С. В. Востоков, П. М. Винник

ВЫЧИСЛЕНИЕ ЧИСЛА ПРЕДСТАВЛЕНИЙ ЭЛЕМЕНТОВ ПОЛЯ $GF(p)$ В ВИДЕ СУММЫ l-ЫХ СТЕПЕНЕЙ

1. Введение. Настоящая работа является обобщением работы [1] на случай представления элементов суммами произвольных степеней, а не суммами квадратов. Используемые методы и полученные результаты, в целом, аналогичны методам и результатам [1], однако появляется своя специфика, связанная с тем, что вещественное квадратичное расширение поля $\mathbb{Q}$ заменяется расширениями поля $\mathbb{Q}$ большей степени, которые являются подрасширениями максимального вещественного подполя $\mathbb{Q}(\zeta_p)^+$ кругового поля $\mathbb{Q}(\zeta_p)$.

Итак, пусть заданы $l > 1$, p – простое число, такое что $p \equiv 1 \mod l$, натуральное $k \geqslant 2$. Через $R = \mathbb{F}_p^{*l}$ обозначается подгруппа l-степеней мультипликативной группы поля. Для любого $b \in \mathbb{F}_p$ обозначим через t_b число наборов $(\alpha_a)_{a\in R}$, таких что $\alpha_a \in \{0, 1, \dots, k-1\}$ и $\sum\limits_{a\in R} \alpha_a a = b$. Очевидно, что если $c \in bR$, то $t_c = t_b$, то есть t_b зависит только от класса смежности bR в $\mathbb{F}_p$. Через r, $n_2, \dots, n_1$, z будет обозначаться t_b, если $b \in R$, $b \in N_2, \dots, b \in N_l$, $b = 0$ соответственно ($N_2, \dots, N_l$ – это классы смежности невычетов l-ой степени). Полагаем

$$A = z + r\sum_{a\in R}\zeta_p^a + n_2\sum_{a\in N_2}\zeta_p^a + \ldots + n_l\sum_{a\in N_l}\zeta_p^a.$$

$$F = \mathbb{Q}\left(\sum_{a\in R}\zeta_p^a\right);$$

$$L = \mathbb{Q}(\zeta_p)^+;$$

$$\varkappa = \min(k \mod p, -k \mod p).$$

2. Пусть $p = 1 + 2lm$ для некоторого $m \in \mathbb{N}$ (это заведомо так для нечетного l).

Теорема 1.

1) *Если* $k \equiv 0 \mod p$, *то* $r = n_2 = \ldots = n_l = z$.

2) *Если* k *– вычет* l*-ой степени по модулю* p, *то* $r = n_2 = \ldots = n_l = z - 1$.

3) *Если* k *– невычет* l*-ой степени по модулю* p, *то тогда* $N_{L/F}(\xi_\varkappa^2) = A$, *где* $\xi_\varkappa = \zeta_p^{\frac{1-\varkappa}{2}}(1 + \zeta_p + \ldots + \zeta_p^{\varkappa-1})$ *– одна из образующих группы* C_+ *круговых единиц поля* L.

Доказательство. В точности как в [1], рассмотрим алгебру $\mathbb{Q}[x]/(x^p - 1)$ и гомоморфизм

$$\sigma : \mathbb{Q}[x]/(x^p - 1) \to \mathbb{Q}(\zeta_p), \quad \left(\text{где} \quad \zeta_p = e^{\frac{2\pi i}{p}}\right),$$

такой, что $\sigma(x) = \zeta_p$.

Представим

$$T = \prod_{a \in R} \left(1 + x^a + \ldots + x^{(k-1)a}\right) \in \mathbb{Q}[x]/(x^p - 1)$$

в виде многочлена $t_0 + t_1 x + \ldots + t_{p-1}x^{p-1}$ степени не выше $p - 1$. Тогда t_b для $b = 0, 1, \ldots, p - 1$ будут совпадать с теми, которые мы ввели в пункте 1. Пусть $\sigma(T)$ – образ T при гомоморфизме σ. Тогда, с одной стороны,

$$\sigma(T) = A.$$

С другой сторны,

$$\sigma(T) = \prod_{a \in R} \left(1 + \zeta_p^a + \ldots + \zeta_p^{(k-1)a}\right) = \prod_{a \in R} \frac{1 - \zeta_p^{ka}}{1 - \zeta_p^a}.$$

Легко проверить, что $\sigma(T) = 0, 1$ для случаев 1), 2) теоремы 1. В случае 3) согласно [2, Лемма 8.1]

$$\xi_i = \zeta_p^{\frac{1-i}{2}} \left(1 + \zeta_p + \ldots + \zeta_p^{i-1}\right)$$

при $1 < i < \frac{p}{2}$ и -1 являются образующими группы C_+ поля $L = \mathbb{Q}(\zeta_p)+$. Так как -1 является вычетом, то $(1 < \varkappa < \frac{p}{2})$

$$\xi_\varkappa^2 = \big(\zeta^{-\frac{(\varkappa-1)}{2}} + \zeta^{-\frac{(\varkappa-1)}{2}+1} + \ldots + \zeta^{-\frac{(\varkappa-1)}{2}-1} + \zeta^{\frac{(\varkappa-1)}{2}}\big)^2 =$$
$$= \varkappa + (\varkappa-1)(\zeta_p + \zeta_p^{-1}) + (\varkappa-2)(\zeta_p^2 + \zeta_p^{-2}) + \ldots +$$
$$+2\big(\zeta_p^{(\varkappa-2)} + \zeta_p^{-(\varkappa-2)}\big) + \big(\zeta_p^{(\varkappa-1)} + \zeta_p^{-(\varkappa-1)}\big) =$$
$$= \big(1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{(\varkappa-1)}\big)\big(1 + \zeta_p^{-1} + \zeta_p^{-2} + \ldots + \zeta_p^{-(\varkappa-1)}\big) =$$
$$= \frac{1-\zeta_p^k}{1-\zeta_p} \cdot \frac{1-\zeta_p^{-k}}{1-\zeta_p^{-1}}.$$

Элементы $\zeta_p^{ai} + \zeta_p^{-ai}$ и $\zeta_p^{bi} + \zeta_p^{-bi}$ для a, $b \in R/\pm 1$ и любого i сопряжены над F. Поэтому

$$N_{L/F}(\xi_\varkappa^2) = \prod_{a \in R/\pm 1} \left(\frac{1-\zeta_p^{ak}}{1-\zeta_p} \cdot \frac{1-\zeta_p^{-ak}}{1-\zeta_p^{-a}} \right) = \prod_{a \in R} \left(\frac{1-\zeta_p^{ak}}{1-\zeta_p^{a}} \right) = A.$$

3. Пусть теперь $l = 2^\alpha l_0$, где $(l_0, 2) = 1$, $\alpha \geqslant 1$, $p = 1 + lm$, $(m, 2) = 1$, $m > 1$.

Теорема 2.

1) *Если* $k \equiv 0 \mod p$, *то* $r = n_2 = \ldots = n_l = z$.

2) *Если* k – *вычет* l-*ой степени по модулю* p, *то* $r = n_2 = \ldots = n_l = z - 1$.

3) *Если* k – *невычет* l-*ой степени, но вычет* $2^{\alpha-1}l_0$-*ой степени по модулю* p, *то* $r = n_2 = \ldots = n_l = z + 1$.

4) *Если* k – *невычет* $2^{\alpha-1}l_0$-*ой степени по модулю* p, *то тогда* $N_{L/F_1}(\xi_\varkappa^2) = A^2$, *где* $\xi_\varkappa = \zeta_p^{\frac{1-\varkappa}{2}}(1 + \zeta_p + \ldots + \zeta_p^{\varkappa-1})$ – *одна из образующих группы* C_+ *круговых единиц поля* $L\ F_1 = \mathbb{Q}(\sum_{a \in R_1} \xi_p^a)$, *где* R_1 – *подгруппа вычетов степени* $2^{\alpha-1}l_0$.

Доказательство. Действуя как в теореме 1, немедленно имеем $\sigma(T) = 0; 1$ в случаях 1) и 2) соответственно. Очевидно, что в условиях теоремы – 1 является невычетом l-ой степени, но вычетом $2^{\alpha-1}l_0$-ой степени по модулю p. Поэтому в случае 3 имеем:

$$\sigma(T) = \prod_{a\in R}\left(\frac{1-\zeta_p^{ak}}{1-\zeta_p}\right) = \prod_{a\in R}\left(\frac{1-\zeta_p^{-(-ak)}}{1-\zeta_p}\right) =$$

так как $-k$ – вычет l-ой степени, то

$$= \frac{\prod\limits_{(-ka)\in R}(1-\frac{1}{\zeta_p^{-ak}})}{\prod\limits_{a\in R}(1-\zeta_p^a)} = \frac{\prod\limits_{b\in R}(\zeta_p^b-1)}{\prod\limits_{a\in R}(1-\zeta_p^a)\prod\limits_{b\in R}(\zeta_p^b)} =$$

$$= \frac{(-1)^{\operatorname{card} R}}{\prod\limits_{a\in R}(\zeta_p^b)} = \frac{(-1)^{\frac{p-1}{l}}}{\zeta_p^{\sum\limits_{b\in R} b}}.$$

Так как

$$\sum_{i=1}^{p-1} i^l = l\cdot\sum_{b\in R} b,$$

и так как

$$p \mid \sum_{i=1}^{p-1} i^l$$

по теореме Штаудта, то в случае 3 окончательно имеем: $\sigma(T) = = (-1)^{\frac{p-1}{l}} = -1$.

В случае 4 пусть

$$A_1 = \prod_{\substack{a-\text{вычет}\\ 2^{\alpha-1}l_0\,\text{степени}}} \frac{1-\zeta_p^{ka}}{1-\zeta_p^a} =$$

$$= \prod_{\substack{a-\text{вычет}\\ 2^{\alpha}l_0\,\text{степени}}} \frac{1-\zeta_p^{ka}}{1-\zeta_p^a}\cdot \prod_{\substack{b-\text{невычет}\\ 2^{\alpha}l_0\,\text{степени,}\\ \text{но вычет}\,2^{\alpha-1}l_0-\text{степени}}} \frac{1-\zeta_p^{kb}}{1-\zeta_p^b} =$$

$$= \prod_{\substack{a-\text{вычет}\\ 2^{\alpha}l_0\,\text{степени}}} \frac{1-\zeta_p^{ka}}{1-\zeta_p^a}\cdot \prod_{\substack{-b-\text{вычет}\\ 2^{\alpha}l_0\,\text{степени}}} \frac{1-\zeta_p^{-k(-b)}}{1-\zeta_p^{-(-b)}} = A^2.$$

Так как $p = 1 + 2\cdot(2^{\alpha-1}l_0)m$, то по теореме 1

$$A_1 = N_{L/F_1}(\xi_\varkappa^2).$$

Таким образом, $N_{L/F_1}(\xi_\varkappa^2) = A^2$.

Замечание. Если

$$A(k) = \sigma(T(k)) = \prod_{\substack{a-\text{вычет} \\ 2^\alpha l_0 \text{ степени}}} \frac{1-\zeta_p^{ka}}{1-\zeta_p^a},$$

то $A(k) = -A(-k)$.

Замечание. Поскольку общее количество сумм для различных $b \in \mathbb{Z}/p\mathbb{Z}$ равно $k^{\frac{p-1}{2}}$, то имеет место равенство $z + \frac{p-1}{l}(r + n_2 + \ldots + n_i) = k^{\frac{p-1}{l}}$. Отсюда и из равенств теорем 1 и 2 легко находятся $r, n_2, \ldots, n_l$ и z.

Литература

1. Г. В. Абрамов, П. М. Винник, *Вычисление числа представлений элементов кольца $\mathbb{Z}/d\mathbb{Z}$ в виде суммы квадратов.* — Зап. научн. семин. ПОМИ **227** (1995), 5–8.
2. L. C. Washington, *Introduction to cyclotomic fields.* New York 1982.

Vostokov S. V., Vinnik P. M. The numbers of representations of elements of GF(p) as sums of lth degrees

The numbers of representations of elements of the field GF(p) as sums of invertible l degrees are calculated in this paper under the condition that each l degree occurs in the sum less than k times. The problem reduces to some calculations in cyclotomic fields. The results obtained are formulated in elementary form.

С.-Петербургский государственный университет

Балтийский государственный технический университет

Поступило 20 февраля 1997 г.