DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Bakalaura studiju programma "Matemātika"

Studiju kurss

Polinomu algebra

5.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis - apgūt pamatfaktus par polinomu faktorizāciju virs $\mathbb{Z}$ un $\mathbb{Q}$.

Lekcijas kopsavilkums:

- polinoms ar veseliem koeficientiem ir nedalāms virs $\mathbb{Z}$ tad un tikai tad, ja tas ir nedalāms virs $\mathbb{Q}$;
- ir lietderīgi pētīt polinomu redukcijas mod p;
- var faktorizēt polinomus virs $\mathbb{Z}$ vai $\mathbb{Q}$ izmantojot Kronekera algoritmu.

Svarīgākie jēdzieni: polinoma redukcija mod p.

Svarīgākie fakti un metodes: $\mathbb{Z}[X]$ ir VFG un Eiklīda gredzens,

satura multiplikativitāte, faktorizācijas ekvivalence virs $\mathbb{Z}$ un $\mathbb{Q}$, racionālās saknes tests, faktorizācijas mod p īpašības, Eizenšteina kritērijs, Kronekera faktorizācijas algoritms.

1. Faktorizācija virs $\mathbb{Z}$ un $\mathbb{Q}$

1.1. Pamatfakti

1.1.1. Viennozīmīgā faktorizācija virs $\mathbb{Z}$

1.1. teorēma.

1. $\mathbb{Z}[X]$ ir GFG un VFG.
2. $\mathbb{Z}[X]$ nav Eiklīda gredzens.

PIERĀDĪJUMS

1. Skatīt papildmateriālu.

2. Pierādīt patstāvīgi, ka neeksistē normas funkcija. ■

1.1.2. Skaitļu gredzenu iekļaušanas sekas

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \implies \mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X] \implies \forall\, f \in \mathbb{Z}[X]$ var uzskatīt par piederošu $\mathbb{Q}[X]$, $\mathbb{R}[X]$ vai $\mathbb{C}[X]$.

$f \in \mathbb{Q}[X] \implies \exists\, a \in \mathbb{Z} :\ af \in \mathbb{Z}[X]$ - a ir f koeficientu saucēju MKD daudzkārtnis.

Ja ir zināms polinoma sadalījums virs lielāka lauka, tad izmantojot viennozīmīgās faktorizācijas īpašību, var izdarīt atbilstošus secinājumus par polinoma faktorizāciju virs $\mathbb{Z}$.

Naivs algoritms polinoma faktorizācijai virs $\mathbb{Z}$ vai $\mathbb{Q}$:

1. sadalīt polinomu nedalāmos reizinātājos virs $\mathbb{R}$ vai $\mathbb{C}$;
2. mēģināt apvienot vairākus nedalāmus polinomus reizinājumos tā, lai $\forall$ reizinātājs ir virs $\mathbb{Z}$ vai $\mathbb{Q}$.

1.1. piemērs. $X^2 - 3 = \underbrace{(X - \sqrt{3})(X + \sqrt{3})}_{\in \mathbb{R}[X]} \in \mathcal{I}(\mathbb{Z}[X])$.

1.2. Faktorizācijas virs $\mathbb{Z}$ un $\mathbb{Q}$ ir ekvivalentas

$\mathbb{Z}$ gadījumā aizvietosim $\sim$ ar $= \pm$, jo $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.

1.2.1. Satura multiplikativitāte

1.2. teorēma. (*satura multiplikativitāte*) $f, g \in \mathbb{Z}[X]$. Tad

$$cont(fg) = \pm cont(f)cont(g).$$

PIERĀDĪJUMS

Reducēšana uz speciālgadījumu.

$$\begin{cases} f = cont(f)f_0 \\ g = cont(g)g_0 \end{cases} \Longrightarrow cont(fg) = \pm cont(f)cont(g)\underbrace{cont(f_0g_0)}_{?}$$

Pietiek pierādīt, ka primitīvu polinomu reizinājums ir primitīvs polinoms.

Speciālgadījums - f un g ir primitīvi polinomi, jāpierāda, ka fg ir primitīvs polinoms. Pierādījums no pretējā.

Ir doti polinomi $\begin{cases} f(X)=\sum_{i=0}^{n} a_i X^i, LKD(a_0,...,a_n)=1 \\ g(X)=\sum_{j=0}^{m} b_j X^j, LKD(b_0,...,b_m)=1. \end{cases}$

Pieņemsim, ka $cont(fg) \notin \{-1,1\} \implies \exists\, p \in \mathbb{P}:\ p|cont(fg) \implies$ p dala katru fg koeficientu.

Pieņemsim, ka

$$\begin{cases} k \text{ ir mazākais indekss, kuram } p \nmid a_k \\ l \text{ ir mazākais indekss, kuram } p \nmid b_l \end{cases}.$$

k, l eksistē, jo pretējā gadījumā visi f un g koeficieni dalītos ar p, un tie nebūtu primitīvi polinomi.

Apskatīsim koeficientu pie X^{k+l} reizinājumam fg, tas ir vienāds ar

$$\underbrace{\sum_{i=0}^{k+l} a_i b_{k+l-i}}_{\text{dalās ar } p} = \underbrace{(a_0 b_{k+l} + ... + a_{k-1} b_{l+1})}_{\text{dalās ar } p, \text{ jo } a_0,...,a_{k-1} \text{ dalās}} + a_k b_l + \underbrace{(a_{k+1} b_{l-1} + ... + a_{k+l} b_0)}_{\text{dalās ar } p, \text{ jo } b_0,...,b_{l-1} \text{ dalās}}.$$

$\implies p|a_k b_l$ - pretruna, jo $p|a_k$ vai $p|b_l$. ■

1.2.2. Galvenā teorēma

1.3. teorēma. $f \in \mathbb{Z}[X]$. $f \in \mathcal{I}(\mathbb{Z}[X]) \iff f \in \mathcal{I}(\mathbb{Q}[X])$.

PIERĀDĪJUMS

$\underline{f \in \mathcal{I}(\mathbb{Q}[X]) \implies f \in \mathcal{I}(\mathbb{Z}[X])}$ - acīmredzami, jo $\mathbb{Z} \subseteq \mathbb{Q}$.

$\underline{f \in \mathcal{I}(\mathbb{Z}[X]) \implies f \in \mathcal{I}(\mathbb{Q}[X])}$

Ja $f \in \mathcal{I}(\mathbb{Z}[X])$, tad pieņemsim, ka $f \notin \mathcal{I}(\mathbb{Q}[X])$:

$$f = gh, \text{ kur } g, h \in \mathbb{Q}[X].$$

$f \in \mathcal{I}(\mathbb{Z}[X]) \implies cont(f) = 1 (\in \mathbb{Z})$.

Reizināsim g un h ar atbilstošiem veseliem skaitļiem (kopsaucējiem) tā, lai tie pārvērstos par primitīviem polinomiem virs $\mathbb{Z}$:

- g reizinām ar tādu $n \in \mathbb{Z}$, lai $g_1 = ng \in \mathbb{Z}[X]$,
- g_1 izdalām ar $cont(g_1)$, iegūstam primitīvu polinomu

$$g_2 = \frac{1}{cont(g_1)} g_1 \in \mathbb{Z}[X],$$

- h reizinām ar tādu $m \in \mathbb{Z}$, lai $h_1 = mh \in \mathbb{Z}[X]$,
- h_1 izdalām ar $cont(h_1)$, iegūstam primitīvu polinomu $h_2 \in \mathbb{Z}[X]$.

Redzam, ka

$$g_2 h_2 = (...g)(...h) = \frac{\alpha}{\beta} gh = \frac{\alpha}{\beta} f, \text{ kur } \alpha, \beta \in \mathbb{Z} \Longrightarrow \alpha f = \beta g_2 h_2.$$

Izmantojot satura multiplikativitāti, redzam, ka

$$cont(\alpha f) = cont(\alpha) \cdot cont(f) = cont(\alpha) \cdot 1 = cont(\alpha) = cont(\beta g_2 h_2) = cont(\beta) \cdot cont(g_2) \cdot cont(h_2) = cont(\beta) \cdot 1 \cdot 1 = cont(\beta).$$

$\Longrightarrow$ $cont(\alpha) = \pm cont(\beta)$ $\Longrightarrow$ $\alpha = \pm\beta$ $\Longrightarrow$ $f = \pm g_2 h_2$ - pretruna, jo f ir nedalāms, bet $g_2, h_2 \in \mathbb{Z}[X]$. ■

1.2.3. Secinājumi attiecībā uz faktorizāciju

$f \in \mathbb{Z}[X]$ - faktorizācija virs $\mathbb{Q}$ ir tāda pati kā faktorizācija virs $\mathbb{Z}$, ja neskaita konstantos reizinātājus.

$f \in \mathbb{Q}[X]$ - iespējamie faktorizācijas algoritmi:

- var mēģināt faktorizēt f virs Q,
- var reizināt f ar $a \in \mathbb{Z}$: $af \in \mathbb{Z}[X]$, tad faktorizēt af virs $\mathbb{Z}$:

$$af = g_1 ... g_m \in \mathbb{Z}[X] \implies f = \frac{1}{a}(g_1 ... g_m) \in \mathbb{Q}[X].$$

1.3. Racionālās saknes tests

1.4. teorēma. (*Racionālās saknes tests*) $f(X) = \sum_{i=0}^{n} f_i X^i \in \mathbb{Z}[X]$, $LKD(r,s) = 1$, $r \neq 0$, $f\left(\frac{r}{s}\right) = 0$. Tad

1. $r | f_0$;
2. $s | f_n$.

PIERĀDĪJUMS Vienādību $f\left(\frac{r}{s}\right) = 0$ reizināsim ar s^n:

$$f_n \cdot \left(\frac{r}{s}\right)^n + f_{n-1} \cdot \left(\frac{r}{s}\right)^{n-1} + ... + f_1 \cdot \left(\frac{r}{s}\right) + f_0 = 0 \implies$$

$$\overbrace{\underbrace{f_n r^n + f_{n-1} r^{n-1} s + \ldots + f_1 r s^{n-1}}_{\equiv 0 (\mathrm{mod}\ s)} + f_0 s^n}^{\equiv 0 (\mathrm{mod}\ r)} = 0.$$

Apskatīsim redukcijas mod r un s. Redzam, ka

$$\begin{cases} f_0 s^n \equiv 0 (\mathrm{mod}\ r) \\ f_n r^n \equiv 0 (\mathrm{mod}\ s). \end{cases}$$

$$LKD(r,s) = 1 \Longrightarrow \begin{cases} r \in \mathcal{U}_s \\ s \in \mathcal{U}_r. \end{cases}$$

Tādējādi

$$\begin{cases} f_0 s^n \cdot (s^{-1})^n \equiv f_0 \equiv 0 \cdot (s^{-1})^n \equiv 0 (\mathrm{mod}\ r) \\ f_n r^n \cdot (r^{-1})^n \equiv f_n \equiv 0 \cdot (r^{-1})^n \equiv 0 (\mathrm{mod}\ s). \end{cases}$$ ■

1.2. piemērs. Mēģināsim faktorizēt $f = 2X^4 - 5X^3 + 6X^2 - 10X + 4$.

Ja r/s ir f sakne, tad $r|4$ un $s|2$.

Iespējamās racionālās saknes ir ± 4, ± 2, ± 1, $\pm 1/2$.

Ar tiešu pārbaudi atrodam, ka saknes ir 2 un 1/2.

Izdalot f ar $(X-\frac{1}{2})(X-2)$, iegūstam

$$f=(X-\frac{1}{2})(X-2)(2X^2+4)=(2X-1)(X-2)(X^2+2).$$

1.4. Factorizācija mod p un tās pielietojumi

1.4.1. Polinoma redukcija mod p

$p\in\mathbb{P}$, $f=\sum_{i=1}^{n}a_iX^i\in\mathbb{Z}[X]$. Par f redukciju mod p sauc polinomu

$$[f]_p=\sum_{i=1}^{n}[a_i]_pX^i\in\mathbb{F}_p[X],\ \text{kur } [a_i]_p \text{ ir } a_i \text{ redukcija mod } p.$$

1.3. piemērs. $f=X^3-3X^2+6X-1$.

$[f]_2=X^3+X^2+1$.

$[f]_3=X^3-1$.

$$\forall\, p:\ [(X+1)^p]_p = X^p + 1.$$

1.4.2. Galvenā teorēma

1.5. teorēma. $f, g \in \mathbb{Z}$. Tad

1. $[f+g]_p = [f]_p + [g]_p, \forall\, p \in \mathbb{P}$.
2. $[fg]_p = [f]_p[g]_p,\ \forall\, p \in \mathbb{P}$.

PIERĀDĪJUMS Seko no tā, ka redukcija mod p ir gredzenu homomorfisms $\mathbb{Z} \to \mathbb{F}_p$: $\begin{cases} [a+b] = [a] + [b] \\ \Big[ab] = [a][b]. \end{cases}$

$$[f+g]_p = \Big[\underbrace{\sum_{i=0}^{n} a_i X^i}_{=f} + \underbrace{\sum_{i=0}^{n} b_i X^i}_{=g} \Big]_p = \Big[\textstyle\sum_{i=1}^{n} (a_i + b_i) X^i \Big]_p =$$

$$= \textstyle\sum_{i=1}^{n} [a_i + b_i] X^i = \sum_{i=1}^{n} \Big([a_i] + [b_i] \Big) X^i =$$

$\sum_{i=1}^{n}[a_i]X^i + \sum_{i=1}^{n}[b_i]X^i = [f]_p + [g]_p.$

$$[fg]_p = \left[\sum_{i=0}^{n} a_i X^i \cdot \sum_{i=0}^{m} b_i X^i\right]_p = \left[\sum_{i,j=0}^{n,m}(a_i b_j)X^{i+j}\right]_p =$$
$$= \sum_{i,j=0}^{n,m}[a_i b_j]X^{i+j} = \sum_{i,j=0}^{n,m}[a_i][b_j]X^{i+j} =$$
$$\sum_{i,j=0}^{n,m}[a_i]X^i[b_j]X^j = \sum_{i=1}^{n}[a_i]X^i \sum_{j=1}^{n}[b_j]X^j = [f]_p[g]_p. \blacksquare$$

1.6. teorēma. $f \in \mathbb{Z}[X]$ ir normalizēts polinoms.

1. $f \notin \mathcal{I}(\mathbb{Z}[X]) \implies [f]_p \notin \mathcal{I}(\mathbb{F}_p[X]), \forall\, p \in \mathbb{P}.$
2. $\exists\, p: \ [f]_p \in \mathcal{I}(\mathbb{F}_p[X]) \implies f \in \mathcal{I}(\mathbb{Z}[X]).$

PIERĀDĪJUMS

1. Seko no iepriekšējās teorēmas:

$$f = gh \in \mathbb{Z}[\mathbb{X}] \implies [f]_p = [g]_p[h]_p \in \mathbb{F}_p[X], \forall\, p \in \mathbb{P}.$$

2. Kontrapozīcijas likums piemērots pirmajam apgalvojumam. $\blacksquare$

1.4. piemērs. $f = X^4 - 3X^3 + 6X^2 + 4X + 7$.

$p = 2$, $[f]_2 = X^4 + X + 1 \in \mathcal{I}(\mathbb{F}_2[X]) \implies f \in \mathcal{I}(\mathbb{Z}[X])$.

1.4.3. Eizenšteina kritērijs

1.7. teorēma. $f = \sum_{i=0}^{n} f_i X^i \in \mathbb{Z}[X]$, $\exists\, p \in \mathbb{P}$:

- $f_n \not\equiv 0 (\text{mod } p)$.
- $\forall\, l < n$: $f_l \equiv 0 (\text{mod } p)$,
- $f_0 \not\equiv 0 (\text{mod } p^2)$.

Tad $f \in \mathcal{I}(\mathbb{Z}[X])$.

PIERĀDĪJUMS Reducējot mod p, iegūsim, ka $[f]_p = X^n$.

$$f = gh \in \mathbb{Z}[X] \implies [f]_p = [g]_p [h]_p \in \mathbb{F}_p[X] \implies \begin{cases} [g]_p = X^j, \\ \left[h\right]_p = X^{n-j} \end{cases}$$

$$\Longrightarrow \begin{cases} g_0 \equiv 0(\mathrm{mod}\ p), \\ h_0 \equiv 0(\mathrm{mod}\ p), \end{cases} \Longrightarrow f_0 = g_0 h_0 \equiv 0(\mathrm{mod}\ p^2) \text{ - pretruna.}$$

■

1.5. piemērs. $X^4 - 3X^2 + 6X - 3 \in \mathcal{I}(\mathbb{Z}[X])$, jo visi koeficienti, izņemot vecāko, dalās ar $p = 3$, bet brīvais loceklis nedalās ar $3^2 = 9$.

Dažreiz var mēģināt izmantot argumenta lineāru substitūciju - nobīdi: $X^3 - 9X + 11 = (X-1)^3 + 3(X-1)^2 - 6(X-1) + 3$ - nedalāms, $p = 3$.

$X^2 - 8$ nedalāmību nevar pierādīt ar Eizenšteina kritēriju ne ar kādu nobīdi.

1.1. piezīme. Izmantojot Eizenšteina kritēriju, var pierādīt, ka $\mathbb{Z}[X]$ (un tātad arī $\mathbb{Q}[X]$) nedalāmu polinomu pakāpes nav ierobežotas. Piemēram, $\forall\ n$ polinoms $X^n + 2X + 2$ ir nedalāms.

1.5. Kronekera faktorizācijas algoritms

1.5.1. Ievads

Kronekera algoritms ir algoritms, ar kura palīdzību var faktorizēt polinomus virs $\mathbb{Z}[X]$, un tātad arī virs $\mathbb{Q}[X]$.

Tas ir *rupja spēka* jeb *izsmeļošās pārlases* tipa algoritms - tiek noteikta galīga kopa, kuras visus elementus pārskatot, tiek atrisināts uzdevums.

Atzīmēsim šādus faktus:

- $f \in \mathbb{Z}[X]$, $\deg f = n$ ir dalāms $\Longrightarrow$ $\exists$ f dalītājs g : $\deg g \leq l = [\frac{n}{2}]$ - *meklēsim šādu f dalītāju g,*
- $\deg g \leq l \Longrightarrow$ g ir viennozīmīgi noteikts ar savām vērtībām $l+1$ punktos, šādu polinomu var atrast ar Lagranža interpolācijas formulas palīdzību - *pietiek zināt g vērtības $l+1$ punktos,*
- $f = gh \Longrightarrow g(c)|f(c)\ \forall\ c \in \mathbb{Z}$ - *izvēlēsimies $l+1$ c vērtības un pārbaudīsim visus $f(c)$ dalītājus kā iespējamās $g(c)$ vērtības.*

1.5.2. Algoritms

$f \in \mathbb{Z}[X]$, $\deg(f) = n$. Apzīmēsim $[\frac{n}{2}]$ ar l.

1. Izvēlēsimies $l+1$ veselu punktu virkni $\mathcal{C} = (c_0, ..., c_l)$, piemēram, $(0, 1, ..., l)$ vai $(0, \pm 1, \pm 2, ...)$ (lai atvieglotu skaitļošanu, vēlams izvēlēties pēc iespējas mazākus skaitļus).
2. Ja kādam i izpildās $f(c_i) = 0$ (nejauši trāpījām uz f saknes), tad izdalām f ar $X - c_i$ un atgriežamies uz soli 1 ar polinomu $f/(X - c_i)$.
3. Atradīsim virkni $f(\mathcal{C}) = (f(c_0), ..., f(c_l))$ (vēlams panākt, lai $f(\mathcal{C})$ elementi ir mazi un tiem ir maz dalītāju).
4. Pēctecīgi apskatīsim visas virknes $\mathcal{D} = (d_0, ..., d_l)$, kur $d_i | f(c_i)$:
   (a) ar Lagranža interpolācijas formulas palīdzību konstruēsim polinomu $g_{\mathcal{D}}$, kuram izpildās nosacījums

$$g_{\mathcal{D}}(c_i) = d_i, \forall i : 0 \leq i \leq l,$$

(b) ja $\begin{cases} g_{\mathcal{D}} \in \mathbb{Z}[X] \\ \deg g_{\mathcal{D}} > 0 \\ g_{\mathcal{D}} | f \text{ virs } \mathbb{Z} \end{cases} \Longrightarrow$ atkārtoti pielietojam Kronekera algoritmu polinomiem $g_{\mathcal{D}}$ un $f/g_{\mathcal{D}}$,

(c) ja $g_{\mathcal{D}} \notin \mathbb{Z}[X]$ vai $g_{\mathcal{D}} \nmid f$ virs $\mathbb{Z}$, tad pārejam uz nākamo virkni $\mathcal{D}$.

5. Ja pēc visu virkņu $\mathcal{D}$ apskatīšanas nav atrasts neviens f dalītājs, tad f ir nedalāms.

1.6. piemērs. Faktorizēsim virs $\mathbb{Z}$ polinomu

$$f = X^4 - 4X^3 + 3X^2 + 2X - 1.$$

Ja tas ir dalāms, tad tam eksistē dalītājs, kura pakāpe nepārsniedz 2.

Izvēlēsimies 3 punktu virkni $\mathcal{C} = (0, 1, 2)$.

Atradīsim $f(\mathcal{C}) = (-1, 1, -1)$.

Jāapskata 8 virknes, jo $\forall$ virknes $f(\mathcal{C})$ elementam ir 2 veseli dalītāji: $(1, 1, 1,)$, $(1, 1, -1)$, $(1, -1, 1)$, $(1, -1, -1,)$, $(-1, 1, 1,)$, $(-1, 1, -1)$, $(-1, -1, 1)$, $(-1, -1, -1)$.

1. $\mathcal{D} = (1, 1, 1)$, šajā gadījumā polinoms ir konstants.
2. $\mathcal{D} = (1, 1, -1)$,

$$f_{\mathcal{D}} = 1 \cdot \frac{(X-1)(X-2)}{(0-1)(0-2)} +$$

$$1 \cdot \frac{(X-0)(X-2)}{(1-0)(1-2)} + (-1) \cdot \frac{(X-0)(X-1)}{(2-0)(2-1)} = -X^2 + X + 1.$$

$f/f_{\mathcal{D}} = -X^2 + 3X - 1$. Pārbaudot kvadrātvienādojumu saknes, redzam, ka $-X^2 + X + 1$ un $-X^2 + 3X - 1$ ir nedalāmi virs $\mathbb{Z}$, tāpēc uzdevums ir atrisināts un

$$f = (X^2 - X - 1)(X^2 - 3X + 1).$$

2. 5.mājasdarbs

2.1. Obligātie uzdevumi

5.1 $f \in \mathbb{Q}[X]$ ir nedalāms. Pierādīt, ka vienādojumam

$$f(z) = 0$$

nav vairākkārtīgu saķņu laukā $\mathbb{C}$. (*Norādījums: izmantojiet kvadrātbrīvās faktorizācijas formulu, pierādiet, ka* $LKD(f, f') = 1$).

5.2 Faktorizēt polinomus virs $\mathbb{Q}$ izmantojot racionālo saķņu testu.

(a) $3X^2 - 5X - 2$;
(b) $24X^3 + 14X^2 - 7X - 3$;
(c) $72X^4 + 102X^3 - 37X^2 - 48X - 9$.

5.3 Izmantojot Kronekera algoritmu sadalīt polinomus nedalāmajos reizinātājos virs $\mathbb{Z}$:

(a) $2X^4 - 13X^3 + 25X^2 - 14X + 2$,
(b) $X^6 - 9X^5 + 29X^4 - 39X^3 + 17X^2 + 3X - 1$.

5.4 Pierādiet, ka dotie polinomi ir nedalāmi virs $\mathbb{Z}$:
(a) $X^3 - 2X^2 + 4X - 4 \pmod 3$,
(b) $X^4 - 10X^3 + 6X^2 - 12X + 6$ (Eizenšteina kritērijs),
(c) $X^3 - X^2 - 3X + 5$ (Eizenšteina kritērijs ar nelielu nobīdi),
(d) $X^{15} - 9$ (*Norādījums: izpētiet iespējamo dalītāju koeficientus mod* 3 *un* 9).

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

5.5 (2010.g.Sanktpēterburgas Universitātes studentu konkurss, http://www.mathsoc.spb.ru/konkurs/index.html) $a, b \in \mathbb{Z}$ apmierina sakarību $a^2+ab+b^2 \equiv 0 (\mathrm{mod}\ p)$, $p \in \mathbb{P}$, $p > 3$. Pierādīt, ka $f(a,b) = (a+b)^p - a^p - b^p \equiv 0 (\mathrm{mod}\ p^3)$. (*Norādījums: pierādiet, ka* $f(a,b)$ *dalās ar* a^2+ab+b^2, *ja* $p-1 \not\equiv 0 (mod\ 3)$ *un dalās ar* $(a^2+ab+b^2)^2$, *ja* $p-1 \equiv 0 (mod\ 3)$).

5.6 Atrodiet visus polinomus $f \in \mathbb{C}[X]$, kas apmierina funkcionālo vienādojumu

$$f(X^2) + f(X)f(X+1) = 0.$$

(*Norādījums: izmantojiet* $\mathbb{C}[X]$ *VFG īpašību, meklējiet* f *formā*

$$f = a(X - c_1)...(X - c_m),$$

apskatīt gadījumus $c = 0$, $c = 1$ *u.t.t.*)

5.7 Nosakiet, vai zemāk dotie polinomi ir dalāmi:

(a) $X^n \pm X \pm 1 \in \mathbb{Z}[X]$,
(b) $X^n + tX \pm 1 \in \mathbb{Z}[X]$, ja $|t| \geq 3$,
(c) $X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Z}[X]$, kur $p \in \mathbb{P}$.

5.8 $a_1, ..., a_n$ - dažādi veseli skaitļi. Noskaidrot, vai zemāk dotie polinomi ir dalāmi.

(a) $(X - a_1)...(X - a_n) - 1$;
(b) $(X - a_1)...(X - a_n) + 1$;
(c) $(X - a_1)^2...(X - a_n)^2 + 1$.

5.9 Izpētīt, kādiem $f \in \mathcal{I}(\mathbb{Z}[X])$ $\exists\, p \in \mathbb{P}$: f nedalāmību var pierādīt ar nobīdīto Eizenšteina kritēriju mod p (veikt substitūciju $X = Y + t$ un sekmīgi pielietot Eizenšteina kritēriju mod p polinomam $\tilde{f}(Y) = f(Y + t)$).