Algebros pratybos.

Rimantas Grigutis

3 pratybos.
Laipsnio ir atvirkštinio skaičiavimas mod m Oilerio teorema
Lyginių sistemų sprendimas.
Paslapties pasidalijimo schema
RSA kriptosistema

1. Laipsnio ir atvirkštinio skaičiavimas modm Oilerio teorema.

1. Oilerio teorema teorema : Jei $(a,m)=1$, tai $a^{\varphi(m)} \equiv 1 \pmod m$.
2. Jei $(a,m)=1$, tai $a^{\varphi(m)-1} \equiv a^{-1} \pmod m$
3. Jei m nesidalija iš jokio pirminio skaičiaus kvadrato ($p \nmid m$), tai $\mathrm{a}^{\varphi(m)+1} \equiv a \pmod m$.

Pavyzdys.
Apskaičiuosime :$7^{9999} \bmod (1000)$. Apskaičiuokime
$\varphi(1000) = \varphi(2^3 \cdot 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400.$
Tada
$7^{9999} = 7^{10000-1} = 7^{400 \cdot 25 - 1} = 7^{400 \cdot 25} \cdot 7^{-1} = (7^{400})^{25} \cdot 7^{-1} \equiv 7^{-1} \pmod{1000} \equiv 11 \cdot 13 \pmod{1000} = 143$, nes $7 \cdot 11 \cdot 13 = 1001 \equiv 1 \pmod{1000}$.

Uždaviniai.
Apskaičiuokite
1) $11^{9999} \pmod{1000}$ 2) $13^{9999} \pmod{1000}$
3) $91^{-1} \pmod{501}$ 4) $3379^{-1} \pmod{4061}$.

2. Lyginių sistemų sprendimas.

Nagrinėkime sistemą:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \cdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases},$$

čia $(m_i, m_j) = 1$, kai $i \neq j$.
Lyginių sistemos sprendžiamos nuosekliai sprendžiant vieną lyginį po kito.
Išnaginėkime pavyzdį.

$$\begin{cases} 10x \equiv 1 \,(\mathrm{mod}\, 13) \\ 8x \equiv 10 \,(\mathrm{mod}\, 18) \\ 6x \equiv 5 \,(\mathrm{mod}\, 23) \end{cases}$$

1. Išsprendę pirmąjį lyginį (*2 pratybos*) $10x \equiv 1 \,(\mathrm{mod}\, 13)$ turėsime $x \equiv 4 \,(\mathrm{mod}\, 13)$, t.y. $x = 4 + 13y, y \in \mathbf{Z}$.

2. Įrašę šią išraišką į antrąjį lyginį ir išsprendę jį turėsime

$$\begin{gathered} 8\,(4 + 13y) \equiv 10 \,(\mathrm{mod}\, 18) \mid :2 \text{ pagal } 2.4.6(2 \text{ paskaita}) \\ 4\,(4 + 13y) \equiv 5 \,(\mathrm{mod}\, 9) \\ 16 + 52y \equiv 5 \,(\mathrm{mod}\, 9) \\ 52y \equiv -11 \,(\mathrm{mod}\, 9) \\ 7y \equiv 7 \,(\mathrm{mod}\, 9) \\ y \equiv 1 \,(\mathrm{mod}\, 9)\,, \end{gathered}$$

t.y. $y = 1 + 9z, z \in \mathbf{Z}$ ir $x = 4 + 13\,(1 + 9z) = 17 + 117z, z \in \mathbf{Z}$.

3. Įrašę šią išraišką į trečiąjį lyginį ir išsprendę jį turėsime

$$\begin{gathered} 6\,(17 + 117z) \equiv 5 \,(\mathrm{mod}\, 23) \\ 102 + 702z \equiv 5 \,(\mathrm{mod}\, 23) \\ 10 + 12z \equiv 5 \,(\mathrm{mod}\, 23) \\ 12z \equiv -5 \,(\mathrm{mod}\, 23) \\ 12z \equiv 18 \,(\mathrm{mod}\, 23) \mid :6 \text{ pagal } 2.4.7(2 \text{ paskaita}), \text{ nes } (6, 23) = 1 \\ 2z \equiv 3 \,(\mathrm{mod}\, 23) \\ z \equiv 13 \,(\mathrm{mod}\, 23) \ (\textit{2 pratybos}), \end{gathered}$$

t.y. $z = 13 + 23t, t \in \mathbf{Z}$ ir$x = 17 + 117\,(13 + 23t) = 1538 + 2691t, t \in \mathbf{Z}$.

4. Sistemos sprendiniai yra vienoje klasėje moduliu *2691*: ${}_{2691}K_{1538}$ arba dviejose klasėse moduliu $2691 \cdot 2 = 5382 :$ ${}_{5382}K_{1538,5382}\,K_{4229}$, čia $1538 + 2691 = 4229$.

5. Ats.: sistema turi dvi sprendinių klases moduliu $M = 13 \cdot 18 \cdot 23 = 5382 :$ $\overline{1538}, \overline{4229}$.

Uždaviniai.

Išspręskite lyginių sistemas.

1) $\begin{cases} 2x \equiv -1 \,(\mathrm{mod}\, 3) \\ 3x \equiv 2 \,(\mathrm{mod}\, 5) \end{cases}$ 2) $\begin{cases} 3x \equiv 6 \,(\mathrm{mod}\, 9) \\ 5x \equiv 1 \,(\mathrm{mod}\, 8) \end{cases}$ 3) $\begin{cases} 11x \equiv 2 \,(\mathrm{mod}\, 5) \\ -x \equiv 3 \,(\mathrm{mod}\, 6) \end{cases}$

4) $\begin{cases} 12x \equiv 15 \,(\mathrm{mod}\, 17) \\ 10x \equiv 4 \,(\mathrm{mod}\, 19) \\ 21x \equiv 16 \,(\mathrm{mod}\, 23) \end{cases}$ 5) $\begin{cases} 5x \equiv 1 \,(\mathrm{mod}\, 41) \\ 5x \equiv 1 \,(\mathrm{mod}\, 51) \\ 5x \equiv 1 \,(\mathrm{mod}\, 61) \end{cases}$ 6) $\begin{cases} 3x \equiv 1 \,(\mathrm{mod}\, 11) \\ 5x \equiv 2 \,(\mathrm{mod}\, 13) \\ 7x \equiv 3 \,(\mathrm{mod}\, 15) \end{cases}$

3. Asmutho-Bloomo paslapties pasidalijimo schema su sleksčiu t.

Paslapties dalijimas n dalyviams.
Dalytojas parenka skaičius
$p < p_1 < p_2 < \cdots < p_n$, $(p_i, p_j) = 1, i \neq j$
$p_1 p_2 \cdots p_t > p p_n p_{n-1} \cdots p_{n-t+2}$
$N = p_1 p_2 \cdots p_t$
$r, r < \dfrac{N}{p-1}$
Paslaptimi yra skaičius $S, S < p$.
Dalytojas apskaičiuoja $S^* = S + pr$
ir *dalyviui* D_i paskiria skaičių p_i ir perduoda paslapties dalį $S_i \equiv S^* \pmod{p_i}$.
Paslapties atkūrimas
t *dalyvių* $D_{i_1}, \ldots, D_{i_t}$ kiniškąja liekanų teorema sprendžia lyginių sistemą

$$\begin{cases} x \equiv S_{i_1} \pmod{p_{i_1}} \\ \qquad \cdots \\ x \equiv S_{i_t} \pmod{p_{i_t}} \end{cases}$$

ir randa sprendinį $x = S^*$. Paslaptis $S \equiv S^* \pmod{p}$.

Užduotis
(Asmutho-Bloomo paslapties pasidalijimo schema 4 dalyviams su sleksčiu t=2)

Skelbiami skaičiai:
$p = 31, p_1 = 39, p_2 = 41, p_3 = 43, p_4 = 44$.
Dalyvių porai atkurti paslaptį, jei kiekvienam dalyviui priskirta pora (p_i, S_i) :
1) $(p_1, 14)$ ir $(p_3, 11)$
2) $(p_2, 32)$ ir $(p_4, 37)$
3) $(p_1, 20)$ ir $(p_4, 42)$
4) $(p_2, 37)$ ir $(p_3, 16)$

4. $\mathbf{R}_{Rivest}\mathbf{S}_{Shamir}\mathbf{A}_{Adleman}$ kriptosistema(1978) **(Kriptografijos uždavinys).**

Apibrėžkime kriptografijos uždavinį tokia schema:

$$\boxed{\text{Tekstas } \mathbf{T}} \overset{\text{kodavimas}}{\longrightarrow} \mathbf{T} \to \mathbf{x} \in \mathbf{Z}_n \overset{\text{šifravimas}}{\longrightarrow} \mathbf{y} = e(\mathbf{x}) = \mathbf{x}^{\mathbf{E}} \pmod n$$

$$\overset{y \text{ siuntimas}}{\rightsquigarrow} \boxed{\mathbf{y} \in \mathbf{Z}_n} \overset{\text{dešifravimas}}{\longrightarrow}$$

$$\boxed{d(\mathbf{y}) = \mathbf{y}^{\mathbf{D}} = \mathbf{x}^{\mathbf{ED}(\bmod \varphi(n))} \equiv \mathbf{x} \pmod n} \to \boxed{\mathbf{x}} \overset{\text{dekodavimas}}{\to} \boxed{\mathbf{T}}.$$

RSA kriptosistema - tai penketas$\{n, p, q, \mathbf{E}, \mathbf{D}\}$ gaunamas šiomis sąlygomis:

1. Generuojami du (dideli) pirminiai skaičiai p ir q ir randama $n = p \cdot q$.

2. Skaičiuojama $\varphi(n) = (p-1)(q-1)$ ir parenkamas tarpusavyje pirminis su $\varphi(n)$ skaičius $\mathbf{E}$.

3. Sprendžiant lyginį $\mathbf{E}x \equiv 1 \pmod{\varphi(n)}$ gaunamas sprendinys:

$$\mathbf{D} = \mathbf{E}^{-1} \pmod{\varphi(n)}.$$

Skaičiai $(n, \mathbf{E})$ vadinami kriptosistemos *atviru raktu(public key)* ir talpinami į atvirą katalogą; skaičiai $(p, q, \mathbf{D})$ vadinami *slaptu raktu(private key)* ir reikalauja apsaugos.

Abonentas A norėdamas siųsti tekstą T abonentui B, renkasi pastarojo atvirame kataloge skaičių porą $(n, \mathbf{E})$, koduoja jį, šifruoja gautą kodą ir siunčia užšifruotą tekstą kartu su skaičių pora $(n, \mathbf{E})$ abonentui B, kuris, žinodamas slaptąjį raktą $(p, q, \mathbf{D})$, dešifruoja, o poto dekoduoja bei skaito gautą pranešimą.

Slaptumo minimumas:

1. Kiekvienas vartotojas turi nepriklausomai ir slaptai generuoti skaičius p ir q. Tas pats skaičius $n = p \cdot q$ negali būti bendras dviems vartotojams.

2. Skaičiai p ir q negali būti žinomuose pirminių skaičių sąrašuose. Jokių išorinių dėsningumų!

3. Skaičiai p ir q negali būti artimi pirminiai skaičiai tam, kad Ferma Faktorizacijos Procesas būtų neveiksmingas.

4. Skaičiai $p, p-1.p+1, \frac{p-1}{2}, \frac{p+1}{2}; q, q-1, q+1, \frac{q-1}{2}, \frac{q+1}{2}$ neturi turėti mažų pirminių daliklių, bei turėti bent vieną didelį pirminį daliklį.

5. Grupėje U_n neturi būti daug mažos eilės elementų.

Pavyzdys. Kriptosistemos parametrai:

1. $p = 3, q = 11; n = 3 \cdot 11 = 33$.

2. $\varphi(33) = (3-1)(11-1) = 20$. Skaičius $\mathbf{E} = 3$ yra tarpusavyje pirminis su 20.

3. Sprendžiant lyginį $3\mathbf{D} \equiv 1 \pmod{20}$ randamas $\mathbf{D} = \mathbf{7} \pmod{20}$.

Abonentas A nori siųsti žodį *gerai*, kurį koduoja skaičiumi $x = 8$.

Pasirinkęs atvirą raktą $(33, 3)$ šifruoja kodą: $y = 8^3 = 512 \equiv 17 \pmod{33}$.

Vėliau $(y, n, \mathbf{E}) = (17, 33, 3)$ siunčia abonentui B: $(y, n, \mathbf{E}) = (17, 33, 3)$.

Abonentas B gavę šifruotę 17 ir atvirąjį raktą $(33, 3)$, slaptuoju raktu $(p, q, D) = (3, 11, 7)$ skaičiuodamas dešifruoja $17^7 = 410\,338\,673 \equiv 8 \pmod{33}$, o poto ir dekoduoja bei perskaito žodį *gerai*.(Abu abonentai iš anksto yra pasirinkę vieną ir tą pačią koduotę).

Uždaviniai.

1. Šifruokite ir dešifruokite simbolį $\mathbf{x} = \mathbf{4}, \mathbf{7}, \mathbf{12}, \mathbf{18}$, kai
$n = 33, 39, 51, 57, 39, 35, 55, 85, 77$.

2. Dešifruokite simbolį $\mathbf{y} = \mathbf{8}, \mathbf{12}, \mathbf{16}, \mathbf{23}$, kai
a) $n = 3397, E = 55$; b) $n = 4183$, $E = 85$; c) $n = 3869$, $E = 2205$.

3. Dešifruokite simbolį $\mathbf{y} = \mathbf{8}, \mathbf{12}, \mathbf{16}, \mathbf{23}$, kai
a) $n = 11189, E = 17, \varphi(11189) = 10956$;
b) $n = 10229, E = 17, \varphi(10229) = 9984$;
c) $n = 8507, E = 17, \varphi(8507) = 8280$;
d) $n = 10207, E = 17, \varphi(10207) = 9976$.