УДК 511

КАФЕДРА МАТЕМАТИЧЕСКИХ И КОМПЬЮТЕРНЫХ МЕТОДОВ АНАЛИЗА

В. Н. Чубариков[1]

В работе дан обзор основных результатов научной деятельности кафедры математических и компьютерных методов анализа за последние 15 лет.

Ключевые слова: аналитическая теория чисел, дзета-функция Римана, тригонометрические суммы и интегралы, численный анализ, применения теории чисел в криптографии.

In this paper the view of main results of the scientific work of the Chair of Mathematical and Computers Methods of Analysis for last 15 years is given.

Key words: analytic number theory, Riemann's zeta-function, trigonometric sums and integrals, numerical analysis, applications of the number theory to the cryptography.

DOI: 10.55959/MSU0579-9368-1-66-1-7

1. Введение. Цель настоящего обзора — представить исследования, выполненные сотрудниками кафедры математических и компьютерных методов анализа.

Методологическая основа нашей работы сформулирована в 1937 г. И. М. Виноградовым в его работе "О проблемах аналитической теории чисел". Он писал: "Анализ делает возможным значительно расширить область проблем теории чисел и служит более быстрому развитию этой науки. Я также хочу подчеркнуть одну более полезную черту аналитического метода в теории чисел. В то время как решаются новые трудные проблемы, анализ сам развивается и совершенствуется. Ряды Дирихле и теория $\zeta(s)$-функции могут служить хорошим примером, как и некоторые свойства функций Бесселя, ряд замечательных теорем, относящихся к теории функций комплексного переменного (например, теоремы Линделёфа, Фрагмена, Меллина), разрывные суммы и интегралы и др. Таким образом, применение аналитических методов в теории чисел обогащает эту науку новыми ценными достижениями и в то же время развивает и совершенствует сам анализ".

В 1924–1928 гг. И. М. Виноградов использовал анализ Фурье и конечные тригонометрические суммы для вывода асимптотических оценок числа решений уравнения в проблеме Варинга. В 1934 г. он нашел новый мощный метод получения оценок тригонометрических сумм, который позволил ему существенно и принципиально продвинуться в проблеме Варинга.

Постановки подобных задач берут начало в исследованиях Кронекера по поведению дробных долей линейных форм с целыми переменными. Начальный период развития современной теории равномерного распределения значений функций связан с именами П. Боля (P. Bohl), В. Серпинского (V. Sierpinski), Г. Вейля (H. Weyl), Э. Бореля (E. Borel), Ф. Бернштейна (F. Bernstein), Г. Харди (G. Hardy) и Дж. Литлвуда (J. Littlewood). Само понятие **равномерного распределения по модулю единица** предложено в 1914 г. и 1916 г. Г. Вейлем и ему принадлежат разные формы критерия равномерного распределения [1]. Он обратил внимание на пользу анализа Фурье в данном им критерии.

2. Суммы Г. Вейля и метод И. М. Виноградова [2–4]. Пусть $P \geqslant 1$ — натуральное число, $(\alpha_1, \ldots, \alpha_n)$ —набор действительных чисел, $f(x) = \alpha_1 x + \ldots + \alpha_n x^n$. Тогда тригонометрическая сумма $S_P = S_P(\alpha_1, \ldots, \alpha_n)$ вида

$$S_P = \sum_{x=1}^{P} e^{2\pi i f(x)}$$

называется суммой Г. Вейля. Сумма S является периодической функцией по каждому аргументу $\alpha_s, s \geqslant 1$, с периодом, равным единице. Поэтому достаточно оценить ее в каждой точке единичного куба $0 \leqslant \alpha_s < 1, 1 \leqslant s \leqslant n$. И. М. Виноградов показал, что задача об оценке суммы

[0] *Чубариков Владимир Николаевич* — доктор физико-математических наук, проф., зав. каф. математических и компьютерных методов анализа мех.-мат. ф-та МГУ, e-mail: chubarik2020@mail.ru.

Chubarikov Vladimir Nikolaevich — Doctor of Physical and Mathematical Sciences, Professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Head of the Chair of Mathematical and Computers Methods of Analysis.

$S_P = S_P(\alpha_1, \ldots, \alpha_n)$ существенно зависит от оценки $J = J(P; k, n)$ — среднего значения $2k$-й степени модуля S, т.е.

$$J = \int_0^1 \cdots \int_0^1 |S(\alpha_1, \ldots, \alpha_n)|^{2k} \, d\alpha_1 \ldots d\alpha_n,$$

и что J равно числу решений следующей системы диофантовых уравнений вида

$$\begin{cases} x_1 + \ldots + x_k = x_{k+1} + \ldots + x_{2k}, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ x_1^n + \ldots + x_k^n = x_{k+1}^n + \ldots + x_{2k}^n, \end{cases}$$

$$1 \leqslant x_1, \ldots, x_{2k} \leqslant P.$$

Теорема И. М. Виноградова о среднем. *Пусть $\tau \geqslant 0, k \geqslant n\tau, P \geqslant 1$ — целые. Тогда имеем*

$$J = J(P; k, n) \leqslant D_\tau P^{2k - \Delta(\tau)},$$

где

$$\Delta(\tau) = 0,5n(n+1)(1 - (1 - 1/n)^\tau), D_\tau = (n\tau)^{6n\tau}(2n)^{4n(n+1)\tau}.$$

3. Теорема о среднем значении кратных тригонометрических сумм общего вида [5]. Пусть $r \geqslant 1, 0 \leqslant n_1, \ldots, n_r, P_1, \ldots, P_r \geqslant 1$ — целые числа, и пусть

$$F(x_1, \ldots, x_r) = \sum_{x_1=0}^{n_1} \cdots \sum_{x_r=0}^{n_r} \alpha(t_1, \ldots, t_r) x_1^{t_1} \ldots x_r^{t_r}$$

обозначает многочлен с действительными коэффициентами $\alpha(t_1, \ldots, t_r)$, A — набор, составленный из коэффициентов многочлена $F(x_1, \ldots, x_r)$, упорядоченных некоторым образом. Положим

$$S(A) = \sum_{x_1 \leqslant P_1} \cdots \sum_{x_r \leqslant P_r} e^{2\pi i F(x_1, \ldots, x_r)}.$$

Пусть Ω обозначает единичный m-мерный куб, $m = (n_1 + 1) \ldots (n_r + 1)$, следующего вида:

$$0 \leqslant \alpha(t_1, \ldots, t_r) < 1, \quad 0 \leqslant t_1 \leqslant n_1, \ldots, 0 \leqslant t_r \leqslant n_r.$$

Тогда среднее значение $2k$-й степени модуля кратной тригонометрической суммы $S(A)$ имеет вид

$$J = J(P; k, r, \bar{n}) = \int_A \cdots \int |S(A)|^{2k} \, dA,$$

где $\bar{n} = (n_1, \ldots, n_r)$, $\quad dA = \prod_{t_1}^{n_1} \ldots \prod_{t_r}^{n_r} \alpha(t_1, \ldots, t_r)$.

Теорема 1 (о среднем). *Пусть $\tau \geqslant 0, r \geqslant 1, n_1, \ldots n_r \geqslant 0, k \geqslant m\tau, P \geqslant 1$ — целые числа. Тогда*

$$J = J(P; k, r, \bar{n}) \leqslant D_\tau (P_1 \ldots P_r)^{2k} P^{-n\Delta_\tau},$$

где

$$D_\tau = k^{2m\tau} n^{4\varkappa^2 \Delta(\tau)} 2^{8m\varkappa\tau}, \quad n = n_1\nu_1 + \ldots + n_r\nu_r, \gamma n = 1, m = (n_1 + 1) \ldots (n_r + 1),$$

$$\Delta_\tau = 0,5m(1 - (1 - \gamma)^\tau), \quad P = (P_1^{n_1} \ldots P_r^{n_r})^\gamma, P_1 = \min\{P_1, \ldots, P_r\}.$$

Здесь $\nu_1, \ldots, \nu_r$ — натуральные числа, такие, что

$$-1 < \frac{\ln P_s}{\ln P_1} \leqslant 0, \quad s = 1, \ldots, r.$$

4. Оценки кратных тригонометрических сумм и интегралов [5, 6]. И. М. Виноградов [2] доказал следующее утверждение. *Пусть* $f(x) = \alpha_n x^n + \ldots + \alpha_1 x$, *где* $\alpha_n, \ldots, \alpha_1$ — *действительные числа, наибольший из модулей которых обозначим символом* α. *Тогда*

$$\left| \int_0^1 e^{2\pi i f(x)}\, dx \right| \leqslant \min\{1, 32\alpha^{-1/n}\}.$$

Теорема 2. *Пусть* $\alpha = \max\limits_{0 \leqslant t_1, \ldots, t_r \leqslant n} |\alpha(t_1, \ldots, t_r)|$, $\alpha(0, \ldots, 0) = 0$,

$$I_r = \int_0^1 \cdots \int_0^1 e^{2\pi i F(x_1, \ldots, x_r)}\, dx_1 \ldots dx_r,$$

где

$$F(x_1, \ldots, x_r) = \sum_{t_1=0}^{n} \cdots \sum_{t_r=0}^{n} \alpha(t_1, \ldots, t_r) x_1^{t_1} \ldots x_r^{t_r}.$$

Тогда

$$|I_r| \leqslant \min\{1,\ 32^r \alpha^{-1/n} \ln^{r-1}(\alpha + 2)\}.$$

Теорема 3. *Пусть* $n \geqslant 1, \alpha_1, \ldots, \alpha_n$ — *действительные числа,*

$$f(x) = \alpha_n x^n + \ldots + \alpha_1 x, \quad \beta_r(x) = f^r(x)/r!, \quad r = 1, \ldots, n,$$

$$H = H(\alpha_n, \ldots, \alpha_1) = \min_{a \leqslant x \leqslant b} \sum_{r=1}^{n} |\beta_r(x)|^{1/r}.$$

Тогда для интеграла

$$J = \int_a^b e^{2\pi i f(x)}\, dx$$

справедлива оценка

$$|J| \leqslant \min\{b - a, 6en^3 H^{-1}\}.$$

Особый интеграл проблемы Терри имеет вид

$$\theta = \theta(k, n) = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \left| \int_0^1 e^{2\pi i(\alpha_n x^n + \ldots + \alpha_1 x)}\, dx \right|^{2k} d\alpha_n \ldots d\alpha_1.$$

Теорема 4. *Особый интеграл* $\theta = \theta(k, n)$ *сходится при* $2k > 0,5(n^2 + n) + 1$ *и расходится при* $2k \leqslant 0,5(n^2 + n) + 1$.

Пусть $\theta' = \theta'(k, n)$ обозначает особый интеграл неполной системы уравнений в проблеме Терри:

$$\theta' = \theta'(k, n) = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \left| \int_0^1 e^{2\pi i(\alpha_n x^n + \alpha_m x^m + \ldots + \alpha_r x^r)}\, dx \right|^{2k} d\alpha_n d\alpha_m \ldots d\alpha_r,$$

где $1 \leqslant r < \ldots < m < n, r + \ldots + m + n < 0,5(n^2 + n)$.

Теорема 5. *Особый интеграл* $\theta' = \theta'(k, n)$ *сходится при* $2k > n + m + \ldots + r$ *и расходится при* $2k \leqslant n + m + \ldots + r$.

5. Численный анализ, кратные интегралы и представление чисел суммами квадратов [7]. Здесь мы рассматриваем линейные квадратуры для классов функций от нескольких переменных, периодических по каждой переменной и разлагающихся в абсолютно сходящиеся ряды Фурье вида

$$f(\mathbf{x}) = f(x_1, \ldots, x_n) = \sum_{\mathbf{m} \in \mathbf{Z}^n} c(\mathbf{m}) e^{2\pi i(\mathbf{m}, \mathbf{x})}, \tag{1}$$

где $\mathbf{m} = (m_1, \ldots, m_n)$,

$$c(\mathbf{m}) = c(\mathbf{m}; f) = \int_0^1 \cdots \int_0^1 f(\mathbf{x}) e^{-2\pi i(\mathbf{m},\mathbf{x})}\, d\mathbf{x}. \tag{2}$$

Нами решается задача построения с помощью методов теории чисел квадратурных формул, которые дают возможность точно интегрировать тригонометрические многочлены возможно более высокой степени при заданном числе узлов интегрирования.

5.1. *Двумерный случай.* Пусть $F(x_1, x_2)$ — периодическая функция по каждой переменной x_1 и x_2 с периодом единица и разлагающаяся в абсолютно сходящийся ряд Фурье вида (1), (2) при $n = 2$. Предположим, что число узлов интегрирования N^2 представимо в форме

$$N^2 = N_1^2 + N_2^2,\ (N_1, N_2) = 1,\ N_1, N_2 > 0.$$

Заметим, что этому неопределенному уравнению в натуральных числах N_1, N_2, N удовлетворяют те и только те числа N_1, N_2, N, которые имеют вид

$$\begin{cases} N_1 = 2uv, \\ N_2 = u^2 - v^2, \\ N = u^2 + v^2, \end{cases}$$

где u, v — любые натуральные числа с условиями $u > v > 0, (u, v) = 1, uv$ — четное число.

Теорема 6. *Пусть коэффициенты $c(m_1, m_2)$ определены равенством* (2). *Тогда квадратура*

$$L_N(f) = \frac{1}{N^2} \sum_{\nu=0}^{N^2-1} f\left(\frac{N_1\nu}{N^2}, \frac{N_2\nu}{N^2}\right)$$

точна для тригонометрических многочленов вида

$$f(x_1, x_2) = \sum_{\substack{k_1=0\ k_2=0 \\ k_1^2+k_2^2<N^2}}^{N\ N} c(k_1, k_2) e^{2\pi i(k_1x_1+k_2x_2)}.$$

Доказательство. Преобразуем формулу для $L_N(f)$. Находим

$$L_N(f) = \frac{1}{N^2} \sum_{\nu=0}^{N^2-1} \sum_{\substack{k_1=0\ k_2=0 \\ k_1^2+k_2^2<N^2}}^{N\ N} c(k_1, k_2) e^{2\pi i \frac{(k_1N_1+k_2N_2)\nu}{N^2}} =$$

$$= \sum_{\substack{k_1=0\ k_2=0 \\ k_1^2+k_2^2<N^2}}^{N\ N} c(k_1, k_2) \cdot \frac{1}{N^2} \sum_{\nu=0}^{N^2-1} e^{2\pi i \frac{(k_1N_1+k_2N_2)\nu}{N^2}} = \sum_{\substack{k_1=0\ k_2=0 \\ k_1^2+k_2^2<N^2}}^{N\ N\ \prime} c(k_1, k_2),$$

где штрих в знаке суммирования означает, что переменные суммирования k_1 и k_2 удовлетворяют сравнению $k_1N_1 + k_2N_2 \equiv 0 \pmod{N^2}$. Из неравенства Коши имеем

$$0 \leqslant k_1N_1 + k_2N_2 \leqslant (k_1^2 + k_2^2)^{1/2}(N_1^2 + N_2^2)^{1/2} < N^2.$$

Следовательно, сравнение $k_1N_1 + k_2N_2 \equiv 0 \pmod{N^2}$ при $k_1^2 + k_2^2 < N$ имеет единственное решение $k_1 = k_2 = 0$. Таким образом,

$$L_N(f) = c(0, 0) = \int_0^1 \int_0^1 f(x_1, x_2)\, dx_1 dx_2.$$

Теорема доказана.

5.2. *Общий случай.* Предположим, что число N^2 узлов интегрирования удовлетворяет соотношению

$$N^2 = N_1^2 + \ldots + N_n^2,$$

где $N_s \in \mathbf{Z}, (N_s, N) = 1$ при $1 \leqslant s \leqslant n$.

Справедливо следующее утверждение.

Теорема 7. *Пусть коэффициенты $c(\mathbf{m})$ определены формулой* (2). *Тогда квадратура*

$$L_N(f) = \frac{1}{N^2} \sum_{\nu=0}^{N^2-1} f\left(\frac{N_1\nu}{N^2}, \ldots, \frac{N_n\nu}{N^2}\right)$$

точна для тригонометрических многочленов вида

$$f(\mathbf{x}) = \sum_{\substack{k_1=0 \\ k_1^2+\ldots+k_n^2<N^2}}^{N} \ldots \sum_{k_n=0}^{N} c(\mathbf{k}) e^{2\pi i(\mathbf{k},\mathbf{x})}.$$

Доказательство. Преобразуем формулу для $L_N(f)$. Находим

$$L_N(f) = \frac{1}{N^2} \sum_{\nu=0}^{N^2-1} \sum_{\substack{k_1=0 \\ k_1^2+\ldots+k_n^2<N^2}}^{N} \cdots \sum_{k_n=0}^{N} c(\mathbf{k}) e^{2\pi i \frac{(k_1N_1+\ldots+k_nN_n)\nu}{N^2}} =$$

$$= \sum_{\substack{k_1=0 \\ k_1^2+\ldots+k_n^2<N^2}}^{N} \cdots \sum_{k_n=0}^{N} c(\mathbf{k}) \cdot \frac{1}{N^2} \sum_{\nu=0}^{N^2-1} e^{2\pi i \frac{(k_1N_1+\ldots+k_nN_n)\nu}{N^2}} = \sum_{\substack{k_1=0 \\ k_1^2+\ldots+k_n^2<N^2}}^{N} \ldots \sum_{k_n=0}^{N}{}' c(\mathbf{k}),$$

где штрих в знаке суммирования означает, что переменные суммирования $k_1, \ldots, k_n$ удовлетворяют сравнению $k_1N_1 + \ldots + k_nN_n \equiv 0 \pmod{N^2}$. Из неравенства Коши имеем

$$0 \leqslant k_1N_1 + \ldots + k_nN_n \leqslant (k_1^2 + \ldots + k_n^2)^{1/2}(N_1^2 + \ldots + N_n^2)^{1/2} < N^2.$$

Следовательно, сравнение $k_1N_1 + \ldots + k_nN_n \equiv 0 \pmod{N^2}$ при $k_1^2 + \ldots + k_n^2 < N$ имеет единственное решение $k_1 = \ldots = k_n = 0$. Таким образом,

$$L_N(f) = c(0, \ldots, 0) = \int_0^1 \ldots \int_0^1 f(x_1, \ldots, x_n)\, dx_1 \ldots dx_n.$$

Теорема доказана.

6.1. Короткие и очень короткие суммы Гаусса [8–10]. Рассмотрим неполную сумму Гаусса вида

$$S_h(x) = \sum_{n=x+1}^{x+h} \chi(n) e^{2\pi i \frac{an}{p}},$$

где p — простое, $(a, p) = 1$, числа x, h — целые и $0 \leqslant x < p, 0 < h < p, \chi(n)$ — комплексный характер Дирихле по модулю p. Пусть $N_p\{\ldots\}$ обозначает число целых чисел $0 \leqslant x < p$, удовлетворяющих условиям, которые указываются в фигурных скобках.

Теорема 8. *Пусть $h(p) \to \infty, \frac{\ln h}{\ln p} \to 0$ при $p \to \infty$. Тогда величина*

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

асимптотически имеет показательное распределение с параметром 1, *т.е. для любого фиксированного $y > 0$ имеем*

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

Пусть

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

где q пробегает последовательно значения всех простых чисел, $qq^*\equiv 1 \pmod p$, $|\varepsilon(q)|=1$.

Теорема 9. *Пусть* $h(p)\to\infty$, $\frac{\ln h}{\ln p}\to 0$ *при* $p\to\infty$, *и пусть*

$$N_p(\lambda)=N_p\{0\leqslant x<p;|S_p(x;h)|<\sqrt{\lambda h}\}.$$

Тогда при любом фиксированном $\lambda>0$ *имеем*

$$\lim_{p\to\infty}\frac{N_p(\lambda)}{p}=1-e^{-\lambda}.$$

Пусть $p_1,\dots,p_k$ — различные простые числа, $Q=p_1\dots p_k, a_1,\dots,a_k$ — любые фиксированные целые числа, и пусть

$$S_Q(x;h)=\sum_{n=x+1}^{x+h}\left(\frac{n+a_1}{p_1}\right)\dots\left(\frac{n+a_k}{p_k}\right).$$

Теорема 10. *Пусть* $h(Q)\to\infty$, $\frac{\ln h}{\ln Q}\to 0$ *при* $Q\to\infty$, *и пусть*

$$N_Q(\lambda)=N_Q\{0\leqslant x<p;S_Q(x;h)<\lambda\sqrt{h}\}.$$

Тогда при любом фиксированном вещественном λ *имеем*

$$\lim_{Q\to\infty}\frac{N_Q(\lambda)}{Q}=\frac{1}{\sqrt{2\pi}}\int\limits_{-\infty}^{\lambda}e^{\frac{-x^2}{2}}\,dx.$$

Пусть задана последовательность Фибоначчи $f_0=1, f_1=1,\dots,f_{k+1}=f_k+f_{k-1}$ при $n\geqslant 2$, m,x — любые натуральные числа, и пусть

$$S_m(x;h)=\sum_{n=0}^{h-1}e^{2\pi i\frac{xf_n}{m}}.$$

Теорема 11. *Пусть* $h(m)\to\infty$, $\frac{\ln h}{\ln m}\to 0$ *при* $m\to\infty$, *и пусть*

$$N_m(\lambda)=N_Q\{0\leqslant x<p;|S_m(x;h)|<\sqrt{\lambda h}\}.$$

Тогда при любом фиксированном вещественном $\lambda>0$ *имеем*

$$\lim_{m\to\infty}\frac{N_m(\lambda)}{m}=1-e^{-\lambda}.$$

6.2. Среднее значение произведений символов Лежандра по "сдвинутым" простым [8].

Теорема 12 (Э. К. Жимбо, 2000). *Пусть, как и раньше,* $p_1,\dots,p_k$ *— различные простые числа,* $Q=p_1\dots p_k, a_1,\dots,a_k$ *— любые фиксированные целые числа, и пусть* $T=T(Q)$ *обозначает число натуральных значений* n, *принадлежащих отрезку* $[x+1,x+h], 0\leqslant x, x+h\leqslant Q$, *и удовлетворяющих соотношениям*

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

где $\varepsilon_s, s=1,\dots,k$, *могут принимать значения либо* $+1$, *либо* -1. *Тогда*

$$T=\frac{h}{2^k}+\theta\sqrt{Q}\ln Q, |\theta|\leqslant 1.$$

В 2013 г. Д. В. Копьёв, в частности, доказал, что для любого $\varepsilon > 0$ при $h \geqslant Q^{\frac{1}{4}+\varepsilon}$ найдется постоянная $c > 0$, такая, что при $Q \to \infty$ справедлива асимптотика

$$T = \frac{h}{2^k} + R, R \ll hQ^{-c\varepsilon^2}.$$

Здесь продолжены исследования И. М. Виноградова по нахождению нетривиальных оценок сумм по простым числам p. Эти суммы имеют вид

$$\sum_{p \leqslant N} \Phi(p), \quad \Phi(p) = \prod_{s=1}^{r} \left(\frac{p + k_s}{q_s} \right),$$

причем $q_1, \ldots, q_r$ — различные нечетные простые числа, $(k_s, q_s) = 1, s = 1, \ldots, r$. К этим условиям добавим следующее: $k_s \not\equiv k_t \pmod{q_s}, 1 \leqslant s, t \leqslant r, s \neq t$, которое обеспечивает отличие от тождественной единицы произведения символов Лежандра.

Теорема 13. *Пусть p пробегает последовательные значения простых чисел, $q_1, \ldots, q_r$ — различные нечетные простые числа, $q = q_1 \ldots q_r$, $(k_s, q_s) = 1, 1 \leqslant k_s \leqslant q_s$, $k_s \not\equiv k_t \pmod{q_t}$, $s \neq t$, $s, t = 1, \ldots, r$, и*

$$T = \sum_{p \leqslant N} \left(\frac{p + k_1}{q_1} \right) \ldots \left(\frac{p + k_r}{q_r} \right).$$

Тогда имеем

$$T \ll 2^r N^{1+\varepsilon} \left(\sqrt{\frac{1}{q} + \frac{q}{N}} + N^{-1/6} \right),$$

где постоянная в знаке $\ll$ зависит только от ε.

Теорема 14. *Пусть p пробегает последовательные значения простых чисел, $q_1, \ldots, q_r$ — различные нечетные простые числа, $q = q_1 \ldots q_r$, $(k_s, q_s) = 1$, $1 \leqslant k_s \leqslant q_s$, $k_s \not\equiv k_t \pmod{q_s}$, $s \neq t$, $s, t = 1, \ldots, r$, и $S(N)$ — число решений в простых числах $p \leqslant N$ следующей системы уравнений:*

$$\left(\frac{p + k_s}{q_s} \right) = \tau_s, s = 1, \ldots, r,$$

где τ_s может принимать лишь два значения: $+1$ или -1. Тогда имеем

$$S(N) = 2^{-r}\pi(N) + R(N), \quad R(N) \ll N^{1+\varepsilon} \left(\sqrt{\frac{1}{q} + \frac{q}{N}} + N^{-1/6} \right),$$

где постоянная в знаке $\ll$ зависит только от ε.

7.1. О методе Адамара в теории L-функций Дирихле [11]. Здесь мы изложим вариант метода Адамара, предложенный О. В. Поповым. Рассмотрим сначала задачу об отсутствии нулей L-функции Дирихле на единичной прямой.

Теорема 15. *Пусть χ — комплексный характер Дирихле по модулю q. Тогда L-функция Дирихле $L(s, \chi) = \sum\limits_{n=1}^{\infty} \chi(n) n^{-s}$ не обращается в нуль на прямой $\Re s = 1$.*

Доказательство. Пусть $\rho = 1 + it_0$ — нуль $L(s, \chi)$, т.е. $L(\rho, \chi) = 0$, тогда он простой. Предположим, что его кратность равна $k \geqslant 2$. Возьмем $s = \sigma + it_0, \sigma > 1$. Тогда при $\sigma \to 1 + 0$ имеем

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} = -\frac{k}{\sigma - 1} + O(1)$$

и для главного характера χ_0 по модулю q при $\sigma > 1$ получим

$$L(s, \chi_0) = \sum_{n=1}^{\infty} \chi_0(n) n^{-s} = \zeta(s) \prod_{p|q} (1 - p^{-s}), -\frac{L'(\sigma, \chi_0)}{L(\sigma, \chi_0)} = \frac{1}{\sigma - 1} + O(1).$$

Далее находим

$$\delta = \sum_{\substack{n=1 \\ (n,q)=1}}^{\infty} \frac{\Lambda(n)}{n^{\sigma}} \left(1 + \Re(\chi(n) n^{it_0}) \right) \geqslant 0$$

и при $\sigma \to 1+0$ получим

$$\delta = -\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} + \Re\left\{-\frac{L'(s,\chi)}{L(s,\chi)}\right\} = \frac{1-k}{\sigma-1} + O(1) \to -\infty.$$

Это противоречие показывает, что $k \leqslant 1$.

Предположим, как и раньше, что $L(1+it_0,\chi)=0$, и пусть $\chi(n)n^{it_0} = e^{i\varphi}$. Тогда находим

$$\Delta = -\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} + \Re\left\{\frac{L'(\sigma+2it_0,\chi^2)}{L(\sigma+2it_0,\chi^2)}\right\} = \sum_{\substack{n=1\\(n,q)=1}}^{\infty} \frac{\Lambda(n)}{n^\sigma}\,(1-\cos 2\varphi) \geqslant 0.$$

Оценим Δ при $\sigma \to 1+0$. Получим

$$\Delta = 2\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma}\,(1-\cos\varphi)\,(1+\cos\varphi) \leqslant 4\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma}\,(1+\cos\varphi) = 4\delta = O(1).$$

Это означает, что $L(s,\chi)$ имеет полюс в точке $1+2it_0$. Данное утверждение противоречит тому факту, что $L(s,\chi)$ является аналитической функцией при $\Re s > 0$. Теорема доказана.

7.2. Отсутствие нулей L-функции Дирихле в окрестности единичной прямой. Итак, для любого $\sigma > 1$ и для любого $t \in \mathbf{R}$ установлено неравенство $\Delta \leqslant 4\delta$, где $s = \sigma + it$,

$$\delta = -\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} + \Re\left\{-\frac{L'(s,\chi)}{L(s,\chi)}\right\}, \quad \Delta = -\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)} + \Re\left\{\frac{L'(\sigma+2it,\chi^2)}{L(\sigma+2it,\chi^2)}\right\}.$$

Отсюда находим

$$0 \leqslant 4\delta - \Delta = 3\left\{-\frac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)}\right\} + 4\Re\left\{-\frac{L'(\sigma+it,\chi_0)}{L(\sigma+it,\chi_0)}\right\} + \Re\left\{-\frac{L'(\sigma+2it,\chi^2)}{L(\sigma+2it,\chi^2)}\right\}.$$

7.3. О простых в редких последовательностях. Пусть p, q — простые числа и $\pi_C(x)$ обозначает количество простых чисел p, не превосходящих x, в последовательности C вида $2^p + p$, т.е.

$$\pi_C(x) = \sum_{\substack{p\leqslant x\\2^p+p=q}} 1\ .$$

Теорема 16 (А. Мильуоло). *При $x \to \infty$ имеем*

$$\pi_C(x) = o(\pi(x)).$$

В основе доказательства теоремы 16 лежит утверждение о последовательности натуральных чисел d, удовлетворяющих условию $(d, \varphi(d)) = 1$.

8. О нелинейных диофантовых неравенствах [2, 5, 12]. Метод И. М. Виноградова оценок тригонометрических сумм в качестве своей составной части имеет утверждение о кратности пересечения областей [2, лемма 5, с. 59], в котором оценка числа решений системы нелинейных диофантовых неравенств сводится к подобной задаче для линейных диофантовых неравенств.

Пусть $n \geqslant 3$ и $\alpha_n, \ldots, \alpha_1 \in \mathbf{R}$, $f(x) = \alpha_n x_n + \ldots + \alpha_1 x$. Каждому $y \in \mathbf{Z}$ поставим в соответствие точку $(Y_{n-1}, \ldots, Y_1)$ из разложения многочлена $f(x+y) - f(y)$ по степеням x, т.е.

$$f(x+y) - f(y) = \alpha_n x^n + Y_{n-1}x^{n-1} + \ldots + Y_1 x, Y_s = Y_s(y), s = n-1, \ldots, 1.$$

Пусть $Y \leqslant P$ — натуральные числа, $P > 1$. Тогда для любого $y_0 \leqslant Y$ число решений системы сравнений $Y_s(y) - Y_s(y_0) \equiv \theta_s P^{-s} \pmod 1 (s = n-1, \ldots, 1)$ при некоторых $|\theta_s| \leqslant 1$ не превосходит числа решений линейной системы неравенств:

$$\|n \ldots s\alpha_s(y - y_0)\| \leqslant n \ldots (s+1)\,(1,5n)^{n-1}\,P^{-s+1} (s = n, \ldots, 2),$$

где $\|h\|$ — расстояние от вещественного числа h до ближайшего целого.

Первое нетривиальное обобщение этой теоремы И. М. Виноградова на кратный случай дал Г. И. Архипов. Пусть многочлен $F(x_1,\dots,x_r)\in\mathbf{R}[x_1,\dots,x_r]$ имеет вид

$$F(x_1,\dots,x_r)=\sum_{t_1=0}^{n_1}\cdots\sum_{t_r=0}^{n_r}\alpha(t_1,\dots,t_r)x_1^{t_1}\dots x_r^{t_r}.$$

Тогда

$$F(x_1+y_1,\dots,x_r+y_r)-F(x_1+z_1,\dots,x_r+z_r)=\sum_{t_1=0}^{n_1}\cdots\sum_{t_r=0}^{n_r}B(t_1,\dots,t_r)x_1^{t_1}\dots x_r^{t_r},$$

где

$$B(u_1,\dots,u_r)=\sum_{t_1=u_1}^{n_1}\cdots\sum_{t_r=u_r}^{n_r}\alpha(t_1,\dots,t_r)\binom{t_1}{u_1}\dots\binom{t_r}{u_r}(y_1^{t_1-u_1}\dots y_r^{t_r-u_r}-z_1^{t_1-u_1}\dots z_r^{t_r-u_r}).$$

Пусть далее $\mathbf{u}=(u_1,\dots,u_r), u=u_1+\ldots+u_r$,

$$A(\mathbf{u};s)=\sum_{\substack{t_1=u_1\\ v=s+u}}^{n_1}\cdots\sum_{t_r=u_r}^{n_r}\alpha(t_1,\dots,t_r)\binom{t_1}{u_1}\dots\binom{t_r}{u_r}(y_1^{t_1-u_1}\dots y_r^{t_r-u_r}-z_1^{t_1-u_1}\dots z_r^{t_r-u_r})$$

— форма степени s многочлена $B(\mathbf{u})=\sum\limits_{s=0}^{n-u}A(\mathbf{u};s)$.

Выделим формы $A(\mathbf{u};1)$ первой степени. Они имеют вид

$$A(\mathbf{u};1)=\sum_{j=1}^{r}(u_j+1)\alpha(u_1,\dots,u_j+1,\dots,u_r)(y_j-z_j).$$

Теорема 17. *Существуют многочлены $H(\mathbf{u};\mathbf{v};s)$ от переменных $y_1,\dots,y_r,z_1,\dots,z_r$ с целыми неотрицательными коэффициентами и такие, что выполняются равенства*

$$A(\mathbf{u};s)=\frac{1}{u_1!\dots u_r!s!}\sum_{\substack{v_1=u_1\\ v=s-1+u}}^{n_1}\dots\sum_{v_r=u_r}^{n_r}v_1!\dots v_r!H(\mathbf{u};\mathbf{v};s)A(\mathbf{v};1);$$

при этом сумма коэффициентов каждого многочлена $H(\mathbf{u};\mathbf{v};s)$ не превосходит sr^{s-1}, а сумма степеней переменных $y_j,z_j(j=1,\dots,r)$, входящих в любой одночлен многочлена H, не превосходит $v_j-u_j(j=1,\dots,r)$.

9. Метод искажения знаков в шифре простой замены с помощью извлечения корня квадратного [13, 14]. Пусть алфавит открытого текста состоит из n букв. Шифрование исходного текста способом простой однобуквенной замены основано на некоторой подстановке множества букв алфавита. Следовательно, эта подстановка является ключом такой криптосистемы и значит, количество возможных ключей будет равно $n!$. Отметим, что различным символам шифрованного текста соответствуют различные буквы. В исходном тексте различные буквы, как правило, встречаются с разной частотой.

В качестве модельной ситуации рассмотрим русский алфавит, состоящий из 31 буквы (отождествляются буквы е, ё и ь, ъ). Известна таблица относительных частот встречаемости букв этого алфавита, упорядоченная в порядке убывания частот, в тексте на русском языке. Поскольку число 31 — простое, все вычеты по модулю 31 можно разбить на три класса: квадратичные вычеты, квадратичные невычеты и вычет, отвечающий нулю. Как известно, количество квадратичных невычетов и количество квадратичных вычетов в полной системе вычетов по простому модулю одинаково и в данном случае равно 15. Все квадратичные вычеты по модулю 31 исчерпываются следующими классами вычетов по модулю 31: $1, 2^2, 3^2, \dots, 15^2$. Занумеруем сначала все наименьшие положительные квадратичные вычеты по модулю 31 по убыванию их величины, а затем также занумеруем

квадратичные невычеты в порядке убывания. Если a — квадратичный вычет по модулю 31, то решения сравнения $x^2 \equiv a \pmod{31}$ представляют собой два различных вычета по модулю 31: $a_1 = b$ и $a_2 = 31 - b$. Рассмотрим теперь некоторый открытый текст и зашифруем его с помощью метода простой замены. Расположим буквы шифрованного текста в порядке убывания частот, нумеруя их от 1 до 31. Каждой из первых пятнадцати занумерованных букв взаимно однозначно сопоставим квадратичные вычеты по модулю 31 в соответствии с их порядком нумерации, затем следующие пятнадцать букв взаимно однозначно отобразим в квадратичные невычеты по модулю 31 также в соответствии с их порядком нумерации и, наконец, оставшейся букве сопоставим нулевой вычет по модулю 31. Далее продолжим шифрование следующим образом. Пусть буква α зашифрована числом a и a — квадратичный вычет по модулю 31, и пусть вычеты a_1, a_2 — решения сравнения $x^2 \equiv a \pmod{31}$. Тогда последовательности указанного числа a в криптограмме шифра простой замены ставим в соответствие последовательность чисел $a_1, a_2, a_1, a_2, \ldots$. Например, если в криптограмме имеется 5 мест, на которых стоит число a, то заменяем в этих местах число a на последовательность чисел a_1, a_2, a_1, a_2, a_1. Пусть теперь буква α закодирована числом a и a — квадратичный невычет по модулю 31 или 0. Тогда в криптограмме это число a оставляем без изменения. Для восстановления первоначальной криптограммы следует все числа, отвечающие квадратичным вычетам по модулю 31, возвести в квадрат по модулю 31. Остается передать получателю текста номера тех мест, на которых стоят квадратичные невычеты по модулю 31. Далее можно рекуррентным образом продолжить процедуру "сжатия алфавита". Пусть l — натуральное число и q — простое число вида $q = 2^l + 1$. Тогда простое число q обязано быть простым числом Ферма $q = F_m = 2^{2^m} + 1, m \geqslant 0$. На сегодняшний день известно только пять простых чисел Ферма: $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 2^8 + 1 = 257$ и $F_4 = 2^{16} + 1 = 65537$. Мультипликативная группа поля F_q является циклической и состоит из $q - 1 = 2^l$ элементов. Каждый из них имеет порядок $2^k, 0 \leqslant k \leqslant 2^l$. Пусть теперь алфавит A состоит из $q = 2^l + 1, l = 2^m, 0 \leqslant m \leqslant 4$, символов. Тогда, используя процедуру, описанную выше, в точности l раз, приходим к шифрованному тексту, алфавит которого отвечает только квадратичным невычетам и нулевому вычету по модулю q. Таким образом, алфавит шифрованного текста будет состоять из $(q + 1)/2$ символов.

СПИСОК ЛИТЕРАТУРЫ

1. *Weyl H.* Über die Gleichverteilung der Zahlen mod. Eins // Math. Ann. 1916. **77**. 313–352.
2. *Виноградов И.М.* Метод тригонометрических сумм в теории чисел. М.: Наука, 1980.
3. *Hua L.-K.* An improvement of Vinogradov's mean-value theorem and several applications // Quart. J. Math. 1949. **20**. 48–61.
4. *Карацуба А.А.* Основы аналитической теориии чисел. М.: ФИЗМАТЛИТ, 1983.
5. *Arkhipov G.I., Chubarikov V.N., Karatsuba A.A.* Trigonometric Sums in Number Theory and Analysis. De Gruyter Expositions in Mathematics. Vol. 39. Berlin; New York, 2004.
6. *Чубариков В.Н.* Кратные полные рациональные арифметические суммы от значений многочлена // Докл. РАН. 2018. **478**, № 1. 22–24.
7. *Чубариков В.Н.* О квадратурных формулах // Докл. РАН. 2018. **481**, № 2. 136–137.
8. *Постников А.Г.* Избранные труды. М.: ФИЗМАТЛИТ, 2005.
9. *Жимбо Э.К., Чубариков В.Н.* Об асимптотическом распределении значений арифметических функций // Докл. РАН. 2001. **377**, № 2. 156–157.
10. *Бояринов Р.Н., Чубариков В.Н.* О распределении значений функций на последовательности Фибоначчи // Докл. РАН. 2001. **379**, № 1. 9–11.
11. *Колпакова О.В., Попов О.В., Чубариков В.Н.* Об одном варианте метода Адамара в теории L-функций Дирихле // Чебышёв. сб. 2019. **20**, № 3. 282–295.
12. *Архипов Г.И.* Избранные труды. Орел: Изд-во Орлов. гос. ун-та, 2013.
13. *Минеев М.П., Чубариков В.Н.* Об одном методе искажения частоты появления знаков в шифре простой замены // Докл. РАН. 2008. **420**, № 6. 736–738.
14. *Минеев М.П., Чубариков В.Н.* К вопросу об искажении частот появления знаков в шифре простой замены // Докл. РАН. 2009. **426**, № 1. 6–8.

Поступила в редакцию
04.09.2024