[14] N. Tchudakoff, *On Goldbach–Vinogradov's theorem*, Ann. of Math. 48 (1947), 515–545.
[15] E. C. Titchmarsh, *Theory of the Riemann Zeta-function* (revised by D. R. Heath-Brown), Oxford 1986.
[16] I. M. Vinogradov, *Special Variants of the Method of Trigonometric Sums* (Russian), Nauka, Moscow 1976.

SCHOOL OF MATHEMATICS
UNIVERSITY OF WALES
COLLEGE OF CARDIFF
MATHEMATICS INSTITUTE
Senghenydd Road
Cardiff CF2 4AG, U.K.

Received on 18.9.1989 (1937)

ACTA ARITHMETICA
LVIII.2 (1991)

О полиномиальных сравнениях

И. Е. Шпарлинский (Москва)

Для натуральных n и q через $\mathfrak{M}_n(q)$ обозначим множество всех многочленов

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$$

с условием $(a_n, \ldots, a_0, q) = 1$, для $f(x) \in \mathbf{Z}[x]$ и натурального P через $\varrho(f, P, q)$ обозначим количество решений сравнения

$$f(x) \equiv 0 \pmod q, \quad 0 \leqslant x \leqslant P-1. \tag{1}$$

Положим

$$N_n(P, q) = \max_{f \in \mathfrak{M}_n(q)} \varrho(f, P, q); \quad N_n(q) = N_n(q, q).$$

Величина $N_n(q)$ исследовалась в ряде работ (см. [1], [5] и ссылки в них). В [1] была получена неулучшаемая оценка

$$N_n(q) \ll q^{1-1/n} \tag{2}$$

(постоянные в символе "$\ll$" здесь и далее зависят только от n и, возможно, $\varepsilon > 0$).

В работе [2], в связи с оценками некоторых тригонометрических сумм, оценивалась величина $N_n(P, q)$ для q равного степени простого числа. В [4] была доказана оценка

$$N_n(P, q) \ll Pq^{-1/n} + q^{1-1/n-\varrho_n+\varepsilon}, \tag{3}$$

где $\varrho_n = (n-1)/n(n^2-n+1)$, нетривиальная при $P \geqslant q^{1-1/n-\varrho_n}$.

Здесь получена оценка, нетривиальная при всех $P \leqslant q$.

Теорема. *При любом $\varepsilon > 0$ справедлива оценка*

$$N_n(P, q) \ll P^{\varepsilon}(P^{1-1/n-\theta_n} + Pq^{-1/n}), \quad \textit{где } \theta_n = (n-1)/n(n^3-n^2+1).$$

Доказательство. Выберем многочлен $f \in \mathfrak{M}_n(q)$, для которого $\varrho(f, P, q) = N_n(P, q)$, и пусть $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_\Omega$ — все простые делители q с учетом кратности. Положим $P_1 = [P/p_1]+1$. Тогда число решений сравнения (1) не превосходит числа решений сравнения

$$f(z + p_1 x) \equiv 0 \pmod q, \quad 0 \leqslant z \leqslant p_1 - 1, \; 0 \leqslant x \leqslant P_1 - 1. \tag{4}$$

Так как $f \in \mathfrak{M}_n(q)$, то для любого целого z имеем

$$(f(z), f^{(1)}(z)/1!, \ldots, f^{(n)}(z)/n!, q) = 1. \tag{5}$$

Из сравнения (4) вытекает, что

$$f(z) \equiv 0 \pmod{p_1}, \quad 0 \leqslant z \leqslant p_1 - 1.$$

Пусть $z_1, \ldots, z_m$ — все корни этого сравнения, $m \leqslant n$. Положим

$$d_v = (f(z), f^{(1)}(z)p_1/1!, \ldots, f^{(n)}(z)p_1^n/n!, q), \quad v = 1, \ldots, m.$$

В силу (5) имеем $p_1 \leqslant d_v \leqslant p_1^n$. Определим многочлены f_v равенствами

$$f_v(x) = f(z_v + p_1 x)/d_v, \quad v = 1, \ldots, m.$$

Ясно, что $f_v \in \mathfrak{M}_n(q/d_v)$, $v = 1, \ldots, m$, следовательно

$$\varrho(f, P, q) \leqslant \sum_{v=1}^{m} N_n(P_1, q/d_v).$$

Обозначая через v_0 номер наибольшего слагаемого в правой части последнего неравенства и полагая $q_1 = q/d_{v_0}$, будем иметь

$$N_n(P, q) \leqslant \varrho(f, P, q) \leqslant nN_n(P_1, q_1),$$

где

$$q/p_1^n \leqslant q_1 \leqslant q/p_1, \quad P_1 = [P/p_1] + 1 \leqslant P/p_1 + 2.$$

Продолжая этот процесс дальше, через $r \leqslant \Omega$ шагов получим неравенство

$$N_n(P, q) \leqslant n^r N_n(P_r, q_r),$$

где

$$q/(p_1 \ldots p_r)^n \leqslant q_r \leqslant q/p_1 \ldots p_r, \quad P_r \leqslant P/p_1 \ldots p_r + 2.$$

В частности, имеем

$$P_r q_r^{-1/n} \leqslant (P/p_1 \ldots p_r + 2) q_r^{-1/n} \ll P/p_1 \ldots p_r q_r^{1/n} + 1 \ll Pq^{-1/n} + 1.$$

Положим

$$t = [\ln q / \ln\ln(q+2)].$$

Если $q_r = 1$ при некотором $r \leqslant t$, то

$$N_n(P, q) \leqslant n^r N_n(P_r, q_r) = n^r P_r \ll q^{\varepsilon}(P/p_1 \ldots p_r + 1).$$

Учитывая, что $1 = q_r \geqslant q/(p_1 \ldots p_r)^n$, получаем

$$N_n(P, q) \ll q^{\varepsilon}(Pq^{-1/n} + 1). \tag{6}$$

Пусть теперь $q_t > 1$. Рассмотрим три случая.

1. Если $q_t \leqslant P_t$, то в силу оценки (2) имеем

$$N_n(P, q) \leqslant n^t N_n(P_t, q_t) = n^t (P_t/q_t + 1) N_n(q_t)$$
$$\leqslant 2n^t P_t q_t^{-1} N_n(q_t) \ll n^t P_t q_t^{-1/n} \ll q^{\varepsilon}(Pq^{-1/n} + 1).$$

2. Если $q_t > P_t \geqslant q_t^{1-\varrho_n}$, то в силу оценки (3) имеем

$$N_n(P, q) \leqslant n^t N_n(P_t, q_t) \ll n^t (P_t q_t^{-1/n+\varepsilon/2} + q_t^{1-1/n-\varrho_n+\varepsilon/2})$$
$$\ll q^{\varepsilon}(Pq^{-1/n} + 1 + P_t^{(1-1/n-\varrho_n)/(1-\varrho_n)})$$
$$\ll q^{\varepsilon}(Pq^{-1/n} + P_t^{(1-1/n-\varrho_n)/(1-\varrho_n)}) \ll q^{\varepsilon}(Pq^{-1/n} + P^{1-1/n-\theta_n}).$$

3. Если $q_t^{1-\varrho_n} \geqslant P_t$, то обозначим через Q минимальный из делителей q_t с условием $P_t \leqslant Q^{1-\varrho_n}$.

Очевидно, что простыми делителями q_t могут быть только $p_{t+1} \geqslant \ldots \geqslant p_\Omega$. Так как $q \geqslant (p_1 \ldots p_t) \geqslant (p_{t+1})^t$, то все простые делители q_t не превосходят $q^{1/t}$. Тогда в силу выбора Q получаем

$$Q \geqslant P_t^{1/(1-\varrho_n)} \geqslant Qq^{-1/t}.$$

В силу (3) имеем

$$N_n(P, q) \leqslant n^t N_n(P_t, q_t) \ll n^t N_n(P_t, Q) \ll n^t (P_t Q^{-1/n} + Q^{1-1/n-\varrho_n+\varepsilon/4})$$
$$\ll q^{\varepsilon/2}(P_t^{1-1/n(1-\varrho_n)} + q^{1/t} P_t^{(1-1/n-\varrho_n)/(1-\varrho_n)})$$
$$\ll q^{\varepsilon} P^{1-1/n(1-\varrho_n)} = q^{\varepsilon} P^{1-1/n-\theta_n}.$$

Таким образом, в любом случае имеем

$$N_n(P, q) \ll q^{\varepsilon}(P^{1-1/n-\theta_n} + Pq^{-1/n}).$$

Для завершения доказательства теоремы осталось показать, что q^{ε} можно заменить на P^{ε}. При $P \geqslant q^{1/(n+1)}$ это очевидно. Покажем, что при $P < q^{1/(n+1)}$ справедлива более сильная оценка

$$N_n(P, q) \ll Pq^{-2/n(n+1)} + 1. \tag{7}$$

Пусть $f \in \mathfrak{M}_n(q)$. Положим $T = [q^{2/n(n+1)}] - 1$. Для доказательства оценки (7) достаточно доказать, что при любом целом M число решений сравнения

$$f(M + x) \equiv 0 \pmod{q}, \quad 0 \leqslant x \leqslant T - 1,$$

не превосходит n.

Предположим противное, пусть $0 \leqslant x_1 \leqslant \ldots \leqslant x_{n+1} \leqslant T - 1$ — попарно различные решения этого сравнения. Тогда

$$\sum_{v=0}^{n} x_i^v f^{(v)}(M)/v! \equiv 0 \pmod{q}, \quad i = 1, \ldots, n+1.$$

Так как $f \in \mathfrak{M}_n(q)$, то, очевидно, имеем

$$(f(M), f^{(1)}(M)/1!, \ldots, f^{(n)}(M)/n!, q) = 1.$$

Следовательно система сравнений

$$\sum_{\nu=0}^{n} x_i^{\nu} u_i \equiv 0 \pmod{q}, \quad i = 1, \ldots, n+1,$$

имеет решение с условием $(u_0, u_1, \ldots, u_n, q) = 1$. Отсюда вытекает, что ее определитель Δ делится на q. Учитывая, что

$$0 < \Delta \leqslant \prod_{1 \leqslant i < j \leqslant n+1} (x_j - x_i) \leqslant T^{n(n+1)/2} < q,$$

получаем противоречие. Тем самым оценка (7), а вместе с ней и теорема, доказаны.

В заключение заметим, что для $\Omega(q)$ – количества простых делителей q с учетом кратности, для почти всех в смысле асимптотической плотности натуральных q справедлива оценка

$$\Omega(q) \leqslant 10 \ln\ln q$$

(см. [3]). Отсюда вытекает, что для почти всех натуральных q выполнена оценка (6).

Литература

[1] С. В. Конягин, *О числе решений сравнения n-й степени с одним неизвестным*, Мат. сб. 102 (2) (1979), 171–187.

[2] Н. М. Коробов, *Двойные тригонометрические суммы и их приложения к оценке рациональных сумм*, Мат. заметки 6 (1) (1969), 25–34.

[3] Ю. В. Линник, *Дисперсионный метод в бинарных аддитивных задачах*, Изд. Ленинградского гос. ун.-та, 1961.

[4] Д. А. Митькин, *Об оценках и асимптотических формулах для рациональных тригонометрических сумм, близких к полным*, Мат. сб. 122 (4) (1983), 527–545.

[5] С. Б. Стечкин, *Оценка полной рациональной тригонометрической суммы*, Труды Мат. ин-та АН СССР 143 (1977), 188–207.

СССР 119 285
Москва
Мосфильмовская ул., д2, корп. В, кв. 41

Поступило 28.9.1989
и в исправленной форме 29.3.1990 (1970)

ACTA ARITHMETICA
LVIII.2 (1991)

An improvement of Lenstra's criterion for euclidean number fields: The totally real case

by

GERHARD NIKLASCH (München) and ROLAND QUÊME (Breuillet)

1. Introduction. By a theorem of H. W. Lenstra jr. [Le 77], an algebraic number field is euclidean for the norm provided that it contains a sufficiently long "exceptional sequence" of elements whose pairwise differences are units. More precisely, the length must exceed the square root of the discriminant times a (number-geometric) coefficient depending on the signature of the field. We show that a modification of Lenstra's argument leads, for totally real fields, to significantly smaller coefficients, and present seven new euclidean number fields thus obtained. (The totally real case is the hardest to handle because the field discriminants are comparatively large.)

More than 600 euclidean number fields are known; see [Le 80], [LM 82], [LN 87] and the references there. The majority of these was found with the help of Lenstra's criterion, originally formulated in [Le 74, Section 14], and published in its final form in the celebrated *Inventiones* article [Le 77]. [Le 80] provides a very readable survey of the topic.

In order to state the criterion, we need to fix a few notions and notations. Let K be an algebraic number field and R its ring of (algebraic) integers. Let N denote the absolute norm, defined on R by $N(0) = 0$, $N(\alpha) = \#(R/\alpha R)$ for $\alpha \in R \setminus \{0\}$, and extended to K by multiplicativity. R (or K, by a traditional abuse of language) is called *euclidean* (*for the norm*) if for any $\alpha, \beta \in R$ with $\beta \neq 0$ we can find $\kappa, \varrho \in R$ such that $\alpha = \kappa\beta + \varrho$ and $N(\varrho) < N(\beta)$. Equivalently, for each $\xi \in K$ we need to find $\kappa \in R$ such that $N(\xi - \kappa) < 1$.

DEFINITION. An *exceptional sequence of length* m in K is a subset

$$\{\omega_1, \ldots, \omega_m\} \subset K$$

such that each difference $\omega_i - \omega_j$ $(1 \leqslant i < j \leqslant m)$ is an invertible element of R (i.e., a Dirichlet unit in K).

THEOREM 1 [Le 77]. *There are positive constants $\alpha = \alpha(r, s)$, such that every number field K with discriminant D, with r real and s complex places, and containing an exceptional sequence of length $m > \alpha(r, s) \cdot \sqrt{|D|}$ is euclidean for the norm.*