УДК 621.391:519.7+621.391.1:004.7

ПРИМЕНЕНИЕ СУММ ГАУССА ДЛЯ ВЫЧИСЛЕНИЯ ТОЧНЫХ ЗНАЧЕНИЙ ЧИСЛА ПОЯВЛЕНИЙ ЭЛЕМЕНТОВ ПОЛЯ НА ЦИКЛАХ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

М. М. Глухов*, О. В. Камловский**

*Московский технологический университет (МИРЭА), г. Москва, Россия
**ООО «Центр сертификационных исследований», г. Москва, Россия

Рассматривается задача получения точных значений для числа появлений элементов на циклах линейных рекуррентных последовательностей немаксимального периода над произвольными конечными полями. Для решения данной задачи применяется аппарат сумм Гаусса.

Ключевые слова: *линейные рекуррентные последовательности, суммы Гаусса, число появлений элементов на циклах.*

DOI 10.17223/20710410/36/3

APPLICATION OF GAUSS SUMS TO CALCULATE THE EXACT VALUES OF THE NUMBER OF APPEARANCES OF ELEMENTS ON CYCLES OF LINEAR RECURRENCES

M. M. Glukhov*, O. V. Kamlovskii**

*Moscow Technological University (MIREA), Moscow, Russia
**Certification Research Center, Moscow, Russia

E-mail: ov-kam@yandex.ru

Using Gauss sums, we solve the problem of obtaining the formulas for the exact values $N(z, u)$ of appearances of z among the elements $u(0)$, $u(1)$, …, $u(T-1)$ of a linear recurrence sequence (LRS) u generated by an irreducible polynomial of a degree m over a field $P = \mathrm{GF}(q)$ in the case, when the period of u is equal to $T = (q^m - 1)/d$, where $d|(p^j+1)$ for some natural number j and $p = \mathrm{char}\, P$, that is, p is a semiprimitive number modulo d. Such a sequence u is obtained from a LRS of the maximal period $q^m - 1$ by regular sampling with step d.

The results of the article generalize the formulas for $N(z, u)$ which are well-known in the case of prime q or $z = 0$. In fact, we give some formulas for $N(z, u)$ in the following cases: 1) $d = 2$; 2) $d > 2$ and $z = 0$; 3) $d > 2$, $z \neq 0$, and $d = d_1$ or $d_1 = 1$, where $d_1 = ((q^m - 1)/(q - 1), d)$; 4) $d > 2$, $z \neq 0$, $d_1 = 2$, and $d/2$ is odd or $(p^{l_1} + 1)/(d/2)$ is even, where l_1 is the least positive integer such that $(d/2) \mid (p^{l_1} + 1)$. Thus, as a corollary, we have a complete solution of the problem in the situation when d is a prime number.

Keywords: *linear recurrent sequences, Gauss sum.*

Введение

Решается задача получения точных значений частот $N(z,u)$ появлений элемента z поля $P=\mathrm{GF}(q)$ среди элементов $u(0)$, $u(1)$, …, $u(T-1)$ линейной рекуррентной последовательности (ЛРП) $u=(u(i))_{i=0}^{\infty}$ над полем P с неприводимым характеристическим многочленом $f(x)\in P[x]$ степени m и периода $T=(q^m-1)/d$ [1, 2]. На число d накладывается следующее условие: d делит p^j+1 для некоторого натурального числа j, где p — характеристика поля. В этом случае говорят, что число p *полупримитивно* по модулю d [3]. Такие последовательности u получаются в результате регулярной выборки с шагом d из ЛРП максимального периода q^m-1 [4, 5].

В [6, теоремы 6, 7] с использованием сумм Гаусса данная задача решена для случая, когда P — простое поле, т. е. $q=p$. При этом выписаны только типы распределений, но не указано значение $N(z,u)$ при каждой конкретной ЛРП u. Позже, в работе [3], задача была решена для случая, когда $z=0$, а P — произвольное поле. Полное решение рассматриваемой задачи приводится в [7, теорема 1.1], однако при доказательстве в самом начале работы автор использовал ошибочное равенство (2.3) для суммы Гаусса, которое привело к ошибочным формулам. Отметим также, что случай, когда $d=2$, а P — произвольное поле, рассмотрен в [1, теорема 23, с. 359], где выписаны только возможные типы распределений.

Цель данной работы — обобщить известные факты о частотах $N(z,u)$ и изложить доказательства в рамках одной статьи. Основными результатами являются теоремы 4, 5, 7, 8, 9, в частности, позволяющие получить полное решение поставленной задачи в ситуации, когда d — простое число.

1. Некоторые свойства характеров конечных полей

Укажем некоторые свойства характеров конечных полей и дадим необходимые определения. Доказательства приведённых результатов подробно изложены в [2].

Пусть $(G,\cdot)$ — конечная абелева группа с нейтральным элементом e. *Характером* группы G называется любой гомоморфизм χ группы G в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел. Обозначим $\hat{G}$ множество всех характеров группы G. Множество $\hat{G}$ не пусто, так как там содержится, например, характер χ_0, определённый равенствами $\chi_0(g)=1$ для всех $g\in G$. Характер χ_0 называется *тривиальным*, а все остальные характеры из множества $\hat{G}$ называются *нетривиальными*.

Зададим операцию произведения характеров, положив для любых $\chi_1,\chi_2\in\hat{G}$ $\chi_1\cdot\chi_2=\chi$, где $\chi: G\to\mathbb{C}$ и $\chi(g)=\chi_1(g)\chi_2(g)$ для всех $g\in G$. Тогда $(\hat{G},\cdot)$ — конечная абелева группа, изоморфная группе G. Обратным к характеру $\chi\in\hat{G}$ является характер $\bar{\chi}$ (*сопряжённый* к характеру χ), определённый равенством $\bar{\chi}(g)=\overline{\chi(g)}$ для всех $g\in G$, где черта означает комплексное сопряжение.

Пусть χ — произвольный нетривиальный характер конечной абелевой группы G, тогда справедливо соотношение

$$\sum_{g\in G}\chi(g)=\begin{cases}|G|, & \text{если } \chi=\chi_0,\\ 0, & \text{если } \chi\neq\chi_0.\end{cases}\tag{1}$$

Пусть H — подгруппа конечной абелевой группы G. Обозначим через A множество всех характеров χ группы G, которые удовлетворяют условию $\chi(h)=1$ для всех $h\in H$. В этом случае говорят, что характер χ *аннулирует* подгруппу H. Тогда A является подгруппой группы $\hat{G}$ и имеет место равенство

$$|A|=\frac{|G|}{|H|}.\tag{2}$$

Рассмотрим конечное поле $P = \mathrm{GF}(q)$ из q элементов, где $q = p^s$, p — простое число. С полем P связаны две абелевы группы: $(P^*, \cdot)$ — мультипликативная группа поля P и $(P, +)$ — аддитивная группа поля P. Рассмотрим характеры аддитивной группы поля P. Такие характеры будем называть *аддитивными* характерами поля P. Для каждого элемента $b \in P$ рассмотрим отображение $\chi_b : P \to \mathbb{C}^*$, осуществляемое по правилу

$$\chi_b(x) = e^{2\pi i \frac{\mathrm{tr}_p^q(bx)}{p}},$$

для всех $x \in P$, где tr_p^q — функция следа из поля P в простое подполе. Тогда группа аддитивных характеров поля P имеет вид $\{\chi_b : b \in P\}$. При $b = 0$ получим тривиальный характер χ_0, а при $b = e$ — характер χ_e, который называется *каноническим* аддитивным характером поля P.

В дальнейшем будет полезна конструкция поднятия аддитивного характера χ поля $P = \mathrm{GF}(q)$. Пусть $\chi = \chi_b$, где $b \in P$, $b \neq 0$; $Q = \mathrm{GF}(q^m)$ — расширение степени m поля P. Зададим отображение $\chi' : Q \to \mathbb{C}^*$, осуществляемое для всех $z \in Q$ по правилу

$$\chi'(z) = \chi(\mathrm{tr}_q^{q^m}(z)). \tag{3}$$

Тогда

$$\chi'(z) = e^{2\pi i \frac{\mathrm{tr}_p^{q^m}(bz)}{p}}, \quad z \in Q,$$

а значит, χ' является нетривиальным аддитивным характером поля Q. Характер χ' называется *поднятием* характера χ до поля Q. Если χ — канонический аддитивный характер поля P, то его поднятие до поля Q также будет каноническим аддитивным характером поля Q.

Рассмотрим теперь группу мультипликативных характеров поля $P = \mathrm{GF}(q)$. Группа P^* циклическая, поэтому группа мультипликативных характеров — циклическая группа, порождённая характером ψ_1, который задаётся по правилу

$$\psi_1(g^k) = e^{2\pi i \frac{k}{q-1}}, \quad k = 0, 1, \ldots, q-2,$$

где g — некоторый примитивный элемент поля P. Для всех $j \in \{0, 1, \ldots, q-2\}$ обозначим через ψ_j характер ψ_1^j, тогда группа мультипликативных характеров поля P имеет вид $\{\psi_0, \psi_1, \ldots, \psi_{q-2}\} = \langle\psi_1\rangle$. Характер ψ_0 является тривиальным.

Пусть $P = \mathrm{GF}(q)$, ψ — мультипликативный характер поля P, а χ — аддитивный характер поля P. *Сумма Гаусса* $G(\psi, \chi)$ определяется следующим равенством:

$$G(\psi, \chi) = \sum_{c \in P^*} \psi(c)\chi(c).$$

Теорема 1. Для сумм Гаусса справедливы следующие соотношения:

$$G(\psi, \chi) = \begin{cases} q-1, & \text{если } \psi = \psi_0,\ \chi = \chi_0, \\ -1, & \text{если } \psi = \psi_0,\ \chi \neq \chi_0, \\ 0, & \text{если } \psi \neq \psi_0,\ \chi = \chi_0; \end{cases}$$

если $\psi \neq \psi_0$, $\chi \neq \chi_0$, то

$$|G(\psi, \chi)| = \sqrt{q};$$

если χ — произвольный аддитивный характер поля $P = \mathrm{GF}(q)$, то для всех $c \in P^*$

$$\chi(c) = \frac{1}{q-1} \sum_{\psi} G(\bar{\psi}, \chi)\psi(c), \tag{4}$$

где суммирование осуществляется по всем мультипликативным характерам ψ поля P.

2. Сведение задачи к исследованию сумм Гаусса

Пусть $u = (u(i))_{i=0}^{\infty}$ — произвольная чисто периодическая последовательность элементов поля $P = \mathrm{GF}(q)$ периода $T(u)$. Для каждого элемента $z \in P$ обозначим через $N(z, u)$ число появлений z среди элементов $u(0)$, $u(1)$, …, $u(T(u)-1)$.

Покажем, что исследование частоты $N(z, u)$ сводится к исследованию суммы

$$\sigma_z(u) = \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{T(u)-1} \chi(cu(i)),$$

где χ — нетривиальный аддитивный характер поля P. С использованием равенства (1) и описания всех аддитивных характеров поля P получим

$$N(z, u) = \sum_{i=0}^{T(u)-1} \frac{1}{q} \sum_{c \in P} \chi(c(u(i) - z)),$$

откуда

$$N(z, u) = \frac{T(u)}{q} + \frac{\sigma_z(u)}{q}. \tag{5}$$

Для каждого элемента $z \in P$ обозначим λ_z — отображение из поля P в множество $\mathbb{C}^*$, задаваемое по правилу $\lambda_z(x) = \chi(-zx)$ для всех $x \in P$. Очевидно, что λ_z является аддитивным характером поля P.

Обозначим через $L_P(f)$ множество всех ЛРП над полем P с характеристическим многочленом $f(x)$. Приведём результаты работы [3] (см. также [2, теорема 8.84]). С целью полноты изложения дадим их доказательство в удобных для нас обозначениях. Часть фрагментов доказательства будет использоваться в дальнейшем.

Теорема 2. Пусть $f(x)$ — неприводимый многочлен степени m над полем $P = \mathrm{GF}(q)$, $f(x) \neq x$, $t = T(f) = (q^m - 1)/d$, α — корень $f(x)$ в поле $Q = \mathrm{GF}(q^m)$, u — ненулевая ЛРП из множества $L_P(f)$, имеющая представление $u(i) = \mathrm{tr}_q^{q^m}(a\alpha^i)$, $i \geqslant 0$, $a \in Q$. Тогда

$$\sigma_0(u) = -\frac{q-1}{d} + \frac{q-1}{d} \sum_{\psi' \in B \setminus \{\psi'_0\}} \psi'(a) G(\bar{\psi}', \chi'), \tag{6}$$

а при $z \neq 0$

$$\sigma_z(u) = \frac{1}{d} - \frac{1}{d} \sum_{\psi' \in B \setminus \{\psi'_0\}} \psi'(a) G(\bar{\psi}', \chi') + \frac{1}{d} \sum_{\psi' \in A \setminus B} \psi'(a) G(\bar{\psi}', \chi') G(\psi, \lambda_z), \tag{7}$$

где ψ — ограничение характера ψ' на поле P; A — группа мультипликативных характеров поля Q, аннулирующих элемент α; ψ'_0 — её нейтральный элемент; B — её подгруппа, состоящая из характеров, аннулирующих группу P^*, причём

$$|A| = \frac{q^m - 1}{t}, \quad |B| = \frac{q^m - 1}{[t, q-1]}.$$

Доказательство. Заметим, что элемент a в представлении элементов ЛРП u с использованием функции след из условия теоремы — однозначно определённый ненулевой элемент поля Q. Тогда если χ' — поднятие характера χ до поля Q, определённое равенством (3), то

$$\sigma_z(u) = \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{t-1} \chi'(ca\alpha^i).$$

С использованием соотношения (4) представим $\sigma_z(u)$ в виде

$$\sigma_z(u) = \sum_{c\in P^*} \chi(-cz) \sum_{i=0}^{t-1} \left(\frac{1}{q^m-1} \sum_{\psi'} G(\bar{\psi}', \chi')\psi'(ca\alpha^i) \right),$$

где суммирование ведётся по всем мультипликативным характерам ψ' поля Q. Изменив порядок суммирования, получим

$$\sigma_z(u) = \frac{1}{q^m-1} \sum_{c\in P^*} \chi(-cz) \sum_{\psi'} G(\bar{\psi}', \chi')\psi'(ca) \sum_{i=0}^{t-1} \psi'(\alpha^i). \tag{8}$$

Заметим, что если $\psi'(\alpha) \neq 1$, то так как $\operatorname{ord}\alpha = t$, справедливы равенства

$$\sum_{i=0}^{t-1} \psi'(\alpha^i) = \sum_{i=0}^{t-1} (\psi'(\alpha))^i = \frac{(\psi'(\alpha))^t - 1}{\psi'(\alpha) - 1} = \frac{\psi'(\alpha^t) - 1}{\psi'(\alpha) - 1} = \frac{\psi'(e) - 1}{\psi'(\alpha) - 1} = 0.$$

Таким образом, в правой части равенства (8) достаточно ограничиться суммированием по всем мультипликативным характерам ψ', для которых $\psi'(\alpha) = 1$. Значит,

$$\sigma_z(u) = \frac{t}{q^m-1} \sum_{c\in P^*} \chi(-cz) \sum_{\psi'\in A} G(\bar{\psi}', \chi')\psi'(ca).$$

Тогда

$$\sigma_z(u) = \frac{1}{d} \sum_{\psi'\in A} \psi'(a) G(\bar{\psi}', \chi') \sum_{c\in P^*} \psi'(c)\lambda_z(c) = \frac{1}{d} \sum_{\psi'\in A} \psi'(a) G(\bar{\psi}', \chi') G(\psi, \lambda_z), \tag{9}$$

где ψ — ограничение характера ψ' на поле P.

Пусть $z = 0$, тогда характер λ_z тривиален и, согласно теореме 1,

$$G(\psi, \lambda_z) = \begin{cases} q-1, & \text{если } \psi = \psi_0, \\ 0, & \text{если } \psi \neq \psi_0. \end{cases}$$

Множество B состоит из всех мультипликативных характеров ψ' поля Q, для которых выполнены соотношения $\psi'(\alpha) = 1$, $\psi'(c) = 1$ для всех $c \in P^*$. Тогда, согласно равенству (9), получим

$$\sigma_0(u) = \frac{q-1}{d} \sum_{\psi'\in B} \psi'(a) G(\bar{\psi}', \chi'). \tag{10}$$

Найдём $|B|$. Пусть θ — примитивный элемент поля P, тогда множество B состоит из всех мультипликативных характеров ψ' поля Q, для которых $\psi'(\alpha) = 1$ и $\psi'(\theta) = 1$, т. е. таких характеров, которые аннулируют группу $H = \langle \alpha, \theta \rangle$, порождённую элементами α и θ. Порядок h группы H равен $[\operatorname{ord}\alpha, q-1] = [t, q-1]$, поэтому, согласно равенству (2),

$$|B| = \frac{q^m-1}{h} = \frac{q^m-1}{[t, q-1]}.$$

Выделив в равенстве (10) отдельно слагаемое, соответствующее тривиальному характеру $\psi'_0 \in B$, и воспользовавшись теоремой 1, будем иметь

$$\sigma_0(u) + \frac{q-1}{d} = \frac{q-1}{d} \sum_{\psi'\in B\setminus\{\psi'_0\}} \psi'(a) G(\bar{\psi}', \chi').$$

Пусть теперь $z \neq 0$, тогда λ_z является нетривиальным аддитивным характером поля P и, согласно теореме 1, $G(\psi, \lambda_z) = -1$ для всех $\psi' \in B$. Тогда из равенства (9) получим

$$\sigma_z(u) = -\frac{1}{d} \sum_{\psi' \in B} \psi'(a) G(\bar{\psi}', \chi') + \frac{1}{d} \sum_{\psi' \in A \setminus B} \psi'(a) G(\bar{\psi}', \chi') G(\psi, \lambda_z).$$

Выделяя отдельно слагаемое, соответствующее тривиальному характеру ψ'_0, согласно теореме 1, получим

$$\sigma_z(u) - \frac{1}{d} = -\frac{1}{d} \sum_{\psi' \in B \setminus \{\psi'_0\}} \psi'(a) G(\bar{\psi}', \chi') + \frac{1}{d} \sum_{\psi' \in A \setminus B} \psi'(a) G(\bar{\psi}', \chi') G(\psi, \lambda_z).$$

Осталось заметить, что множество A состоит из всех мультипликативных характеров, которые аннулируют группу $\langle \alpha \rangle$, поэтому, согласно равенству (2),

$$|A| = \frac{q^m - 1}{\operatorname{ord} \alpha} = \frac{q^m - 1}{t}.$$

Теорема доказана. ■

3. Линейные рекурренты максимального периода

Приведём первый простейший случай, когда теорема 2 позволяет найти точные значения частот появлений элементов на циклах ЛРП.

Пусть $P = \mathrm{GF}(q)$, $f(x) \in P[x]$ — многочлен максимального периода $T(f) = q^m - 1$. Каждая ненулевая ЛРП $u \in L_P(f)$ является ЛРП максимального периода $T(u) = q^m - 1$. Как показано в теореме 2, в этом случае $|A| = |B| = 1$, $\sigma_0(u) = q - 1$, а при $z \neq 0$ выполнено $\sigma_z(u) = 1$. Таким образом, из равенства (5) получим хорошо известный результат [4, 5] для числа $N(z, u)$ появлений элемента $z \in P$ среди элементов $u(0)$, $u(1)$, …, $u(T(f) - 1)$:

$$N(z, u) = \begin{cases} q^{m-1} - 1, & \text{если } z = 0, \\ q^{m-1}, & \text{если } z \neq 0. \end{cases}$$

Отметим, что в работах [4, 5] для доказательства этих формул используется комбинаторный метод.

4. Линейные рекурренты периода $(q^m - 1)/2$

Пусть $P = \mathrm{GF}(q)$, где q — нечётное число, $f(x)$ — неприводимый многочлен степени m над полем P, имеющий период $T(f) = (q^m - 1)/2$. Получим точные значения для числа $N(z, u)$ появлений элемента $z \in P$ среди элементов $u(0)$, $u(1)$, …, $u(T(f) - 1)$ для всех ЛРП $u \in L_P(f)$.

Нам понадобятся некоторые дополнительные сведения о суммах Гаусса над конечными полями. Рассмотрим отображение $\eta : P^* \to \mathbb{C}^*$, определённое для всех $a \in P^*$ по правилу

$$\eta(a) = \begin{cases} 1, & \text{если } a \text{ является квадратом в поле } P, \\ -1, & \text{если } a \text{ не является квадратом в поле } P. \end{cases}$$

Отображение η является мультипликативным характером поля P, имеющим порядок 2. Характер η называется *квадратичным* мультипликативным характером поля P. Если γ — примитивный элемент поля P, то $\eta(a) = 1$ тогда и только тогда, когда

$a \in \langle\gamma^2\rangle$, где $\langle\gamma^2\rangle = H$ — группа порядка $(q-1)/2$, порождённая элементом γ^2. Согласно равенству (2), η является единственным нетривиальным характером, аннулирующим группу H. Для суммы Гаусса $G(\psi, \chi)$, где $\psi = \eta$, а χ — канонический аддитивный характер поля P, можно точно вычислить её значение.

Теорема 3 [2, теорема 5.15]. Пусть $P = \mathrm{GF}(q)$, где $q = p^s$, p — простое число, $s \in \mathbb{N}$. Тогда

$$G(\eta, \chi) = \begin{cases} (-1)^{s-1}\sqrt{q}, & \text{если } p \equiv 1 \pmod 4, \\ (-1)^{s-1} i^s \sqrt{q}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Нам понадобится несколько вспомогательных результатов.

Лемма 1. Пусть η — квадратичный характер поля $P = \mathrm{GF}(q)$, $q = p^s$, p — простое число, $s \in \mathbb{N}$, e — единица поля P. Тогда

$$\eta(-e) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod 4, \\ (-1)^s, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Доказательство. Пусть γ — примитивный элемент поля P, тогда элемент $\gamma^{(q-1)/2}$ отличен от e и является решением уравнения $x^2 = e$. Значит, $\gamma^{(q-1)/2} = -e$ и $\eta(-e) = \eta(\gamma^{(q-1)/2}) = (\eta(\gamma))^{(q-1)/2} = (-1)^{(q-1)/2}$, так как γ не является квадратом в поле P. Таким образом, $\eta(-e) = 1$ тогда и только тогда, когда $(q-1)/2$ — чётное число. Это равносильно тому, что $4 \,|\, (p^s - 1) = (p-1)(1 + p + \ldots + p^{s-1})$. Если $p \equiv 1 \pmod 4$, то данное соотношение верно для всех $s \in \mathbb{N}$. Если $p \equiv 3 \pmod 4$, то $p-1 \equiv 2 \pmod 4$, и рассматриваемое соотношение выполнено, если $2 \,|\, (1+p+\ldots+p^{s-1})$, т. е. если s — чётное число. ■

Лемма 2. Пусть η' — квадратичный характер поля $Q = \mathrm{GF}(q^m)$, где q — нечётное число, ψ — ограничение характера η' на поле $P = \mathrm{GF}(q)$. Тогда

1) если m — нечётное число, то $\psi = \eta$ — квадратичный характер поля P;
2) если m — чётное число, то $\psi = \psi_0$ — тривиальный характер поля P.

Доказательство. Пусть γ' и γ — примитивные элементы полей Q и P соответственно. Так как ψ аннулирует группу $H = \langle\gamma^2\rangle$, то из равенства (2) либо $\psi = \eta$, либо $\psi = \psi_0$. Характер η' аннулирует группу $H' = \langle(\gamma')^2\rangle$, поэтому $\psi = \psi_0$ тогда и только тогда, когда P^* — подгруппа группы H'. Это выполнено, только если $q-1$ делит $(q^m - 1)/2 = (q-1)(1 + q + \ldots + q^{m-1})/2$, т. е. если m — чётное число. ■

Докажем теорему, обобщающую на случай произвольного q результаты из [6, теорема 7], где рассматривается ситуация, когда $q = p$ — простое число.

Теорема 4. Пусть $f(x)$ — неприводимый многочлен степени $m = 2\lambda+1$ над полем $P = \mathrm{GF}(q)$, где $q = p^s$, p — нечётное простое число, $s \in \mathbb{N}$. Тогда если $T(f) = (q^m - 1)/2$ и ненулевая ЛРП $u \in L_P(f)$ имеет представление

$$u(i) = \mathrm{tr}_P^Q(a\alpha^i), \quad i \geqslant 0,$$

то

$$N(0, u) = \frac{q^{m-1} - 1}{2},$$

а если $z \neq 0$, то

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} + \eta'(az)q^{\lambda}}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{q^{m-1} + \eta'(az)(-1)^{\lambda s}q^{\lambda}}{2}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

где η' — квадратичный характер поля $Q = \mathrm{GF}(q^m)$.

Доказательство. Согласно соотношению (5), справедливо равенство

$$N(z,u) = \frac{T(u)}{q} + \frac{1}{q}\sigma_z(u),$$

где

$$\sigma_z(u) = \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{T(u)-1} \chi(cu(i)), \tag{11}$$

χ — канонический аддитивный характер поля P. Изучим величину $\sigma_z(u)$.

1) Пусть $z = 0$. Тогда из равенства (6) получим

$$\sigma_0(u) = -\frac{q-1}{2} + \frac{q-1}{2} \sum_{\psi' \in B \setminus \{\psi'_0\}} \psi'(a) G(\overline{\psi'}, \chi'), \tag{12}$$

где χ' и ψ'_0 — канонический аддитивный и тривиальный мультипликативный характеры поля Q соответственно; B — множество всех мультипликативных характеров ψ' поля Q, аннулирующих группу $\langle \alpha, \gamma \rangle$, порождённую корнем α многочлена $f(x)$ и примитивным элементом γ поля P. Так как $\psi'(\alpha) = 1$ для каждого характера $\psi' \in B$ и $|\langle \alpha \rangle| = T(f) = (q^m - 1)/2$, то из (2) либо $\psi' = \eta'$, либо $\psi' = \psi'_0$. Согласно доказательству леммы 2, число $q - 1$ не делит $(q^m - 1)/2$, а значит, $\langle \alpha \rangle \neq \langle \alpha, \gamma \rangle$. Таким образом, $\langle \alpha, \gamma \rangle = Q^*$, $B = \{\psi'_0\}$ и из равенства (12) получим

$$\sigma_0(u) = -\frac{q-1}{2}, \quad N(0,u) = \frac{T(u)}{q} + \frac{\sigma_0(u)}{q} = \frac{q^{m-1} - 1}{2}.$$

2) Пусть $z \neq 0$. Тогда из равенства (7) и соотношения $B = \{\psi'_0\}$ будем иметь

$$\sigma_z(u) = \frac{1}{2} + \frac{1}{2} \sum_{\psi' \in A \setminus \{\psi'_0\}} \psi'(a) G(\overline{\psi'}, \chi') G(\psi, \lambda_z),$$

где A — множество всех мультипликативных характеров ψ' поля Q, аннулирующих группу $\langle \alpha \rangle$; ψ — ограничение характера ψ' на поле P; λ_z — аддитивный характер поля P, определённый равенством $\lambda_z(x) = \chi(-zx)$, $x \in P$. Как отмечалось при доказательстве п. 1, элемент α аннулируется только характерами ψ'_0, η'. Значит, $A = \{\psi'_0, \eta'\}$. Поэтому с использованием леммы 2 и равенства $\overline{\eta'} = \eta'$ получим

$$\sigma_z(u) = \frac{1}{2} + \frac{1}{2}\eta'(a) G(\eta', \chi') G(\eta, \lambda_z).$$

Для суммы Гаусса $G(\eta, \lambda_z)$ имеем

$$G(\eta, \lambda_z) = \sum_{c \in P^*} \eta(c)\lambda_z(c) = \sum_{c \in P^*} \eta(c)\chi(-cz) = \sum_{b \in P^*} \eta(-bz^{-1})\chi(b) =$$
$$= \eta(-z^{-1}) G(\eta, \chi) = \eta(-e)\eta(z^{-1}) G(\eta, \chi) = \eta(-e)\eta(z) G(\eta, \chi).$$

Таким образом,

$$\sigma_z(u) = \frac{1}{2} + \frac{1}{2}\eta'(az)\eta(-e)G(\eta,\chi)G(\eta',\chi'). \tag{13}$$

Согласно теореме 3 и лемме 1,

$$\eta(-e)G(\eta,\chi) = \begin{cases} (-1)^{s-1}\sqrt{q}, & \text{если } p \equiv 1 \pmod 4, \\ -i^s\sqrt{q}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

$$G(\eta',\chi') = \begin{cases} (-1)^{ms-1}q^{m/2}, & \text{если } p \equiv 1 \pmod 4, \\ (-1)^{ms-1}i^{ms}q^{m/2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Тогда из равенства (13) получим

$$\sigma_z(u) = \begin{cases} \dfrac{1+\eta'(az)q^{(m+1)/2}}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{1+(-1)^{ms}\eta'(az)i^{(m+1)s}q^{(m+1)/2}}{2}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

а значит, согласно (11),

$$N(z,u) = \frac{T(u)}{q} + \frac{\sigma_z(u)}{q} = \begin{cases} \dfrac{q^{m-1}+\eta'(az)q^{\lambda}}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{q^{m-1}+\eta'(az)(-1)^{\lambda s}q^{\lambda}}{2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Теорема доказана. ■

Следствие 1. В условиях теоремы 4 имеют место соотношения

$$N(0,u) = \frac{q^{m-1}-1}{2}, \quad N(z,u) = \frac{q^{m-1} \pm q^{\lambda}}{2},\ z \in P^*,$$

причём у каждой ЛРП u для половины элементов $z \in P^*$ в последней формуле надо взять знак «+», а для другой половины — знак «−».

Рассмотрим теперь случай, когда m — чётное число. Следующая теорема обобщает на случай произвольного q результаты из [6, теорема 7].

Теорема 5. Пусть $f(x)$ — неприводимый многочлен степени $m = 2\lambda$ над полем $P = \mathrm{GF}(q)$, где $q = p^s$, p — нечётное простое число, $s \in \mathbb{N}$. Тогда если $T(f) = (q^m-1)/2$ и ненулевая ЛРП $u \in L_P(f)$ имеет представление $u(i) = \mathrm{tr}_P^Q(a\alpha^i)$, $i \geqslant 0$, то

$$N(0,u) = \begin{cases} \dfrac{q^{m-1}-(q-1)\eta'(a)q^{\lambda-1}-1}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{q^{m-1}-(q-1)\eta'(a)(-1)^{\lambda s}q^{\lambda-1}-1}{2}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

а если $z \neq 0$, то

$$N(z,u) = \begin{cases} \dfrac{q^{m-1}+\eta'(a)q^{\lambda-1}}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{q^{m-1}+\eta'(a)(-1)^{\lambda s}q^{\lambda-1}}{2}, & \text{если } p \equiv 3 \pmod 4, \end{cases}$$

где η' — квадратичный характер поля $Q = \mathrm{GF}(q^m)$.

Доказательство. С использованием доказательства леммы 2 при чётном m имеем P^* — подгруппа группы $\langle\alpha\rangle$, поэтому в обозначениях доказательства теоремы 4 $B = \{\psi_0', \eta'\} = A$.

1) Пусть $z = 0$. Из равенства (12) получим

$$\sigma_0(u) = -\frac{q-1}{2} + \frac{q-1}{2}\eta'(a)G(\eta', \chi'),$$

а значит, согласно теореме 3,

$$\sigma_0(u) = \begin{cases} \dfrac{-(q-1)(1+\eta'(a)q^{m/2})}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{-(q-1)(1+\eta'(a)i^{ms}q^{m/2})}{2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Тогда будем иметь

$$N(0,u) = \frac{T(u)}{q} + \frac{\sigma_0(u)}{q} = \begin{cases} \dfrac{q^{m-1} - (q-1)\eta'(a)q^{\lambda-1} - 1}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{q^{m-1} - (q-1)\eta'(a)(-1)^{\lambda s}q^{\lambda-1} - 1}{2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

2) Пусть $z \neq 0$. Из равенства (7) получим

$$\sigma_z(u) = \frac{1}{2} - \frac{1}{2}\eta'(a)G(\eta', \chi'),$$

а значит, согласно теореме 3,

$$\sigma_z(u) = \begin{cases} \dfrac{1+\eta'(a)q^{m/2}}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{1+\eta'(a)i^{ms}q^{m/2}}{2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Тогда будем иметь

$$N(z,u) = \frac{T(u)}{q} + \frac{\sigma_z(u)}{q} = \begin{cases} \dfrac{q^{m-1} + \eta'(a)q^{\lambda-1}}{2}, & \text{если } p \equiv 1 \pmod 4, \\ \dfrac{q^{m-1} + \eta'(a)(-1)^{\lambda s}q^{\lambda-1}}{2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Теорема доказана. ■

Следствие 2. В условиях теоремы 5 имеют место соотношения

$$N(0,u) = \frac{q^{m-1} \pm (q-1)q^{\lambda-1} - 1}{2}, \quad N(z,u) = \frac{q^{m-1} \mp q^{\lambda-1}}{2},\ z \in P^*,$$

причём у каждой ЛРП u все элементы $z \in P^*$ появляются одинаково часто.

5. Суммы Гаусса в полупримитивном случае

Пусть $P = \mathrm{GF}(q)$ — поле порядка $q = p^s$, где p — простое число, $s \in \mathbb{N}$, $f(x)$ — неприводимый многочлен степени m над полем P, $f(x) \neq x$. Рассмотрим ситуацию, когда $T(f) = (q^m - 1)/d$, где d — делитель числа $q^m - 1$, причём найдётся натуральное число j, такое, что $d \,|\, (p^j + 1)$.

Так как ранее был изучен случай $d = 1$ и 2, далее будем рассматривать случай $d > 2$. Найдём точные значения для числа $N(z, u)$ появлений элемента $z \in P$ среди элементов $u(0)$, $u(1)$, …, $u(T(f) - 1)$ в каждой ненулевой ЛРП $u \in L_P(f)$. Отметим, что в этом случае $T(u) = T(f)$. Нам понадобится ряд вспомогательных результатов.

Лемма 3. Пусть число p полупримитивно по модулю d, $q = p^s$, $d \,|\, (q^m - 1)$, $d > 2$ и $l = \min\{j \in \mathbb{N} : d \,|\, (p^j + 1)\}$. Тогда $2l \,|\, sm$.

Доказательство. Рассмотрим кольцо $\mathbb{Z}/d$ классов вычетов по модулю d. Из условия следует, что для класса $\beta = [p]_d$ справедливы равенства $\beta^{ms} = [1]_d$, $\beta^l = [-1]_d$, $\beta^{2l} = [1]_d$. Пусть $k = \operatorname{ord} \beta$ — мультипликативный порядок элемента β. Покажем, что $k = 2l$, тогда отсюда будет следовать, что $2l \,|\, sm$. Ясно, что $k \,|\, 2l$. Допустим, что $k < 2l$, тогда $k \leqslant l$ и из равенств $\beta^k = [1]_d$, $\beta^l = [-1]_d$ получим $\beta^k + \beta^l = \beta^k([1]_d + \beta^{l-k}) = [0]_d$. В силу обратимости элемента β отсюда будем иметь

$$\beta^{l-k} = [-1]_d. \tag{14}$$

Так как $d > 2$, то $[1]_d \neq [-1]_d$, а значит, $l - k \neq 0$. Покажем, что $k \neq 0$. В случае $k = 0$ имеем $\beta = [1]_d$, $d \,|\, (p - 1)$, $d \,|\, (p^l + 1)$, следовательно, $d \,|\, (p^l + p)$, $d \,|\, p(p^{l-1} + 1)$ и, значит, $d \,|\, (p^{l-1} + 1)$. Чтобы не получить противоречие с выбором l в условии, имеем $l = 1$, что приводит к противоречию с условием на d. Таким образом, $k \neq 0$, и в равенстве (14) получаем $0 < l - k < l$, что противоречит выбору l. ■

Доказательство следующего результата подробно изложено в [2, теорема 5.16].

Лемма 4 (теорема Штикельбергера). Пусть в условиях леммы 3 ψ — мультипликативный характер порядка d в поле $T = \mathrm{GF}(p^{2l})$, χ — канонический аддитивный характер поля T, тогда

$$G(\psi, \chi) = \begin{cases} -p^l, & \text{если } d \text{ чётно, а } \dfrac{p^l + 1}{d} \text{ нечётно,} \\ p^l, & \text{если } d \text{ нечётно или } \dfrac{p^l + 1}{d} \text{ чётно.} \end{cases}$$

Следствие 3. В условиях леммы 4 для каждого $i = 1, 2, \ldots, d - 1$

$$G(\psi^i, \chi) = \begin{cases} (-1)^i p^l, & \text{если } d \text{ чётно, а } \dfrac{p^l + 1}{d} \text{ нечётно,} \\ p^l, & \text{если } d \text{ нечётно или } \dfrac{p^l + 1}{d} \text{ чётно.} \end{cases}$$

Доказательство. Пусть $G_i = G(\psi^i, \chi)$, $d_i = \operatorname{ord} \psi^i$, где $i = 1, 2, \ldots, d - 1$. Тогда

$$d_i = \frac{d}{(d, i)}, \quad \frac{p^l + 1}{d_i} = \frac{(p^l + 1)(d, i)}{d}. \tag{15}$$

Рассмотрим несколько случаев.

1) Если d — нечётное число, то из равенств (15) получим d_i — нечётное число, $d_i \,|\, (p^l + 1)$. Тогда по лемме 4 $G_i = p^l$.

2) Если d — чётное число и $(p^l+1)/d$ — чётное число, то, согласно (15), $(p^l+1)/d_i$ — чётное число, и по лемме 4 $G_i = p^l$.
3) Если d — чётное число, а $(p^l+1)/d$ — нечётное число, то рассмотрим два случая:
   3а) если i — чётное число, то, согласно (15), $(p^l+1)/d_i$ — чётное число, и по лемме 4 $G_i = p^l$;
   3б) если i — нечётное число, то, согласно (15), $(p^l+1)/d_i$ — нечётное число, и по лемме 4 $G_i = -p^l$.

Следствие доказано. ■

Нам понадобится конструкция поднятия мультипликативного характера. Пусть $T = \mathrm{GF}(q_1)$ и $Q = \mathrm{GF}(q_2)$ — расширение степени r поля T, т. е. $q_2 = q_1^r$. Определим *норму* элемента $a \in Q^*$ над полем T следующим равенством:

$$N_{q_1}^{q_2}(a) = a \cdot a^{q_1} \cdot a^{q_1^2} \cdots a^{q_1^{r-1}} = a^{\frac{q_1^r-1}{q_1-1}} = a^{\frac{q_2-1}{q_1-1}}.$$

Так как $(N_{q_1}^{q_2}(a))^{q_1-1} = e$, таким образом определено отображение $N_{q_1}^{q_2} : Q^* \to T^*$, которое обладает следующими свойствами:

1) $N_{q_1}^{q_2}(ab) = N_{q_1}^{q_2}(a)N_{q_1}^{q_2}(b)$ для всех $a, b \in Q^*$;
2) $N_{q_1}^{q_2}$ сюръективно.

Пусть ψ — мультипликативный характер поля T. Рассмотрим отображение $\psi' : Q^* \to \mathbb{C}^*$, осуществляемое по правилу

$$\psi'(a) = \psi(N_{q_1}^{q_2}(a)), \quad a \in Q^*.$$

Из свойства 1 для нормы получим, что ψ' является мультипликативным характером поля Q. Его называют *поднятием мультипликативного характера* ψ до поля Q. Обозначим ψ_0 и ψ'_0 тривиальные мультипликативные характеры полей T и Q соответственно. Заметим, что для каждого $k \in \mathbb{N}_0$ справедливы равенства

$$(\psi')^k(a) = (\psi'(a))^k = (\psi(N_{q_1}^{q_2}(a)))^k = \psi^k(N_{q_1}^{q_2}(a)), \quad a \in Q^*. \tag{16}$$

Отсюда с учётом сюръективности отображения $N_{q_1}^{q_2}$ получим, что $(\psi')^k = \psi'_0$ тогда и только тогда, когда $\psi^k = \psi_0$. Таким образом, для порядков характеров ψ и ψ' имеем

$$\operatorname{ord}\psi = \operatorname{ord}\psi'. \tag{17}$$

Следующий результат подробно доказан в [2, теорема 5.14].

Лемма 5 (теорема Дэвенпорта — Хассе). Пусть χ — аддитивный, а ψ — мультипликативный характеры поля $T = \mathrm{GF}(q_1)$, не являющиеся одновременно тривиальными. Тогда если $Q = \mathrm{GF}(q_2)$ — расширение степени r поля T и χ', ψ' — поднятия характеров χ и ψ соответственно до поля Q, то

$$G(\psi', \chi') = (-1)^{r-1} G(\psi, \chi)^r.$$

Теорема 6. Пусть простое число p полупримитивно по модулю d, $d > 2$, $d \,|\, (q^m - 1)$, $q = p^s$ и число l выбрано так, как в лемме 3. Тогда если ψ' — мультипликативный характер поля $Q = \mathrm{GF}(q^m)$, имеющий порядок d, а χ' — канонический аддитивный характер поля Q, то для всех $i = 1, 2, \ldots, d-1$

$$G((\psi')^i, \chi') = \begin{cases} (-1)^{(i+1)r-1} q^{m/2}, & \text{если } d \text{ чётно, а } \dfrac{p^l+1}{d} \text{ нечётно,} \\ (-1)^{r-1} q^{m/2}, & \text{если } d \text{ нечётно или } \dfrac{p^l+1}{d} \text{ чётно,} \end{cases}$$

где $r = (ms)/(2l)$.

Доказательство. Из леммы 3 следует, что поле $T = GF(p^{2l})$ является подполем поля Q. Так как $d \mid (p^{2l}-1)$, в циклической группе всех мультипликативных характеров поля T есть подгруппа порядка d. Разные характеры из этой подгруппы имеют разные поднятия до поля Q, которые, согласно (17), имеют такие же порядки. Таким образом, найдётся мультипликативный характер ψ поля T, такой, что $\operatorname{ord}\psi = d$ и его поднятие до поля Q совпадает с ψ'. Кроме того, согласно (16), поднятие характера ψ^i до поля Q будет совпадать с характером $(\psi')^i$ для всех $i = 1, 2, \ldots, d-1$. Для завершения доказательства остаётся воспользоваться следствием 3 и леммой 5. ■

Лемма 6. Пусть в условиях теоремы 6 d_1 — натуральный делитель числа d, $\psi_1' = (\psi')^{d/d_1}$, γ — примитивный элемент поля Q. Тогда для каждого $a \in Q^*$:

1) $\psi_1'(a) = 1$ тогда и только тогда, когда $a \in \langle\gamma^{d_1}\rangle$;
2) $\psi_1'(a) = -1$ тогда и только тогда, когда d_1 — чётное число, $a \notin \langle\gamma^{d_1}\rangle$ и $a \in \langle\gamma^{d_1/2}\rangle$;
3) $\psi_1'(a^{-1}) = (-1)^{\varepsilon}$ для некоторого $\varepsilon \in \mathbb{N}_0$ тогда и только тогда, когда $\psi_1'(a) = (-1)^{\varepsilon}$.

Доказательство.

1) Рассмотрим группу всех мультипликативных характеров поля Q, аннулирующих подгруппу $\langle\gamma^{d_1}\rangle$ группы Q^*. Из равенства (2) следует, что её порядок равен d_1. Таким образом, группа $\langle\psi_1'\rangle$, имеющая порядок d_1, совпадает с группой всех характеров, аннулирующих группу $\langle\gamma^{d_1}\rangle$. Так как ψ_1' — её образующий, то $\psi_1'(a) = 1$ тогда и только тогда, когда $a \in \langle\gamma^{d_1}\rangle$.

2) Равенство $\psi_1'(a) = -1$ равносильно тому, что $(\psi_1'(a))^2 = \psi_1'(a^2) = 1$, а $\psi_1'(a) \neq 1$, т. е. по п. 1 $a^2 \in \langle\gamma^{d_1}\rangle$ и $a \notin \langle\gamma^{d_1}\rangle$. Если d_1 — нечётное число, то соотношение $(\psi_1'(a))^{d_1} = (-1)^{d_1} = -1$ противоречит условию $\operatorname{ord}\psi' = d$. Пусть d_1 — чётное число. Опишем все элементы $a \in Q^*$, такие, что $a^2 \in \langle\gamma^{d_1}\rangle$. Используя представление $a = \gamma^s$, где $s = 0, 1, \ldots, q^m - 2$, получим, что $\gamma^{2s} \in \langle\gamma^{d_1}\rangle$ тогда и только тогда, когда $d_1 \mid 2s$, т. е. $(d_1/2) \mid s$. Таким образом, $a = \gamma^{d_1 t/2}$, где $t = 0, 1, \ldots, (2(q^m-1)/d_1) - 1$, или $a \in \langle\gamma^{d_1/2}\rangle$.

3) Доказательство непосредственно следует из п. 1 и 2. ■

6. Полупримитивный случай. Нулевые элементы на циклах

Рассмотрим вопрос о распределении нулей на циклах ЛРП. Следующая теорема обобщает результаты [3, формулы (3.2)], где указаны только типы распределений, но не получены условия, при которых каждая конкретная ЛРП u имеет данный тип.

Теорема 7. Пусть $f(x)$ — неприводимый многочлен степени m над полем $\mathrm{GF}(q)$, $q = p^s$, p — простое число, $s \in \mathbb{N}$, $T(f) = (q^m-1)/d$, $d > 2$, число p полупримитивно по модулю d, $d_1 = ((q^m-1)/(q-1), d)$, $r = (ms)/(2l)$, где l определено в лемме 3. Тогда для каждой ненулевой ЛРП $u \in L_P(f)$, имеющей представление $u(i) = \mathrm{tr}_P^Q(a\alpha^i)$, $i \geqslant 0$, справедливо:

1) если dr/d_1 — чётное, или d — нечётное, или $(p^l+1)/d$ — чётное, то

$$N(0,u) = \begin{cases} \dfrac{q^{m-1} + (-1)^r (q-1) q^{m/2-1} - 1}{d}, & \text{если } a \notin \langle\gamma^{d_1}\rangle, \\ \dfrac{q^{m-1} + (-1)^{r-1} (q-1)(d_1-1) q^{m/2-1} - 1}{d}, & \text{если } a \in \langle\gamma^{d_1}\rangle; \end{cases}$$

2) если dr/d_1 — нечётное, d — чётное, $(p^l+1)/d$ — нечётное, то d_1 — чётное и

$$N(0,u)=\begin{cases}\dfrac{q^{m-1}+(-1)^r(q-1)q^{m/2-1}-1}{d}, & \text{если } a\in\langle\gamma^{d_1}\rangle \text{ или } a\notin\langle\gamma^{d_1/2}\rangle,\\[2ex] \dfrac{q^{m-1}+(-1)^{r-1}(q-1)(d_1-1)q^{m/2-1}-1}{d}, & \text{если } a\notin\langle\gamma^{d_1}\rangle \text{ и } a\in\langle\gamma^{d_1/2}\rangle.\end{cases}$$

Доказательство. С использованием равенства (5) получим

$$N(0,u)=\frac{T(u)}{q}+\frac{\sigma_0(u)}{q},$$

где $\sigma_0(u)=\sum\limits_{c\in P^*}\sum\limits_{i=0}^{T(f)-1}\chi(cu(i))$; χ — канонический аддитивный характер поля P. Из равенства (6) будем иметь

$$\sigma_0(u)=-\frac{q-1}{d}+\frac{q-1}{d}\sum_{\psi'\in B\setminus\{\psi'_0\}}\psi'(a)G(\overline{\psi'},\chi'),$$

где χ' и ψ'_0 — канонический аддитивный и тривиальный мультипликативный характеры поля Q соответственно; B — множество всех мультипликативных характеров ψ' поля Q, аннулирующих группу $\langle\alpha,\gamma\rangle$, порождённую корнем α многочлена $f(x)$ и примитивным элементом γ поля P. Порядок группы $\langle\alpha,\gamma\rangle$ делится на $(q^m-1)/d$, а значит, он равен $(q^m-1)/d'$, где d' — делитель d. Как показано при доказательстве теоремы 2,

$$d'=|B|=\frac{q^m-1}{[(q^m-1)/d,q-1]}=\frac{d(q^m-1)}{(q^m-1)(q-1)}((q^m-1)/d,q-1)=$$
$$=\frac{d}{q-1}((q^m-1)/d,q-1)=\frac{(q^m-1,d(q-1))}{q-1}=((q^m-1)/(q-1),d)=d_1.$$

Тогда группа B является циклической группой, порождённой характером $(\psi')^{d/d_1}=\psi'_1$, где ψ' — мультипликативный характер порядка d поля $Q=\mathrm{GF}(q^m)$. Заметим, что если характеры пробегают всю группу B, то характеры, сопряжённые к ним, также пробегают всю группу B, поэтому

$$\begin{aligned}\sigma_0(u)&=-\frac{q-1}{d}+\frac{q-1}{d}\sum_{i=1}^{d_1-1}(\psi'_1)^i(a)G(\overline{(\psi'_1)^i},\chi')=\\ &=-\frac{q-1}{d}+\frac{q-1}{d}\sum_{i=1}^{d_1-1}(\psi'_1)^i(a^{-1})G((\psi'_1)^i,\chi')=\\ &=-\frac{q-1}{d}+\frac{q-1}{d}\sum_{i=1}^{d_1-1}(\psi')^{di/d_1}(a^{-1})G((\psi')^{di/d_1},\chi').\end{aligned}\tag{18}$$

Рассмотрим два случая.

С л у ч а й 1. Пусть d — нечётное число или $(p^l+1)/d$ — чётное число. Тогда по теореме 6

$$\sigma_0(u)=-\frac{q-1}{d}+\frac{q-1}{d}\sum_{i=1}^{d_1-1}(\psi'_1)^i(a^{-1})(-1)^{r-1}q^{m/2}=\frac{q-1}{d}\left(-1+(-1)^{r-1}q^{m/2}\sum_{i=1}^{d_1-1}(\psi'_1(a^{-1}))^i\right),$$

а значит,

$$\sigma_0(u) = \frac{q-1}{d}\left(-1 + (-1)^r q^{m/2} + (-1)^{r-1} q^{m/2} \sum_{i=0}^{d_1-1} (\psi_1'(a^{-1}))^i\right). \tag{19}$$

Заметим, что

$$\sum_{i=0}^{d_1-1} (\psi_1'(a^{-1}))^i = \begin{cases} \dfrac{(\psi_1'(a^{-1}))^{d_1}-1}{\psi_1'(a^{-1})-1}, & \text{если } \psi_1'(a^{-1}) \neq 1, \\ d_1, & \text{если } \psi_1'(a^{-1}) = 1, \end{cases}$$

а так как $\operatorname{ord}\psi_1' = d_1$, то

$$\sum_{i=0}^{d_1-1} (\psi_1'(a^{-1}))^i = \begin{cases} 0, & \text{если } \psi_1'(a^{-1}) \neq 1, \\ d_1, & \text{если } \psi_1'(a^{-1}) = 1. \end{cases}$$

Тогда из равенства (19) и леммы 6 получим

$$\sigma_0(u) = \begin{cases} \dfrac{q-1}{d}\left(-1 + (-1)^r q^{m/2}\right), & \text{если } a \notin \langle\gamma^{d_1}\rangle, \\ \dfrac{q-1}{d}\left(-1 + (-1)^{r-1}(d_1-1) q^{m/2}\right), & \text{если } a \in \langle\gamma^{d_1}\rangle. \end{cases}$$

Подставляя найденные значения $\sigma_0(u)$ в равенство для частот $N(0,u)$, получим

$$N(0,u) = \frac{q^m-1}{dq} + \frac{\sigma_0(u)}{q} = \begin{cases} \dfrac{q^{m-1}-1+(-1)^r(q-1)q^{m/2-1}}{d}, & \text{если } a \notin \langle\gamma^{d_1}\rangle, \\ \dfrac{q^{m-1}-1+(-1)^{r-1}(q-1)(d_1-1)q^{m/2-1}}{d}, & \text{если } a \in \langle\gamma^{d_1}\rangle. \end{cases}$$

С л у ч а й 2. Пусть d — чётное число, $(p^l+1)/d$ — нечётное число. Из равенства (18) с использованием теоремы 6 будем иметь

$$\sigma_0(u) = \frac{q-1}{d}\left(-1 + \sum_{i=1}^{d_1-1} (\psi_1'(a^{-1}))^i (-1)^{(ki+1)r-1} q^{m/2}\right),$$

где $k = d/d_1$. Тогда

$$\sigma_0(u) = \frac{q-1}{d}\left(-1 + (-1)^{r-1} q^{m/2} \sum_{i=1}^{d_1-1} (\psi_1'(a^{-1})(-1)^{kr})^i\right),$$

и значит,

$$\sigma_0(u) = \frac{q-1}{d}\left(-1 + (-1)^r q^{m/2} + (-1)^{r-1} q^{m/2} \sum_{i=0}^{d_1-1} (\psi_1'(a^{-1})(-1)^{kr})^i\right).$$

Заметим, что

$$\sum_{i=0}^{d_1-1} (\psi_1'(a^{-1})(-1)^{kr})^i = \begin{cases} \dfrac{(\psi_1'(a^{-1})(-1)^{kr})^{d_1}-1}{\psi_1'(a^{-1})(-1)^{kr}-1}, & \text{если } \psi_1'(a^{-1}) \neq (-1)^{kr}, \\ d_1, & \text{если } \psi_1'(a^{-1}) = (-1)^{kr}. \end{cases}$$

Так как d — чётное число и $\operatorname{ord}\psi_1' = d_1$, то

$$(\psi_1'(a^{-1})(-1)^{kr})^{d_1} = (\psi_1')^{d_1}(a^{-1})(-1)^{krd_1} = (-1)^{dr} = 1,$$

поэтому

$$\sum_{i=0}^{d_1-1}(\psi_1'(a^{-1})(-1)^{kr})^i = \begin{cases} 0, & \text{если } \psi_1'(a^{-1}) \neq (-1)^{kr}, \\ d_1, & \text{если } \psi_1'(a^{-1}) = (-1)^{kr}. \end{cases}$$

Если теперь $kr = dr/d_1$ — чётное число, то ответ совпадает с ответом, полученным для случая 1. Пусть kr — нечётное число. Тогда $k = d/d_1$ — нечётное, и так как d — чётное, то d_1 — чётное число. В итоге по аналогии с доказательством случая 1 и с учётом леммы 6 получим

$$N(0,u) = \begin{cases} \dfrac{q^{m-1} - 1 + (-1)^r(q-1)q^{m/2-1}}{d}, & \text{если } a \in \langle\gamma^{d_1}\rangle \text{ или } a \notin \langle\gamma^{d_1/2}\rangle, \\ \dfrac{q^{m-1} - 1 + (-1)^{r-1}(q-1)(d_1-1)q^{m/2-1}}{d}, & \text{если } a \notin \langle\gamma^{d_1}\rangle, a \in \langle\gamma^{d_1/2}\rangle. \end{cases}$$

Теорема доказана. ■

7. Полупримитивный случай, $d = d_1$. Ненулевые элементы на циклах

Исследование частот появлений ненулевых элементов разобьём на несколько случаев. Сначала рассмотрим ситуацию, когда $d = d_1$.

Теорема 8. Пусть в условиях теоремы 7 $d = d_1$, тогда все ненулевые элементы $z \in P$ появляются в ЛРП u одинаково часто и справедливы следующие равенства:

1) если r — чётное число, или d — нечётное число, или $\dfrac{p^l+1}{d}$ — чётное число, то

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} + (-1)^{r-1}q^{m/2-1}}{d}, & \text{если } a \notin \langle\gamma^d\rangle, \\ \dfrac{q^{m-1} + (-1)^r(d-1)q^{m/2-1}}{d}, & \text{если } a \in \langle\gamma^d\rangle; \end{cases}$$

2) если r — нечётное число, d — чётное число, $\dfrac{p^l+1}{d}$ — нечётное число, то

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} + (-1)^{r-1}q^{m/2-1}}{d}, & \text{если } a \in \langle\gamma^d\rangle \text{ или } a \notin \langle\gamma^{d/2}\rangle, \\ \dfrac{q^{m-1} + (-1)^r(d-1)q^{m/2-1}}{d}, & \text{если } a \notin \langle\gamma^d\rangle \text{ и } a \in \langle\gamma^{d/2}\rangle. \end{cases}$$

В частности, если $q = p$, то $d = d_1$ и число $N(z,u)$ появлений каждого ненулевого элемента $z \in P$ удовлетворяет указанным формулам.

Доказательство. Пусть $z \in P$, $z \neq 0$, тогда из равенства (5) получим

$$N(z,u) = \frac{T(u)}{q} + \frac{\sigma_z(u)}{q},$$

где $\sigma_z(u) = \sum\limits_{c\in P^*} \chi(-cz) \sum\limits_{i=0}^{T(u)-1} \chi(cu(i))$. С использованием формулы (7) получим

$$\sigma_z(u) = \frac{1}{d}\left(1 - \sum_{\psi'\in B\setminus\{\psi'_0\}} \psi'(a)G(\overline{\psi'},\chi') + \sum_{\psi'\in A\setminus B} \psi'(a)G(\overline{\psi'},\chi')G(\psi,\lambda_z)\right),$$

где B (A) — множество всех мультипликативных характеров поля Q, аннулирующих группу $\langle\alpha, P^*\rangle$ ($\langle\alpha\rangle$). Как показано при доказательстве теоремы 7, $|B| = d_1$, а по доказательству теоремы 2 $|A| = (q^m-1)/|\langle\alpha\rangle| = d$. По условию $d = d_1$, поэтому $A = B$ и

$$\sigma_z(u) = \frac{1}{d}\left(1 - \sum_{\psi'\in B\setminus\{\psi'_0\}} \psi'(a)G(\overline{\psi'},\chi')\right).$$

Таким образом, $\sigma_z(u)$, а значит, $N(z,u)$ не зависят от элемента $z \in P^*$ и справедливо равенство

$$N(z,u) = (T(u) - N(0,u))/(q-1).$$

Подставляя в полученную формулу значения $N(0,u)$, подсчитанные в теореме 7, получим искомые равенства.

Заметим, что если $q = p$, то из соотношений

$$d \,|\, (p^l+1), \quad d \,|\, (p^l+1)(p^l-1), \quad (p^l+1)(p^l-1) \,|\, (p^m-1), \quad (p-1) \,|\, (p^l-1)$$

получим $(p-1) \,|\, (p^m-1)/d$, а значит,

$$d_1 = \frac{d((p^m-1)/d, p-1)}{p-1} = d.$$

Теорема доказана. ■

Отметим, что типы распределений, указанные в теореме 8, ранее были получены в [6, теорема 6] для случая $q = p$.

Рассмотрим наиболее интересный случай $p = 2$.

Следствие 4. Пусть $f(x)$ — неприводимый многочлен степени m над полем $P = \mathrm{GF}(2)$, $T(f) = (2^m-1)/3$, тогда $m = 2\lambda$ и для каждой ненулевой ЛРП u, имеющей представление $u(i) = \mathrm{tr}_P^Q(a\alpha^i)$, $i \geqslant 0$, где $Q = \mathrm{GF}(2^m)$, $a, \alpha \in Q$, справедливы равенства

$$N(0,u) = \begin{cases} \dfrac{2^{m-1} + (-1)^\lambda 2^{\lambda-1} - 1}{3}, & \text{если } a \text{ не является кубом в } Q, \\ \dfrac{2^{m-1} + (-1)^{\lambda-1} 2^\lambda - 1}{3}, & \text{если } a \text{ является кубом в } Q; \end{cases}$$

$$N(1,u) = \begin{cases} \dfrac{2^{m-1} + (-1)^{\lambda-1} 2^{\lambda-1}}{3}, & \text{если } a \text{ не является кубом в } Q, \\ \dfrac{2^{m-1} + (-1)^\lambda 2^\lambda}{3}, & \text{если } a \text{ является кубом в } Q. \end{cases}$$

Доказательство. Достаточно заметить, что в условиях теорем 7 и 8 $l = 1$, $s = 1$, $d = d_1 = 3$. ■

Следствие 5. Пусть $f(x)$ — неприводимый многочлен степени m над полем $P = \mathrm{GF}(2)$, $T(f) = (2^m - 1)/5$, тогда $m = 2\lambda$, λ — чётное число и для каждой ненулевой ЛРП u, имеющей представление $u(i) = \mathrm{tr}_P^Q(a\alpha^i)$, $i \geqslant 0$, где $Q = \mathrm{GF}(2^m)$, $a, \alpha \in Q$, справедливы равенства

$$N(0,u) = \begin{cases} \dfrac{2^{m-1} + (-1)^{\lambda/2} 2^{\lambda-1} - 1}{5}, & \text{если не существует } \sqrt[5]{a} \text{ в поле } Q, \\ \dfrac{2^{m-1} + (-1)^{\lambda/2-1} 2^{\lambda+1} - 1}{5}, & \text{если существует } \sqrt[5]{a} \text{ в поле } Q; \end{cases}$$

$$N(1,u) = \begin{cases} \dfrac{2^{m-1} + (-1)^{\lambda/2-1} 2^{\lambda-1}}{5}, & \text{если не существует } \sqrt[5]{a} \text{ в поле } Q, \\ \dfrac{2^{m-1} + (-1)^{\lambda/2} 2^{\lambda+1}}{5}, & \text{если существует } \sqrt[5]{a} \text{ в поле } Q. \end{cases}$$

Доказательство. Достаточно заметить, что в условиях теорем 7 и 8 $l = 2$, $s = 1$, $d = d_1 = 5$. ■

По аналогии со следствиями 4 и 5 нетрудно получить точные значения для числа элементов на цикле любой двоичной ЛРП u с неприводимым характеристическим многочленом $f(x) \in \mathrm{GF}(2)[x]$ степени m и периода $(2^m - 1)/d$, где $d = 9, 11, 13, 17$, а также для других чисел d, при которых число 2 полупримитивно по модулю d (см. таблицу таких чисел на с. 47).

8. Полупримитивный случай, $d \neq d_1$, $d_1 = 1$. Ненулевые элементы на циклах

Рассмотрим теперь частный случай, когда $d > 2$ и

$$d_1 = \left(\frac{q^m - 1}{q - 1}, d \right) = 1.$$

Согласно доказательству теоремы 7, в этой ситуации имеют место соотношения

$$\left(\frac{q^m - 1}{d}, q - 1 \right) = \frac{d_1(q-1)}{d} = \frac{q-1}{d}.$$

В дальнейшем нам понадобятся несколько вспомогательных результатов.

Лемма 7. Пусть ψ' — мультипликативный характер порядка d поля $Q = \mathrm{GF}(q^m)$, $d_1 = ((q^m - 1)/(q-1), d)$. Тогда ограничение ψ характера ψ' на поле $P = \mathrm{GF}(q)$ является мультипликативным характером порядка d/d_1.

Доказательство. Пусть ψ_1' — мультипликативный характер поля Q порядка $\operatorname{ord} \psi_1' = q^m - 1$, определённый равенствами

$$\psi_1'(\gamma^j) = e^{2\pi i (j/(q^m-1))}, \quad j = 0, 1, \ldots, q^m - 2,$$

где γ — примитивный элемент поля Q. Характер ψ' в силу равенства $\operatorname{ord} \psi' = d$ принадлежит циклической группе, порождённой характером $(\psi_1')^{(q^m-1)/d}$. Найдётся натуральное число k, такое, что $\psi' = (\psi_1')^{(q^m-1)k/d}$, причём $(d, k) = 1$. Пусть $\gamma_0 = \gamma^{(q^m-1)/(q-1)}$. Ясно, что γ_0 является примитивным элементом поля $P = \mathrm{GF}(q)$. Справедливы равенства

$$\psi(\gamma_0^j) = \psi'(\gamma_0^j) = (\psi_1')^{(q^m-1)k/d}(\gamma_0^j) = (\psi_1')^{(q^m-1)k/d}(\gamma^{(q^m-1)j/(q-1)}) = e^{2\pi i((q^m-1)/d)kj/(q-1)} = \psi(\gamma_0)^j.$$

Отсюда получим

$$\operatorname{ord}\psi = \min\left\{j \in \mathbb{N} : (q-1) \,\Big|\, \frac{q^m-1}{d}kj\right\} =$$
$$= \min\left\{j \in \mathbb{N} : \frac{q-1}{((q-1),(q^m-1)/d)} \,\Big|\, \frac{(q^m-1)/d}{((q-1),(q^m-1)/d)}kj\right\} =$$
$$= \min\left\{j \in \mathbb{N} : \frac{q-1}{((q-1),(q^m-1)/d)} \,\Big|\, kj\right\},$$

а так как $(q-1,(q^m-1)/d) = d_1(q-1)/d$, то, учитывая $(k,d)=1$, будем иметь

$$\operatorname{ord}\psi = \min\left\{j \in \mathbb{N} : \frac{d}{d_1} \,\Big|\, kj\right\} = \min\left\{j \in \mathbb{N} : \frac{d}{d_1} \,\Big|\, j\right\} = \frac{d}{d_1}.$$

Лемма доказана. ■

Лемма 8. Пусть в условиях леммы 7 $d_1 = 1$, тогда для каждого $i = 1, 2, \ldots, d-1$

$$G(\psi^i,\chi) = \begin{cases} (-1)^{(i+1)r/m-1}\sqrt{q}, & \text{если } d \text{ чётно, а } \dfrac{p^l+1}{d} \text{ нечётно,} \\ (-1)^{r/m-1}\sqrt{q}, & \text{если } d \text{ нечётно или } \dfrac{p^l+1}{d} \text{ чётно,} \end{cases}$$

где χ — канонический аддитивный характер поля P; параметры l и r определены в теореме 6.

Доказательство. Согласно лемме 7, характер ψ имеет порядок d. Число l — наименьшее из натуральных j, таких, что $d \,|\, (p^j+1)$. Из равенства $((q^m-1)/d, q-1) = (q-1)/d$ следует, что число d делит $q-1 = p^s-1$. Отсюда с использованием леммы 3 (подставляя $m=1$) получим $2l \,|\, s$. Для завершения доказательства остаётся воспользоваться теоремой 6 (применённой к случаю $m=1$). ■

Следующая лемма доказывается аналогично лемме 6.

Лемма 9. Пусть ψ' — мультипликативный характер поля Q порядка d, γ — примитивный элемент поля Q. Тогда для каждого $a \in Q^*$:

1) $\psi'(a) = 1$ тогда и только тогда, когда $a \in \langle\gamma^d\rangle$;
2) $\psi'(a) = -1$ тогда и только тогда, когда d — чётное число, $a \notin \langle\gamma^d\rangle$ и $a \in \langle\gamma^{d/2}\rangle$.

Теорема 9. Пусть в условиях теоремы 7 $d_1 = 1$, $z \neq 0$. Тогда:

1) если $r(m+1)/m$ — чётное, или d — нечётное, или $(p^l+1)/d$ — чётное, то

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} + (-1)^{r(m+1)/m}(d-1)q^{(m-1)/2}}{d}, & \text{если } -z^{-1}a \in \langle\gamma^d\rangle, \\ \dfrac{q^{m-1} - (-1)^{r(m+1)/m}q^{(m-1)/2}}{d}, & \text{если } -z^{-1}a \notin \langle\gamma^d\rangle; \end{cases}$$

2) если $r(m+1)/m$ — нечётное, d — чётное, $(p^l+1)/d$ — нечётное, то

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} - (d-1)q^{(m-1)/2}}{d}, & \text{если } -az^{-1} \notin \langle\gamma^d\rangle \text{ и } -az^{-1} \in \langle\gamma^{d/2}\rangle, \\ \dfrac{q^{m-1} + q^{(m-1)/2}}{d}, & \text{если } -az^{-1} \in \langle\gamma^d\rangle \text{ или } -az^{-1} \notin \langle\gamma^{d/2}\rangle. \end{cases}$$

Доказательство. С использованием равенства (5) и теоремы 2 получим

$$|B| = d_1 = 1, \quad N(z,u) = \frac{T(u)}{q} + \frac{\sigma_z(u)}{q},$$

где

$$\sigma_z(u) = \frac{1}{d} + \frac{1}{d}\sum_{\psi' \in A\setminus\{\psi'_0\}} \psi'(a)G(\overline{\psi'},\chi')G(\psi,\lambda_z) = \frac{1}{d} + \frac{1}{d}\sum_{\psi' \in A\setminus\{\psi'_0\}} \overline{\psi'(a)}G(\psi',\chi')G(\bar{\psi},\lambda_z).$$

Рассмотрим два случая.

С л у ч а й 1. Пусть d — нечётное число или $(p^l+1)/d$ — чётное число. Тогда по теореме 6

$$\sigma_z(u) = \frac{1}{d} + \frac{1}{d}\sum_{i=1}^{d-1} (\bar{\psi}')^i(a)G((\psi')^i,\chi')G(\bar{\psi}^i,\lambda_z) =$$

$$= \frac{1}{d} + \frac{1}{d}\sum_{i=1}^{d-1} (\bar{\psi}')^i(a)(-1)^{r-1}q^{m/2}G(\bar{\psi}^i,\lambda_z) = \frac{1}{d} + \frac{1}{d}(-1)^{r-1}q^{m/2}\sum_{i=1}^{d-1} (\psi')^i(a)G(\psi^i,\lambda_z),$$

где ψ' — мультипликативный характер порядка d поля Q. Для суммы Гаусса $G(\psi^i,\lambda_z)$ имеем

$$G(\psi^i,\lambda_z) = \sum_{x\in P^*} \psi^i(x)\chi(-zx) = \sum_{y\in P^*} \psi^i(-z^{-1}y)\chi(y) = \psi^i(-z^{-1})G(\psi^i,\chi).$$

Поэтому с использованием леммы 8 получим

$$\sigma_z(u) = \frac{1}{d} + \frac{1}{d}(-1)^{r-1}q^{m/2}(-1)^{r/m-1}\sqrt{q}\sum_{i=1}^{d-1} (\psi')^i(a)\psi^i(-z^{-1}) =$$

$$= \frac{1}{d} + \frac{1}{d}(-1)^{r(m+1)/m}q^{(m+1)/2}\sum_{i=1}^{d-1} (\psi')^i(-z^{-1}a).$$

Остаётся вычислить сумму

$$\sum_{i=1}^{d-1} (\psi')^i(-z^{-1}a) = -1 + \sum_{i=0}^{d-1} (\psi')^i(-z^{-1}a) = \begin{cases} d-1, & \text{если } \psi'(-z^{-1}a) = 1, \\ -1, & \text{если } \psi'(-z^{-1}a) \neq 1, \end{cases}$$

которая, согласно лемме 9, принимает вид

$$\sum_{i=1}^{d-1} (\psi')^i(-z^{-1}a) = \begin{cases} d-1, & \text{если } -z^{-1}a \in \langle\gamma^d\rangle, \\ -1, & \text{если } -z^{-1}a \notin \langle\gamma^d\rangle. \end{cases}$$

Таким образом,

$$\sigma_z(u) = \begin{cases} \dfrac{1}{d} + \dfrac{1}{d}(-1)^{r(m+1)/m}q^{(m+1)/2}(d-1), & \text{если } -z^{-1}a \in \langle\gamma^d\rangle, \\ \dfrac{1}{d} - \dfrac{1}{d}(-1)^{r(m+1)/m}q^{(m+1)/2}, & \text{если } -z^{-1}a \notin \langle\gamma^d\rangle, \end{cases}$$

и значит,

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} + (-1)^{r(m+1)/m}(d-1)q^{(m-1)/2}}{d}, & \text{если } -z^{-1}a \in \langle\gamma^d\rangle, \\ \dfrac{q^{m-1} - (-1)^{r(m+1)/m}q^{(m-1)/2}}{d}, & \text{если } -z^{-1}a \notin \langle\gamma^d\rangle. \end{cases}$$

С л у ч а й 2. Пусть d — чётное число, $(p^l+1)/d$ — нечётное число. С использованием теоремы 6 получим

$$\sigma_z(u) = \frac{1}{d} + \frac{1}{d}\sum_{i=1}^{d-1} (\bar{\psi}')^i(a)G((\psi')^i, \chi')G(\bar{\psi}^i, \lambda_z) =$$

$$= \frac{1}{d} + \frac{1}{d}\sum_{i=1}^{d-1} (\bar{\psi}')^i(a)(-1)^{(i+1)r-1}q^{m/2}G(\bar{\psi}^i, \lambda_z) = \frac{1}{d} + \frac{q^{m/2}}{d}\sum_{i=1}^{d-1} (\psi')^i(a)(-1)^{(i+1)r-1}G(\psi^i, \lambda_z).$$

По аналогии с доказательством случая 1, используя лемму 8, будем иметь

$$\sigma_z(u) = \frac{1}{d} + \frac{q^{(m+1)/2}}{d}\sum_{i=1}^{d-1} (\psi')^i(a)(-1)^{(i+1)r-1}\psi^i(-z^{-1})(-1)^{(i+1)r/m-1} =$$

$$= \frac{1}{d} + \frac{q^{(m+1)/2}}{d}\sum_{i=1}^{d-1} (\psi')^i(-z^{-1}a)(-1)^{(i+1)(m+1)r/m} =$$

$$= \frac{1}{d} + \frac{(-1)^{(m+1)r/m}q^{(m+1)/2}}{d}\sum_{i=1}^{d-1} (\psi')^i(-z^{-1}a)(-1)^{i(m+1)r/m}.$$

Рассмотрим два подслучая:

2а) Если число $\dfrac{(m+1)r}{m} = \dfrac{(m+1)s}{2l}$ чётно, то по аналогии со случаем 1 получим

$$N(z,u) = \frac{T(u)}{q} + \frac{\sigma_z(u)}{q} = \begin{cases} \dfrac{q^{m-1} + (d-1)q^{(m-1)/2}}{d}, & \text{если } -z^{-1}a \in \langle\gamma^d\rangle, \\ \dfrac{q^{m-1} - q^{(m-1)/2}}{d}, & \text{если } -z^{-1}a \notin \langle\gamma^d\rangle. \end{cases}$$

2б) Если число $\dfrac{(m+1)r}{m} = \dfrac{(m+1)s}{2l}$ нечётно, то по аналогии со случаем 1 получим

$$\sigma_z(u) = \frac{1}{d} - \frac{q^{(m+1)/2}}{d}\sum_{i=1}^{d-1} (\psi')^i(-z^{-1}a)(-1)^i =$$

$$= \frac{1}{d} - \frac{q^{(m+1)/2}}{d} \cdot \begin{cases} d-1, & \text{если } \psi'(-z^{-1}a) = -1, \\ -1, & \text{если } \psi'(-z^{-1}a) \neq -1 \end{cases} =$$

$$= \begin{cases} \dfrac{1}{d} - \dfrac{q^{(m+1)/2}(d-1)}{d}, & \text{если } -az^{-1} \notin \langle\gamma^d\rangle \text{ и } -az^{-1} \in \langle\gamma^{d/2}\rangle, \\ \dfrac{1}{d} + \dfrac{q^{(m+1)/2}}{d}, & \text{если } -az^{-1} \in \langle\gamma^d\rangle \text{ или } -az^{-1} \notin \langle\gamma^{d/2}\rangle. \end{cases}$$

Таким образом,

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} - (d-1)q^{(m-1)/2}}{d}, & \text{если } -az^{-1} \notin \langle\gamma^d\rangle \text{ и } -az^{-1} \in \langle\gamma^{d/2}\rangle, \\ \dfrac{q^{m-1} + q^{(m-1)/2}}{d}, & \text{если } -az^{-1} \in \langle\gamma^d\rangle \text{ или } -az^{-1} \notin \langle\gamma^{d/2}\rangle. \end{cases}$$

Теорема доказана. ■

Заметим, что теоремы 8 и 9 позволяют найти точные значения частот $N(z,u)$, $z \neq 0$, в каждой ЛРП u периода $T(u) = (q^m-1)/d$, где $d > 2$, d — произвольное простое число,

такое, что p полупримитивно по модулю d (в этом случае $d_1 = 1$ или $d_1 = d$). Кроме того, напомним, что теорема 7 описывает частоты $N(0, u)$ при каждом не обязательно простом числе d.

Приведём несколько наиболее интересных следствий из полученных результатов. Пусть u — ЛРП порядка m периода $T(u) = (2^{8m} - 1)/3$ над полем $\mathrm{GF}(2^8)$. Нетрудно видеть, что 3 делит $2^{8m} - 1$ при всех $m \in \mathbb{N}$, при этом

$$d_1 = \left(\frac{2^{8m} - 1}{2^8 - 1}, 3\right) = \begin{cases} 3, & \text{если 3 делит } m, \\ 1, & \text{если 3 не делит } m. \end{cases}$$

Каждая регулярная выборка из ЛРП максимального периода $2^{8m} - 1$ с шагом выбора 3 приведёт к рассматриваемой последовательности u [4].

Следствие 6. Пусть $f(x)$ — неприводимый многочлен степени m над полем $P = \mathrm{GF}(q) = \mathrm{GF}(2^8)$, $T(f) = (2^{8m} - 1)/3$, тогда для каждой ненулевой ЛРП u, имеющей представление $u(i) = \mathrm{tr}_P^Q(a\alpha^i)$, $i \geqslant 0$, где $Q = \mathrm{GF}(2^{8m})$, $a, \alpha \in Q$, справедливы следующие равенства:

1) если m кратно 3, то

$$N(0, u) = \begin{cases} \dfrac{q^{m-1} + (q-1)q^{m/2-1} - 1}{3}, & \text{если } a \text{ не является кубом в } Q, \\ \dfrac{q^{m-1} - 2(q-1)q^{m/2-1} - 1}{3}, & \text{если } a \text{ является кубом в } Q; \end{cases}$$

для $z \neq 0$

$$N(z, u) = \begin{cases} \dfrac{q^{m-1} - q^{m/2-1}}{3}, & \text{если } a \text{ не является кубом в } Q, \\ \dfrac{q^{m-1} + 2q^{m/2-1}}{3}, & \text{если } a \text{ является кубом в } Q; \end{cases}$$

2) если m не кратно 3, то $N(0, u) = \dfrac{q^{m-1} - 1}{3}$; для $z \neq 0$

$$N(z, u) = \begin{cases} \dfrac{q^{m-1} + 2q^{(m-1)/2}}{3}, & \text{если } z^{-1}a \text{ является кубом в } Q, \\ \dfrac{q^{m-1} - q^{(m-1)/2}}{3}, & \text{если } z^{-1}a \text{ не является кубом в } Q. \end{cases}$$

Доказательство. Достаточно заметить, что в условиях теорем 7–9 $d = 3$, $l = 1$, $s = 8$, $r = 4m$. ■

Пусть u — ЛРП порядка m периода $T(u) = (2^{8m} - 1)/5$ над полем $\mathrm{GF}(2^8)$. Нетрудно видеть, что 5 делит $2^{8m} - 1$ при всех $m \in \mathbb{N}$, при этом

$$d_1 = \left(\frac{2^{8m} - 1}{2^8 - 1}, 5\right) = \begin{cases} 5, & \text{если 5 делит } m, \\ 1, & \text{если 5 не делит } m. \end{cases}$$

Каждая регулярная выборка из ЛРП максимального периода $2^{8m} - 1$ с шагом выбора 5 приведёт к рассматриваемой последовательности u [4].

Следствие 7. Пусть $f(x)$ — неприводимый многочлен степени m над полем $P = \mathrm{GF}(q) = \mathrm{GF}(2^8)$, $T(f) = (2^{8m} - 1)/5$, тогда для каждой ненулевой ЛРП u, имеющей

представление $u(i) = \mathrm{tr}_P^Q(a\alpha^i)$, $i \geqslant 0$, где $Q = \mathrm{GF}(2^{8m})$, $a, \alpha \in Q$, справедливы следующие равенства:

1) если m кратно 5, то

$$N(0,u) = \begin{cases} \dfrac{q^{m-1} + (q-1)q^{m/2-1} - 1}{5}, & \text{если } a \text{ не является корнем пятой степени в } Q, \\ \dfrac{q^{m-1} - 4(q-1)q^{m/2-1} - 1}{5}, & \text{если } a \text{ является корнем пятой степени в } Q; \end{cases}$$

для $z \neq 0$

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} - q^{m/2-1}}{5}, & \text{если } a \text{ не является корнем пятой степени в } Q, \\ \dfrac{q^{m-1} + 4q^{m/2-1}}{5}, & \text{если } a \text{ является корнем пятой степени в } Q; \end{cases}$$

2) если m не кратно 5, то $N(0,u) = \dfrac{q^{m-1} - 1}{5}$; для $z \neq 0$

$$N(z,u) = \begin{cases} \dfrac{q^{m-1} + 4q^{(m-1)/2}}{5}, & \text{если } z^{-1}a \text{ является корнем пятой степени в } Q, \\ \dfrac{q^{m-1} - q^{(m-1)/2}}{5}, & \text{если } z^{-1}a \text{ не является корнем пятой степени в } Q. \end{cases}$$

Доказательство. Достаточно заметить, что в условиях теорем 7–9 $d = 5$, $l = 2$, $s = 8$, $r = 2m$. ■

Приведём таблицы небольших модулей, по которым полупримитивны простые числа 2, 3, 5, 7. При этом будем использовать введённые в лемме 3 обозначения d и l.

$p = 2$

d	3	5	9	11	13	17	19	25	27	29	33	37	41	43	53	57
l	1	2	3	5	6	4	9	10	9	14	5	18	10	7	26	9

$p = 3$

d	4	5	7	10	14	17	19	25	28	29	31	34	37	38	41	43
l	1	2	3	2	3	8	9	10	3	14	15	8	9	9	4	21

$p = 5$

d	3	6	7	9	13	14	17	18	21	23	26	27	29	34	37	41
l	1	1	3	3	2	3	8	3	3	11	2	9	7	8	18	10

$p = 7$

d	4	5	8	10	11	13	17	22	23	25	26	34	41	43	44	46
l	1	2	1	2	5	6	8	5	11	2	6	8	20	3	5	11

9. Полупримитивный случай, $d \neq d_1$, $d_1 \neq 1$. Ненулевые элементы на циклах

Сначала рассмотрим частный случай, когда $d > 2$ и

$$d_1 = \left(\frac{q^m - 1}{q - 1}, d\right) = 2.$$

В этом случае, очевидно, подразумевается, что d чётно, $q = p^s$ нечётно и m чётно.

Лемма 10. В условиях теоремы 7 при $d > 2$ и $d_1 = \left(\dfrac{q^m - 1}{q - 1}, d\right) = 2$ для любого ненулевого элемента $z \in \mathrm{GF}(q)$ справедливо равенство

$$\sigma_z(u) = \frac{1}{d} + \frac{1}{d}\sum_{i=1}^{d-1} \bar{\psi}'^i(a) G(\psi'^i, \chi') G(\bar{\psi}^i, \lambda_z).$$

Доказательство. Для доказательства рассмотрим отдельно каждую из сумм равенства (7):

$$\sigma_z(u) = \frac{1}{d} - \frac{1}{d}\sum_{\psi' \in B\setminus\{\psi'_0\}} \psi'(a)G(\bar{\psi}', \chi') + \frac{1}{d}\sum_{\psi' \in A\setminus B} \psi'(a)G(\bar{\psi}', \chi')G(\psi, \lambda_z).$$

В рассматриваемом случае группа B есть группа $\langle \psi'^{d/2} \rangle$, где ψ' — мультипликативный характер порядка d поля $Q = \mathrm{GF}(q^m)$. Тогда первую сумму можно переписать следующим образом:

$$W = \sum_{\psi'' \in B\setminus\{\psi'_0\}} \psi''(a)G(\bar{\psi}'', \chi') = \psi'^{d/2}(a)G(\bar{\psi}'^{d/2}, \chi') = \eta'(a)G(\eta', \chi'),$$

где η' — квадратичный характер поля Q. Теперь по теореме 3 имеем

$$W = \begin{cases} -\eta'(a)q^{m/2}, & \text{если } p \equiv 1 \pmod 4, \\ -\eta'(a)(-1)^{sm/2}q^{m/2}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Вторую сумму равенства (7) перепишем следующим образом:

$$V = \sum_{\psi'' \in A\setminus B} \psi''(a)G(\bar{\psi}'', \chi')G(\psi, \lambda_z) = \sum_{i=1}^{d-1} \bar{\psi}'^i(a)G(\psi'^i, \chi')G(\bar{\psi}^i, \lambda_z) - W \cdot G(\psi^{d/2}, \lambda_z),$$

где ψ — ограничение характера ψ' на поле P.

По лемме 2 $\psi^{d/2} = \psi_0$ и, значит, $G(\psi^{\frac{d}{2}}, \lambda_z) = -1$. Таким образом,

$$V = \sum_{i=1}^{d-1} \bar{\psi}'^i(a)G(\psi'^i, \chi')G(\bar{\psi}^i, \lambda_z) + W$$

и

$$\begin{aligned}\sigma_z(u) &= \frac{1}{d} - \frac{1}{d}W + \frac{1}{d}\left(\sum_{i=1}^{d-1} \bar{\psi}'^i(a)G(\psi'^i, \chi')G(\bar{\psi}^i, \lambda_z) + W\right) = \\ &= \frac{1}{d} + \frac{1}{d}\sum_{i=1}^{d-1} \bar{\psi}'^i(a)G(\psi'^i, \chi')G(\bar{\psi}^i, \lambda_z).\end{aligned}$$

Лемма доказана. ■

Далее, воспользуемся идеей доказательства теоремы 9, в которой подсчитано значение суммы $\sigma_z(u)$ при условии, что порядок характера ψ есть d (а в нашем случае, согласно лемме 7, $d/2$), и докажем справедливость следующей теоремы.

Теорема 10. Пусть в условиях теоремы 7 $d > 2$, $d_1 = \left(\dfrac{q^m - 1}{q - 1}, d\right) = 2$, l_1 — наименьшее натуральное число, такое, что $\dfrac{d}{2} \Big| (p^{l_1} + 1)$, $r_1 = \dfrac{ms}{2l_1}$. Тогда:

1) если $\dfrac{p^l + 1}{d}$ чётно, то

$$\sigma_z(u) = \begin{cases} \dfrac{1}{d} + \dfrac{1}{d}(-1)^r q^{(m+1)/2} \displaystyle\sum_{i=1}^{d-1} (-1)^{(i+1)r_1/m} \psi'^i(-z^{-1}a), \text{если } d/2 \text{ чётно, а } \dfrac{p^{l_1}+1}{d/2} \text{ нечётно}, \\ \dfrac{1}{d} + \dfrac{1}{d}(-1)^{r+r_1/m} q^{(m+1)/2} \displaystyle\sum_{i=1}^{d-1} \psi'^i(-z^{-1}a), \text{если } d/2 \text{ нечётно или } \dfrac{p^{l_1}+1}{d/2} \text{ чётно}; \end{cases}$$

2) если $d/2$ нечётно или $\dfrac{p^{l_1}+1}{d/2}$ чётно, то

$$\sigma_z(u)=\begin{cases}\dfrac{1}{d}+\dfrac{1}{d}(-1)^{r+r_1/m}q^{(m+1)/2}(d-1), & \text{если } \psi'(-z^{-1}a)=1,\\ \dfrac{1}{d}-\dfrac{1}{d}(-1)^{r+r_1/m}q^{(m+1)/2}, & \text{если } \psi'(-z^{-1}a)\neq 1.\end{cases}$$

Доказательство. Напомним, что $G(\psi^i,\lambda_z)=\psi^i(-z^{-1})G(\psi^i,\chi)$ и $\left(\dfrac{q^m-1}{q-1},d\right)=2$. Из последнего равенства следует, что либо $d|(q-1)$, либо, если это не так, то $\dfrac{d}{2}\Big|(q-1)$ и, значит, $d|(q^2-1)$.

Рассмотрим случай $d|(q-1)$. Согласно теореме 6, для каждого $i=1,2,\ldots,d-1$

$$G(\psi^i,\chi)=\begin{cases}(-1)^{(i+1)r_1/m-1}\sqrt{q}, & \text{если } d/2 \text{ чётно, а } \dfrac{p^{l_1}+1}{d/2} \text{ нечётно},\\ (-1)^{r_1/m-1}\sqrt{q}, & \text{если } d/2 \text{ нечётно или } \dfrac{p^{l_1}+1}{d/2} \text{ чётно};\end{cases}$$

$$G(\psi'^i,\chi')=\begin{cases}(-1)^{(i+1)r-1}q^{m/2}, & \text{если } \dfrac{p^l+1}{d} \text{ нечётно},\\ (-1)^{r-1}q^{m/2}, & \text{если } \dfrac{p^l+1}{d} \text{ чётно}.\end{cases}$$

Тогда если $\dfrac{p^l+1}{d}$ чётно, то

$$\sigma_z(u)=\frac{1}{d}+\frac{1}{d}\sum_{i=1}^{d-1}\bar{\psi}'^i(a)(-1)^{r-1}q^{m/2}G(\bar{\psi}^i,\lambda_z)=\frac{1}{d}+\frac{1}{d}(-1)^{r-1}q^{m/2}\sum_{i=1}^{d-1}\psi'^i(a)G(\psi^i,\lambda_z)=$$

$$=\frac{1}{d}+\frac{1}{d}(-1)^{r-1}q^{m/2}\sum_{i=1}^{d-1}\psi'^i(a)\psi^i(-z^{-1})G(\psi^i,\chi)=$$

$$=\begin{cases}\dfrac{1}{d}+\dfrac{1}{d}(-1)^{r}q^{(m+1)/2}\sum\limits_{i=1}^{d-1}(-1)^{(i+1)r_1/m}\psi'^i(-z^{-1}a), & \text{если } d/2 \text{ чётно, а } \dfrac{p^{l_1}+1}{d/2} \text{ нечётно},\\ \dfrac{1}{d}+\dfrac{1}{d}(-1)^{r+r_1/m}q^{(m+1)/2}\sum\limits_{i=1}^{d-1}\psi'^i(-z^{-1}a), & \text{если } d/2 \text{ нечётно или } \dfrac{p^{l_1}+1}{d/2} \text{ чётно}.\end{cases}$$

Во втором случае, когда $d/2$ нечётно или $\dfrac{p^{l_1}+1}{d/2}$ чётно, получим

$$\sigma_z(u)=\begin{cases}\dfrac{1}{d}+\dfrac{1}{d}(-1)^{r+r_1/m}q^{(m+1)/2}(d-1), & \text{если } \psi'(-z^{-1}a)=1,\\ \dfrac{1}{d}-\dfrac{1}{d}(-1)^{r+r_1/m}q^{(m+1)/2}, & \text{если } \psi'(-z^{-1}a)\neq 1.\end{cases}$$

Теорема доказана. ■

Следствие 8. В условиях теоремы 10 при нечётном $d/2$ или чётном $\dfrac{p^{l_1}+1}{d/2}$ для любого ненулевого элемента поля z справедливо

$$N(z,u)=\begin{cases}\dfrac{q^{m-1}+(-1)^{r+r_1/m}q^{(m-1)/2}(d-1)}{d}, & \text{если } -z^{-1}a\in\langle\gamma^d\rangle,\\ \dfrac{q^{m-1}-(-1)^{r+r_1/m}q^{(m-1)/2}}{d}, & \text{если } -z^{-1}a\notin\langle\gamma^d\rangle.\end{cases}$$

ЛИТЕРАТУРА

1. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: учебник. Т. 2. М.: Гелиос АРВ, 2003. 416 с.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
3. *McEliece R. J.* Irreducible cyclic codes and Gauss sums // Combinatorics. 1975. P. 185–202.
4. *Цирлер Н.* Линейные возвратные последовательности // Кибернетический сборник. 1963. № 6. С. 55–79.
5. *Лаксов Д.* Линейные рекуррентные последовательности над конечными полями // Математика. Сборник переводов. 1967. Т. 11. № 6. С. 145–158.
6. *Baumert L. D. and McEliece R. J.* Weights of irreducible cyclic codes // Information and Control. 1972. V. 20. P. 158–175.
7. *Nelubin A. S.* Distribution of elements on cycles of linear recurrences over Galois fields // Formal Power Series and Algebraic Combinatorics. 12-th Intern. Conf. FPSAC. Moscow, 2000. P. 534–542.

REFERENCES

1. *Glukhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra [Algebra], vol. 2. Moscow, Gelios ARV Publ., 2003. 416 p. (in Russian)
2. *Lidl R. and Niederreiter H.* Finite Fields. Addison-Wesley Publ., 1983.
3. *McEliece R. J.* Irreducible cyclic codes and Gauss sums. Combinatorics, 1975, pp. 185–202.
4. *Tsirler N.* Lineynye vozvratnye posledovatel'nosti [Linear recurrence sequences]. Kiberneticheskiy Sbornik, 1963, no. 6, pp. 55–79. (in Russian)
5. *Laksov D.* Lineynye rekurrentnye posledovatel'nosti nad konechnymi polyami [Linear recurring sequences over finite fields]. Matematika. Sbornik perevodov, 1967, vol. 11, no. 6, pp. 145–158. (in Russian)
6. *Baumert L. D. and McEliece R. J.* Weights of irreducible cyclic codes. Information and Control, 1972, vol. 20, pp. 158–175.
7. *Nelubin A. S.* Distribution of elements on cycles of linear recurrences over Galois fields. Formal Power Series and Algebraic Combinatorics. 12-th Intern. Conf. FPSAC, Moscow, 2000, pp. 534–542.