# ЦИКЛИЧЕСКИЕ МАТРИЦЫ И АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ НАД КОНЕЧНЫМ ПОЛЕМ

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

Пусть

$$f(x) = a_0 + a_1 x + \ldots + a_{q-2}x^{q-2}, \quad a_0 \neq 0, \tag{1}$$

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

$$\mathbf{A} = \begin{pmatrix} a_0 & a_1 & a_2 \ldots a_{q-2} \\ a_{q-2} & a_0 & a_1 \ldots a_{q-3} \\ \vdots & & \vdots \\ a_1 & a_2 & a_3 \ldots a_0 \end{pmatrix}. \tag{2}$$

Известна теорема Кенига-Радоса (смотри [3], стр. 501), которая формулируется так: Пусть $\sigma_1$ — 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 $\sigma_i$ $(1 \leqq i \leqq q-2)$ обозначает число различных неприводимых факторов полинома (1) степени $i$. Во втором разделе выведена формула для числа $\sigma_i$, в которой выступают ранги некоторых циклических матриц порядков $q-1$, $q^2-1, \ldots, q^i-1$.

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

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

б) если $n > r$, то первая строка — $(b_0, b_1, \ldots, b_{r-1}, \underbrace{0, \ldots, 0}_{(n-r)\text{ раз}})$, а остальные получим из нее циклической заменой. Значит,

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

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

$$x^n - 1 = 0 \tag{3}$$

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

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

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

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

Обозначим через $\sigma$ число корней уравнения (3), которые являются одновременно корнями уравнения

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

Если $\sigma \geqq 1$, то можно без нарушения общности предположить, что рассматриваемыми корнями будут элементы $\varepsilon_{n-\sigma+1}, \varepsilon_{n-\sigma+2}, \ldots, \varepsilon_n$. Тогда последние $\sigma$ 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 $\sigma$ столбцов и $\sigma$ строк, равен элементу

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

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

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

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

Примечание. Допустим, что $G(x) = c_0 + c_1 x + \ldots + c_{r-1} x^{r-1}$, $c_{r-1} \neq 0$, полином степени $r - 1$ над полем $\mathbf{T}$ и выполняется $n \leqq r - 1$. 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

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

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

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

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

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



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

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

Путем сравнения получаем:

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

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

а) Если $s_n = s_{n-1} = \ldots = s_{t+1} = 0$, но $s_t \neq 0$, то из соотношения (6) вытекает, что полином $\lambda^n - s_1 \lambda^{n-1} + \ldots + (-1)^n s_n$ имеет $\lambda = 0$ в качестве $(n - t)$-кратной нулевой точки. Из соотношения (5) вытекает, что среди элементов $f(\varepsilon_1), f(\varepsilon_2), \ldots, f(\varepsilon_n)$ 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 удовлетворят $f(x) = 0$. Пусть это будут корни $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-t}$. Из соотношений (7) вытекает: $s_n = s_{n-1} = \ldots = s_{t+1} = 0$ (так как каждое слагаемое направо имеет хотя бы один нулевой фактор), тогда как $s_t = f(\varepsilon_t) f(\varepsilon_{t+1}) \ldots f(\varepsilon_n) \neq 0$. Тем самым мы доказали:

**Теорема 2.** *Пусть* $F(x) = a_0 + a_1 x + \ldots + a_{r-1} x^{r-1}$ *— 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* $\mathbf{Z}(a_0, a_1, \ldots, a_{r-1}; n)$. *Пусть* $s_t$ *— последний отличный от нуля элемент последовательности* $s_1, s_2, \ldots, s_n$ *и пусть* $\sigma$ *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 $q = p^s$, $s \geqq 1$ и $p$ — простое число. Пусть

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

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

Пусть $i \geqq 1$ — целое число и $i > i' > i'' > \ldots > 1$ — 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 $i, i', i'', \ldots, 1$. Каждый ненулевой элемент поля $\mathbf{T}(j)$ притом удовлетворяет уравнению

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

Это уравнение не имеет многократных корней.

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

Рассмотрим циклическую матрицу

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

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

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

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

Применяя формулу Мебиуса для инверсии, получаем

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

Тем самым мы доказали обобщение теоремы Кенига-Радоса:

**Теорема 3.** *Пусть* (8) *— полином не более* $(q-2)$*-ой степени над полем* $GF(q)$. *Пусть* $\sigma_i$ *обозначает число различных неприводимых факторов степени* $i \geqq 1$ *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 $\sigma_1, \sigma_2, \ldots, \sigma_i$ существуют и другие интересные формулы.

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

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

Характеристическими корнями матрицы $\mathbf{A}_i$ являются элементы $f(\varepsilon_1), \ldots, f(\varepsilon_{q^i-1})$. Поэтому характеристическими корнями матрицы $\mathbf{A}_i^{q^i-1}$ являются элементы $[f(\varepsilon_1)]^{q^i-1}, \ldots, [f(\varepsilon_{q^i-1})]^{q^i-1}$. 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 $i\sigma_i + i'\sigma_{i'} + \ldots + \sigma_1$ нулей и $q^i - 1 - (i\sigma_i + i'\sigma_{i'} + \ldots + \sigma_1)$ единиц. Значит,

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

Тем самым мы доказали:

**Теорема 4.** *Пусть* $i \geqq 1$ *— натуральное число, пусть* $i > i' > i'' > \ldots > 1$ *— 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 $\mathrm{Sp}(\mathbf{B})$ обозначает в дальнейшем след матрицы $\mathbf{B}$. Из соотношения (12) следует, что в поле $GF(q)$ справедливо

$$\mathrm{Sp}(A_i^{q^i-1}) = (i\sigma_i + \ldots + \sigma_1) \cdot 0 + (q^i - 1 - i\sigma_i - i'\sigma_{i'} - \ldots - \sigma_1) \cdot 1.$$

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

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

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

$$i\sigma_i \equiv \sum_{k/i} \{-1 - \mathrm{Sp}(\mathbf{A}_k^{qk-1})\}\, \mu\left(\frac{i}{k}\right) \pmod{p}$$

Отсюда для $i = 1$ получаем

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

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

(14) $$i\sigma_i \equiv -\sum_{k/i} \mu\left(\frac{i}{k}\right) \mathrm{Sp}(\mathbf{A}_k^{qk-1}) \pmod{p}.$$

Тем самым мы доказали:

**Теорема 5.** *Пусть выполнены условия теоремы* 4. *Тогда для чисел* $\sigma_1, \sigma_2, \ldots, \sigma_{q-2} \pmod{p}$ *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 $\sigma_i (i = 1, 2, \ldots, p-2)$ выполняется неравенство $0 \leqq \sigma_i \leqq p - 2$. Значит, числа $\sigma_i$ 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 $\sigma_1 (\mathrm{mod}\, p)$ 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 $k < q-1$

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

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

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

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 $(\mathrm{mod}\, p)$ равен неотрицательному целому числу $\dfrac{(q-1)!}{\lambda_0!\lambda_1!\dots\lambda_{q-2}!}$, где $\lambda_0 + \lambda_1 + \dots + \lambda_{q-2} = q-1$.

Имеем

$$\mathbf{A}_1^{q-1} = [a_0\mathbf{E}_{q-1} + a_1\mathbf{N}_1 + \dots + a_{q-2}\mathbf{N}_2^{q-2}]^{q-1} =$$
$$= \sum P^{(1)}(\lambda_0, \lambda_1, \dots, \lambda_{q-2})\, a_0^{\lambda_0}a_1^{\lambda_1}\dots a_{q-2}^{\lambda_{q-2}}\mathbf{N}_1^{\lambda_n + 2\lambda_2 + \dots + (q-2)\lambda_{q-2}},$$

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

$$\lambda_1 + 2\lambda_2 + \dots + (q-2)\lambda_{q-2} \equiv 0 \qquad [\mathrm{mod}\,(q-1)].$$

Для слагаемых такого вида след равен элементу

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

Значит (смысл знака суммы ясен),

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

Подставляя в (13), получаем

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

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

$$\begin{aligned} &\lambda_0 + \lambda_1 + \dots + \lambda_{q-2} = q-1, \\ &\lambda_1 + 2\lambda_2 + \dots + (q-2)\lambda_{q-2} \equiv 0 \qquad [\mathrm{mod}\,(q-1)]. \end{aligned} \tag{17}$$

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

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

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 $\varrho \equiv \sigma\,[\mathrm{mod}\,(q^k-1)]$. Дальше,

$$\mathrm{Sp}\,(\mathbf{N}_k^l) = \begin{cases} 0 & , \text{ для } q^k - 1 \nmid l, \\ q^k - 1, & \text{для } q^k - 1 \mid l, \end{cases}$$

$$\mathbf{A}_k^{q^k-1} = [a_0\mathbf{E}_{q^k-1} + a_1\mathbf{N}_k + a_2\mathbf{N}_k^2 + \dots + a_{q-2}\mathbf{N}_k^{q-2}]^{q^k-1}.$$

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

$$\mathrm{Sp}\,(\mathbf{A}_k^{q^k-1}) = -\Sigma P^{(k)}(\lambda_0^{(k)}, \lambda_1^{(k)}, \ldots, \lambda_{q-2}^{(k)})\, a_0^{\lambda_0^{(k)}} \cdot a_1^{\lambda_1^{(k)}} \ldots a_{q-2}^{\lambda_{q-2}^{(k)}},$$

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

$$\begin{aligned} &\lambda_0^{(k)} + \lambda_1^{(k)} + \ldots + \lambda_{q-2}^{(k)} = q^k - 1, \\ &\lambda_1^{(k)} + 2\lambda_2^{(k)} + \ldots + (q-2)\,\lambda_{q-2}^{(k)} \equiv 0 \qquad [\mathrm{mod}\,(q^k - 1)]. \end{aligned} \tag{18}$$

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

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

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

Выведенный результат можно сформулировать так:

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

## 5

В этом разделе покажем, как можно вывести формулы для чисел $\sigma_i$, 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

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

Разложение группы $G_1$ по подгруппе $G_k$ имеет вид

$$G_1 = G_k \cup \eta_2 G_k \cup \ldots \cup \eta_k G_k, \tag{21}$$

где $\eta_1 = 1, \eta_2, \ldots, \eta_k$ — подходящим образом выбранные элементы $\in G_1$.

Будем находить число тех корней уравнения

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

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

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

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 $r \leqq t_k - 1$, где $t_k = (q-1)/k$.

Построим циклическую матрицу

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

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

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

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

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

значит,

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

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

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

Эти результаты можно свести в теорему:

**Теорема 7.** *Пусть* $k$ *— целое число,* $k/(q-1)$ *и* $t_k = (q-1)/k$. *Пусть* $\sigma_1$ *обозначает число корней уравнения*

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

*в поле* $GF(q)$. *Пусть* $\mathbf{B}(i, k)$ *— циклическая матрица* (23), *в которой* $\eta_1, \ldots, \eta_k$ *имеют смысл из разложения* (21) *и пусть* $h(i, k)$ *— ранг матрицы* $\mathbf{B}(i, k)$. *Тогда имеет место:*

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

б) $\sigma_1 \equiv -1 - \mathrm{Sp}\left\{\mathbf{B}(1, k)^{q-1} + \mathbf{B}(2, k)^{q-1} + \ldots + \mathbf{B}(k, k)^{q-1}\right\} \pmod{p}$.

Значение теоремы состоит в том, что число $\sigma_1$ определяется с помощью матриц, порядок которых меньше, чем число $q - 1$.

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

## 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 Aritmetica 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 $\sigma_i$ $(1 \leqq i \leqq q - 2)$ 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 $Sp(\mathbf{B})$ 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 $\sigma_1$ is clarifyed.

In section 5 a brief mention is given concerning the possibility of reducing the orders of matrices needed for the determination of the number $\sigma_1$.