

Matematicko-fyzikálny časopis

Kornélia Horáková; Štefan Schwarz

Циклические матрицы и алгебраические уравнения над конечным полем

Matematicko-fyzikálny časopis, Vol. 12 (1962), No. 1, 36--46

Persistent URL: <http://dml.cz/dmlcz/126590>

Terms of use:

© Mathematical Institute of the Slovak Academy of Sciences, 1962

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

ЦИКЛИЧЕСКИЕ МАТРИЦЫ И АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ НАД КОНЕЧНЫМ ПОЛЕМ

КОРНЕЛИЯ ГОРАКОВА (Kornélia Horáková), Братислава
и ШТЕФАН ШВАРЦ (Štefan Schwarz), Братислава

Пусть

$$(1) \quad f(x) = a_0 + a_1x + \dots + a_{q-2}x^{q-2}, \quad a_0 \neq 0,$$

полином степени не более $q - 2$ над конечным полем $GF(q)$, $q = p^s$, $s \geq 1$, где p — простое число. Пусть \mathbf{A} — циклическая матрица

$$(2) \quad \mathbf{A} = \begin{pmatrix} a_0 & a_1 & a_2 \dots a_{q-2} \\ a_{q-2} & a_0 & a_1 \dots a_{q-3} \\ \vdots & & \vdots \\ a_1 & a_2 & a_3 \dots a_0 \end{pmatrix}.$$

Известна теорема Кенига-Радоса (смотри [3], стр. 501), которая формулируется так: Пусть σ_1 — число различных корней уравнения $f(x) = 0$ в поле $GF(q)$ и h — ранг матрицы \mathbf{A} . Тогда $\sigma_1 = q - 1 - h$.

В первом разделе этой работы доказано более общее утверждение, из которого вытекает эта теорема как частный случай. Одновременно обобщена и одна из теорем из работы [4]. (Смотри также [6].)

Пусть σ_i ($1 \leq i \leq q - 2$) обозначает число различных неприводимых факторов полинома (1) степени i . Во втором разделе выведена формула для числа σ_i , в которой выступают ранги некоторых циклических матриц порядков $q - 1$, $q^2 - 1, \dots, q^i - 1$.

В третьем разделе выведены формулы для числа $\sigma_i \pmod{p}$, в которых выступают следы степеней тех же самых циклических матриц.

В случае $s = 1$ Гурвиц вывел формулу, которая определяет число $\sigma_1 \pmod{p}$, используя коэффициенты полинома (1). Поскольку мы смогли установить, нигде в литературе не указывалось на прямую связь формулы Гурвица с матрицей \mathbf{A} . В четвертом разделе показываем, как вытекает обобщенная формула Гурвица из результатов раздела 1. Одновременно найдены аналогичные формулы к формуле Гурвица для числа $\sigma_i \pmod{p}$ и для случая $i > 1$.

Использование выведенных формул для вычислений вызывает трудности. потому что выступающие циклические матрицы очень высокого порядка. В пятом разделе показано, как можно задачу свести к исследованию k матриц порядка $(q - 1)/k$, где $k/(q - 1)$.

1

В дальнейшем будем пользоваться такими обозначениями. Пусть b_0, b_1, \dots, b_{r-1} — элементы поля \mathbf{T} . Пусть n — натуральное число, $n \geq r$. Под символом $\mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n)$ будем понимать матрицу n -того порядка, которая получится таким образом:

а) Если $n = r$, то ее первой строкой является $(b_0, b_1, \dots, b_{r-1})$, а остальные строки возникнут из первой циклической заменой;

б) если $n > r$, то первая строка — $(b_0, b_1, \dots, b_{r-1}, \underbrace{0, \dots, 0}_{(n-r) \text{ раз}})$, а остальные

получим из нее циклической заменой. Значит,

$$\begin{pmatrix} b_0 & b_1 \dots b_{r-1} & 0 & \dots & 0 & 0 \\ 0 & b_0 \dots b_{r-2} & b_{r-1} & \dots & 0 & 0 \\ \vdots & & & & & \\ b_1 & b_2 \dots 0 & 0 & \dots & 0 & b_0 \end{pmatrix}.$$

Пусть \mathbf{T} и n — такие, что уравнение

$$(3) \quad x^n - 1 = 0$$

не имеет многократных корней, т. е. n не является кратным характеристики поля \mathbf{T} . Обозначим корни уравнения (3) через $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$. Тогда матрица Вандермонда

$$\mathbf{V}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \varepsilon_1 & \varepsilon_2 & \dots & \varepsilon_n \\ \vdots & \vdots & & \vdots \\ \varepsilon_1^{n-1} & \varepsilon_2^{n-1} & \dots & \varepsilon_n^{n-1} \end{pmatrix}$$

имеет определитель отличный от нуля. Если обозначим $f(z) = b_0 + b_1 z + \dots + b_{r-1} z^{r-1}$, получим

$$(4) \quad \mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n) \mathbf{V}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) = \begin{pmatrix} f(\varepsilon_1) & f(\varepsilon_2) & \dots & f(\varepsilon_n) \\ \varepsilon_1 f(\varepsilon_1) & \varepsilon_2 f(\varepsilon_2) & \dots & \varepsilon_n f(\varepsilon_n) \\ \vdots & \vdots & & \vdots \\ \varepsilon_1^{n-1} f(\varepsilon_1) & \varepsilon_2^{n-1} f(\varepsilon_2) & \dots & \varepsilon_n^{n-1} f(\varepsilon_n) \end{pmatrix}.$$

Обозначим через σ число корней уравнения (3), которые являются одновременно корнями уравнения

$$f(z) = b_0 + b_1 z + \dots + b_{r-1} z^{r-1} = 0.$$

Если $\sigma \geq 1$, то можно без нарушения общности предположить, что рассматриваемыми корнями будут элементы $\varepsilon_{n-\sigma+1}, \varepsilon_{n-\sigma+2}, \dots, \varepsilon_n$. Тогда последние σ столбцов матрицы (4) имеют только нулевые элементы, значит, матрица (4) имеет ранг не более $n - \sigma$. Но этот ранг точно равен числу $n - \sigma$, потому что определитель матрицы, которая остается после отбрасывания последних σ столбцов и σ строк, равен элементу

$$f(\varepsilon_1) \dots f(\varepsilon_{n-\sigma}) \cdot |\mathbf{V}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-\sigma})|.$$

Этот результат, очевидно, остается в силе и если $\sigma = 0$.

Поскольку матрицы $\mathbf{Z}(b_0, \dots, b_{r-1}; n)$ и $\mathbf{Z}(b_0, \dots, b_{r-1}; n) \cdot \mathbf{V}(\varepsilon_1, \dots, \varepsilon_n)$ имеют одинаковый ранг, то можем сформулировать такую теорему:

Теорема 1. Пусть $F(x) = a_0 + a_1 x + \dots + a_{r-1} x^{r-1}$ — полином степени не более $r - 1$ над полем \mathbf{T} . Пусть $n > r - 1$ и пусть n не является кратным характеристике поля \mathbf{T} . Если σ обозначает число корней уравнения $x^n - 1 = 0$ циклической матрицы $\mathbf{Z}(a_0, a_1, \dots, a_{r-1}; n)$, то имеет место $\sigma = n - h$.

Примечание. Допустим, что $G(x) = c_0 + c_1 x + \dots + c_{r-1} x^{r-1}$, $c_{r-1} \neq 0$, полином степени $r - 1$ над полем \mathbf{T} и выполняется $n \leq r - 1$. Найдем два полинома $h(x)$ и $k(x)$ так, чтобы было $G(x) = (x^n - 1)k(x) + h(x)$, где $h(x)$ — полином степени меньше n . Если $h(x)$ — нулевой полином, то корнями уравнения $G(x) = 0$ будут все нулевые точки полинома $x^n - 1$. Если $h(x)$ — отличный от нуля полином, то каждая общая нулевая точка полиномов $G(x)$ и $x^n - 1$ будет также нулевой точкой полинома $h(x)$, и, наоборот, каждая общая нулевая точка полиномов $h(x)$ и $x^n - 1$ будет также нулевой точкой полинома $G(x)$. Поэтому можно нахождение общих нулевых точек полиномов $G(x)$ и $x^n - 1$ свести к нахождению общих нулевых точек полинома $x^n - 1$ и полинома $h(x)$, который имеет степень меньше n . Как раз этот случай и рассмотрен в теореме 1.

Из уравнения (4) следует для определителя циклической матрицы

$$|\mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n)| = f(\varepsilon_1) \dots f(\varepsilon_n).$$

Пусть \mathbf{E}_k , $k \geq 1$, обозначает в дальнейшем единичную матрицу порядка k . Матрица $\mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n) - \lambda \mathbf{E}_n = \mathbf{Z}(b_0 - \lambda, b_1, \dots, b_{r-1}; n)$ также циклическая. Значит, для ее определителя имеет место

$$|\mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n) - \lambda \mathbf{E}_n| = \varphi(\varepsilon_1) \cdot \varphi(\varepsilon_2) \dots \varphi(\varepsilon_n),$$

где $\varphi(z) = (b_0 - \lambda) + b_1 z + \dots + b_{r-1} z^{r-1} = f(z) - \lambda$. Поэтому

$$(5) \quad |\mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n) - \lambda \mathbf{E}_n| = (-1)^n [\lambda - f(\varepsilon_1)] [\lambda - f(\varepsilon_2)] \dots [\lambda - f(\varepsilon_n)].$$

Обозначим через s_k сумму всех главных миноров k -того порядка матрицы $\mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n)$. Известно, что

$$(6) \quad |\mathbf{Z}(b_0, b_1, \dots, b_{r-1}; n) - \lambda \mathbf{E}_n| = (-1)^n (\lambda^n - s_1 \lambda^{n-1} + s_2 \lambda^{n-2} + \dots + (-1)^n s_n).$$

Путем сравнения получаем:

$$(7) \quad \begin{aligned} s_1 &= \sum_{i=1}^n f(\varepsilon_i), \\ s_2 &= \sum_{\substack{i,k=1 \\ i \neq k}}^n f(\varepsilon_i) f(\varepsilon_k), \\ &\vdots \\ s_n &= f(\varepsilon_1) f(\varepsilon_2) \dots f(\varepsilon_n). \end{aligned}$$

Пусть в последовательности s_1, s_2, \dots, s_n последним отличным от нуля элементом будет s_t . Тогда утверждаем, что $\sigma = n - t$.

а) Если $s_n = s_{n-1} = \dots = s_{t+1} = 0$, но $s_t \neq 0$, то из соотношения (6) вытекает, что полином $\lambda^n - s_1 \lambda^{n-1} + \dots + (-1)^n s_n$ имеет $\lambda = 0$ в качестве $(n - t)$ -кратной нулевой точки. Из соотношения (5) вытекает, что среди элементов $f(\varepsilon_1), f(\varepsilon_2), \dots, f(\varepsilon_n)$ находится точно $n - t$ нулей, т. е. $x^n - 1 = 0$ имеет точно $n - t$ (различных) корней, которые одновременно удовлетворяют $f(x) = 0$.

б) Пусть, наоборот, $x^n - 1 = 0$ имеет $n - t$ (различных) корней, которые удовлетворяют $f(x) = 0$. Пусть это будут корни $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-t}$. Из соотношений (7) вытекает: $s_n = s_{n-1} = \dots = s_{t+1} = 0$ (так как каждое слагаемое направо имеет хотя бы один нулевой фактор), тогда как $s_t = f(\varepsilon_1) f(\varepsilon_2) \dots f(\varepsilon_{n-t}) \neq 0$. Тем самым мы доказали:

Теорема 2. Пусть $F(x) = a_0 + a_1 x + \dots + a_{r-1} x^{r-1}$ — полином не более $(r - 1)$ -ой степени над полем \mathbf{T} . Пусть $n > r - 1$ и пусть n не является кратным характеристики поля. Обозначим через s_k сумму всех главных миноров k -того порядка циклической матрицы $\mathbf{Z}(a_0, a_1, \dots, a_{r-1}; n)$. Пусть s_t — последний отличный от нуля элемент последовательности s_1, s_2, \dots, s_n и пусть σ обозначает число корней уравнения $x^n - 1 = 0$, которые являются одновременно корнями уравнения $F(x) = 0$. Тогда справедливо $\sigma = n - t$.

Примечание. Из теорем 1 и 2 следует: $h = t$.

2

Применим теорему 1 для случая конечных полей. Пусть \mathbf{T} — конечное поле, $\mathbf{T} = GF(q)$, где $q = p^s$, $s \geq 1$ и p — простое число. Пусть

$$(8) \quad f(x) = a_0 + a_1 x + \dots + a_{q-2} x^{q-2}, \quad a_i \in GF(q), \quad a_0 \neq 0,$$

полином не более $(q - 2)$ -ой степени над полем $\mathbf{T} = GF(q)$.

Пусть $i \geq 1$ — целое число и $i > i' > i'' > \dots > 1$ — все делители числа i . Если $\varphi(x)$ — некоторый неприводимый полином над полем \mathbf{T} степени i и $\varphi(j) = 0$, то известно, что в поле $\mathbf{T}(j) \simeq GF(q^i)$ лежат все корни всех неприводимых полиномов над T степеней $i, i', i'', \dots, 1$. Каждый ненулевой элемент поля $\mathbf{T}(j)$ притом удовлетворяет уравнению

$$(9) \quad x^{q^i - 1} - 1 = 0.$$

Это уравнение не имеет многократных корней.

Если $f(x)$ имеет σ_i различных неприводимых факторов степени i , дальше $\sigma_{i'}$ различных неприводимых факторов степени i', \dots, σ_1 линейных факторов, то (9) имеет как раз $i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1$ корней, которые удовлетворяют уравнению $f(x) = 0$.

Рассмотрим циклическую матрицу

$$(10) \quad \mathbf{A}_i = \mathbf{Z}(a_0, a_1, \dots, a_{q^i - 2}; q^i - 1).$$

Если ранг этой матрицы h_i , то согласно теореме 1 имеет место

$$i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1 = q^i - 1 - h_i,$$

$$\sum_{k/i} k\sigma_k = q^i - 1 - h_i.$$

Применяя формулу Мебиуса для инверсии, получаем

$$(11) \quad \sigma_i = \frac{1}{i} \sum_{k/i} \mu\left(\frac{i}{k}\right) (q^k - 1 - h_k).$$

Тем самым мы доказали обобщение теоремы Кенига-Радоса:

Теорема 3. Пусть (8) — полином не более $(q - 2)$ -ой степени над полем $GF(q)$. Пусть σ_i обозначает число различных неприводимых факторов степени $i \geq 1$ полинома (8). Если h_i — ранг матрицы (10), то имеет место формула (11).

3

В этом разделе покажем, что для взаимного соотношения матриц \mathbf{A}_i и чисел $\sigma_1, \sigma_2, \dots, \sigma_i$ существуют и другие интересные формулы.

Применим формулу (5) к полиному (8) и уравнению (9). Если все корни уравнения (9) — $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{q^i - 1}$, то согласно (5) имеет место

$$|\mathbf{A} - \lambda \mathbf{E}_{q^i - 1}| = [\lambda - f(\varepsilon_1)] [\lambda - f(\varepsilon_2)] \dots [\lambda - f(\varepsilon_{q^i - 1})].$$

Характеристическими корнями матрицы \mathbf{A}_i являются элементы $f(\varepsilon_1), \dots, f(\varepsilon_{q^i - 1})$. Поэтому характеристическими корнями матрицы $\mathbf{A}_i^{q^i - 1}$ являются элементы $[f(\varepsilon_1)]^{q^i - 1}, \dots, [f(\varepsilon_{q^i - 1})]^{q^i - 1}$. Однако

$$[f(\varepsilon_k)]^{q^i - 1} = \begin{cases} 0, & \text{если } \varepsilon_k \text{ — корень уравнения } f(x) = 0. \\ 1, & \text{если } \varepsilon_k \text{ — не корень уравнения } f(x) = 0. \end{cases}$$

Если оставим введенные выше обозначения, то спектр матрицы $\mathbf{A}_i^{q^{i-1}}$ состоит из $i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1$ нулей и $q^i - 1 - (i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1)$ единиц. Значит,

$$(12) \quad \left| \mathbf{A}_i^{q^{i-1}} - \lambda \mathbf{E}_{q^{i-1}} \right| = \lambda^{i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1} (\lambda - 1)^{q^i - 1 - (i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1)}.$$

Тем самым мы доказали:

Теорема 4. Пусть $i \geq 1$ — натуральное число, пусть $i > i' > i'' > \dots > 1$ — все делители числа i и пусть \mathbf{A}_i — циклическая матрица (10) порядка q^{i-1} . Тогда для характеристического полинома матрицы $\mathbf{A}_i^{q^{i-1}}$ имеет место формула (12).

Пусть $\text{Sp}(\mathbf{B})$ обозначает в дальнейшем след матрицы \mathbf{B} . Из соотношения (12) следует, что в поле $GF(q)$ справедливо

$$\text{Sp}(\mathbf{A}_i^{q^{i-1}}) = (i\sigma_i + \dots + \sigma_1) \cdot 0 + (q^i - 1 - i\sigma_i - i'\sigma_{i'} - \dots - \sigma_1) \cdot 1.$$

Значит, $\text{Sp}(\mathbf{A}_i^{q^{i-1}})$ — элемент поля $GF(p) \subset GF(q)$ и справедливо

$$i\sigma_i + i'\sigma_{i'} + \dots + \sigma_1 \equiv -1 - \text{Sp}(\mathbf{A}_i^{q^{i-1}}) \pmod{p},$$

$$\sum_{i/k} k\sigma_k \equiv -1 - \text{Sp}(\mathbf{A}_i^{q^{i-1}}) \pmod{p},$$

$$i\sigma_i \equiv \sum_{k|i} \left\{ -1 - \text{Sp}(\mathbf{A}_k^{q^{k-1}}) \right\} \mu\left(\frac{i}{k}\right) \pmod{p}$$

Отсюда для $i = 1$ получаем

$$(13) \quad \sigma_1 \equiv -1 - \text{Sp}(\mathbf{A}_1^{q-1}) \pmod{p}.$$

Для $i > 1$ (ввиду $\sum_{k|i} \mu\left(\frac{i}{k}\right) = 0$)

$$(14) \quad i\sigma_i \equiv -\sum_{k|i} \mu\left(\frac{i}{k}\right) \text{Sp}(\mathbf{A}_k^{q^{k-1}}) \pmod{p}.$$

Тем самым мы доказали:

Теорема 5. Пусть выполнены условия теоремы 4. Тогда для чисел $\sigma_1, \sigma_2, \dots, \sigma_{q-2} \pmod{p}$ имеют силу соответственно формулы (13) и (14).

Примечание 1. Если $q = p$, т. е. полином (8) имеет коэффициенты из поля $GF(p)$, то для всех чисел $\sigma_i (i = 1, 2, \dots, p-2)$ выполняется неравенство $0 \leq \sigma_i \leq p-2$. Значит, числа σ_i определены соотношениями (13) и (14) однозначно.

Примечание 2. Формула (14) формально аналогична формуле (8), выведенной в работе [6]. Однако, матрицы, выступающие в работе [6], не тождественны с матрицами, выступающими в нашей работе.

В этом разделе прежде всего покажем, что из формулы (13), в которой выступает циклическая матрица \mathbf{A}_1 , можно легко вывести обобщение формулы Гурвица, о которой шла речь во введении, и которая задает число $\sigma_1(\text{mod } p)$ тоже в случае, когда $s > 1$.

Обозначим через \mathbf{N}_1 следующую матрицу порядка $q-1$:

$$\mathbf{N}_1 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Очевидно, для $k < q-1$

$$\mathbf{N}_1^k = \begin{matrix} & & & & k+1 & & & & \\ \begin{pmatrix} 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & & 0 & 0 & \dots & 0 & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 & 0 \end{pmatrix} & & & & & & & & \end{matrix}.$$

Для $k = q-1$ будет $\mathbf{N}_1^{q-1} = \mathbf{E}_{q-1}$. В общем случае $\mathbf{N}^\rho = \mathbf{N}^\sigma$, если $\rho \equiv \sigma \pmod{q-1}$. Очевидно, дальше

$$(15) \quad \text{Sp}(\mathbf{N}_1^k) = \begin{cases} 0, & \text{если } q-1 \nmid k, \\ q-1, & \text{если } q-1 \mid k. \end{cases}$$

Матрицу \mathbf{A}_1 можно записать в виде

$$\mathbf{A}_1 = a_0 \mathbf{E}_{q-1} + a_1 \mathbf{N}_1 + \dots + a_{q-2} \mathbf{N}_1^{q-2}.$$

Обозначим через $P^{(1)}(\lambda_0, \lambda_1, \dots, \lambda_{q-2})$ тот элемент поля $GF(p)$, который $(\text{mod } p)$ равен неотрицательному целому числу $\frac{(q-1)!}{\lambda_0! \lambda_1! \dots \lambda_{q-2}!}$, где $\lambda_0 + \lambda_1 + \dots + \lambda_{q-2} = q-1$.

Имеем

$$\begin{aligned} \mathbf{A}_1^{q-1} &= [a_0 \mathbf{E}_{q-1} + a_1 \mathbf{N}_1 + \dots + a_{q-2} \mathbf{N}_1^{q-2}]^{q-1} = \\ &= \sum P^{(1)}(\lambda_0, \lambda_1, \dots, \lambda_{q-2}) a_0^{\lambda_0} a_1^{\lambda_1} \dots a_{q-2}^{\lambda_{q-2}} \mathbf{N}_1^{\lambda_0 + 2\lambda_1 + \dots + (q-2)\lambda_{q-2}}, \end{aligned}$$

где сумма относится ко всем неотрицательным целым решениям $(\lambda_0, \lambda_1, \dots, \lambda_{q-2})$ уравнения $\lambda_0 + \lambda_1 + \dots + \lambda_{q-2} = q-1$.

В силу соотношения (15) след каждого слагаемого равен нулю (в поле $GF(q)$), за исключением тех слагаемых, в которых числа $(\lambda_0, \lambda_1, \dots, \lambda_{q-2})$ удовлетворяют соотношению

$$\lambda_1 + 2\lambda_2 + \dots + (q-2)\lambda_{q-2} \equiv 0 \pmod{q-1}.$$

Для слагаемых такого вида след равен элементу

$$\begin{aligned} P^{(1)}(\lambda_0, \lambda_1, \dots, \lambda_{q-2}) \cdot (q-1) \cdot a_0^{\lambda_0} a_1^{\lambda_1} \dots a_{q-2}^{\lambda_{q-2}} = \\ = -P^{(1)}(\lambda_0, \lambda_1, \dots, \lambda_{q-2}) a_0^{\lambda_0} \dots a_{q-2}^{\lambda_{q-2}} \in GF(q) \end{aligned}$$

Значит (смысл знака суммы ясен),

$$Sp(\mathbf{A}_1^{q-1}) = -\sum P^{(1)}(\lambda_0, \lambda_1, \dots, \lambda_{q-2}) a_0^{\lambda_0} \dots a_{q-2}^{\lambda_{q-2}}.$$

Подставляя в (13), получаем

$$(16) \quad \sigma_1 \equiv -1 + \sum P^{(1)}(\lambda_0, \lambda_1, \dots, \lambda_{q-2}) a_0^{\lambda_0} a_1^{\lambda_1} \dots a_{q-2}^{\lambda_{q-2}} \pmod{p},$$

где сумма относится к целым неотрицательным решениям $(\lambda_0, \lambda_1, \dots, \lambda_{q-2})$, удовлетворяющим

$$(17) \quad \begin{aligned} \lambda_0 + \lambda_1 + \dots + \lambda_{q-2} &= q-1, \\ \lambda_1 + 2\lambda_2 + \dots + (q-2)\lambda_{q-2} &\equiv 0 \pmod{q-1}. \end{aligned}$$

Это — обобщенное утверждение Гурвица, доказанное Диксоном (смотри [1], стр. 232).

Формулу (14) можно применить для нахождения явных формул для числа $\sigma_i \pmod{p}$, где $i \geq 2$.

Пусть \mathbf{N}_k обозначает матрицу порядка $q^k - 1$ вида

$$\mathbf{N}_k = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Очевидно, $\mathbf{N}_k^{q^k-1} = \mathbf{E}_{q^k-1}$ и $\mathbf{N}^\rho = \mathbf{N}^\sigma$ для $\rho \equiv \sigma \pmod{q^k-1}$. Далее,

$$\begin{aligned} Sp(\mathbf{N}_k^l) &= \begin{cases} 0, & \text{для } q^k - 1 \nmid l, \\ q^k - 1, & \text{для } q^k - 1 \mid l, \end{cases} \\ \mathbf{A}_k^{q^k-1} &= [a_0 \mathbf{E}_{q^k-1} + a_1 \mathbf{N}_k + a_2 \mathbf{N}_k^2 + \dots + a_{q-2} \mathbf{N}_k^{q-2}]^{q^k-1}. \end{aligned}$$

Обозначим — в том же смысле, что и выше —

$$P^{(k)}(\lambda_0^{(k)}, \lambda_1^{(k)}, \dots, \lambda_{q-2}^{(k)}) = \frac{(q^k-1)!}{\lambda_0^{(k)}! \lambda_1^{(k)}! \dots \lambda_{q-2}^{(k)}!}.$$

где $\lambda_0^{(k)} + \lambda_1^{(k)} + \dots + \lambda_{q-2}^{(k)} = q^k - 1$. Тогда

$$\text{Sp}(\mathbf{A}_k^{q^k-1}) = -\sum P^{(k)}(\lambda_0^{(k)}, \lambda_1^{(k)}, \dots, \lambda_{q-2}^{(k)}) a_0^{\lambda_0^{(k)}} \cdot a_1^{\lambda_1^{(k)}} \dots a_{q-2}^{\lambda_{q-2}^{(k)}}.$$

где сумма относится к системам неотрицательных целых чисел $(\lambda_0^{(k)}, \lambda_1^{(k)}, \dots, \lambda_{q-2}^{(k)})$, для которых имеет место

$$(18) \quad \begin{aligned} \lambda_0^{(k)} + \lambda_1^{(k)} + \dots + \lambda_{q-2}^{(k)} &= q^k - 1, \\ \lambda_1^{(k)} + 2\lambda_2^{(k)} + \dots + (q-2)\lambda_{q-2}^{(k)} &\equiv 0 \pmod{q^k - 1}. \end{aligned}$$

Подстановкой в (14) получаем наконец (для $i \geq 2$)

$$(19) \quad i\sigma_i \equiv \sum_{k|i} \mu\left(\frac{i}{k}\right) \left(\sum P^{(k)}(\lambda_0^{(k)}, \lambda_1^{(k)}, \dots, \lambda_{q-2}^{(k)}) a_0^{\lambda_0^{(k)}}, \dots, a_{q-2}^{\lambda_{q-2}^{(k)}} \right) \pmod{p},$$

где внутренняя сумма относится ко всем решениям $(\lambda_0^{(k)}, \lambda_1^{(k)}, \dots, \lambda_{q-2}^{(k)})$, удовлетворяющим соотношениям (18).

Выведенный результат можно сформулировать так:

Теорема 6. Пусть (8) — полином не более $(q-2)$ -ой степени над полем $GF(q)$. Пусть σ_i — число различных неприводимых факторов полинома (8) над полем $GF(q)$ степени $i \geq 2$. Тогда для числа $\sigma_i \pmod{p}$ справедливо соотношение (19).

5

В этом разделе покажем, как можно вывести формулы для чисел σ_i , которые содержат циклические матрицы меньшего порядка, чем $q^i - 1$.

Обозначим через G_1 ненулевые элементы поля $GF(q)$. Известно, что элементы $\in G_1$ образуют относительно умножения циклическую группу порядка $q-1$. Пусть k — целое число, $k|(q-1)$. Тогда ненулевые элементы $\in GF(q)$, которые являются k -тыми степенями элементов $\in GF(q)$, образуют циклическую подгруппу порядка $(q-1)/k$. Обозначим ее через G_k . Каждый элемент $\in G_k$ удовлетворяет уравнению

$$(20) \quad z^{(q-1)/k} - 1 = 0.$$

Разложение группы G_1 по подгруппе G_k имеет вид

$$(21) \quad G_1 = G_k \cup \eta_2 G_k \cup \dots \cup \eta_k G_k,$$

где $\eta_1 = 1$, η_2, \dots, η_k — подходящим образом выбранные элементы $\in G_1$.

Будем находить число тех корней уравнения

$$(22) \quad f(x) = a_0 + a_1 x + \dots + a_r x^r = 0, \quad a_i \in GF(q), \quad a_0 \neq 0,$$

в поле $GF(q)$, которые попадут в класс $\eta_i G_k$, т. е. они вида $\xi \eta_i$, где $\xi \in G_k$. Число таких корней обозначим через $\sigma_1(i, k)$. Очевидно, $\sigma_1 = \sum_{i=1}^k \sigma_1(i, k)$.

Подставим $x = \eta_i y$. Тогда $f(x)$ приобретет вид

$$\varphi_i(y) = a_0 + a_1 \eta_i y + a_2 \eta_i^2 y^2 + \dots + a_r \eta_i^r y^r, \quad a_0 \neq 0,$$

и достаточно искать число корней уравнения $\varphi_i(y) = 0$, для которых y будет элементом группы G_k , т. е. (ненулевой) k -той степенью из $GF(q)$.

Поскольку каждый элемент $y \in G_k$ удовлетворяет уравнению (20), будем предполагать, что $r \leq t_k - 1$, где $t_k = (q - 1)/k$.

Построим циклическую матрицу

$$(23) \quad \mathbf{B}(i, k) = \mathbf{Z} \left(a_0, a_1 \eta_i, a_2 \eta_i^2, \dots, a_r \eta_i^r; \frac{q-1}{k} \right).$$

а) Если $h(i, k)$ — ранг матрицы $\mathbf{B}(i, k)$, то согласно теореме 1 имеет место соотношение $\sigma_1(i, k) = \frac{q-1}{k} h(i, k)$. Значит,

$$\sigma_1 = \sum_{i=1}^k \sigma_1(i, k) = q - 1 - \sum_{i=1}^k h(i, k).$$

б) Из соотношения (5) следует

$$|\mathbf{B}(i, k) - \lambda \mathbf{E}_{t_k}| = (-1)^{q-1/k} [\lambda - f(\eta_i \xi_1)] [\lambda - f(\eta_i \xi_2)] \dots [\lambda - f(\eta_i \xi_{t_k})],$$

где $\xi_1, \xi_2, \dots, \xi_{t_k}$ — все элементы группы G_k . Так как элементы $f(\eta_i \xi_1), \dots, f(\eta_i \xi_{t_k})$ являются как раз всеми характеристическими корнями матрицы $\mathbf{B}(i, k)$, получим (точно так же, как при доказательстве теоремы 5)

$$\text{Sp} [\mathbf{B}(i, k)^{q-1}] = \sigma_1(i, k) \cdot 0 + \left[\frac{q-1}{k} - \sigma_1(i, k) \right] \cdot 1,$$

значит,

$$\sigma_1(i, k) \equiv \frac{q-1}{k} - \text{Sp} [\mathbf{B}(i, k)]^{q-1} \pmod{p}.$$

Из уравнения $\sigma_1 = \sum_{i=1}^k \sigma_1(i, k)$ получаем

$$\sigma_1 \equiv -1 - \text{Sp} \{ \mathbf{B}(1, k)^{q-1} + \mathbf{B}(2, k)^{q-1} + \dots + \mathbf{B}(k, k)^{q-1} \} \pmod{p}$$

Эти результаты можно свести в теорему:

Теорема 7. Пусть k — целое число, $k|(q-1)$ и $t_k = (q-1)/k$. Пусть σ_1 обозначает число корней уравнения

$$f(x) = a_0 + a_1 x + \dots + a_{t_k} x^{t_k-1} = 0, \quad a_i \in GF(q), \quad a_0 \neq 0,$$

в поле $GF(q)$. Пусть $\mathbf{B}(i, k)$ — циклическая матрица (23), в которой η_1, \dots, η_k имеют смысл из разложения (21) и пусть $h(i, k)$ — ранг матрицы $\mathbf{B}(i, k)$. Тогда имеет место:

$$a) \sigma_1 = q - 1 - \sum_{i=1}^k h(i, k),$$

$$б) \sigma_1 \equiv -1 - \text{Sp} \{ \mathbf{B}(1, k)^{q-1} + \mathbf{B}(2, k)^{q-1} + \dots + \mathbf{B}(k, k)^{q-1} \} \pmod{p}.$$

Значение теоремы состоит в том, что число σ_1 определяется с помощью матриц, порядок которых меньше, чем число $q - 1$.

Примечание. Аналогичные формулы можно вывести и для чисел $\sigma_2, \sigma_3, \dots, \sigma_r$.

ЛИТЕРАТУРА

- [1] Dickson L. E., *History of the Theory of Numbers*, Vol. I, New York, reprinted 1934.
- [2] Hurwitz L., *Über höhere Kongruenzen*, Archiv der Math. u. Phys. (3) 5 (1903), 17—27.
- [3] Rédei L., *Algebra*, Akademische Verlagsgesellschaft, Leipzig 1959.
- [4] Rédei L., Turán P., *Zur Theorie der algebraischen Gleichungen über endlichen Körpern*, Acta Arithmetica 5 (1959), 223—225.
- [5] Segre B., *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.
- [6] Schwarz Š., *О числе неприводимых факторов данного многочлена над конечным полем*, Чех. мат. ж. 11 (86) (1961), 213—225.

Поступило 20. 10. 1961 г.

*Katedra matematiky
Slovenskej vysokej školy technickej
v Bratislave*

CYCLIC MATRICES AND ALGEBRAIC EQUATIONS OVER A FINITE FIELD

Kornélia Horáková and Štefan Schwarz

Summary

In section 1 of this paper some generalizations of the Theorem of Rados—König are given. As an application we prove in section 2: Let (8) be a polynomial of degree at most $q-2$ over the finite field $GF(q)$. Let σ_i ($1 \leq i \leq q-2$) be the number of different irreducible factors of (8) of degree i . If h_i is the rank of the cyclic matrix (10), and $\mu(t)$ the Möbius function, then the relation (11) holds.

In section 3 an other type of formulas is given. If $\text{Sp}(\mathbf{B})$ denotes the trace of the matrix \mathbf{B} , then $i\sigma_i \pmod{p}$ is given by the formulas (13) and (14). This is used in section 4 to deduce explicit formulas for $i\sigma_i \pmod{p}$ in terms of the coefficients of (8). Also the relation between two types of formulas (namely those of König—Rados and L. Hurwitz) concerning the determination of σ_1 is clarified.

In section 5 a brief mention is given concerning the possibility of reducing the orders of matrices needed for the determination of the number σ_1 .