18. POLINOMŲ FAKTORIZACIJA VIRŠ BAIGTINIŲ KŪNŲ

Polinomo $f(x) \in GF(q)[x]$ faktorizacija atliekama keliais žingsniais:

I *(bekvadratė faktorizacija). Ieškoma tokių polinomų* $f_1, f_2, \ldots, f_k \in GF(q)[x]$, *kad:*

a) $f = f_1^1 f_2^2 \ldots f_k^k$,

b) polinomai f_i *būtų tarpusavyje pirminiai ir bekvadračiai, t.y. savo kanoniniuose skaidiniuose virš kūno* $GF(q)$ *neturėtų neredukuojamų polinomų laipsnių.*

II. Faktorizuojami polinomai f_i, $1 \leqslant i \leqslant k$.

III. Gautame polinomo f skaidinyje sutraukiami panašūs nariai ir gaunamas polinomo f kanoninis skaidinys.

Tegu kūno $GF(q)$ charakteristika yra p.

Aptarsime šiuos polinomo f faktorizacijos žingsnius.

I. Tegu $f = \prod\limits_{i=1}^{k} f_i^i$ (čia f_i yra bekvadračiai) - tarpusavyje pirminiai polinomai. Tada polinomo f išvestinė yra

$$f' = \sum_{i=1}^{k} \left(i\, f_i'\, f_i^{i-1} \prod_{\substack{j \neq i \\ 1 \leqslant j \leqslant k}} f_j^j \right) = \sum_{i=1}^{k} c_i(x).$$

Tegu $d(x) = \mathrm{DBD}\,(f, f')$. Pastebėsime, jeigu neredukuojamas polinomas $r(x)$ yra polinomo $f(x)$ daliklis, tai $r(x)$ yra ir $f_{i_0}(x)$ daliklis kuriam nors $i_0 = i_0(r)$, $1 \leqslant i_0 \leqslant k$. Todėl neredukuojamo polinomo $r(x)$ laipsnio rodiklis $e = e_r(d)$ kanoniniame polinomo $d(x)$ skaidinyje apibrėžiamas taip:

a) jeigu $i \neq i_0$, tai $e_r(d)$ i-ajame polinomo f' dėmenyje $c_i(x)$ yra didesnis arba lygus i_0;

b) jeigu $i = i_0$, tai $e_r(d) = i_0 - 1$, kai p nėra i_0 daliklis, ir $e_r(d) = i_0$, kai p yra i_0 daliklis.

Taigi

$$e_r(d) = \begin{cases} i_0 - 1, & \text{kai } p \text{ nėra } i_0 \text{ daliklis },\\ i_0, & \text{kai } p \text{ yra } i_0 \text{ daliklis.}\end{cases}$$

$$d(x) = \mathrm{DBD}\,(f, f') = \prod_{\substack{i=1\\ p \text{ nėra } i \text{ daliklis}}}^{k} f_i^{i-1} \prod_{\substack{i=1\\ p \text{ yra } i \text{ daliklis}}}^{k} f_i^i.$$

Apibrėžkime rekurenčiuosius sąryšius.

Tegu $d_1(x) = d(x)$, o

$$g_1(x) = \frac{f(x)}{d(x)} = \prod_{\substack{i=1\\ p \text{ nėra } i \text{ daliklis}}}^{k} f_i(x).$$

Kai $l \geqslant 2$, tai

$$g_l(x) = \begin{cases} DBD\,(d_{l-1}, g_{l-1}), & \text{kai } p \text{ nėra } l \text{ daliklis,}\\ g_{l-1}(x), & \text{kai } p \text{ yra } l \text{ daliklis,}\end{cases}$$

$$d_l(x) = \frac{d_{l-1}(x)}{g_l(x)}, \text{ kai } p \text{ nėra } l \text{ daliklis.}$$

Taigi

$$g_l(x) = \prod_{\substack{i>l-1\\ p \text{ nėra } i \text{ daliklis}}} f_i(x)$$

ir

$$d_l(x) = \prod_{\substack{i>l\\ p \text{ nėra } i \text{ daliklis}}} f_i^{i-l} \prod_{\substack{i=1\\ p \text{ yra } i \text{ daliklis}}}^{k} f_i^i.$$

Iš čia

$$f_l(x) = \frac{g_l(x)}{g_{l+1}(x)}, \text{ kai } p \text{ nėra } l \text{ daliklis ir}$$

$g_l(x)$ nėra lygus konstantai. Jeigu $g_l(x)$ yra kūno $GF(q)$ elementas, tai

$$d_l(x) = \prod_{\substack{i=1\\ p \text{ yra } i \text{ daliklis}}}^{k} f_i^i = \big(h(x)\big)^p = h\big(x^p\big).$$

Norint tęsti bekvadratę faktorizaciją, polinomui $h(x)$ reikia taikyti anksčiau nurodytą procedūrą.

Šiais samprotavimais remiasi algoritmas.

13.1 algoritmas. *Žinoma: polinomas* $f(x) \in GF(q)[x]$, $q = p^s$, p – *pirminis.*

Rezultatas: randami nelygūs konstantai bekvadračiai tarpusavyje pirminiai polinomai ir jų laipsnių rodikliai kanoniniame polinomo $f(x)$ *skaidinyje* $(1, f_1) = f_1, (2, f_2) = f_2, \ldots, (k, f_k) = f_k$; $f = f_1^1 f_2^2 \ldots f_k^k$.

1. Priskiriame $e := 1$, $f := f(x)$.

2. Jeigu f yra konstanta, tai išvedame (e, f) ir skaičiavimai baigiami. Jeigu f nėra konstanta, tai priskiriame $k := 0$, $d := \mathrm{DBD}\,(f, f')$, $g := \frac{f}{d}$.

3. Jeigu g nėra konstanta, tai pereiname prie 4. Jeigu g yra konstanta, tai turėtų būti

$$d = \sum_{p \,|\, j} t_j x^j = \sum_{p \,|\, j} t_j x^{j/p} = \left(\sum_{q \,|\, j} t_j x^{j/p} \right)^p,$$

todėl priskiriame

$$e := pe, \quad f := \sum_{p \,|\, j} t_j x^{j/p}$$

ir pereiname prie 2.

4. Priskiriame $k := k + 1$. Jeigu p nėra k daliklis, tai pereiname prie 5.

Jeigu p yra k daliklis, tai priskiriame $d := \frac{d}{g}$, $\quad k := k+1$ ir pereiname prie 5.

5. Skaičiuojame ir priskiriame $d_{ek} := \mathrm{DBD}\,(d, g)$, $\quad f_{ek}(x) := \frac{g}{d_{ek}}$, $g := d_{ek}$, $\quad d := \frac{d}{g}$. Jeigu f_{ek} yra konstanta, tai pereiname prie 3. Jeigu f_{ek} nėra konstanta, tai išvedame (ek, f_{ek}) ir pereiname prie 3.

$\triangle$

13.2 pavyzdys. $f(x) = x^{10} + x^8 + x^6 + x^4 + x^2 + 1 \in GF(3)[x]$.

$$e = 1, \quad k = 0. \quad f'(x) = x^9 + 2x^7 + x^3 + 2x,$$
$$d(x) = \text{DBD}\big(f(x), f'(x)\big) = x^8 + 2x^6 + x^2 + 2,$$
$$g_{11}(x) = \frac{f(x)}{d(x)} = x^2 + 2.$$

$$k = 1. \quad d_1(x) = \text{DBD}\big(d(x), g_{11}(x)\big) = x^2 + 2,$$
$$f_1(x) = \frac{g_{11}(x)}{d_1(x)} = 1,$$
$$g_{12}(x) = d_1(x) = x^2 + 2,$$
$$d(x) := \frac{d(x)}{g_{12}(x)} = x^6 + 1.$$

$$k = 2. \quad d_2(x) = \text{DBD}\big(d(x), g_{12}(x)\big) = 1,$$
$$f_2(x) = \frac{g_{12}(x)}{d_2(x)} = x^2 + 2,$$
$$g_{13}(x) = d_2(x) = 1,$$
$$d(x) := \frac{d(x)}{g_{13}(x)} = x^6 + 1 = (x^2 + 1)^3,$$

$g_{13}(x)$ – konstanta, todėl belieka suskaidyti polinomą $x^2 + 1$. Šiam polinomui vėl taikome algoritmą.

$$e = 3 \cdot 1 = 3, \quad k = 0. \quad f(x) = x^2 + 1,$$
$$f'(x) = 2x,$$
$$d(x) = \text{DBD}(x^2 + 1, 2x) = 1,$$
$$g_{31}(x) = \frac{f(x)}{d(x)} = x^2 + 1.$$

$$k = 1. \quad d_3(x) = \text{DBD}\big(d(x), g_{31}(x)\big) = 1,$$
$$f_3(x) = \frac{g_{31}(x)}{d_3(x)} = x^2 + 1.$$

Skaičiavimai baigiami. Gavome

$$f(x) = x^{10} + x^8 + x^6 + x^4 + x^2 + 1 = \big(x^2 + 2\big)^2 \big(x^2 + 1\big)^3.$$

Polinomas x^2+2 yra redukuojamas (1-as yra jo šaknis), todėl nesunkiai randame, kad $x^2+2=(x+1)(x+2)$. Polinomas x^2+1 neredukuojamas virš $GF(3)$, todėl

$$f(x)=(x+1)^2(x+2)^2\left(x^2+1\right)^3.$$

II. Bekvadračio polinomo faktorizacija remiasi šiais teiginiais:

13.3 teiginys (kinų teorema liekanoms, polinominis variantas).

Tegu $f_1(x), f_2(x), \ldots, f_n(x)$ yra poromis tarpusavyje pirminiai polinomai virš kūno $GF(q)$, o $c_1(x), c_2(x), \ldots, c_n(x)$ – bet kurie polinomai virš kūno $GF(q)$. Tada lyginių sistema

$$\begin{aligned} f(x) &\equiv c_1(x) \left(\operatorname{mod} f_1(x)\right), \\ f(x) &\equiv c_2(x) \left(\operatorname{mod} f_2(x)\right), \\ &\dots\dots\dots\dots\dots\dots \\ f(x) &\equiv c_n(x) \left(\operatorname{mod} f_n(x)\right) \end{aligned}$$

turi vienintelį sprendinį $f(x)$ moduliu $f_1(x)f_2(x)\ldots f_n(x)$.

Įrodymas. Vienatinumas. Tegu $f(x)$ ir $g(x)$ yra teiginyje nurodytos lyginių sistemos sprendiniai. Tada

$$f(x)\equiv g(x) \left(\operatorname{mod} f_i(x)\right), \quad 1\leqslant i\leqslant n,$$

t.y.

$$f(x)-g(x) \text{ dalijasi iš } f_i(x), \quad 1\leqslant i\leqslant n.$$

Bet $f_i(x)$, $1\leqslant i\leqslant n$, yra poromis tarpusavyje pirminiai, todėl $f(x)-g(x)$ dalijasi iš $f_1(x)f_2(x)\ldots f_n(x)$ ir

$$f(x)\equiv g(x) \left(\operatorname{mod} f_1(x)f_2(x)\ldots f_n(x)\right).$$

Egzistavimas. Pažymėkime $\overline{f}_i(x)=\frac{f_1(x)f_2(x)\ldots f_n(x)}{f_i(x)}$.

Polinomai $f_i(x)$ ir $\overline{f}_i(x)$ yra tarpusavyje pirminiai, todėl pagal Euklido algoritmą galime rasti tokius polinomus $u_i(x)$ ir $v_i(x)$, kad

$$u_i(x)f_i(x)+v_i(x)\overline{f}_i(x)=1.$$

Tada

$$f(x) = u_1(x)\,\overline{f}_1(x)\cdot c_1(x) + \ldots + u_n(x)\,\overline{f}_n(x)\,c_n(x)$$

ir

$$f(x) \equiv u_i(x)\overline{f}_i(x)\,c_i(x) \equiv c_i(x) \pmod{f_i(x)},$$

nes $\overline{f}_j(x)$ dalijasi iš $f_i(x)$, kai $j \neq i$. Taigi $f(x)$ yra lyginių sistemos sprendinys.

$\triangle$

13.4 teiginys. *Tegu bekvadračio polinomo $f(x) \in GF(q)[x]$ kanoninis skaidinys yra*

$$f(x) = f_1(x)f_2(x)\ldots f_n(x).$$

Tada bet kuriam kūno $GF(q)$ elementų rinkiniui $(c_1, c_2, \ldots, c_n)$ egzistuoja toks vienintelis polinomas $h(x) \in GF(q)[x]$, kad

$$\begin{aligned} h(x) &\equiv c_i \pmod{f_i(x)},\ 1 \leqslant i \leqslant n,\ \deg h(x) < \deg f(x), \\ h^q(x) &\equiv h(x) \pmod{f(x)},\ \deg h(x) < \deg f(x) \end{aligned}$$

ir tokių polinomų $h(x)$, tenkinančių paskutinį lygini, yra lygiai q^n.

Įrodymas. Iš 13.3 teiginio žinome, kad bet kuriam kūno $GF(q)$ elementų rinkiniui $(c_1, c_2, \ldots, c_n)$ egzistuoja vienintelis polinomas $h(x)$, kad

$$h(x) \equiv c_i \pmod{f_i(x)},\ 1 \leqslant i \leqslant n,\ \deg h(x) < \deg f(x).$$

Taigi

$$h^q(x) \equiv c_i^q \equiv c_i \equiv h(x) \pmod{f_i(x)},\ 1 \leqslant i \leqslant n$$

ir

$$h^q(x) \equiv h(x) \pmod{f(x)},\ \deg h(x) < \deg f(x).$$

Kita vertus, mes žinome, kad virš kūno $GF(q)$ galioja lygybė (žr. 9.3 teiginį)

$$x^q - x = \prod_{c \in GF(q)} (x - c),$$

todėl

$$h^q(x) - h(x) = \prod_{c \in GF(q)} \big(h(x) - c\big).$$

Bet jeigu $h^q(x) \equiv h(x) \pmod{f(x)}$, tai

$$f_i(x) \text{ yra } \prod_{c \in GF(q)} \big(h(x) - c\big) \text{ daliklis su visais } i,\ 1 \leqslant i \leqslant n.$$

Polinomai $f_i(x)$, $1 \leqslant i \leqslant n$ yra neredukuojami, todėl kiekvienam i atsiras toks $c_i \in GF(q)$, kad

$$f_i(x) \text{ yra } \big(h(x) - c_i\big) \text{ daliklis, t.y.}$$

$$h(x) \equiv c_i \pmod{f_i(x)}.$$

△

13.5 teiginys. *Tegu $f(x)$ yra unitarusis polinomas virš kūno $GF(q)$, o $h(x) \in GF(q)[x]$ – toks polinomas, kad $h^q(x) \equiv h(x) \pmod{f(x)}$. Tada*

$$f(x) = \prod_{c \in GF(q)} \mathrm{DBD}\big(f(x), h(x) - c\big).$$

Įrodymas. Visi polinomai $\mathrm{DBD}\big(f(x), h(x) - c\big)$, $c \in GF(q)$, yra polinomo $f(x)$ dalikliai. Polinomai $h(x) - c_1$ ir $h(x) - c_2$ yra tarpusavyje pirminiai, kai $c_1 \neq c_2$, todėl tarpusavyje pirminiai bus ir polinomai $\mathrm{DBD}\big(f(x), h(x) - c_1\big)$ ir $\mathrm{DBD}\big(f(x), h(x) - c_2\big)$, kai $c_1 \neq c_2$. Taigi poromis tarpusavyje pirminių polinomų sandauga

$$\prod_{c \in GF(q)} \mathrm{DBD}\big(f(x), h(x) - c\big)$$

yra polinomo $f(x)$ daliklis.

Kita vertus, žinome, kad

$$x^q - x = \prod_{c \in GF(q)} (x - c),$$

todėl

$$h^q(x) - h(x) = \prod_{c \in GF(q)} \big(h(x) - c\big)$$

ir $f(x)$ yra $\prod_{c \in GF(q)} \big(h(x) - c\big)$ daliklis, todėl $f(x)$ yra $\prod_{c \in GF(q)} \mathrm{DBD}\big(f(x), h(x) - c\big)$ daliklis.

Bet du vienas kitą dalijantys unitarieji polinomai sutampa, todėl teiginys įrodytas.

$\triangle$

Iš 13.5 teiginio matome, kad norint rasti polinomo $f(x) \in GF(q)[x]$ skaidinį, reiktų rasti polinomą $h(x) \in GF(q)[x]$, tenkinantį sąlygą $h^q(x) \equiv h(x) \bigl(\operatorname{mod} f(x)\bigr)$. Bekvadračiui polinomui $f(x)$ tokio polinomo egzistavimą garantuoja 13.4 teiginys. Parodysime, kaip galima sukonstruoti 13.4 teiginyje esančius polinomus $h(x)$.

Rasime lyginio

$$h^q(x) \equiv h(x) \bigl(\operatorname{mod} f(x)\bigr), \ \deg h < \deg f \qquad (*)$$

sprendinius. Tegu $h(x) = \sum\limits_{i=0}^{n-1} a_i x^i$; čia $n = \deg f(x)$ ir $a_i \in GF(q)$.

Žinome, kad $h^q(x) = \sum\limits_{i=0}^{n-1} a_i x^{iq}$, todėl,

jeigu

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \bigl(\operatorname{mod} f(x)\bigr), \quad i = 0, 1, \ldots, n-1,$$

tai

$$h(x) \equiv h^q(x) \equiv \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} b_{ij} x^j = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_i b_{ij} \right) x^j \bigl(\operatorname{mod} f(x)\bigr).$$

Lyginys $h^q(x) \equiv h(x) \bigl(\operatorname{mod} f(x)\bigr)$ ekvivalentus lygybėms

$$a_j = \sum_{i=0}^{n-1} a_i b_{ij}, \quad j = 0, 1, \ldots, n-1.$$

Jeigu matrica $B = (b_{ij})_{0 \leqslant i,\, j \leqslant n-1}$, tai paskutinės lygybės ekvivalenčios matricų lygybėms

$$\begin{aligned} &(a_0, a_1, \ldots, a_{n-1})\, B = (a_0, a_1, \ldots, a_{n-1}), \\ &(a_0, a_1, \ldots, a_{n-1})\, (B - I) = (0, 0, \ldots, 0); \end{aligned} \qquad (**)$$

čia I – vienetinė $n \times n$ matrica virš $GF(q)$. Jau žinome, kad pastaroji homogeninė tiesinių lygčių sistema turi q^k sprendinių, t.y. sprendinių poerdvio dimensija yra lygi k, ir matricos $B - I$ rangas lygus $n - k$; čia k – polinomo $f(x)$ kanoniniame skaidinyje esančių neredukuojamų polinomų skaičius. Taigi matricos $B - I$ rangas nustato polinomo $f(x)$ kanoniniame skaidinyje esančių neredukuojamų polinomų skaičių. Jeigu $k = 1$, tai polinomo $f(x)$ kanoniniame skaidinyje yra vienas neredukuojamas polinomas, t.y. pats polinomas $f(x)$ neredukuojamas. Šiuo atveju sistemos $(**)$ sprendiniai yra eilutės $(d, 0, \ldots, 0)$, $d \in GF(q)$.

Jeigu $k > 1$, tai sistemos $(**)$ fundamentaliąją sprendinių sistemą

$$d_1 = (d_{10}, d_{11}, \ldots, d_{1n-1}), \ldots, d_k = (d_{k0}, d_{k1}, \ldots, d_{kn-1})$$

atitinka baziniai lyginio $(*)$ polinomai

$$h_j(x) = \sum_{i=0}^{n-1} d_{ji} x^i.$$

Aišku, kad $h_1(x) = 1$, nes eilutė $(1, 0, \ldots, 0)$ yra sistemos $(**)$ sprendinys.

Pasirinkę polinomą $h_2(x)$, gausime polinomo $f(x)$ skaidinį

$$f(x) = \prod_{c \in GF(q)} \mathrm{DBD}\big(f(x), h_2(x) - c\big) = g_1(x) \ldots g_l(x); \qquad (***)$$

čia $g_1(x), \ldots, g_l(x)$ – polinomai, kurių laipsniai didesni už 1. Jeigu $l = k$, tai visi $g_i(x)$ yra neredukuojami polinomai ir $(***)$ yra polinomo $f(x)$ kanoninis skaidinys. Jeigu $l < k$, tai pasirinkę polinomą $h_3(x)$, randame visų polinomų $g_i(x)$, $1 \leqslant i \leqslant l$, skaidinius

$$g_i(x) = \prod_{c \in GF(q)} \big(g_i(x),\, h_3(x)\big), \quad 1 \leqslant i \leqslant l.$$

Šį procesą tęsime tol, kol negausime visų k neredukuojamų polinomo $f(x)$ daugiklių. Proceso baigtinumą garantuoja kitas teiginys.

13.6 teiginys. *Tegu $f_u(x)$ ir $f_v(x)$ yra bet kurie skirtingi neredukuojami polinomo $f(x)$ dalikliai. Tada egzistuoja $j \in \mathbb{N}$ ir $c \in GF(q)$, kad*

$$\begin{aligned} &f_u(x) \ \text{ yra } \ h_j(x) - c \ \text{ daliklis, bet} \\ &f_v(x) \ \text{ nėra } \ h_j(x) - c \ \text{ daliklis.} \end{aligned}$$

Įrodymas. Iš 13.3 teiginio įrodymo matome, kad kiekvieną bazinį polinomą $h_i(x)$, $1 \leqslant i \leqslant k$, atitinka tokia eilutė $c_i = (c_{i1}, c_{i2}, \ldots, c_{ik})$, kad

$$h_i(x) \equiv c_{is} \pmod{f_s(x)}, \quad 1 \leqslant s \leqslant k,\ 1 \leqslant i \leqslant k.$$

Tegu visiems i, $1 \leqslant i \leqslant k$, $c_{iu} = c_{iv}$. Jeigu $h(x)$ yra bet kuris lyginio $h^q(x) \equiv h(x) \pmod{f(x)}$, $\deg(h) < \deg(f)$ sprendinys, tai jis yra bazinių sprendinių $h_1(x), h_2(x), \ldots, h_k(x)$ tiesinė kombinacija $h(x) = \alpha_1 h_1(x) + \ldots + \alpha_k h(x)$, $\alpha_i \in GF(q)$. Tada

$$\begin{aligned} h(x) &\equiv \alpha_1 c_{1u} + \ldots + \alpha_k c_{ku} \pmod{f_u(x)}, \\ h(x) &\equiv \alpha_1 c_{1v} + \ldots + \alpha_k c_{kv} \pmod{f_v(x)} \end{aligned}$$

ir

$$h(x) \pmod{f_u(x)} = h(x) \pmod{f_v(x)}.$$

Tačiau eilutę $(c_1, \ldots, c_k)$, kai $c_u = 0$, $c_v = 1$, atitinkantis polinomas $h(x)$ tenkina lyginius $h(x) \equiv c_i \pmod{f_i(x)}$, $1 \leqslant i \leqslant k$. Bet tai prieštarauja paskutinei lygybei, nes

$$h(x) \pmod{f_u(x)} = 0 \neq 1 = h(x) \pmod{f_v(x)}.$$

Taigi egzistuoja toks j, $1 \leqslant j \leqslant k$, kad $c_{ju} \neq c_{jv}$ ir

$$\begin{aligned} h_j(x) &\equiv c_{ju} \pmod{f_u(x)}, \\ h_j(x) &\equiv c_{jv} \pmod{f_v(x)}, \\ h_j(x) &\not\equiv c_{jv} \pmod{f_u(x)}, \quad \text{t.y.} \end{aligned}$$

$$\begin{aligned} &f_v(x) \text{ yra polinomo } h_j(x) - c_{jv} \text{ daliklis, bet} \\ &f_u(x) \text{ nėra polinomo } h_j(x) - c_{jv} \text{ daliklis.} \end{aligned}$$

$\triangle$

Bekvadračio polinomo $f(x) \in GF(q)[x]$ faktorizacijos proceso aptarimą apibendrina *Berlekampo*[1] *algoritmas.*

[1] E. R. Berlekamp, g. 1940, – amerikiečių matematikas

13.7 algoritmas. *Žinoma: bekvadratis polinomas* $f(x) \in GF(q)[x]$, $\deg f(x) = n$.

Rezultatas: algoritmas faktorizuoja polinomą $f(x)$ *virš kūno* $GF(q)$.

1. Konstruojame matricą $B = (b_{ij})_{0 \leqslant i,j \leqslant n-1}$, skaičiuodami

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij}\, x^j \pmod{f(x)}, \ \ 0 \leqslant i \leqslant n-1.$$

2. Tiesinėje algebroje žinomais metodais randame matricos $B - I$ branduolio bazę (fundamentaliąją homogeninės sistemos $(a_0, a_1, \ldots, a_{n-1}) \cdot (B - I) = (0, 0, \ldots, 0)$ sprendinių sistemą) $d_1 = (1, 0, \ldots, 0), \ldots, d_k = (d_{k0}, d_{k1}, \ldots, d_{kn-1})$. Skaičius k yra polinomo $f(x)$ kanoniniame skaidinyje esančių neredukuojamų polinomų skaičius. Tegu S yra polinomo $f(x)$ skaidinyje esančių polinomų aibė.

Priskiriame $S := \{f(x)\}$, $r := 1$, $t := 1$.

3. Jeigu $k = r$, tai aibėje S esantys polinomai yra polinomo $f(x)$ kanoninio skaidinio polinomai; skaičiavimai baigiami.

Jeigu $k < r$, tai $t := t + 1$ ir $h(x) := \sum\limits_{i=0}^{n-1} d_{ti} x^i$.

4. Visiems $g(x) \in E$, $\deg g(x) > 1$ ir visiems $c \in GF(q)$ skaičiuojame polinomus: DBD $\big(g(x), h(x) - c\big)$. Tegu T yra šių polinomų, kurių laipsnis didesnis už 1, aibė.

Priskiriame $S := (S - \{g\}) \cup T$; $r := r - 1 + |T|$.

Pereiname prie 3.

$\triangle$

13.8 pavyzdys. Faktorizuosime polinomą $f(x) = x^8 + x^6 + x^4 + x + 1$ virš kūno $GF(2)$. Šis polinomas yra bekvadratis, nes DBD $\big(f, f'(x)\big) = 1$. Taikome Berlekampo algoritmą

$$\begin{array}{lllllllllllllllll}
x^0 & \equiv & 1 \\
x^2 & \equiv & & & & & x^2 \\
x^4 & \equiv & & & & & & & & & x^4 \\
x^6 & \equiv & & & & & & & & & & & & & x^6 \\
x^8 & \equiv & 1 & + & x & & & & & + & x^4 & & & + & x^6 \\
x^{10} & \equiv & 1 & + & x & + & x^2 & + & x^3 & + & x^4 \\
x^{12} & \equiv & & & & & x^2 & + & x^3 & + & x^4 & + & x^5 & + & x^6 \\
x^{14} & \equiv & 1 & + & x & & & + & x^3 & & & + & x^5 & & & + & x^7,
\end{array}$$

todėl matrica B yra

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

o matrica $B - I$ yra

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Matricos $B - I$ rangas lygus 6 ir todėl polinomo $f(x)$ kanoniniame skaidinyje virš $GF(2)$ yra $k = 8 - 6 = 2$ neredukuojami polinomai. Sistemos $(**)$ sprendinių aibė yra

$$\big\{(\alpha, 0, \beta, \beta, \beta, 0, \beta, \beta) \mid \alpha, \beta \in GF(2)\big\}.$$

Fundamentaliuosius sprendinius $d_1 = (1, 0, 0, 0, 0, 0, 0, 0)$ ir $d_2 = (0, 0, 1, 1, 1, 0, 1, 1,)$ atitinka polinomai

$$h_1(x) = 1,$$
$$h_2(x) = x^2 + x^3 + x^4 + x^6 + x^7.$$

Pasinaudoję Euklido algoritmu, gausime

$$\mathrm{DBD}\big(f(x), h_2(x)\big) = x^5 + x^4 + x^2 + x + 1$$

ir

$$\mathrm{DBD}\big(f(x), h_2(x) - 1\big) = x^3 + x^2 + 1.$$

Taigi polinomo $f(x)$ kanoninis skaidinys yra

$$f(x) = x^8 + x^6 + x^4 + x + 1 = (x^5 + x^4 + x^2 + x + 1)\,(x^3 + x^2 + 1).$$