# Izbrana poglavja iz matematike

## Kolobarji polinomov

(1) Reši v obsegu kompleksnih števil dane enačbe in nato skiciraj rešitve:

(a) $z^3 = 1$,

(b) $z^6 = 1$,

(c) $z^2 = 4i$,

(d) $z^4 = i$.

*Rešitev:* Za poljubno neničelno kompleksno število $a$ ima enačba

$$z^n = a$$

natanko $n$ različnih kompleksnih rešitev, ki jim rečemo $n$-ti koreni števila $a$.

(a) Iščemo rešitve enačbe $z^3 = 1$. Pišimo $z = |z|e^{i\phi}$. Sledi

$$|z|^3 e^{i3\phi} = 1 \cdot e^{i2k\pi}.$$

Vidimo, da je:

$$|z| = 1,$$
$$\phi = \frac{2k\pi}{3}.$$

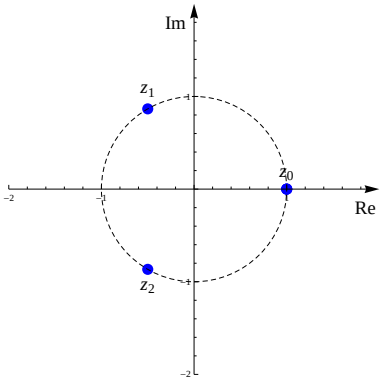
Ker nas zanimajo polarni koti $\phi \in [0, 2\pi)$, pridejo v poštev samo $k \in \{0, 1, 2\}$. Rešitve enačbe so

$$z_k = e^{\frac{2k\pi i}{3}}, \quad k \in \{0, 1, 2\}.$$

Eksplicitno so to števila:

$$z_0 = 1,$$
$$z_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2},$$
$$z_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Geometrijsko so rešitve enačbe $z^3 = 1$ oglišča enakostraničnega trikotnika, ležijo pa na enotski krožnici.



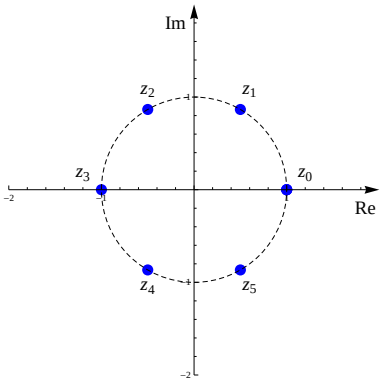
(b) Poiščimo sedaj rešitve enačbe $z^6 = 1$. Spet pišimo $z = |z|e^{i\phi}$. Sledi

$$|z|^6 e^{6i\phi} = 1 \cdot e^{2k\pi i}.$$

Vidimo, da je $|z| = 1$ in $\phi = \frac{k\pi}{3}$. V poštev pridejo $k \in \{0, 1, 2, 3, 4, 5\}$. Rešitve enačbe

$$z_k = e^{\frac{k\pi i}{3}}, \quad k \in \{0, 1, 2, 3, 4, 5\}.$$

so oglišča enakostraničnega šestkotnika.




Opomba: Za splošen $n$ tvorijo $n$-ti koreni enote oglišča enakostraničnega $n$-kotnika. Eno izmed oglišč je zmeraj $z_0 = 1$. Če je $n$ lih, je to hkrati tudi edini realni koren enačbe $z^n = 1$. Če je $n$ sod, pa je realen še $z_{\frac{n}{2}} = -1$.

(c) Rešitvi enačbe $z^2 = 4i$ sta kvadratna korena števila $4i$. Velja

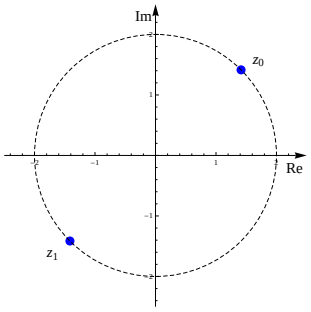
$$4i = 4 \cdot e^{i\left(\frac{\pi}{2} + 2k\pi\right)}.$$

Če pišemo $z = |z|e^{i\phi}$, mora torej veljati

$$|z|^2 e^{2i\phi} = 4 \cdot e^{i\left(\frac{\pi}{2} + 2k\pi\right)}.$$

Sledi $|z| = 2$ in $\phi = \frac{\pi}{4} + k\pi$ za $k \in \{0, 1\}$. Rešitvi enačbe sta

$$z_k = 2e^{i\left(\frac{\pi}{4} + k\pi\right)}, \quad k \in \{0, 1\}.$$




(d) Rešimo še enačbo $z^4 = i$. Če pišemo $z = |z|e^{i\phi}$, dobimo

$$|z|^4 e^{i4\phi} = 1 \cdot e^{i\left(\frac{\pi}{2} + 2k\pi\right)}.$$

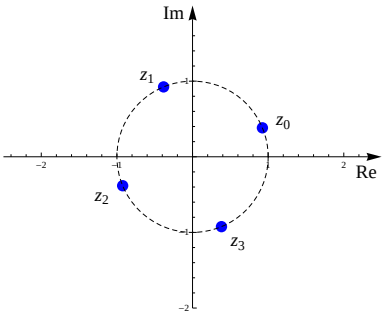
Od tod dobimo:

$$|z| = 1,$$
$$\phi = \frac{\pi}{8} + \frac{k\pi}{2}$$

za $k \in \{0, 1, 2, 3\}$. Rešitve enačbe so torej

$$z_k = e^{i\left(\frac{\pi}{8} + \frac{k\pi}{2}\right)}, \quad k \in \{0, 1, 2, 3\}.$$

Rešitve enačbe tokrat tvorijo oglišča kvadrata in ležijo na enotski krožnici. Kvadrat je zavrten za kot $\frac{\pi}{8}$ glede na koordinatne osi.




Opomba: $n$-te korene kompleksnega števila $a$ dobimo tudi na naslednji način. Če pišemo $a = |a|e^{i\phi}$, je $z_0 = \sqrt[n]{|a|}e^{\frac{i\phi}{n}}$ eden izmed $n$-tih korenov števila $a$. Preostale $n$-te korene dobimo, če $z_0$ pomnožimo z $n$-timi koreni enote. Vidimo, da $n$-ti koreni števila $a$ določajo oglišča enakostraničnega $n$-kotnika, ki leži na krožnici s središčem v 0 in s polmerom $\sqrt[n]{|a|}$. Glede na standardni $n$-kotnik korenov enote je ta $n$-kotnik zavrten za kot $\frac{\phi}{n}$. □

(2) Reši v obsegu kompleksnih števil enačbi:

(a) $z^2 - 2iz - 2 = 0$,

(b) $z^2 - (1 - 4i)z - 5 - 5i = 0$.

*Rešitev:* (a) Rešujemo kompleksno kvadratno enačbo

$$z^2 - 2iz - 2 = 0.$$

Podobno kot pri realnih enačbah ima tudi ta enačba dve rešitvi, ki ju lahko izračunamo z uporabo znane formule

$$z_{1,2} = \frac{2i \pm \sqrt{(-2i)^2 + 8}}{2} = \frac{2i \pm 2}{2}.$$

Rešitvi kvadratne enačbe sta torej:

$$z_1 = 1 + i,$$
$$z_2 = -1 + i.$$

(b) Rešujemo kompleksno kvadratno enačbo

$$z^2 - (1 - 4i)z - 5 - 5i = 0.$$

Njeni rešitvi sta

$$z_{1,2} = \frac{1 - 4i \pm \sqrt{(1-4i)^2 + 4(5+5i)}}{2} = \frac{1 - 4i \pm \sqrt{5 + 12i}}{2}.$$

Kvadratni koren $\sqrt{5+12i}$ moramo sedaj izračunati v kompleksnem. Recimo, da računamo koren kompleksnega števila $z = |z|(\cos\phi + i\sin\phi)$. Če je $z \neq 0$, ima $z$ dva kvadratna korena, ki sta določena z izrazom

$$\sqrt{z} = \pm\sqrt{|z|}(\cos\tfrac{\phi}{2} + i\sin\tfrac{\phi}{2}).$$

To število lahko natančno izračunamo z uporabo trigonometričnih formul:

$$\cos\tfrac{\phi}{2} = \pm\sqrt{\frac{1+\cos\phi}{2}},$$
$$\sin\tfrac{\phi}{2} = \pm\sqrt{\frac{1-\cos\phi}{2}}.$$

Predznaka izberemo z upoštevanjem kvadranta, v katerem leži število $z$.

V našem primeru je $|z| = \sqrt{25+144} = 13$ in $\cos\phi = \frac{x}{|z|} = \frac{5}{13}$. Ker število $z$ leži v prvem kvadrantu, bomo obakrat vzeli predznak plus, da dobimo:

$$\cos\tfrac{\phi}{2} = \sqrt{\frac{1+\frac{5}{13}}{2}} = \sqrt{\frac{9}{13}},$$
$$\sin\tfrac{\phi}{2} = \sqrt{\frac{1-\frac{5}{13}}{2}} = \sqrt{\frac{4}{13}}.$$

Od tod sledi, da je

$$\sqrt{5+12i} = \pm\sqrt{13}(\sqrt{\tfrac{9}{13}} + i\sqrt{\tfrac{4}{13}}) = \pm(3+2i).$$

Rešitvi kvadratne enačbe sta torej:

$$z_1 = 2 - i,$$
$$z_2 = -1 - 3i.$$

□

(3) Poišči ničle danih polinomov:

(a) $p(x) = x^3 + x + 1$ v $\mathbb{Z}_2[x]$,
(b) $p(x) = 3x^3 - 4x^2 - x + 4$ v $\mathbb{Z}_5[x]$.

*Rešitev:* (a) Preverimo lahko, da je $p(0) = p(1) = 1$, kar pomeni, da $p$ nima ničel.

(b) Sedaj lahko uganemo, da je $p(2) = 0$. Z deljenjem pridemo do oblike

$$p(x) = 3x^3 - 4x^2 - x + 4 = (x-2)(3x^2 + 2x + 3).$$

Za polinom $k(x) = 3x^2 + 2x + 3$ lahko preverimo, da nima ničel v $\mathbb{Z}_5$. Torej je $x = 2$ edina ničla polinoma $p$. □

(4) Poišči ničle polinoma $x^p - x$ v $\mathbb{Z}_p[x]$, če je $p$ praštevilo.

*Rešitev:* Poglejmo najprej primere $p = 2$, $p = 3$ in $p = 5$:

$$x^2 - x = x(x-1),$$
$$x^3 - x = x(x^2-1) = x(x-1)(x-2),$$
$$x^5 - x = x(x-1)(x+1)(x^2+1) = x(x-1)(x-4)(x-2)(x-3).$$

V teh treh primerih vidimo, da ima polinom $x^p - x$ nad $\mathbb{Z}_p$ ničle $\{0, 1, 2 \ldots, p-1\}$. Za poljubno praštevilo $p$ pa to sledi iz malega Fermatovega izreka, ki pravi, da za vsak $x \in \mathbb{Z}$ in vsako praštevilo $p$ velja

$$x^p \equiv x (\mathrm{mod}\ p).$$

To pomeni, da imamo v $\mathbb{Z}_p[x]$ faktorizacijo

$$x^p - x = x(x-1)(x-2)\ldots(x-p+1).$$

□

(5) Naj bo $F$ obseg in $p \in F[x]$ polinom stopnje $n \geq 1$. Pokaži, da ima polinom $p$ največ $n$ ničel.

*Rešitev:* Trditev bomo dokazali z uporabo indukcije na stopnjo $n$. Denimo najprej, da je $p(x) = kx + n \in F[x]$ polinom stopnje ena. Če sta $a, b \in F$ ničli polinoma $p$, je:

$$ka + n = kb + n,$$
$$ka = kb.$$

Po privzetku je $k \in F$ neničeln element, zato lahko zgornjo enačbo pomnožimo z njegovim inverzom, da dobimo $a = b$. Torej ima $p$ kvečjemu eno ničlo.

Predpostavimo sedaj, da ima vsak polinom v $F[x]$ stopnje $n$ največ $n$ ničel in vzemimo poljuben $p \in F[x]$ stopnje $n+1$. Pokazati želimo, da ima $p$ največ $n+1$ ničel.

Če $p$ nima ničel, ni kaj dokazovati, zato privzemimo, da je $p(a) = 0$ za nek $a \in F$. Ker gledamo polinome s koeficienti v obsegu, obstaja natanko določen polinom $k$ stopnje $n$, da velja

$$p(x) = (x-a)k(x).$$

Za poljubno ničlo $b$ polinoma $p$ potem od tod sledi, da je

$$p(b) = (b-a)k(b) = 0.$$

Če je $b \neq a$, lahko od tod sklepamo, da je $k(b) = 0$. Po indukcijski predpostavki pa od tod sledi, da ima $p$ lahko največ $n$ ničel, ki niso enake $a$. Skupaj z $a$ pa ima lahko največ $n+1$ ničel. □

(6) Poišči polinom $p \in K[x]$ stopnje $n$ z več kot $n$ ničlami.

*Rešitev:* Vzemimo na primer kvadratni polinom $p \in \mathbb{Z}_6[x]$ s predpisom

$$p(x) = (x+1)(x+2) = x^2 + 3x + 2.$$

Preverimo lahko, da je $p(1) = p(2) = p(4) = p(5) = 0$, kar pomeni, da ima $p$ štiri ničle. Razlog je v tem, da ima kolobar $\mathbb{Z}_6$ delitelje niča. □

(7) Pokaži, da je produkt primitivnih polinomov primitiven polinom.

*Rešitev:* Polinom $a(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ je *primitiven*, če je $\gcd(a_0, a_1, \ldots, a_n) = 1$. To pomeni, da je največji skupni delitelj njegovih koeficientov enak 1. Denimo sedaj, da sta:

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$
$$b(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$$

primitivna polinoma in izberimo poljubno praštevilo $p$. Ker sta $a$ in $b$ primitivna, obstajata koeficienta $a_i$ in $b_j$, ki nista deljiva s $p$. Privzamemo lahko, da sta to koeficienta z najmanjšima indeksoma, ki nista deljiva s $p$, kar pomeni, da $p$ deli $a_0, a_1, \ldots, a_{i-1}, b_0, b_1, \ldots, b_{j-1}$. Produkt polinomov $a$ in $b$ je polinom $c(x) = c_{n+m}x^{n+m} + \ldots + c_1 x + c_0$, kjer je

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0.$$

Če vzamemo $k = i + j$ tako dobimo

$$c_{i+j} = a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0.$$

V zgornji vsoti so vsi členi razen člena $a_i b_j$ deljivi s $p$. Posledično od tod sledi, da $p$ ne deli $c_{i+j}$, kar pa pomeni, da je tudi $c$ primitiven polinom. □

(8) Dokaži Gaussovo lemo: Polinom $p(x) \in \mathbb{Z}[x]$ je razcepen v $\mathbb{Z}[x]$ natanko takrat, ko je razcepen v $\mathbb{Q}[x]$.

*Rešitev:* Polinom $p \in K[x]$ je *razcepen*, če ga lahko faktoriziramo v obliki $p(x) = p_1(x)p_2(x)$, kjer sta $p_1, p_2 \in K[x]$ nekonstantna polinoma. Če je $p$ nekonstanten polinom, ki ga ne moremo razcepiti, rečemo, da je *nerazcepen*.

Če je polinom $p$ razcepen v $\mathbb{Z}[x]$, je jasno razcepen tudi v $\mathbb{Q}[x]$, zato moramo dokazati samo implikacijo v obratno smer. Pa denimo, da lahko polinom $p \in \mathbb{Z}[x]$ faktoriziramo v obliki $p = p_1 p_2$, kjer sta $p_1, p_2 \in \mathbb{Q}[x]$. Koeficienti polinomov $p_1$ in $p_2$ so racionalna števila. Če označimo s $C_1$ in $C_2$ najmanjša skupna večkratnika vseh imenovalcev koeficientov polinomov $p_1$ in $p_2$, bosta imela polinoma $\tilde{p}_1 = C_1 p_1$ in $\tilde{p}_2 = C_2 p_2$ celoštevilske koeficiente. Tako dobimo enakost

$$C_1 C_2 p = \tilde{p}_1 \tilde{p}_2.$$

Iz obeh polinomov na desni lahko izpostavimo največja skupna delitelja vseh koeficientov, da dobimo faktorizacijo $\tilde{p}_1 = D_1 \overline{p}_1$ in $\tilde{p}_2 = D_2 \overline{p}_2$, kjer sta sedaj $\overline{p}_1$ in $\overline{p}_2$ primitivna polinoma. Podobno lahko tudi polinom $p$ zapišemo v obliki $p = D\overline{p}$, kjer je polinom $\overline{p}$ primitiven. Tako dobimo enakost

$$C_1 C_2 D\overline{p} = D_1 \overline{p}_1 D_2 \overline{p}_2 = D_1 D_2 \overline{p}_1 \overline{p}_2.$$

Po prejšnji trditvi je polinom $\overline{p}_1 \overline{p}_2$ primitiven, od koder dobimo enakost

$$C_1 C_2 D = D_1 D_2,$$

kar pa pomeni, da je število $D = \frac{D_1 D_2}{C_1 C_2}$ celo. Tako dobimo faktorizacijo

$$p = D\overline{p} = D\overline{p}_1 \overline{p}_2.$$

Če s konstanto $D$ pomnožimo enega izmed polinomov na desni, dobimo iskani razcep polinoma $p$ v $\mathbb{Z}[x]$. □

(9) Ugotovi, ali sta dana polinoma nerazcepna v $\mathbb{Q}[x]$:

(a) $p(x) = x^4 + 4$,
(b) $p(x) = x^4 - 2x^3 + x + 1$.

*Rešitev:* (a) Začnimo s polinomom $p(x) = x^4 + 4$. Njegove ničle so rešitve enačbe

$$x^4 = -4,$$

kar pa so ravno četrti koreni števila $-4$. To pa so števila

$$\{1 + i, 1 - i, -1 + i, -1 - i\}.$$

Vsak par konjugirano kompleksnih ničel nam da en nerazcepen kvadratni faktor. Tako dobimo

$$x^4 + 4 = (x - (1 + i))(x - (1 - i))(x - (-1 + i))(x - (-1 - i)) = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

Polinom $p$ je torej razcepen v $\mathbb{Q}[x]$ in $\mathbb{Z}[x]$ kot produkt nerazcepnih kvadratnih faktorjev.
(b) Preverimo lahko, da polinom $p(x) = x^4 - 2x^3 + x + 1$ nima racionalnih ničel. Če bi bil razcepen, bi torej moral biti produkt kvadratnih faktorjev oblike

$$p(x) = x^4 - 2x^3 + x + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd.$$

Od tod dobimo sistem enačb:

$$\begin{aligned} a + c &= -2, \\ b + d + ac &= 0, \\ ad + bc &= 1, \\ bd &= 1. \end{aligned}$$

Po Gaussovi lemi lahko predpostavimo, da so $a, b, c, d \in \mathbb{Z}$. Iz zadnje enačbe potem sledi, da je $b = d = 1$ ali pa $b = d = -1$. Ko to vstavimo v tretjo enačbo, dobimo $a + c = \pm 1$, kar pa ni kompatibilno s prvo enačbo. Od tod sklepamo, da je polinom $p$ nerazcepen v $\mathbb{Q}[x]$ in $\mathbb{Z}[x]$. □

(10) Dokaži Eisensteinov kriterij: Naj bo $a(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ tak polinom, da obstaja praštevilo $p$, da $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$, $p \nmid a_n$ in $p^2 \nmid a_0$. Potem je $a$ nerazcepen v $\mathbb{Q}[x]$. Nato za vsako naravno število $n$ konstruiraj nerazcepen polinom stopnje $n$ v $\mathbb{Q}[x]$.

*Rešitev:* Denimo, da lahko polinom $a$ razcepimo v obliki

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = (b_r x^r + \ldots + b_1 x + b_0)(c_s x^s + \ldots + c_1 x + c_0),$$

kjer sta $r, s < n$. Po Gaussovi lemi lahko privzamemo, da so koeficienti obeh faktorjev na desni cela števila. Prosti člen produkta obeh faktorjev je enak

$$a_0 = b_0 c_0.$$

Po predpostavki $p \mid a_0$ in $p^2 \nmid a_0$. Torej $p$ deli natanko eno od števil $b_0$ in $c_0$. Privzamemo lahko, da $p \mid b_0$ in $p \nmid c_0$. Če pogledamo koeficienta pri linearnih členih na obeh straneh, dobimo enakost

$$a_1 = b_0c_1 + b_1c_0.$$

Po predpostavki $p$ deli člena $a_1$ in $b_0c_1$. Ker $p$ ne deli $c_0$, mora torej deliti tudi $b_1$. Pri kvadratnih členih sedaj dobimo enakost

$$a_2 = b_0c_2 + b_1c_1 + b_2c_0.$$

Podobno kot prej sklepamo, da mora $p$ deliti število $b_2$. Isti sklep lahko sedaj ponavljamo, da dobimo, da so vsi koeficienti $b_0, b_1, \ldots, b_{n-1}$ deljivi s $p$, dokler ne pridemo do člena

$$a_n = b_0c_n + b_1c_{n-1} + \ldots + b_{n-1}c_1 + b_nc_0.$$

Ker sta stopnji faktorjev manjši od $n$, je $b_n = 0$, kar pomeni, da je desna stran deljiva s $p$. To pa je v protislovju s predpostavko, da $p$ ne deli $a_n$. Od tod sledi, da je polinom $q$ nerazcepen.

Z uporabo Eisensteinovega kriterija lahko preprosto konstruiramo nerazcepne polinome v $\mathbb{Q}[x]$. Polinom

$$q(x) = x^n + 2$$

je na primer nerazcepen v $\mathbb{Q}[x]$ za vsak $n \in \mathbb{N}$. □

(11) Pokaži, da je polinom $q(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ nerazcepen v $\mathbb{Q}[x]$ za poljubno praštevilo $p$.

*Rešitev:* Za dokaz nerazcepnosti polinoma $q$ bomo uporabili Eisensteinov kriterij. Najprej opazimo, da je

$$q(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Definirajmo sedaj polinom $r(x) = q(x + 1)$. Polinom $r$ je potem nerazcepen natanko takrat, ko je nerazcepen polinom $q$. Eksplicitno lahko izračunamo, da je

$$r(x) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1}x^{p-1} + \ldots + \binom{p}{p-1}x + 1 - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-1} + \ldots + \binom{p}{p-1}.$$

Ker je $p$ praštevilo, so vsi binomski koeficienti $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$ za $k = 1, \ldots, p-1$ deljivi s $p$, medtem ko prosti člen $\binom{p}{p-1} = p$ ni deljiv s $p^2$. Po Eisensteinovem kriteriju je torej polinom $r$ nerazcepen. □

(12) Poišči vse nerazcepne polinome stopnje največ 3 v kolobarju polinomov $\mathbb{Z}_2[x]$.

*Rešitev:* Najprej naštejmo vse nekonstantne polinome stopnje največ 3 s koeficienti v $\mathbb{Z}_2$:

stopnja 1 : $x, x + 1$,

stopnja 2 : $x^2, x^2 + x, x^2 + 1, x^2 + x + 1$,

stopnja 3 : $x^3, x^3 + x^2, x^3 + x, x^3 + 1, x^3 + x^2 + x, x^3 + x^2 + 1, x^3 + x + 1, x^3 + x^2 + x + 1$.

Polinom stopnje največ 3 je nerazcepen natanko takrat, ko nima ničel. Z uporabo tega dejstva lahko preverimo, da so v kolobarju $\mathbb{Z}_2[x]$ nerazcepni naslednji polinomi:

$$\begin{aligned}&\text{stopnja } 1: \ x, x+1,\\ &\text{stopnja } 2: \ x^2+x+1,\\ &\text{stopnja } 3: \ x^3+x^2+1, x^3+x+1.\end{aligned}$$

Opomba: Nerazcepne polinome je težko najti, obstaja pa vsaj eden nerazcepen polinom poljubne stopnje $n \geq 1$. Natančno število nerazcepnih polinomov lahko izračunamo z uporabo Mobiusove funkcije

$$\mu(n) = \begin{cases} 1 & ; \ n = 1, \\ 0 & ; \ n \text{ je deljiv s kvadratom nekega praštevila}, \\ (-1)^k & ; \ n \text{ je produkt } k \text{ različnih praštevil}. \end{cases}$$

**Izrek.** *Število nerazcepnih polinomov v $\mathbb{Z}_p[x]$ stopnje $n$ je enako*

$$N_p(n) = \frac{p-1}{n} \sum_{d|n} \mu(\tfrac{n}{d}) p^d.$$

V primeru, ko je $p = 2$ in $n$ praštevilo, tako dobimo

$$N_p(n) = \frac{2^n - 2}{n}.$$

□

(13) Naj bo $p$ liho praštevilo.

(a) Pokaži, da tvori množica neničelnih kvadratov v $\mathbb{Z}_p$ grupo za množenje moči $\frac{p-1}{2}$.

(b) Pokaži, da je polinom $x^2 + 1$ nerazcepen v $\mathbb{Z}_p[x]$ natanko takrat, ko je $p$ oblike $p = 4k + 3$.

*Rešitev:* (a) Za občutek si najprej poglejmo množice neničelnih kvadratov v nekaterih majhnih obsegih:

$$\begin{aligned}\mathbb{Z}_3 &: \{1\},\\ \mathbb{Z}_5 &: \{1, 4\},\\ \mathbb{Z}_7 &: \{1, 2, 4\},\\ \mathbb{Z}_{11} &: \{1, 3, 4, 5, 9\}.\end{aligned}$$

Opazimo lahko, da tvorijo te množice grupe za množenje moči $\frac{p-1}{2}$. Da bi to formalno pokazali, definirajmo za vsako praštevilo $p$ homomorfizem grup $s : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ s predpisom

$$s(x) = x^2.$$

Da je to res homomorfizem, sledi iz komutativnosti množenja v $\mathbb{Z}_p$. Iz splošne teorije sledi, da je slika tega homomorfizma podgrupa v $\mathbb{Z}_p^*$, ki pa se ravno ujema z množico neničelnih kvadratov. V jedru tega homomorfizma so števila $x$, ki zadoščajo enačbi $x^2 = 1$. To pa je

kvadratna enačba v $\mathbb{Z}_p$, ki ima rešitvi $x = \pm 1$. Jedro je torej grupa z dvema elementoma, od koder pa sledi, da je moč slike ravno $\frac{p-1}{2}$.

(b) Sedaj bomo pokazali, da je polinom $x^2 + 1$ nerazcepen v $\mathbb{Z}_p[x]$ natanko takrat, ko je $p$ oblike $p = 4k + 3$. V ta namen si poglejmo enačbo

$$x^{p-1} - 1 = 0$$

v $\mathbb{Z}_p$. Pokazali smo že, da so rešitve te enačbe natanko vsi neničelni elementi $\mathbb{Z}_p$.

Če je praštevilo $p$ oblike $p = 4k + 1$, pa lahko to enačbo faktoriziramo v obliki

$$x^{p-1} - 1 = (x^{2k} - 1)(x^{2k} + 1).$$

Moč grupe neničelnih kvadratov je $\frac{p-1}{2} = 2k$. Če je torej število $x \in \mathbb{Z}_p^*$ kvadrat, je $x^{2k} = 1$, kar pomeni, da vsi kvadrati zadoščajo enačbi $x^{2k} = 1$, vsi nekvadrati pa enačbi $x^{2k} = -1$. V posebnem od tod sledi, da je za poljuben nekvadrat $x$ število $x^k$ ničla polinoma $x^2 + 1$.

Denimo sedaj, da je $p$ oblike $p = 4k + 3$ in da je $x^2 + 1$ razcepen. Potem obstaja $x \in \mathbb{Z}_p$, da velja $x^2 = -1$. Posledično potem za ta $x$ velja

$$1 = x^{p-1} = x^{4k+2} = (x^2)^{2k+1} = (-1)^{2k+1} = -1,$$

kar pa nas privede v protislovje. □

(14) Izračunaj kvocienta in ostanka pri deljenju polinoma $p$ s polinomom $q$.

(a) $p(x) = x^5 + x^3 - x^2 - x$ in $q(x) = x^3 + x$ v $\mathbb{Z}_2[x]$,
(b) $p(x) = x^5 - x^3 + x + 4$ in $q(x) = 2x^3 + x + 1$ v $\mathbb{Z}_5[x]$.

*Rešitev:* Deljenje polinomov ima podobne lastnosti kot celoštevilsko deljenje celih števil. To nam zagotavlja naslednji izrek.

**Izrek.** *Naj bo $F$ obseg in $p, q \in F[x]$ poljubna polinoma. Potem obstajata enolično določena polinoma $k, r \in F[x]$, kjer je* $\deg(r) < \deg(q)$, *da velja*

$$p(x) = k(x)q(x) + r(x).$$

Polinomu $k$ rečemo kvocient, polinomu $r$ pa ostanek pri deljenju polinoma $p$ s polinomom $q$. Kvocient in ostanek izračunamo s postopkom, ki ga poznamo iz srednje šole.

(a) Velja

$$x^5 + x^3 - x^2 - x = x^2(x^3 + x) + (x^2 + x),$$

zato je $k(x) = x^2$ in $r(x) = x^2 + x$. Pri tem primeru moramo biti pozorni, da računamo nad obsegom $\mathbb{Z}_2$, kar pomeni, da je na primer $x = -x$, $x^2 = -x^2$, $2x = 0$ itd.

(b) Ko računamo kvocient polinoma $p(x) = x^5 - x^3 + x + 4$ s polinomom $q(x) = 2x^3 + x + 1$ v $\mathbb{Z}_5[x]$, moramo upoštevati, da v obsegu $\mathbb{Z}_5$ velja $2^{-1} = 3$. Tako dobimo

$$x^5 - x^3 + x + 4 = (3x^2 + 3)(2x^3 + x + 1) + (2x^2 + 3x + 1)$$

in $k(x) = 3x^2 + 3$ ter $r(x) = 2x^2 + 3x + 1$.

Opomba: V kolobarjih polinomov $K[x]$, kjer $K$ ni nujno obseg, zgornji izrek ne velja.

(1) Če na primer izberemo polinoma $p(x) = x^2 + 1$ in $q(x) = 2x + 3$ v $\mathbb{Z}[x]$, iskana polinoma $k$ in $r$ ne obstajata. Razlog je v tem, da število 2 nima obratne vrednosti v celih številih.

(2) Če pa izberemo $p(x) = 4x^2 + 8$ in $q(x) = 4x + 8$ v $\mathbb{Z}_{12}[x]$, pa lahko preverimo, da je $r(x) = 0$, kot kvocient pa lahko dobimo več možnosti. Dve različni sta na primer $k_1(x) = x + 1$ in $k_2(x) = x + 4$. Kvocient torej ni enoličen. To je posledica dejstva, da je število 4 delitelj niča v kolobarju $\mathbb{Z}_{12}$.

V splošnih polinomskih kolobarjih $K[x]$, kjer je $K$ komutativen kolobar z enoto 1, velja podoben izrek, če se omejimo na primer, ko je vodilni koeficient polinoma $q$ enak 1. □

(15) Izračunaj največji skupni delitelj $d$ polinomov $p$ in $q$ in nato poišči polinoma $s$ in $t$, da bo veljalo $sp + tq = d$.

(a) $p(x) = x^3 + 4x^2 + 3x - 2$ in $q(x) = x^3 + 3x^2 + 3x + 2$ v $\mathbb{Q}[x]$,

(b) $p(x) = x^3 + x^2 - x + 1$ in $q(x) = x^3 + x - 1$ v $\mathbb{Z}_2[x]$.

*Rešitev:* Naj bo $F$ obseg in $p, q \in F[x]$. *Največji skupni delitelj* polinomov $p$ in $q$ je polinom $d = \gcd(p, q)$, ki zadošča pogojem:

(1) $d$ deli $p$ in $q$,

(2) vsak polinom, ki deli $p$ in $q$, deli tudi $d$,

(3) vodilni koeficient polinoma $d$ je enak 1.

**Izrek.** *Največji skupni delitelj $d = \gcd(p, q)$ obstaja in je enolično določen. Obstajata tudi polinoma $s, t \in F[x]$, da je*

$$sp + tq = d.$$

Največji skupni delitelj lahko izračunamo z Evklidovim algoritmom. Označimo $r_0 = p$ in $r_1 = q$, nato pa induktivno definirajmo polinome $k_i$ in $r_i$ za $i \geq 2$ z implicitnim predpisom:

$$\begin{aligned} r_0 &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\vdots \\ r_m &= k_{m+2} r_{m+1} + r_{m+2}, \\ r_{m+1} &= k_{m+3} r_{m+2} + 0. \end{aligned}$$

Zadnji neničelni ostanek, ki ga dobimo po tem postopku, je do skalarnega večkratnika natančno polinom $d$.

(a) V našem primeru je $r_0 = x^3 + 4x^2 + 3x - 2$ in $r_1 = x^3 + 3x^2 + 3x + 2$. Z deljenjem dobimo

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

od koder sledi $k_2(x) = 1$ in $r_2(x) = x^2 - 4$. V naslednjem koraku dobimo

$$x^3 + 3x^2 + 3x + 2 = (x + 3)(x^2 - 4) + (7x + 14),$$

zato je $k_3(x) = x + 3$ in $r_3(x) = 7x + 14$. Opazimo lahko, da imata polinoma $r_2$ in $r_3$ skupno ničlo $x = -2$. Ker je $r_3$ linearen polinom, od tod sledi, da deli polinom $r_2$. Največji skupni delitelj polinomov $p$ in $q$ je torej polinom

$$d(x) = x + 2.$$

Če sedaj Evklidov algoritem preberemo od spodaj navzgor, lahko izpeljemo, da je

$$r_3 = r_1 - k_3 r_2 = r_1 - k_3(r_0 - k_2 r_1) = -k_3 r_0 + (1 + k_2 k_3) r_1 = -(x+3)p + (x+4)q.$$

Ker je $r_3 = 7d$, lahko $d$ izrazimo v obliki

$$d = -\tfrac{1}{7}(x+3)p + \tfrac{1}{7}(x+4)q$$

in od tod preberemo, da je $s(x) = -\frac{1}{7}(x+3)$ in $t(x) = \frac{1}{7}(x+4)$. Polinoma $s$ in $t$, ki smo ju izračunali, nista edina polinoma, ki zadoščata dani enačbi.

Bolj elegantno lahko polinoma $s$ in $t$ izračunamo z uporabo razširjenega Evklidovega algoritma. Denimo, da polinoma $s_i$ in $t_i$ zadoščata enačbi

$$s_i p + t_i q = r_i.$$

Potem lahko polinome $s_{i+2}$ in $t_{i+2}$ računamo rekurzivno tako, da od $i$-te vrstice tabele odštejemo $k_{i+2}$-kratnik $(i+1)$-ve vrstice.

| $r_i$ | $s_i$ | $t_i$ | $k_i$ |
|---|---|---|---|
| $x^3 + 4x^2 + 3x - 2$ | $1$ | $0$ | |
| $x^3 + 3x^2 + 3x + 2$ | $0$ | $1$ | |
| $x^2 - 4$ | $1$ | $-1$ | $1$ |
| $7x + 14$ | $-(x+3)$ | $x+4$ | $x+3$ |

Iz zadnje vrstice lahko preberemo, da je

$$7x + 14 = -(x+3)p + (x+4)q$$

in nato po deljenju s 7 pridemo do izrazov za $s$ in $t$.

(b) Zapišimo sedaj samo tabelo. Upoštevali bomo, da računamo s polinomi v $\mathbb{Z}_2[x]$.

| $r_i$ | $s_i$ | $t_i$ | $k_i$ |
|---|---|---|---|
| $x^3 + x^2 - x + 1$ | $1$ | $0$ | |
| $x^3 + x - 1$ | $0$ | $1$ | |
| $x^2$ | $1$ | $1$ | $1$ |
| $x + 1$ | $x$ | $x+1$ | $x$ |
| $1$ | $x^2 + x + 1$ | $x^2$ | $x+1$ |

Sedaj dobimo, da je $d(x) = 1$, kar pomeni, da sta polinoma $p$ in $q$ tuja. Velja pa še $s(x) = x^2 + x + 1$ in $t(x) = x^2$. □