17. CIKLOTOMINIAI POLINOMAI

Ieškodami polinomo $u_n(x) = x^n - 1 \in GF(q)[x]$ kanoninio skaidinio, naudojomės šio polinomo skaidinio kūnu $GF(q^s)$. Norint faktorizuoti šį polinomą be kūno $GF(q^s)$, svarbūs yra polinomai, kurių šaknys – visos primityviosios n-ojo laipsnio vieneto šaknys.

12.8 apibrėžimas. *Tegu $GF(q)$ yra baigtinis kūnas, o k – toks natūralusis skaičius, kad* $\mathrm{DBD}(k,q) = 1$. *Jeigu ω – primityvioji k-ojo laipsnio vieneto šaknis, tai polinomas*

$$Q_k(x) = \prod_{\substack{s=1 \\ \mathrm{DBD}(s,k)=1}}^{k} (x - \omega^s)$$

vadinamas k-ciklotominiu polinomu virš kūno $GF(q)$.

Aišku, kad k-ciklotominio polinomo $Q_k(x)$ šaknys yra visos primityviosios k-ojo laipsnio vieneto šaknys. Šio polinomo laipsnis yra lygus $\varphi(k)$; čia φ – Oilerio funkcija.

12.9 teiginys. *Tegu $GF(q)$ yra baigtinis kūnas, kurio charakteristika yra p, t.y. $q = p^r$, o n– toks natūralusis skaičius, kad* $\mathrm{DBD}(n,q) = 1$. *Tada:*

1.
$$x^n - 1 = \prod_{k|n} Q_k(x).$$

2. k-ciklotominio polinomo $Q_k(x)$ koeficientai yra kūno $GF(p)$ elementai, t.y. $Q_k(x) \in GF(p)[x]$.

3. Jeigu skaičiaus q eilė $\bmod k$ *yra s, $s = \mathrm{ord}_k(q)$, tai k-ciklotominio polinomo kanoniniame skaidinyje yra $\frac{\varphi(k)}{s}$ skirtingų vieno ir to paties s laipsnio neredukuojamų polinomų virš $GF(q)$.*

4. Jeigu μ – Miobiuso funkcija, tai

$$Q_k(x) = \prod_{d|k} (x^d - 1)^{\mu(\frac{k}{d})} = \prod_{d|k} (x^{\frac{k}{d}} - 1)^{\mu(d)}.$$

Įrodymas. 1. Jeigu ω yra primityvioji n-ojo laipsnio vieneto šaknis, tai visos n-ojo laipsnio vieneto šaknys yra ω laipsniai ω^i, $1 \leqslant i \leqslant n$. Elementas ω^i taip pat yra primityvioji $\frac{n}{\mathrm{DBD}\,(n,i)} = k$-laipsnio vieneto šaknis. Pastebėsime, kad k yra elemento ω^i eilė ciklinėje grupėje E_n. Todėl tokių skirtingų n-ojo laipsnio vieneto šaknų, kurios taip pat būtų ir k-ojo laipsnio primityviosios vieneto šaknys, yra $\varphi\,(k)$ (žr. 5.43 teiginio 4a) dalį). Polinomo $u_n(k)$ skaidinyje

$$x^n - 1 = \prod_{i=1}^{n} (x - \omega^i)$$

sugrupavę tuos daugiklius $(x - \omega^i)$, kuriuose ω^i yra primityvioji k-ojo laipsnio vieneto šaknis (k – bet kuris teigiamas skaičiaus n daliklis), ir gausime teiginyje esančią išraišką.

2. Prisiminkime, kad polinomo $u_n(x)$ kanoninis skaidinys virš kūno $GF(p)$ yra

$$x^n - 1 = \prod_i m_i(x);$$

čia $m_i(x)$ yra skirtingi minimalieji n-ojo laipsnio vieneto šaknų polinomai. Tada $Q_k(x)$ yra tokių minimaliųjų polinomų $m_i(x)$ sandauga, kad $k = \operatorname{ord} m_i(x)$ ir todėl $Q_k(x) \in GF(p)[x]$.

3. Jeigu ω yra bet kuri primityvioji k-ojo laipsnio vieneto šaknis virš kūno $GF(q)$, tai

$$\omega \in GF(q^i) \iff \omega^{q^i} = \omega \iff q^i \equiv 1 \,(\mathrm{mod}\, k)$$

ir $s = \operatorname{ord}_k(q)$ yra toks mažiausias natūralusis skaičius, kad

$$\omega \in GF(q^s), \quad \text{bet} \quad \omega \notin GF(q^j), \;\; j < s.$$

Tada minimaliojo elemento ω polinomo laipsnis yra lygus s ir todėl visų skirtingų minimaliųjų polinomų, kurių šaknys yra primityviosios k-ojo laipsnio vieneto šaknys, laipsniai yra lygūs s. Bet iš viso yra $\varphi\,(k)$ skirtingų primityviųjų k-ojo laipsnio vieneto šaknų, todėl skirtingų neredukuojamų polinomų virš $GF(q)$, kurių laipsnis yra s, yra $\frac{\varphi\,(k)}{s}$. Šių polinomų sandauga ir yra k-ciklotominio polinomo kanoninis skaidinys.

4. Tegu $h(k) = Q_k(x)$ ir $H(k) = x^k - 1$ su visais $k \in \mathbb{N}$ yra funkcijos, kurių reikšmės yra multiplikacinėje nenulinių racionaliųjų funkcijų virš kūno $GF(q)$ grupėje. Iš šio teiginio 1-osios dalies $x^k - 1 = \prod\limits_{d|k} Q_d(x)$, t.y. $H(k) = \prod\limits_{d|k} h(d)$. Paskutinei lygybei pritaikę Miobiuso apgręžimo formulės multiplikatyvųjį variantą (žr. 11.16 teiginio 3.2 dalį), gausime norimą ciklotominio polinomo $Q_k(x)$ išraišką.

12.10 pavyzdžiai. 1. $Q_1(x) = x - 1$ virš bet kokio kūno K.

2. Tegu $GF(q)$ yra baigtinis kūnas, o r – pirminis skaičius, tarpusavyje pirminis skaičiui q. Tada:

a) $x^r - 1 = Q_1(x)\, Q_r(x)$ ir todėl

$$Q_r(x) = \frac{x^r - 1}{Q_1(x)} = \frac{x^r - 1}{x - 1} = x^{r-1} + x^{r-2} + \ldots + x^2 + x + 1;$$

b) $x^{r^k} - 1 = Q_1(x)\, Q_r(x)\, Q_{r^2}(x) \ldots Q_{r^k}(x)$ ir todėl

$$\begin{aligned} Q_{r^k}(x) &= \frac{x^{r^k} - 1}{Q_1(x)\, Q_r(x)\, Q_{r^2}(x) \ldots Q_{r^{k-1}}(x)} \\ &= \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1} = x^{(r-1)r^{k-1}} + x^{(r-2)r^{k-1}} + \ldots + x^{r^{k-1}} + 1. \end{aligned}$$

3. Virš kūno $GF(2)$ teisinga

$$x^{15} - 1 = Q_1(x)\, Q_3(x)\, Q_5(x)\, Q_{15}(x).$$

Žinome, kad:

$$\begin{aligned} Q_1(x) &= x - 1 = x + 1, \\ Q_3(x) &= x^2 + x + 1, \\ Q_5(x) &= x^4 + x^3 + x^2 + x + 1, \\ Q_{15}(x) &= \prod_{d|15} \left(x^{\frac{15}{d}} - 1\right)^{\mu(d)} \\ &= \left(x^{15} - 1\right)^{\mu(1)} \left(x^5 - 1\right)^{\mu(3)} \left(x^3 - 1\right)^{\mu(5)} (x - 1)^{\mu(15)} \\ &= \left(x^{15} - 1\right)\left(x^5 - 1\right)^{-1}\left(x^3 - 1\right)^{-1}(x - 1) = \frac{(x^{15} - 1)(x - 1)}{(x^5 - 1)(x^3 - 1)} \\ &= x^8 + x^7 + x^5 + x^4 + x^3 + x + 1. \end{aligned}$$

Taigi turime polinomo $u_n(x)$ skaidinį ciklotominių polinomų sandauga:

$$x^{15}-1=(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)\\ \cdot(x^8+x^7+x^5+x^4+x^3+x+1).$$

Palyginę šį polinomo $u_n(x)$ skaidinį su kanoniniu $u_n(x)$ skaidiniu

$$x^{15}-1=(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)\\ \cdot(x^4+x^3+1)(x^4+x+1),$$

matome, kad polinomo $Q_{15}(x)$ kanoninis skaidinys yra

$$Q_{15}(x)=(x^4+x^3+1)(x^4+x+1);$$

čia polinomai x^4+x^3+1 ir x^4+x+1 yra 15-ojo laipsnio primityviųjų vieneto šaknų minimalieji polinomai ir todėl šių polinomų eilė yra lygi 15. Apibrėžtas 12.9 teiginio 3 dalyje natūralusis skaičius $s=\mathrm{ord}_k(q)$ šiuo atveju yra lygus $s=\mathrm{ord}_{15}(2)=4$ ir todėl $Q_{15}(x)$ yra $\frac{\varphi(15)}{4}=2$ neredukuojamų polinomų virš $GF(2)$ sandauga.

12.11 pastaba. Visos ciklotominio polinomo $Q_{q^n-1}(x)\in GF(q)[x]$ šaknys yra (q^n-1) laipsnio primityviosios vieneto šaknys virš kūno $GF(q)$, ir todėl šio polinomo kanoniniame skaidinyje yra visi primityvieji n-ojo laipsnio polinomai virš $GF(q)$. Taigi dar kartą įsitikiname, kad polinomai x^4+x^3+1 ir x^4+x+1 yra visi primityvieji 4-ojo laipsnio polinomai virš kūno $GF(2)$.

Nagrinėjant neredukuojamus polinomus virš kūno $GF(q)$, naudinga žinoti, kada jie išlieka neredukuojamais polinomais virš minėto kūno plėtinio $GF(q^k)$. Dabar mes galime atsakyti į šį klausimą.

12.12 teiginys. *Tegu f yra n-ojo laipsnio neredukuojamas polinomas virš kūno $GF(q)$. Tada:*

1. Jeigu $k\in\mathbb{N}$, tai polinomų žiede $GF(q^k)[x]$ polinomo f kanoniniame skaidinyje yra $d=\mathrm{DBD}(k,n)$ neredukuojamų to paties $\frac{n}{d}$ laipsnio polinomų.

2. Polinomas f yra neredukuojamas virš $GF(q^k)$ tada ir tik tada, kai $\mathrm{DBD}(k,n)=1$.

Įrodymas. 1. Tegu polinomo f eilė lygi e, $\operatorname{ord}(f) = e$ (žr. 11.5 apibrėžimą). Jeigu polinomas g yra bet kuris neredukuojamas polinomo f daliklis, tai $\operatorname{ord}(g) = \operatorname{ord}(f) = e$, nes visos polinomo g šaknys yra polinomo f šaknys, o polinomo f eilė yra lygi kurios nors (nesvarbu kurios) savo šaknies eilei polinomo f skaidinio kūno multiplikacinėje grupėje. Žinome, kad šie teiginiai yra ekvivalentūs (žr. 11.6 teiginį):

1) $\operatorname{ord} f = e$;

2) visos polinomo f šaknys yra primityviosios e-ojo laipsnio vieneto šaknys;

3) polinomas f yra ciklotominio polinomo $Q_e(x)$ daliklis;

4) neredukuojamo polinomo f laipsnis n yra toks mažiausias natūralusis skaičius, kuriam $q^n \equiv 1 \,(\operatorname{mod} e)$, o neredukuojamo polinomo g laipsnis m yra toks mažiausias natūralusis skaičius, kuriam $(q^k)^m \equiv 1 \,(\operatorname{mod} e)$.

Bet elemento q^k eilė ciklinėje grupėje G

$$G = \left\{q \,(\operatorname{mod} e), q^2 (\operatorname{mod} e), \ldots, q^{n-1} \,(\operatorname{mod} e), q^n \,(\operatorname{mod} e) = 1\right\} \approx \mathbb{Z}_n,$$

yra lygi

$$\operatorname{ord}_G q^k = \frac{n}{\operatorname{DBD}(k,n)} = \frac{n}{d},$$

todėl polinomo g laipsnis yra lygus $\frac{n}{d}$. Dabar aišku, kodėl polinomo f kanoniniame skaidinyje yra d neredukuojamų polinomų.

2. Jeigu $\operatorname{DBD}(k,n) = 1$, tai iš ką tik įrodyto teiginio žinome, kad polinomo f kanoniniame skaidinyje virš kūno $GF(q^k)$ yra vienas neredukuojamas polinomas, t.y. tas pats polinomas f.

△

12.13 pavyzdys. Polinomas $f(x) = x^4 + x^3 + 1$ yra neredukuojamas polinomas virš kūno $GF(2)$. Neredukuojamu šis polinomas yra ir virš kūnų $GF\left(2^{2n-1}\right)$, $n \in \mathbb{N}$, (pavyzdžiui, $GF(8)$, $GF(32)$), o štai virš kūnų $GF\left(2^{2n}\right)$, $n \in \mathbb{N}$, polinomo $f(x)$ kanoniniame skaidinyje yra arba du 2-ojo laipsnio neredukuojami polinomai (kai $n = 2k+1$, $k \in \mathbb{N}$, nes $\operatorname{DBD}(4, 4k+2) = 2$), arba keturi 1-ojo laispnio neredukuojami polinomai (kai $n = 2k$, $k \in \mathbb{N}$, nes $\operatorname{DBD}(4, 4k) = 4$).

Polinomo $f(x) = x^4 + x^3 + 1$ kanoniniame skaidinyje virš kūno $GF(4)$ yra du 2-ojo laipsnio neredukuojami polinomai: $f(x) = f_1(x)\, f_2(x)$. Tegu a yra polinomo $f_1(x)$ viena iš šaknų. Tada jungtinis virš kūno $GF(4)$ šiam elementui elementas a^4 – irgi polinomo $f_1(x)$ šaknis. Elementas a

yra primityvusis polinomo $f(x)$ skaidinio kūno $GF(16)$ elementas (plg. su 10.2 pavyzdžiu). Todėl

$$\begin{aligned} f_1(x) &= (x-a)(x-a^4) = x^2 - x(a+a^4) + a^5 \\ &= x^2 + x(a^3+a+1) + a^5 = x^2 + xa^5 + a^5. \end{aligned}$$

Padaliję polinomą $f(x)$ iš $f_1(x)$, gausime polinomą $f_2(x)$:

$$f_2(x) = x^2 + x \cdot a^{10} + a^{10}.$$

Elementas $b = a^5$ yra primityvioji 3-ojo laipsnio vieneto šaknis virš kūno $GF(2)$, todėl

$$f(x) = (x^2 + bx + b)(x^2 + xb^2 + b^2);$$

čia b – primityvioji 3-ojo laipsnio vieneto šaknis virš $GF(2)$.