Paskaita 16

Matricos virš žiedo

Žiedas yra struktūra $(R, +, \cdot)$

a) $(R, +)$ yra Abelio grupė

b) $(R, \cdot)$ yra pusgrupė

c) $x \cdot (y+z) = x \cdot y + x \cdot z$

$(x+y) \cdot z = x \cdot z + y \cdot z.$

Vienetinis elementas (arba vienetinis elementas) yra pusgrupės $(R, \cdot)$ neutralus elementas

Jeigu $(R, \cdot)$ yra Abelio grupė ir laikas nemažiau kaip komutuoja. elementas $a \in R$, $a \neq e$ turi atvirkštinį $a \cdot a' = 1$.)

Norėdami apibendrinti Afininius šifravimo algoritmus nagrinėsime tiesinės algebros (vektorių, matricų) apibendrinimus virš žiedų.

Tegul R yra *komutatyvus* žiedas ir jis turi vienetinį elementą 1.

Pav. $R = \mathbb{Z}/m\mathbb{Z}$, kur $m \in \mathbb{N}$.

$1 := 1 + m\mathbb{Z}$

tai m pirminis skaičius

a' egzistuoja $\gcd(a, m) = 1$.

Ap. $k \times n$ matrica virš R yra stačiakampė lentelė (schema)

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}$$

Taip pat žymėsime $A = (a_{ij})$

Ap. Jeigu $k = n$, tai matrica vadinsime *kvadratine*.

Analogiškai klasikiniams matricoms apibrėžiame matricos eilutes ir stulpelius.

$k \times n$ Matrica virš R aibę žymėsime $R^{(k,n)}$.

Pav. $R = \mathbb{Z}$.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in \mathbb{Z}^{(2,3)}$$

yra 2×3 matrica virš $\mathbb{Z}$. Jos dvi eilutės ir 3 stulpeliai.

Ap. Matrica $A \in R^{(k,n)}$ ir vektorius (stulpelis) $V \in R^n$ sandauga apibrėžiama taip ($V \in R^{(n,1)}$)

$$AV = W, \quad W \in R^k$$

$$W_i = \sum_{j=1}^{n} a_{ij} V_j, \quad i = 1, \dots, k.$$

Pav. $A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$, $V = (1, 2)$

$R = \mathbb{Z}/5\mathbb{Z}$.

$AV = (5, 8) \equiv (0, 3) \mod 5$.

Ap. Matricų $A, B \in R^{(n,n)}$ suma ir sandauga yra apibrėžiamos taip

$$A + B = (a_{ij} + b_{ij})$$

$$A \cdot B = (c_{ij}) \quad (= AB)$$

$$c_{ij} = \sum_{k=1}^{n} c_{ik} \cdot b_{kj}$$

Pav. $A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix}$, $R = \mathbb{Z}/9\mathbb{Z}$

$$A + B = \begin{pmatrix} 5 & 7 \\ 8 & 10 \end{pmatrix} \equiv \begin{pmatrix} 5 & 7 \\ 8 & 1 \end{pmatrix} \bmod 9$$

$$AB = \begin{pmatrix} 16 & 19 \\ 26 & 31 \end{pmatrix} \equiv \begin{pmatrix} 7 & 1 \\ 8 & 4 \end{pmatrix} \bmod 9$$

$$BA = \begin{pmatrix} 5 & 5 \\ 2 & 6 \end{pmatrix} \bmod 9 \qquad AB \neq BA.$$

Tarpinius veiksmus irgi galima atlikti likinių klasėje (t.y. su R elementais)

$$c_{22} = ~~8\ 7~~\ 2 \cdot 5 + 3 \cdot 7 \equiv 1 + 3 = 4 \bmod 9$$

Matricų žiedas $(R^{(n,n)}, +, \cdot)$

~~Vienetas~~ Nulinė matrica (neutralus elementas operacijos + atžvilgiu) žiūr $\mathbb{Z}$:

$$0 = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} e & e & \dots & e \\ e & e & \dots & e \\ \vdots & \vdots & & \vdots \\ e & e & \dots & e \end{pmatrix}$$

Vienetinė matrica (neutralus elementas operacijos $\cdot$ atžvilgiu)

$$1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$ Žymėsime E_n.

Pav. ~~$R^{(3,3)}$~~ atvejui

$$0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Bendrieji atvejai šis žiedas nėra komutatyvus. (pateikite pvz. kai $n=2$, $R = \mathbb{Z}/5\mathbb{Z}$)

Ap. Matricos determinanto apibrėžimui naudodami rekursiją, taip gauname konstruktyvų algoritmą, kaip skaičiuoti determinantus ~~virš~~ matricoms virš žiedo (pvz. kai R yra liekanų klasių žiedas $R = \mathbb{Z}/m\mathbb{Z}$)

$$A \in R^{(n,n)}$$

~~1)~~

1) Jeigu $n = 1$, tai $A = (a)$ ir

$$\det A = a$$

2) $n \geq 2$. Pažymėkime A_{ij} matricą kurią gauname iš A pašalinę i-tąją eilutę ir j-tąjį stulpelį. Fiksuokime:

i - parametras

$$\det A := \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$$

$$\det A := \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$$

} rekursija

Tai apibrėžimas ir, aišku, kad nereikia jokių įrodymų, ar jis „teisingas", tik reikia parodyti, kad apibr. nepriklauso nuo to kurios eilutės ar stulpelio atžvilgiu skleidž.?

Pav.

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$A_{11} = (a_{22}) \qquad A_{12} = (a_{21})$$

$$A_{21} = (a_{12}) \qquad A_{22} = (a_{11})$$

$$\det A = (-1)^{1+1} a_{11} \det A_{11} + (-1)^{1+2} a_{12} \det A_{12}$$

$$= a_{11} a_{22} - a_{12} a_{21}$$

$$\det A = (-1)^{1+2} a_{21} \det A_{21} + (-1)^{2+2} a_{22} \det A_{22}$$

$$= - a_{21} a_{12} + a_{22} a_{11}$$

Ap. Atvirkštinė matrica $A^{-1} \in R^{(n,n)}$

$$A A^{-1} = A^{-1} A = E_n$$

T. A^{-1} egzistuoja $\Leftrightarrow$ $\det A$ yra R unit (vienetinis) elementas, t. y. $\det A$ turi simetrišką elementą (yra vieneto dalikli)

Inkime $R = \mathbb{Z}/m\mathbb{Z}$

$$A = \begin{pmatrix} 5 & 1 \\ 7 & 3 \end{pmatrix} \qquad \det A = 8$$

1) $m = 3$ $\quad \gcd(8,3) = 1$

$\det A \equiv 2 \mod 3$

$2 \cdot 2 \equiv 1 \mod 3 \Rightarrow 2^{-1} = 2 \mod 3$

$$\bar{A} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \qquad \det \bar{A} = -1 \equiv 2 \mod 3.$$

$\bar{a}_{ij} \equiv a_{ij} \mod 3$

2) $m = 6$ $\quad \gcd(8,6) = 2$

$\det A \equiv 2 \mod 6$ (nera inmetinis elementas)

$$\bar{A} = \begin{pmatrix} 5 & 1 \\ 1 & 3 \end{pmatrix} = 14 \equiv 2 \mod 6.$$

$\bar{a}_{ij} = a_{ij} \mod 6.$ $\quad \bar{A}^{-1}$ neegzistuoja.

Algoritmas atvirkstinei matricai

1) $A \in R^{(n,n)}$

$n = 1.$

$A^{-1} = (a_{11}^{-1})$.

Čia $a_{11} \cdot a_{11}^{-1} = 1$.

Pvz

$\bar{A}\,\bar{A}^{-1} = E_n \mod m$

$\bar{A} \in (\mathbb{Z}/m\mathbb{Z})^{(n,n)}$

$n > 1$ Apibrėžkime jungtinę matricą

$$\operatorname{adj} A = \left((-1)^{i+j} \det A_{ji} \right) = (c_{ij})$$

$$A^{-1} = (\det A)^{-1} \operatorname{adj} A.$$

T.y. surandame simetrinį elementą žiede $R^{(n,n)}$

$$\boxed{A A' = E_n}$$

Pav.

$$\bar{A} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{Z}/3\mathbb{Z}$$

$\det \bar{A} = 2$, $2 \cdot 2 \equiv 1$

$2' = 2$.

$\bar{A}_{11} = (0)$ $\bar{A}_{12} = (1)$

$\bar{A}_{21} = (1)$ $\bar{A}_{22} = (2)$

$$\bar{A}' = 2 \cdot \begin{pmatrix} 0 & -1 \\ -1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 0 & -2 \\ -2 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\bar{A}\,\bar{A}^{-1} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Gauso algoritmas

$$\left(\bar{A} \mid E_n\right) \Rightarrow \left(E_n \mid \bar{A}^{-1}\right)$$

mod 3 ?

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) \overset{\times 2}{\Rightarrow} \left(\begin{array}{cc|cc} 1 & 2 & 2 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

Galima sukeisti eilutes vietomis ir tada pratęsti

1 eilutė atimame iš 2 $\Rightarrow$

$$\left(\begin{array}{cc|cc} 1 & 2 & 2 & 0 \\ 0 & -2 & -2 & 1 \end{array}\right) \overset{\text{mod } 3}{\Rightarrow} \left(\begin{array}{cc|cc} 1 & 2 & 2 & 0 \\ 0 & 1 & 1 & 1 \end{array}\right)$$

2 eilutė dauginame iš 2 ir atimame iš pirmos eilutės $\Rightarrow$

$$\left(\begin{array}{cc|cc} 1 & 0 & 0 & -2 \\ 0 & 1 & 1 & 1 \end{array}\right) \overset{\text{mod } 3}{=}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right)$$

$$\bar{A}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Pratybos

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Norime rasti A' tokią, kad

$$A A' = E_2 \mod 11.$$

(Ats.: $\begin{pmatrix} 9 & 1 \\ 7 & 5 \end{pmatrix}$)

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) \Rightarrow \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{array}\right) \overset{\cdot(-2)}{\Rightarrow} \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & -2 \end{array}\right)$$

$$\overset{\mod 3}{=} \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right)$$

Apsk determinanty Gauso metodu.

ElGamal šifravimo algoritmas

(Diffie-Hellman raktų paskirstymo algoritmo modifikacija!)

1. Pasirenkame pirminį skaičių p

2. Pasirenkame generuojantį elementą g (jų yra $\varphi(p-1)$).

Tai elementas, kurio eilė $|g| = p-1$.

3. Pasirenkame eksponentę $a \in \{0, \dots, p-2\}$

4. Apskaičiuojame $A = g^a \bmod p$

Viešasis raktas (p, g, A).

Šifravimo algoritmo saugumas grindžiamas tuo, kad diskretusis logaritmas

$a = \mathrm{dlog}_g A$ gali būti ~~tik~~ randamas

iš ~~tik~~lygties $g^a = A$ perrenkant visas galimas reikšm

Šifravimo žingsnis

Pranešimas
$m \in \{0, 1, \dots, p-1\}$

Bobas pasirenka slaptą raktą dalį
$b \in \{1, \dots, p-2\}$ ir apskaičiuoja

$$B = g^b \bmod p$$

Pranešimo šifravimas

$$c = A^b m \bmod p$$

užšifruotą
Jis nusiunčia pranešimą Alice

(B, c).

Dešifravimo žingsnis

$$m \equiv c\, B^{-a} \mod p.$$

Teisingumo analizė

$$c\, B^{-a} \equiv m A^{b} B^{-a} \equiv m \left(g^{a}\right)^{b} \cdot \left(g^{b}\right)^{-a}$$

$$\equiv m\, g^{ab}\, g^{-ba} \equiv m,$$

nes $\boxed{ab = ba}$

Algoritmas

$x = p - 1 - a$

$$\boxed{m = B^{x} \cdot c}$$

$$\| $$

$$\boxed{m = B^{p-1} \cdot B^{-a} c}$$

~~$B^{x} B^{-a} = B$~~

Mažoji Ferma teorema

$B^{p-1} = 1$

$p = 13 \quad a = 5$ $\boxed{x = 12 - 5 = 7}$

Kitas variantas:

- skaičiuojame $y = B^a$
- randame $y^{-1} \cdot y = 1$

$$\boxed{m = y^{-1} \cdot c} \mod p.$$