МАТЕМАТИЧЕСКИЕ ЗАМЕТКИ

т. 38, № 1 (1985)

МНОГОЧЛЕНЫ С МИНИМАЛЬНЫМ МНОЖЕСТВОМ ЗНАЧЕНИЙ И УРАВНЕНИЕ $f(x) = f(y)$ В ПРОСТОМ КОНЕЧНОМ ПОЛЕ

Д. А. Митькин

Пусть $p > 3$ — простое, Z_p — поле вычетов $\bmod p$, многочлен $f(x) \in Z_p[x]$ степени $n \geqslant 3$, $n < p$. Обозначим через r_f количество всех различных значений $f(x)$ при $x \in Z_p$. Легко видеть, что выполняется неравенство

$$[(p-1)/n] + 1 \leqslant r_f \leqslant p.$$

Е. Г. Страус предположил, что если $n \mid p-1$ и

$$r_f = [(p-1)/n] + 1 > 2, \tag{1}$$

то $f(x)$ имеет вид

$$a(x+b)^n + c, \quad a \neq 0. \tag{2}$$

В [1] было доказано более сильное утверждение, что если r_f удовлетворяет (1), то $f(x)$ имеет вид (2) и $n \mid p-1$. Морделл [2] связал предположение Е. Г. Страуса с уравнением

$$f(x) = f(y); \quad x, y \in Z_p. \tag{3}$$

Из результатов Морделла следует, что если

$$r_f = p/n + o(p) \quad (p \to \infty) \text{ и } p \geqslant p_0(n),$$

то $f(x)$ имеет вид (2) и $n \mid p-1$.

Берч и Суиннертон-Дайер [3] доказали, что при фиксированном n имеет место соотношение

$$r_f = \lambda p + O(p^{1/2}), \tag{4}$$

где λ — постоянная, зависящая от n и типа многочлена $f(x)$. В случае, если многочлен $(f(x) - f(y))/(x - y)$ абсолютно неприводим, λ определяется формулой $\lambda = 1 - 1/2! + \ldots + (-1)^n/n!$. В [4, 5] дано другое доказательство соотношения (4) при $n = 3, 4$ с вычислением всех возможных значений λ.

Исследования крайнего случая $r_f = p$ (многочлен $f(x)$ в этом случае называется перестановочным) имеются в [6—9]. Оценки $r(f)$ в среднем рассматривались в [10—12].

Уравнение (3) систематически не изучалось. Однако в [13—15] рассматривалось уравнение $f(x) = g(y)$ над полем комплексных чисел. Некоторые результаты этих работ могут быть перенесены и на конечные поля. В большинстве приложений для числа N_f решений уравнения (3) достаточно очевидной оценки $N_f \leqslant np$. Морделл [2] использовал для N_f оценку, основанную на результатах А. Вейля [16]: если k — число абсолютно неприводимых множителей в разложении $f(x) - f(y)$ на неприводимые множители над Z_p, то

$$N_f = kp + O(p^{1/2}).$$

Если $n \mid p - 1$ и $f(x)$ имеет вид (2), то (см., например, [17, гл. 6])

$$N_f = n(p - 1) + 1.$$

Исключая этот случай, в настоящей работе для величины N_f устанавливаются следующие три оценки, первая и третья из которых неулучшаемы:

1) $N_f \leqslant np - (2n - 2)$;

2) $N_f \leqslant (n - 1)p$, если $n \mid p - 1$ или $n > 4$, $p > (n - 1)^2$;

3) $N_f \leqslant ([n/2] + 1)p + c(n)p^{1/2}$.

В качестве следствия этих оценок в работе дано усиление указанных выше [1, 2] границ для r_f, характеризующих многочлены вида (2) с условием $n \mid p - 1$.

Простейшее соотношение, связывающее величины r_f и N_f, устанавливается в следующей лемме.

ЛЕММА 1. *Имеет место неравенство*

$$p^2/N_f \leqslant r_f \leqslant \frac{1}{n}\left(p + \left[\frac{np - N_f}{n - 1}\right](n - 1)\right). \tag{5}$$

Доказательство. Пусть $a_1, \ldots, a_r$, где $r = r_f$,— все различные значения, которые принимает $f(x)$ при $x \in Z_p$. Обозначим через n_i $(i = 1, \ldots, r)$ число решений уравнения $f(x) = a_i$, $x \in Z_p$. Тогда, очевидно, $1 \leqslant n_i \leqslant n$ и имеют место равенства:

$$n_1 + \ldots + n_r = p \tag{6}$$

и

$$n_1^2 + \ldots + n_r^2 = N_f. \tag{7}$$

Применяя к (6) неравенство Коши, получим

$$p \leqslant \left(r \cdot \sum_{i=1}^{r} n_i^2\right)^{1/2} = (r_f \cdot N_f)^{1/2},$$

откуда следует левая часть неравенства (5). Пусть далее t — количество величин n_i $(i = 1, \ldots, r)$ с условием $n_i < n$. Без ограничения общности полагаем, что $n_1 < n, \ldots, n_t < n$. Тогда из (6) и (7) получим равенства

$$\begin{aligned} n_1 + \ldots + n_t + n(r - t) &= p, \\ n_1^2 + \ldots + n_t^2 + n^2(r - t) &= N_f, \end{aligned} \tag{8}$$

из которых следует, что

$$(n - 1)\, t \leqslant n_1 (n - n_1) + \ldots + n_t (n - n_t) = np - N_f.$$

Так как t — целое число, то $t \leqslant [(np - N_f)/(n - 1)]$. Из (8) имеем $t + n(r - t) \leqslant p$, откуда и следует правая часть (5). Лемма доказана.

ТЕОРЕМА 1. *Пусть $f(x)$ не является многочленом вида* (2), *если $n \mid p - 1$, $3 \leqslant n < p$. Тогда*

$$N_f \leqslant np - (2n - 2). \tag{9}$$

Доказательство. Предположим, что $N_f > np - (2n - 2)$. Тогда из (5) получим, что $r_f \leqslant (p - 1)/n + 1$ и, следовательно, $r_f = [(p - 1)/n] + 1$. Если $r_f > 2$, то из указанного выше результата [1] следует, что $f(x)$ имеет вид (2) и $n \mid p - 1$, а это противоречит условию теоремы. Пусть $r_f = 2$. Тогда $f(x)$ принимает только два значения. Обозначим их через α_1, α_2. Как отмечено в [1], многочлен из $Z_p[x]$ степени $< p$ однозначно определяется своими значениями, и поэтому $f(x)$ имеет вид

$$f(x) = \alpha_1 \cdot \sum_{\gamma \in M} (1 - (x - \gamma)^{p-1}) + \alpha_2 \cdot$$

$$\cdot \sum_{\gamma \notin M} (1 - (x - \gamma)^{p-1}),$$

где M — непустое собственное подмножество Z_p. Пусть k — число элементов M. Если $k = 1$, $p - 1$, то, очевидно, $f(x)$ тогда будет иметь вид (2) с $n = p - 1$. Поэтому полагаем, что $k \neq 1$, $p - 1$. Так как степень $f(x)$ равна $p - 1$, то

$$N_f = (p-k)^2 + k^2 \leqslant (p-2)^2 + 2^2 < np - (2n-2).$$

Теорема доказана.

Замечание 1. Оценка (9) неулучшаема. Рассмотрим многочлен степени $p - 2$

$$f(x) = 1 + x^{p-1} - (x-1)^{p-1}.$$

Величина N_f, очевидно, равна $(p-2)^2 + 2 = np - (2n-2)$, где $n = p - 2$.

В теореме 2 устанавливается более точная оценка N_f при $n \mid p - 1$, $n < p - 1$.

ТЕОРЕМА 2. *Пусть* $n \mid p - 1$ *и* $f(x)$ *не является многочленом вида* (2). *Тогда справедлива оценка*

$$N_f \leqslant (n-1)\,p.$$

Доказательство теоремы 2 основывается на следующей лемме.

ЛЕММА 2. *Пусть* $\varphi(x, y) \in Z_p[x, y]$ — *многочлен степени* $k \geqslant 1$ *и его старшая форма раскладывается на линейные множители над* Z_p. *Тогда, если число решений уравнения*

$$\varphi(x, y) = 0, \quad x, y \in Z_p, \tag{10}$$

больше $(k-1)\,p$, *то* $\varphi(x, y)$ *раскладывается на линейные множители над* Z_p.

Доказательство. Утверждение леммы докажем индукцией по k. При $k = 1$ лемма очевидна. Пусть утверждение леммы верно для многочленов с разложимой над Z_p старшей формой степени $k - 1$ и $k > 1$. Разложим старшую форму $F(x, y)$ многочлена $\varphi(x, y)$ на линейные множители над Z_p:

$$F(x, y) = \prod_{i=1}^{k} (a_i x + b_i y), \quad a_i, b_i \in Z_p.$$

Из двух элементов a_1 и b_1 по крайней мере один не равен 0, поэтому, без ограничения общности, полагаем, что $a_1 \neq 0$. Легко видеть, что многочлен $\psi(t, y) = \varphi(t - b_1 a_1^{-1} y, y)$ имеет по y степень $\leqslant k - 1$, а число решений уравнения

$$\psi(t, y) = 0, \quad t, y \in Z_p, \tag{11}$$

равно числу решений уравнения (10). Таким образом, число решений уравнения (11) больше $(k-1)\,p$. С другой стороны, для каждого фиксированного $t_0 \in Z_p$ уравнение $\psi(t_0, y) = 0$, $y \in Z_p$, либо имеет не более $k-1$ решений, либо $\psi(t_0, y) = 0$. Отсюда получим, что по крайней мере для одного $t_0 \in Z_p$ имеет место равенство $\psi(t_0, y) = 0$ и, следовательно, $\psi(t, y)$ имеет линейный делитель $t - t_0$. Но тогда и $\varphi(x, y)$ имеет линейный делитель $x + b_1 a_1^{-1} y - t_0$. Определим многочлен $\varphi_0(x, y) \in Z_p[x, y]$ степени $k-1$ из равенства

$$\varphi(x, y) = (x + b_1 a_1^{-1} y - t_0)\,\varphi_0(x, y). \tag{12}$$

Очевидно, что $\varphi_0(x, y)$ удовлетворяет условиям леммы с $k-1$ вместо k. По предположению индукции $\varphi_0(x, y)$ раскладывается на линейные множители над Z_p, что в сочетании с равенством (12) дает разложение на линейные множители для $\varphi(x, y)$. Лемма доказана.

Доказательство теоремы 2. Допустим, что $N_f > (n-1)\,p$. Старшая форма многочлена $f(x) - f(y)$ имеет вид $a(x^n - y^n)$, где $a \neq 0$. Так как $n \mid p-1$, то она раскладывается на линейные множители над Z_p (см. [17, гл. 5]). Согласно лемме 2 тогда и $f(x) - f(y)$ раскладывается на линейные множители над Z_p. Из разложимости $f(x) - f(y)$ на линейные множители над Z_p следует, как показано в [2], что $f(x)$ имеет вид (2). Но это противоречит условию теоремы. Следовательно, $N_f \leqslant (n-1)\,p$. Теорема доказана.

Замечание 2. При $n \nmid p-1$ оценка теоремы 2 не выполняется: для многочлена $f(x) = x^3 + ax$, где a — квадрат в Z_p, имеет место равенство $N_f = 2p + 1$.

Далее будем использовать следующее следствие из результатов А. Вейля [16] (см. также [18, § 58]):

Если $\varphi(x, y) \in Z_p[x, y]$ — *абсолютно неприводимый многочлен, то для числа* N *решений уравнения*

$$\varphi(x, y) = 0, \quad x, y \in Z_p, \tag{13}$$

справедлива оценка сверху

$$N \leqslant p + 1 + 2g\sqrt{p}, \tag{14}$$

где g — *род кривой, определяемой уравнением* (13).

Нам потребуется оценка рода g в зависимости от степени k многочлена $\varphi(x, y)$ (см. [19, гл. 2]):

$$g \leqslant (k-1)\,(k-2)/2. \tag{15}$$

Так как величины r_f и N_f, а также свойство $f(x)$ иметь или не иметь вид (2), инвариантны при замене $f(x)$ на $\lambda f(ax+b)+\mu$, где λ, a, b, $\mu \in Z_p$ и λ, $a \neq 0$, то, без ограничения общности, полагаем далее, что $f(x)$ имеет вид

$$f(x) = x^n + a_{n-2}x^{n-2} + \ldots + a_1 x. \qquad (16)$$

Морделл [2] использовал для оценки N_f сверху результаты А. Вейля, но при этом не учитывалась специфика разложения $f(x) - f(y)$ на множители. В следующей лемме устанавливается зависимость между числом линейных делителей $f(x) - f(y)$ и видом многочлена $f(x)$.

ЛЕММА 3. *Пусть*

$$f(x) - f(y) = L_1(x, y) \ldots L_s(x, y)\, \varphi_1(x, y) \ldots \varphi_k(x, y)\, Q(x, y) \qquad (17)$$

— разложение на множители в $Z_p[x, y]$, *где* $L_1(x, y), \ldots, L_s(x, y)$ *— многочлены первой степени,* $\varphi_1(x, y), \ldots, \varphi_k(x, y)$ $(k \geqslant 0)$ *— абсолютно неприводимые многочлены степени* $\geqslant 2$, *а* $Q(x, y)$ *— произведение неприводимых многочленов, не являющихся абсолютно неприводимыми. Тогда* $s \mid (n, p-1)$, $n \geqslant (k+1)s$, $f(x)$ *имеет вид* $g(x^s)$, *где* $g(x) \in Z_p[x]$, *и степени* $\varphi_1(x, y), \ldots, \varphi_k(x, y) \geqslant s$. *В частности, если* $s > n/2$, *то* $f(x) = x^n$.

Доказательство. Без ограничения общности полагаем, что коэффициенты при x в многочленах $L_2(x, y), \ldots, L_s(x, y)$ равны 1. Пусть

$$L_1(x, y) \ldots L_s(x, y) = \prod_{i=1}^{s} (x - \lambda_i y - \mu_i),$$

где $\lambda_1 = 1$, $\mu_1 = 0$ соответствуют многочлену $L_1(x, y) = x - y$. Из условия (16), очевидно, следует, что $\mu_i = 0$ при $i = 1, \ldots, s$. Кроме того, ясно, что $\lambda_1, \ldots, \lambda_s$ представляют s различных корней уравнения $x^n = 1$ и

$$f(\lambda_i y) = f(y) \qquad (i = 1, \ldots, s). \qquad (18)$$

Рассмотрим множество M всех $\lambda \in Z_p$, для которых $f(\lambda y) = f(y)$. Множество M является, очевидно, группой по умножению, подгруппой циклической группы корней n-й степени из 1 в Z_p. При этом, если $\lambda \in M$, то $x - \lambda y$ делит $f(x) - f(y)$ над Z_p. Следовательно, M состоит в точности из $\lambda_1, \ldots, \lambda_s$ и является циклической группой порядка s, причем $s \mid (n, p-1)$. Сравнивая коэффициенты в равенствах (18) при степенях y, найдем, что

если коэффициент a_j при y^j многочлена $f(y)$ не равен 0, то $\lambda_i^j = 1$ при $i = 1, \ldots, s$, откуда следует, что $s \mid j$. Таким образом, $f(x) = g(x^s)$ при некотором $g(x) \in Z_p[x]$. Если $s > n/2$, то из условия $s \mid n$ следует, что $s = n$, но тогда $f(x) = x^n$.

Покажем, что степени $\varphi_1(x, y), \ldots, \varphi_k(x, y) \geqslant s$. Пусть $\varphi(x, y)$ — один из многочленов $\varphi_i(x, y)$ $(i = 1, \ldots, k)$ и

$$f(x) - f(y) = \varphi(x, y)\,\psi(x, y) = g(x^s) - g(y^s).$$

Представим $\varphi(x, y)$ и $\psi(x, y)$ в виде суммы ненулевых форм

$$\varphi(x, y) = \sum_{i=1}^{l} F_i(x, y), \qquad \psi(x, y) = \sum_{j=1}^{m} G_j(x, y),$$

где формы $F_1, \ldots, F_l$ и $G_1, \ldots, G_m$ расположены в порядке убывания степеней

$$\deg F_1 > \ldots > \deg F_l, \quad \deg G_1 > \ldots > \deg G_m,$$

причем $l \geqslant 2$. Имеем равенство

$$F_1(x, y)\, G_1(x, y) = x^n - y^n \tag{19}$$

и, полагая $G_2(x, y) = 0$ при $m = 1$,— неравенство

$$\deg (F_1(x, y)\, G_2(x, y) + G_1(x, y)\, F_2(x, y)) \leqslant n - s.$$

Так как, в силу соотношения (19), $F_1(x, y)$ и $G_1(x, y)$ не имеют общих делителей в $Z_p[x, y]$, отличных от констант, а $\deg F_1 > \deg F_2$, $F_2 \neq 0$, то равенство $F_1G_2 + G_1F_2 = 0$ невозможно и, следовательно, каждая из форм G_1F_2 и F_1G_2 степени $\leqslant n - s$. Отсюда получаем, что $\deg F_2 \leqslant \deg F_1 - s$ и, значит, $\deg F_1 \geqslant s$. Тем самым лемма доказана.

ТЕОРЕМА 3. *Пусть $f(x)$ удовлетворяет условиям леммы 3 с $s \leqslant n/2$. Тогда имеют место неравенства*

$$N_f \leqslant \begin{cases} (n-1)\,p, & \text{если } n > 4,\ p > (n-1)^2; \\ (n-1)\,p + 1, & \text{если } n = 3, 4, \end{cases} \tag{20}$$

и

$$N_f \leqslant (s + [(n-s)/s_0])\ p + O(\sqrt{p}) \leqslant ([n/2] + 1)p + O(\sqrt{p}), \tag{21}$$

где $s_0 = \max(2, s)$ и постоянная в символе O зависит только от n.

Доказательство. Пусть для $f(x) - f(y)$ выполняется разложение (17). Обозначим через $n_1, \ldots, n_k$ степени многочленов $\varphi_1(x, y), \ldots, \varphi_k(x, y)$ соответственно. Так как $\varphi_1(x, y), \ldots, \varphi_k(x, y)$ абсолютно неприводимы, то число нулей произведения $\varphi_1(x, y) \ldots \varphi_k(x, y)$ над Z_p согласно (14), (15) оценивается сверху величиной

$$\sum_{i=1}^{k} (p + 1 + (n_i - 1)(n_i - 2)\sqrt{p}).$$

Число нулей произведения $L_1(x, y) \ldots L_s(x, y)$ над Z_p, совпадающего с точностью до постоянного множителя с $x^s - y^s$, равно $s(p-1) + 1$. Известно, что все нули над Z_p неприводимого над Z_p многочлена от двух пременных, не являющегося абсолютно неприводимым, особые (см. [20, гл. 16, § 4]). Поэтому все нули $Q(x, y)$ над Z_p являются особыми нулями $f(x) - f(y)$. Так как $f(x) = g(x^s)$, то легко видеть, что число нулей $Q(x, y)$ над Z_p оценивается сверху величиной

$$(n - s + 1)\left(n - s - \sum_{i=1}^{k} n_i\right).$$

В итоге получим, что

$$N_f \leqslant (k + s)p + \sum_{i=1}^{k} ((n_i - 1)(n_i - 2)\sqrt{p} - n_i(n - s + 1)) + k - s + 1 + (n - s + 1)(n - s). \quad (22)$$

Так как согласно лемме 3 $n_i \geqslant s_0$, то $k \leqslant [(n - s)/s_0]$ и, следовательно, справедлива оценка (21). Случаи $n = 3, 4$ проверяются непосредственным вычислением N_f или с помощью (22). Далее полагаем, что $n \geqslant 5$, $p > (n-1)^2$. Пусть $n_1 + \ldots + n_k = \gamma$. Легко показать, что при фиксированном $\gamma \geqslant ks_0$ и $k \geqslant 2$ максимальное значение выражения в (22) по $n_1, \ldots, n_k \geqslant s_0$ достигается, когда $k - 1$ величин n_i принимают минимальное значение s_0 и одна — максимальное. Следовательно,

$$N_f \leqslant (k + s)p + (k - 1)(s_0 - 1)(s_0 - 2)\sqrt{p} + k - s + 1 + (n - s + 1)(n - s) + \max_{\gamma = ks_0, n-s} ((\gamma - (k-1)s_0 - 1)(\gamma - (k-1)s_0 - 2)\sqrt{p} - \gamma(n - s + 1)). \quad (23)$$

Эта оценка выполняется также и при $k = 1$. Максимум, указанный в (23), в силу условий $n \geqslant 5$, $p > (n-1)^2$

достигается при $\gamma = n - s$. Поэтому при $k \geqslant 1$ получим

$$N_f \leqslant \max_{\lambda=1,\ (n-s)/s_0} ((\lambda + s)\ p + \\ + (\lambda - 1)\ (s_0 - 1)\ (s_0 - 2)\sqrt{p} + \lambda - s + 1 + \\ + (n - s - (\lambda - 1)\ s_0 - 1)\ (n - s - (\lambda - 1)\ s_0 - \\ - 2)\sqrt{p}) \leqslant (n - 1)\ p.$$

При $k = 0$ из (22) следует, что при $n \geqslant 5$, $p > (n-1)^2$

$$N_f \leqslant \max_{s=1,\ n/2} (sp - s + 1 + (n - s + 1)\ (n - s)) \leqslant \\ \leqslant (n - 1)\ p.$$

Теорема доказана.

Следствие 1. *Существуют такие величины* $c\ (n) > 0$, $p_0\ (n)$, *что если*

$$2 < r_f < p/([n/2] + 1) - c\ (n)\sqrt{p},\quad p \geqslant p_0\ (n),$$

то $n \mid p - 1$ *и* $f\ (x)$ *имеет вид* (2).

Доказательство. Результат непосредственно следует из оценки (21) теоремы 3 и леммы 1.

Следствие 2. *Если* $2 < r_f \leqslant p/(n-1)$, *то* $n \mid p - 1$ *и* $f\ (x)$ *имеет вид* (2).

Доказательство. При $p \geqslant (n-1)^2$ результат следствия получается из оценки (20) и леммы 1, так как $p^2/((n-1)\ p + 1) > (p-1)/(n-1)$, а при $p < (n-1)^2$, в силу неравенства $p/(n-1) < p/n + 1$, — из результата [1].

Замечание 3. Оценку (21) нельзя улучшить при любом фиксированном четном n. Действительно, пусть $n = 2s$, s — натуральное. Выберем достаточно большое простое p с условием $p \equiv 1 \pmod{s}$ и возьмем $f\ (x) = x^{2s} + x^s$. Тогда $N_f = (n/2 + 1)p + O\ (\sqrt{p})$.

В теореме 4 устанавливается, что оценка (21) неулучшаема при любом фиксированном нечетном $n \geqslant 5$.

ЛЕММА 4. *Пусть* $\varphi\ (x,\ y) \in Z_p\ [x,\ y]$ — *многочлен степени* k, *не имеющий кратных делителей и не делящийся на* $x - y$, *и пусть для результанта* $\varphi\ (x,\ y)$ *и* $\varphi\ (z,\ y)$ *по* y *выполняется равенство*

$$\mathrm{Res}_y\ (\varphi\ (x,\ y),\ \varphi\ (z,\ y)) = c\ (x - z)^k\ (\varphi\ (x,\ z))^{k-1},\\ c \neq 0. \qquad (24)$$

Тогда существует $f\ (x) \in Z_p\ [x]$ *такой, что* $f\ (x) - f\ (y) = (x - y)\ \varphi\ (x,\ y)$.

Доказательство. Пусть μ — трансцендентный над Z_p элемент и K — алгебраическое замыкание поля $Z_p(\mu)$. Если l — степень $\varphi(x, y)$ по y, то по свойствам результанта (см. [21, гл. 4, § 4]) степень $\mathrm{Res}_y(\varphi(x, y), \varphi(z, y))$ не превосходит $(2k - l)\,l$, что меньше k^2 при $l < k$. Отсюда получаем, что $l = k$ и, следовательно, $\varphi(\mu, y)$ имеет в K ровно k корней $\mu_1, \ldots, \mu_k$. Так как $\varphi(x, y)$ не имеет над Z_p кратных делителей, а μ трансцендентен над Z_p, то $\mu_1, \ldots, \mu_k$ различны. Кроме того, так как $\varphi(x, y)$ не делится на $x - y$, то μ отлично от $\mu_1, \ldots, \mu_k$. Аналогично устанавливается, что $\varphi(\mu_i, y)$ имеет k различных корней $\mu_1^{(i)}, \ldots, \mu_k^{(i)}$ в K, отличных от μ_i. Имеем разложение

$$\varphi(\mu_i, y) = \gamma(y - \mu_1^{(i)}) \ldots (y - \mu_k^{(i)}), \quad \gamma \neq 0.$$

Из (24), пользуясь мультипликативным свойством результанта, получим

$$c(x - \mu_i)^k (\varphi(x, \mu_i))^{k-1} = \mathrm{Res}_y(\varphi(x, y), \varphi(\mu_i, y)) = \\ = (-\gamma)^k \prod_{j=1}^{k} \varphi(x, \mu_j^{(i)}). \qquad (25)$$

Многочлены $\varphi(x, \mu_j^{(i)})$ $(j = 1, \ldots, k)$ не имеют кратных корней, поэтому из равенства (25) следует, что $\varphi(\mu, \mu_j^{(i)}) = 0$ при всех $j = 1, \ldots, k$, за исключением одного значения. Из симметричности результанта с точностью до знака и соотношения (24) следует, что $\varphi(x, y) = c\varphi(y, x)$, где $c^2 = 1$. Отсюда получаем, что $\varphi(\mu_i, \mu) = 0$, и, следовательно, $\mu_1^{(i)}, \ldots, \mu_k^{(i)}$ совпадают с точностью до порядка следования с $\mu, \mu_1, \ldots, \mu_{i-1}, \mu_{i+1}, \ldots, \mu_k$. Рассмотрим многочлен $(x - y)\,\varphi(x, y)$. Он обращается в 0 на декартовом квадрате множества $\{\mu, \mu_1, \ldots, \mu_k\}$. Применяя теорему Безу, получим, что

$$(x - y)\,\varphi(x, y) = \gamma_1 (x - \mu)(x - \mu_1) \ldots (x - \mu_k) + \\ + \gamma_2 (y - \mu)(y - \mu_1) \ldots (y - \mu_k),$$

где $\gamma_2 = -\gamma_1$. Очевидно, что многочлен $f(x) = \gamma_1 (x - \mu)(x - \mu_1) \ldots (x - \mu_k)$ является искомым. Лемма доказана.

ТЕОРЕМА 4. *Пусть $n \geqslant 5$ — нечетное, $n \mid p - 1$ или $n \mid p + 1$, $\lambda \in GF[p^2]$ — примитивный корень степени n из 1. Тогда при любом $\gamma \in Z_p$, $\gamma \neq 0$, существует*

$f(x) \in Z_p[x]$ *такой, что*

$$f(x) - f(y) = (x-y)\prod_{k=1}^{(n-1)/2}(x^2 - (\lambda^k + \lambda^{-k})xy + y^2 + (\lambda^{2k} + \lambda^{-2k} - 2)\gamma). \quad (26)$$

Для величины N_f *справедлива формула*

$$N_f = \frac{n+1}{2}p + O(n^2). \quad (27)$$

Доказательство. Так как $n \mid p^2 - 1$, то в поле $GF[p^2]$ есть примитивный корень λ степени n из 1. Обозначим

$$\varphi_k(x, y) = x^2 - (\lambda^k + \lambda^{-k})xy + y^2 + (\lambda^{2k} + \lambda^{-2k} - 2)\gamma, \quad k \not\equiv 0 \pmod{n}.$$

Если $n \mid p-1$, то $\lambda \in Z_p$. Если же $n \mid p+1$, то $\lambda^{-1} = \lambda^p$ и, следовательно, $\lambda^k + \lambda^{-k} \in Z_p$. В обоих случаях имеем, что $\varphi_k(x, y) \in Z_p[x, y]$. Непосредственным вычислением устанавливается

$$\mathrm{Res}_y(\varphi_k(x, y), \varphi_m(z, y)) = \begin{cases} (x-z)^2\varphi_{2k}(x, z), & \text{если } k \equiv \pm m \pmod{n}; \\ \varphi_{k-m}(x, z)\varphi_{k+m}(x, z), & \text{если } k \not\equiv \pm m \pmod{n}. \end{cases}$$

Отсюда, полагая $F(x, y) = \varphi_1(x, y) \ldots \varphi_{(n-1)/2}(x, y)$, в силу мультипликативного свойства результанта получим, что

$$\mathrm{Res}_y(F(x, y), F(z, y)) = (x-z)^{n-1}(F(x, z))^{n-2}.$$

Многочлен $F(x, y)$ удовлетворяет условиям леммы 4,— поэтому существует $f(x) \in Z_p[x]$ такой, что $f(x) - f(y) = (x-y)F(x, y)$, т. е. выполняется (26). Так как число нулей $\varphi_k(x, y)$ над Z_p равно $p-1$ или $p+1$ (см. [22, гл. 5, § 11, упр. 5]), то отсюда следует, очевидно, формула (27). Теорема доказана.

Автор благодарит В. Н. Чубарикова за обсуждение результатов этой работы.

Московский государственный
педагогический институт им. В. И. Ленина

Поступило
27.07.83

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] Carlitz L., Lewis D. J., Mills W. H., Straus E. G. Polinomials over finite fields with minimal value sets.— Mathematika, 1961, v. 8, № 2, p. 121—130.

[2] Mordell L. J. A congruence problem of E. G. Straus.— J. London Math. Soc., 1963, v. 38, № 149, p. 108—110.
[3] Birch B. J., Swinnerton-Dyer H. P. F. Note on a problem of Chowla.— Acta Arithm., 1959, v. 5, № 4, p. 417—423.
[4] McCann K., Williams K. S. On the residues of a cubic polinomial (Mod p).— Canad. Math. Bull., 1967, v. 10, № 1, p. 29—38.
[5] McCann K., Williams K. S. The distribution of the residues of a quartic polinomial.— Glasgow Math. J., 1967, v. 8, p. 67—88.
[6] Dickson L. E. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group.— Ann. of Math., 1897, v. 11, p. 65—120.
[7] Dickson L. E. Linear groups with an exposition of the Galois field theory.— New York: Dover, 1958.
[8] Carlitz L. A note on permutations in a finite field.— Proc. Amer. Math. Soc., 1953, v. 4, № 4, p. 538.
[9] Carlitz L., Lutz Jo Ann. A characterisation of permutation polinomials over a finite field.— Amer. Math. Monthly, 1978, v. 85, № 9, p. 746—748.
[10] Carlitz L. On the number of distinct values of a polynomial with coefficients in a finite field.— Proc. Japan Acad., 1955, v. 31, № 3, p. 119—120.
[11] Uchiyama S. Note on the mean value of $V(f)$.— Proc. Japan Acad., 1955, v. 31, № 4, p. 199—200.
[12] Uchiyama S. Note on the mean value of $V(f)$, II.— Proc. Japan Acad., 1955, v. 31, № 6, p. 321—323.
[13] Davenport H., Lewis D. J., Schinzel A. Equations of the form $f(x) = g(y)$.— Quart. J. Math. Oxford (2), 1961, v. 12, № 48, p. 304—312.
[14] Schinzel A. Reducibility of polynomials of the form $f(x) - g(y)$.— Colloq. Math., 1967, v. 18, p. 213—218.
[15] Rubel L. A., Schinzel A., Tverberg H. On difference polynomials and hereditarily irreducible polynomials.— J. Number Theory, 1980, v. 12, № 2, p. 230—235.
[16] Weil A. Sur les courbes algebriques et les variétés qui s'en deduisent.— Publ. Inst. Math. Strasbourg, 1948, v. 1041, p. 1—85.
[17] Виноградов И. М. Основы теории чисел.— М.: Наука, 1981.
[18] Чеботарев Н. Г. Теория алгебраических функций.— М.— Л.: ГИТТЛ, 1948.
[19] Гриффитс Ф., Харрис Д. Принципы алгебраической геометрии, т. 1.— М.: Мир, 1982.
[20] Ходж В., Пидо Д. Методы алгебраической геометрии, т. 3.— М.: ИЛ, 1955.
[21] Ходж В., Пидо Д. Методы алгебраической геометрии, т. 1.— М.: ИЛ, 1954.
[22] Бурбаки Н. Алгебра: Многочлены и поля. Упорядоченные группы.— М.: Наука, 1965.