KAUNO TECHNOLOGIJOS UNIVERSITETAS

FUNDAMENTALIŲJŲ MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

ANDRIUS ALEKNA

MATRICINĖS LYGČIŲ SISTEMOS SPRENDINIŲ PAIEŠKA

Magistro darbas

Vadovas
prof. dr. Eligijus Sakalauskas

KAUNAS, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS

FUNDAMENTALIŲJŲ MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

TVIRTINU
Katedros vedėjas
doc. dr. N. Listopadskis
2011 06 02

MATRICINĖS LYGČIŲ SISTEMOS SPRENDINIŲ PAIEŠKA

Taikomosios matematikos magistro baigiamasis darbas

Vadovas
prof. dr. Eligijus Sakalauskas
2011 06 02

Recenzentas
doc.dr. K. Plukas
2011 06 02

Atliko
FMMM 9 gr. stud.
A. Alekna
2011 06 02

KAUNAS, 2011

KVALIFIKACINĖ KOMISIJA

Pirmininkas: Leonas Saulis, profesorius (VGTU)

Sekretorius: Eimutis Valakevičius, docentas (KTU)

Nariai: Algimantas Jonas Aksomaitis, profesorius (KTU)

Vytautas Janilionis, docentas (KTU)

Vidmantas Povilas Pekarskas, profesorius (KTU)

Rimantas Rudzkis, habil. dr., vyriausiasis analitikas (DnB NORD Bankas)

Zenonas Navickas, profesorius (KTU)

Arūnas Barauskas, dr., vice-prezidentas projektams (UAB „Baltic Amadeus“)

Alekna A. Matricinės lygčių sistemos sprendinių paieška: Taikomosios matematikos magistro baigiamsis darbas/vadovas prof. dr. E. Sakalauskas; Taikomosios matematikos katedra, Fundamentaliųjų mokslų fakultetas, Kauno technologijos universitetas. – Kaunas, 2011. – 44 p.

SANTRAUKA

Rakto apsikeitimo protokolo, kaip ir bet kurio asimetrinės kriptografijos algoritmo, pagrindas yra vienkryptės funkcijos, kurias paprasta apskaičiuoti, tačiau apskaičiuoti atvirkštinę jų reikšmę per priimtiną laiko tarpą neįmanoma. Darbe bus bandoma įrodyti, kad tiriamoji lygčių sistema turi mažai sprendinių ir yra tinkama kriptografiniams algoritmams. Iš pradžių tyrinėta atskiros lygties sprendinių aibė, paskui pereita prie lygčių sistemos sprendinių aibės. Sprendiniai ieškomi naudojant matricų perrinkima, tai pat pasitelkiant kitus metodus. Nustatyta, kad lygčių sistemos sprendinių skaičius, nepriklauso nuo matricos eilės *m*.

Alenka A. Finding solutions of matrix equations system: Master's work in applied mathematics / supervisor prof. dr. E. Sakalauskas, Applied Mathematics Department, Faculty of Fundamental Sciences, Kaunas University of Technology. - Kaunas, 2011 - 44p.

SUMMARY

Key agreement protocol, as well as any asymmetric cryptographic algorithm, is based on one-way functions which are easy to calculate, but to calculate the inverse of their value within a reasonable period of time is impossible. The paper will attempt to prove that the system of equations has not much solutions ant that it could be used in cryptographic algorithm. At first individual equation was solved, set of solutions was found. Then moved explore to the set of solutions of equations system. Solutions were found using brute force algorithm for matrices. As well as through other methods. It was found that the number of solutions of equations system does not depend on the matrix size.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSĖLIŲ SĄRAŠAS

ĮVADAS

Šiuo metu beveik visose informacinėse sistemose reikia spręsti informacijos konfidencialumo, vientisumo, autentiškumo ir daug kitų problemų, kurios gali būti įveikiamos pasitelkus tik kriptografinius metodus. Visa tai sudaro kriptografijos, kaip mokslo, objektą, taikomą kuriant naujas informacijos saugos technologijas. Mūsų, kaip kriptosistemų kūrėjų, tikslas – pasiekti, kad šis uždavinys būtų kuo sunkiau išsprendžiamas.

Rakto apsikeitimo protokolo, kaip ir bet kurio asimetrinės kriptografijos algoritmo, pagrindas yra vienkryptės funkcijos, kurias paprasta apskaičiuoti, tačiau apskaičiuoti atvirkštinę jų reikšmę per priimtiną laiko tarpą neįmanoma. Darbe bus bandoma įrodyti tiriamosios lygčių sistemos tinkamumą kriptografiniams algoritmams.

Darbo tikslas - nustatyti matricinės lygčių sistemos, apibrėžtos virš baigtinio lauko sprendinių, aibės galią.

Užduoties formuluotė. Duota matricinė lygčių sistema virš lauko $GF(p)$:

$$\begin{cases} A_1 X = XB_1 \\ A_2 X = XB_2 \end{cases}$$

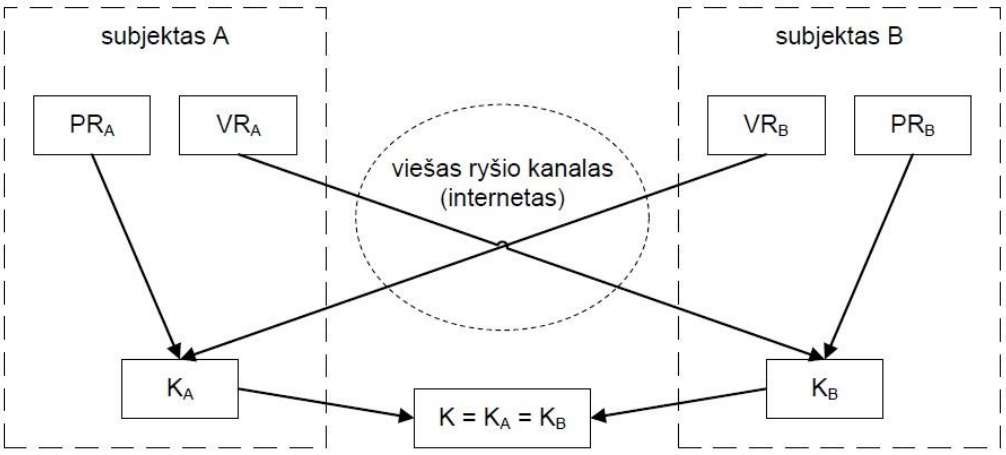
Poros A_1, A_2 ir B_1, B_2 yra $n \times n$ matrcos. Lygtį spręsti X atžvilgiu. Rasti $S = S_1 \bigcap S_2$, kur S_1 -lygties pirmosios lygybės sprendinių aibė, S_2 - lygties antrosios lygybės sprendinių aibė.

1. TEORINĖ DALIS

1.1. TEORINIS RAKTO APSIKEITIMO PROTOKOLAS

Rakto apsikeitimo protokolas yra asimetrinis kriptografinis primityvas, kurio paskirtis – dviem subjektam ar didesnei jų grupei sukurti bendrą privatųjį raktą. Algoritmo vykdymo metu subjektai keičiasi tarpusavyje tam tikrais apskaičiuotais dydžiais, kuriuos gali stebėti pašaliniai subjektai. Baigę keistis pranešimais, kiekvienas subjektas savarankiškai apskaičiuoja privatųjį raktą, kuris yra vienodas visiems protokolo dalyviams.

Dviejų subjektų RAP principas pateiktas 1.1 pav. Kiekvienas vartotojas turi porą raktų – viešąjį (VR) ir slaptąjį (PR). Viešasis ir slaptasis raktai yra tarpusavyje matematiškai susieti, tačiau žinant viešąjį raktą praktiškai neįmanoma apskaičiuoti slaptojo. Tai vienas pagrindinių asimetrinės kriptografijos principų. Dažnai inicijuojant RAP, subjektai atsitiktinai generuoja savo slaptuosius raktus, o viešąjį apskaičiuoja algoritmo vykdymo eigoje. Viešieji raktai nelaikomi paslaptyje ir kiekvienas vartotojas, naudodamas savo slaptąjį ir kito vartotojo viešąjį raktą bei kitus viešai skelbiamus duomenis, pasirinkdamas algoritmą ir algoritmo sisteminių parametrų reikšmes, apskaičiuoja bendrąjį slaptąjį raktą.



1.1 pav. Rakto apsikeitimo protokolo struktūra.

Formaliai bendrą rakto apsikeitimo protokolo schemą galima aprašyti taip:

1) Duotoje grupėje *G* subjektai *A* ir *B* pasirenka pogrupius S_A ir S_B. Taip pasirenkami ir viešai paskelbiami sisteminiai algoritmo parametrai *S*. Subjektas *A* susigeneruoja elementą $PR_A \in S$, o vartotojas $B - PR_B \in S$. Šie elementai yra subjektų privatūs raktai.

2) Kiekvienas subjektas apskaičiuoja funkcijos $\beta(PR,S)$ reikšmę ir persiunčia vienas kitam. Gautoji funkcijos reikšmė $VR=\beta(PR,S)$ yra subjektų viešieji raktai. Funkcija $\beta(PR,S)$ turi būti vienkryptė, t. y. žinant rezultatą $\beta(PR,S)$ ir vieną jos argumentą *S* turi būti praktiškai neįmanoma apskaičiuoti antro argumento *PR*.

3) Subjektas *A* apskaičiuoja $\gamma(PR_A,\beta(PR_B,S))$, o subjektas B – $\gamma(PR_B,\beta(PR_A,S))$. Funkcijos β ir γ turi būti susietos taip, kad $\gamma(PR_A,\beta(PR_B,S))=\gamma(PR_B,\beta(PR_A,S))$. Tuomet, po šių veiksmų abu subjektai turės bendrą slaptą raktą $K=\gamma(PR_A,\beta(PR_B,S))=\gamma(PR_B,\beta(PR_A,S))$.

Reikia pastebėti, kad rakto apsikeitimo protokolas nėra šifravimo sistema. Algoritmo vykdymo metu duomenys nėra šifruojami, o tik perduodami viešieji subjektų raktai. Tačiau rakto apsikeitimo protokolas yra sukuriamas taip, kad abu vartotojai, naudodami vienodą algoritmą, bet skirtingus įvesties duomenis, gautų vienodus išvesties rezultatus.

Skyrelyje pateikta informacija iš A. Katvickio darbo „*Rakto apsikeitimo protokolas ir galimos jo atakos”*.

1.2. VIENKRYPTĖS FUNKCIJOS

Rakto apsikeitimo protokolo, kaip ir bet kurio asimetrinės kriptografijos algoritmo, pagrindas yra vienkryptės funkcijos. Tai bijekcinės funkcijos, kurias paprasta apskaičiuoti, tačiau apskaičiuoti atvirkštinę jų reikšmę per priimtiną laiko tarpą neįmanoma.

Vienkrypčių funkcijų sudarymas pagrįstas sudėtingomis algoritminėmis problemomis. Problemos formuluotėje nurodytos sąlygos atitinka tiesioginę vienkryptės funkcijos reikšmę, o iškeltos problemos sprendimas – vienkryptės funkcijos atvirkštinės reikšmės radimą (suformuluoti problemą paprasta, tačiau jos sprendimas dažnai reikalauja didelių pastangų). Visų asimetrinių kriptografinių algoritmų saugumas grindžiamas viena ar kita sudėtinga algoritmine problema, kurių pagrindu sudarytos vienkryptės funkcijos. Verta pastebėti, kad su vienkrypčių funkcijų apvertimu susijusios problemos turi neefektyvius sprendimo būdus t. y. visi žinomi sprendimo algoritmai yra eksponentiniai arba subeksponentiniai. Kadangi nėra griežtai įrodytas kai kurių sudėtingų problemų sprendimo sudėtingumas, asimetrinių kriptografinių sistemų saugumas pagrįstas tikėjimu, kad neegzistuoja šių problemų polinominiai sprendimo algoritmai. Šis tikėjimas stiprinamas faktu, jog gana paprastos struktūros RSA sistema yra nesukompromituota jau daugiau kaip tris dešimtmečius. Jei būtų rasti

efektyvūs būdai spręsti skaičių faktorizacijos arba diskretinio logaritmo problemas, didžioji dalis šiuo metu naudojamų asimetrinių kriptografinių sistemų būtų pažeidžiamos.

Skyrelyje pateikta informacija iš A. Katvickio darbo „*Rakto apsikeitimo protokolas ir galimos jo atakos”*.

1.3. DETERMINANTAS

Tiesinėje algebroje Laplaso skleidimas (POOLE, 2005) yra kvadratinės $n \times n$ matricos B determinanto $|B|$ išraiška. Ji pagrįsta n adjunktų suma. Tai vienas iš būdų praktiškai suskaičiuoti matricos determinantą.

Matricos i,j adjunktas yra skaliarinis dydis apibrėžiamas šitokia lygybe

$$A_{i,j} = (-1)^{i+j} \mid M_{ij} \mid$$

kur M_{ij} yra matricos B *i,j* minoras. Išbraukime matricos B *i*-ąją eilutę ir *j*-ajį stulpelį. Iš likusių elementų sudarytas *n-1* eilės determinantas vadinamas elemento b_{ij} ***minoru.***

Teorema. Tarkime $B = (b_{ij})$ yra $n \times n$ matrica, o $\mathrm{i}, \mathrm{j} \in \{1, 2, ..., n\}$. Determinantas $|B|$ apibrėžiamas tokiu būdu:

$$\begin{aligned} |B| &= b_{i1}A_{i1} + b_{i2}A_{i2} + ... + b_{in}A_{in} = \\ &= b_{1j}A_{1j} + b_{2j}A_{2j} + ... + b_{nj}A_{nj}. \end{aligned}$$

Pavyzdys.

Tarkim $B = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$. Matricos determinantas gali būti paskaičiuotas naudojant Laplaso skeidimą pagal pirmąją eilutę:

$$\begin{aligned} |B| &= 1 \cdot (-1)^{1+1} \cdot \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} + 2 \cdot (-1)^{1+2} \cdot \begin{vmatrix} 4 & 6 \\ 7 & 9 \end{vmatrix} + 3 \cdot (-1)^{1+3} \cdot \begin{vmatrix} 4 & 5 \\ 7 & 8 \end{vmatrix} = \\ &= 1 \cdot (-3) - 2 \cdot (-6) + 3 \cdot (-3) = 0 \end{aligned}$$

Jei paskaičiuotume, tarkim, pagal antrąjį stulpelį, gautume tą patį rezultatą.

1.4. MATRICŲ STRUKTŪRA

Šiame skyrelyje bus pasakojama apie matricų struktūrą. Apibrėžiamos ir išryškinamos pagrindinės matricų vidinės struktūros charakteristikos – tikrinės reikšmės ir tikriniai vektoriai. Remiamasi KVEDARO ir MEYER knygomis. Kalbant apie tikrines reikšmes, kyla klausimas: kiek jų yra, ir kaip jos yra charakterizuojamos?

Apibrėžimas. Jei $A \in M_n$ ir $x \in F^n$ (n-mačių vektorių aibei), tai turime lygtį

$$Ax = \lambda x, \; x \neq 0 \qquad \textbf{(1.1)}$$

kur λ yra skaliaras. Jei skaliaras λ ir nenulinis vektorius x tenkina lygtį, tada λ vadiname matricos A tikrine reikšme, o x – matricos A tikriniu vektoriumi, susijusiu su λ. λ ir x vadinami tikrine pora.

Tikrinių reikšmių – vektorių lygtis, **(1.2)** gali būti perrašyta,

$$(\lambda I - A)x = 0, \; x \neq 0$$

Ši lygtis vadinama A charakteringuoju polinomu. Čia λ yra tikrinė reikšmė tada ir tik tada, kai matrica $\lambda I - A$ yra singuliari, t. y. $\det(\lambda I - A) = 0$

Apibrėžimas. $p_A(t)$ yra $A \in M_n$ charakteristinis polinomas, jei jis apibrėžiamas tokia lygybe

$$p_A(t) = \det(tI - A).$$

$p_A(t)$ yra n-tojo laipsnio polinomas , kurio šaknys yra A tikrinės reikšmės.

$$p_A(\lambda) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{vmatrix}$$

Apibrėžimas. Matrica $B \in M_n$ yra panaši į matricą $A \in M_n$, jei egzistuoja nesinguliari matrica $S \in M_n$ tokia, kad

$$B = S^{-1}AS$$

Transformacija $A \to S^{-1}AS$ vadinama panašumo transformacija, pagal panašumo matricą S. Ryšys „B panaši į A“ kartais žymimas $B \square A$.

Teorema. Tegu $A, B \in M_n$ ir jei A ir B panašios, tada B charakteristinis polinomas yra toks pat kaip ir A.

Irodymas. Tegu matricos A ir B panašios, tada egzistuoja neišsigimusi matrica T tokia, kad $\mathrm{B} = T^{-1}AT$. Matricos b charakteringas polinomas

$$\det(B-\lambda I)=\det(T^{-1}AT-\lambda I)=\det\left[T^{-1}(A-\lambda I)T\right]=$$
$$=\det T^{-1}\det(A-\lambda I)\det T=\det(A-\lambda I),$$

kaip matome, lygus matricos A charakteringajam polinomui, nes $\det T^{-1}=1/\det T$

Išvada. Jei $A,B\in M_n$ ir jei A ir B panašios, tada jos turi tas pačias tikrines reikšmes. Tai reikalinga, tačiau nepakankama sąlyga.

Paprastosios struktūros matricos – tai matricos, turinčios pilną tikrinių vektorių sistemą. Kitaip tariant, tikriniai vektoriai sudaro erdvės bazę. Žemiau parodysiu, kad tokias matricas galima diagonalizuoti. Diagonalioji jų forma vadinama kanonine. Jei matrica yra diagonalizuojama, tai ir atvirkštinė diagonalizuojama, laipsniai ir apskritai visos su ja komutuojančios matricos yra diagonalizuojamos.

Apibrėžimas. Jei matrica $A\in M_n$ yra panaši į diagonalinę matricą, tada A vadinama diagonalizuojama.

Teorema. Tegu $A\in M_n$. A diagonalizuojama tada ir tik tada, kai n yra tiesiškai nepriklausomų vektorių rinkinys, iš kurių kiekvienas yra A tikrinis vektorius.

Įrodymas. Jei A turi n tiesiškai nepriklausomų tikrinių vektorių $x^{(1)},...,x^{(n)}$, juos sudėdami į stulpelius suformuojame nesinguliarią matricą S ir apskaičiuojame

$$S^{-1}AS=S^{-1}\left[Ax^{(1)}Ax^{(2)}...Ax^{(n)}\right]$$
$$=S^{-1}\left[\lambda_1x^{(1)}\lambda_2x^{(2)}...\lambda_nx^{(n)}\right]=S^{-1}\left[x^{(1)}...x^{(n)}\right]\Lambda$$
$$=S^{-1}S\Lambda=\Lambda.$$

Kur

$$\Lambda=\begin{bmatrix}\lambda_1 & & 0\\ & \ddots & \\ 0 & & \lambda_n\end{bmatrix},\ \text{o}\ \lambda_1,...\lambda_n\ \text{yra}\ A\ \text{tikrinės reikšmės.}$$

Lema. Tarkim $\lambda_1,...\lambda_n$ yra $A\in M_n$ tikrinės reikšmės, tarp kurių nėra dviejų vienodų. Tarkim $x^{(j)}$ tikrinis vektorius susijęs su λ_i, $i=1,...,n$. Tada $\left\{x^{(1)},...,x^{(n)}\right\}$ yra tiesiškai nepriklausomų vektorių rinkinys.

Teorema. Jei $A\in M_n$ turi n skirtingas tikrines reikšmes, tada A diagonalizuojama.

Tikrinė dekompozicija leidžia daug lengviau apskaičiuoti matricų laipsnines eilutes. Tarkim turim funkciją

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$$

Tada galioja lygybė

$$f(A) = S^{-1} f(\Lambda) S$$

Kadangi Λ yra diagonalinė matrica, tai funkcija nuo Λ yra daug lengviau paskaičiuojama

$$[f(\Lambda)]_{ii} = f(\lambda_i)$$

Pavyzdys.

$$A^2 = (S^{-1}\Lambda S)(S^{-1}\Lambda S) = S^{-1}\Lambda(SS^{-1})\Lambda S = S^{-1}\Lambda^2 S$$
$$A^n = S^{-1}\Lambda^n S$$

1.5. BAIGTINIO LAUKO TEORIJA

Kad suprastume kriptografines sistemas, butina žinoti šį tą apie baigtinius laukus. Skyrelis sudarytas naudojant medžiagą iš E. Sakalausko knygų „*Kriptografijos teorija*“ ir „*Kriptografinės sistemos*“.

Sąryšis „lygsta moduliu *m*” $a \equiv b \pmod m$ yra ekvivalentumo sąryšis sveikųjų skaičių aibėje **Z**, todėl suskaido ją į nesikertančias ekvivalentumo klases $\bar{a}$; $a \equiv b \pmod m \Leftrightarrow \bar{a} = \bar{b}$ (Sakalauskas, et al., 2007).

Ekvivalentumo klasei moduliu *m* aibėje **Z** priklauso visi sveikieji skaičiai, kurie lygsta vienas kitam moduliu *m*, t. y. dalijant juos iš *m*, gaunama ta pati liekana.

Apibrėžimas. Rinkinys skaičių, paimtų po vieną iš kiekvienos liekanų klasės moduliu *m*, vadinamas pilnąja liekanų sistema tuo moduliu; žymima p. l. s.

Pilnoji liekanų sistema moduliu 5. Klases sudaro aibės:

$$\bar{0} = \{0 + 5k \mid k \in Z\};$$
$$\bar{1} = \{1 + 5k \mid k \in Z\};$$
$$\bar{2} = \{2 + 5k \mid k \in Z\};$$
$$\bar{3} = \{3 + 5k \mid k \in Z\};$$
$$\bar{4} = \{4 + 5k \mid k \in Z\}.$$

Apibrėžimas. Oilerio funkcija $\varphi(m)$ yra natūraliųjų skaičių, mažesnių už *m* ir tarpusavyje pirminių su *m*, skaičius, t. y.

$$\varphi(m) = \{i \mid 1 \le i \le m, (i, m) = 1\},$$

$\varphi(1)=1$ – pagal susitarimą. Tuomet gauname $\varphi(4)=2,\ \varphi(5)=4,\ \varphi(6)=2$.

Teorema (Ferma). Jeigu p – pirminis skaičius, o a nesidalija iš p, tuomet $a^{p^m-1}=1 \bmod(p)$

▲ Tai įrodome prisiminę, kad $\varphi(p)=p-1$, ir pasinaudoję Oilerio teorema. Beje, Ferma teoremą galima užrašyti ir taip: $a^p=a \bmod(p)$ ▼

Apibrėžimas. Grupe vadinama netuščia elementų aibė G su tokia apibrėžta dvinare operacija $*$, kad $G\times G\to G$, t. y. bet kuriai elementų $a,b\in G$ porai $(a,\ b)$ priskiriamas tos pačios aibės elementas: $(a,\ b)\to a*b\in G$ ir tenkinamos tokios aksiomos:

a) operacija $*$ yra asociatyvioji su visais $a,b,c\in G$, t. y. $(a*b)*c=a*(b*c)$;

b) egzistuoja toks vienetinis neutralusis operacijos $*$ elementas e, kad su visais $a\in G$ $a*e=e*a=a$;

c) kiekvienam $a\in G$ egzistuoja toks atvirkštinis (simetriškasis) elementas $a^{-1}\in G$, kad $a*a^{-1}=a^{-1}*a=e$.

Grupę žymėsime simboliu $<G;*>$.

Grupės $<G;*>$ elementų skaičių žymėsime $|G|$.

Bet kurią grupę galima užrašyti išvardinus elementų aibę bei ryšių tarp elementų aibę $G=\langle g_1,g_2,...|R_1,R_2,...\rangle$. Toks grupės pavaizdavimas vadinamas grupės raiškos lygmeniu. Elementai g_1, g_2, ... vadinami grupės generatoriais.

Homomorfizmu φ vadiname vaizdavimą vienos grupės $\langle G_1;*_1\rangle$ į kitą $\langle G_2;*_2\rangle$, išlaikantį operaciją, t. y. bet kuriems $a,b\in G_1$ teisinga $\varphi(a*b)=\varphi(a)*\varphi(b)$.

Jeigu grupėje $<G;*>$ reikalaujame, kad būtų tenkinama komutatyvumo aksioma $a*b=b*a$, *t*uomet sakome, kad grupė yra *komutatyvioji* (*Abelio*).

Apibrėžimas. Žiedu vadiname dviveiksmę algebrinę struktūrą, nusakytą netuščioje aibėje $\Re$, t. y. $<\Re;\ +;\ \cdot>$ jeigu:

a) struktūra $<\Re;\ +>$ yra adicinė Abelio grupė;

b) $<\Re;\ \cdot>$ – multiplikacinė asociatyvioji struktūra (pusgrupė);

c) su visais $a,\ b,\ c\in R$ tenkinami distributyvumo dėsniai:

$a(b+c)=ab+bc$ ir $(b+c)a=ba+ca$.

Paprasčiausias žiedo pavyzdys – sveikųjų skaičių žiedas $<Z;+;\cdot>$.

Apibrėžimas. Žiedą vadiname lauku, jeigu struktūra $< \Re; \cdot >$ yra multiplikacinė Abelio grupė.

Teorema. Liekanų žiedas $< Z_m;+;\cdot >$ yra laukas, kai m yra pirminis, t. y. $m = p$.

Pavyzdys. Imkime žiedą $< Z_4;+;\cdot >$ ir sudarykime struktūrų $< Z_4;+ >$ ir $< Z_4;\cdot >$ lenteles, t. y. elementų sudėties ir daugybos lenteles:

1.1 lentelė

`Sudeties ir daugybos operacijos GF(3)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

1.2 lentelė

Atvirkštiniai elementai GF(5)

Skaičius	**Sudėties atvirkštinis**
0	0
1	4
2	3
3	2
4	1

Skaičius	**Daugybos atvirkštinis**
1	1
2	3
3	2
4	4

Kodėl $< Z_m;+;\cdot >$ m turi būti pirminis?

Laukas turi dvi operacijas (sudėtį ir daugybą). Dalyba lauke yra tiesiog sandauga atvirkštinio (pvz. $6 \div 3 = 6 \times 3^{-1} = 6 \times \frac{1}{3} = 2$), o atimtis – sudėtis atvirkštinio (pvz. 5 – 4 = 5 + (-4) = 1). Žiedas taip pat turi šias dvi operacijas, tačiau žiede nėra salygos, kad turi egzistuoti daugybos atvirkštinis elementas.

Pavyzdys. Skaičiai $\bmod 26$ nesuformuoja lauko. Jie gali buti sudėti, padauginti (suformuoja žiedą). Bet iš jų tik 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 ir 25 atvirkštinius elementus daugybos atžvilgiu, operacijas atliekant $\bmod 26$. Nes tik šie 12 skaičių yra tarpusavyje pirminiai su 26.

Kai m – pirminis. Tai reiškia, kad jis bus tarpusavyje pirminis su visais elementais, priklausančiais $\bmod m$, tai reiškia visiem elementam galesime rasti atvirkštinį elementą daugybos atžvilgiu. Taigi, kiekvienam pirminiui p galime sukonstruoti baigtinį lauką iš p elementų.

Taigi $< Z_4;+;\cdot >$ nėra grupė; $\mathbf{Z}_4^{*} = \mathbf{Z}_4 \setminus \{0\}$; elementas 2 neturi atvirkštinio.

Amerikiečių matematikas E. H. Moore (1862-1932) įrodė, kad baigtinio lauko elementų skaičius turi būti p^n, kiekvienam pirminiam p ir teigiamui sveikajam skaičiui n, taip pat kad kiekvienai p ir n kombinacijai egzistuoja unikalus baigtinis laukas iš p^n elementų.

Apibrėžimas. Kiekvienas baigtinis laukas vadinamas Galua lauku ir žymimas F arba $GF(q)$ (*Galois Field*). Reikia pastebėti, kad egzistuoja baigtiniai Galua laukai, turintys $q = p^n$ elementų; čia p – pirminis, o n – bet kuris teigiamas sveikasis skaičius.

Pažymėkime pirminį skaičių p atitinkančią sveikųjų skaičių aibę $\mathbf{F}_p = \{0,\ 1,\ 2,\ ...,\ p-\ 1\}$. Tegu $\varphi : \mathbf{Z}_p \to \mathbf{F}_p$ atvaizdis nusakomas taisykle $\varphi(\overline{a}) \to a$, $a = 0,\ 1,...,\ p-\ 1$. Tuomet aibė F_p, turinti lauko struktūrą, indukuojamą atvaizdžio φ, vadinama p eilės Galua lauku – $GF(p)$.

Remiantis tuo, kas pasakyta, atvaizdis $\varphi : \mathbf{Z}_p \to \mathbf{F}_p$ yra izomorfizmas, todėl skaičiavimuose naudojant lauko F_p elementus pasitelkiama įprasta sveikųjų skaičių aritmetika, redukuojant moduliu p (sudarant liekanų klases) (Lidl, 1983).

Daugianarių žiedas $\mathbf{Z}_m[x]$**.** Imkime daugianarį $f(x) = a_0 + a_1 x + ... + a_m x^m = \sum_{k=0}^{m} a_k x^k$, $a_k \in \mathbf{Z}_m, a_m \neq 0$; a_k yra daugianario koeficientas, skaičius $m \geq 0$ – daugianario eilė, x – kintamasis. Daugianariai $f(x)$ ir $g(x)$ lygūs tada ir tik tada, kai $a_k = b_k$ visiems k, t. y.

$$f(x) = \sum_{k=0}^{m} a_k x^k = \sum_{k=0}^{m} b_k x^k = g(x) \Leftrightarrow a_k = b_k,\ k = \overline{1, m}.$$

Sudedant daugianarius pakanka sudėti koeficientus prie vienodų x laipsnių, t. y.

$$h(x) = f(x) + g(x) = \sum_{k=0}^{m} a_k x^k + \sum_{k=0}^{m} b_k x^k = \sum_{k=0}^{m} c_k x^k,$$

$$c_k = \begin{cases} a_k + b_k, \text{ kai } k \leq \min(m, r), \\ b_k, \text{ kai } m < k \leq r, \text{ esant r} > m, \\ a_k, \text{ kai } r < k \leq m, \text{ esant } r < m. \end{cases}$$

Daugianarių sandauga $p(x) = f(x) \cdot g(x)$ apibrėžiama formule

$$p(x) = p_0 + p_1 x + \ ... \ + p_{m+r} x^{m+r},$$
$$p_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq m, 0 \leq j \leq r}} a_i b_i.$$

Daugianarių aibė $\mathbf{Z}_m[x]$ su apibrėžtomis sudėties ir daugybos operacijomis sudaro žiedą.

Imkime daugianarių žiedą $\mathbf{Z}_2[x]$**,** t. y. žiedą, kurį sudaro daugianariai su koeficientais, priklausančiais laukui $\mathbf{Z}_2$. Daugianaris, neturintis šaknų tame lauke, vadinamas ***pirminiu***. Pirminis daugianaris žiede $\mathbf{Z}_p[x]$ atlieka tą patį vaidmenį kaip ir pirminis *p* skaičius lauke $\mathbf{Z}_p$. Pavyzdžiui, lygtis $x^2 + x + 1 = 0$ lauke $\mathbf{Z}_2$ neišsprendžiama. Dalijant daugianarį, kurio eilė $m = 2$, tame lauke gaunamos liekanos ne didesnio kaip antro laipsnio, kur koeficientai priklauso $\mathbf{Z}_2$, t. y. 0 arba 1, todėl yra 4 galimos liekanos $0x+0=0,\ 0x+1=1, 1x+0=x,\ 1x+1=x+1,$ atstovaujančios liekanų klasėms moduliu $\left(x^2 + x + 1\right)$. Todėl faktoržiedą $\mathbf{Z}_2[x]/(x^2 + x + 1)$ sudaro 4 elementai. Pateikiame veiksmų lentelę faktoržiede $\mathbf{Z}_2[x]/(x^2 + x + 1)$:

1.3 lentelė

Veiksmai faktoržiede

+	**0**	**1**	***x***	***x*+1**
0	0	1	*x*	*x*+1
1	1	0	*x*+1	*x*
x	*x*	*x*+1	0	1
***x*+1**	*x*+1	*x*	1	0

×	**0**	**1**	***x***	***x*+1**
0	0	0	0	0
1	0	1	*x*	*x*+1
x	0	*x*	*x*+1	1
***x*+1**	0	*x*+1	1	*x*

Dažniausiai polinomai asocijuojasi su kažkokiu nežinomuoju, kurį reikia rasti. Tačiau kalbant apie baigtinius laukus, žiūrima į pačią polinomo konstrukciją, t. y. į koeficientus ir jo laipnius. Galime polinomą įsivaizduoti kaip vektorių, kurio komponentai yra polinomo koeficientai. Keturios liekanos, aprašytos aukščiau, gali būti užrašytos šitaip: $(0,0),\ (0,1),\ (1,0),\ (1,1)$.

Iš lentelių matome, kad faktoržiedas $\mathbf{Z}_2[x]/(x^2 + x + 1)$ yra laukas. Rezultatas analogiškas faktoržiedui $\mathbf{Z}/(p)$, kai $p = 2$. Todėl pirminiai skaičiai ir pirminiai daugianariai yra labai svarbūs konstruojant laukus.

Teorema. Tarkime, kad *f* yra daugianaris, priklausantis žiedui $\mathbf{F}[x]$. Faktoržiedas $\mathbf{F}[x]/(f)$ yra laukas tada ir tik tada, kai daugianaris *f* neskaidomas lauke **F**, t. y. kai jis yra pirminis.

Teorema. Baigtiniame lauke $\mathbf{F}_q$, turinčiame *q* elementų, kiekvienam elementui $a \in \mathbf{F}_q$ teisinga lygybė $a^q = a$.

Teorema. Jei *f* neredukuojamas *m*-tojo laipsnio daugianaris lauke $F_q[x]$, tada jis turi šaknį *a* lauke F_{q^m}. Taip pat, *f* turi *m* skirtingų paprastųjų šaknų: $a, a^2, \ldots, a^{q^{m-1}}$, priklausančių F_{q^m}.

Baigtinio lauko elementų reiškimas. Imkime pirminį daugianarį $f = x^4 + x^3 + 1$ ir sudarykime visus Galua lauko elementus, kuriuos gausime faktorizuodami žiedą $\mathbf{Z}_2[x]$ moduliu *f*. Kadangi dalydami žiedo $\mathbf{Z}_2[x]$ daugianarį gauname liekaną $a_0 + a_1x + a_2x^2 + a_3x^3$, turėsime 2^4 elementų, nes $a_i = \mathbf{Z}^2$, t. y. $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$. Išvardykime juos.

Konstantos: 0, 1.

Tiesiniai elementai: $a, a + 1$.

Kvadratiniai elementai: $a^2, a^2 + 1, a^2 + a + 1, a^2 + a$.

Kubiniai elementai: $a^3, a^3 + 1, a^3 + a + 1, a^3 + a^2, a^3 + a^2 + 1, a^3 + a^2 + a, a^3 + a^2 + a + 1, a^3 + a$.

Taip išreikštų lauko $GF(2^4)$ elementų sudėtis – tai ne didesnio kaip trečiojo laipsnio polinomų sudėtis, veiksmus atliekant su koeficientais lauke $\mathbf{Z}_2$.

Dauginant elementus, reikia atsižvelgti į tai, kad $a^4 + a^3 + 1 = 0 \pmod f$ ir laikyti tiesiog, kad $a^4 + a^3 + 1 = 0$. Pavyzdžiui, $a^7 = a^4 \cdot a^3 = (a^3 + 1)a^3 = a^6 + a^3 = a^4 \cdot a^2 + a^3$, nes $a^4 + a^3 + 1 = 0$, ir iš čia $a^4 = a^3 + 1$. Lauke $\mathbf{Z}_2$ $-1 = 1$.

Toliau tęsdami skaičiavimus gauname

$a^4 \cdot a^2 + a^3 = (a^3 + 1)a^2 + a^3 = a^5 + a^2 + a^3 = a^4 \cdot a + a^2 + a^3 = (a^3 + 1)a + a^2 + a^3 = 1 + a + a^2$

(Grigutis, 1998).

Palyginimui sudarome lentelę, atsižvelgdami į tai, kad multiplikacinė grupė $GF(2^4)$ — ciklinė grupė, kurią generuoja elementas *a*:

1.4 lentelė

Elementų išraiškos GF(24)

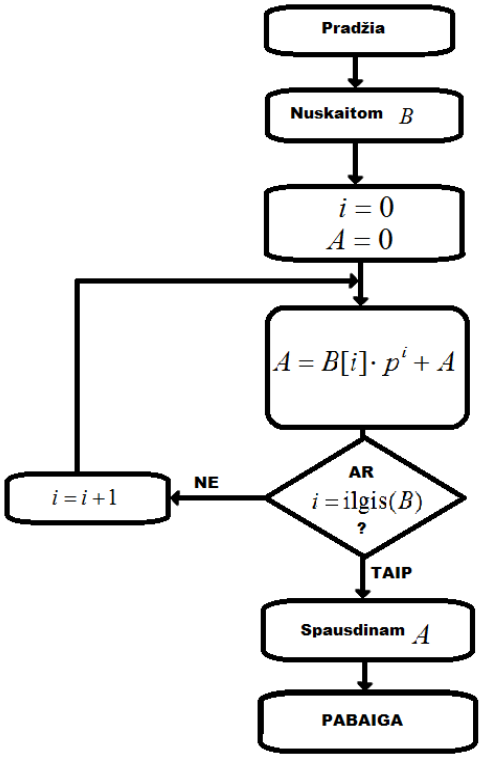
Laipsninis reiškimas	Polinominis reiškimas	Vektorinis reiškimas
0	0	(0000)
1	1	(0001)
a	a	(0010)
a^2	a^2	(0100)
a^3	a^3	(1000)
a^4	a^3+1	(1001)
a^5	a^3+a+1	(1011)
a^6	a^3+a^2+a+1	(1111)
a^7	a^2+a+1	(0111)
a^8	a^3+a^2+a	(1110)
a^9	a^2+1	(0101)
a^{10}	a^3+a	(1010)
a^{11}	a^3+a^2+1	(1101)
a^{12}	$a+1$	(0011)
a^{13}	a^2+a	(0110)
a^{14}	a^3+a^2	(1100)

Polinomą $a_0+a_1x+a_2x^2+a_3x^3$ tapatiname su dvejetainiu žodžiu $(a_0a_1a_2a_3)$, $a_i=\mathbf{Z}_2$.

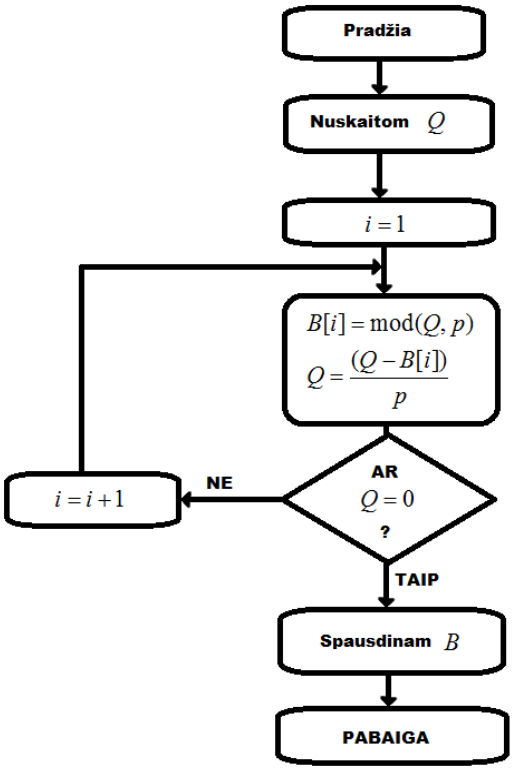
Atlikdamas skaičiavimus programa Matlab, elementus priklausančius praplėstam baigtiniam laukui atvaizduodavau sveikaisiais skaičiais nuo 0 iki p^m. Tarkim elementą, pavaizduotą vektoriniu reiškimu $(a_0a_1...a_{m-1})$, norime atvaizduoti į sveikąjį skaičių. Tada naudojama formulė:

$$E=a_{m-1}p^{m-1}+...+a_2p^2+a_1p+a_0$$

Taip vaizduoti patogu, nes matricos atrodo tvarkingiau.**1.2 pav.** pateiktas programinis algoritmas. Atlekant veiksmus, būtina grįžti prie vektorinio reiškimo. **1.3 pav**. pateiktas vaizdavimas



1.2 pav. Vektorinis reiškimas į sveikąjį



1.3 pav. Sveikasis reiškimas į vektornį

Lentelėje pateiksiu $GF(3^2)$ elementus abiem aukščiau aprašytiem atvejam.

1.5 lentelė

Vektorinis ir sveikasis elementų vaizdavimai

Vektorinis reiškimas	Sveikasis reiškimas
(0 0)	0
(1 0)	1
(2 0)	2
(0 1)	3
(1 1)	4
(2 1)	5
(0 2)	6
(1 2)	7
(2 2)	8

Tyrime pateikta nemažai pavyzdžių, kurių daugumos veiksmai atliekami lauke $GF\left(3^2\right)$, norintiems paskaičiuoti, pateiksiu sudėties ir daugybos lenteles.

1.6 lentelė

Sudėties lentelė

+	**0**	**1**	**2**	***x***	***x*+1**	***x*+2**	**2*x***	**2*x*+1**	**2*x*+2**
0	0	1	2	*x*	*x*+1	*x*+2	2*x*	2*x*+1	2*x*+2
1	1	2	1	*x*+1	*x*+2	*x*	2*x*+1	2*x*+2	2*x*
2	2	1	1	*x*+2	*x*	*x*+1	*0*	2*x*	2*x+1*
x	*x*	*x*+1	*x*+2	2	2*x*	2*x*+2	0	1	2
***x*+1**	*x*+1	*x*+2	*x*	2*x*	2*x*+2	0	1	2	0
***x*+2**	*x*+2	*x*	*x*+1	2*x*+2	0	2*x+1*	2	0	1
2*x*	2*x*	2*x*+1	*0*	0	2*x+1*	2	*x*	*x*+1	*x*+2
2*x*+1	2*x*+1	2*x*+2	2*x*	1	2	0	*x*+1	*x*+2	*x*
2*x*+2	2*x*+2	2*x*	2*x+1*	2	0	1	*x*+2	*x*	*x*+1

1.7 lentelė

Daugybos lentelė

$\times$	**0**	**1**	**2**	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+1$	$x+2$
x	0	x	$2x$	$2x+1$	1	$x+1$	$x+2$	$2x+2$	2
$x+1$	0	$x+1$	$2x+2$	1	$x+2$	$2x$	2	3	$2x+1$
$x+2$	0	$x+2$	$2x+1$	$x+1$	$2x$	2	$2x+2$	1	x
$2x$	0	$2x$	x	$x+2$	2	$2x+2$	$2x+1$	$x+1$	1
$2x+1$	0	$2x+1$	$x+1$	$2x+2$	3	1	$x+1$	2	$2x$
$2x+2$	0	$2x+2$	$x+2$	2	$2x+1$	x	1	$2x$	$x+2$

2. ANALITINĖ DALIS

2.1 DARBO TIKSLAS IR UŽDAVINIAI

Tikslas - nustatytis matricinės lygčių sistemos

$$\begin{cases} A_1 X = XB_1 \\ A_2 X = XB_2 \end{cases} \quad \textbf{(2.1)}$$

apibrėžtos virš baigtinio lauko, sprendinių aibės galią *S*.

Uždavinio formuluotė. Duota matricinė lygčių sistema **(2.1)** virš lauko $GF(p)$. Poros A_1, A_2 ir B_1, B_2 $n \times n$ matricos . Sistemą sprendžiame X atžvilgiu.

Lygtis $|A_i - \lambda I| = 0$ neturi sprendinių lauke $GF(p)$.

Rasti $S = S_1 \bigcap S_2$, kur S_1-lygties pirmosios lygybės sprendinių aibė, S_2 - lygties antrosios lygybės sprendinių aibė.

Prieš pradėdamas nagrinėti lygčių sistemą **(2.1)**, pateiksiu pavyzdį, kaip ji panaudojama konkrečiame rakto apsikeitimo protokole. Tokį RAP aprašė Kauno techologijos universiteto Taikomosios matematikos katedros dėstytojai E. Sakalauskas, P. Tvarijonas, N. Listopackis savo straipsnyje „Komutatoriumi paremtu RAP realizacija“.

Komutatoriumi paremtu RAP realizacija

Tarkime Aldona $\mathcal{A}$ ir Bronius $\mathcal{B}$ bando susitari dėl bendro slaptojo rakto *K*.

RAP viešieji parametrai – tai dvi poros matricų $A_1, A_2 \in M$ ir $B_1, B_2 \in M$. Abu dalyviai sutaria naudoti matricos eksponentinę funkciją $f_{q,r} : M \times M \to M$, apibrėžiamą skaičiais $q, r \in Z_n$, kur $Z_n = \{0,1,...,n-1\}$. Tada kiekvienam $M_i, M_j \in M$ egzistuoja $M \in \mathcal{M}$, tenkinantis lygybę

$$f_{q,r}(M_i, M_j) = M_i^q M_j^r = M \ .$$

Protokolas veikia pagal šiuos žingsnelius:

1. $\mathcal{A}$ atsitiktinai pasirenka slaptuosius parametrus q, r ir indeksus $i, j \in \{1,2\}$ ir naudodama funkciją $f_{q,r}(A_i, A_j)$ suskaičiuoja slaptąją matricą

$$X = f_{q,r}(A_i, A_j) = A_i^q A_j^r$$

Tada ji suskaičiuoja matricas

$$U_1 = XB_1X^{-1}, U_2 = XB_2X^{-1}$$

ir siunčia jas $\mathcal{B}$.

2. Tuo tarpu $\mathcal{B}$ atsitiktinai pasirenka slaptuosius parametrus $s,t \in Z_n$ ir indeksus $k,l \in \{1,2\}$, ir naudojant funkciją $f_{s,t}(B_k, B_l)$, suskaičiuoja slaptąją matricą

$$\boldsymbol{Y} = f_{s,t}(B_k, B_l) = B_k{}^s B_l{}^t .$$

Tada jis suskaičiuoja matricas

$$V_1 = YA_1Y^{-1}, V_2 = YA_2Y^{-1}$$

ir nusiunčia jas $\mathcal{A}$.

3. $\mathcal{A}$ paima savo slaptuosius parametrus q,r, indeksus i, j ir matricą *X* ir suskaičiuoja savo slaptąjį raktą

$$K_A = f_{q,r}(K_i, K_j)X^{-1} = V_i^q, V_j{}^r X^{-1} = YA_i{}^q Y^{-1} YA_j{}^r Y^{-1} X^{-1} = YA_i{}^q A_j{}^r Y^{-1} X^{-1} = YXY^{-1} X^{-1} \quad \textbf{(2.2)}$$

4. $\mathcal{B}$ paima savo slaptuosius parametrus s,t, indeksus k,l, matricą *X* ir suskaičiuoja savo slaptąjį raktą

$$\begin{aligned} K_B &= Y\left[f_{s,t}(U_k, U_l) \right]^{-1} = Y\left[U_k{}^s U_l{}^t \right]^{-1} = Y\left[XB_k{}^s X^{-1} XB_l{}^t X^{-1} \right]^{-1} \\ &= Y\left[XB_k{}^s B_l{}^t X^{-1} \right]^{-1} = Y\left[XYX^{-1} \right]^{-1} = YXY^{-1} X^{-1} \end{aligned} \quad \textbf{(2.3)}$$

Matome, kad Aldonai $\mathcal{A}$ ir Broniui $\mathcal{B}$ pavyko susikurti savo bendrąjį slaptą raktą

$$K = K_{\mathrm{A}} = K_{\mathrm{B}}$$

Saugumo analizė

Norint pašaliniam žmogui pasinaudoti slaptuoju raktu, jis turi žinoti K_{A} arba K_{B} iš **(2.2)** ir **(2.3)** lygčių. Tai galima padaryti dviem būdais.

Pirmuoju būdu galima rasti matricas *X* ir *Y* ir apskaičiuoti K_{A} arba K_{B} iš **(2.2)** arba **(2.3)**.

Antruoju būdu reiktų rasti slaptuosius parametrus q,r arba s,t. Turint juos galima paskaičiuoti matricą *X,* generuojamą žinomų matricų A_1, A_2, arba matricą *Y,* generuojamą žinomų matricų B_1, B_2. Įsibrovėlis, turėdamas slaptuosius parametrus q,r arba s,t, gali apskaičiuoti K_{A} arba K_{B} iš **(2.2)** arba **(2.3)**.

Pagal pirmąjį scenarijų, ieškant X ir Y matricų, reikia išspręsti matricinę lygčių sistemą

$$\begin{cases} XB_1 = U_1 X, \\ XB_2 = U_2 X, \end{cases}$$
$$\begin{cases} YA_1 = V_1 Y, \\ YA_2 = V_2 Y. \end{cases}$$

Kad iššspręstume šią keturių lygčių sistemą, turime mokėti spręst tokią

$$\begin{cases} A_1 X = XB_1 \\ A_2 X = XB_2 \end{cases}$$

Tai ir yra mūsų tiriamoji lygtis **(2.1)**.

2.2. LYGTIES SPRENDINIŲ ANALIZĖ

Apibrėžimas. Matricų A_i, B_i ciklas yra $p^m - 1$.

Įrodysime matricai A_i. Diagonalizuojame matricą $\left(U_i^{-1} D_i U_i\right) = A_i$, čia D_i - diagonalinė matrica, kurios įstrižainėje A_i tikrinės reikšmės, o U_i - tikrinių vektorių matrica. $U_i = \left(p_1, p_2, \ldots, p_n\right)$, kur p_i tikriniai vektoriai.

Pakeliam abi puses laipsniu $p^m - 1$

$$\left(U_i^{-1} D_i U_i\right)^{p^m - 1} = A_i^{p^m - 1}.$$

Pasinaudoję matricų dekompozicijos savybėmis galime perrašyti

$U_i^{-1} D_i^{p^m - 1} U_i = A_i^{p^m - 1}$. Diagonalinę matricą keliame $p^m - 1$ laipsniu.

$$U_i^{-1} \begin{pmatrix} \lambda_1^{p^m - 1} & 0 & \cdots & 0 \\ 0 & \lambda_2^{p^m - 1} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & \lambda_n^{p^m - 1} \end{pmatrix} U_i = A_i^{p^m - 1}.$$

Iš Ferma teoremos $\lambda_1^{p^m - 1} = 1$,todėl

$$U_i^{-1} \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix} U_i = A_i^{p^m - 1}$$

$A_i^{p^m - 1} = I$, reiškia matricos A_i ciklas yra $p^m - 1$.

Lygties $\mathbf{A_1X = XB_1}$ sprendinių analizė

Matematinio modeliavimo būdu ieškosime lygties

$$A_1X = XB_1 \tag{2.4}$$

sprendinių. Kaip ir prieš tai, *m* eilės matricas A_1 ir B_1 faktorizuojame:

$$A_1 = U_1\tilde{A}_1U_1^{-1}, B_1 = V_1\tilde{B}_1V_1^{-1},$$

kur $\tilde{A}_1$, $\tilde{B}_1$ yra vienodos diagonalinės matricos, kurių įstrižainėse A_1 ir B_1 tikrinės reikšmės.

Gauname:

$$U_1\tilde{A}_1U_1^{-1}X = XV_1\tilde{B}_1V_1^{-1},$$

tada abi lygybės puses padauginę iš *V* ir padalinę iš *U*, gauname

$$\tilde{A}_1U_1^{-1}XV_1 = U_1^{-1}XV_1\tilde{B}_1,$$

pažymime $\tilde{X} = U_1^{-1}XV_1$. Tada gaunam, kad

$$\tilde{A}_1\tilde{X} = \tilde{X}\tilde{B}_1 \tag{2.5}$$

Parodysiu, kad matrica $\tilde{X}$ yra diagonalinė, kai matricų A_1 ir B_1 tikrinės reikšmės vienodos ir tarpusavyje skirtingos, t. y. $a_{ii} = b_{ii}, \forall i = 1,m$ ir $a_{ii} \neq a_{jj}$, kai $i \neq j$.

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & & \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & a_{mm} \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & & \\ \vdots & & \ddots & \vdots \\ x_{m1} & & \ldots & x_{mm} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & & \\ \vdots & & \ddots & \vdots \\ x_{m1} & & \ldots & x_{mm} \end{pmatrix}\begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & & \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & b_{mm} \end{pmatrix}$$

Sudauginame:

$$\begin{pmatrix} a_{11}x_{11} & a_{11}x_{12} & \cdots & a_{11}x_{1m} \\ a_{22}x_{21} & a_{22}x_{22} & & \\ \vdots & & \ddots & \vdots \\ a_{mm}x_{m1} & & \ldots & a_{mm}x_{mm} \end{pmatrix} = \begin{pmatrix} b_{11}x_{11} & b_{22}x_{12} & \cdots & b_{mm}x_{1m} \\ b_{11}x_{21} & b_{22}x_{22} & & \\ \vdots & & \ddots & \vdots \\ b_{11}x_{m1} & & \ldots & b_{mm}x_{mm} \end{pmatrix}.$$

Matricos yra lygios, kai jų elementai yra lygūs, todėl

$$\begin{array}{ll} a_{11}x_{11} = b_{11}x_{11} & (a_{11} - b_{11})x_{11} = 0 \\ a_{11}x_{12} = b_{22}x_{12} & (a_{11} - b_{22})x_{12} = 0 \\ \cdots & \cdots \\ a_{mm}x_{mm} = b_{mm}x_{mm} & (a_{mm} - b_{mm})x_{mm} = 0 \end{array} \Rightarrow , \tag{2.6}$$

kadangi $a_{ii} = b_{ii}$, o $a_{ii} \neq b_{jj}$ skirtingiems *i* ir *j*, gauname

$$\begin{aligned} 0 \cdot x_{11} &= 0 \\ (a_{11} - b_{22})\, x_{12} &= 0 \\ &\cdots \\ 0 \cdot x_{mm} &= 0 \end{aligned}.$$

Gauname $x_{ij} = 0$, jei $i \neq j$, tai reiškia, kad lygybė galioja, kai visos A_1 ir B_1 tikrinės reikšmės tarpusavyje skirtingos

$$\tilde{X} = \begin{pmatrix} x_{11} & 0 & \cdots & 0 \\ 0 & x_{22} & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & x_{mm} \end{pmatrix}$$

čia $x_{11,\ldots}, x_{mm}$ gali buti bet kokie skaičiai, priklausantys baigtiniam laukui. Tarkime, baigtinio lauko eilė yra *p*.

Kadangi $x_{11,\ldots}, x_{mm}$ gali būti bet kokie, reiškia matricų $\tilde{X}$, tenkinančių lygybę $\tilde{A}_1 \tilde{X} = \tilde{X} \tilde{B}_1$ yra p^m, reiškia tiek pat yra matricų *X*, tenkinančių **(2.4)**. Matrica X turi p^{m^2} skirtingų variantų.

Jei matricos A_1 tikrinės reikšmės nebūtų skirtingos. Tarkim, yra dvi sutampančios tikrinės reiksmės $\lambda_1 = \lambda_2$, tada **(2.5)** lygybėje $a_{11} = a_{22} = b_{11} = b_{22}$. Lygčių sitema atrodytų šitaip:

$$\begin{aligned} (a_{11} - b_{11})\, x_{11} &= 0 \\ (a_{11} - b_{22})\, x_{12} &= 0 \\ (a_{11} - b_{33})\, x_{12} &= 0 \\ &\cdots \\ (a_{mm} - b_{mm})\, x_{mm} &= 0 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 0 \cdot x_{11} &= 0 \\ 0 \cdot x_{12} &= 0 \\ (a_{11} - b_{33})\, x_{12} &= 0 \\ &\cdots \\ 0 \cdot x_{mm} &= 0 \end{aligned}$$

Palyginus su ta situacija, kai visos tikrinės reikšmės buvo skitingos, dabar atsirado x_{21}, x_{12} kurių visos reikšmės tenkina **(2.5)** lygtį.

$\tilde{X}$ matrica dabar bus tokia:

$$\tilde{X} = \begin{pmatrix} x_{11} & x_{12} & \cdots & 0 \\ x_{21} & x_{22} & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & x_{mm} \end{pmatrix}$$

Tai reiškia, kad sprendinių skaičius žymiai padidėja. Tai pamatysime tolimesniuose skaičiavimuose.

Toliau patyrinėsiu, kaip keičiasi sprendinių skaičius, keičiant lygties parametrus: matricos eilę *m*, tikrinių reikšmių ir vektorių, bei pačių matricų laukus, kuriuose atliekami skaičiavimai.

Kitas variantas, kai matricos A_1 ir B_1 neturi sutampančių tikrinių reikšmių. Tada iš **(2.6)** sistemos

$$\begin{aligned}
&(a_{11}-b_{11})x_{11}=0\\
&(a_{11}-b_{22})x_{12}=0\\
&\cdots\\
&(a_{mm}-b_{mm})x_{mm}=0
\end{aligned}$$

Kadangi $a_{ii}\neq b_{jj}$ bet kokiam *i* ir *j*, gauname, kad sistemą tenkina sprendinys $x_{ij}=0,\ \forall i,j$, gauname $\tilde{X}=0$, reiškia egzistuoja vienintelis trivialus **(2.4)** lygties sprendinys $X=0$.

Kai $A_1,B_1\in GF(p)$ bei jų tikrinės reikšmės priklauso $GF(p)$

Tikrinės reikšmės skirtingos. Tarkime matricos A_1 ir B_1, kaip ir jų tikrinės reikšmės bei tikriniai vektoriai, priklauso $GF(p)$.

Ieškomos matricos *X* diagonalinė matrica

$$\tilde{X}=\begin{pmatrix} x_{11} & 0 & \cdots & 0\\ 0 & x_{22} & & \vdots\\ \vdots & & \ddots & \\ 0 & \cdots & & x_{mm}\end{pmatrix}$$

$x_{11,\dots},x_{mm}\in GF(p)$. Iš viso yra p^m diagonolinės matricos kombinacijų. Iš lygybės $\tilde{X}=U_1^{-1}XV_1$ gauname, kad

$$X=U_1\tilde{X}V_1^{-1}$$

$\tilde{X}$ tenkinančių lygtį yra p^m, todėl lygties $A_1X=XB_1$ sprendinių taip pat yra p^m.

Pavyzdys. $A_1,B_1\in M_2$. $A_1,B_1\in GF(3)$

Pasirenkame

$$A_1=\begin{pmatrix}1&2\\0&2\end{pmatrix}\text{ ir }\ B_1=\begin{pmatrix}1&0\\2&2\end{pmatrix}.$$

Kaip ir turi būti, abiejų matricų tikrinės reikšmės $\lambda_1=1,\lambda_2=2$. Taip pat jos abi $\lambda_1,\lambda_2\in GF(3)$. Reiškia, yra tokios matricos *X*, kurios tenkina lygybę

$$A_1X=XB_1.$$

Pagal teoriją, turėtume rast 3^2 tokių matricų *X*. Matematinio modeliavimo būdu randame visus sprendinius *X*.

2.1 lentelė

Lygties sprendinių aibė *GF(3)*

0	0	1	1	2	2
0	0	1	0	2	0
0	0	1	1	2	2
0	1	1	1	2	1
0	0	1	1	2	2
0	2	1	2	2	2

Patikrinimui paimam tarkim $X = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. Statome į lygtį

$$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}.$$

Atliekame veiksmus

$$\begin{pmatrix} 1\cdot 1+2\cdot 1 & 1\cdot 1+2\cdot 2 \\ 0\cdot 1+2\cdot 1 & 0\cdot 1+2\cdot 2 \end{pmatrix} = \begin{pmatrix} 1\cdot 1+1\cdot 2 & 1\cdot 0+1\cdot 2 \\ 1\cdot 1+2\cdot 2 & 1\cdot 0+2\cdot 2 \end{pmatrix}.$$

Gauname lygybę

$$\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}.$$

Reiškia *X* yra lygties sprendinys.

Apibendrinimui noriu pasakyti, lygtis $A_1X = XB_1$, kai veiksmai atliekami $GF(p)$lauke, tikrinės reikšmės $\lambda_1,\ldots,\lambda_m \in GF(p)$, tai egzistuoja p^m sprendinių, tenkinančių lygtį. Šie sprendiniai yra pakankamai nesunkiai randami. Panašiai yra ir su praplėstu baigtiniu lauku $GF\left(p^m\right)$. Tada lygtis turės $\left(p^m\right)^m$ sprendinių. Sprendinių skaičiusskaičiuojamas taip pat, kaip ir lauke $GF(p)$, tik reikia atsižvelgti į lauko charakteristikas bei matricos eilę.

Kai $A_1, B_1 \in GF(p)$, tačiau tikrinės reikšmės priklauso $GF\left(p^m\right)$

Tarkime matricos $A_1, B_1 \in GF\left(p\right)$, o jų tikrinės reikšmės ir tikriniai vektoriai priklauso $GF\left(p^m\right)$, nes lygtis $\left|A_i - \lambda I\right| = 0$ neturi sprendinių lauke $GF\left(p\right)$.

Pavyzdys. Tarkime

$$A=\begin{pmatrix}0 & 2\\ 2 & 2\end{pmatrix}.\ A\in GF(3).$$

Užrašome šios matricos charakteringąją lygtį $|A-\lambda I|=0$.

$$\begin{vmatrix}0-\lambda & 2\\ 2 & 2-\lambda\end{vmatrix}=0$$

t.y. $-\lambda(2-\lambda)-2\cdot 2=0$. Atliekame veiksmus

$$\begin{aligned}-\lambda(2-\lambda)-(2\cdot 2)&=0\\ \lambda^2-2\lambda-4&=0\\ \lambda^2+1\lambda-1&=0\end{aligned}$$

Gavome, kad charakteringoji lygtis yra $\lambda^2+1\lambda+2=0$. Tačiau jos netenkina joks elementas, priklausantis $GF(3)$. Lygtis neturi sprendinių lauke $GF(3)$. Tačiau ji turi sprendinį praplėstame lauke $GF(3^2)$. Pirminis daugianaris lauke $GF(3^2)$ yra x^2+x+2, jis sutampa su charakteringąja lygtimi, todėl iškart žinome, kad $\lambda_1=x$.

Matematinio modeliavimo būdu apskaičiuojame ir antrą šaknį $\lambda_2=2x+2$. Statome λ_2 į lygtį.

$$\begin{aligned}(2x+2)^2+2x+2+2&=0\\ 4x^2+8x+4+2x+2+2&=0\\ x^2+2x+1+2x+2+2&=0\\ x^2+x+2&=0\end{aligned}$$

Gavome, kad lygties $\lambda^2+1\lambda+2=0$ sprendiniai $\lambda_1=x$ ir $\lambda_2=2x+2$ priklauso praplėstam baigtiniam laukui $GF(3^2)$.

Tada ($\tilde{A}_1\tilde{X}=\tilde{X}\tilde{B}_1$) lygybės visi nariai taip pat priklausys praplėstam baigtiniam laukui $GF(p^m)$.

() lygtis turės $(p^m)^m$ sprendinių. Tačiau dauguma sprendinių nepriklausys laukui $GF(p^m)$. Tai netenkina pradinės sąlygos, todėl reikia nustatyti, kiek sprendinių priklauso $GF(p)$. Tai darome matematinio modeliavimo būdu, ieškodami kiek iš $(p^m)^m$ sprendinių, priklausančių $GF(p^m)$, priklauso ir $GF(p)$. Tendenciją pastebime atlikdami skaičiavimus, keičiant matricos eilę *m* bei lauko charakteristiką *p*. Sprendinių skaičius gautas p^m, t. y. toks pats, kaip ir pirmuoju atveju (kai $A_1, B_1\in GF(p)$ ir tikrinės reikšmes priklausė $GF(p)$), tačiau šituo atveju reikia daug daugiau skaičiavimų. Kad butų aiškiau, pateiksiu pavyzdį.

Pavyzdys. $A_1, B_1 \in GF(2)$, o jų tikrinės reikšmės ir tikriniai vektoriai priklauso $GF(2^2)$, nes lygtis $|A_i - \lambda I| = 0$ neturi sprendinių lauke $GF(2)$.

$A_1 X = X B_1$ sprendiniai:

2.2 lentelė

Lygties sprendinių aibė lauke GF(22)

0	**0**	**1**	**0**	2	0	3	0
0	**0**	**1**	**1**	2	2	3	3
0	**1**	**1**	**1**	2	1	3	1
1	**0**	**0**	**1**	3	2	2	3
0	2	1	2	2	2	3	2
2	0	3	1	0	2	1	3
0	3	1	3	2	3	3	3
3	0	2	1	1	2	0	3

Matome, kad lygtis turi 2^4 sprendinių, iš kurių 2^2 priklauso $GF(2)$.

Lentelėje matosi, kaip didėja sprendinių skaičius prie charakteristikų: matricos eilės *m* ir lauko charakteristikos *p*.

2.3 lentelė

Lygties sprendinių skaičius

p \ *m*	**2**	**3**	**4**	**5**
2	4	8	16	32
3	9	27	81	243
5	25	125	625	3125
7	49	343	2401	16807
11	121	1 331	14641	161051
17	289	4 913	83521	1419857

Dabar kyla klausimas, kokiam laukui priklauso **(2.5)** tenkinančios matricos $\tilde{X}$. Nes $X = U_1 \tilde{X} V_1^{-1}$ lygybėje: $X \in GF(p)$, $U_1, V_1 \in GF(p^m)$. Jei $\tilde{X}$ priklausytų $GF(p)$, tada sprendinių skaičius sumažėtų

iki p^m. Charakteringos lygties sprendinių nebuvimas lauke $GF(p)$ neduotų jokių vaisių, rezultatai butų identiški aukščiau aprašytam charakteristikų rinkiniui, kai tikrinės reikšmės priklausė $GF(p)$. Atsakymą į šį klausimą pateiksiu pavyzdžiu.

Pavyzdys.

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} B_1 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \ \lambda_1 = 5,\ \lambda_2 = 7\,.$$

Visi sprendiniai *X*:

2.4 lentelė

Lygties sprendinių aibė GF(3)

0	0	2	0	1	0
0	0	0	1	0	2
1	1	0	1	2	1
2	0	2	1	2	2
2	2	1	2	0	2
1	0	1	1	1	2

Kadangi $\tilde{X} = U_1^{-1} X V_1$, kad rastume $\tilde{X}$, turime apskaičiuoti matricas U_1, V_1.

$$U_1 = \begin{pmatrix} 6 & 4 \\ 2 & 2 \end{pmatrix} \text{ ir } V_1 = \begin{pmatrix} 3 & 8 \\ 2 & 2 \end{pmatrix}.$$

Tada galime apskaičiuoti $\tilde{X}$, su kiekviena *X* reikšmę. Gauname tokias matricas $\tilde{X}$:

2.5 lentelė

Diagonaliųjų matricų aibė GF(32)

0	0	1	0	2	0
0	0	0	1	0	2
3	0	4	0	5	0
0	8	0	6	0	7
6	0	7	0	8	0
0	4	0	5	0	3

Matome, kad kaip ir buvo rašyta, visos matricos $\tilde{X}$ diagonalios, nes tikrinės reikšmės skirtingos. Ir $\tilde{X} \in GF(p^m)$. Tai reiškia, kad norint rasti sprendinius, reikia skaičiuoti su matricomis $\tilde{X} \in GF(p^m)$, iš apskaičiuotų $\left(p^m\right)^m$ matricų, atlikus daugybą $X = U_1 \tilde{X} V_1^{-1}$, tik p^m sprendinių priklausys $GF(p)$.

Dabar jau galime pateikti bendrus lygties $A_1X = XB_1$ sprendinių paieškos rezultatus:

1) Kai matricos $A, X, B \in GF(p)$, tikrinė pora $\lambda, x \in GF(p)$, lygtis () turi p^m sprendinių.

2) Kai matricos $A, X, B \in GF(p^m)$, tikrinė pora $\lambda, x \in GF(p^m)$, lygtis () turi $\left(p^m\right)^m$ sprendinių.

3) Kai matricos $A, X, B \in GF(p)$, tikrinė pora $\lambda, x \in GF(p^m)$, lygtis () turi p^m sprendinių, tačiau jų paieška yra sunkesnė nei pirmais dviem atvejais, nes juos atrinkti reikia iš $\left(p^m\right)^m$ elementų aibės.

$\left(p^m\right)^m = p^{m \cdot m}$. Tai reiškia, aukščiau aprašyta sprendinių paieška šitam atvejui, prilygsta matricos X pilnam perrinkimui. X turi $m \times m$ elementų, kurie gali igyti reikšmes nuo 0 iki p, X turi $p^{m \cdot m}$ skirtingų variantų, tarp kurių p^m lygties sprendinių.

2.3 LYGČIŲ SISTEMOS ANALIZĖ

Išnagrinėjome lygties $A_1X = XB_1$ sprendinių aibės galią $|S_1|$. Tačiau rakto apsikeitimo protokole figuruoja dviejų tokių lygčių sistema.

$$\begin{cases} A_1X = XB_1 \\ A_2X = XB_2 \end{cases}$$

Žinome, kiek sprendinių turi pirma ir antra lygtis, tačiau mum reikia rasti bendrąjį lygčių sistemos sprendinį, t. y. rasti $S = S_1 \bigcap S_2$, kur S_1 - pirmosios lygties sprendinių aibė , S_2 - antrosios lygties sprendinių aibė. Šiai lygčių sistemai spręsti nėra konkretaus algoritmo, todėl tenka daryti išvadas remiantis kompiuterio apskaičiavimais. Koją kiša tai, kad spręsti apie lygčių sistemos sprendinių skaičių reikia iš labai mažai duomenų. Tačiau nieko negalime padaryti, nes kompiuterių resursai yra riboti, bet neverta dėl to liūdėti, nes to mes ir siekiame, kad lygčių sistema nebūtų paprastai išsprendžiama.

Modeliuojam šią sistemą pagal pirmąjį scenarijų, kai matricos $A_1, A_2, B_1, B_2, X \in GF(p)$, tikrinės poros $\lambda_1, \lambda_2, x_1, x_2 \in GF(p)$.

Pavyzdys. Matricos $A, X, B \in GF(3)$, tikrinė pora $\lambda, x \in GF(3)$.

$$A_1 = \begin{pmatrix} 2 & 2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ B_1 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 2 \\ 2 & 1 & 0 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 2 & 1 & 0 \end{pmatrix},\ B_2 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix}$$

(2.1) matricinė lygčių sistema turi 3 sprendinius.

2.6 lentelė

Lygčių sistemos sprendinių aibė *GF(3)*

0	0	0	1	1	1	2	2	2
0	0	0	0	2	2	0	1	1
0	0	0	0	2	1	0	1	2

Gauname, kad aibių S_1 ir S_2 galia $|S_1| = |S_2| = 3^3 = 27$. Sprendinių aibės galia $|S| = 3$.

Antrojo scenarijaus, kai matricos $A_1, A_2, B_1, B_2, X \in GF(p^m)$ ir tikrinės poros $\lambda_1, \lambda_2, x_1, x_2 \in GF(p^m)$, nenagrinėsime, nes skaičiuojasi taip pat, kaip ir lauke $GF(p)$, tik reikia atsižvelgti į lauko charakteristikas bei matricos eilę.

Modeliuojam šią sistemą pagal trečiąjį scenarijų, kuris davė geriausius rezultatus.

Pavyzdys. Matricos $A, X, B \in GF(3)$, tikrinė pora $\lambda, x \in GF(3^2)$.

$$A_1 = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}, B_1 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 1 & 1 & 0 \end{pmatrix}, B_2 = \begin{pmatrix} 2 & 2 & 0 \\ 1 & 0 & 2 \\ 2 & 2 & 1 \end{pmatrix}$$

2.7 lentelė

Visi *X* sprendiniai

S₁									***S₂***								
0	0	0	2	1	0	1	2	0	0	0	0	1	1	0	2	2	0

0	0	0	1	1	0	2	2	0		0	0	0	1	2	0	2	1	0
0	0	0	0	2	1	0	1	2		0	0	0	0	2	1	0	1	2
0	0	1	2	1	1	1	2	1		2	0	1	0	1	1	1	2	1
0	1	0	1	2	0	2	0	0		1	0	0	2	2	0	0	1	0
2	1	0	2	0	1	2	2	2		1	2	0	1	1	1	1	0	2
0	0	2	2	1	2	1	2	2		1	0	2	2	1	2	0	2	2
0	2	0	1	0	0	2	1	0		2	0	0	0	2	0	1	1	0
1	2	0	1	1	1	1	0	2		2	1	0	2	0	1	2	2	2
0	1	0	2	2	0	1	0	0		0	1	0	1	2	0	2	0	0
1	1	1	2	2	1	0	0	1		0	0	1	1	2	1	2	1	1
1	1	0	1	0	1	1	2	2		2	0	0	2	2	1	2	1	2
0	1	1	2	2	1	1	0	1		2	1	1	0	2	1	1	0	1
1	2	1	2	0	1	0	1	1		1	0	1	2	2	1	0	1	1
0	2	0	0	1	1	0	0	2		0	2	0	0	1	1	0	0	2
0	1	2	2	2	2	1	0	2		1	1	2	2	2	2	0	0	2
1	0	1	2	1	1	0	2	1		2	0	1	0	2	1	1	1	1
2	0	0	2	2	1	2	1	2		1	1	0	1	0	1	1	2	2
0	2	0	2	0	0	1	1	0		0	2	0	1	0	0	2	1	0
2	2	2	0	0	2	1	1	2		0	0	2	1	2	2	2	1	2
2	2	0	2	1	1	2	0	2		1	0	0	1	2	1	1	1	2
0	2	1	2	0	1	1	1	1		2	2	1	0	0	1	1	1	1
2	0	2	0	1	2	1	2	2		1	0	2	2	2	2	0	1	2
1	0	0	1	2	1	1	1	2		2	2	0	2	1	1	2	0	2
0	2	2	2	0	2	1	1	2		1	2	2	2	0	2	0	1	2
2	1	2	0	2	2	1	0	2		2	0	2	0	2	2	1	1	2
0	1	0	0	0	1	0	2	2		0	1	0	0	0	1	0	2	2

Aibių S_1 ir S_2 galia $|S_1| = |S_2| = 3^3 = 27$. Sprendinių aibės galia $|S| = 3$.

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in S$$

Patikriname antrąjį sprendinį:

$$\begin{cases}\begin{pmatrix}2&0&1\\1&0&1\\0&1&2\end{pmatrix}\begin{pmatrix}2&0&2\\0&2&2\\0&0&1\end{pmatrix}=\begin{pmatrix}2&0&2\\0&2&2\\0&0&1\end{pmatrix}\begin{pmatrix}2&1&0\\1&1&2\\0&2&1\end{pmatrix}\\ \begin{pmatrix}1&1&1\\0&2&2\\1&1&0\end{pmatrix}\begin{pmatrix}2&0&2\\0&2&2\\0&0&1\end{pmatrix}=\begin{pmatrix}2&0&2\\0&2&2\\0&0&1\end{pmatrix}\begin{pmatrix}2&2&0\\1&0&2\\2&2&1\end{pmatrix}\end{cases}$$

Atliekame veiksmus:

$$\begin{cases}\begin{pmatrix}2\cdot2+0\cdot0+1\cdot0&2\cdot0+0\cdot2+1\cdot0&2\cdot2+0\cdot2+1\cdot1\\1\cdot2+0\cdot0+1\cdot0&1\cdot0+0\cdot2+1\cdot0&1\cdot2+0\cdot2+1\cdot1\\0\cdot2+1\cdot0+2\cdot0&0\cdot2+1\cdot2+2\cdot0&0\cdot2+1\cdot2+2\cdot1\end{pmatrix}=\begin{pmatrix}2\cdot2+0\cdot1+2\cdot0&2\cdot1+0\cdot1+2\cdot2&2\cdot0+0\cdot2+2\cdot1\\0\cdot2+2\cdot1+2\cdot0&0\cdot1+2\cdot1+2\cdot2&0\cdot0+2\cdot2+2\cdot1\\0\cdot2+0\cdot1+1\cdot0&0\cdot1+0\cdot1+1\cdot2&0\cdot0+0\cdot2+1\cdot1\end{pmatrix}\\ \begin{pmatrix}1\cdot2+1\cdot0+1\cdot0&1\cdot0+1\cdot2+1\cdot0&1\cdot2+1\cdot2+1\cdot0\\0\cdot2+2\cdot0+2\cdot0&0\cdot0+2\cdot2+2\cdot0&0\cdot2+2\cdot2+2\cdot0\\1\cdot2+1\cdot0+0\cdot0&1\cdot0+1\cdot2+0\cdot0&1\cdot2+1\cdot2+1\cdot0\end{pmatrix}=\begin{pmatrix}2\cdot2+0\cdot1+2\cdot2&2\cdot2+0\cdot0+2\cdot2&2\cdot0+0\cdot2+2\cdot1\\0\cdot2+2\cdot1+2\cdot2&0\cdot2+2\cdot0+2\cdot2&0\cdot0+2\cdot2+2\cdot1\\0\cdot2+0\cdot1+1\cdot2&0\cdot2+0\cdot0+1\cdot2&0\cdot0+0\cdot2+1\cdot1\end{pmatrix}\end{cases}$$

Suskaičiuojame:

$$\begin{cases}\begin{pmatrix}1&0&2\\2&0&0\\0&2&1\end{pmatrix}=\begin{pmatrix}1&0&2\\2&0&0\\0&2&1\end{pmatrix}\\ \begin{pmatrix}2&2&2\\0&1&0\\2&2&1\end{pmatrix}=\begin{pmatrix}2&2&2\\0&1&0\\2&2&1\end{pmatrix}\end{cases}$$

Lygtis išspręsta teisingai, jos sprendinys:

$$X=\begin{pmatrix}2&0&2\\0&2&2\\0&0&1\end{pmatrix}$$

Dabar patikrinsime, kuriam laukui priklauso matricos $\tilde{X}$, jei $\tilde{X}\in GF(p)$, kiekviena iš lygčių taptų lengvai išsprendžiamos, t. y. pagal aukščiau aprašytą sprendimo algoritmą, greitai rastume aibės S_1 ir S_2, užtektų rasti tik jų sankirtą S.

Kadangi $\tilde{X}=U_1^{-1}XV_1$, kad rastume $\tilde{X}$, turime apskaičiuoti matricas U_1,V_1. U_2,V_2.

$$U_1=\begin{pmatrix}23&26&18\\10&17&14\\2&2&2\end{pmatrix}\text{ ir }V_1=\begin{pmatrix}17&14&10\\18&23&26\\2&2&2\end{pmatrix}.\ U_2=\begin{pmatrix}17&10&14\\24&21&19\\2&2&2\end{pmatrix}\text{ ir }V_2=\begin{pmatrix}5&4&3\\16&9&13\\2&2&2\end{pmatrix}$$

Tada galime apskaičiuoti $\tilde{X}$, su kiekviena X reikšme. Gauname tokias matricas $\tilde{X}$:

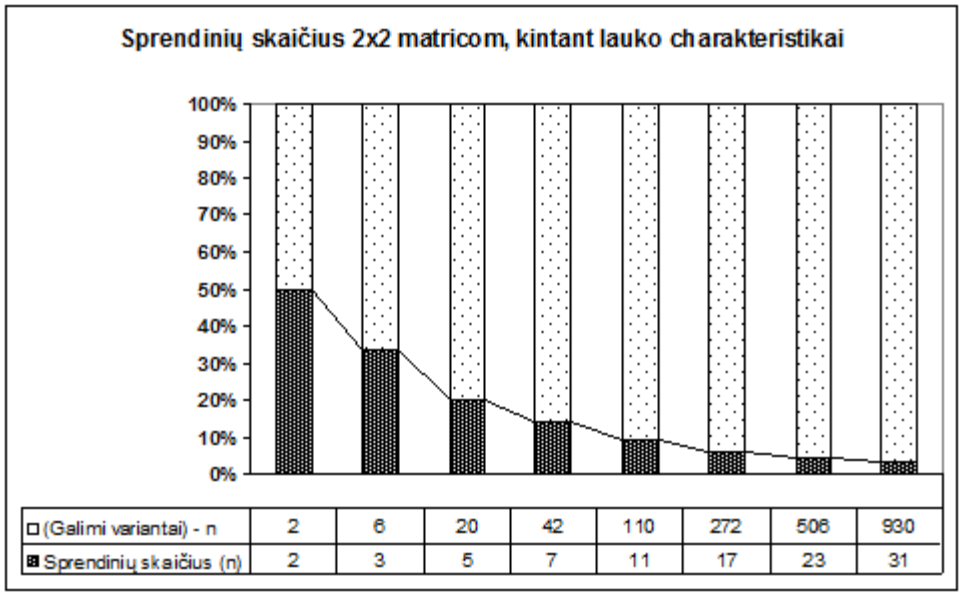
$$\tilde{X}_1: \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 21 & 0 & 0 \\ 0 & 19 & 0 \\ 0 & 0 & 24 \end{pmatrix}, \begin{pmatrix} 15 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

$$\tilde{X}_2: \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 25 & 0 & 0 \\ 0 & 20 & 0 \\ 0 & 0 & 22 \end{pmatrix}, \begin{pmatrix} 14 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 17 \end{pmatrix}$$

Matricos $\tilde{X}$ priklauso $GF(3^2)$.

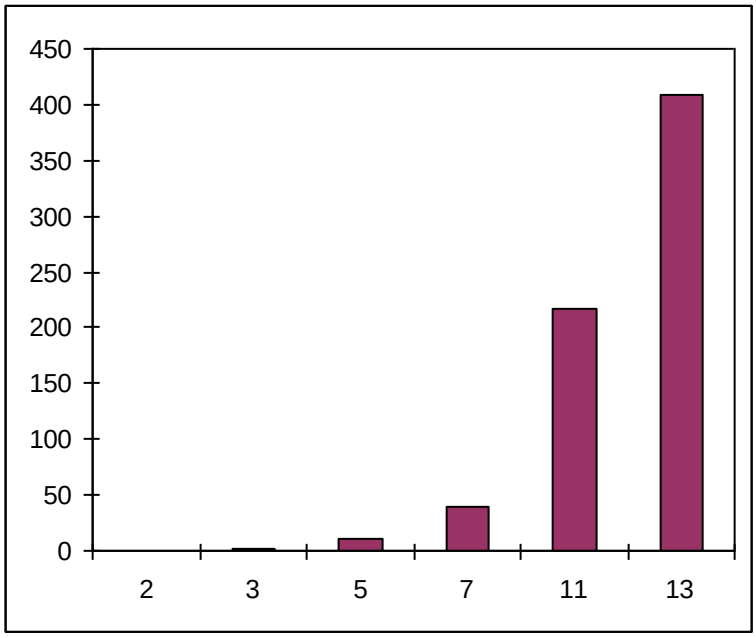
Matome, kad kaip ir buvo rašyta, visos matricos $\tilde{X}$ diagonalios, nes tikrinės reikšmės skirtingos, išskyrus trivialųjį sprendinį. Ir $\tilde{X} \in GF(p^m)$. Tai reiškia, kad norint rasti sprendinius, reikia skaičiuoti su matricomis $\tilde{X} \in GF(p^m)$, iš apskaičiuotų $\left(p^m\right)^m$ matricų, atlikus daugyba $X = U_1 \tilde{X} V_1^{-1}$, tik p^m sprendinių priklausys $GF\left(p\right)$.

2.1 pav. pateikiau kokią dalį sudaro sprendiniai tarp visų galimų variantų matricom $A, B \in GF(2)$.



2.1 pav. Sprendinių skaičiaus santykis su galimais variantais

Viena iš didžiausių kliūčių sprendinių paieškai yra ilga skaičiavimo trukmė, **2.2 pav** pateikiau, kaip ilgėja skaičiavimo trukmė, keičiant lauko charakteristiką *p*. Matricos $A, B \in M_2$.



2.2 pav. Sprendinių paieškos trukmė (*s*), kintant lauko charakteristikai *p*

2.8 lentelė

Skaičiavimo trukmės

m \ p	2	3	4
2	0.3	16.5	4000
3	1.5	639	$2{,}6\cdot10^{6}$
5	11.3	55500	$9.3\cdot10^{9}$
7	39	$1{,}2\cdot10^{6}$	$2.03\cdot10^{12}$
11	216	$7{,}2\cdot10^{7}$	$2.8\cdot10^{15}$
13	408	$3.26\cdot10^{8}$	$4.06\cdot10^{16}$

Lentelėje pateiktos kitos skaičiavimo trukmės (*s*). Skaičiavimai atlikti 2 x 2,2 GHz procesuriumi, 4 GB (RAM). Darbo užduotis – tyrinėti sprendinius, o ne kuo greičiau juo rasti, todėl programiniai algoritmai nėra greičiausi. Galima juos tobulinti, kad skaičiuotų greičiau, tačiau laiko trukmės toliau sparčiai didės, didėjant lauko charakteristikai *p* ir matricos eilei *m*.

3. PROGRAMINĖ REALIZACIJA IR INSTRUKCIJA VARTOTOJUI

3.1 PROGRAMOS VEIKIMO PRINCIPAS

Lygčių sistemos sprendimas sumodeliuotas matematinio paketo Matlab (2009b) aplinkoje. Sukurta visa bazė, reikalinga skaičiavimams baigtiniuose laukuose. Sukurtos tokios funkcijos:

1) *kintamieji.m* (visiems reikalingiems kintamiesiems vartotojas priskiria reikšmes, taip pat iškviečia kitas funkcijas, reikalingas sprendžiant lygčių sistemą)
2) *brute.m* (matricų pilno perrinkimo algoritmas)
3) *inverse.m* (suskaičiuoja atvirkštinį elementą)
4) *determinant.m* (skaičiuoja matricos determinantą)
5) *invM.m* (randa atvirštinę matricą)
6) *tikrinės.m* (randa matricos tikrines reikšmes)
7) *laipsnis.m* (kelia matricą laipsniu)
8) *eigen.m* (randa matricą sudarytą is tikrinių vektorių)
9) *patikrinimas.m* (ieško bendrų dviem aibėm sprendinių)
10) *decbit.m* (desimtainių skaičių vektorinis vaizdavimas)
11) *bitdec.m* (vektorių atvaizdavimas į dešimtainius skaičius)
12) *plius.m* (baigtinių skaičių sudėtis)
13) *minius.m* (baigtinių skaičių „atimtis“)
14) *kart.m* (baigtinių skaičių sandauga)
15) *dalyba.m* (baigtinių skaičių „dalyba“)
16) *kartM.m* (matricų daugyba)

Naudojant šias funkcijas, galima spręsti ne vien mano konkretų uždavinį, nesunkiai programą galima adaptuoti ir kitokiem tyrimam Galua lauke.

3.2 INSTRUKCIJA VARTOTOJUI

Darbą pradedame faile *kintamieji.m*. Šis failas suskirstytas į 7 ląsteles:

1) Kintamųjų parinkimas ir matricų generavimas.

Pasirenkame lauko ir matricų charakteristikas:

p – pagrindinio lauko dydis

m – matricos eilė

n – pasirenkame norėdami atlikti veiksmus praplėstame lauke (p^n).

Paspaudus ląstelės paleidimo mygtuką, kintamieji priskiriami visai programai, taip pat sugeneruojamos $m \times m$ matricos: $A_1, A_2, X \in GF(p^n)$.

2) Tikrinių reikšmių skaičiavimas praplestame lauke.

Suskaičiuojamos tikrinės reikšmės matricų A_1, A_2 ir jos priskiriamos *alfa1* ir *alfa2* vektoriams.

3) Grįžimas prie pagrindinio lauko.

Prieš ieškant matričų B_1, B_2, skaičiavimai perjungiami į lauką $GF(p)$.

4) B apskaičiavimas su tam tikru X.

Apskaičiuojamos matricos B_1, B_2 su konkrečia X reikšme, kad tikrai egzistuotų sprendinys.

$$B_1 = X^{-1} A_1 X$$
$$B_2 = X^{-1} A_2 X$$

5) Tikrinių vektorių matricų V, U radimas

Randamos U ir V, su kuriomis

$A_1 = U_1 \tilde{A}_1 U_1^{-1}, B_1 = V_1 \tilde{B}_1 V_1^{-1}$,

6) Sprendinių paieška pilno perrinkimo būdu.

Funkcija *brute.m* perrenkamos visos galimos *X* reikšmės. Pirmosios lygties sprendinių aibė surašoma į didelę matricą S_1, antrosios – į S_2. Funkcija *patikrinimas.m* suskaičiuoja, kiek abi sprendinių aibės turi bendrų sprendinių, prireikus gali ir juos pateikti.

7) Srendinių paieška kitu metodu.

Perrenkamos visos galimos $\tilde{X}$ reikšmės. Tada iš lygybės $X = U_1 \tilde{X} V_1^{-1}$ randami visi *X*, priklausantys *S1*. O iš $X = U_2 \tilde{X} V_2^{-1}$ randami *X*, priklausantys *S2*

IŠVADOS

1) Tiriant vienos lygties sprendinių aibės galią gauta, kad lygtis $A_1X = XB_1$ turi p^m sprendinių.
2) Tiriant dviejų lygčių sistemos

$$\begin{cases} A_1X = XB_1 \\ A_2X = XB_2 \end{cases}$$

sprendinių aibės galią, nustatyta, kad sistema turi *p* sprendinių,
3) Reiškia lygčių sistemos sprendinių skaičius nepriklauso nuo matricos eilės *m*, o priklauso nuo lauko charakteristikos *p*.
4) Sprendinių sankirtos aibę rasti neįmanoma, nes šios aibės galios santykis su pavienės lygties sprendinių aibės galia nykstamai mažėja kai *m* didėja.
5) 2^{80} yra riba, po kurios aibė tampa neperrenkama. $2^{80} \approx 17^{20}$. Lauke $GF(17)$, kai matricos eile $m = 20$, gauname, kad pavienės lygties sprendinių aibės negalėsime patikrinti ieškant 17 sprendinių.
6) Gauti rezultatai leidžia teikti, kad lygčių sistema, gali būti kandidatė pritaikymui kriptografiniams algoritmams.

LITERATŪRA

1) KATVICKIS, A. *Rakto apsikeitimo protokolas ir galimos jo atakos.* http://kpst.elen.ktu.lt/studentai/_media/katvickis_rap.pdf, 2008

2) KVEDARAS, B., *Matricų teorija*. Kaunas, 1999.

3) LIDL, R. *Introduction to finite fields and their applications*. Cambridge, 1986.

4) MACHER, G., *Matrix Theory*. Chelsea, 1959.

5) MEYER, C. *Matrix analysis and applied linear algebra*. Philadephia, 2000.

6) POOLE, D., *Linear Algebra. A Modern Introduction*. Toronto, 2005.

7) SAKALAUSKAS, E., LISTOPADSKIS,, N., DOSINAS, G. S., *Kriptografijos teorija. Kaunas, 2008.*

8) SAKALAUSKAS, ir kt., *Kriptografinės sistemos*. Kaunas, 2008.

PRIEDAI

Failas ***kintamieji.m***

```
%% Kintam?j? parinkimas ir matric? generavimas
global field
global p
global n
global prim_poly
global m
m = 2
p = 5
n = 1
X1 = randint(m,m,p^n)
A1 = randint(m,m,p^n)
A2 = randint(m,m,p^n)

%% Tikrini? reikšmi? skaiciavimas praplestame lauke
n=m
prim_poly = gfprimdf(n,p)
field = gftuple([-1:p^n-2]',prim_poly,p);
[alfa1]=tikrines(A1)
[alfa2]=tikrines(A2)
invM(X1)
%% Gr?žimas prie pagrindinio lauko
n = 1
prim_poly = gfprimdf(n,p)
field = gftuple([-1:p^n-2]',prim_poly,p);
%% B apskai?iavimas su tam tikru X
B1 = kartM(kartM(invM(X1),A1),X1)
B2 = kartM(kartM(invM(X1),A2),X1)
%% Tikrini? vektori? V, U radimas
[V1]=eigen(B1,alfa1)
[U1]=eigen(A1,alfa1)
[V2]=eigen(B2,alfa2)
[U2]=eigen(A2,alfa2)

%% Sprendini? paieška brute force
t = cputime;
[Xn1,count1]=brute(A1,B1)
e=cputime -t
[Xn2,count2]=brute(A2,B2)
%count1
%count2
%[sk, BB]=patikrinimas(Xn1,Xn2)

%% Srendiniu paieska kitu metodu
BB1=[0 0]
for i=2:m:size(Xn1,1)
    B=Xn1([i:i+m-1],:)
    BB1=vertcat(BB1,kartM(kartM(invM(U1),B),V1));
end
BB2=[0 0]
for i=2:m:size(Xn1,1)
    B=Xn2([i:i+m-1],:)
    BB2=vertcat(BB2,kartM(kartM(invM(U2),B),V2));
end
BB1
```

Failas ***determinant.m***

```
function [d]=determinant(X)
global p;
m=size(X,1);
if (m==2)
    d=minius(kart(X(1,1),X(2,2)),kart(X(1,2),X(2,1)));
    return
else
d=0;
for r=1:m
    h=1;
    k=1;
    for i=2:m
        for j=1:m
             if(j==r)
                 continue
             end
            C(h,k)=X(i,j);
            k=k+1;
            if(k==m)
                h=h+1;
                k=1;
            end
        end
    end
   d=plius(d, kart(X(1,r),kart(mod((-1)^(r+1),p),determinant(C))));
end
end
```

Failas *invM.m*

```
function [A]=invM(M)
global p;
m=size(M,1);
if(m==2)
    A=[M(2,2) kart(minius(0,1),M(1,2)); kart(minius(0,1),M(2,1)) M(1,1)];
    A=kartM(inverse(determinant(M)),A);
else
    for i=1:m
        for j=1:m
            B=M;
            B(:,j)=[];
            B(i,:)=[];
            A(i,j)=kart(mod((-1)^(j+i),p),determinant(B));
        end
    end
    A=kartM(inverse(determinant(M)),A');
end
```