

УДК 511

МАТЕМАТИКА

В. И. НЕЧАЕВ

ТРИГОНОМЕТРИЧЕСКИЕ СУММЫ ДЛЯ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

(Представлено академиком И. М. Виноградовым 13 III 1972)

1. Обозначения. n — натуральное, p — простое число; F — конечное поле из q элементов характеристики p ; $f = f(\lambda)$ — многочлен над полем F с условием, что $f(0) \neq 0$; $\deg f$ — степень многочлена f ; $\text{per } f$ — наименьшее натуральное число m такое, что $f|\lambda^m - 1$; V_n — n -мерное векторное пространство над полем F ; θ — нулевой вектор пространства V_n ; $\alpha \cdot \beta$ — скалярное произведение векторов α и β пространства V_n ; χ — характер аддитивной группы поля F , т. е. комплексно-значная функция с условием, что

$$\chi(a + b) = \chi(a) \cdot \chi(b) \quad (1)$$

для любых элементов a и b поля F и

$$\chi(c) \neq 0 \quad (2)$$

для какого-нибудь элемента c поля F ; χ_0 — главный характер, т. е. $\chi_0(a) = 1$ для каждого элемента a поля F .

Рассматривается линейное рекуррентное уравнение

$$\delta_{x+y} = a_1 \delta_x + \dots + a_n \delta_{x+n-1}, \quad a_1, \dots, a_n \in F, \quad a_1 \neq 0, \quad (3)$$

с характеристическим многочленом

$$f = f(\lambda) = \lambda^n - a_n \lambda^{n-1} - \dots - a_1.$$

Пусть $d_0, \dots, d_{n-1}$ — какие-угодно элементы поля F . Легко видеть, что существует и только одна двусторонняя последовательность $\delta = \{\delta_x\}_x = \{\delta_x\}_{x=-\infty}^{+\infty}$ элементов поля F , которая удовлетворяет уравнению (3) и для которой

$$\delta_0 = d_0, \dots, \delta_{n-1} = d_{n-1}.$$

Решения уравнения (3), отличающиеся одно от другого только сдвигом, мы не будем считать различными. Множество всех решений уравнения (3) мы будем обозначать символом $\mathcal{L}(f)$. Известно, что любое решение уравнения (3) — периодическая последовательность. Прimitивный период решения δ мы будем обозначать символом $\text{per } \delta$, а сумму

$$\sum_{x=1}^{\tau} \chi(\delta_x),$$

где $\tau = \text{per } \delta$, — символом $\sigma(\delta)$. Нетрудно заметить, что $\sigma(\delta)$ — аналог полной тригонометрической суммы для последовательности, удовлетворяющей линейному рекуррентному сравнению по модулю p с целочисленными коэффициентами.

В настоящей заметке доказывается, что

$$\sum_{\delta \in \mathcal{L}(f)} \frac{|\sigma(\delta)|^2}{\text{per } \delta} = \frac{q^{\deg f}}{\text{per } f} \quad (4)$$

и даже несколько более общее соотношение.

Пусть $q = p \geq 3$, $n = \deg f$, f — неприводимый над полем F многочлен с условием $\text{per } f = \frac{1}{2}(p^n - 1) = t$. Как известно ⁽¹⁾, уравнение (3) в этом случае имеет два ненулевых решения $\delta^{(1)}$ и $\delta^{(2)}$ периода t , и поэтому после несложных выкладок из тождества (4) получается равенство, найденное ранее ⁽²⁾ Н. М. Коробовым,

$$|\sigma(\delta^{(1)})|^2 + |\sigma(\delta^{(2)})|^2 = \frac{1}{2}(p^n + 1).$$

Из тождества (4) можно получать и другие следствия. Пусть, например, f — степень неприводимого над полем F многочлена $p(\lambda)$. В таком случае множество $\mathcal{L}^*(f)$ всех решений уравнения (3) с максимальным примитивным периодом, равным $\text{per } f$, есть теоретико-множественная разность $\mathcal{L}(f) \setminus \mathcal{L}(f/p(\lambda))$. Поэтому из тождества (4) получаем следующее равенство:

$$\frac{1}{\text{per } f} \sum_{\delta \in \mathcal{L}^*(f)} |\sigma(\delta)|^2 = \frac{q^{\deg f}}{\text{per } f} - \frac{q^{\deg f - \deg p(\lambda)}}{\text{per } f/p(\lambda)}.$$

2. Введем далее следующие обозначения: $t = \text{per } f$; δ — любое решение уравнения (3); $\delta^{(j)}$, $0 \leq j \leq k$, — все различные решения уравнения (3); $\tau_j = \text{per } \delta^{(j)}$; $\rho^{(j)}$, $0 \leq j \leq n-1$, — решения уравнения (3), определяемые из условий:

$$\rho_x^{(j)} = \begin{cases} 1, & \text{если } x = j, \\ 0, & \text{если } x \neq j \text{ и } 0 \leq x \leq n-1; \end{cases}$$

$\Delta_x, \Delta_x^{(j)}, \beta_x$ — n -мерные векторы вида

$$\Delta_x = \begin{pmatrix} \delta_x \\ \vdots \\ \delta_{x+n-1} \end{pmatrix}, \quad \Delta_x^{(j)} = \begin{pmatrix} \delta_x^{(j)} \\ \vdots \\ \delta_{x+n-1}^{(j)} \end{pmatrix}, \quad \beta_x = \begin{pmatrix} \rho_x^{(0)} \\ \vdots \\ \rho_x^{(n-1)} \end{pmatrix};$$

A и B — квадратные матрицы порядка n вида

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, \quad B = \begin{pmatrix} \rho_1^{(0)} & \dots & \rho_n^{(0)} \\ \rho_1^{(1)} & \dots & \rho_n^{(1)} \\ \vdots & \vdots & \vdots \\ \rho_1^{(n-1)} & \dots & \rho_n^{(n-1)} \end{pmatrix};$$

B^T — матрица, транспонированная относительно матрицы B .

Очевидна

Л е м м а 1. Множество

$$\{\Delta_x^{(j)} \mid 0 \leq j \leq k, 0 \leq x < \tau_j\}$$

суть множество всех векторов пространства V_n .

Из теории линейных рекуррентных последовательностей ⁽¹⁾ следует, что $\text{per } \rho^{(0)} = \text{per } f$ и что примитивный период любого решения уравнения (3) — делитель $\text{per } f$. Поэтому $\text{per } \{\beta_x\}_x = t$.

Легко проверить, что,

$$\delta_{x+y} = \rho_x^{(0)} \cdot \delta_y + \dots + \rho_x^{(n-1)} \cdot \delta_{y+n-1} \quad (5)$$

для всех целых x от 0 до $n-1$, а значит, и для любых целых x и y . Из равенства (5) непосредственно следует, что

$$A \cdot \Delta_x = \Delta_{x+1}, \quad B^T \cdot \Delta_x = \Delta_{x+1}$$

для любого целого x . А так как δ — любое решение уравнения (3), то $A = B^T$ и, следовательно, матрица B , как и A , является невырожденной. Из равенства (5) следует, что

$$\rho_{1+y}^{(j)} = \rho_1^{(0)} \cdot \rho_y^{(j)} + \dots + \rho_1^{(n-1)} \cdot \rho_{y+n-1}^{(j)}$$

и что, таким образом, $B \cdot \beta_y = \beta_{y+1}$ для каждого целого y . Из этих рассуждений следует

Л е м м а 2. Для любых целых x и z

$$\beta_x = \beta_z \Leftrightarrow x \equiv z \pmod{t}.$$

Из условий (1) и (2) легко получается, что

$$\sum_{a \in F} \chi(a) = \begin{cases} q, & \text{если } \chi = \chi_0, \\ 0, & \text{если } \chi \neq \chi_0. \end{cases}$$

Поэтому для любого неглавного характера χ имеем:

$$\sum_{a \in F} \chi(ac) = \begin{cases} q, & \text{если } c = 0; \\ 0, & \text{если } c \in F \text{ и } c \neq 0. \end{cases}$$

Отсюда и из очевидного равенства

$$\sum_{a_1, \dots, a_n \in F} \chi(a_1 c_1 + \dots + a_n c_n) = \sum_{a_1 \in F} \chi(a_1 c_1) \times \dots \times \sum_{a_n \in F} \chi(a_n c_n)$$

следует

Л е м м а 3. Пусть $\gamma \in V_n$, $\chi \neq \chi_0$. Тогда

$$\sum_{\alpha \in V_n} \chi(\alpha \cdot \gamma) = \begin{cases} q^n, & \text{если } \gamma = \theta, \\ 0, & \text{если } \gamma \neq \theta. \end{cases}$$

3. Пусть теперь a целое, τ натуральное, t/τ , $e_\tau(x) = \exp\left(2\pi i \frac{x}{\tau}\right)$;

$$\begin{aligned} \sigma_{a,\tau}(\delta) &= \sum_{x=1}^{\tau} \chi(\delta_x) e_\tau(ax); \\ \sigma_{a,\tau}^{(j)} &= \sigma_{a,\tau}(\delta^{(j)}). \end{aligned}$$

Легко видеть, что

$$|\sigma_{a,\tau}^{(j)}| = \left| \sum_{x=1}^{\tau} \chi(\delta_{x+y}^{(j)}) e_\tau(ax) \right|.$$

Поэтому, воспользовавшись равенством (5), получаем

$$\tau_j |\sigma_{a,\tau}^{(j)}|^2 = \sum_{y=1}^{\tau_j} \left| \sum_{x=1}^{\tau} \chi(\beta_x \cdot \Delta_y^{(j)}) e_\tau(ax) \right|^2.$$

Далее суммируем полученное равенство по всем j и применяем лемму 1:

$$\sum_{j=0}^k \tau_j |\sigma_{a,\tau}^{(j)}|^2 = \sum_{\alpha \in V_n} \left| \sum_{x=1}^{\tau} \chi(\beta_x \cdot \alpha) e_\tau(ax) \right|^2.$$

Наконец, возвышая в квадрат и изменяя порядок суммирования, находим, что

$$\sum_{j=0}^k \tau_j |\sigma_{a,\tau}^{(j)}|^2 = \sum_{x=1}^{\tau} \sum_{z=1}^{\tau} e_\tau(a(x-z)) \sum_{\alpha \in V_n} \chi((\beta_x - \beta_z) \cdot \alpha).$$

Отсюда и из лемм 2 и 3 следует

Теорема. Пусть χ — неглавный характер аддитивной группы поля F ; $t \nmid \tau$;

$$R_{a,\tau}(t) = \begin{cases} \tau^2 \cdot t^{-1}, & \text{если } \tau \nmid at, \\ 0, & \text{если } \tau \mid at. \end{cases}$$

Тогда

$$\sum_{\delta \in \mathcal{L}(f)} \text{per } \delta \cdot |\sigma_{a,\tau}(\delta)|^2 = q^n \cdot R_{a,\tau}(t).$$

Полагая в доказанном равенстве $a = 0$ и замечая, что

$$\sigma_{0,\tau}(\delta) = \frac{\tau}{\text{per } \delta} \cdot \sigma(\delta),$$

мы сразу получаем равенство (4).

4. Доказанная теорема верна и в случае, если F — произвольное коммутативное кольцо с единицей, χ — характер с условием, что $\chi(a) \neq 1$ для каждого $a \neq 0$ коэффициент a_1 уравнения (3) — обратимый элемент кольца F . Полученные результаты обобщаются для линейных рекуррентных уравнений с периодическими коэффициентами.

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

Поступило
9 III 1972

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

¹ M. Ward, Trans. Am. Math. Soc., **35**, 600 (1935). ² Н. М. Коробов, Докторская диссертация, 1953.