ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК АРМЕНИИ

Том 94 1993 № 2

МАТЕМАТИКА

УДК 512.62

Г. Р. Варшамов

Об одном классе операторов в конечных полях

(Представлено 2/IV 1992)

Пусть F_q — конечное поле характеристики p ($q = p^s$), $F_q[x]$ — кольцо многочленов над F_q, t — натуральное число, не делящееся на p, $f(x) = a(x^t)$ — многочлен[*] степени $n \geqslant 1$ над полем F_q, и пусть

$$a(x)^{p-1} = \sum_{u=0}^{p-1} x^{p-u-1} a_u(x)^p. \qquad (1)$$

Определим последовательность $b_0, b_1, \ldots$, элементов кольца следующим образом:

$$b_v = x^p a_u(x^t), \quad v \geqslant 0,$$

где u — наименьший неотрицательный вычет выражения $t^{-1}(v+1)-1$ по модулю p и $\rho = [p^{-1}v] + [p^{-1}t(p-u-1)]$.

В кольце многочленов $F_q[x]$ введем в рассмотрение класс квазилинейных операторов $A_0, A_1, \ldots, A_{p-1}$. Будем считать, что над многочленом $g(x) \in F_q[x]$ произведена операция A_v ($0 \leqslant v \leqslant p-1$), и писать $g(x)A_v$, если

$$g(x)A_v = \sum_u g_u^{(v)} b_{u+v}, \qquad g(x) = \sum_u g_u x^u,$$

По определению для любого натурального числа k

$$\prod_{i=0}^{k} A_{v_i} = \left(\prod_{i=0}^{k-1} A_{v_i}\right) A_{v_k} \qquad (0 \leqslant v_i \leqslant p-1) \text{ и } A_v^0 = E,$$

где E — единичный оператор.

Если $g(x)$, $s(x)$, $\alpha(x)$ и $\beta(x) \in F_q(x)$, то

$$(a(x)^p g(x) + \beta(x)^p s(x))A_v = a(x)(g(x)A_v) + \beta(x)(s(x)A_v). \qquad (2)$$

Если $b_{p-1} = \beta^{p-1}$ и m — натуральное число, то

$$1 \cdot A_{p-1}^m = x^{p^m-1} A_0^m = \beta^{(p^m-1)p^{1-m}}. \qquad (3)$$

---

[*] Все рассматриваемые в статье многочлены предполагаются нормированными.

Рассмотрим последовательность многочленов S_m^u над полем F_q, удовлетворяющую рекуррентному соотношению

$$S_m^u = S_{m-1}^u A^{s-1} + S_{m-1}^{u-1} A_1, \quad 1 \leqslant u \leqslant m, \tag{4}$$

где $S_m^0 = 1 \cdot A_0^{(m-1)s+1}$ $(S_0^0 A_0^{s-1} = 1)$ и $S_{m-1}^m = 0$.

Пусть многочлен $f(x)$ сепарабельный и пусть

$$S_m^u(\xi) = S_m^u A_0^{s-1} - (-1)^u \xi, \quad 0 \leqslant u \leqslant m, \tag{5}$$

где ξ — произвольный элемент поля F_q.

В этих обозначениях справедлива

Теорема 1. *Для любых m, u и ξ многочлен $S_m^u(\xi)$ степени меньше n делится на все неприводимые делители $f(x)$ степени m, коэффициенты при переменной x^{m-u} которых равны ξ.*

Замечание 1. Аналогичное утверждение имеет место также и для функции $l_m^u(\xi)$, где

$$l_m^0(1) = S_m^0 A_0^{s-1} - 1 \cdot A_{p-1}^{ms}, \quad 1 \leqslant m, \tag{6}$$

$$l_m^u(\xi) = S_m^u - (-1)^u \xi^{1/p} S_m^0, \quad 1 \leqslant u \leqslant m.$$

Из теоремы 1 вытекает ряд интересных следствий. Так, например,

Лемма 1. *Для любых m и ξ многочлен $S_m^1(\xi)$ степени меньше n делится на все неприводимые делители $f(x)$, степени m_i которых делят число m, а их первые коэффициенты* a_i удовлетворяют условию $m_i^{-1} \cdot m a_i = \xi$.*

Замечание 2. Равенство $S_m^1(\xi) = 0$ означает, что степени всех неприводимых делителей многочлена $f(x)$ делят число m.

Пусть $S_m = (l_m^0(1), f(x))$ и $\lambda_m = L_m^{-1} S_m$, где $L_m = \prod_{\substack{u \mid m \\ u \neq m}} \lambda_u$.

Тогда

Лемма 2. *Для любого натурального числа m многочлен S_m (соответственно λ_m) суть произведения всех** простых делителей $f(x)$, степень которых делит число m (соответственно равно числу m).*

Лемма 3. *Для того чтобы многочлен $f(x)$ был неприводим над полем F_q, необходимо и достаточно, чтобы $l_n^0(1) = 0$ и $S_d = 1$, где d — любой собственный делитель n.*

---

* Первым коэффициентом многочлена степени m будем называть его коэффициент при переменной x^{m-1}.

** За исключением разве лишь одночлена x.

Пусть N — натуральное число, $N = \sum_{u=0}^{k} k_u p^u$, где $0 \leqslant k_u < p-1$ и пусть $B_N = 1 \cdot \sum_{l=0}^{k} A_{k_l}$.

Теорема 2. *Многочлен* $\omega_N = B_N - 1 \cdot A_0^{k+1}$ *делится на все неприводимые делители* $f(x)$, *периоды которых делят число* N.

Пусть $\bar{\omega}_v = (\omega_v, f(x))$ и $\Delta_N = \bar{L}_v^{-1} \bar{\omega}_v$, где $\bar{L}_v = \prod_{\substack{u \mid v \\ u \neq v}} \Delta_u$ и $\bar{L}_1 = 1$.

Тогда

Лемма 4. *Многочлен* ω_N (*соответственно* Δ_N) *суть произведение всех неприводимых делителей* $f(x)$, *периоды которых делят число* N (*соответственно равны числу* N).

Пусть $\theta_m \neq \text{const}$ некоторый произвольный делитель многочлена λ_m и пусть

$$\theta_m^u = (\theta_m^{u-1}, S_m^u(\xi_u)), \qquad 1 \leqslant u \leqslant m, \tag{7}$$

где $\theta_m^0 = \theta_m$ и ξ_u — некоторый элемент поля F_q, выбранный так, чтобы выполнялось условие $\theta_m^u \neq \text{const}$. Тогда

Теорема 3. *Всегда найдется целое неотрицательное число* $\delta < m$ *такое, что* $\deg \theta_m^\delta = m$, *и многочлен* θ_m^δ *не будет разлагаться в* $F_q[x]$.

Пусть многочлен $a(x)$ является неприводимым над полем F_q и пусть $t \mid T^{-1}(q^m - 1)$ и $(t_l, T) > 1$, где $T = \operatorname{ord} a(x)$ и t_l — любой простой делитель t, тогда будет иметь место

Лемма 5. *Период многочлена* θ_m^δ *степени* m (*здесь* $m = n$) *равен* T.

Если условие $(t_l, T) > 1$ не выполняется, то взяв в равенстве (7) в качестве функции $\theta_m = \theta_m^0$ любой нетривиальный делитель многочлена Δ_N, где $N = tT$, мы вновь получим результат, аналогичный лемме 5. А поэтому

Следствие. Если $t = T^{-1}(q^n - 1)$, то многочлен θ_n^0 степени n является примитивным многочленом над полем F_q.

В качестве иллюстрации рассмотрим два примера

Пример 1. Пусть дан сепарабельный трехчлен $f_q(n; x) = x^{q^n+1} + ax + \beta$ ($t = 1$) над полем F_q. Требуется определить степени всех его неприводимых делителей.

Имеем

$$f(n; x)^{p-1} = ((x^{q^n+1} + ax) + \beta)^{p-1} =$$

$$= \sum_{u=0}^{p-1} x^{p-u-1} \left(\beta^u C_{p-1}^u \sum_{v=0}^{p-u-1} a^v C_{p-u-1}^v x^{q^n(p-1-u-v)} \right),$$

откуда в силу (1) находим

$$a_u(x) = \beta_1^u \sum_{v=0}^{p-u-1} \alpha^{v/p} C_{p-u-1}^v x^{p^{ns-1}(p-1-u-v)} \qquad (8)$$

и в частности

$$a_0(x) = \sum_{v=0}^{p-1} \alpha_1^v x^{q^n-(v+1)p^{ns-1}},$$

где $\beta_i = -\beta^{1/p^i}$ и $\alpha_i = -\alpha^{1/p^i}$.

Вычислим вначале значение функции $1 \cdot A_0^m$ для $m = 1, 2, \ldots, sn$.

При $m = 1$ получим

$$1 \cdot A_0 = a_0(x) = \sum_{v=0}^{p-1} \alpha_1^v x^{q^n-(v+1)p^{ns-1}}.$$

Далее для $m \geqslant 2$, согласно (2), находим

$$1 \cdot A_0^2 = (1 \cdot A_0) A_0 = \left(\sum_{v=0}^{p-1} \alpha_1^v x^{q^n-(v+1)p^{ns-1}} \right)^{1/p} a_0(x) = \sum_{v=0}^{p^2-1} \alpha_2^v x^{q^n-(v+1)p^{ns-2}},$$

$$1 \cdot A_0^3 = (1 \cdot A_0^2) A_0 = \sum_{v=0}^{p^3-1} \alpha_3^v x^{q^n-(v+1)p^{ns-3}}$$

и т. д.

$$1 \cdot A_s^{ns} = \sum_{v=0}^{q^n-1} \alpha_{ns}^v x^{q^n-v-1} = \sum_{v=0}^{p^{ns}-1} \alpha_0^{pv} x^{q^n-(v+1)p} \sum_{u=0}^{p-1} \alpha_0^u x^{p-u-1}$$

ввиду $\alpha_{ns} = \alpha_0$.

Продолжая этот процесс, получим

$$1 \cdot A_0^{ns+1} = \left[\left(\sum_{v=0}^{p^{ns}-1} \alpha_0^v x^{p^{ns}-v-1} \right)^p \sum_{u=0}^{p-1} \alpha_0^u x^{p-u-1} \right] A_0 =$$

$$= \sum_{v=0}^{p^{ns}-1} \alpha_0^v x^{p^{ns-1}-v-1} \sum_{u=0}^{p-1} \alpha_1^u a_{p-u-1}(x).$$

Но, в силу (8),

$$\sum_{u=0}^{p-1} \alpha_1^u a_{p-u-1}(x) = \sum_{u=0}^{p-1} \alpha_1 \beta^{p-u-1} \sum_{v=0}^{u} \alpha^{v/p} C_u^v x^{p^{ns-1}(u-v)} =$$

$$= \sum_{u=0}^{p-1} \alpha_1 \beta^{p-u-1} x^{up^{sn-1}} \sum_{v=0}^{p-1} \alpha_1^v \beta_1^{-v} \alpha^{v/p} C_{u+v}^v. \qquad (9)$$

Если теперь потребовать, чтобы выполнялось условие $\alpha_1 \beta_1 \alpha^{1/p} = 1$ (т. е. $\beta = \alpha^2$), то внутренняя сумма, стоящая в правой части (9), поскольку $\sum_{v=0}^{p-u-1} C_{v+u}^v = C_p^{u+1}$, будет сравнима с нулем по модулю p для всех $u < p-1$ и равна 1 при $u = p-1$. Следовательно,

$$\sum_{u=0}^{p-1} \alpha_1^u a_{p-u-1}(x) = \alpha_1^{p-1} x^{q^n-p^{ns-1}}$$

$$1 \cdot A_0^{ns} = a_1^{p-1} \sum_{v=0}^{p^{ns}-1} a_0^v x^{q^n-v-1}.$$

Рассуждая подобным образом, мы получим

$$1 \cdot A_0^{ns+2} = (a_1 a_2)^{p-1} \sum_{v=0}^{p^{ns-2}-1} a_0^v x^{q^n-v-1}$$

$$1 \cdot A_0^{ns+3} = (a_1 a_2 a_3)^{p-1} \sum_{v=0}^{p^{ns-3}-1} a_0^v x^{q^n-v-1}$$

и т. д.

$$1 \cdot A_0^{2ns} = (a_1 a_2, \ldots, a_{ns})_a^{p-1} \sum_{v=0}^{0} x^{q^n-v-1} = x^{q^n-1} \qquad (10)$$

поскольку $(a_1 a_2, \ldots, a_{ns})^{p-} = \alpha^{\frac{q^n-1}{q^n}} = 1$.

Опираясь на (10) и используя (3), найдем

$$1 \cdot A_{p-1}^{n,s} = 1 \cdot A_0^{3ns} = \beta^{\frac{q^n-1}{q^n}} = 1$$

и, согласно (6), $\overline{e}_{3n}^{0}(1) = 0$. А это, в силу леммы 2, означает, что степени всех неприводимых делителей

$f_q(n; x)$ при $\beta = \alpha^2$ делят число $3n$.

С другой стороны, можно показать, что трехчлен $f_q(n; x)$ не имеет простых делителей, степень которых делит число n, за исключением лишь одного сомножителя $\psi(x)$, являющегося делителем выражения $x^2 + \alpha x + \beta$.

Это следует из того, что

$$f_q(n; x) - (x^{q^n} - x)x = x^2 + \alpha x + \beta.$$

и, как легко видеть, $\psi(x) = 1$, если $q^n \equiv -1 \pmod 3$, $\psi(x) = x, +$ $+ \alpha x + \beta$, если $q^n \equiv 1 \pmod 3$*, и $\psi(x) = x - \alpha$ при $p = 3$. Стало быть, справедливо

Утверждение 1. В кольце $F_q[x]$ имеет место разложение

$$x^{q^n+1} + \alpha x + \alpha^2 = \psi(x) \prod_{\substack{d \mid n \\ (d^{-1}3n,\, 3)=1}} I_n^{t_n(d)}(x), \qquad (11)$$

где $I_n^{t_n(d)}(x)$ произведение всех $t_n(d)$ неприводимых делителей $f_q(n; x)$ $(\beta = \alpha^2)$, степень которых равна d.

На этом этапе, однако, еще не ясно, существует ли для каждого натурального числа d, удовлетворяющего условиям $d/3n$ и $d \times n$, неприводимый делитель $f_q(n; x)$ степени d. Следующее утверждение полностью решает этот вопрос.

---

* Если $p = 1 \pmod 3$, то $x^2 + dx + a^2 = (x + 2^{-1}a(1 + \sqrt{-3}))(x + 2^{-1}a(1 - \sqrt{-3}))$.

Утверждение 2. Для любого натурального числа n, удовлетворяющего условию $d \setminus 3n$ и $d \times n$ (т. е. $(d^{-1}3n, 3) = 1$), справедлива формула

$$t_n(d) = \frac{1}{d} \sum_{\substack{u \setminus d \\ (u, 3)=1}} \mu(u)\,(q^{\frac{d}{3u}} - \varepsilon_q(d/3u), \qquad (12)$$

где $\mu(u)$ — функция Мебиуса и $\varepsilon_q(u)$ — наименьший по абсолютному значению вычет выражения q^u по модулю 3. В самом деле, согласно (11) имеем

$$q^n - \varepsilon_q(n) = \sum_{d \setminus n_1} 3^{\delta+1} d \cdot t_n(3^{\delta+1} d),$$

где $n = 3^{\delta} n_1 (3 \nmid n_1)$,
откуда следует, что

$$\sum_{d \setminus n_1} \mu(d)\,(q^{\frac{n}{d}} - \varepsilon_q(n/d) = \sum_{d \setminus n_1} \mu(d) \sum_{v \setminus \frac{n_1}{d}} 3^{\delta+1} v t_{n/d}(3^{\delta+1} v). \qquad (13)$$

Но

$$t_n(3^{s+i} v) = t_{n/d}(3^{s+1} v). \qquad (14)$$

поскольку, как легко проверить,

$$f_q(n;\ x)^{q^{\varepsilon n_2}} - x^{q^{\varepsilon n_2}} (x^{q^{3k n_2}} - x)^{q^{(1-\varepsilon) n_2}} = x^{q^{n_2}+1} + \alpha x^{q^{\varepsilon n_2}} + \beta,$$

где $n_2 = d^{-1} n$, $d = 3k + \delta$ $(\delta = +1)$, $\varepsilon = \frac{1}{2}(|\delta| - \delta)$ и два многочлена $x^{q^{n_2}+1} + \alpha x + \alpha^2$ и $x^{q^{n_2}+1} + \alpha x^{q^{n_2}} + \alpha^2$, изоморфно приводимы. Поэтому, собирая слагаемые двойной суммы (13) с одними и теми же значениями v, мы получим

$$\sum_{d \setminus n_1} \mu(d) \sum_{v \setminus n_1/d} 3^{\delta+1} v t_{n/d}(3^{\delta+1} v) =$$

$$= \sum_{v \setminus n_1} 3^{\delta+1} v t_n(3^{\delta+1} v) \sum_{d \setminus n_1/v} \mu(d) = 3n t_n(3n)$$

и

$$\sum_{d \setminus n_1} \mu(d)(q^{\frac{n}{d}} - \varepsilon_q(n/d)) = 3n t_n(3n).$$

Стало быть, в силу (14), для любого натурального числа d, удовлетворяющего условию $(d^{-1}3n, 3) = 1$, имеет место равенство (12).

Пример 2. Пусть дан аффинный сепарабельный многочлен $\bar{f}_q(n;\ x) = x^{q^n} - \alpha x + \beta$ $(\alpha \neq 0)$ над полем F_q. Требуется установить зависимость между первыми коэффициентами всех его неприводимых делителей и элементами α и β.

Имеем

$$\overline{f}_q(n;\ x)^{p-1} = ((x^{q^n} - \alpha x) + \beta)^{p-1} =$$

$$= \sum_{u=0}^{p-1} x^{p-u-1}((-\alpha))^{p-u-1} \sum_{v=0}^{u} \beta^v C_{p-1}^{v} C_{p-v-1}^{u-v} x^{q^n(u-v)},$$

откуда в силу (1) находим

$$a_0(x) = \alpha^{p^{-1}(p-1)}, \quad a_1(x) = \alpha^{p^{-1}(p-2)}(x^{p^{sn}-1} + \beta^{1/p}) \text{ и } b_{up} = \alpha^{p^{-1}(p-1)} x^u.$$

Поскольку $b_0 = \alpha^{p^{-1}(p-1)}$, то очевидно $\xi \cdot A_0^s = \xi$, где $\xi \in F_q$ и в силу (4), для всякого натурального числа m,

$$S_m^1 = S_{m-1} A_0^s + 1 \cdot A_1. \tag{15}$$

Пользуясь (15) при $m = 1$, так как $S_0^1 = 0$, получим

$$S_1^1 = 1 \cdot A_1 = b_1(x) = \gamma x^{p^{sn-1}} + \gamma\beta^{1/p} \qquad (\gamma = \alpha^{p^{-1}(p-2)}).$$

Далее для $m = 2, \ldots, n$ в силу (2) будем иметь

$$S_2^1 = S_1^1 A_0^s + A_1 = \gamma_1 x^{p^{s(n-1)-1}} + \gamma_1 x^{p^{s(n-1)-1}} + 2\gamma_1\beta^{1/p},$$

$$S_3^1 = S_2^1 A_0^s + A_1 = \gamma_1 x^{p^{s(n-2)-1}} + \gamma_1 x^{p^{s(n-1)-1}} + 3\gamma_1\beta^{1/p},$$

и т. д.

$$S_n^1 = \gamma \sum_{u=1}^{n} x^{p^{su-1}} + n\beta\gamma^{1/p}.$$

Проделав эту процедуру подряд k раз и учитывая при этом, что $1 \cdot A_0^{s-1} = \alpha^{1-p}$, мы получим

$$S_{2n}^1 = \gamma(1 + \gamma\gamma_1) \sum_{u=}^{n} x^{p^{su-1}} + 2n\gamma\beta^{1/p} + n\gamma^2\gamma_1\beta^{1/p} \quad (\gamma_1 = \gamma^{p^{-1}(1-p)})$$

и т. д.

$$S_{kn}^1 = \gamma(1 + \gamma\gamma_1 + \cdots + (\gamma\gamma_1)^{k-1}) \sum_{u=1}^{n} x^{p^{su-1}} +$$

$$+ n\gamma\beta^{1/p} \sum_{u=1}^{k} (k + 1 - u)(\gamma\gamma_1)^{u-1},$$

или, согласно (5)

$$S_{kn}^1(\xi) = \Gamma_k \sum_{u=0}^{n-1} x^{q^u} + n\gamma^p \gamma_1^p \beta \sum_{u=1}^{k} (k + 1 - u)(\gamma\gamma_1)^{p(u-1)} + \xi, \tag{16}$$

где

$$\Gamma_k = (\gamma\gamma_1)^p(1 + \gamma\gamma_1 + \cdots + (\gamma\gamma_1)^{k-1})^p = \alpha^{-1} + \alpha^{-2} + \cdots + \alpha^{-k}$$

$$(\gamma\gamma_1)^p = \alpha^{-1} \quad \text{и} \quad \xi \in F_q.$$

Пусть e — минимальное натуральное число, удовлетворяющее условию $\Gamma_e = 0$*. Тогда, очевидно,

$$S^1_{en}(\xi) = \xi - n\beta \sum_{u=1}^{e} u x^{-u}. \qquad (17)$$

Это все дает возможность сделать следующее

Утверждение 3. В кольце $F_q[x]$ многочлен $\bar{f}_q(n; x)$ полностью разлагается на неприводимые делители, степень которых делит число en и не делит $e_1 n$, где e_1 — любой собственный делитель e, за исключением лишь одного линейного сомножителя $\psi_1(x) = (1-\alpha)x + \beta$**, и при этом первый коэффициент a любого неприводимого делителя $\bar{f}_q(n; x)$ степени d удовлетворяет условию $a^{-1} = n\beta \sum_{u=1}^{e} u x^{-u}$. Данное утверждение следует из (16), (17), леммы 1, замечания 2 и того факта, что для любого e_1 и ξ выполняются два соотношения

$$(S^1_{e,n}(\xi),\ \bar{f}_q(n; x)) = \psi_1(x)$$

поскольку

$$\Gamma^{-1}_{e_1}(S^1_{e,n}(\xi) - S^1_{e,n}(\xi)^q) + \bar{f}_q(n; x) = \psi_1(x)$$

и

$$\psi_1(x) \nmid \bar{f}_q(n; x)$$

Сейчас мы покажем, что если $\psi_1(x) \neq 0$, то для любого натурального числа d, удовлетворяющего условию $(d^{-1}en, e) = 1$, справедливо равенство

$$\bar{t}_n(d) = \frac{1}{d} \sum_{\substack{u \mid d \\ (u, e)=1}} \mu(u)(q^{d/u} - \varepsilon_p),$$

где $\bar{t}_n(d)$ — общее количество неприводимых делителей многочлена $\bar{f}_q(n; x)$, степени d и $\varepsilon_p = \frac{1}{2}(1 - (-1)^p)$.

В самом деле, согласно утверждению 3, имеем

$$q^n - 1 = \sum_{d \mid n_1} \lambda e d \bar{t}_n(\lambda e d), \qquad (18)$$

где $n = \lambda n_1$, $(n_1, e) = 1$, $\lambda_i \mid e$ и λ_i — любой простой делитель λ.

Из равенства (18) следует, что

$$\sum_{d \mid n_1} \mu(d)(q^{n/d} - 1) = \sum_{d \mid n_1} \mu(d) \sum_{v \mid n_1/d} \lambda e v \bar{t}_n(\lambda e v). \qquad (19)$$

---

* Т. е. e равно порядку элемента α в группе F^*_q, если $\alpha \neq 0$, и $e = p$ если $\alpha = 1$.

** Если, конечно, $\psi_1(x) \neq 0$.

Но

$$\bar{t}_n(\lambda e v) = \bar{t}_{n d}(\lambda e v), \qquad (20)$$

поскольку

$$\bar{f}_q(n;\, x) - \sum_{a=1}^{d} \left(x^{q^{n_1}} - \gamma x + \theta\right)^{q^{n_1(d-a)}} = 0,$$

где

$$n_1 = d^{-1} n, \qquad \gamma = \alpha^{1/d}, \qquad \theta = \frac{\alpha^{-1}(\gamma^{-1} - 1)}{\gamma^{-1}(\alpha^{-1} - 1)}\beta,$$

и два многочлена $x^{q^{n_1}} - \alpha x + \beta$ и $x^{q^{n_1}} - \gamma x - \theta$ изоморфно приводимы. Поэтому, собирая слагаемые двойной суммы (19) с одинаковыми значениями v, мы получим

$$\sum_{d \setminus n_1} \mu(d) \sum_{v \setminus n_1 d} \lambda e v \bar{t}_{n_1 d}(\lambda e v) = \sum_{v \setminus n_1} \lambda e v \bar{t}_n(\lambda e v) \sum_{d \setminus n_1 v} \mu(d) = e n \bar{t}_n(e n),$$

т. е.

$$\sum_{d \setminus n_1} \mu(d) \left(q^{n/d} - \varepsilon_p\right) = e n \bar{t}(e n)$$

и в силу (20)

$$\bar{t}_n(d) = \frac{1}{d} \sum_{\substack{u \setminus d \\ (u,\, e) = 1}} \mu(u) \left(q^{d/eu} - \varepsilon_p\right),$$

что и требовалось доказать.

В заключение отметим, что в случае, когда $\beta = 0$ (условие несколько более слабое, чем $\psi_1(x) = 0$) можно, повторив описанную процедуру „слово в слово", показать, что двучлен $x^{q^n} - \alpha x$ в кольце $F_q[x]$ полностью разлагается на неприводимые делители, степень d которых удовлетворяет условию $(d^{-1} e^* n;\, e^*) = 1$, где e^* — порядок элемента α в группе F_q^*, а их общее количество $t_n^*(d)$ для любого такого d связано равенством

$$t_n^*(d) = \frac{1}{d} \sum_{\substack{u \setminus d \\ (u,\, e^*) = 1}} \mu(u)\, q^{\frac{d}{e^* u}}.$$

Вычислительный центр Национальной академии наук Армении
и Ереванского государственного университета

Հայաստանի ԳԱԱ ակադեմիկոս Ռ. Ռ. ՎԱՐՇԱՄՈՎ

Վերջավոր դաշտերում օպերատորների մի դասի մասին

Վերջավոր դաշտի վրա ցանկացած բազմանդամի համար առանձնացվում են նախապես տրված գործակիցներով չվերածվող բաժանարարներ։ Դրա հիման վրա մասնավորապես լուծվում է եռանդամի վերածումը չվերածվող բաժանարարների մասին խնդիրը։ Մասնավոր դեպքում $F_q[x]$ *օղակում*

2—59

$f_q(n, x) = x^{qn+1} + ax + \beta$ բազմանդամը վերածվում է չվերածվող բաժանարարների, որոնց աստիճանը բաժանում է en թիվը և չի բաժանում $e_1 n_1$-ը, որտեղ e_1-ը e-ի ցանկացած սեփական բաժանարարն է (e-ն a-ի կարգն է), բացառությամբ մի դեպքի՝ $\varphi_1(x) = (1-a)x + \frac{\beta}{p}$, և այդ դեպքում d-րդ աստիճանի ցանկացած չվերածվող $f_q(n_1, x) = x_{qn+1} - ax + \beta$ բաժանարարի առաջին a գործակիցը բավարարում է $d^{-1} en = n_\beta \sum_{u=1}^{e} ua^{-u}$ պայմանին:

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1 *Р. Р. Варшамов*, ДАН СССР, т. 319, № 4 (1991).