Czechoslovak Mathematical Journal

Štefan Schwarz

О числе неприводимых факторов данного многочлена над конечным полем

Czechoslovak Mathematical Journal, Vol. 11 (1961), No. 2, 213–225

Persistent URL: http://dml.cz/dmlcz/100455

Чехословацкий математический журнал т. 11 (86) 1961, Прага

О ЧИСЛЕ НЕПРИВОДИМЫХ ФАКТОРОВ ДАННОГО МНОГОЧЛЕНА НАД КОНЕЧНЫМ ПОЛЕМ

ШТЕФАН ШВАРЦ, (Štefan Schwarz), Братислава

(Поступило в редакцию 8/I 1960 г.)

Посвящается памяти проф. Карла Петра по поводу десятой годовщины его смерти 14-го февраля 1950 г.

В работе выводятся формулы для числа различных неприводимых факторов i-й степени данного многочлена $f(x)$ над конечным полем $GF(q)$.

Пусть $f(x)$ — многочлен n-й степени над конечным полем $\mathbf{T} = GF(q)$, где $q = p^s$, p — простое число, $s \geqq 1$. Пусть

$$f(x) = f_1(x)^{k_1} . f_2(x)^{k_2} \dots f_r(x)^{k_r}, \quad k_i \geqq 1 \tag{1}$$

есть разложение многочлена $f(x)$ на различные неприводимые факторы над полем $\mathbf{T}$. Пусть степени многочленов $f_i(x)$ равны $m_i \geqq 1$ $(i = 1, 2, \dots, r)$.

Одной из основных задач теории многочленов над полем $\mathbf{T}$ является определение чисел $m_1, m_2, \dots, m_r$ (а также, быть может, чисел $k_1, k_2, \dots, k_r$). Эту задачу можно сформулировать и несколько иначе:

Обозначим символом σ_i число различных неприводимых факторов многочлена $f(x)$ степени i, $1 \leqq i \leqq n$. (В частности, σ_1 тогда означает число разных корней уравнения $f(x) = 0$ в поле $\mathbf{T}$.) Очевидно, $0 \leqq i\sigma_i \leqq n$. Если $f(x)$ не имеет кратных факторов (т. е. $k_1 = k_2 = \dots = k_r = 1$), то $\sum_{i=1}^{n} i\sigma_i = n$. Нужно найти систематический (т. е. не основанный на догадках) метод для определения чисел $\sigma_1, \sigma_2, \dots, \sigma_n$.

Хорошо известно, что это можно сделать так: Пусть i — целое число, $1 \leqq \leqq i \leqq n$. Пусть $i' > i'' > \dots > 1$ — все делители числа i, меньшие чем число i. Обозначим через δ_i степень общего наибольшего делителя многочлена $f(x)$ и многочлена $x^{q^i} - x$. Тогда $i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1 = \delta_i$. Находя последовательно общие наибольшие делители многочлена $f(x)$ и многочленов $x^q - x$, $x^{q^2} - x$, $\dots$, $x^{q^n} - x$, можно последовательно найти все числа $\sigma_1, \sigma_2, \dots, \sigma_n$. Однако, этот метод весьма кропотлив и мало пригоден для практических целей.

Указанной задачей занимался *К. Петр* в работе [4]. Приведем многочлены $x^0, x^q, x^{2q}, \ldots, x^{(n-1)q} \pmod{f(x)}$ к как можно более низкой степени

$$
\begin{aligned}
x^0 &\equiv c_{00} + c_{01}x + \ldots + c_{0,n-1}x^{n-1}, \\
x^q &\equiv c_{10} + c_{11}x + \ldots + c_{1,n-1}x^{n-1}, \\
x^{2q} &\equiv c_{20} + c_{21}x + \ldots + c_{2,n-1}x^{n-1}, \\
&\vdots \\
x^{(n-1)q} &\equiv c_{n-1,0} + c_{n-1,1}x + \ldots + c_{n-1,n-1}x^{n-1}, \quad (\mathrm{mod}\,(f(x)),
\end{aligned} \tag{2}
$$

где c_{ik} — многочлены от коэффициентов многочлена $f(x)$. Притом, очевидно, $c_{00} = 1$, $c_{01} = c_{02} = \ldots = c_{0,n-1} = 0$. Обозначим символом $\mathbf{C}$ матрицу коэффициентов (c_{ik}), а символом $\mathbf{E}_n$ — единичную матрицу порядка n. Из результатов Петра [4] и автора [8] следует, что характеристический многочлен матрицы $\mathbf{C} - \lambda\mathbf{E}_n$ можно записать в виде

$$
|\mathbf{C} - \lambda\mathbf{E}_n| = (-1)^n (\lambda^{m_1} - 1)(\lambda^{m_2} - 1) \ldots (\lambda^{m_r} - 1)\, \lambda^{(k_1-1)m_1 + (k_2-1)m_2 + \ldots + (k_r-1)m_r} \tag{3}
$$

Нетрудно доказать, что разложение характеристического многочлена матрицы $\mathbf{C}$ в виде, указанном в правой части соотношения (3), будет однозначно определенным, например, в тех случаях, когда $p > n$. В работе [4] формула выводится лишь для случая $q = p$; обобщение на случай $q = p^s$, $s > 1$ не представляет никаких трудностей. (Смотри также работу [11], где дается другой вывод соотношения (3) в общем случае.)

В работе [11] автор доказал следующий результат: Если h_l $(1 \leqq l \leqq n)$ означает ранг матрицы $\mathbf{C}^l - \mathbf{E}_n$, то числа $\sigma_1, \sigma_2, \ldots, \sigma_n$ однозначно определяются системой линейных уравнений

$$
\sum_{j=1}^{n} (l, j)\, \sigma_j = m - h_l, \quad (l = 1, 2, \ldots, n), \tag{4}
$$

где (l, j) обозначает общий наибольший делитель чисел l и j.

Практическое использование соотношения (3) для определения степеней неприводимых факторов, однако, довольно сложно, так как требует вычисления характеристического многочлена матрицы $\mathbf{C}$ и его разложения на факторы вида, указанного в правой части соотношения (3).

Точно так же и результат (4) имеет, понятно, скорее теоретическое значение, поскольку для действительного вычисления он требует вычисления рангов матриц $\mathbf{C} - \mathbf{E}_n$, $\mathbf{C}^2 - \mathbf{E}_n, \ldots, \mathbf{C}^n - \mathbf{E}_n$, связанного со значительной затратой времени.

Целью настоящей работы является вывод новых интересных и притом сравнительно весьма простых формул, позволяющих при некоторых условиях определить числа $\sigma_1, \sigma_2, \ldots, \sigma_n$. Для вычислений нужно знать только следы

матриц $\mathbf{C}, \mathbf{C}^2, \ldots, \mathbf{C}^n$. Если $p > n$, то формулы, выведенные в указанной ниже теореме, однозначно определяют числа σ_i.

Поскольку автор мог установить по литературе, выведенный в настоящей работе результат значительно проще, чем все известные результаты, касающиеся решаемой проблемы. В действительности, однако, подавляющее большинство работ, посвященных многочленам над конечным полем, решают вопрос о числе корней уравнения $f(x) = 0$ в поле $\mathbf{T}$, т. е. об определении числа σ_1. И в этом частном случае выведенный в этой работе результат для числа σ_1 проще, чем теоремы из ряда теорем Радоса-Кенига (см. *Л. Редей* [5], стр. 501 и Л. Редей — *П. Туран* [7]). Обзор более старых результатов, касающихся главным образом определения числа σ_1, можно найти в книге *Л. Э. Диксона* [2]. Современное изложение некоторых результатов, касающихся многочленов над конечным полем, можно найти в недавно вышедшей в свет книге *А. А. Альберта* [1].

1. Сохраним обозначения, применяемые в введении. Тогда справедлива

Теорема. *Пусть $f(x)$ — многочлен степени n над полем $\mathbf{T}$. Тогда для числа σ_i $(1 \leqq i \leqq n)$ имеет место*

$$i\sigma_i \equiv \sum_{t/i} \mu\left(\frac{i}{t}\right) \tau(\mathbf{C}^t) \pmod{p},$$

где $\mu(\xi)$ — функция Мебиуса, а $\tau(\mathbf{C}^t)$ обозначает след матрицы $\mathbf{C}^t$.[1])

Доказательство. Пусть (1) — разложение многочлена $f(x)$ на разные неприводимые факторы над полем $\mathbf{T}$. В работе [11] автором было доказано, что матрица $\mathbf{C}$ подобна матрице

$$\mathbf{N} = \operatorname{diag}[\mathbf{N}^{(1)}, \mathbf{N}^{(2)}, \ldots, \mathbf{N}^{(r)}],$$

где каждая матрица $\mathbf{N}^{(j)}$ имеет вид

$$\mathbf{N}^{(j)} = \begin{bmatrix} \mathbf{N}_1^{(j)} & \vdots & \mathbf{N}_2^{(j)} \\ \cdots & \cdots & \cdots \\ 0 & \vdots & \mathbf{N}_3^{(j)} \end{bmatrix}.$$

Притом $\mathbf{N}_1^{(j)}$ — квадратная матрица порядка m_j и вида

$$\mathbf{N}_1^{(j)} = \begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & & & & & 0 \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

[1]) Числа σ_i — неотрицательные целые числа, $\tau(C^t)$ — элементы поля $GF(q)$. Не опасаясь недоразумений, можем числа $\sigma_i \pmod p$ считать элементами тела $GF(p) \subset GF(q)$.

и $\mathbf{N}_3^{(j)}$ — квадратная матрица порядка $m_j(k_j - 1)$ и вида

$$\mathbf{N}_3^{(j)} = \begin{pmatrix} 0 & . & . & . & . & . \\ 0 & 0 & . & . & . & . \\ 0 & 0 & 0 & . & . & . \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & 0 & \end{pmatrix},$$

т. е. матрица, в которой все элементы главной диагонали и слева от нее равны нулю. Если $k_j = 1$, то член $\mathbf{N}_3^{(j)}$, конечно, отпадает. Отсюда следует, что матрица $\mathbf{C}$ подобна матрице

$$\mathbf{N}' = \begin{pmatrix} \mathbf{D} & \vdots & \mathbf{D}_1 \\ \cdots & \cdots & \cdots \\ 0 & \vdots & \mathbf{M} \end{pmatrix},$$

где

$$\mathbf{D} = \operatorname{diag}\left\{ \underbrace{1, \dots, 1}_{\sigma_1 \text{раз}}, \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\sigma_2 \text{раз}}, \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}}_{\sigma_3 \text{раз}}, \dots, \underbrace{\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}}_{\sigma_n \text{раз}} \right\}. \tag{5}$$

Если $n - \sum_{i=1}^{n} i\sigma_i = \sum_{j=1}^{r} m_j(k_j - 1) = 0$, то член $\mathbf{M}$ отпадает. Если же $n - \sum_{i=1}^{n} i\sigma_i \neq 0$, то $\mathbf{M}$ — матрица порядка $n - \sum_{i=1}^{n} i\sigma_i$ и вида

$$\mathbf{M} = \begin{pmatrix} 0 & . & . & . \\ & 0 & . & . \\ & & 0 & . \\ & & & 0 \end{pmatrix},$$

в которой все члены главной диагонали и слева от нее равны нулю.

Из соотношения (5), очевидно, следует $\tau(\mathbf{N}') = \tau(\mathbf{D}) + \tau(\mathbf{M}) \equiv \sigma_1 \pmod p$ и, ввиду того, что следы подобных матриц равны между собой, получаем

$$\sigma_1 \equiv \tau(\mathbf{C}) \pmod p.$$

В целях дальнейшего изложения заметим следующее: Если $\mathbf{R}$ — квадратная матрица порядка l и вида

$$\mathbf{R} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix},$$

то, если $k = \alpha_k l + \beta_k$, где α_k — целое число и $0 \leqq \beta_k < l$, имеет место соотношение

$$\mathbf{R}^k = \begin{bmatrix} 0\ 0\ \dots\ 0\ \overbrace{1}^{\beta_k+1}\ 0\ \dots\ 0 \\ 0\ 0\ \dots\ 0\ 0\ 1\ \dots\ 0 \\ \vdots \\ 0\ 0\ \dots\ 0\ 0\ 0\ \dots\ 1 \\ 1\ 0\ \dots\ 0\ 0\ 0\ \dots\ 0 \\ 0\ 1\ \dots\ 0\ 0\ 0\ \dots\ 0 \\ \vdots \\ 0\ 0\ \dots\ 1\ 0\ 0\ \dots\ 0 \end{bmatrix}.$$

В частности, $\mathbf{R}^l = \mathbf{E}_l$, где $\mathbf{E}_l$ — единичная матрица порядка l. Очевидно, будет

$$\tau(\mathbf{R}^k) = \begin{cases} 0 & \text{для } l \nmid k, \\ l & \text{для } l \mid k. \end{cases} \tag{6}$$

Пусть теперь k — произвольное целое положительное число и $k' > k'' > \dots > 1$ — все делители числа k, меньшие чем k. Рассмотрим матрицу $\mathbf{N}'^k$, подобную матрице $\mathbf{C}^k$

$$\mathbf{N}'^k = \begin{bmatrix} \mathbf{D}^k & \vdots & \mathbf{D}_k \\ \dots\dots\dots & & \\ 0 & \vdots & \mathbf{M}^k \end{bmatrix},$$

$$\mathbf{D}^k = \operatorname{diag}\left\{ \underbrace{1,}_{\sigma_1\text{раз}}\ \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^k}_{\sigma_2\text{раз}},\ \underbrace{\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}^k}_{\sigma_3\text{раз}}, \dots,\ \underbrace{\begin{bmatrix} 0 & 1 & 0 & \dots & \overbrace{0}^{n} \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}^k}_{\sigma_n\text{раз}} \right\}.$$

Для каждого $k > 0$ будет $\tau(\mathbf{M}^k) = 0$. Так как, далее, $\tau(\mathbf{C}^k) = \tau(\mathbf{N}'^k) = \tau(\mathbf{D}^k)$, получаем в силу (6)

$$\begin{aligned} &\tau(\mathbf{C}^k) \equiv k\sigma_k + k'\sigma_{k'} + \dots + \sigma_1 \pmod p, \\ &\tau(\mathbf{C}^k) \equiv \sum_{t/k} t\sigma_t \pmod p. \end{aligned} \tag{7}$$

Если написать эти соотношения для $k = 1, 2, \dots, n$ и воспользоваться формулой Мебиуса для инверсии, то мы получим

$$k\sigma_k \equiv \sum_{t/k} \mu\left(\frac{k}{t}\right) \tau(\mathbf{C}^t) \pmod p. \tag{8}$$

Этим самым наша теорема доказана.

Замечание 1. Соотношение (7) показывает, что след $\tau(\mathbf{C}^k)$ является для каждого $k > 0$ элементом поля $GF(p)$, содержащегося в $\mathbf{T} = GF(p^s)$.

Расписанные в явном виде соотношения (7) имеют вид

$$\begin{aligned} \sigma_1 &\equiv \tau(\mathbf{C}), \\ 2\sigma_2 + \sigma_1 &\equiv \tau(\mathbf{C}^2), \\ 3\sigma_3 + \sigma_1 &\equiv \tau(\mathbf{C}^3), \\ 4\sigma_4 + 2\sigma_2 + \sigma_1 &\equiv \tau(\mathbf{C}^4) \pmod{p}. \\ &\vdots \end{aligned} \tag{9}$$

Если $n < p$, то система (9) однозначно определяет числа $\sigma_1, \sigma_2, \ldots, \sigma_n$ как целые числа, удовлетворяющие неравенствам $0 \leqq \sigma_i < p$ $(i = 1, 2, \ldots, n)$.

Если же $n \geqq p$, то система (9) не дает никаких сведений о числах $\sigma_p, \sigma_{2p}, \sigma_{3p}, \ldots$. Действительно, соответствующие уравнения из системы (9) имеют вид

$$\begin{aligned} p\sigma_p + \sigma_1 &\equiv \tau(\mathbf{C}^p), \\ 2p\sigma_{2p} + p\sigma_p + 2\sigma_2 + \sigma_1 &\equiv \tau(\mathbf{C}^{2p}), \\ 3p\sigma_{3p} + p\sigma_p + 3\sigma_3 + \sigma_1 &\equiv \tau(\mathbf{C}^{3p}), \pmod{p}. \\ &\vdots \end{aligned} \tag{10}$$

Слагаемые, содержащие $\sigma_p, \sigma_{2p}, \sigma_{3p}, \ldots$, суть $\equiv 0 \pmod{p}$, и соотношения (10) сводятся к первым из уравнений (9) вместе с равенствами $\tau(\mathbf{C}^p) = \tau(\mathbf{C})$, $\tau(\mathbf{C}^{2p}) = \tau(\mathbf{C}^2)$, ..., которые можно доказать и непосредственно. В этом случае и числа $\sigma_1, \sigma_2, \ldots, \sigma_{p-1}, \sigma_{p+1}, \ldots, \sigma_{2p-1}, \sigma_{2p+1}, \ldots$ не определяются однозначно, но только $\pmod{p}$. (В конкретных случаях можно, конечно, иногда выйти из положения, воспользовавшись еще тривиальным неравенством $\sigma_1 + 2\sigma_2 + \ldots + n\sigma_n \leqq n$.)

Из полученных результатов можно непосредственно вывести следующие следствия:

Следствие 1. *Пусть степень многочлена $f(x)$ меньше, чем число p. Тогда $f(x) = 0$ обладает в поле $\mathbf{T}$ корнем в том и только в том сличае, если $\tau(\mathbf{C}) \neq 0$. При выполнении этого условия число различных корней дано соотношением $\sigma_1 \equiv \tau(\mathbf{C}) \pmod{p}$.*

Следствие 2. *Пусть степень n многочлена $f(x)$ меньше, чем число p. Тогда $f(x)$ бидет неприводимым над $\mathbf{T}$ в том и только в том случае, если $\tau(\mathbf{C}^n) = n$, но для каждого делителя t числа n, $t < n$, бидет $\tau(\mathbf{C}^t) = 0$.*

Доказательство. Пусть $n' > n'' > \ldots > 1$ — все делители числа n, меньшие чем n. Тогда

$$n\sigma_n + n'\sigma_{n'} + \ldots + \sigma_1 \equiv \tau(\mathbf{C}^n) \pmod{p}. \tag{11}$$

Если $f(x)$ — неприводимый многочлен, то $\sigma_n = 1$, $\sigma_{n'} = \sigma_{n''} = \ldots = \sigma_1 = 0$. Из соотношения (11) следует $\tau(\mathbf{C}^n) = n$. Для каждого делителя t числа n, $t < n$, из соотношения $\sum\limits_{k/t} k\sigma_k \equiv \tau(\mathbf{C}^t) \pmod{p}$ и из предположения $\sigma_t = \sigma_{t'} = \ldots = \sigma_1 = 0$ вытекает, что $\tau(\mathbf{C}^t) = 0$.

Допустим наоборот, что условия следствия 2 выполняются. Формула (8) дает

$$\sigma_n \equiv \frac{1}{n} \sum_{t/n} \mu\left(\frac{n}{t}\right) \tau(\mathbf{C}^t) \pmod{p}.$$

Так как все слагаемые в правой части, за исключением последнего, равны нулю, имеем

$$\sigma_n \equiv \frac{1}{n} \mu(1)\, \tau(\mathbf{C}^n) \equiv \frac{n}{n} \equiv 1 \pmod{p}.$$

Итак, $\sigma_n = 1$, т. е. полином $f(x)$ является неприводимым над $\mathbf{T}$.

Замечание 2. Ясно, что для использования формул (9) существенно знать матрицы $\mathbf{C}, \mathbf{C}^2, \ldots, \mathbf{C}^n$. Натрицы $\mathbf{C}^t$ для $t > 1$ можно построить и несколько иным способом, чем если считать их только степенями матрицы $\mathbf{C}$.

Рассмотрим соотношения

$$x^{kq} \equiv c_{k,0}^{(1)} + c_{k,1}^{(1)} x + \ldots + c_{k,n-1}^{(1)} x^{n-1} \pmod{f(x)} \tag{12}$$

для $k = 0, 1, \ldots, n-1$, причем ради единства обозначений в дальнейшем мы положили $c_{k,i}^{(1)} = c_{k,i}$.

Возведя соотношение (12) в q-ю степень, мы получаем

$$x^{kq^2} \equiv c_{k,0}^{(1)} + c_{k,1}^{(1)} x^q + \ldots + c_{k,n-1}^{(1)} x^{q(n-1)} \pmod{f(x)}.$$

Если сюда подставить зхачения $x^q, x^{2q}, \ldots, x^{(n-1)q}$ из соотношений (2), то получается

$$x^{kq^2} \equiv c_{k,0}^{(2)} + c_{k,1}^{(2)} x + \ldots + c_{k,n-1}^{(2)} x^{n-1} \pmod{f(x)}.$$

Очевидно, что матрица $(c_{k,i}^{(2)})$ тождественна матрице $\mathbf{C}^2$.

Аналогично, если x^{kq^l}, $l \geqq 1$, $k = 0, 1, \ldots, (n-1)$, выразить $(\mathrm{mod}\, f(x))$ в виде

$$x^{kq^l} \equiv c_{k,0}^{(l)} + c_{k,1}^{(l)} x + \ldots + c_{k,n-1}^{(l)} x^{n-1} \pmod{f(x)}, \tag{12a}$$

то матрица коэффициентов $(c_{k,i}^{(l)})$ в точности равна матрице $\mathbf{C}^l$.

Это замечание иногда полезно при действительном построении матрицы $\mathbf{C}^l$ $(l = 1, 2, \ldots, n)$.

2. В этом параграфе мы укажем несколько применений выведенной формулы. Первый пример имеет численный характер.

Пример 1. Требуется найти степени неприводимых факторов многочлена

$$f(x) = x^5 + 2x^4 + 3x^3 + x^2 + 4x + 4$$

над полем $GF(5)$.

Последовательным возведением в степень получаем

$$x^5 \equiv 3x^4 + 2x^3 + 4x^2 + x + 1, \quad x^{10} \equiv 2x^4 + 2x^3 + x^2 + 1,$$
$$x^{15} \equiv x^4 + 3x^3 + 4x^2 + 2x + 1, \quad x^{20} \equiv 3x^3 + 4x + 4 \pmod{f(x)}.$$

Матрица $\mathbf{C}$ и ее степени имеют вид

$$\mathbf{C} = \begin{vmatrix} 1&0&0&0&0 \\ 1&1&4&2&3 \\ 1&0&1&2&2 \\ 1&2&4&3&1 \\ 4&4&0&3&0 \end{vmatrix}, \quad \mathbf{C}^2 = \begin{vmatrix} 1&0&0&0&0 \\ 0&2&1&0&3 \\ 2&2&4&4&4 \\ 4&2&4&4&2 \\ 1&0&3&2&0 \end{vmatrix}, \quad \mathbf{C}^3 = \begin{vmatrix} 1&0&0&0&0 \\ 0&4&4&0&3 \\ 3&1&3&1&3 \\ 2&3&3&0&3 \\ 1&4&2&2&3 \end{vmatrix},$$

$$\mathbf{C}^4 = \begin{vmatrix} 1&0&0&0&0 \\ 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{vmatrix}, \quad \mathbf{C}^5 = \mathbf{C}.$$

Итак, $\tau(\mathbf{C}) = 1$, $\tau(\mathbf{C}^2) = 1$, $\tau(\mathbf{C}^3) = 1$, $\tau(\mathbf{C}^4) = 0$, $\tau(\mathbf{C}^5) = 1$. Соотношения (9) дают в нашем случае

$$(13) \qquad \sigma_1 \equiv 1\,, \quad 2\sigma_2 + \sigma_1 \equiv 1\,, \quad 3\sigma_3 + \sigma_1 \equiv 1\,, \quad 4\sigma_4 + 2\sigma_2 + \sigma_1 \equiv 0\,, \quad 5\sigma_5 + \sigma_1 \equiv 1 \pmod 5\,.$$

С учетом неравенства $\sigma_1 + 2\sigma_2 + 3\sigma_3 + 4\sigma_4 + 5\sigma_5 \leqq 5$ из соотношений (13) следует $\sigma_1 = 1$, $\sigma_2 = \sigma_3 = 0$, $\sigma_4 = 1$, $\sigma_5 = 0$.

Итак, многочлен $f(x)$ можно над полем $GF(5)$ разложить на один линейный фактор и на один неприводимый фактор четвертой степени.

Пример 2. Требуется найти степени неприводимых факторов многочлена

$$f(x) = x^n - a\,, \quad a \in \mathbf{T} = GF(q)\,, \quad a \neq 0\,,$$

над полем $\mathbf{T}$.

Для нахождения матрицы $\mathbf{C}^\rho$ ($\rho \geqq 1$) достаточно выразить 1, x^{q^ρ}, x^{2q^ρ}, ..., $x^{(n-1)q^\rho} \pmod{x^n - a}$ в виде (12a). Коэффициенты соответствующей подстановки дают матрицу $\mathbf{C}^\rho$.

Для каждого k, $0 \leqq k \leqq n-1$, можно написать

$$(14) \qquad kq^\rho = l_k^{(\rho)} \cdot n + r_k^{(\rho)}\,,$$

где $l_k^{(\rho)}$ — неотрицательное целое число и $0 \leqq r_k^{(\rho)} < n$. Из равенства $x^{kq^\rho} = (x^n)^{l_k^{(\rho)}} \cdot x^{r_k^{(\rho)}}$ следует

$$x^{kq^\rho} \equiv a^{l_k^{(\rho)}} \cdot x^{r_k^{(\rho)}} \pmod{f(x)}\,.$$

Из этого представления видно, что в каждой строке матрицы $\mathbf{C}^\rho$ имеется лишь один отличный от нуля элемент. В $(k+1)$-й строке это будет элемент, лежащий в $(r_k^{(\rho)} + 1)$-м столбце. Этот элемент равен $a^{l_k^{(\rho)}}$. Так как нас интересует лишь след матрицы $\mathbf{C}^\rho$, достаточно найти только элементы главной диагонали матрицы $\mathbf{C}^\rho$. Элемент $a^{l_k^{(\rho)}}$ лежит на главной диагонали для тех k, для которых $r_k^{(\rho)} = k$, т. е. в силу (14) для тех k, для которых $kq^\rho \equiv k \pmod n$. Если обозначить

$d_\rho = (q^\rho - 1, n)$, то это будут числа $k = 0, n/d_\rho, 2 \cdot n/d_\rho, \ldots, (d_\rho - 1) \cdot n/d_\rho$. Для соответствующих $l_k^{(\rho)}$ из соотношения (14) вытекает $l_k^{(\rho)} = k(q^\rho - 1)/n$. Итак, для следа матрицы $\mathbf{C}^\rho$ мы получаем:

$$\tau(\mathbf{C}^\rho) = \sum_k a^{k(q^\rho-1)/n} = \sum_{j=0}^{d_\rho-1} a^{j(n/d_\rho)(q^\rho-1)/n} = \sum_{j=0}^{d_\rho-1} a^{j(q^\rho-1)/d_\rho},$$

то есть

$$\tau(\mathbf{C}^\rho) = \begin{cases} d_\rho, & \text{если } a^{(q^\rho-1)/d_\rho} = 1, \\ 0, & \text{если } a^{(q^\rho-1)/d_\rho} \neq 1. \end{cases} \tag{15}$$

Формула $k\sigma_k \equiv \sum_{\rho/k} \mu(k/\rho)\, \tau(\mathbf{C}^\rho) \pmod p$ вместе с соотношениями (15) дает числа $\sigma_k \pmod p$ для всех k, для которых $p \nmid k$. (Если $n < p$, то числа σ_k определяются таким образом однозначно.)

Замечание. Для случая $q = p$ эта формула была выдевена автором иным способом в работе [9]. В работе [10] (см. также Редей [6]) автор доказал, кроме того, что если в случае $q = p$ обозначить

$$\delta_t = \begin{cases} d_t, & \text{если } a^{(p^t-1)/d_t} = 1, \\ 0, & \text{если } a^{(p^t-1)/d_t} \neq 1, \end{cases}$$

и если предположить $(n, p) = (a, p) = 1$, то формула $\sigma_k = 1/k \sum_{t/k} \mu(k/t)\, \delta_t$ дает непосредственно значение числа σ_k для каждого k. (Слово „непосредственно" означает, что эти значения получаем не только по модулю p, но и в абсолютном смысле слова.) В работе [10] приводится аналогичная формула и для случая $q = p^s$, $s > 1$.

Пример 3. Пусть $a \neq 0$, b — элементы поля $\mathbf{T} = GF(p^s)$. Пусть m/s. Исследуем разложимость многочлена

$$f(x) = x^{p^m} - ax - b \tag{16}$$

над полем $\mathbf{T}$.

Положим $r = p^m$. Если $s = m \cdot l$ (l — целое число), то $q = p^s = r^l$. Из соотношения

$$x^r \equiv ax + b \pmod{f(x)}$$

мы получаем последовательным возведением в степень

$$\begin{aligned} x^{r^2} &\equiv a^{1+r}x + a^r b + b^r, \\ x^{r^3} &\equiv a^{1+r+r^2}x + a^{r^2+r}b + a^r \cdot b^r + b^{r^2}, \\ &\vdots \\ x^{r^l} &\equiv a^{1+r+r^2+\ldots+r^{l-1}}\, x + \beta, \pmod{f(x)}, \end{aligned}$$

где

$$\beta = a^{r^{l-1}+r^{l-2}+\ldots+r} \cdot b + a^{r^{l-1}+r^{l-2}+\ldots+r^2} b^r + \ldots + a^{r^{l-1}} b^{r^{l-2}} + b^{r^{l-1}} =$$
$$= a^{(q-r)/(r-1)} b + a^{(q-r^2)/(r-1)} b^r + a^{(q-r^3)/(r-1)} b^{r^2} + \ldots + a^{(q-r^{l-1})/(r-1)} b^{r^{l-2}} + b^{r^{l-1}}.$$

Если положить

$$\alpha = a^{1+r+r^2+\ldots+r^{l-1}} = a^{(q-1)/(r-1)},$$

то получаем наконец,

$$x^q \equiv \alpha x + \beta \pmod{f(x)}. \tag{16a}$$

Соотношения (2) имеют вид

$$\begin{aligned}
&x^0 \equiv 1,\\
&x^q \equiv \beta + \alpha x,\\
&x^{2q} \equiv \beta^2 + 2\alpha\beta x + \alpha^2 x^2,\\
&\vdots\\
&x^{(r-1)q} \equiv \beta^{r-1} + (r-1)\beta^{r-2}\alpha x + \ldots + \alpha^{r-1}x^{r-1} \pmod{f(x)}.
\end{aligned}$$

Матрица $\mathbf{C}$ имеет, следовательно, вид

$$\mathbf{C} = \begin{pmatrix}
1 & 0 & 0 & \ldots & 0 & 0\\
. & \alpha & 0 & \ldots & 0 & 0\\
. & . & \alpha^2 & \ldots & 0 & 0\\
\vdots & & & & & \\
. & . & . & & \alpha^{r-2} & 0\\
. & . & . & & 0 & \alpha^{r-1}
\end{pmatrix},$$

где все элементы справа от главной диагонали равны нулю.

Аналогичный вид имеет в матрица $\mathbf{C}^t$, причем главная диагональ содержит элементы $1, \alpha^t, \alpha^{2t}, \ldots, \alpha^{(r-1)t}$. Итак,

$$\tau(\mathbf{C}^t) = \sum_{j=0}^{r-1} \alpha^{jt} = \begin{cases} 0 & \text{для тех } t, \text{ для которых } \alpha^t = 1,\\ 1 & \text{для тех } t, \text{ для которых } \alpha^t \neq 1. \end{cases}$$

Теперь мы будем различать следующие случаи:

А. Пусть $\alpha = a^{(q-1)/(r-1)}$ принадлежит к показателю $e > 1$. Это возможно только тогда, если $r > 2$. Очевидно, $e/r - 1$. Так как в таком случае $\tau(\mathbf{C}) = \tau(\mathbf{C}^2) = \ldots = \tau(\mathbf{C}^{e-1}) = 1$ и $\tau(\mathbf{C}^e) = 0$, то мы получаем из соотношений

$$\begin{aligned}
&\sigma_1 \equiv \tau(\mathbf{C}),\\
&e\sigma_e \equiv \sum_{k/e} \mu(e/k)\,\tau(\mathbf{C}^k) = \sum_{k/e} \mu(e/k)\,1 - \mu(1) + \mu(1)\,\tau(\mathbf{C}^e) \pmod{p},
\end{aligned}$$

с одной стороны,

$$\sigma_1 \equiv 1 \pmod{p}, \tag{17}$$

и далее, $e\sigma_e \equiv -1 \pmod{p}$, то есть

$$\sigma_e \equiv (r-1)/e \pmod{p}. \tag{18}$$

α) Если $e = r - 1$, т. е. a есть примитивный элемент поля $GF(q)$, то $\sigma_1 \equiv 1$, $\sigma_{r-1} \equiv 1 \pmod{p}$. Итак, $\sigma_1 = 1$, $\sigma_{r-1} = 1$. Мы доказали:

Следствие 1. *Пусть* a *— примитивный элемент поля* $\mathbf{T} = GF(p^s)$. *Пусть* $r = p^m > 2$, *где* m/s. *Тогда*

$$x^r - ax - b\,, \quad a, b \in \mathbf{T}$$

можно разложить над полем $\mathbf{T}$ *на один линейный фактор и на один неприводимый фактор степени* $r - 1$.

Это утверждение представляет собой обобщение Альберта одной более старой теоремы Диксона. (См. А. А. Альберт [1], стр. 141.)

β) Предложим в (16), что $m = 1$. Тогда из соотношения (18) следует, что многочлен $x^p - ax - b$ имеет по крайней мере $(p-1)e$ различных неприводимых факторов степени e и хоть один линейный фактор. В силу соотношения $\sigma_1 + e\sigma_e \leqq p$ он не может, однако, иметь большее количество неприводимых факторов степени e. Итак, справедливо

Следствие 2. *Пусть* $p > 2$, $q = p^s$ $(s \geqq 1)$. *Пусть* $a^{(q-1)/(p-1)}$ *принадлежит к показателю* e. *Тогда многочлен* $x^p - ax - b$, $a, b \in GF(q)$ *распадается над полем* $GF(q)$ *на один линейный фактор и на* $(p-1)/e$ *неприводимых факторов степени* e.

γ) Если предположить в случае многочлена (16), что $e \geqq (r-1)/(p-1)$, то $(r-1)/e \leqq p-1$, т. е. (16) имеет по крайней мере $(r-1)/e$ неприводимых факторов степени e. В силу соотношения $\sigma_1 + e\sigma_e \leqq r$ и здесь не может существовать большее количество разных неприводимых факторов степени e. Итак, имеет место

Следствие 3. *Пусть* $r = p^m > 2$, $q = p^s$ *и* m/s. *Если* $a^{(q-1)/(r-1)}$ *принадлежит к показателю* $e > 1$ *и* $e \geqq (r-1)/(p-1)$, *то многочлен* $x^r - ax - b$, $a, b \in GF(q)$ *можно разложить над полем* $GF(q)$ *на один линейный фактор и* $(r-1)/e$ *различных неприводимых факторов степени* e.

Замечание. Можно доказать (см. [12]), что следствие 3 справедливо и без предложения $e \geqq (r-1)/(p-1)$. Нашим методом этого доказать, конечно, нельзя так как σ_e определяется формулой (18) вплоть до целочисленного кратного числа p.

Б. Исследуем теперь случай $\alpha = a^{(q-1)/(r-1)} = 1$. В этом случае будет для каждого $t > 0$ $\tau(\mathbf{C}^t) = 0$. Из соотношений $k\sigma_k \equiv \sum_{t/k} \mu(k/t)\,\tau(\mathbf{C}^t) \pmod p$ мы получаем $\sigma_k \equiv 0 \pmod p$ для всех k, для которых $(k, p) = 1$.

В случае $r = p$ можно рассуждать так: В виду того, что $k\sigma_k \leqq p$, будет обязательно $\sigma_2 = \sigma_3 = \ldots = \sigma_{p-1} = 0$. Следовательно, будет или $\sigma_1 = 0$ и тогда $\sigma_p = 1$, или $\sigma_1 = p$ и тогда $\sigma_p = 0$.

Соотношение $\sigma_1 = p$ означает, что все нули многочлена $x^p - ax - b$, $a, b \in$ $\in GF(q)$ лежат в поле $GF(q)$. Так как каждый элемент $\in GF(q)$ удовлетворяет

$x^q - x = 0$, из соотношения (16а), в котором $l = s$, $r = p$, $\alpha = 1$, вытекает соотношение $\beta = 0$, т. е.

$$a^{(q-p)/(p-1)}b + a^{(q-p^2)/(p-1)}b^p + a^{(q-p^3)/(p-1)}b^{p^2} + \\ + \ldots + a^{(q-p^{s-1})/(p-1)}b^{p^{s-2}} + b^{p^{s-1}} = 0\,. \tag{19}$$

Наоборот, если имеет место (19), то для любого нуля многочлена $x^p - ax - b$ справедливо соотношение $x^q - x = 0$, т. е. каждый нуль лежит в поле $GF(q)$. Этим мы доказали

Следствие 4. *Пусть* $a, b \in GF(p^s)$, $s \geqq 1$, $a^{(p^s-1)/(p-1)} = 1$. *Тогда многочлен* $x^p - ax - b$ *будет над полем* $GF(p^s)$ *или неприводимым, или будет распадаться на* p *линейных факторов. Второй случай наступает тогда и только тогда, если выполняется соотношение* (19).

Этот результат обобщает известную теорему, выведенную *O. Ope* ([3]).

В частности: *Многочлен* $x^p - x - b$, $b \in GF(p^s)$ *является над полем* $GF(p^s)$ *или неприводимым, или распадается на* p *линейных факторов. Последний случай наступает тогда и только тогда, если* $b + b^p + \ldots + b^{p^{s-1}} = 0$.

Этот частный случай представляет собой очень хорошо известный результат. (См., напр., А. А. Альберт [1], стр. 140.)

Замечание. Мы не произвели подробного анализа разложимости многочлена $x^{p^m} - ax - b$, $m > 1$, $\alpha = 1$, так как наши соотношения $\sigma_k \equiv 0 \pmod p$ для $(k, p) = 1$ не дают возможности в каждом случае определить числа σ_k однозначно. Подробное обсуждение разложимости многочлена (16) для всех возможных случаев было проведено на основании формул (4) в работе автора [12].

Литература

[1] *A. A. Albert*: Fundamental concepts of higher algebra. Univ. of Chicago Press, 1956.

[2] *L. E. Dickson*: History of the Theory of Numbers. Vol. I, New York, reprinted 1934.

[3] *O. Ore:* Contributions to the theory of finite fields. Trans. Amer. Math. Soc. *36* (1934), 243—274.

[4] *K. Petr:* Über die Reduzibilität eines Polynoms mit ganzzahligen Koeffizienten nach einem Primzahlmodul. Časopis pěst. mat. fys. *66* (1937), 85—94.

[5] *L. Rédei:* Algebra. Akademische Verlagsgesellschaft, Leipzig, 1959.

[6] *L. Rédei:* A short proof of a theorem of Š. Schwarz concerning finite fields. Časopis pěst. mat. fys. *75* (1950), 211—212.

[7] *L. Rédei-P. Turán:* Zur Theorie der algebraischen Gleichungen über endlichen Körpern. Acta aritmetica *5* (1959), 223—225.

[8] *Š. Schwarz:* Contribution à la réductibilité des polynômes dans la théorie des congruences. Věstník Král. české spol. nauk, Třída matemat.-přírodověd. (1939), 1—7.

[9] *Š. Schwarz:* Příspěvek k reducibilitě binomických kongruencí. Časopis pěst. mat. fys. *71* (1946), 21—31.

[10] *Š. Schwarz:* On the reducibility of binomial congruences and the bound of the least integer belonging to a given exponent (mod p). Časopis pěst. mat. fys. *74* (1949), 1—16.
[11] *Š. Schwarz:* On the reducibility of polynomials over a finite field. Quart. J. of Math. (Oxford) (2) *7* (1956), 110—124.
[12] *Š. Schwarz:* Об обном классе полиномов над конечным полем. Mat. fyz. čas. SAV, *10* (1960), 68—80.[2])

Summary

ON THE NUMBER OF IRREDUCIBLE FACTORS OF A POLYNOMIAL OVER A FINITE FIELD

ŠTEFAN SCHWARZ (Bratislava)

The main result of this paper is the proof of the following Theorem:

Let $f(x)$ be a polynomial of degree n over the finite field $GF(q)$, $q = p^s$, where p is a prime and $s \geqq 1$. Let $\mathbf{C}$ by the matrix of the substitution (2). Let $\sigma_i\,(1 \leqq i \leqq n)$ be the number of different irreducible factors of $f(x)$ of degree i. We then have

$$i\sigma_i \equiv \sum_{t/i} \mu(i/t)\, \tau(\mathbf{C}^t) \pmod{p},$$

where $\mu(\xi)$ is the Möbius function and $\tau(\mathbf{C}^t)$ the trace of the matrix $\mathbf{C}^t$.

Some applications of this formula are given.

[2]) (Замечание при корректуре, 20/V 1961 г.) Определением числа σ_1 занимается в последное время тоже работа: *Б. Сегре (B. Segre):* Sulla teoria delle equazioni e delle congruenze algebriche (Note I e II). Rend. Accad. Naz. dei Lincei, (*8*) *27* (1959), 155—161 e 303—311.