

VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
TIKIMYBIŲ TEORIJOS IR SKAIČIŲ TEORIJOS KATEDRA

Saulius Lipkevičius

**Kinų liekanų teorema ir paslapties pasidalijimo
schemos**
**Chinese Remainder Theorem and Secret Sharing
Schemes**

Bakalauro baigiamasis darbas

Leidžiu ginti

Darbo vadovas doc. Vilius Stakėnas

Vilnius 2020

Turiny

Įvadas	2
1 Teorinė dalis	4
1.1 Pagrindiniai apibrėžimai ir sąvokos	4
1.2 Bezout tapatybė	7
1.3 Kinų liekanų teoremos įrodymas	8
1.4 Paslapties pasidalijimo schemas	10
1.5 Asmuth-Bloomo schema	10
1.6 Asmuth-Bloomo schema daugianariams virš baigtinio kūno	12
2 Praktinė dalis	14
2.1 Asmuth-Bloomo paslapties padalijimo schemas paslapties atkūrimas .	14
Summary	19
Literatūra	20

Ivadas

Kinų liekanų teorema, pagrįsta „Pars pro toto“ (liet. *dalis vietoj visumos*) principu, laikoma matematiniu perlu ir kelia klausimą – ką tiriamo objekto dalis gali pasakyti apie patį objektą. Pirmąją kartą kinų liekanų teorema pasirodė kinų matematiko Sun Zie knygoje maždaug trečiame amžiuje [3]: teorema pradėta taikyti paprastuose vienetų skaičiavimuose, pavyzdžiui, kaip armijos dydis, tačiau ir šiandien randami nauji teoremos pritaikymo tipai.

Šio darbo tikslas susideda iš dviejų krypčių: visų pirma, bus pateikiami pagrindiniai apibrėžimai ir teiginiai, reikalingi įrodyti kinų liekanų teorema, kuria yra grindžiama vėliau pristatoma Asmuth-Bloomo slenkstinė paslapties pasidalijimo schema. Antra, bus rašomos programos, pirma padalinti paslapties dalis, kita padėsianti atskleisti schemas paslaptį.

Teorinėje šio darbo dalyje bus pateikiamos pagrindinės sąvokos ir apibrėžimai, kurie padės įrodyti kinų liekanų teorema. Remiantis šios teoremos įrodymu, bus pristatoma slenkstinė Asmuth-Bloomo paslapties pasidalijimo schema daugianariams virš baigtinio kūno. Vėliau praktinėje dalyje bus pateikiamas programos kodas, padedantis atkurti slenkstinės Asmuth-Bloomo paslapties pasidalijimo schemas paslaptį.

1 skyrius

Teorinė dalis

1.1 Pagrindiniai apibrėžimai ir sąvokos

Prieš pradedant nagrinėti kūnus, apibrėžiamas žiedas.

1 apibrėžimas. Aibę $\mathbb{A}$ su joje apibrėžtomis jos elementų sudėties $+$ ir daugybos $*$ atžvilgiu, vadinsime žiedu, jei

1. Sudėtis $+$ yra asociatyvi: bet kuriems $x, y, z \in \mathbb{A}$, $(x + y) + z = x + (y + z)$.
2. Egzistuoja neutralus elementas 0 sudėties $+$ atžvilgiu: kiekvienam $x \in \mathbb{A}$, $x + 0 = 0 + x = x$.
3. Kiekvienam aibės A elementui x egzistuoja simetrinis elementas y sudėties $+$ atžvilgiu: $x + y = y + x = 0$. Elementui x sudėties $+$ atžvilgiu simetrinį elementą žymėsime $-x$ ir vadinsime priešingu elementu elementui x .
4. Sudėtis $+$ yra komutatyvi: bet kuriems $x, y \in \mathbb{A}$, $x + y = y + x$.
5. Daugyba $*$ yra asociatyvi: bet kuriems $x, y, z \in \mathbb{A}$, $(x * y) * z = x * (y * z)$.
6. Sudėtis $+$ ir daugyba $*$ yra susijusios distributyvumo dėsniais: bet kuriems $x, y, z \in \mathbb{A}$, $(x + y) * z = x * z + y * z$, $z * (x + y) = z * x + z * y$.

2 apibrėžimas. Komutatyvusis žiedas $(\mathbb{A}, +, *)$ su vienetu 1 vadinamas kūnu, jei kiekvienam $x \in \mathbb{A}$, $x \neq 0$, egzistuoja atvirkštinis elementas $x^{-1} \in \mathbb{A}$.

Jeigu p – pirminis skaičius, tai sveikųjų skaičių moduliu p aibė sudaro baigtinį kūną iš p elementų $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, šiame kūne operacijos atliekamos moduliu

p , pavyzdžiui, kūne $\mathbb{F}_3 = \{0, 1, 2\}$ gauname, kad $1 + 2 = 3 \equiv 0 \pmod{3}$, o daugyboje $2 \cdot 2 = 1$, nes $2 \cdot 2 = 4 \equiv 1 \pmod{3}$. [2] Apibrėžiamas kūnas, turintis baigtinį skaičių elementų, vadinamas baigtiniu kūnu.

Pažymėkime daugianarių aibę, kurią naudosime viso darbo eigoje:

$$\mathbb{F}_p[x] = \{a_0 + a_1x + \dots + a_mx^m : a_i \in \mathbb{F}_p, a_m \neq 0; 0 \leq m\}.$$

Toliau apibrėžiamos svarbiausios charakteristikos, reikalingos atlikti veiksmus su šios aibės elementais, t.y. daugianariais virš baigtinio kūno $\mathbb{F}_p$.

3 apibrėžimas. Fiksuojamas piminis skaičius p , tuomet

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{F}_p[x], \text{ kur } a_i \in \mathbb{F}_p, a_n \neq 0$$

vadinsime kintamojo x daugianariu (polinomu) su koeficientais virš kūno $\mathbb{F}_p$. Didžiausio laipsnio narį a_n vadinsime vyriausiuoju nariu, o jo laipsnį daugianario laipsniu, kuri žymėsime $\deg(f(x)) = n$. Nulinio daugianario laipsnis yra $\deg[0] := -\infty$.

4 apibrėžimas. Polinomial

$$f(x) = \sum_{0 \leq j} a_j x^j \text{ ir } g(x) = \sum_{0 \leq j} b_j x^j \in \mathbb{F}_p,$$

jų suma ir sandauga yra apibrėžiamos taip:

$$\begin{aligned} f(x) + g(x) &= \sum_{0 \leq j} (a_j + b_j) x^j \in \mathbb{F}_p[x], \\ f(x) \cdot g(x) &= \sum_{0 \leq j} \left(\sum_{\substack{r+s=j, \\ 0 \leq r,s}} a_r \cdot b_s \right) x^j \in \mathbb{F}_p[x]. \end{aligned}$$

Daugianario daugyba iš $t \in \mathbb{F}_p$:

$$(t \cdot g)(x) = (tb_0) + (tb_1)x + \dots + (tb_m)x^m \in \mathbb{F}_p[x].$$

Dalybos liekanos teorema galioja ir daugianariams virš baigtinio kūno.

5 teorema. Tegul $f(x), g(x) \in \mathbb{F}_p[x]$ yra du daugianariai, $\deg(g(x)) < \deg(f(x))$.

Tada egzistuoja vienintelė daugianarių pora $q(x), r(x) \in \mathbb{F}_p[x]$, kad

$$f(x) = q(x)g(x) + r(x), \quad 0 \leq \deg(r) < \deg(g).$$

6 apibrėžimas. Tegul $f(x), g(x) \in \mathbb{F}_p[x]$, polinomas $g(x)$ dalija polinomą $f(x)$ (arba polinomas $g(x)$ yra $f(x)$ daliklis) ir žymėsime $g(x)|f(x)$, jei egzistuoja toks $h(x) \in \mathbb{F}_p[x]$, kad $f(x) = g(x) \cdot h(x)$.

7 apibrėžimas. Didžiausio laipsnio polinomas $f(x) \in \mathbb{F}_p[x]$, vadinamas nenuliniu polinomu $g_1(x), g_2(x) \in \mathbb{F}_p[x]$ didžiausiu bendruoju dalikliu ir žymimas $dbd(g_1(x), g_2(x))$ arba $(g_1(x), g_2(x))$, jei

1. $f(x)|g_1(x), f(x)|g_2(x)$;
2. Jei $h(x) \in \mathbb{F}_p[x]$ ir $h(x)|g_1(x), h(x)|g_2(x)$, tai $h(x)|f(x)$.

8 apibrėžimas. Nenulinis polinomas $p(x) \in \mathbb{F}_p[x]$, vadinamas redukuojamu virš kūno $\mathbb{F}_p$, jei egzistuoja tokie polinamai $f(x), g(x) \in \mathbb{F}_p[x]$, kad

- $p(x) = f(x)g(x)$,
- $0 < \deg(f(x)) < \deg(p(x))$,
- $0 < \deg(g(x)) < \deg(p(x))$.

Polinomas $p(x) \in \mathbb{F}_p[x]$, $\deg(p(x)) > 1$, vadinamas neredukuojamu (pirminiu) virš kūno $\mathbb{F}_p$, jei jis nėra redukuojamas – jo neįmanoma išskaidyti į dviejų polinomų $f(x), g(x) \in \mathbb{F}_p[x]$, kurių laipsniai mažesni už $p(x)$ laipsnį, sandaugą $f(x) \cdot g(x)$.

9 pavyzdys. Polinomas $f(x) = x^2 - 2 \in \mathbb{F}_3[x]$ yra neredukuojamas (pirminis) virš baigtinio kūno $\mathbb{F}_3$, nes polinomas neišsiskaido šiame kūne.

Toliau pateikiami lyginių apibrėžimai ir teiginiai, kurie yra reikalingi įrodyti kinų liekanų teoremą.

10 apibrėžimas. Tegul $a, b, c \in \mathbb{Z}$. Jei skirtumas $a - b$ dalijasi iš c , tai rašysime $a \equiv b \pmod{c}$. Taigi $a \equiv b \pmod{c} \iff c|a - b$, o $a \equiv b \pmod{c}$ vadinsime lyginiu. Be to, a ir b vadinami kongruenčiais moduliu c .

11 teiginys. Su visais $a, b, c, d, e \in \mathbb{Z}$ teisingi šie lyginiai:

1. $a \equiv a \pmod{b}$.
2. Jei $a \equiv b \pmod{c}$ ir $d \equiv e \pmod{c}$, tai $a \pm d \equiv b \pm e \pmod{c}$ ir $a \cdot d \equiv b \cdot e \pmod{c}$.
3. Jei $d \neq 0$, tai $a \cdot d \equiv b \cdot d \pmod{c \cdot d} \iff a \equiv b \pmod{c}$.
4. Jei $(c, d) = 1$, tai $a \cdot d \equiv b \cdot d \pmod{c} \iff a \equiv b \pmod{c}$,

kur $dbd(c_i, c_j) = 1$, kai $i \neq j$.

12 apibrėžimas. Tegul $a, b, c \in \mathbb{Z}$, lyginių sistema:

$$\begin{aligned} a_1x &\equiv b_1 \pmod{c_1} \\ a_2x &\equiv b_2 \pmod{c_2} \\ &\vdots \\ a_nx &\equiv b_n \pmod{c_n}, \end{aligned} \tag{1.1}$$

kur $\text{dbd}(c_i, c_j) = 1$, kai $i \neq j$. x vadinsime sistemos sprendiniu, jei jis yra kiekvieno tos sistemos lyginio sprendinys. Dvi lyginių sistemos vadinamos ekvivalenčiomis, jei jų sprendinių aibės sutampa.

(10), (12) apibrėžimus ir (11) teiginį galima apibendrinti ir daugianariams virš baigtinio kūno.

1.2 Bezout tapatybė

13 teiginys. Tegul $f(x)$ ir $g(x) \in \mathbb{F}_p[x]$, kurių didžiausias bendrasis daliklis yra $d(x) \in \mathbb{F}_p[x]$, tada egzistuoja $a(x), b(x) \in \mathbb{F}_p[x]$ tokie, kad

$$f(x)a(x) + g(x)b(x) = d(x), \tag{1.2}$$

reiškiniai formos $f(x)a(x) + g(x)b(x)$ yra tiksliai $d(x)$ kartotiniai, be to daugianarius $a(x)$ ir $b(x)$, kurie nėra unikalūs, vadinsime Bezout koeficientais.

14 pavyzdys. Tegul $f(x) = 2x^4 + x^3 + 2$, $g(x) = x^4 + 2 \in \mathbb{F}_3[x]$ du ketvirto laipsnio polinamai, kurie išskaidomi baigtiniame kūne $\mathbb{F}_3$. Pasinaudojus Euklido algoritmu, kuris aprašytas knygoje [5], puslapiuose 285-287, randamas šių polinomų didžiausias bendrasis daliklis:

$$\begin{aligned} 2x^4 + x^3 + 2 &= (x^4 + 2)(2) + (x^3 + 1), & r_0(x) &= x^3 + 1 \\ x^4 + 2 &= (x^3 + 1)(x) + (2x + 2), & r_1(x) &= 2x + 2 \\ x^3 + 1 &= (2x + 2)(2x^2 + x + 2) + (0), & r_2(x) &= 0, \end{aligned} \tag{1.3}$$

taigi paskutinė nelygi nuliui liekana $r_1 = \text{dbd}(f(x), g(x)) = 2x + 2$. Iš (1.3) išreiškiamos liekanos $r_0(x), r_1(x)$ atitinkamai per $f(x), g(x)$:

$$2x + 2 = x^4 + 2 - (x^3 + 1)(x) \tag{1.4}$$

$$x^3 + 1 = 2x^4 + x^3 + 2 - (x^4 + 2)(2) \tag{1.5}$$

išreiškus (1.4) lygtį per (1.5):

$$\begin{aligned} 2x + 2 &= x^4 + 2 - (x^3 + 1)(x) \\ &= x^4 + 2 - (2x^4 + x^3 + 2 - (x^4 + 2)(2))(x) \\ &= (2x^4 + x^3 + 2)(-x) + (x^4 + 2)(1 + 2x) \end{aligned}$$

gaunami Bezout koeficientai polinomų porai $f(x)$, $g(x)$, atitinkamai $a(x) = -x$, $b(x) = 2x + 1 \in \mathbb{F}_3$.

1.3 Kinų liekanų teoremos įrodymas

15 teorema. [6] Tegu $n = m_1 m_2 \cdots m_k$, kur visi m_i yra paporiui tarpusavyje pirminiai. Visiems sveikiesiems $r_1, r_2, \dots, r_k$ lyginių sistema

$$\begin{cases} x \equiv x_1 \pmod{m_1} \\ x \equiv x_2 \pmod{m_2} \\ \vdots \\ x \equiv x_k \pmod{m_k} \end{cases}$$

turi vienintelį sprendinį intervale $[0, n - 1]$. Įrodymas. Pirmiausia įrodykime, kad bent vieną sprendinį turi paprastesnė lyginių sistema:

$$\begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \vdots \\ x \equiv 0 \pmod{m_k} \end{cases}$$

Išties, kadangi m_1 ir $m_2 m_3 \cdots m_k$ yra tarpusavyje pirminiai, t.y. jų didžiausias bendras daliklis yra lygus 1, tai pagal Euklido algoritmo išvadą (arba kitaip Bezout tapatybę) egzistuoja tokie sveikieji x ir y , kad $xm_1 + ym_2 m_3 \cdots m_k = 1$. Skaičius $ym_2 m_3 \cdots m_k$ kaip tik ir bus sprendinys. Pažymėkime jį e_1 . Išsprendę analogiškas sistemas, kur liekana 1 atitiks vis kitą m_i gausime k skaičių $e_1, e_2, \dots, e_k$. Nesunku įsitikinti, kad sudauginę paporiui $e_1 r_1 + e_2 r_2 + \dots + e_k r_k$ gausime pradinės sistemos sprendinį. Parodysime, kad visi sistemos sprendiniai skiriasi per n kartotinį. Tarkime, kad turime du sistemos sprendinius r ir r' . Jie duoda vienodas liekanas dalijami iš visų m_i , todėl $m_1 | (r - r'), m_2 | (r - r'), \dots, m_k | (r - r')$. Kadangi visi m_i yra paporiui tarpusavyje pirminiai, tai gauname, kad $n | (r - r')$. Galiausiai pastebėkime, kad jei

prie vieno sprendinio pridėsime ar atimsime n , gausime kitą sprendinį. Tai ir įrodo, kad bus lygiai vienas sprendinys intervale $[0, n - 1]$.

Be to, teorema gali būti apibendrinta ir polinomams virš baigtinio kūno $\mathbb{F}_p$.

16 teorema. [4] Tegul F kūnas ir $m_1(x), \dots, m_n(x) \in \mathbb{F}_p[x]$ yra tarpusavyje pirminiai. Daugianariams $s_1(x), \dots, s_n(x) \in \mathbb{F}_p[x]$ egzistuoja toks $f(x)$, kad

$$f(x) \equiv s_i(x) \pmod{m_i(x)}, \quad \forall i = 1, 2, \dots, n$$

ir $f(x)$ yra unikalus, jeigu $g(x)$ kitas sprendinys tenkinantis lyginių sistemą, tada:

$$f(x) \equiv g(x) \pmod{\prod_{i=1}^n m_i(x)}.$$

Reikia pabrėžti, kad $f(x)$ unikalus tik jeigu kalbame apie polinomus laipsnio mažesnius už $\sum_{i=1}^n \deg(m_i(x))$.

17 teorema. Tegul $m_1(x), \dots, m_n(x) \in \mathbb{F}_p[x]$ ir tarpusavyje pirminiai elementai, $s_1, \dots, s_n \in \mathbb{F}_p[x]$ ir lyginių sistema

$$g(x) \equiv s_i(x) \pmod{m_i(x)} \quad \forall i = 1, 2, \dots, n,$$

tegul

$$M(x) = \prod_{i=1}^n m_i(x), \quad M_i(x) = \frac{M(x)}{m_i(x)}, \quad a_i(x) \in \mathbb{F}_p, \quad a_i(x)M_i(x) \equiv 1 \pmod{m_i(x)},$$

tada

$$g(x) = \sum_{i=1}^n a_i(x)M_i(x)s_i(x)$$

yra lyginių sistemos sprendinys.

18 pavyzdys. Tegul $\mathbb{F}_3$ baigtinis kūnas, lyginių sistema su tarpusavyje pirminiais moduliais virš baigtinio kūno $m_1 = x$, $m_2 = x + 2$, $m_3 = x^2 + 1 \in \mathbb{F}_3[x]$ ir atitinkamomis dalybos liekanomis $s_1 = 1$, $s_2 = 2$, $s_3 = x + 1 \in \mathbb{F}_3[x]$:

$$\begin{cases} g(x) & \equiv 1 \pmod{x} \\ g(x) & \equiv 2 \pmod{x+2} \\ g(x) & \equiv x+1 \pmod{x^2+1} \end{cases} \quad (1.6)$$

Suporuojamos dvi (1.6) lyginių lygtys ir ieškomas šios poros sprendinys, pasitelkus Euklido algoritmu, gaunami Bezout koeficientai lygčių modulių porai $m_1(x), m_2(x)$.

$m_1(x), m_2(x)$ didžiausias bendrasis daliklis yra

$$dbd(x, x+2) = x \cdot 1 + (x+2) \cdot 2 = 1,$$

pasinaudojus (17) teorema gaunamas lyginių poros sprendinys $g(x)$:

$$\begin{aligned} g(x) &= x \cdot 1 \cdot 2 + (x+2) \cdot 2 \cdot 1 \pmod{x \cdot (x+2)} \\ &= x + 1 \pmod{x^2 + 2x}, \end{aligned}$$

lieka lyginių sistema:

$$\begin{cases} g(x) \equiv x + 1 \pmod{x^2 + 2x} \\ g(x) \equiv x + 1 \pmod{x^2 + 1}. \end{cases}$$

Kartojame algoritmą:

$$dbd(x^2 + 1, x^2 + 2x) = (x^2 + 1) \cdot (x + 1) + (x^2 + 2x) \cdot (2x + 1) = 1.$$

Galutinis (1.6) sistemos sprendinys pagal (17) teoremą yra:

$$\begin{aligned} g(x) &= (x^2 + 1) \cdot (x + 1) \cdot (x + 1) + (x^2 + 2x) \cdot (2x + 1) \cdot 2 \pmod{x^2 + 1 \cdot x^2 + 2x} \\ &= x^4 + 1 \pmod{x^4 + 2x^3 + 2^2 + 2x}. \end{aligned}$$

1.4 Paslapties pasidalijimo schemos

Paslapties pasidalijimo schemos yra puiki priemonė saugoti duomenis, konfidencialią ir svarbią informaciją nuo trečiųjų šalių. Toliau nagrinėjama, kokias sąlygas šios schemos turi tenkinti, kad būtų laikomos saugiomis.

19 apibrėžimas. [1] Tegul S yra paslaptis, o $S_1, S_2, \dots, S_n$ yra jos dalys, kurias dalintojas D įteikia dalyviams $D_1, D_2, \dots, D_n$. Slenkstinė (t, n) paslapties dalijimosi schema apibūdinama taip: n dalyvių skaičius, t paslapčių dalių skaičius reikalingas atkurti paslaptį S , kai yra laikomasi sąlygų:

1. Kiekvienas dalyvis turi paslapties dalį S_i , kuri nežinoma kitiems dalyviams.
2. Paslaptis S gali būti lengvai atkurta iš bet kurių t paslapties S dalių.
3. Turint bet kurias $t - 1$ ar mažiau paslapties dalių, jokia paslapties informacija nebus atskleidžiama.

1.5 Asmuth-Bloomo schema

Panagrinėkime, kaip Asmuth-Bloomo slenkstinė paslapties pasidalijimo schema, pasitelkianti kinų liekanų teoremą bei jos savybes, sukonstruoja paslapties dalis, kaip paslaptis atkurama, užtikrinamas paslapties saugumas.

20 algoritmas. [5] *Slenkstinės Asmuth-Bloomo paslapties pasidalijimo schemos sveikiesiems skaičiams konstravimas su slenksčiu t .*

1. *Dalintojas parenka $n + 1$ tarpusavyje pirminius (kitu atveju negalėsime taikyti kinų liekanų teoremos ieškant paslapties) skaičius p_i , tenkinančius sąlygas*

$$p_0 < p_1 < p_2 < \dots < p_n \quad (1.7)$$

$$p_0 p_n p_{n-1} \dots p_{n-t+2} < p_1 p_2 \dots p_t. \quad (1.8)$$

2. *Parenkama paslaptis $S < p_0$ ir kiek įmanoma didesnis $r \in \mathbb{N}$, kad*

$$S^* = S + r p_0 \in \left(\prod_{i=n-t+2}^n p_i, \prod_{i=1}^t p_i \right). \quad (1.9)$$

3. *Kiekvienam dalyviui D_i priskiriamas modulis p_i ir saugiu kanalu perduodama paslapties dalis S_i*

$$S_i \equiv S^* \pmod{p_i}$$

Svarbu įsitikinti, kad aptarta schema tenkina (19) apibrėžimą. Tegul dalyvių grupė, net turinti didžiausius modulius p_i , su $t - 1$ dalių sudarys lyginių sistemą, kurios modulių suma $M_1 = p_n p_{n-1} \dots p_{n-t+2}$, bet tai nepadės atskleisti paslapties, nes remiantis kinų liekanų teorema, lyginių sistemos sprendinys unikalus intervale $[0, M_1 - 1]$, taigi remiantis (1.9) sąryšiu gaunama $M_1 = \prod_{i=n-t+2}^n p_i < S^* \implies$ paslaptis nepatenka į $[0, M_1 - 1]$ ir nebus neatskleidžiama. Alternatyviai grindžiama ir kita sąlyga – bet kuri grupė dalyvių, net su mažiausiais t moduliais p_i galės atskleisti paslaptį. Ši sąlygą išplaukia iš (1.9), (1.8) bei minėtos kinų liekanų teoremos išvados apie lyginių sistemos sprendinį, grupės modulių sandauga bus didesnė, nei S^* ir paslaptis bus unikalus grupės sudarytos lyginių sistemos sprendinys.

21 algoritmas. [5] *Slenkstinės Asmuth-Bloomo paslapties pasidalijimo schemos paslapties atkūrimas.*

1. *Tegul t dalyvių $i_1, i_2, \dots, i_t, t \in [1, n]$ nori atkurti paslaptį. Grupė dalyvių privalo išspręsti lyginių sistemą kartu sudedant savo paslapties dalis S_{i_j}*

$$\begin{cases} x \equiv S_{i_1} \pmod{p_{i_1}} \\ x \equiv S_{i_2} \pmod{p_{i_2}} \\ \vdots \\ x \equiv S_{i_t} \pmod{p_{i_t}} \end{cases} \quad (1.10)$$

(15) teorema nurodo, kad gautas sistemos sprendinys x yra unikalus intervale $0 \leq x < \prod_{i=t}^n p_i$, (17) teorema naudojama rasti šį sprendinį. Kadangi, S^* tenkina sąlygą

$$S^* = S + rp_0 < \prod_{i=t}^n p_i \leq \prod_{k=t}^n p_{i_k} \quad (1.11)$$

remiantis kinų liekanų teorema (15) $S^* = x$ yra lyginių sistemos (1.10) sprendinys.

2. Paslaptis gaunama iš lyginio $S \equiv S^* \pmod{p_0}$

1.6 Asmuth-Bloomo schema daugianariams virš baigtinio kūno

Toliau apibendrinama Asmuth-Bloom slenkstinė paslapties pasidalijimo schema daugianariams virš baigtinio kūno.

22 algoritmas. Slenkstinės Asmuth-Bloomo paslapties pasidalijimo schemas konstravimas su slenkščiu t daugianariams virš baigtinio kūno $\mathbb{F}_p$.

1. Dalintojas parenka $n + 1$ tarpusavyje pirminius daugianarius (kitu atveju būtų negalima taikyti kinų liekanų teoremos) $m_0(x), m_1(x), m_2(x), \dots, m_n(x) \in \mathbb{F}_p[x]$ tenkinančius sąlygas

$$d_0 \leq d_1 \leq \dots \leq d_n \quad (1.12)$$

$$d_0 + \sum_{i=n-t+2}^n d_i \leq \sum_{i=1}^t d_i, \quad (1.13)$$

kur $d_i = \deg(m_i(x))$.

2. Parenkama paslaptis $S(x)$ iš erdvės

$$\mathbb{S} = \{S(x) \in \mathbb{F}_p[x] \mid \deg(S(x)) < d_0\}, \quad (1.14)$$

tada dalintojas pasirenka daugianarį $a(x)$ iš

$$\mathbb{A} = \{a(x) \in \mathbb{F}_p[x] \mid \deg(a(x)) \leq \sum_{i=1}^t d_i - d_0 - 1\}. \quad (1.15)$$

$S^* = S(x) + a(x)m_0(x) \in \mathbb{F}_p[x]$. Iš (1.13), (1.14), (1.15), (1.16) išplaukia, kad S^* tenkina sąlygą:

$$d_0 + \sum_{i=n-t+2}^n d_i < \deg(S^*(x)) \leq \sum_{i=1}^t d_i - 1 \quad (1.16)$$

3. Kiekvienam dalyviui D_i priskiriamas modulis $m_i(x)$ ir saugiu kanalu perduodama paslapties dalis $S_i \in \mathbb{F}_p[x]$

$$S_i(x) \equiv S^*(x) \pmod{m_i(x)}, \quad (1.17)$$

Schema atitinka (19) apibrėžimo keliamas sąlygas slenkstinėms paslapties pasidalijimo schemoms, tai įrodoma alternatyviai, kaip ir schemai su sveikaisiais skaičiais.

23 algoritmas. *Slenkstinės Asmuth-Bloomo paslapties pasidalijimo schemos paslapties atkūrimas su daugianariais virš baigtinio kūno $\mathbb{F}_p$.*

1. Tegul t dalyvių $i_1, i_2, \dots, i_t, t \in [1, n]$ nori atkurti paslaptį. Grupė dalyvių privalo išspręsti lyginių sistemą kartu sudedant savo paslapties dalis $S_{i_j}(x)$

$$\begin{cases} f(x) \equiv S_{i_1}(x) \pmod{m_{i_1}(x)} \\ f(x) \equiv S_{i_2}(x) \pmod{m_{i_2}(x)} \\ \vdots \\ f(x) \equiv S_{i_t}(x) \pmod{m_{i_t}(x)} \end{cases}$$

(16) teorema nurodo, kad gautas sistemos sprendinys yra unikalus, kai $0 \leq \deg(f(x)) < \sum_{i=1}^t d_i$, (17) teorema naudojama rasti šį sprendinį $f(x) \in \mathbb{F}_p[x]$. Kadangi, $S^*(x)$ tenkina sąlygą

$$\deg(S^*) = \deg(S(x)) + \deg(a(x)f_0(x)) < \sum_{i=1}^t d_i \leq \sum_{k=1}^t d_{i_k} \quad (1.18)$$

remiantis kinų liekanų teorema $S^*(x) = g(x)$ yra šios lyginių sistemos sprendinys.

2. Paslaptis gaunama iš lyginio

$$S(x) \equiv S^*(x) \pmod{m_0(x)} \quad (1.19)$$

2 skyrius

Praktinė dalis

2.1 Asmuth-Bloomo paslapties padalijimo schemas paslapties atkūrimas

24 algoritmas. *Asmuth-Bloomo paslapties pasidalijimo schemas paslapčių dalinimas*

Ivestis: daugianariai virš kūno $\mathbb{F}_p$: paslaptis $S(x)$ iš (1.14), moduliai $m_0(x), m_1(x), \dots, m_n(x)$, $a(x)$ iš erdvės (1.15):

1. *Pirmiausia skaičiuojama paslaptis: funkcija **paskirstymas** priima įvestą paslaptį $S(x)$, $m_0(x), m_1(x), \dots, m_n(x)$, $a(x)$ ir pagal formulę $S^* = S(x) + a(x)m_0(x)$ gaunama S^* .*
2. *Toliau, pasinaudojus pirmo žingsnio rezultatais, S^* , galima rasti paslapties dalis, kurios vėliau išdalinamos dalyviams pagal formulę (1.17).*

Išvestis: sąrašas S_i su paslapties dalimis $S_i(x)$

```
1 T=PolynomialRing(GF(p), 'x')
2 x= T.gen()
3
4 Si= []
5 def paskirstymas(paslaptis, ax, moduliai):
6     S_asterisk = paslaptis + moduliai[0] * ax
7
8     for i in range(1, len(moduliai)):
```

```

9         paslaptiesDalis = S_asterisk.quo_rem(moduliai[i])[1]
10        Si.append(paslaptiesDalis)
11
12    return 0

```

25 algoritmas. *Slenkstinės Asmuth-Bloom paslapties pasidalijimo schemos paslapties atkūrimas daugianariams virš baigtinio kūno.*

Ivestis: tarpusavyje pirminiai moduliai $m_1, m_2 \in \mathbb{F}_3[x]$ ir paslapties dalys $S_1, S_2 \in \mathbb{F}_3[x]$.

1. Patikrinama ar įvesti moduliai nėra tarpusavyje pirminiai virš kūno $\mathbb{F}_p$, jeigu yra, einama prie kito žingsnio. Naudojama **crt** funkcija, ji iškviečia kita funkciją **gcd**, kuri tikrina ar moduliai tarpusavyje pirminiai ir jų didžiausio bendrojo daliklio polinomo laipsnis yra lygus nuliui.
2. Ieškoma daugianarių poros (m_1, m_2) Bezout koeficientai. Iškviečiama **eucl_in** funkcija, kuri taiko Euklido algoritmą gauti $\text{dbd}(m_1, m_2)$, toliau taikomas atvirkštinis Euklido algoritmo skaičiavimo metodas – gaunami Bezout koeficientai. Grįžtame į **crt** funkciją.
3. Remiantis kinų liekanų teorema (17) ir pasinaudojus lyginių sąvybėmis, randamas lyginių sistemos sprendinys $S^* \pmod{m_1 m_2}$.

Išvestis: $S^(x) \in \mathbb{F}_p[x]$, reikalingas atskleisti paslaptį S iš lyginio (1.19).*

```

1  T=PolynomialRing(GF(p),'x')
2  x= T.gen()
3
4  def eucl_in(a,b):
5      b=b.quo_rem(a)[1]
6      q=[]
7      ret="neegzistuoja"
8      r=a.quo_rem(b)[1]
9      while((r==0)==False):
10         q.append(a.quo_rem(b)[0])
11         a=b
12         b=r

```

```

13         r=a. quo_rem(b)[1]
14
15     q=q[::-1]
16     u=1
17     v=-q[0]
18     for i in range(1,len(q)):
19         uu=u
20         u=v
21         v=uu-q[i]*v
22     b=1/int(b)%p
23     ret=v*b
24     return ret
25
26 def crt(moduliai, liekanos):
27     d=gcd(moduliai[0],moduliai[1])
28     if d.degree()>0: ret="netinkami moduliai"
29     if d.degree()==0:
30         u0=eucl_in(moduliai[1],moduliai[0])
31         u1=eucl_in(moduliai[0],moduliai[1])
32         spr=liekanos[0]*moduliai[1]*u1+liekanos[1]*moduliai[0]*u0
33         m=moduliai[0]*moduliai[1]
34         ret=spr. quo_rem(m)[1]
35     return ret

```

Algoritmai buvo realizuoti programine kalba Python (versija 3). Naudojamas SageMath (versija 9.0) programinė įranga, kuri remiasi daugybe jau egzistuojančių atviro kodo paketų: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R ir t.t.[informacija iš oficialaus puslapio <https://www.sagemath.org/>] SageMath leidžia atlikti įvairius veiksmus su polinomais, pavyzdžiui, patikrinti, ar polinomas yra neredukuojamas arba rasti dviejų polinomų dalybos liekaną. Tolimesni skaičiavimai buvo atlikti Acer Aspire E5-576G nešiojamu kompiuteriu, su Intel(R) Core(TM) i58250U CPU @ 1.60GHz, 8Gb RAM.

26 pavyzdys. Siekiant sukonstruoti slenkstinę ($t = 2, n = 3$) Asmuth-Bloomo paslapties pasidalijimo schemą daugianariams su koeficientais virš baigtinio kūno, reikia rasti tarpusavyje pirminius modulius, kurie tenkintų sąlygas (1.12), (1.13). Tegul moduliai $m_0(x) = x^2 + 1$, $m_1(x) = x^4 + x$, $m_2(x) = x^4 + x + 2$, $m_3(x) = x^5 + x^2 + 2 \in \mathbb{F}_3[x]$, galima įsitikinti, kad šie moduliai tenkina iškeltas sąlygas (1.12),

(1.13) ir remiantis (7) apibrėžimu moduliai yra tarpusavyje pirminiai:

$$2 \leq 4 \leq 4 \leq 5$$

$$2 + 5 < 4 + 4.$$

Tegul $S^*(x) = S(x) + a(x)m_0(x)$, kur $a(x) = x^5$ iš erdvės (1.15) bei $S(x) = x$ iš erdvės (1.14), kur nagrinėjamas kūnas $\mathbb{F}_3$, tada $S^*(x) = x^7 + x^5 + x$.

Toliau dalintojas paskirsto paslapties dalis $S_i(x)$ dalyviams D_1, D_2, D_3 pagal (1.17), atitinkamai: $S_1(x) = 2x^2 + 2x$, $S_2(x) = x^3 + 2x^2 + 2$, $S_3(x) = 2x^4 + x + 1 \in \mathbb{F}_3$. Turint bent dvi paslapties dalis, galima sudaryti lyginių sistemą ir atkurti paslaptį. Tegul minėtos dalys yra $S_2 = x^2 + 1$, $S_3 = x^4 + x^2 + x$, galima sudaryti lyginių sistemą:

$$\begin{cases} f(x) \equiv x^3 + 2x^2 + 2 \pmod{x^4 + x + 2} \\ f(x) \equiv 2x^4 + x + 1 \pmod{x^5 + x^2 + 2}. \end{cases} \quad (2.1)$$

Pirmiausia, pasitelkiamas Euklido algoritmas:

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

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

$$x + 2 = 1 \cdot (x + 2) + 0$$

Paskutinė liekana $r_3(x)$ lygi nuliui – algoritmas baigtas $\implies r_2(x) = 1 = dbd(m_2, m_3)$.

Atvirkštiniu Euklido algoritmo skaičiavimo metodu gaunami $a(x) = x^4 + x^3 + x^2 + 2x + 1$, $b(x) = 2x^3 + 2x^2 + 2x + 1$, kurie yra atitinkamai polinomų $m_2(x)$, $m_3(x)$ Bezout koeficientai.

Ieškant sprendinio, pritaikoma (17) teorema ir gaunamas (2.1) sistemos sprendinys:

$$\begin{aligned} f(x) &= m_2(x) \cdot a(x) \cdot S_3(x) + m_3(x) \cdot b(x) \cdot S_2(x) \pmod{m_2(x)m_3(x)} \\ &= 2x^{12} + x^{11} + 2x^{10} + x^9 + 2x^7 + 2x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 \\ &\quad \pmod{x^9 + 2x^6 + 2x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1} \\ &= x^7 + x^5 + x \pmod{x^9 + 2x^6 + 2x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1} \end{aligned}$$

Remiantis (16) teorema, gavome unikalų sprendinį $f(x) \in \mathbb{F}_3[x]$ ir $\deg(f(x)) < \deg(M(x))$, kur $M(x) = m_2(x)m_3(x) \implies$ sistemos sprendinys yra $f(x) = S^*(x)$. Iš teiginio (1.19) $\implies$ paslaptis yra $S(x) \equiv S^*(x) \pmod{m_0(x)} = x^7 + x^5 + x \pmod{x^2 + 1} = x$.

Apibendrinimas

Šiame darbe pateiktos pagrindinės sąvokos ir apibrėžimai buvo naudojami kinų liekanų teoremos įrodymui. Vėliau buvo pristatyta ir nagrinėjama Asmuth-Bloomo paslapties pasidalijimo schema daugianariams virš baigtinio kūno, kuri remiasi kinų liekanų teorema bei jos savybėmis paslapties sukūrimui, jos išdalinimui, o prireikus – atkūrimui.

Šiame darbe galiausiai buvo parašyti kodai: pirmasis – randantis paslapčių dalis priskiriamas dalyviams, antrasis – padedantis atskleisti Asmuth-Bloom slenkstinės paslapties pasidalijimo schemos paslaptį.

Chinese Remainder Theorem and Secret Sharing Schemes

Summary

Chinese remainder theorem is based on „Pars pro toto“ (eng. *a part (taken) for the whole*) principle, it raises a question, does a part of an object gives information about the whole. Earliest known Chinese remainder theorem statement was presented in the Chinese mathematician Sun Zie book around 3rd century.[3] At first, theorem were applied to count big units: for example size of the army, however, even today theorem find new types of applications.

The main interest of this paper is divided in two directions: firstly, the main definitions and statements were introduced, that are required to the following introduction of topic Chinese remainder theorem, what is the core of Asmuth-Bloom secret sharing scheme – the main topic of this paper. Secondly, the programs were created that helps to distribute secret shares another to recreate a secret of secret sharing scheme.

In the theoretical part of this paper main definitions and notions were given to prove the Chinese remainder theorem, based on this theorem Asmuth-Bloom threshold secret sharing scheme based on finite fields is introduced. Following, a programs are created to distribute secret shares and another to restore a secret of the Asmuth-Bloom threshold secret sharing scheme.

Keywords: Chinese remainder theorem, secret sharing schemes, Asmuth-Bloom threshold secret sharing scheme.

Literatūra

- [1] P. DINGYI, S. ARTO, D. CUNSHENG. *Chinese Remainder Theorem: Applications In Computing, Coding, Cryptography.*, 157-158 psl., 1996.
- [2] P. DRUNGILAS. *Paskaitų konspektai.*
- [3] KATZ, VICTOR J. *A History of Mathematics / An Introduction (2nd ed.)*, Vilnius, A.M.S., 1998, Addison Wesley Longman, ISBN 978-0-321-01618-8, p. 197.
- [4] Y. NING, F. MIAO, W. HUANG, K. M. Y. XIONG AND X. WANG. *Constructing Ideal Secret Sharing Schemes based on Chinese Remainder Theorem*, 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, p. 4-5, 8-9.
- [5] V. STAKĖNAS. *Kodai ir šifrai*, Vilnius, A.M.S., 2006, p. 285-287, 344-345.
- [6] P. ŠARKA, J. ŠIURYS. *paskaitų konspektas*, p. 16-17.