Э. К. Жимбо, В. Н. Чубариков, О распределении арифметических функций по простому модулю, *Дискрет. матем.*, 2001, том 13, выпуск 3, 32–41

DOI: 10.4213/dm292

Дискретная математика

том 13 выпуск 3 * 2001

УДК 511.37

О распределении арифметических функций по простому модулю

© 2001 г. Э. К. Жимбо, В. Н. Чубариков

В статье рассматриваются задачи, связанные с распределением значений аналогов неполных сумм Клостермана по простому модулю и их обобщений, совместному распределению квадратичных вычетов и невычетов по разным простым модулям.

1. Введение

В настоящей работе рассматриваются задачи, которые связаны с распределением значений аналогов неполных сумм Клостермана по простому модулю и их обобщений, совместному распределению квадратичных вычетов и невычетов по разным простым модулям.

Близкой к рассматриваемым задачам является проблема И. М. Виноградова о нахождении порядка величины наименьшего квадратичного невычета по простому модулю [1–3]. Исследования И. М. Виноградова были продолжены Давенпортом и Эрдешем [4] и Берджессом [5]. В 90-е годы А. А. Карацуба [6–8] получил нетривиальные оценки аналогов неполных сумм Клостермана с весьма короткой длиной промежутка суммирования.

Другой аспект данной проблематики связан с использованием предельных теорем теории вероятностей [4, 9, 11].

Здесь мы существенно пользуемся результатами и методами работ [1–11]. Ранее первым автором (Э. К. Жимбо) был найден закон распределения значений квадрата модуля неполных сумм Гаусса по простому модулю [12].

Обозначим через $N_p\{\cdot\}$ количество натуральных чисел $1 \leqslant x \leqslant p$, удовлетворяющих условиям, которые указываются в фигурных скобках.

В параграфе 2, основываясь на лемме 1, которая по существу принадлежит А. А. Карацубе, доказываются следующие утверждения.

Теорема 1. *Пусть p — простое число, $h < p$ и x — натуральное число. Пусть*

$$S_p(x;h) = \sum_{q \leqslant h} e^{2\pi i x q^*/p},$$

где суммирование ведется по простым числам q и q^* определяется из сравнения

$$qq^* \equiv 1 \pmod{p}.$$

Тогда при $p \to \infty$, $h = h(p) \to \infty$, $\log h / \log p \to \infty$ *величина*

$$\xi = \left| \frac{S_p(x;h)}{\sqrt{h}} \right|^2$$

асимптотически имеет показательное распределение с параметром 1, *то есть при любом фиксированном* $y > 0$

$$\lim_{p\to\infty} \frac{1}{p} N_p\{\xi < y\} = \int_0^y e^{-y} dy.$$

Теорема 2. *Если в условиях теоремы* 1 *вместо суммы* $S_p(x;h)$ *рассмотреть сумму*

$$S_p(a,b;h) = \sum_{q \leqslant h} \varepsilon(q) e^{2\pi i (aq + bq^*)/p},$$

где суммирование ведется по простым числам q, $|\varepsilon(q)| = 1$ *для любого простого* q, *то величина*

$$\xi = \xi(a,b) = \left| \frac{S_p(a,b;h)}{\sqrt{h}} \right|^2$$

асимптотически имеет показательное распределение с параметром 1.

В параграфе 4 с использованием свойств сумм Гаусса (лемма 1) и метода Виноградова [1] получена асимптотическая формула для количества квадратичных вычетов и невычетов в некоторых последовательностях по разным модулям. Точнее, имеет место следующее утверждение.

Теорема 3. *Пусть* $p_1, \dots, p_k$ — *простые числа,* $p_s \neq p_r$ *при* $s \neq r$, $1 \leqslant s, r \leqslant k$, $x + 1 \leqslant n \leqslant x + h$, $\varepsilon_s = \pm 1$ *при* $1 \leqslant s \leqslant k$, *и пусть* T — *количество значений* n, *удовлетворяющих соотношениям*

$$\left(\frac{n + a_1}{p_1}\right) = \varepsilon_1, \dots, \left(\frac{n + a_k}{p_k}\right) = \varepsilon_k.$$

Тогда

$$T = \frac{h}{2^k} + \theta \sqrt{Q} \ln Q,$$

где $Q = p_1 \dots p_k$, $|\theta| \leqslant 1$ *и* $h > 2^k \sqrt{Q}$.

Наконец, в параграфе 5 получен аналог центральной предельной теоремы теории вероятностей для распределения значений сумм символов Лежандра по разным модулям.

Теорема 4. *Пусть* a — *положительная постоянная,* $p_1, \dots, p_s$ — *простые числа,* $s \leqslant a$, $Q = p_1 \dots p_s$, *и пусть*

$$S_h(x) = S_h(x; p_1, \dots, p_s) = \sum_{n=x+1}^{x+h} \left(\frac{n + a_1}{p_1}\right) \dots \left(\frac{n + a_s}{p_s}\right).$$

Тогда при $Q \to \infty$, $h = h(Q) \to \infty$, $\log h / \log Q \to \infty$ *величина*

$$\xi_Q = \frac{S_h(x)}{\sqrt{h}}$$

имеет асимптотически стандартное нормальное распределение.

2. О распределении значений аналогов неполных сумм Клостермана

Доказательство теоремы 1. Пусть p — простое число, $h < p$ и x — натуральное число. Рассмотрим сумму

$$S_p(x;h) = \sum_{q \leqslant h} e^{2\pi i x q^*/p},$$

где суммирование ведется по простым числам q и q^* определяется из сравнения

$$qq^* \equiv 1 \pmod p.$$

Для того чтобы в дальнейшем проводить теоретико-вероятностную аналогию, положим

$$\xi = \xi_p(x) = \left|\frac{S_p(x)}{\sqrt{h}}\right|^2 = \frac{|S_p(x)|^2}{h},$$

и предположим, что любое x с условием $1 \leqslant x \leqslant p$ принимается с одинаковой вероятностью $1/p$. Тогда момент порядка r случайной величины $\xi_p(x)$ будет равен

$$\mathsf{M}\xi_p^r = A_p(r) = \frac{1}{p}\sum_{x=1}^{p} \xi_p^r(x) = \frac{1}{ph^r}\sum_{x=1}^{p}\left|\sum_{q\leqslant h} e^{2\pi i x q^*/p}\right|^{2r}.$$

Обозначим через $T(h) = T_p(h)$ число решений сравнения

$$q_1^* + \ldots + q_r^* - q_{r+1}^* - \ldots - q_{2r}^* \equiv 0 \pmod p.$$

Ясно что

$$A_p(r) = \frac{1}{ph^r}\sum_{1\leqslant q_1,\ldots,q_{2r}\leqslant h}\sum_{x=1}^{p} e^{2\pi i x(q_1^*+\ldots+q_r^*-q_{r+1}^*-\ldots-q_{2r}^*)/p} = h^{-r}T(h).$$

Здесь мы воспользовались тем, что

$$\frac{1}{p}\sum_{x=1}^{p} e^{2\pi i x m/p} = \begin{cases} 1, & \text{если } m \equiv 0 \pmod p, \\ 0, & \text{если } m \not\equiv 0 \pmod p. \end{cases}$$

Найдем асимптотическую формулу для величины $T(h)$ при $h < p$ и $h \to \infty$. Справедливо следующее утверждение.

Лемма 1. *Пусть $q_1, \ldots, q_r, q_{r+1}, \ldots, q_{2r}$ — простые числа, не превосходящие h, и $h^{2r-1} < (2r)^{-1}p$. Тогда для числа $T(h) = T_p(h)$ решений сравнения*

$$q_1^* + \ldots + q_r^* - q_{r+1}^* - \ldots - q_{2r}^* \equiv 0 \pmod p \tag{1}$$

при $h \to \infty$ имеет место асимптотическая формула

$$T(h) = r!\,h^r + O(h^{r-1}).$$

Доказательство. Домножив сравнение (1) на

$$Q = q_1 \dots q_r q_{r+1} \dots q_{2r} \not\equiv 0 \pmod{p},$$

получим сравнение

$$q_2 \dots q_r q_{r+1} \dots q_{2r} + \dots + q_1 \dots q_{r-1} q_{r+1} \dots q_{2r} - q_1 \dots q_{r+1} q_{r+2} \dots q_{2r} - \dots - q_1 \dots q_r q_{r+1} \dots q_{2r-1} \equiv 0 \pmod{p}.$$

Поскольку каждое слагаемое в этом сравнении меньше, чем $p/(2r)$, оно будет уравнением

$$\frac{Q}{q_1} + \dots + \frac{Q}{q_r} - \frac{Q}{q_{r+1}} - \dots - \frac{Q}{q_{2r}} = 0. \tag{2}$$

Наборы $(q_{r+1}, \dots, q_{2r})$, которые являются перестановкой наборов $(q_1, \dots, q_r)$, являются решениями последнего уравнения. Их количество T_1 выражается формулой

$$T_1 = r!\, h^r + O(h^{r-1}).$$

Оценим сверху число решений $(q_1, \dots, q_r, q_{r+1}, \dots, q_{2r})$, для которых $(q_{r+1}, \dots, q_{2r})$ не является перестановкой набора $(q_1, \dots, q_r)$. Без ограничения общности можно считать, что $q_1 \leqslant \dots \leqslant q_r$ и $q_{r+1} \leqslant \dots \leqslant q_{2r}$.

Пусть q — максимальное из чисел q_s и q_{r+s} такое, что

$$q_{2r} = q_r, \dots, q_{r+s+1} = q_{s+1}, q_{r+s} \neq q_s.$$

Тогда уравнение (2) можно переписать в виде

$$\frac{Q}{q_1} + \dots + \frac{Q}{q_s} = \frac{Q}{q_{r+1}} + \dots + \frac{Q}{q_{r+s}}. \tag{3}$$

Рассмотрим две возможности: $q > r$ и $q \leqslant r$.

В первом случае все слагаемые в (3), кроме $q_m = q$, делятся на q. Заметим также, что все слагаемые, отвечающие $q_m = q$, находятся только в одной части равенства (3). Следовательно, для того чтобы выполнялось равенство (3) необходимо, чтобы количество слагаемых, отвечающих $q_m = q$, делилось на q. Отсюда следует, что это количество не меньше $q > r$. Но так как в одной стороне равенства находится ровно r слагаемых, случай не имеет места.

Рассмотрим теперь случай $q \leqslant r$. В этом случае $s \geqslant 1$ и уравнение (3) имеет не более r^{2s} решений. Отсюда следует, что уравнению (2) удовлетворяют не более $r^{2s} h^{r-s} < h^{r-1}$ наборов. Лемма доказана.

Продолжим доказательство теоремы 1. Для любого фиксированного r при $p \to \infty$

$$h \to \infty, \qquad \frac{\log h}{\log p} \to 0,$$

следовательно, при $p \to \infty$

$$A_p(r) \to r!\,.$$

Поэтому предельное распределение ξ_p — это показательное распределение, поскольку его момент порядка $r \geqslant 1$ равен $r!$. Теорема 1 доказана.

3. О распределении значений обобщенных неполных сумм Клостермана

Доказательство теоремы 2. Пусть, как и прежде, p — простое число, $h < p$ и a, b — натуральные числа. Рассмотрим сумму

$$S_p(a,b;h) = \sum_{q \leqslant h} \varepsilon(q) e^{p\pi i(aq+bq^*)/p},$$

где суммирование ведется по простым числам q, $|\varepsilon(q)| = 1$ для любого простого q. Такие суммы мы будем называть обобщенными неполными суммами Клостермана.

Пусть

$$\xi = \xi_p(a,b) = \left| \frac{S_p(a,b;h)}{\sqrt{h}} \right|^2 = \frac{|S_p(a,b;h)|^2}{h}.$$

Предположим, что любой набор (a,b) с условием $1 \leqslant a,b \leqslant p$ принимается с одинаковой вероятностью $1/p^2$. Тогда момент порядка r случайной величины $\xi_p(a,b)$ будет равен

$$\begin{aligned} A_p(r) &= \frac{1}{p^2 h^r} \sum_{a=1}^{p} \sum_{b=1}^{p} \left| \sum_{q \leqslant h} \varepsilon(q) e^{2\pi i(aq+bq^*)/p} \right|^{2r} \\ &= \frac{1}{p^2 h^r} \sum_{1 \leqslant q_1,\ldots,q_{2r} \leqslant h} \varepsilon(q_1)\ldots\varepsilon(q_r)\bar{\varepsilon}(q_{r+1})\ldots\bar{\varepsilon}(q_{2r}) \\ &\quad \cdot \times \sum_{a=1}^{p} e^{2\pi i a(q_1+\ldots+q_r-q_{r+1}-\ldots-q_{2r})/p} \sum_{b=1}^{p} e^{2\pi i b(q_1^*+\ldots+q_r^*-q_{r+1}^*-\ldots-q_{2r}^*)/p} \\ &= h^{-r} T(h;a,b), \end{aligned}$$

где $T(h;a,b)$ — количество решений системы сравнений

$$\begin{aligned} q_1 + \ldots + q_r - q_{r+1} - \ldots - q_{2r} &\equiv 0 \pmod p, \\ q_1^* + \ldots + q_r^* - q_{r+1}^* - \ldots - q_{2r}^* &\equiv 0 \pmod p. \end{aligned}$$

Отбросив первое сравнение этой системы и воспользовавшись леммой 1, получим, что

$$A_p(r) = r! + O(h^{-1}).$$

Отсюда, переходя к пределу при $p \to \infty$, находим, что

$$A_p(r) \to r!.$$

Поэтому величина $\xi_p = |S_p(a,b;h)/\sqrt{h}|^2$ имеет показательное распределение с параметром λ, равным 1. Теорема 2 доказана.

4. Оценка арифметических сумм в классах вычетов по различным модулям

Лемма 2. *Пусть a — целое число,*

$$U_{a,p} = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i a x/p}.$$

Тогда

$$\left(\frac{a}{p}\right) = \frac{U_{a,p}}{U_{1,p}},$$

а при $(a,p)=1$

$$|U_{a,p}| = \sqrt{p}.$$

Доказательство см. [3], стр. 80–81, вопрос 11а.

Лемма 3. *Пусть* $p_1,\dots,p_s$ *— различные простые числа,* $Q = p_1\dots p_s$ *и* $a_1,\dots,a_s$ *— произвольные целые числа. Тогда для суммы*

$$S = \sum_{n=x+1}^{x+h} \left(\frac{n+a_1}{p_1}\right)\dots\left(\frac{n+a_s}{p_s}\right)$$

справедлива оценка

$$|S| \leqslant \sqrt{Q}\log Q.$$

Доказательство. По лемме 2 для суммы Гаусса при некотором ε_{p_j}, $|\varepsilon_{p_j}| = 1$, справедливо равенство

$$\left(\frac{n+a_j}{p_j}\right) = \frac{\varepsilon_{p_j}}{\sqrt{p_j}} \sum_{m \leqslant p_j} \left(\frac{m}{p_j}\right) e^{-2\pi i m(n+a_j)/p_j}, \qquad j = 1,\dots,s,$$

поэтому

$$\begin{aligned} S &= \sum_{n=x+1}^{x+h} \frac{\varepsilon_{p_1}}{\sqrt{p_1}} \sum_{m_1=1}^{p_1-1} \left(\frac{m_1}{p_1}\right) e^{-2\pi i m_1(n+a)/p_1} \dots \frac{\varepsilon_{p_s}}{\sqrt{p_s}} \sum_{m_s=1}^{p_s-1} \left(\frac{m_s}{p_s}\right) e^{-2\pi i m_s(n+a_s)/p_s} \\ &= \frac{\varepsilon_{p_1}\dots\varepsilon_{p_s}}{\sqrt{p_1\dots p_s}} \sum_{m_1=1}^{p_1-1} \left(\frac{m_1}{p_1}\right) e^{-2\pi i m_1(n+a_1)/p_1} \dots \sum_{m_s=1}^{p_s-1} \left(\frac{m_s}{p_s}\right) e^{-2\pi i m_s(n+a_s)/p_s} \\ &\quad \times \sum_{n=x+1}^{x+h} e^{-2\pi i n(m_1/p_1+\dots+m_s/p_s)}. \end{aligned}$$

Отсюда следует оценка

$$\begin{aligned} |S| &\leqslant \frac{1}{\sqrt{Q}} \sum_{m_1=1}^{p_1-1} \dots \sum_{m_s=1}^{p_s-1} \left| \sum_{n=x+1}^{x+h} e^{2\pi i n(m_1/p_1+\dots+m_s/p_s)} \right| \\ &= \frac{1}{\sqrt{Q}} \sum_{1 \leqslant l \leqslant Q}{}' \left| \sum_{n=x+1}^{x+h} e^{2\pi i n l/Q} \right| = T, \end{aligned}$$

где штрих в знаке суммы означает суммирование по l, $1 \leqslant l \leqslant Q$, взаимно простым с Q.

Здесь мы воспользовались тем, что если m_r, $1 \leqslant r \leqslant s$, пробегает приведенную систему вычетов по модулю p_r и

$$\frac{m_1}{p_1} + \dots + \frac{m_s}{p_s} = \frac{l}{Q}, \qquad Q = p_1\dots p_s,$$

то l пробегает полную систему вычетов по модулю Q.

Далее, находим, что

$$|T| \leqslant \frac{2}{\sqrt{Q}} \sum_{0 \leqslant l \leqslant \frac{Q}{2}}{}' \left| \frac{e^{2\pi i l/Q} - e^{2\pi i l(h+1)/Q}}{1 - e^{2\pi i l/Q}} \right|$$

$$= \frac{2}{\sqrt{Q}} \sum_{0 \leqslant l \leqslant Q/2}{}' \left| \frac{\sin(\pi l h/Q)}{\sin(\pi l/Q)} \right| \leqslant \frac{1}{\sqrt{Q}} \sum_{0 \leqslant l \leqslant Q/2}{}' \frac{Q}{l} < \sqrt{Q} \log Q.$$

Лемма 3 доказана.

Доказательство теоремы 3. Очевидно, что

$$\frac{1}{2^k} \left(1 - \varepsilon_1 \left(\frac{n+a_1}{p_1}\right)\right) \dots \left(1 - \varepsilon_k \left(\frac{n+a_k}{p_k}\right)\right)$$

$$= \begin{cases} 1, & \text{если } \left(\frac{n+a_1}{p_1}\right) = \varepsilon_1, \dots, \left(\frac{n+a_k}{p_k}\right) = \varepsilon_k, \\ 0 & \text{в противном случае.} \end{cases}$$

Рассмотрим выражение

$$a(n) = \frac{1}{2^k} \prod_{s=1}^{k} \left(1 - \varepsilon_s \left(\frac{n+a_s}{p_s}\right)\right)$$

$$= \frac{1}{2^k} + \frac{1}{2^k} \sum_{s_1, \dots, s_l} (-1)^l \varepsilon_{s_1} \dots \varepsilon_{s_l} \left(\frac{n+a_{s_1}}{p_{s_1}}\right) \dots \left(\frac{n+a_{s_l}}{p_{s_l}}\right).$$

Просуммировав величины $a(n)$ по n от 1 до h, получим, что

$$\sum_{n=x+1}^{x+h} a(n) = \frac{h}{2^k} + \frac{\theta}{2^k} \sum_{s_1, \dots, s_l} \sqrt{p_{s_1} \dots p_{s_l}} \log(p_{s_1} \dots p_{s_l}) = \frac{h}{2^k} + \frac{\theta \ln Q}{2^k} \prod_{s=1}^{k} (1 + \sqrt{p_s}).$$

Поскольку $1 + \sqrt{p_s} \leqslant 2\sqrt{p_s}$, последнее выражение равно

$$\frac{h}{2^k} + \theta_0 \sqrt{Q} \ln Q,$$

где $|\theta_0| \leqslant 1$ — некоторая постоянная.

Теорема 3 доказана.

5. О совместном распределении арифметических последовательностей по нескольким модулям

Лемма 4. *Пусть χ — мультипликативный характер поля F_q, имеющий порядок $m > 1$, и пусть $f \in F_q[x]$ — нормированный многочлен положительной степени, не являющийся m-й степенью другого многочлена. Если d — количество различных корней многочлена f в его поле разложения над F_q, то для каждого $a \in F_q$ выполняется неравенство*

$$\left| \sum_{c \in F_q} \chi(af(c)) \right| \leqslant (d-1)\sqrt{q}.$$

Доказательство можно найти, например, в [10], стр. 279.

Перейдем к доказательству теоремы 4. Пусть $p_1, \dots, p_s$ — простые числа. Рассмотрим сумму

$$S_h(x) = S_h(x; p_1, \dots, p_s) = \sum_{n=x+1}^{x+h} \left(\frac{n+a_1}{p_1}\right) \dots \left(\frac{n+a_s}{p_s}\right).$$

Вычислим сначала момент порядка $2r$ величины

$$\xi = \xi_{p_1,\dots,p_s} = \frac{S_h(x)}{\sqrt{h}}.$$

Справедливы равенства

$$\begin{aligned} A_{p_1,\dots,p_s}(2r) &= \frac{1}{p_1 \dots p_s h^r} \sum_{x=1}^{p_1 \dots p_s} \left(\sum_{n=x+1}^{x+h} \left(\frac{n+a_1}{p_1}\right) \dots \left(\frac{n+a_s}{p_s}\right)\right)^{2r} \\ &= \frac{1}{p_1 \dots p_s h^r} \sum_{x=1}^{p_1 \dots p_s} \left(\sum_{n=1}^{h} \left(\frac{n+x+a_1}{p_1}\right) \dots \left(\frac{n+x+a_s}{p_s}\right)\right)^{2r} \\ &= \frac{1}{p_1 \dots p_s h^r} \sum_{n_1,\dots,n_{2r}=1}^{h} \left(\frac{f_1(x;\bar{n})}{p_1}\right) \dots \left(\frac{f_s(x;\bar{n})}{p_s}\right), \end{aligned}$$

где $\bar{n} = (n_1, \dots, n_{2r})$ и

$$f_1(x;\bar{n}) = (x+n_1+a_1)\dots(x+n_{2r}+a_1), \dots, f_s(x;\bar{n}) = (x+n_1+a_s)\dots(x+n_{2r}+a_s).$$

По китайской теореме об остатках, если

$$x \equiv Qp_1^{-1}x_1 + \dots + Qp_s^{-1}x_s \pmod{Q}, \qquad Q = p_1 \dots p_s$$

и x пробегает полную систему вычетов по модулю Q, то x_t пробегает полную систему вычетов по модулю p_t, $t = 1, \dots, s$. Поэтому последняя сумма равна

$$\frac{1}{Qh^r} \sum_{n_1,\dots,n_{2r}=1}^{h} \sum_{x_1=1}^{p_1} \left(\frac{f_1(Qp_1^{-1}x_1;\bar{n})}{p_1}\right) \dots \sum_{x_r=1}^{p_r} \left(\frac{f_s(Qp_s^{-1}x_s;\bar{n})}{p_s}\right),$$

где

$$f_t(Qp_t^{-1}x_t;\bar{n}) = (n_1 + Qp_t^{-1}x_t + a_t)\dots(n_{2r} + Qp_t^{-1}x_t + a_t), \qquad t = 1, \dots, s.$$

Отсюда получаем, что

$$A_{p_1,\dots,p_s}(2r) = \frac{1}{p_1 \dots p_s h^r} \sum_{n_1,\dots,n_{2r}=1}^{h} \prod_{t=1}^{s} \sum_{x_t=1}^{p_t} \left(\frac{f_t(Qp_t^{-1}x_t;\bar{n})}{p_t}\right).$$

Далее, разобьем наборы натуральных чисел $(n_1, \dots, n_{2r})$ на два класса.

Прежде всего заметим следующее. Так как $Q = p_1 \dots p_s$, при некотором t, $1 \leqslant t \leqslant s$, существует $p = p_t$ такое, что $p \geqslant Q^{1/s} \geqslant Q^{1/a}$. Поскольку $\log h / \log Q \to 0$

при $Q \to \infty$, можно считать, что при достаточно большом Q выполняется неравенство $Q^{1/a} > h$.

В первый класс отнесем те и только те наборы $(n_1, \dots, n_{2r})$, которые состоят из не более чем r различных натуральных чисел, каждое из которых встречается четное число раз. Оставшиеся наборы отнесем ко второму классу. В соответствии с этим разбиением сумму $A_{p_1,\dots,p_s}(2r)$ представим в виде

$$A_{p_1,\dots,p_s}(2r) = B_1 + B_2,$$

где в сумму B_1 входят наборы первого класса, а в сумму B_2 — наборы второго класса.

Для наборов первого класса по любому модулю p_t, $1 \leqslant t \leqslant s$, многочлены $f_t(Qp_t^{-1}x_t)$ представляют собой точный квадрат по модулю p_t. Следовательно, при любом t, $1 \leqslant t \leqslant s$, сумма

$$\sum_{x_t=1}^{p_t} \left(\frac{f_t(Qp_t^{-1}x_t; \bar{n})}{p_t} \right)$$

равна $p_t - \theta_1 t$ при некотором θ_1, $0 \leqslant \theta_1 \leqslant 1$.

Для наборов второго класса по лемме 4 при выбранном выше p справедлива оценка

$$\left| \sum_{x_t=1}^{p_t} \left(\frac{f_t(Qp_t^{-1}x_t; \bar{n})}{p_t} \right) \right| \leqslant r\sqrt{p}.$$

Следовательно,

$$B_1 = \frac{1}{Qh^r} \left((2r-1)!!\, h^r (Q - \theta r) + O(ph^{r-1}) \right),$$
$$B_2 \leqslant \frac{1}{Qh^r} h^{2r} Q p^{-1} r\sqrt{p} \leqslant h^r Q^{-1/(2a)}.$$

При оценке $A_{p_1,\dots,p_s}(2r-1)$ первый класс будет пустым и $B_1 = 0$, а для второго класса имеет место та же оценка величины B_2.

Таким образом, в зависимости от четности порядка момента величины ξ получаем оценки

$$A_{p_1,\dots,p_s}(2r) = 1 \cdot 3 \dots (2r-1) + O(h^{-1}),$$
$$A_{p_1,\dots,p_s}(2r-1) \ll h^r Q^{-1/(2a)}).$$

Таким образом, при $Q \to \infty$

$$A_p(2r) \to (2r-1)!!,$$
$$A_p(2r-1) \to 0,$$

здесь и выше $(2r-1)!! = 1 \cdot 3 \dots (2r-1)$. Следовательно, величина $\xi_Q = S_h(x)/\sqrt{h}$ при $Q \to \infty$ имеет в пределе стандартное нормальное распределение. Теорема 4 доказана.

Список литературы

1. Виноградов И. М., Sur la distribution des residues et des nonresidues des puissances. *Журнал физ.-матем. об-ва при Пермском ун-те* (1918) **1**, 94–98.
2. Виноградов И. М., О распределении квадратичных вычетов и невычетов. *Журнал физ.-матем. об-ва при Пермском ун-те* (1919) **2**, 1–16.
3. Виноградов И. М., *Основы теории чисел.* Наука, Москва, 1972.
4. Davenport H., Erdös P., The distribution of quadratic and higher residues. *Publ. Math. Debrecen* (1952) **2**, №3-4, 252–265.
5. Burgess D. A., The distribution of quadratic residues and nonresidues. *Math.* (1957) **4**, №8, 106–112.
6. Карацуба А. А., Распределение обратных величин в кольце вычетов по заданному модулю. *Докл. РАН.* (1993) **333**, №2, 138–139.
7. Карацуба А. А., Аналоги сумм Клостермана. *Изв. РАН. Сер. матем.* (1995) **59**, №5, 93–102.
8. Карацуба А. А., Двойные суммы Клостермана. *Матем. заметки* (1999) **66**, №5, 682–687.
9. Кубилюс И. П., Линник Ю. В., Арифметическое моделирование броуновского движения. *Изв. вузов. Математика* (1959) **13**, 88–95.
10. Лидл Р., Нидеррайтер Г., *Конечные поля,* т. 1. Мир, Москва, 1988.
11. Линник Ю. В., *Эргодические свойства алгебраических полей.* Наука, Ленинград, 1967.
12. Жимбо Э. К., О распределении значений модулей неполных сумм Гаусса. В сб.: *Тезисы Международной конф. "Современное состояние и перспективы развития математики в рамках программы «Казахстан в третьем тысячелетии»".* Алматы, 26–28 октября 2000, с. 80.

Статья поступила 18.12.2000.