Доклады Академии Наук СССР
1953. Том LXXXVIII, № 4

МАТЕМАТИКА

Н. М. КОРОБОВ

РАСПРЕДЕЛЕНИЕ НЕВЫЧЕТОВ И ПЕРВООБРАЗНЫХ КОРНЕЙ В РЕКУРРЕНТНЫХ РЯДАХ

(Представлено академиком И. М. Виноградовым 4 XII 1952)

Рассмотрим функции $\psi(x)$, удовлетворяющие линейному конечно-разностному уравнению с целыми коэффициентами:

$$\psi(x) = a_1\psi(x-1) + \ldots + a_n\psi(x-n) \quad (n \geqslant 1;\ x > n;\ a_n \neq 0). \qquad (1)$$

Начальные значения $\psi(1), \ldots, \psi(n)$ предполагаем целыми, не равными одновременно нулю.

Пусть $p > n$ простое. Функцию $\psi(x)$ назовем рекуррентной функцией порядка n по модулю p, если коэффициент a_n и хотя бы одно из чисел $\psi(i)$ $(i = 1, 2, \ldots, n)$ не делится на p. Последовательность

$$\delta_1, \delta_2, \ldots, \delta_n, \ldots, \delta_x, \ldots, \qquad (2)$$

составленную из наименьших неотрицательных вычетов функции $\psi(x)$ по модулю p, назовем в этом случае рекуррентным рядом порядка n.

Легко показать, что рекуррентный ряд (2) периодичен; его наименьший период τ удовлетворяет условию $1 \leqslant \tau \leqslant p^n - 1$.

Ниже приведены некоторые теоремы, характеризующие распределение в рекуррентных рядах степенных вычетов и невычетов, а также первообразных корней и чисел, принадлежащих данному показателю. Доказательства теорем основываются на возможности получения нетривиальных оценок для тригонометрических сумм вида

$$S(\tau) = \sum_{x=1}^{\tau} e^{2\pi i \frac{\psi(x)}{p}} \quad \text{и} \quad S(N) = \sum_{x=1}^{N} e^{2\pi i \frac{\psi(x)}{p}} \qquad (N < \tau).$$

Суммы $S(\tau)$ и $S(N)$ будем называть рекуррентными суммами. Интересно отметить, что, в отличие от случая распределения невычетов и первообразных корней в натуральном ряде, где вопрос о возможности улучшения известных результатов, полученных И. М. Виноградовым, остается открытым, в случае рекуррентных рядов отдельные результаты уже не допускают существенного улучшения.

Теорема 1. *Справедливы следующие оценки рекуррентных сумм* $S(\tau)$ *и* $S(N)$:

$$\left| \sum_{x=1}^{\tau} e^{2\pi i \frac{\psi(x)}{p}} \right| \leqslant p^{\frac{n}{2}}; \quad \left| \sum_{x=1}^{N} e^{2\pi i \frac{\psi(x)}{p}} \right| \leqslant p^{\frac{n}{2}} (1 + n \ln p).$$

Доказательство. Пусть a — целое из интервала $0 \leqslant a \leqslant \tau - 1$. Рассмотрим сумму

$$S_a = \sum_{x=1}^{\tau} e^{2\pi i \left(\frac{\psi(x)}{p} + \frac{ax}{\tau}\right)}.$$

Пользуясь тем, что

$$\left\{\frac{\psi(x+\tau)}{p} + \frac{a(x+\tau)}{\tau}\right\} = \left\{\frac{\psi(x)}{p} + \frac{ax}{\tau}\right\},$$

получим для любого целого $y \geqslant 0$

$$\left| \sum_{x=1}^{\tau} e^{2\pi i \left(\frac{\psi(x)}{p} + \frac{ax}{\tau}\right)} \right| = \left| \sum_{x=1}^{\tau} e^{2\pi i \left(\frac{\psi(x+y)}{p} + \frac{ax}{\tau}\right)} \right|.$$

Возведение в квадрат и суммирование по y дает:

$$\tau |S_a|^2 = \sum_{y=0}^{\tau-1} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(\frac{\psi(x+y)}{p} + \frac{ax}{\tau}\right)} \right|^2. \tag{3}$$

Обозначим через $\psi_i(x)$ $(i = 1, 2, \ldots, n)$ рекуррентные функции, удовлетворяющие уравнению (1) и определенные начальными условиями

$$\psi_i(x) = \begin{cases} 1 \text{ для } x = i, \\ 0 \text{ для } 1 \leqslant x \leqslant n, \quad x \neq i. \end{cases}$$

Легко показать, что

$$\psi(x+y) = \psi(y+1)\psi_1(x) + \ldots + \psi(y+n)\psi_n(x). \tag{4}$$

Пусть δ_y — наименьший неотрицательный вычет функции $\psi(y)$ по модулю p. В силу (3) и (4) получим:

$$\tau |S_a|^2 = \sum_{y=0}^{\tau-1} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(\frac{\delta_{y+1}\psi_1(x) + \ldots + \delta_{y+n}\psi_n(x)}{p} + \frac{ax}{\tau}\right)} \right|^2. \tag{5}$$

Будем называть системы значений $\delta_{y+1}, \ldots, \delta_{y+n}$ и $\delta_{y'+1}, \ldots, \delta_{y'+n}$ различными, если хотя бы одна из величин δ_{y+i} не равна $\delta_{y'+i}$ $(i = 1, 2, \ldots, n)$. Очевидно, что все системы $\delta_{y+i}, \ldots, \delta_{y+n}$ при $y = 0, 1, \ldots, \tau - 1$ различны. (Иначе τ не было бы наименьшим периодом по модулю p функции $\psi(x)$.)

Распространим суммирование в правой части (5) на всевозможные системы $b_1, \ldots, b_n$, где каждая из величин b_i независимо от остальных пробегает значения $0, 1, \ldots, p-1$. Тогда

$$\tau |S_a|^2 \leqslant \sum_{b_1 \ldots b_n} \left| \sum_{x=1}^{\tau} e^{2\pi i \left(\frac{b_1\psi_1(x) + \ldots + b_n\psi_n(x)}{p} + \frac{ax}{\tau}\right)} \right|^2 =$$

$$= \sum_{b_1 \ldots b_n} \sum_{x=1}^{\tau} \sum_{z=1}^{\tau} e^{2\pi i \left[\frac{b_1(\psi_1(x) - \psi_1(z)) + \ldots + b_n(\psi_n(x) - \psi_n(z))}{p} + \frac{a(x-z)}{\tau}\right]} = p^n \sum_{x,z} e^{2\pi i \frac{a(x-z)}{\tau}}.$$

Суммирование в последней сумме распространяется на значения x и z, удовлетворяющие системе сравнений:

$$\psi_1(x) \equiv \psi_1(z), \ldots, \psi_n(x) \equiv \psi_n(z) \pmod{p}, \quad 1 \leqslant x, z \leqslant \tau. \tag{6}$$

Без труда получаем (снова в связи с тем, что τ является по модулю p наименьшим периодом функции $\psi(x)$), что сравнения (6) выполняются только при $z = x$, $x = 1, 2, \ldots, \tau$. Но тогда

$$p^n \sum_{x,z} e^{2\pi i \frac{a(x-z)}{p}} = p^n \tau,$$

$$\tau |S_a|^2 \leqslant p^n \tau, \quad |S_a| \leqslant p^{\frac{n}{2}}.$$

При $a = 0$ имеем $S_0 = S(\tau)$, чем доказано первое утверждение теоремы 1. Для доказательства второго утверждения представим $S(N)$ в виде

$$S(N) = \sum_{x=1}^{N} e^{2\pi i \frac{\psi(x)}{p}} = \frac{1}{\tau} \sum_{a=0}^{\tau-1} \sum_{x=1}^{\tau} \sum_{y=1}^{N} e^{2\pi i \left(\frac{\psi(x)}{p} + a\frac{x-y}{\tau}\right)} =$$

$$= \frac{N}{\tau} \sum_{x=1}^{\tau} e^{2\pi i \frac{\psi(x)}{p}} + \frac{1}{\tau} \sum_{a=1}^{\tau-1} \left(\sum_{x=1}^{\tau} e^{2\pi i \left(\frac{\psi(x)}{p} + \frac{ax}{\tau}\right)} \right) \left(\sum_{y=1}^{N} e^{-2\pi i \frac{ay}{\tau}} \right).$$

Отсюда следует, что

$$|S(N)| \leqslant \frac{N}{\tau}|S_0| + \frac{1}{\tau}\sum_{a=1}^{\tau-1}|S_a| \cdot \left|\sum_{y=1}^{N} e^{-2\pi i \frac{ay}{\tau}}\right| \leqslant$$

$$\leqslant p^{\frac{n}{2}}\left(1 + \frac{1}{\tau}\sum_{a=1}^{\tau-1}\left|\sum_{y=1}^{N} e^{2\pi i \frac{ay}{\tau}}\right|\right) \leqslant p^{\frac{n}{2}}(1 + \ln \tau) \leqslant p^{\frac{n}{2}}(1 + n \ln p),$$

чем теорема 1 доказана полностью.

Теорема 2. *Пусть m — делитель $p-1$. Обозначим через N_m и N'_m число вычетов и, соответственно, невычетов степени m среди N соседних членов рекуррентного ряда порядка n с периодом τ. Тогда*

$$N_m = \frac{p-1}{mp}N + \theta R; \quad N'_m = \frac{(m-1)(p-1)}{mp}N + \theta' R;$$

$$0 \leqslant \theta, \theta' \leqslant 1; \quad |R| < \begin{cases} Cp^{\frac{n}{2}} & \text{при } N = \tau \\ Cnp^{\frac{n}{2}} \ln p & \text{при } N < \tau \end{cases}$$

(C — *абсолютная константа*)

Теорема 3. *Если период τ рекуррентного ряда n-го порядка больше, чем $p^{\frac{n}{2}}(\sqrt{p}+1)$, то ряд содержит невычеты* $(\mathrm{mod}\, p)$ *любой степени m ($m \mid p-1$; $1 < m < p-1$); если $\tau > p^{\frac{n}{2}}(\sqrt{p}+1) \times (1 + n \ln p)$, то невычеты степени m найдутся среди любых $N = [p^{\frac{n}{2}}(\sqrt{p}+1)(1 + n \ln p)] + 1$ соседних членов ряда.*

Теорема 4. *Каково бы ни было m, делящее $p-1$ ($1 < m < p-1$), для всякого $n \geqslant m+1$ найдется рекуррентный ряд порядка n, не содержащий невычетов степени m, с периодом $\tau = \frac{p^r - 1}{m}$, где r определяется условиями*

$$r(r+1)\ldots(r+m-1) \leqslant m!\, n < (r+1)\ldots(r+m).$$

Замечание. Из теоремы 3 при $n=3$, $m=2$ и $p>3$ следует, что рекуррентные ряды третьего порядка, период которых $\tau > p^2 + p\sqrt{p}$, содержат квадратичные невычеты. Это утверждение нельзя существенно усилить, так как, согласно теореме 4, существуют ряды третьего порядка с периодом $\tau = \frac{p^2-1}{2} > 0{,}4p^2$, не содержащие квадратичных невычетов.

Теорема 5. *Для всякого $\varepsilon > 0$ найдется $c = c(\varepsilon, n)$ такое, что для каждого из рекуррентных рядов порядка n, период которых $\tau > cp^{\frac{n+1}{2}+\varepsilon}$, среди любых $N = [cp^{\frac{n+1}{2}+\varepsilon}] + 1$ соседних членов ряда встретится первообразный корень по модулю p.*

В частности, каждый ряд третьего порядка, период которого $\tau > c(\varepsilon)p^{2+\varepsilon}$, содержит первообразные корни по модулю p.

Это утверждение также не допускает значительного усиления, так как существуют рекуррентные ряды третьего порядка с периодом $\tau > cp^2$ (см. замечание), не содержащие квадратичных невычетов, и, следовательно, не содержащие первообразных корней.

В заключение приведем две общие теоремы, из которых получаются асимптотические формулы для числа рядом стоящих вычетов или невычетов заданных степеней и числа групп чисел, принадлежащих заданным показателям.

Теорема 6. *Пусть $\alpha_1, \ldots, \alpha_k$ — произвольные целые, не делящиеся на p; $m_1, \ldots, m_k$ — любая система отличных от единицы делителей $p-1$; $\psi(x)$ — рекуррентная функция порядка $n > k$ с перио-*

дом τ; *характеристическое уравнение* $\lambda^n = a_1\lambda^{n-1} + \ldots + a_n$* *неприводимо по модулю* p.

Обозначим через $N(\alpha_1, \ldots, \alpha_k)$ *число решений системы сравнений*

$$\left.\begin{aligned} \operatorname{ind}\psi(x+1) &\equiv \operatorname{ind}\alpha_1 \pmod{m_1} \\ &\cdots\cdots\cdots\cdots \\ \operatorname{ind}\psi(x+k) &\equiv \operatorname{ind}\alpha_k \pmod{m_k} \end{aligned}\right\} \quad x = 0,\ 1, \ldots,\ N-1;\ N \leqslant \tau,$$

где индексы заданы с помощью произвольного первообразного корня по модулю p. *Тогда*

$$N(\alpha_1, \ldots, \alpha_k) = \frac{(p-1)^k}{m_1 \ldots m_k p^k} N + \theta R, \quad 0 \leqslant \theta \leqslant 1;$$

$$|R| < \begin{cases} p^{\frac{n+k}{2}} & \text{при } N = \tau, \\ p^{\frac{n+k}{2}}(1 + n\ln p) & \text{при } N < \tau. \end{cases}$$

Выбирая в этой теореме, например, $\alpha_1 = \ldots = \alpha_k = 1$, $m_1 = \ldots = m_k = m$, $N = \tau$, получим асимптотическую формулу для числа $N(1, \ldots, 1)$ содержащихся в периоде рекуррентного ряда групп из k соседних членов, являющихся вычетами степени m:

$$N(1, \ldots, 1) = \frac{(p-1)^k}{m^k p^k}\tau + \theta_1 p^{\frac{n+k}{2}}; \quad |\theta_1| \leqslant 1.$$

Теорема 7. *Пусть* $\delta_1, \ldots, \delta_k$ — *произвольная система делителей* $p-1$; $\varphi(x)$ — *функция Эйлера*; $\psi(x)$ — *рекуррентная функция порядка* $n > k$ *с периодом* τ; *уравнение* $\lambda^n = a_1\lambda^{n-1} + \ldots + a_n$ *неприводимо по модулю* p; $\gamma[\psi(x)]$ — *показатель, которому принадлежит* $\psi(x)$. *Обозначим через* $\tilde{N}(\delta_1, \ldots, \delta_k)$ *число решений системы уравнений*

$$\left.\begin{aligned} \gamma[\psi(x+1)] &= \delta_1 \\ &\cdots\cdots\cdots \\ \gamma[\psi(x+k)] &= \delta_k \end{aligned}\right\} x = 0,\ 1, \ldots,\ N-1;\ N \leqslant \tau.$$

Тогда для любого $\varepsilon > 0$ *найдется* $c(n, \varepsilon)$ *такое, что*

$$\tilde{N}(\delta_1, \ldots, \delta_k) = \frac{\varphi(\delta)\ldots\varphi(\delta_k)}{p^k} N + cp^{\frac{n+k}{2} + k\varepsilon}; \quad |c| < c(n, \varepsilon).$$

В частности, для числа групп из k соседних первообразных корней среди N последовательных членов рекуррентного ряда получим

$$\tilde{N}(p-1, \ldots, p-1) = \left(\frac{\varphi(p-1)}{p}\right)^k N + cp^{\frac{n+k}{2} + \varepsilon k} \quad (N \leqslant \tau).$$

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

Поступило
26 XI 1952

* Коэффициенты этого уравнения выбираются равными коэффициентам рекуррентного уравнения (1).