Доклады Академии наук СССР
1971. Том 196, № 4

УДК 511

МАТЕМАТИКА

А. А. КАРАЦУБА

РАСПРЕДЕЛЕНИЕ СТЕПЕННЫХ ВЫЧЕТОВ И НЕВЫЧЕТОВ В АДДИТИВНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ

(Представлено академиком И. М. Виноградовым 3 VII 1970)

Обозначения. q — простое число, χ — неглавный характер mod q; P — множество простых чисел; p — простое число, т. е. $p \in P$; U — произвольное множество целых положительных чисел, u — элемент U, т. е. $u \in U$; $g(x) = g(x; U)$ — количество чисел $u \in U$ таких, что $u \leqslant x$; k — целое положительное число; $\nu = 1/k$; $\varepsilon_0 > 0$ — сколь угодно малое фиксированное число; $\varepsilon > 0$ — сколь угодно малое число, не всегда одно и то же; $c_1, c_2, \ldots$ — положительные абсолютные константы; кроме введенных, будем пользоваться также общепринятыми теоретико-числовыми обозначениями.

Под аддитивной последовательностью мы понимаем некоторую последовательность натуральных чисел C, которая является суммою двух других последовательностей натуральных чисел A и B, т. е. для любого $c \in C$ существуют $a \in A$ и $b \in B$ такие, что $c = a + b$, и, наоборот, $a + b \in C$ при любых $a \in A$ и $b \in B$. Мы будем заниматься проблемой распределения степенных вычетов и невычетов в аддитивных последовательностях $C = A + B$, причем $A = P$ и $B = U$. В работе (1) изучалась аналогичная проблема в случае, когда U, грубо говоря, состояло из одного числа; рассмотрение густых множеств U дает возможность получить более тонкие результаты, именно, удается не тривиально оценить значительно более короткие суммы характеров, что позволяет, в свою очередь, получить соответствующие результаты в теории степенных вычетов и невычетов и др.

Следует отметить, что арифметическая природа чисел $u \in U$ ниже не используется совсем; основной характеристикой множества U, которая только и используется, является функция $g(x) = g(x; U)$.

Основной теоремой статьи является теорема 1 об оценке суммы значений неглавного характера mod q. Все другие теоремы являются следствием этой основной теоремы. Мы существенно пользуемся цитированной выше работой автора (1). Схема доказательства теоремы 1 совпадает со схемой доказательства основной теоремы из (1); основную трудность при доказательстве доставляют длинные суммы по сплошному интервалу суммирования; эта трудность обходится с помощью леммы.

Лемма. *Пусть* ω — *число решений уравнения*

$$xy(ay_1 + z) = x_1y_1(ay + z_1),$$

$$1 \leqslant x,\ x_1 \leqslant X,\quad 1 \leqslant y,\ y_1 \leqslant Y,\quad 1 \leqslant z,\ z_1 \leqslant Z,\quad 0 \leqslant a \leqslant XYZ,$$

в целых числах x, y, z, x_1, y_1, z_1 (a — *фиксированное целое число*). *Тогда для* ω *имеет место оценка*

$$\omega \leqslant c_1(XYZ)^{1+\varepsilon}.$$

Доказательство. При фиксированных x_1, y_1, z_1 для величины ω получаем неравенство

$$\omega \leqslant XYZ\omega_1,$$

где ω_1 — максимальное по x_1, y_1, z_1 число решений уравнения

$$n = y(x(m+z)-r),$$

причем $n = x_1y_1z_1$, $m = ay_1$, $r = ax_1y_1$. Далее имеем

$$\omega_1 \leqslant n^{\varepsilon}\omega_2 \leqslant (XYZ)^{\varepsilon}\omega_2,$$

где ω_2 — максимальное по n_1, $1 \leqslant n_1 \leqslant aXY + XZ$, число решений уравнения

$$n_1 = x(m+z)-r.$$

Следовательно, $\omega_2 \leqslant (XYZ)^{\varepsilon}$. Из полученных оценок величин ω, ω_1, ω_2 следует утверждение леммы.

Теорема 1. *Рассмотрим сумму*

$$S = S(N, M) = \sum_{p \leqslant N} \sum_{u \leqslant M} \chi(p+u),$$

где $p \in P$, $u \in U$, *а числа* N *и* M *такие, что*

$$1 \leqslant MN < q.$$

При любом $k \geqslant \ln q / \ln N$ *для* S *справедлива оценка*

$$S \ll \pi(N)\, g(M) \cdot \Delta, \quad \Delta = \left(\frac{q^{0,5+0,5\nu}}{Ng(M)}\right)^{\gamma\nu},$$

где $\gamma > 0$ — *абсолютная константа, а постоянная в знаке* $\ll$ *зависит только от* $\nu = 1/k$.

Теорема 2. *При любом* $k \geqslant \min(\ln q / \ln N,\ \ln q / \ln M)$ *справедлива оценка*

$$S^* = S^*(N, M) = \sum_{p \leqslant N} \sum_{p' \leqslant M} \chi(p+p') \ll \pi(N)\,\pi(M) \cdot \Delta,$$

$$\Delta = (q^{0,5+0,5\nu}/NM)^{\gamma\nu},$$

где p, $p' \in P$, $\gamma > 0$ — *абсолютная константа, а постоянная в знаке* $\ll$ *зависит только от* $\nu = 1/k$.

Теорема 3. *Пусть* $N \geqslant q^{0,25+\varepsilon_0}$, $M \geqslant q^{0,25+\varepsilon_0}$; *тогда*

$$S^* = S^*(N, M) = \sum_{p \leqslant N} \sum_{p' \leqslant M} \chi(p+p') \ll \pi(N)\,\pi(M)\, q^{-\gamma_0\varepsilon_0^2},$$

где $\gamma_0 > 0$ — *асболютная константа, а постоянная в знаке* $\ll$ *зависит только от* ε_0.

Следствие. *Существует* $q_0 = q_0(\varepsilon_0)$ *такое, что при* $q \geqslant q_0$ *на отрезке* $[1,\ q^{0,25+\varepsilon_0}]$ *содержится* $c_2 q^{0,25+\varepsilon_0}$ *и* $c_3 q^{0,25+\varepsilon_0}$ *соответственно квадратичных вычета и квадратичных невычета* $\bmod q$ *вида* $p+p'$, *где* p *и* p' — *простые числа.*

Аналогично формулируются утверждения о вычетах и невычетах произвольной степени, а также о первообразных корнях, имеющих вид $p+p'$.

Математический институт
им. В. А. Стеклова
Академии наук СССР
Москва

Поступило
23 VI 1970

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] А. А. Карацуба. Изв. АН СССР, сер. матем., **34**, 299 (1970).