Tiesinė algebra ir geometrija bioinformatikams. Paskaitų konspektas.

Rimantas Grigutis

5 paskaita. *Kompleksiniai skaičiai.*

Kompleksinius skaičius galima apibrėžti kvadratinėmis matricomis iš M_2.

5.1 Apibrėžimai. *Kompleksiniu skaičiumi vadiname matricą*

$$z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

čia a ir $b-$ realieji skaičiai.

Kompleksinį skaičių $[a] = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ vadinsime realiu kompleksiniu skaičiumi.

Realius kompleksinius skaičius $[a]$ ir $[b]$ vadinsime atitinkamai realiąja ir menamąja kompleksinio skaičiaus z dalimi. Žymėsime: $[a] = \operatorname{Re} z$ ir $[b] = \operatorname{Im} z$.

Kompleksinį skaičių $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ žymėsime raide i.

Visų komleksinių skaičių aibę žymėsime $\boldsymbol{C}$*.*

Turime, kad

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix} =$$
$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$$
$$= [a] + i\,[b]$$

ir

$$i^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = [-1]\,.$$

Du kompleksiniai skaičiai yra lygūs tada ir tik tada, kai lygios jų realios ir menamos dalys:

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} = [a_1] + i\,[b_1] = [a_2] + i\,[b_2] = \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix}$$
$$\Leftrightarrow a_1 = a_2 \text{ ir } b_1 = b_2.$$

Iš čia tiesiogiai turime, kad kompleksinis skaičius lygus nuliui tada ir tik tada, kai jo realioji ir menamoji dalys lygios nuliui:

$$[a] + i\,[b] = [0] \Leftrightarrow a = 0 \text{ ir } b = 0.$$

4-oje paskaitoje matėme, kad matricas $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ galima sutapatinti su realiu skaičiumi a. Dar daugiau, realiųjų komleksinių skaičių aibėje apibėžti sumos ir sandaugos veiksmai

$$[a] + [b] = [a + b] \text{ ir } [a]\,[b] = [ab]$$

tenkina visas realiems skaičiams būdingas savybes:
K1. $([a] + [b]) + [c] = [a] + ([b] + [c])\,.$
K2. $[a] + [b] = [b] + [a]\,.$
K3. $[a] + [0] = [a]\,.$
K4. $[a] + [-a] = [0]\,.$
K5. $([a]\,[b])\,[c] = [a]\,([b]\,[c])\,.$
K6. $[a]\,[b] = [b]\,[a]\,.$
K7. $[a]\,[1] = [a]\,.$
K8. Su visais $a \neq 0$ teisinga $[a]\,[a^{-1}] = [1]\,.$
K9. $[a]\,([b] + [c]) = [a]\,[b] + [a]\,[c]\,.$
K10. $[0] \neq [1]\,.$

Pastebėsime, kad

$$\begin{gathered} [a] - [b] = [a] + (-\,[b]) = [a] + [-b] = [a - b] \text{ ir} \\ \tfrac{[a]}{[b]} = [a]\,[b]^{-1} = [a]\,[b^{-1}] = [ab^{-1}] = \left[\tfrac{a}{b}\right]. \end{gathered}$$

Taigi realius kompleksinius skaičius $[a]$ galime sutapatinti su pačiais realiais skaičiais a ir kompleksinį skaičių $z = [a] + i\,[b]$ žymėti tiesiog $z = a + ib$.
Žvilgtelkim įdėmiau į pačių kompleksinių skaičių aritmetiką.
Dviejų kompleksinių skaičių suma irgi yra kompleksinis skaičius:

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i\,(b_1 + b_2)\,.$$

Dviejų kompleksinių skaičių sandauga irgi yra kompleksinis skaičius:

$$
\begin{gathered}
\left(a_1+ib_1\right)\left(a_2+ib_2\right) \\
=a_1\left(a_2+ib_2\right)+\left(ib_1\right)\left(a_2+ib_2\right)=a_1a_2+a_1\left(ib_2\right)+\left(ib_1\right)a_2+\left(ib_1\right)\left(ib_2\right) \\
=a_1a_2+ia_1b_2+ib_1a_2+i^2b_1b_2=\left(a_1a_2+(-1)\,b_1b_2\right)+i\left(a_1b_2+b_1a_2\right) \\
=\left(a_1a_2-b_1b_2\right)+i\left(a_1b_2+b_1a_2\right).
\end{gathered}
$$

Pastebėsime taip pat, kad kompleksinio skaičiaus $a+ib$ priešingas skaičius yra $(-a)+i(-b)$, o jei $a+ib\neq 0$, t.y. $a^2+b^2\neq 0$, tai atvirkštinis kompleksinis skaičius yra $(a+ib)^{-1}=c+id=\frac{a}{a^2+b^2}+i\frac{-b}{a^2+b^2}$.

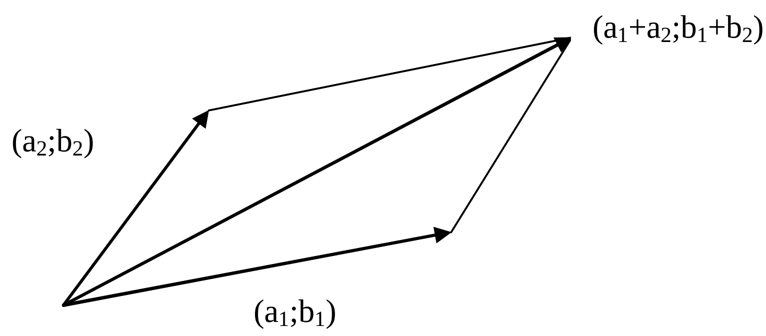
Skaitytojui paliekame savarankiškai įsitikinti, kad kompleksinių skaičų aibė $\mathbf{C}$ sudėties ir sandaugos atžvilgiu sudaro kūną(4.17 apibrėžimas). Taigi nuo šiol žinome tris kūnų pavyzdžius: racionaliųjų skaičių $\mathbf{Q}$, realiųjų skaičių $\mathbf{R}$ ir komleksinių skaičių $\mathbf{C}$: $\mathbf{R}$ yra $\mathbf{Q}$ plėtinys, $\mathbf{C}$ yra $\mathbf{Q}$ ir $\mathbf{R}$ plėtinys

$$\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}.$$

.

Geometrinis ir trigonometrinis kompleksinių skaičių reiškimas.

Kompleksinį skaičių $z=a+ib$ galima vienareikšmiškai reikšti Dekarto plokštumos tašku (a,b). Šis reiškimas pasiteisina jau ir tuo, kad pagrindiniai kompleksinių skaičių veiksmai yra paprastai interpretuojami geometriškai: dviejų kompleksinių skaičių a_1+ib_1 ir a_2+ib_2 sudėtis interpretuojama kaip dvimačių vektorių (a_1,b_1) ir (a_2,b_2) suma $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$ (prisiminkime lygiagretainio taisyklę):



Sandaugos veiksmo interpretacijai naudojamas *trigonometrinis* kompleksinio skaičiaus $z = a+ib$ reiškimas. Šiuo atveju skaičiui $z = a+ib$ priskiriamas vektorius $\overrightarrow{OA} = (a, b)$, kurio *polinės koordinatės* yra $[r, \varphi]$: čia $r = |z| -$ taško $A\,(a, b)$ atstumas iki taško $O\,(0, 0)$ vadinamas z *moduliu* , o $\varphi = \arg z-$ kampas tarp teigiamos $x-$ ašies krypties ir vektoriaus $\overrightarrow{OA}$ vadinamas z *argumentu*. Pastebėsime, kad su kiekvienu $r > 0$ kampas φ yra apibrėžiamas kampo 360° (arba 2π) kartotinio tikslumu; beto, kai $r = 0$, kampas φ neapibrėžiamas. Taigi, kiekvieną kompleksinį skaičių $z = a + ib$ galime reikšti:

$$z = [r, \varphi]\,, \qquad r \geq 0, \qquad 0^\circ \leq \varphi < 360^\circ \ (\ 0 \leq \varphi < 2\pi).$$

Kompleksinio skaičiaus z Dekarto koordinačių (a, b) ir polinių koordinačių $[r, \varphi]$ ryšį matome formulėse:

$$\begin{cases} a = r \cdot \cos\varphi \\ b = r \cdot \sin\varphi \end{cases};$$

ir

$$\begin{cases} r = \sqrt{a^2 + b^2} \\ r \neq 0 \\ \cos\varphi = \dfrac{a}{r} \\ \sin\varphi = \dfrac{b}{r} \\ 0 \leq \varphi < 2\pi \end{cases}.$$

Taigi, skaičių z galima užrašyti lygybe:

$$z = r\cos\varphi + ir\sin\varphi = r\left(\cos\varphi + i\sin\varphi\right).$$

Tai ir yra trigonometrinė kompleksinio skaičiaus z išraiška.

5.2 Apibrėžimas. *Du kompleksiniai skaičiai* $z_1 = [r_1, \varphi_1]$ *ir* $z_2 = [r_2, \varphi_2]$ yra lygūs *jei*

arba $r_1 = r_2 = 0$ *ir* φ_1, φ_2- *bet kokie kampai,*

arba $r_1 = r_2$ *ir* $\varphi_1 = \varphi_2 + k \cdot 2\pi$ *su visais* $k \in Z$.

Grįžkime prie geometrinės sandaugos veiksmo interpretacijos. Tegu

$$z_1 = [r_1, \varphi_1] = r_1\cos\varphi_1 + ir_1\sin\varphi_1$$

ir

$$z_2 = [r_2, \varphi_2] = r_2 \cos\varphi_2 + ir_2 \sin\varphi_2.$$

Tada

$$\begin{gathered} z_1 z_2 = \\ r_1 r_2 \left((\cos\varphi_1 \cos\varphi_2 - \sin\varphi_1 \sin\varphi_2) + i\left(\cos\varphi_1 \sin\varphi_2 + \sin\varphi_1 \cos\varphi_2\right)\right) = \\ r_1 r_2 \left(\cos\left(\varphi_1 + \varphi_2\right) + i \sin\left(\varphi_1 + \varphi_2\right)\right) \end{gathered}$$

ir todėl

$$z_1 z_2 = \left[r_1 r_2, \varphi_1 + \varphi_2\right],$$

t.y.

$$\begin{cases} |z_1 z_2| & = |z_1| \cdot |z_2| \\ \arg\left(z_1 z_2\right) & = \arg z_1 + \arg z_2 \end{cases}.$$

Skaičiaus z_1 sandaugą su skaičiumi z_2 geometriškai galime interpretuoti vektoriaus z_1 posūkiu kampu φ_2 ir "ištempimu" r_2 kartus. Toks kompleksinių skaičių sandaugos interpretavimas nesunkiai leidžia paaiškinti skaičiaus $z \neq 0$ atvirkštinio skaičiaus $z^{-1} = \dfrac{1}{z}$ geometrinę prasmę.

5.3 Apibrėžimas. *Tegu* $z = a + ib \in \mathbf{C}$. *Skaičius* $\bar{z} = a - ib \in \mathbf{C}$ *vadinamas skaičiaus* z *jungtiniu skaičiumi.*

Yra teisingos šios lygybės:

$$\frac{z + \bar{z}}{2} = \mathrm{Re}(z)\,, \quad \frac{z - \bar{z}}{2i} = \mathrm{Im}(z)\,, \quad z \cdot \bar{z} = |z|^2.$$

Tegu skaičiaus $z = [r, \varphi]$ atvirkštinis $z^{-1} = [q, \psi]$. Tada

$$z \cdot z^{-1} = [r, \varphi] \cdot [q, \psi] = [r \cdot q, \varphi + \psi] = 1 = [1, 0]\,,$$

t.y.

$$r \cdot q = 1, \qquad \varphi + \psi = 0 + 2\pi k, \quad k \in \mathbf{Z},$$

ir

$$q = r^{-1}, \qquad \psi = -\varphi + 2\pi k, \quad k \in \mathbf{Z} \text{ ir pvz. } \psi = -\varphi.$$

Atsižvelgę į tai, kad $\cos(-\varphi) = \cos\varphi$, o $\sin(-\varphi) = -\sin\varphi$, turime, kad

$$\begin{gathered} z = r(\cos\varphi + i\sin\varphi), r \neq 0 \Rightarrow \\ \left\{ \begin{array}{c} z^{-1} = r^{-1}(\cos\varphi - i\sin\varphi) \\ \bar{z} = r(\cos\varphi - i\sin\varphi) \end{array} \right\} \Rightarrow \\ z \cdot \bar{z} = r^2 \Rightarrow \\ z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}} = \frac{\bar{z}}{r^2} = \frac{1}{r^2}\bar{z}. \end{gathered}$$

Taigi skaičius z^{-1} yra gaunamas vektorių $\bar{z}$, simetrišką vektoriui z Ox ašies atžvilgiu, "suspaudus" $\frac{1}{r^2}$ karto.

Kompleksinių skaičių dalyba.

Tegu dabar $z_1 = [r_1, \varphi_1]$ ir $z_2 = [r_2, \varphi_2]$, $z_2 \neq 0$(t.y. $r_2 \neq 0$).
Tada

$$\frac{z_1}{z_2} = \left[\frac{r_1}{r_2}, \varphi_1 - \varphi_2\right].$$

Kompleksinio skaičiaus kėlimas sveikuoju laipsniu

Dabar induktyviai apibrėžiame kompleksinio skaičiaus z laipsnį z^n, $n \in \mathbf{N}$:

$$z^0 = 1, \qquad z^{n+1} = z^n \cdot z \qquad \text{su visais } n \in \mathbf{N}.$$

Tada

$$z = [r, \varphi] \Rightarrow r^n = [r^n, n \cdot \varphi] \quad \text{su visais } n \in \mathbf{N}.$$

Žinodami, kad $z^{-1} = [r^{-1}, -\varphi]$ ir $z^{-n} = (z^{-1})^n$, tai

$$z = [r, \varphi] \Rightarrow r^{-n} = [r^{-n}, -n \cdot \varphi] \quad \text{su visais } n \in \mathbf{N}.$$

Taigi

$$z = [r, \varphi] \Rightarrow z^n = [r^n, n \cdot \varphi] \quad \text{su visais } n \in \mathbf{Z},$$

t.y.

$$z = r(\cos\varphi + i\sin\varphi) \Rightarrow$$
$$z^n = r^n(\cos n\varphi + i\sin n\varphi) \text{ su visiais } n \in \mathbf{Z}.$$

Paskutinė lygybė yra vadinama **Muavro** (*Abraham de Moivre*,1667-1754) **formule**.

Šaknies traukimas iš kompleksinio skaičiaus.

5.4 Apibrėžimas. *Su visais $n \geq 2$ $n-$ ojo laipsnio šaknimi iš kompleksinio skaičiaus z vadiname tokius kompleksinius skaičius w, kuriems teisinga lygybė $w^n = z$.*

5.5 Teiginys. *Jei $z = r(\cos\varphi + i\sin\varphi)$, tai kompleksiniai skaičiai $w_k = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right)$, $k = 0, 1, 2, ..., n-1$ yra visos skirtingos n-ojo laipsnio šaknys iš z.*

Įrodymas.

Parodysime, kad egzistuoja lygiai n n - ojo laipsnio šaknų iš kompleksinio skaičiaus z.

Tegu

$$w = [q, \psi] = q(\cos\psi + i\sin\psi)$$

ir

$$w^n = z.$$

Tada

$$[q^n, n\cdot\psi] = [r, \varphi].$$

Jeigu $z = 0$, tai ir $r = 0$, todėl $q^n = 0 \Rightarrow q = 0$, t.y. $w = 0$.
Jeigu $z \neq 0$, tai ir $r \neq 0$, todėl

$$q^n = r, \qquad n\cdot\psi = \varphi + 2\pi k, \qquad k \in \mathbf{Z}$$
$$\Rightarrow q = \sqrt[n]{r}, \qquad \psi = \frac{\varphi + 2\pi k}{n}, \qquad k \in \mathbf{Z}..$$

Jeigu $k_1, k_2 \in \mathbf{Z}$, tai iš lygybės

$$\frac{\varphi + 2\pi k_1}{n} = \frac{\varphi + 2\pi k_2}{n} + 2\pi \cdot l, \qquad l \in \mathbf{Z}$$

turime, kad

$$k_1 - k_2 = l \cdot n \qquad \text{su kažkuriuo } l \in \mathbf{Z}.$$

ir tada $k_1 - k_2$ dalijasi iš n.

Gavome: jeigu $z \neq 0$ ir $z = r(\cos\varphi + i \sin\varphi) \in \mathbf{C}$, tai $n-$ ojo laipsnio šaknimis yra kompleksiniai skaičiai

$$w_k = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i \sin\frac{\varphi + 2\pi k}{n}\right), \qquad k \in \mathbf{Z},$$

ir du tokie skaičiai w_{k_1} ir w_{k_2} yra lygūs tada ir tik tada, kada $k_1 - k_2$ dalijasi iš n. Visos skirtingos $n-$ ojo laipsnio šaknys iš kompleksinio skaičiaus z yra $w_0, w_1, ..., w_{n-1}$.

Įrodyta.

5.6 Apibrėžimas. *Išraiška* $N(z) = z \cdot \bar{z} = |z|^2$ *vadinama skaičiaus* z *norma.*

5.7 Teorema. *Tegu* $z = a + ib,\ z_1,\ z_2 \in \mathbf{C}$. *Tada yra teisingos šios savybės.*

1)

$$\overline{(\bar{z})} = z,$$
$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \text{ atskiru atveju } \overline{-z} = -\bar{z}.$$
$$\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2, \text{ atskiru atveju } \overline{\left(\frac{1}{z}\right)} = \frac{1}{\bar{z}}.$$

2) Jeigu $N(z) = z \cdot \bar{z} = |z|^2$, *tai*

$$N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$$

ir

$$N\left(\frac{z_1}{z_2}\right) = \frac{N(z_1)}{N(z_2)} \text{ su visiais } z_2 \neq 0.$$

3) Jeigu $|z| = \sqrt{a^2 + b^2} = \sqrt{z \cdot \bar{z}}$, *tai*

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|,$$
$$\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|} \qquad \textit{su visiais } z_2 \neq 0.$$

4) (Trikampio nelygybė).

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

Įrodymas. Įrodysime trikampio nelygybę:

$$|z_1 + z_2|^2 = (z_1 + z_2) \cdot (\bar{z}_1 + \bar{z}_2) = |z_1|^2 + |z_2|^2 + z_1 \cdot \bar{z}_2 + \bar{z}_1 \cdot z_2 =$$
$$|z_1|^2 + 2\mathrm{Re}(z_1 \cdot \bar{z}_2) + |z_2|^2 \leq |z_1|^2 + 2|z_1 \cdot \bar{z}_2| + |z_2|^2 = |z_1|^2 + 2|z_1 \cdot z_2| + |z_2|^2 =$$
$$(|z_1| + |z_2|)^2.$$

Ištraukę aritmetinę kvadratinę šaknį, turėsime

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

Įrodyta.

5.8 Išvados. Iš trikampio nelygybės turime

$$|z_1 - z_2| \leq |z_1| + |z_2|$$
$$\left.\begin{array}{l} |z_1 + z_2| \geq |z_1| - |z_2| \\ |z_1 + z_2| \geq |z_2| - |z_1| \end{array}\right\} \Rightarrow |z_1 + z_2| \geq ||z_1| - |z_2||$$

taigi su visais $z_1, z_2 \in \mathbf{C}$ yra teisinga

$$||z_1| - |z_2|| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|.$$

Šaknys iš vieneto

Kaip ir su kiekvienu nenuliniu kompleksiniu skaičiumi, taip ir su 1 turime lygiai n $n-$ojo laipsnio šaknų iš 1 :

$$1 = [1, 0] = \cos 0 + i \sin 0$$
$$\varepsilon_k = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}, k=0,1,2,\ldots,n\text{-}1.$$

Visos $n-$ ojo laipsnio šaknys iš vieneto yra apskritimo, kurio centas yra koordinačių pradžioje ir spindulys lygus 1, taškai. Vienas iš šių taškų sutampa su 1 (kai $k=0$). Šaknies ε_1 argumentas yra $\frac{2\pi}{n}=2\pi\cdot\frac{1}{n}$, t.y. n – oji apskritimo dalis. Kitų šaknų $\varepsilon_2,...,\varepsilon_{n-1}$ argumentai yra $\frac{2\pi k}{n}=2\pi\cdot\frac{2}{n},...,\frac{2\pi\left(n-1\right)}{n}=2\pi\cdot\frac{n-1}{n}$. Visos $n-$ ojo laipsnio šaknys iš vieneto dalija vienetinį apskritimą į n lygių dalių. Visų $n-$ ojo laipsnio šaknų iš vieneto aibę žymėsime $U\left(n\right)$.

5.9 Apibrėžimas. *$n-$ ojo laipsnio šaknis iš vieneto ε vadinama* **primityviąja** *$n-$ ojo laipsnio šaknimi iš vieneto, jei $\varepsilon^m\neq 1$ su $m<n$.*

Aišku, kad skaičius $\varepsilon_1=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto. Kai $n>2$, turime ir daugiau primityviųjų $n-$ ojo laipsnio šaknų iš vieneto. Teisinga tokia teorema:

5.10 Teorema. *Skaičius $\varepsilon_k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}$ yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto tada ir tik tada, kai skaičių k ir n bendras didžiausias daliklis yra lygus 1 (tokius skaičius dar vadina tarpusavyje pirminiais skaičiais).*

Įrodymas. $(\Rightarrow)$. Tegu k ir n yra tarpusavyje pirminiai skaičiai ir $\varepsilon_k^m=1$. Tada

$$\frac{2\pi km}{n}=2r\pi,\text{ čia } r \text{ - sveikas skaičius.}$$

Turime

$$km=nr,$$

ir todėl km dalijasi iš n. Bet k ir n yra tarpusavyje pirminiai skaičiai, todėl m dalijasi iš n. Tada turime, kad $m\geq n$ ir todėl skaičius $\varepsilon_k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}$ yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto.

$(\Leftarrow)$. Tegu ε_k yra primityvioji $n-$ ojo laipsnio šaknis iš vieneto ir $d=$BDD(k,n), $n=n_1d, k=k_1d$. Tada $\varepsilon_k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}=\cos\frac{2\pi k_1 d}{n_1 d}+i\sin\frac{2\pi k_1 d}{n_1 d}=\cos\frac{2\pi k_1}{n_1}+i\sin\frac{2\pi k_1}{n_1}$ ir $\varepsilon_{k_1}^{n_1}=1$. Iš čia turime, kad $n=n_1$ ir $d=1$, t.y. skaičiai n ir k yra tarpusavyje pirminiai.

Įrodyta.

5.11 Pavyzdys.

Primityvios n -ojo laipsnio šaknys iš 1

n	šaknų skaičius	Primityvios šaknys ε_k
3	2	$\varepsilon_1, \varepsilon_2$
4	2	$\varepsilon_1, \varepsilon_3$
5	4	$\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$
6	2	$\varepsilon_1, \varepsilon_5$
7	6	$\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6$
8	4	$\varepsilon_1, \varepsilon_3, \varepsilon_5, \varepsilon_7$
9	6	$\varepsilon_1, \varepsilon_2, \varepsilon_4, \varepsilon_5, \varepsilon_7, \varepsilon_8$
10	4	$\varepsilon_1, \varepsilon_3, \varepsilon_7, \varepsilon_9$
11	10	$\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7, \varepsilon_8, \varepsilon_9, \varepsilon_{10}$
12	4	$\varepsilon_1, \varepsilon_5, \varepsilon_7, \varepsilon_{11}$

.

5.12 Teiginys. *Skaičius* $\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$ *yra primityvioji* $n_1 = \frac{n}{d}-$ *ojo laipsnio šaknis iš vieneto, čia* $d = \mathrm{BDD}(n,k)$.

Įrodymas. Skaičiai $n_1 = \frac{n}{d}$ ir $k_1 = \frac{k}{d}$ yra tarpusavyje pirminiai skaičiai ir todėl pagal ką tik įrodytą teoremą skaičius $\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = \cos\frac{2\pi k_1}{n_1} + i\sin\frac{2\pi k_1}{n_1} = \varepsilon_{k_1}$ yra primityvioji n_1- ojo laipsnio šaknis iš vieneto.

Įrodyta.

5.13 Teiginys(šaknų iš vieneto savybės).

1. Jeigu α *ir* $\beta \in U(n)$, *tai ir* $\alpha \cdot \beta \in U(n)$.

2. Jeigu $\alpha \in U(n)$, *tai* $\alpha^{-1} \in U(n)$.

3. Jeigu ε *yra primityvioji* n*-ojo laipsnio šaknis iš* 1, *o* $\alpha \in U(n)$, *tai egzistuoja toks* $k \in \mathbf{N}$, *kad* $\alpha = \varepsilon^k$.

4. Jeigu ε *yra primityvioji* n*-ojo laipsnio šaknis iš* 1, *o* β *yra kuri nors* n*-ojo laipsnio šaknis iš* α, *tai skaičiai* $\varepsilon^0\beta, \varepsilon^1\beta, \varepsilon^2\beta, ..., \varepsilon^{n-1}\beta$ *yra visos skirtingos* n*-ojo laipsnio šaknys iš* α.

Įrodymas. 1. Jei α ir $\beta \in U(n)$, tai $\alpha^n = \beta^n = 1$. Tada $(\alpha\beta)^n = \alpha^n\beta^n = 1$ ir $\alpha \cdot \beta \in U(n)$.

2. Jei $\alpha \in U(n)$, tai $\alpha^n = 1$. Tada $(\alpha^{-1})^n = \alpha^{-n} = (\alpha^n)^{-1} = 1$ ir $\alpha^{-1} \in U(n)$.

3. Tegu ε yra primityvioji n-ojo laipsnio šaknis iš 1. Tada skaičius $\varepsilon^k \in U(n)$, nes $\left(\varepsilon^k\right)^n = (\varepsilon^n)^k = 1$. Šaknų iš 1 sekoje $1 = \varepsilon^0, \varepsilon^1, \varepsilon^2, ..., \varepsilon^{n-1}$ nėra sutampančių, nes jei būtų $\varepsilon^k = \varepsilon^m$, čia $0 \leq k < m \leq n-1 < n$, tai $\varepsilon^{m-k} = 1$ ir $0 < m-k < n$, o tai prieštarautų tam, kad ε yra primityvioji n-ojo laipsnio šaknis iš 1. Gavome, kad sekoje $1 = \varepsilon^0, \varepsilon^1, \varepsilon^2, ..., \varepsilon^{n-1}$ yra visos skirtingos n-ojo laipsnio šaknys iš 1.

4. Tegu $\beta^n = \alpha$ ir ε yra primityvioji n-ojo laipsnio šaknis iš 1. Tada $\left(\varepsilon^k\beta\right)^n = \left(\varepsilon^k\right)^n \beta^n = 1 \cdot \alpha = \alpha$ ir $\varepsilon^k\beta$ yra n-ojo laipsnio šaknis iš α su visais $k \in \mathbf{Z}$. Skaičių $\beta = \varepsilon^0\beta, \varepsilon^1\beta, \varepsilon^2\beta, ..., \varepsilon^{n-1}\beta$ sekoje nėrs sutampančių,nes jei būtų $\varepsilon^k\beta = \varepsilon^m\beta$, čia $0 \leq k < m \leq n-1 < n$, tai $\varepsilon^{m-k} = 1$ ir $0 < m-k < n$, o tai prieštarautų tam, kad ε yra primityvioji n-ojo laipsnio šaknis iš 1. Gavome, kad sekoje $\beta = \varepsilon^0\beta, \varepsilon^1\beta, \varepsilon^2\beta, ..., \varepsilon^{n-1}\beta$ yra visos skirtingos n-ojo laipsnio šaknys iš α.

Įrodyta.