) соответственно при заданных в леммах ограничениях. Тогда

$$M \le \sum_{|k| \le 2XY} q(k)q(-k) \le 144X^4Y^2 + \sum_{1 \le |k| \le 2XY} q(k)q(-k). \tag{29}$$

Согласно лемме 6 получаем

$$\sum_{1 \le |k| \le 2XY} q(k)q(-k) \le 2 \cdot 40^2(XY)^2 \sum_{1 \le k \le 2XY} \left(\sum_{d|k} \frac{1}{d}\right)^2. \tag{30}$$

Для любого $T \geq 1$ находим

$$S = \sum_{1\leq k\leq T}\left(\sum_{d|k}\frac{1}{d}\right)^2 = \sum_{1\leq d_1,d_2\leq T}\frac{1}{d_1 d_2}\sum_{\substack{k:1\leq k\leq T\\ d_1|k,\, d_2|k}} 1$$

$$= \sum_{1\leq d_1,d_2\leq T}\frac{1}{d_1\cdot d_2}\left[\frac{T\cdot(d_1,d_2)}{d_1\cdot d_2}\right] \leq T\sum_{1\leq d_1,d_2\leq T}\frac{(d_1,d_2)}{(d_1 d_2)^2}.$$

Поскольку

$$(d_1,d_2) \leq \min\{d_1,d_2\} \leq \sqrt{d_1 d_2},$$

оценка S может быть продолжена

$$S \leq T\sum_{1\leq d_1,d_2\leq T}\frac{1}{(d_1 d_2)^{3/2}} = T\left(\sum_{1\leq d\leq T}\frac{1}{d^{3/2}}\right)^2 \leq 9T.$$

Получившаяся оценка при $T = 2XY$ и неравенства (29), (30) дают нам

$$M \leq 144X^4Y^2 + 2\cdot 40^2(XY)^2\cdot 9\cdot 2XY \leq 6\cdot 10^4(XY)^3.$$

В 1943 г. Ю. В. Линник вместо леммы 7 использовал следующее утверждение: *пусть $\ell > 2$ и $1 \leq X < Y \leq c_1X^{\ell-1}$, тогда число решений уравнения*

$$x_1y_1 + \cdots + x_\ell y_\ell = 0$$

при условиях $0 < |x_i| \leq X, |y_i| \leq Y, 1 \leq i \leq 4$, не превосходит $c_2(XY)^{\ell-1}$.

Поскольку эту лемму приходится применять при $Y \sim X^{n-1}$, то Линник должен был использовать ее для $\ell = n$. Хуа Ло-ген освободился от условия $Y = O(X^{\ell-1})$, что привело к упрощению доказательства теоремы 3.

3.4. Комбинаторные леммы.

Здесь, следуя Ю. В. Линнику, мы получим оценки числа решений диофантовых уравнений специального вида.

Лемма 8. *Пусть $F(\overline{x}) \in \mathbb{Z}[x_1,\ldots,x_d]$ и A – конечное подмножество $\mathbb{Z}^d$. При любом $k \in \mathbb{Z}$ количество решений уравнения*

$$F(\overline{x}) - F(\overline{y}) = k, \qquad \overline{x},\overline{y} \in A, \tag{31}$$

не превосходит количества решений уравнения

$$F(\overline{x}) - F(\overline{y}) = 0, \qquad \overline{x}, \overline{y} \in A, \tag{32}$$

Доказательствуо. Обозначим $\lambda(a)$ – количество решений уравнения

$$F(\overline{x}) = a, \qquad \overline{x} \in A,$$

пусть также N и M – количества решений уравнений (31) и (32) соответственно. Тогда

$$N = \sum_a \lambda(a) \cdot \lambda(a-k) \le \frac{1}{2} \sum_a (\lambda(a)^2 + \lambda(a-k)^2) = \sum_a \lambda(a)^2 = M. \qquad \square$$

Лемма 9. *Пусть $F(\overline{x}) \in \mathbb{Z}[x_1, \dots, x_d]$, $A_1, \dots, A_{2k}$ – конечные подмножества $\mathbb{Z}^d$ и $N(A_1, \dots, A_{2k})$ – число решений уравнения*

$$\sum_{j=1}^{2k} (-1)^j F(\overline{x}_j) = 0, \qquad \overline{x}_i \in A_i, \quad 1 \le i \le 2k.$$

Существует индекс r такой, что

$$N(A_1, \dots, A_{2k}) \le N(A_r, \dots, A_r).$$

Доказательство. Множество различных наборов $(A_{j_1}, \dots, A_{j_{2k}})$ конечно. Пусть $(B_1, \dots, B_{2k})$ – один из них, удовлетворяющий следующим условиям:

1. $N(B_1, \dots, B_{2k})$ – наибольшее из чисел $N(A_{j_1}, \dots, A_{j_{2k}})$,

2. Среди всех наборов, удовлетворяющих первому условию, набор $(B_1, \dots, B_{2k})$ содержит наименьшее количество различных множеств.

Обозначим буквой q количество различных множеств среди $B_1, \dots, B_{2k}$. Достаточно доказать, что $q = 1$. Предположим, что $q \ge 2$. Разобьем набор $B_1, \dots, B_{2k}$ на две совокупности по k множеств $B_{j_1}, \dots, B_{j_k}$ и $B_{j_{k+1}}, \dots, B_{j_{2k}}$ так, чтобы первая из них содержала не более $q-1$ различных множеств. Это, очевидно, можно сделать.

Для каждого $T \in \mathbb{Z}$ обозначим $\lambda(T)$ и $\mu(T)$ соответственно количества решений уравнений

$$\sum_{\ell=1}^{k} (-1)^{j_\ell} F(\overline{x}_{j_\ell}) = T, \qquad \sum_{\ell=k+1}^{2k} (-1)^{j_\ell} F(\overline{x}_{j_\ell}) = -T$$

при условиях $\overline{x}_j \in B_j, 1 \leq j \leq 2k$. Тогда

$$N(B_1, \dots, B_{2k}) = \sum_T \lambda(T)\mu(T) \leq \frac{1}{2}\sum_T (\lambda(T)^2 + \mu(T)^2). \tag{33}$$

Число $\sum\limits_T \lambda(T)^2$ есть количество решений уравнения

$$\sum_{\ell=1}^{k} (-1)^{j_\ell} F(\overline{x}_{j_\ell}) - \sum_{\ell=1}^{k} (-1)^{j_\ell} F(\overline{y}_{j_\ell}) = 0 \tag{34}$$

при условиях $\overline{x}_{j_\ell}, \overline{y}_{j_\ell} \in B_{j_\ell}$, $1 \leq \ell \leq k$. Среди чисел $(j_1, \dots, j_k, j_1 + 1, \dots, j_k + 1)$ есть k четных и k нечетных. Поэтому

$$\sum_T \lambda(T)^2 = N(B_{i_1}, \dots, B_{i_{2k}}),$$

где все множества B_{i_ℓ} принадлежат первой из определенных выше совокупностей. Сумма $\sum\limits_T \mu(T)^2$ также может быть интерпретирована, как количество решений уравнения, подобного (34). Поэтому из определения совокупности $(B_1, \dots, B_{2k})$ следуют неравенства

$$\sum_T \lambda(T)^2 < N(B_1, \dots, B_{2k}), \quad \sum_T \mu(T)^2 \leq N(B_1, \dots, B_{2k}),$$

противоречащие (33).

3.5. Доказательство теоремы 4.

Пусть n – наименьшее целое число, для которого теорема 4 неверна и $f(x)$ соответствующий многочлен. Положим $t = 8^{n-2} = s/8$.

Уравнение из теоремы 4 можно переписать в виде

$$\sum_{i=1}^{4} (-1)^i \sum_{j=1}^{t} (-1)^j (f(x_{i,t+j}) - f(x_{i,j})) = 0, \qquad 0 \leq x_{i,j} \leq P. \tag{35}$$

Положим в лемме 9 $k = 2t, d = 2, F(x, y) = f(x) - f(y)$,

$$A_0 = \{\,(x, y) \in \mathbb{Z}^2, \quad | \quad 0 \leq x, y \leq P,\ x = y\,\},$$
$$A_1 = \{\,(x, y) \in \mathbb{Z}^2, \quad | \quad 0 \leq x, y \leq P,\ x \neq y\,\}.$$

Существует 2^{4t} векторов вида

$$(\dots, \ell_{j,i}, \dots), \qquad 1 \le i \le 4, \quad 1 \le j \le t, \qquad \ell_{j,i} = \begin{cases} 1, \\ 0. \end{cases}$$

Все решения уравнения (35) разобьем на 2^{4t} классов в соответствии с принадлежностью

$$(x_{i,j}, x_{i,t+j}) \in A_{\ell_{j,i}}, \qquad 1 \le i \le 4, \quad 1 \le j \le t.$$

Согласно лемме 9 существует $r = 0$ или 1 такое, что для любого набора $(i_1, \dots, i_{4t})$ справедливо неравенство

$$N(A_{i_1}, \dots, A_{i_{4t}}) \le N(A_r, \dots, A_r).$$

Имеем равенство

$$N(A_0, \dots, A_0) = ([P] + 1)^{4t},$$

и, если $N(A_1, \dots, A_1) \le N(A_0, \dots, A_0)$, то число решений уравнения из теоремы 4 не превосходит

$$2^{4t}([P] + 1)^{4t} \le 4^{4t} P^{4t} \le \lambda^{s-3} P^{s-n}$$

при $\lambda \ge 4$. Эта оценка соответствует утверждению теоремы 4, поэтому согласно предположению имеем $r = 1$, т.е. нужное число решений не превосходит величины $2^{4t} N(A_1, \dots, A_1)$.

Для того, чтобы оценить сверху $N(A_1, \dots, A_1)$, рассмотрим сначала случай $n = 2$. Тогда $t = 1$ и уравнение (35) можно переписать в виде

$$\sum_{i=1}^{4} (-1)^i (f(y_i) - f(x_i)) = 0, \qquad x_i \ne y_i, \quad 0 \le x_i, y_i \le P. \tag{36}$$

Поскольку

$$f(y) - f(x) = (y - x)(a_0 y + a_0 x + a_1),$$

то уравнение (36) может быть представлено в виде

$$z_1 h_1 - z_2 h_2 + z_3 h_3 - z_4 h_4 = 0, \tag{37}$$

где $h_i = y_i - x_i, z_i = a_0(x_i + y_i) + a_1$. Кроме того, справедливы неравенства

$$0 < |h_i| \le P, \qquad |z_i| \le 3\lambda P. \tag{38}$$

Так как $a_0 \neq 0$, то каждому набору $(z_1, h_1, \dots, z_4, h_4)$, удовлетворяющему (37), (38), соответствует не более одного решения $(x_1, \dots, x_4, y_1, \dots, y_4)$ уравнения (36). Поэтому согласно лемме 7 выполняется оценка

$$N(A_1, \dots, A_1) \leq c(P \cdot 3\lambda P)^3 \leq \lambda^4 P^6, \qquad \lambda > 27c,$$

а число решений уравнения из теоремы 4 оценивается величиной $\lambda^5 P^6$, как и утверждается теоремой.

Итак, выполнено неравенство $n \geq 3$. Перепишем уравнение (35) в виде

$$\sum_{j=1}^{t} (-1)^j \sum_{i=1}^{4} (-1)^i (f(x_{i,t+j}) - f(x_{i,j})) = 0,$$
$$x_{i,t+j} \neq x_{i,j}, \quad 0 \leq x_{i,j} \leq P. \tag{39}$$

Применим опять лемму 9 с $d = 8, k = t/2$ и

$$F(x_1, \dots, x_4, y_1, \dots, y_4) = \sum_{i=1}^{4} (-1)^i (f(y_i) - f(x_i)).$$

Для любого набора целых чисел $\overline{u} = (u_1, \dots, u_4)$ с условием $0 < |u_j| \leq P$ обозначим символом $M(u_1, \dots, u_4)$ множество векторов

$$(x_1, \dots, y_4) \in \mathbb{Z}^8, \qquad 0 \leq x_i, y_i \leq P, \quad y_i - x_i = u_i, \quad 1 \leq i \leq 4.$$

Пусть $\overline{u}_1, \dots, \overline{u}_t$ – произвольный набор векторов $\overline{u}_i = (u_{i,1}, \dots, u_{i,4})$ с условиями $0 < |u_{i,j}| \leq P$. Множество решений уравнения (39) разобьем на классы $K(\overline{u}_1, \dots, \overline{u}_t)$, отнеся в такой класс решения с условием

$$(x_{1,j}, \dots, x_{4,j}, y_{1,j}, \dots, y_{4,j}) \in M(\overline{u}_j), \qquad 1 \leq j \leq t.$$

Согласно лемме 9 существует вектор $\overline{h} = (h_1, \dots, h_4)$, $0 < |h_j| \leq P$ – один из векторов $\overline{u}_1, \dots, \overline{u}_t$ такой, что

$$|K(\overline{u}_1, \dots, \overline{u}_t)| \leq |K(\overline{h}, \dots, \overline{h})|.$$

Имеем

$$N(A_1, \dots, A_1) \leq \sum_{(\overline{u}_1, \dots, \overline{u}_t)} |K(\overline{u}_1, \dots, \overline{u}_t)| \leq \sum_{\overline{h}} r(\overline{h}) \cdot |K(\overline{h}, \dots, \overline{h})|,$$

где $r(\overline{h})$ – количество наборов $(\overline{u}_1, \dots, \overline{u}_t)$, содержащих вектор $\overline{h}$.

Вектор $\overline{h}$ может занимать любую из t позиций в векторе $(\overline{u}_1, \dots, \overline{u}_t)$. Поэтому

$$r(\overline{h}) \le t \cdot (2P)^{4(t-1)} \le \lambda P^{4t-4}$$

и

$$N(A_1, \dots, A_1) \le \lambda P^{4t-4} \sum_{\overline{h}} |K(\overline{h}, \dots, \overline{h})|.$$

Последняя сумма не превосходит числа решений уравнения

$$\sum_{i=1}^{4} (-1)^i \sum_{j=1}^{t} (-1)^j (f(x_{i,j} + h_i) - f(x_{i,j})) = 0 \tag{40}$$

относительно переменных $h_i, x_{i,j}$ при условиях $0 \le x_{i,j} \le P$, $0 < |h_i| \le P$.

Положим при целом $h \ne 0$

$$\varphi_h(x) = \frac{1}{h}(f(x+h) - f(x)), \qquad z_i = \sum_{j=1}^{t} (-1)^j \varphi_{h_i}(x_{i,j}), \quad i = 1, \dots, 4.$$

Тогда уравнение (40) можно переписать в виде

$$z_1 h_1 - z_2 h_2 + z_3 h_3 - z_4 h_4 = 0. \tag{41}$$

Имеем

$$\varphi_h(x) = \frac{1}{h} \sum_{\ell=0}^{n} a_{n-\ell}((x+h)^\ell - x^\ell) = \frac{1}{h} \sum_{\ell=1}^{n} \sum_{i=0}^{\ell-1} a_{n-\ell} \binom{\ell}{i} x^i h^{\ell-i}$$
$$= \sum_{i=0}^{n-1} b_{n-1-i} x^i,$$

где

$$b_{n-1-i} = \sum_{i < \ell \le n} a_{n-\ell} \binom{\ell}{i} h^{\ell-i-1}.$$

Справедливы неравенства

$$|b_{n-1-i}| \le \sum_{i < \ell \le n} \lambda P^{n-\ell} \cdot \binom{\ell}{i} \cdot P^{\ell-i-1} \le 2^n \lambda P^{n-i-1}, \quad 0 \le i \le n-1,$$

$$|z_i| \le t\sum_{i=0}^{n-1} 2^n\lambda P^{n-i-1}\cdot P^i \le \lambda^2 P^{n-1}.$$

Количество решений уравнения (41) при условиях

$$0 < |h_i| \le P, \qquad |z_i| \le \lambda^2 P^{n-1}$$

не превосходит, согласно лемме 7 величины $c(P\cdot\lambda^2 P^{n-1})^3 \le \lambda^7 P^{3n}$. Количество решений уравнения

$$\sum_{j=1}^{t}(-1)^j\varphi_{h_i}(x_{i,j}) = z_i, \qquad 0\le x_{i,j}\le P,$$

не превосходит, в силу леммы 8 числа решений уравнения

$$\sum_{j=1}^{t}(-1)^j\varphi_{h_i}(x_{i,j}) = 0, \qquad 0\le x_{i,j}\le P,$$

а это число, согласно индуктивному предположению, оценивается сверху при достаточно большом λ величиной $(2^n\lambda)^{t-3}(2^n\lambda P)^{t-n+1}$. Таким образом,

$$N(A_1,\ldots,A_1) \le \lambda P^{4t-4}\cdot\lambda^7P^{3n}(\lambda^{t-2}(\lambda P)^{t-n+1})^4 \le \lambda^{s-4}P^{s-n}.$$

Из полученной оценки следует, что число решений уравнения из теоремы 4 оценивается величиной $\lambda^{s-3}P^{s-n}$. Это завершает доказательство теоремы.

Как известно, наибольшее количество слагаемых в проблеме Варинга необходимо для представимости маленьких чисел. Так число 23 нельзя представить в виде суммы менее чем 9 кубов натуральных чисел. В то же время в 1908 г. Э. Ландау, оперируя с алгебраическими тождествами и используя асимптотику для количества простых в прогрессии $3k+2$, доказал, что каждое достаточно большое число представимо в виде суммы не более чем 8 кубов натуральных чисел. В 1942 г. Ю. В. Линник, [7], установил, что для этого достаточно и 7 кубов. Доказательство использовало элементарный подход, основанный на использовании алгебраических тождеств, а также результаты о представимости чисел тернарными квадратичными формами. В 1951 г. Дж. Ватсон, [19], существенно упростил рассуждения Линника. Его доказательство теоремы о 7 кубах выполнено в духе Ландау, но использует асимптотическую формулу для количества простых в прогрессии $ak+b$, $k \le X$, где a может расти как степень $\ln^{100} X$.

Элементарные доказательства Гильберта и Линника дают очень грубые оценки для количества слагаемых в проблеме Варинга. Пусть $G(n)$, как обычно, обозначает наименьшее количество слагаемых, необходимое для представимости всех достаточно больших чисел в виде суммы n-х степеней. Наилучшая в настоящее время при больших n оценка сверху $G(n) \le n \ln n + n \ln\ln n + O(n)$ принадлежит Т. Д. Вооли и была получена им в 1992г. с помощью глубоких аналитических методов, см. [20].

В 1974 г. в совместной работе Ю. В. Линника и Б. М. Бредихина [2] впервые было указано на возможность применения дисперсионного метода Линника для элементарного решения проблемы Варинга. Реализации этой идеи посвящена вышедшая в 1978 г. статья [1], где приводится элементарное решение проблемы Варинга с оценкой $G(n) = O(n \ln n)$.

Литература

1. Б. М. Бредихин и Т. И. Гришина, *Элементарная оценка $G(n)$ в проблеме Варинга, Математические заметки.* — **24**, вып. 1, 7–18.
2. Б. М. Бредихин и Ю. В. Линник, *Новый метод в аналитической теории чисел, в сб. Актуальные проблемы аналитической теории чисел.* Минск (1974), с. 5–22; см. также Ю. В. Линник, *Избранные труды. Теория чисел. L-функции и дисперсионный метод.* Ленинград, Наука (1980), с. 316–332.
3. А. О. Гельфонд и Ю. В. Линник, *Элементарные методы в аналитической теории чисел, гл.* 2. Физматлит, М. (1962).
4. У. Джоунс и В. Трон, *Непрерывные дроби.* Мир, М. (1985).
5. Д. С. Кузнецов, *Специальные функции.* Высшая школа, М. (1965).
6. Ю. В. Линник, *Элементарное решение проблемы Варинга по методу Шнирельмана.* — Мат. сб. **12**, вып. 2 (1943), с. 225–230; см. также Ю. В. Линник, *Избранные труды. Теория чисел, Эргодический метод и L-функции.* Наука, Ленинград (1979), с. 297–303.
7. Ю. В. Линник, *О разложении больших чисел на семь кубов, Мат. сб.* **12**, вып. 2, (1943), с. 218–224; см. также Ю. В. Линник, *Избранные труды. Теория чисел, Эргодический метод и L-функции.* Наука, Ленинград (1979), с. 122–128.
8. Хуа Ло-ген, *Метод тригонометрических сумм и его применения в теории чисел, гл.* 1. Мир, М. (1964).
9. Л. Г. Шнирельман, *Об аддитивных свойствах чисел.* — Ростов на Дону, Известия Донск. политехн. ин-та **14**, 2–3 (1930), с. 3–28; см. также *Über additive Eigenschaften von Zahlen.* — Math. Ann. **107** (1933), 649–690.
10. L. E. Dickson, *History of the theory of numbers*, v. 2. Chelsea, New York (1971).

11. G. Frobenius, *Über den Stridsbergschen Beweis des Waringschen Satzes*, Sitzungsber. Akad. Wiss. Berlin (1912), 666–670.
12. F. Hausdorff, *Zur Hilbertschen Lözung des Waringschen Problems.* — Math. Ann. **Bd. 67** (1909), S. 301–305.
13. D. Hilbert, *Beweis für Darstellbarkeit deer ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Warindsches Problem).* — Math. Ann. Bd. 67 (1909), S. 281–300; русский перевод в "Избранные труды", т. 1, стр. 312–328, Факториал, Москва (1998).
14. Hua Loo Keng, *Introduction to number theory.* Springer, Berlin (1982), § 19.7.
15. A. Hurwitz, *Über die Darstellung der ganzen Zahlen als Summen von* n^{ten} *Potenzen ganzer Zahlen.* — Math. Ann. **65**, No. 3 (1908), 424–427.
16. A. Hurwitz, *Über definite Polynome.* — Math. Ann. **Bd. 73** (1912), 173–176.
17. R. Remak, *Bemerkung zu Herrn Stridsbergs Beweis des Waringschen Theorems.* — Math. Ann. **Bd 72** (1912), 153–156.
18. E. Stridsberg, *Sur la démonstration de M. Hilbert du théorème de Waring.* — Math. Ann. **B. 72**,No. 2 (1912), 145–152.
19. G. L. Watson, *A proof of the seven cube theorem.* — J. London Math. Soc. **26** (1951), p. 153–156.
20. T. D. Wooley, *Large improvements in Waring's problem.* — Ann. Math. **135**, (2), No. 1 (1992), 131–164.
21. H. Davenport, *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, Cambridge University Press, Second edition (2005).

Nesterenko Yu. V. On Waring's problem (elementary methods).

The paper deals with two elementary methods for solving Waring's problem on the representation of numbers as a sum of equal exponents in powers of natural numbers. The first method is an elementary version of the original Hilbert's proof, and the second one simplifies and makes more precise the elementary Linnik's proof based on the estimation of the number of solutions of a certain system of Diophantine equations.

Московский
государственный университет
E-mail: nester@orc.ru

Поступило 15 марта 2005 г.