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

Studiju kurss

Polinomu algebra

2.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

Lekcijas mērķis - vispārināt dalāmības, pirmskaitļu, LKD, MKD, Eiklīda algoritma jēdzienus patvaļīgu gredzenu un polinomu gredzenu gadījumā.

1. Factorizācija patvaļīgos gredzenos

1.1. Pamatfakti

Šajā lekcijā visi gredzeni ir komutatīvi, integrāli, ar vieninieku.

Teiksim, ka $b \in R$ dalās ar $a \in R$ $(b|a)$, ja eksistē $c \in R$ tāds, ka $a = bc$.

Ja $b|a$ un $a|b$, tad a un b sauksim par *asociētiem elementiem*, apzīmēsim ar $a \sim b$. Šajā gadījumā

$$a = cb = (cc')a,$$

tāpēc $a = cb$, kur $c \in U(R)$.

1.1. piezīme. Ja a ir neinvertējams un u ir invertējams, tad ua ir neinvertējams. Pretējā gadījumā eksistē x tāds, ka $x \cdot ua = 1$. Seko, ka $(xu)a = 1$ - a ir invertējams - pretruna.

1.1. teorēma.

1. Ja gredzena R elementiem $a, b_1, ..., b_n$ izpildās nosacījumi
$$a|b_1,\ a|b_2,\ ...,\ a|b_n,$$
tad
$$a|(b_1 + ... + b_n).$$
.
2. Ja $a|b$ un $b|c$, tad $a|c$.
3. Ja $a|b$, tad katram $c \in R$ izpildās $a|bc$.
4. Ja $a|b$ un $c|d$, tad $ac|bd$.

PIERĀDĪJUMS Pierādām līdzīgi veselo skaitļu gredzena gadījumam. Patstāvīgs darbs. ■

Nenulles elementu $p \in R$ sauksim par *nedalāmu (irreduciblu)*, ja p nav invertējams un to nevar izteikt formā

$$p = ab,$$

kur a un b ir neinvertējami elementi.

Gredzena $R[X]$ nedalāmos elementus sauc par *nedalāmiem (irreducibliem) polinomiem*.

Elementu $p \in R$ sauksim par *pirmelementu*, ja no tā ka $p|ab$ seko, ka $p|a$ vai $p|b$.

1.2. piezīme. Integrālā gredzenā pirmelementi ir nedalāmi. Pierādījums no pretējā. Ja $p = ab$, tad ja $p|a$, tad $a = ab \cdot q$. Saīsinot ar a iegūsim, ka b ir invertējams.

1.3. piezīme. Ja p ir nedalāms, tad up, kur u ir invertējams, arī ir nedalāms. Pretējā gadījumā $up = p_1p_2$ un $p = (u^{-1}p_1)p_2$ - pretruna.

1.1. piemērs. Laukā nav nedalāmu elementu.

Gredzena $\mathbb{Z}$ nedalāmie elementi ir pirmskaitļi ar pozitīvām un negatīvām zīmēm.

Lineāri polinomi (ar pakāpi 1) ir nedalāmi, tas seko no īpašības $deg(fg) = deg(f) + deg(g)$.

Teiksim, ka gredzens R ir *viennozīmīgas faktorizācijas gredzens (VFG, faktoriāls gredzens, unique factorization domain)*, ja katrs $a \in R$, $a \neq 0$, ir izsakāms formā

$$a = up_1p_2...p_k,$$

kur $u \in U(R)$, p_i ir nedalāmi elementi un šāds sadalījums ir noteikts viennozīmīgi ar precizitāti līdz elementu kārtībai un aizvietošanai ar asociētiem elementiem. Citiem vārdiem sakot, ja

$$a = up_1p_2...p_k = u'p'_1p'_2...p'_m,$$

tad $k = m$ un pēc elementu p'_i pārkārtošanas katram i eksistē $u_i \in U(R)$ tāds, ka $p_i = u_ip'_i$.

1.2. piemērs. Jebkurš lauks ir VFG.

$\mathbb{Z}$, Gausa un Eizenšteina skaitļu gredzeni ir VFG.

1.3. piemērs. Gredzenā $\mathbb{Z}[\sqrt{-5}]$ elements 6 ir izsakāms pirmelementu reizinājumā divos dažādos veidos

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Var pierādīt, ka sadalījumos ir neasociēti pirmelementi.

1.2. Viennozīmīgas faktorizācijas kritērijs

1.2. teorēma. Dots, ka gredzenā R katrs neinvertējams nenulles elements ir izsakāms kā nedalāmu elementu reizinājums. R ir VFG tad un tikai tad, ja katram nedalāmam elementam p no tā, ka $p|ab$ seko, ka $p|a$ vai $p|b$ (katrs nedalāms elements ir pirmelements).

PIERĀDĪJUMS

Ja R ir VFG, tad katram p no $p|ab$ seko, ka $p|a$ vai $p|b$.

Ja $p|ab$, tad $ab = cp$. Ja R ir VFG, tad

$$ab = \underbrace{p_1 p_2 ... p_k}_{a} \underbrace{p_{k+1} ... p_n}_{b} = \underbrace{(p_1' p_2' ... p_l')}_{c} p.$$

No viennozīmīgās faktorizācijas īpašības seko, ka p ir asociēts ar vienu no nedalāmajiem elementiem $p_1, p_2, ..., p_n$, tātad $p|a$ vai $p|b$.

Ja katram p no $p|ab$ seko, ka $p|a$ vai $p|b$, tad R ir VFG.

Izmantosim matemātisko indukciju pēc nedalāmo elementu skaita faktorizācijā.

Indukcijas bāze. Ja elements r ir nedalāms, tad to nevar izteikts kā divu vai vairāku nedalāmu reizinājumu un $r = u(u^{-1}r)$, tāpēc apgalvojums ir spēkā.

Indukcijas solis. Pieņemsim, ka apgalvojums ir spēkā visiem R elementiem, kurus var izteikt ne vairāk kā $n-1$ nedalāmu elementu reizinājuma veidā un pierādīsim, ka tad apgalvojums ir spēkā elementiem, kurus var izteikt n nedalāmu elementu reizinājuma viedā.

Pieņemsim, ka elements $r \in R$ ir izsakāms kā n nedalāmu elementu reizinājums:

$$r = p_1 p_2 ... p_n.$$

Pieņemsim, ka r var izteikt kā nedalāmu elementu reizinājumu divos veidos:

$$r = p_1 p_2 ... p_n = p'_1 p'_2 ... p'_l.$$

Redzam, ka $p_n | r$, tātad p_n dala vismaz vienu no nedalāmajiem elementiem $p'_1, p'_2, ..., p'_l$, pieņemsim, ka $p_n | p'_l$.

Seko, ka $p'_l = up_n$, kur u ir invertējams, jo p'_l ir nedalāms.

Izmantojot saīsināšanas īpašību integrālajos gredzenos, saīsinām ar p_n abas puses. Iegūstam vienādību

$$p_1 p_2 ... p_{n-1} = up'_1 p'_2 ... p'_{l-1}.$$

Kreisajā pusē ir elements, kas ir $n-1$ nedalāmu elementu reizinājums, tātad saskaņā ar indukcijas pieņēmumu, labajā pusē ir $n-1$ nedalāmi elementi, kas ir asociēti ar $p_1, .., p_{n-1}$.

Tātad p_n ir asociēts ar p'_l, $n = l$, kopas $\{p_1, ..., p_{n-1}\}$ elementi ir asociēti ar kopas $\{p'_1, ..., p'_{n-1}\}$ elementiem. Apvienojot šos divus apgalvojumus, redzam, ka kopas $\{p_1, ..., p_n\}$ elementi ir asociēti ar kopas $\{p'_1, ..., p'_n\}$ elementiem.

Seko, ka r sadalījums nedalāmu elementu reizinājumā ir noteikts viennozīmīgi atbilstoši VFG definīcijai. ■

2. LKD un MKD patvaļīgos gredzenos

2.1. Pamatfakti

2.1.1. LKD definīcija

Elementu $a \in R$ sauksim par elementu kopas $\{b_1, ..., b_m\} \subseteq R$ *kopīgu dalītāju*, ja katram i izpildās nosacījums $a|b_i$. Apzīmēsim kopas $b_1, ..., b_n$ dalītāju kopu ar $D(b_1, ..., b_n)$. Acīmredzami

$$D(b_1, ..., b_n) = \bigcap_{i=1}^{n} D(b_i).$$

Par kopas $\{b_1, ..., b_m\}$ *lielāko kopīgo dalītāju (LKD)* sauksim to kopīgo dalītāju, kurš dalās ar jebkuru šīs kopas kopīgo dalītāju. Citiem vārdiem sakot, d ir lielākais kopīgais dalītājs, ja

1. katram i izpildās $d|b_i$,
2. ja d' ir tāds, ja katram i izpildās $d'|b_i$, tad $d'|d$.

2.1. piezīme. Var redzēt, ka LKD ir noteikts ar precizitāti līdz asociācijai. Ja $d = LKD(a, b)$, tad $d_1 = ud$, kur u ir invertējams elements arī ir a un b lielākais kopīgais dalītājs.

Var izmainīt LKD definīciju tā, lai tas būtu viennozīmīgi noteikts. Piemēram, polinomu gredzenu gadījumā var pieprasīt, lai vecākais koeficients būtu vienāds ar 1.

Gredzena elementu kopu $\{b_1, ..., b_n\}$ sauksim par *savstarpēji primitīviem elementiem*, ja $LKD(b_1, ...b_n) = 1$.

2.1.2. MKD definīcija

Elementu c sauksim par gredzena elementu kopas $\{b_1, ..., b_m\}$ *kopīgu daudzkārtni*, ja katram i izpildās nosacījums $b_i|c$. Apzīmēsim kopas $b_1, ..., b_n$ daudzkārtņu kopu ar $M(b_1, ..., b_n)$. Acīmredzami

$$M(b_1, ..., b_n) = \bigcap_{i=1}^{n} M(b_i).$$

Par kopas $\{b_1, ..., b_m\}$ *mazāko kopīgo daudzkārtni (MKD)* sauksim to kopīgo daudzkārtni, kurš dala jebkuru šīs kopas kopīgo daudzkārtni. Citiem vārdiem sakot, c ir mazākais kopīgais daudzkārtnis, ja

1. katram i izpildās $b_i|c$,
2. ja c' ir tāds, ja katram i izpildās $b_i|c'$, tad $c|c'$.

2.1.3. LKD un MKD īpašības

2.1. teorēma. (LKD un MKD īpašības patvaļīgos integrālos gredzenos) Ja integrālā gredzenā R eksistē LKD un MKD, tad ir spēkā šādi apgalvojumi.

1. $LKD(a, 0) = a$.
2. $LKD(c \cdot a, c \cdot b) = c \cdot LKD(a, b)$.
3. $LKD(a, b) = a$ tad un tikai tad, ja $a|b$.
4. $LKD(LKD(a, b), c) = LKD(a, LKD(b, c))$.
5. $MKD(a, b) = 0$ tad un tikai tad, ja $ab = 0$.

PIERĀDĪJUMS Pierāda līdzīgi veselo skaitļu gadījumam.■

2.2. LKD un MKD atrašana izmantojot faktorizāciju

Pieņemsim, ka R ir VFG. Fiksēsim pirmelementu kopas apakškopu $\mathcal{P}$ tādu, ka katrs R pirmelements ir asociēts ar kādu kopas $\mathcal{P}$ elementu.

2.1. piemērs. Ja $R = \mathbb{Z}$, tad $\mathcal{P}$ ir (pozitīvo) pirmskaitļu kopa.

2.2. teorēma. Ja ir doti divi VFG R elementi a un b, un

$$a = up_1^{\alpha_1}...p_k^{\alpha_k},$$
$$b = vp_1^{\beta_1}...p_k^{\beta_k},$$

tad

$$LKD(a,b) = p_1^{\delta_1}...p_k^{\delta_k},$$
$$MKD(a,b) = p_1^{\lambda_1}...p_k^{\lambda_k},$$

kur

$$\delta_i = \min(\alpha_i, \beta_i),$$
$$\lambda_i = \max(\alpha_i, \beta_i).$$

PIERĀDĪJUMS Pierāda līdzīgi veselo skaitļu gadījumam.■

3. Eiklīda gredzeni

3.1. Definīcija

Integrālu gredzenu R sauksim par *Eiklīda gredzenu*, ja var definēt *normas funkciju*

$$\mathbf{N} : R\backslash\{0\} \to \mathbb{N} \cup \{0\},$$

kas apmierina šādu nosacījumu: visiem $a, b \in R$, $b \neq 0$ eksistē $q, r \in R$ tādi, ka

- $a = qb + r$,
- $\mathbf{N}(r) < \mathbf{N}(b)$ vai $r = 0$,
- $\mathbf{N}(ab) \geq \mathbf{N}(a)$ visiem $a, b \neq 0$.

3.1. piemērs. Ja $R = \mathbb{Z}$, tad $\mathbf{N}(a) = |a|$ vai $\mathbf{N}(a) = |a|^2$.
Ja $R = S[X]$, tad $\mathbf{N}(a) = deg(a)$.
Ja $R = \mathbb{Z}[i]$, tad $\mathbf{N}(a) = |a|^2$.

3.2. Eiklīda algoritms Eiklīda gredzenos

Pieņemsim, ka R ir Eiklīda gredzens ar normas funkciju $\mathbf{N}$.

3.2.1. Algoritms

Ir uzdoti divi nenulles elementi a un b,$b \nmid a$.

1. Dalām a ar b:

$$a = q_1 b + r_1,$$
$$\mathbf{N}(r_1) < \mathbf{N}(b) \text{ vai } r_1 = 0.$$

Ja $r_1 = 0$, tad apstājamies, ja nē, tad pārejam uz soli 2.

2. Dalām b ar r_1:

$$b = q_2 r_1 + r_2,$$
$$\mathbf{N}(r_2) < \mathbf{N}(r_1) \text{ vai } r_2 = 0.$$

Ja $r_2 = 0$, tad apstājamies, ja nē, tad ejam uz soli 3.

3. Dalām r_1 ar r_2:

$$r_1 = q_3 r_2 + r_3,$$
$$\mathbf{N}(r_3) < \mathbf{N}(r_2) \text{ vai } r_3 = 0.$$

Ja $r_3 = 0$, tad apstājamies, ja nē, tad ejam uz soli 4.

.....

i. Dalām r_{i-2} ar r_{i-1}:

$$r_{i-2} = q_i r_{i-1} + r_i,$$
$$\mathbf{N}(r_i) < \mathbf{N}(r_{i-1}) \text{ vai } r_i = 0.$$

Ja $r_i = 0$, tad apstājamies, ja nē, tad ejam uz soli $i + 1$.

Virkne $\mathbf{N}(r_1), \mathbf{N}(r_2), \ldots$ ir stingri dilstoša virkne, tāpēc šī algoritma realizācijā soļu skaits ir galīgs.

3.2. piemērs. $R = \mathbb{Q}[X]$. $a = X^3 - 5X + 2$, $b = X^2 - X - 2$.

1. $a = (X + 1)b + (-2X + 4)$,
2. $b = (-\frac{1}{2}X - \frac{1}{2})(-2X + 4) + 0$.

$R = \mathbb{F}_2[X]$. $a = X^5 + X^4 + 1$, $b = X^3 + 1$.

1. $a = (X^2 + 1)b + X$,
2. $b = X \cdot X + 1$,
3. $X = X \cdot 1 + 0$.

3.2.2. Eiklīda algoritma saistība ar LKD

3.1. teorēma. Pēdējais nenulles atlikums Eiklīda algoritma realizācijā ar sākuma datiem (a, b) ir vienāds ar $LKD(a, b)$.

PIERĀDĪJUMS Pieņemsim, ka Eiklīda algoritma realizācijas pēdējais solis ir solis ar numuru n. Izteiksim iegūtos atlikumus, izmantojot algoritma soļu rezultātus. Viegli redzēt, ka

$$r_1 = a - q_1 b,$$
$$r_2 = b - q_2 r_1,$$
$$\ldots,$$
$$r_{n-3} = r_{n-1} - q_{n-1} r_{n-2},$$
$$r_{n-2} = q_n r_{n-1}.$$

Pēctecīgi aplūkojot šīs vienādības sākot no pēdējās iegūstam, ka iegūstam, ka $r_{n-1}|r_{n-2}$, $r_{n-1}|r_{n-3}$, ..., $r_{n-1}|b$, $r_{n-1}|a$, tātad r_{n-1} ir skaitļu a un b kopīgais dalītājs. Vēl ir jāpierāda, ka r_{n-1} ir lielākais kopīgais dalītājs.

Ja skaitlis c ir patvaļīgs elementu a un b kopīgais dalītājs, tad

1. no vienādības $r_1 = a - q_1 b$ seko, ka $c|r_1$,
2. no vienādības $r_2 = b - q_2 r_1$ seko, ka $c|r_2$,

   ...,

n. no vienādības $r_{n-2} = q_n r_{n-1}$ seko, ka $c|r_{n-1}$.

Tātad $r_{n-1} = LKD(a, b)$.■

3.3. piemērs. $R = \mathbb{Q}[X]$. $a = X^3 - 5X + 2$, $b = X^2 - X - 2$.

Redzam, ka $LKD(a, b) = -2X + 4$ vai jebkurš polinoms, kas ir asociēts ar to, piemēram, $X - 2$.

$R = \mathbb{F}_2[X]$. $a = X^5 + X^4 + 1$, $b = X^3 + 1$.

Redzam, ka $LKD(a, b) = 1$.

3.2. teorēma. Eiklīda gredzenā eksistē LKD.

3.2.3. *LKD* izteikšana lineāras kombinācijas veidā

3.3. teorēma. Katram Eiklīda gredzena elementu pārim (a, b) eksistē elementu pāris pāris (x, y) tāds, ka $LKD(a, b) = xa + yb$ ($LKD(a, b)$ ir a un b *lineāra kombinācija*.)

PIERĀDĪJUMS Realizēsim R elementiem a un b Eiklīda algoritmu. Pēctecīgi apskatīsim dalīšanas vienādības:

1. no vienādības $r_1 = a - q_1 b$ seko, ka r_1 ir a un b lineāra kombinācija,
2. no vienādības $r_2 = b - q_2 r_1$ seko, ka r_2 ir b un r_1 un tādējādi arī b un a lineāra kombinācija,

   ...,

n-1. no vienādības $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$ seko, ka r_{n-1} ir r_{n-3} un r_{n-2} un tādējādi arī b un a lineāra kombinācija.

■

3.4. piemērs. $R = \mathbb{Q}[X]$. $a = X^3 - 5X + 2$, $b = X^2 - X - 2$.

1. $a = (X + 1)b + (-2X + 4)$,
2. $b = (-\frac{1}{2}X - \frac{1}{2})(-2X + 4) + 0$.

Redzam, ka $LKD(a, b) = -2X + 4$ un no pirmā soļa seko, ka

$$-2X + 4 = 1 \cdot a - (X + 1)b$$

vai

$$X - 2 = (-\frac{1}{2}) \cdot a + (-\frac{X + 1}{2})b$$

$R = \mathbb{F}_2[X]$. $a = X^5 + X^4 + 1$, $b = X^3 + 1$.

1. $a = (X^2 + 1)b + X$,
2. $b = X \cdot X + 1$,
3. $X = X \cdot 1 + 0$.

Redzam, ka $LKD(a, b) = 1$, no otrās soļa seko, ka

$$1 = b + X \cdot X,$$

izsakot X no pirmā soļa, iegūsim

$$1 = b + X \cdot X = b + X(a + (X^2 + 1)b) = X \cdot a + (X^3 + X + 1)b.$$

3.3. Faktorizācija Eiklīda gredzenos

3.4. teorēma. Ja Eiklīda gredzenā $a|bc$ un $LKD(a,b)=1$, tad $a|c$.

PIERĀDĪJUMS Zinām, ka $1=xa+yb$, reizinot abas puses ar c, iegūsim $c=cxa+cyb=a(cx+y)$, tātad $a|c$.

■

3.5. teorēma. Eiklīda gredzenā katrs nenulles elements ir izsakāms nedalāmu elementu reizinājuma veidā.

PIERĀDĪJUMS

1.solis

Pierādīsim palīgapgalvojumu (lemmu): ja $a=bc$, kur b,c ir nedalāmi, tad $\mathbf{N}(a)>\mathbf{N}(b)$.

No normas definīcijas seko, ka $\mathbf{N}(a)\geq\mathbf{N}(b)$. Pieņemsim, ka $\mathbf{N}(a)=\mathbf{N}(b)$. Izdalīsim b ar a:

$$b=qa+r,$$

kur $r = 0$ vai $\mathbf{N}(a) > \mathbf{N}(r)$.

Ja $r = 0$, tad $b = qa$, bet $a = bc = a(qc)$, $1 = qc$ un c ir invertējams - pretruna. Tātad $\mathbf{N}(a) > \mathbf{N}(r)$.

Redzam, ka

$$\mathbf{N}(a) = \mathbf{N}(b) \leq \mathbf{N}(b(1-qc)) = \mathbf{N}(b-bqc) = \mathbf{N}(b-qa) = \mathbf{N}(r) < \mathbf{N}(a).$$

Esam ieguvuši pretrunu, tāpēc $\mathbf{N}(a) > \mathbf{N}(b)$.

2.solis

Ja a ir izsakāms formā $a = b_1...b_k$, kur katram i elements ir b_i ir neinvertējams, tad

$$\mathbf{N}(a) = \mathbf{N}(b_1...b_k) > \mathbf{N}(b_1...b_{k-1}) > ... > \mathbf{N}(b_1)$$

Esam ieguvuši dilstošu nenegatīvu skaitļu virkni, kuras garums nepārsniedz $\mathbf{N}(a)$.

Elementam a apskatīsim sadalījumu ar garāko iespējamo dilstošo

virkni. Tas ir sadalījums ar nedalāmiem elementiem, jo pretējā gadījumā virkni varētu padarīt garāku.

■

3.6. teorēma. Eiklīda gredzens ir VFG.

PIERĀDĪJUMS Jāpierāda, ka Eiklīda gredzenā katrs nedalāms elements ir pirmelements: ja p ir nedalāms elements un $p|ab$, tad $p|a$ vai $p|b$.

Pieņemsim, ka $ab \neq 0$. Definēsim $d = LKD(a, p)$. Tā kā $d|p$, tad $d|1$ vai $d \sim p$.

Ja $d|1$, tad $d = xa + yp$ un $1 = x'a + y'p$, tātad $LKD(p, a) = 1$. Saskaņā ar iepriekšēju teorēmu seko, ka $p|b$.

Ja $d \sim p$, tad $d = up$ un $up|a$, tātad $p|a$.

■

3.7. teorēma. Katram laukam k gredzens $k[X]$ ir VFG.

PIERĀDĪJUMS $k[X]$ ir Eiklīda gredzens ar normu $\mathbf{N}(f) = deg(f)$.

■

4. 2.mājasdarbs

4.1. Obligātie uzdevumi

2.1 Pierādiet, ka bezgalīgā gredzenā nevar būt galīgs skaits neinvertējamu elementu.

2.2 Pierādiet, ka gredzenā $R[X]$ polinomi ar pakāpi 0 dala visus polinomus.

2.3 Atrodiet polinomu $f(X)$ un $g(X)$ LKD un izsakiet to polinomu lineāras kombinācijas veidā:

(a) $f(X) = X^3 - X^2 - 3X + 3$, $g(X) = X^2 - 1$, virs $\mathbb{Q}[X]$,
(b) $f(X) = X^4 + 2$, $g(X) = 2X^2 - 1$, virs $\mathbb{Q}[X]$,
(c) $f(X) = X + 1$, $g(X) = X^4 + X^3 + X^2 + 1$, virs $\mathbb{F}_2[X]$.

2.4 Dotajiem polinomiem f un g virs $\mathbb{Q}[X]$ atrodiet tadus polinomus a un b, lai izpildītos vienādība $a(X)f(X) + b(X)g(X) = 1$:

(a) $f(X) = x^3$, $g(X) = (1 - X)^3$,
(b) $f(X) = x^2$, $g(X) = (1 - X)^4$.

4.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

2.5 Vai $k[[X]]$, kur k ir lauks, ir Eiklīda gredzens?

2.6 Visiem naturāliem n un m polinomiem $f(X) = X^n$ un $g(X) = (1-X)^m$ virs $\mathbb{Q}[X]$ atrodiet tadus polinomus a un b, lai izpildītos vienādība $a(X)f(X) + b(X)g(X) = 1$.