Diskretus, logaritmas, NP ir ... viešos paslaptys

R. Čiegis

Vilniaus Gedimino technikos universitetas
e-mail: rc@vgtu.lt

Gruodžio 10 d., 2019, Vilnius

Metų pabaiga, taigi gera proga neįpareigojančiam pašnekesiui apie moderniųjų technologijų matematikos skyrius.

Šį kartą diskutuosime ne apie naująją studijų programą, o apie tai, ką rudens semestre dėsčiau mūsų studentams – taikomoji algebra, algebrinės struktūros, kriptografijos pagrindai (ir vėl algebra + NP tipo klausimai). Matematikos ten tikrai daug, svarbu įvertinti, ar ji "užkabina".

Pradžioje prisiminsime keletą nesudėtingų apibrėžimų iš grupių teorijos paskaitų.

Algebrinė struktūra $(X, \circ)$ yra Abelio grupė, jei

X yra elementų aibė ir

1. $\circ$ – asociatyvi ir komutatyvi operacija.

2. Egzistuoja neutralus elementas $e \in X$, toks, kad kiekvienam $a \in X$

$$a \circ e = e \circ a = a.$$

3. Kiekvienam $a \in X$ egzistuoja jam simetriškas elementas $a' \in X$

$$a \circ a' = a' \circ a = e.$$

1 pavyzdys.

Imkime $X = \mathbb{Z}$, operacija sudėtis $+$. Tada $(\mathbb{Z}, +)$ yra Abelio grupė.

Neutralus elementas $e = 0$, elementui $a \in \mathbb{Z}$ simetriškas skaičius yra $-a \in \mathbb{Z}$.

2 pavyzdys.

Imkime $X = \mathbb{Q}$, operacija daugyba $\cdot$. Tada $(\mathbb{Q}, \cdot)$ yra Abelio grupė.

Neutralus elementas $e = 1$, elementui $a = \frac{m}{n} \in \mathbb{Q}$, ir $m \neq 0$ simetriškas skaičius yra $a' = \frac{n}{m} \in \mathbb{Q}$.

Pirmoji žinutė mokiniams (Kalėdinė dovanėlė) – atimties ir daugybos operacijų

$$-, \quad /$$

matematikoje nėra (minimaliame operacijų rinkinyje).

Tokios operacijos reikalingos, kai sprendžiame uždavinį

$$a \circ x = b, \quad a, b, x \in X.$$

Tada operacijai $\circ$ apibrėžiame atvirkštinę operaciją $\bullet$:

$$x = b \bullet a := a' \circ b = b \circ a'.$$

Pagrindinę operaciją $\circ$ galėjome apibrėžti taip, kaip norėjome. O atvirkštinę operaciją $\bullet$ jau vienareikšmiškai apibrėžia pagrindinė operacija.

Imkime $X = \mathbb{R}$, tada atimties operaciją apibrėžiame taip:

$$a - b := a + b' = a + (-b).$$

Jeigu $b \neq 0$, tai dalybos operaciją apibrėžiame taip:

$$a/b := a \cdot b' = a \cdot (b^{-1}).$$

$$13 - 7 = x$$

$$1852/48 = y$$

Kriptografijoje svarbūs tokie algebriniai uždaviniai, kai rezultatą randame tik spręsdami tiesioginį uždavinį perrinkimo metodu (NP uždavinių situacija)

$$x = b \bullet a \qquad \Longleftrightarrow \qquad a \circ x = b.$$

Neturime efektyvaus algoritmo, kaip realizuoti atvirkštinę operaciją $\bullet$.

Imkime Abelio grupę $X, \circ$, $a \in X$. Pažymėkime $a^1 = a$ ir apibrėžkime elemento a laipsnius

$$a^{n+1} = a \circ a^n, \quad n \in \mathbb{N}.$$

Nesunkiai įrodome tokias laipsnių savybes

$$a^n \circ a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad (a \circ b)^n = a^n \circ b^n, \quad n, m \in \mathbb{N}.$$

Logaritmas

Duoti skaičiai $g, A \in \mathbb{R}$, $g, A > 0$. Tada skaičiaus A logaritmas pagrindu g yra toks skaičius $a \in \mathbb{R}$, kad

$$g^a = A. \tag{1}$$

Logaritmą žymėsime

$$a = \log_g A.$$

Funkcijos $\log x$ savybės labai išsamiai nagrinėjamos matematinės analizės kurse (Gerda), yra sukurti efektyvūs šios funkcijos reikšmių skaičiavimo algoritmai (Vadimas).

Šioje paskaitoje mums svarbi išvada, kad logaritminė funkcija yra labai patogus analizės įrankis, bet ji irgi nėra būtina nagrinėjant algebrines struktūras.

Elemento A logaritmas $a = \log_g A$ yra lygties

$$g^a = A$$

sprendinys.

Adityvioji liekanų klasių grupė

Nagrinėkime liekanų klases $\mathbb{Z}/n\mathbb{Z}$:

$$a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}, \quad a \in \{0, 1, \ldots, n-1\}.$$

Liekanų klasei $a + n\mathbb{Z}$ priklauso skaičiai $b \in \mathbb{Z}$:

$$b \in a + n\mathbb{Z} \quad \text{jei} \quad b \equiv a \mod n.$$

Pavyzdžiui:

$$3 + 5\mathbb{Z} = \{\ldots, -7, -2, \mathbf{3}, 8, 13, \ldots\}.$$

Imkime grupę $(\mathbb{Z}/n\mathbb{Z}, +)$, kur sumavimo operacija yra apibrėžta taip:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z},$$

čia $(a + b) + n\mathbb{Z} = c + n\mathbb{Z}$, $c \equiv a + b \mod n$.

Šios Abelio grupės neutralus elementas $e = n\mathbb{Z}$.

Elemento $g + n\mathbb{Z}$ laipsnis yra skaičiuojamas taip (žymėsime g^a):

$$(g + n\mathbb{Z})^a = g \cdot a + n\mathbb{Z} = c + n\mathbb{Z}, \quad g \cdot a \equiv c \mod n.$$

Diskretusis logaritmas

Liekanų klasės $A + n\mathbb{Z}$ diskretusis logaritmas pagrindu g yra toks skaičius $a = \mathrm{d}\log_g A \in \{0, 1, \ldots, n-1\}$, kad teisinga lygybė

$$g^a \equiv A \mod n.$$

Pavyzdys. Imkime $n = 13$, $g = 5$.

TABLE : Diskrečiojo logaritmo reikšmės

A	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{d}\log_g A$	8	3	11	6	1	9	4	12	7	2	10	5

Multiplikatyvioji liekanų klasių grupė

Imkime grupę $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z}, \cdot)$, kur daugybos operacija yra apibrėžta taip:

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) := a \cdot b + n\mathbb{Z},$$

čia $a \cdot b + n\mathbb{Z} = c + n\mathbb{Z}$, $c \equiv a \cdot b \mod n$.
Šios Abelio grupės neutralusis elementas yra ekvivalentumo klasė $e = 1 + n\mathbb{Z}$. Grupei priklauso tik tie elementai, kurie turi simetriškus jiems elementus, pavyzdžiui $n\mathbb{Z} \notin (\mathbb{Z}/n\mathbb{Z})^*$.

Elemento $g + n\mathbb{Z}$ laipsnis yra skaičiuojamas taip (žymėsime g^a):

$$(g + n\mathbb{Z})^a = g^a + n\mathbb{Z} = c + n\mathbb{Z}, \quad g^a \equiv c \mod n.$$

Pavyzdys. Imkime $n = 13$, $g = 2$.

TABLE : Diskrečiojo logaritmo reikšmės

A	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{d}\log_g A$	0	1	4	2	9	5	11	3	8	10	7	6

Diffie-Hellman pasikeitimo raktais algoritmas

Norėdami naudoti simetrinius šifravimo algoritmus ir greitai bei saugiai keistis informacija nesaugiu kanalu, turime seanso pradžioje tuo pačiu kanalu pasikeisti slaptais raktais.

Susipažinsime su Diffie-Hellman algoritmu. Šios įdėjos paskelbimas 1976 metais ir tapo esminiu lūžiu kuriant šiuolaikinius viešojo rakto informacijos perdavimo protokolus.

In 1997 it was revealed that James H. Ellis, Clifford Cocks, and Malcolm J. Williamson of GCHQ, the British signals intelligence agency, had previously, in 1969 shown how public-key cryptography could be achieved.

Turime didelį rinkinį spalvotų tirpiklių.

1. Antanas viešai padeda ant stalo indus, kurių 1/3 užpildytas G spalvos tirpalu.

2. Antanas taip pat pasirenka savo slaptą spalvą A ir paruošia indus, 2/3 užpildytus tirpalu $G + A$.

3. Birutė taip pat pasirenka savo slaptą spalvą B ir paruošia indus, 2/3 užpildytus tirpalu $G + B$.

4. Antanas pasiima viešai padėtą Birutės paruoštą tirpalą, papildo jį savo spalvos tirpalu ir gauna slaptąjį raktą $G + B + A$.

5. Birutė pasiima viešai padėtą Antano paruoštą tirpalą, papildo jį savo spalvos tirpalu ir gauna slaptąjį raktą $G + A + B$.

Jie abu turi tą patį raktą, nes skysčių maišymo rezultatas nepriklauso nuo eiliškumo (komutatyvi operacija). Visi gali stebėti šį procesą, bet patys nesugebės pasigaminti tokio pačio mišinio – iš mišinių $G + A$, $G + B$ negalime gauti jo sudėtinių dalių A, B.

1. Antanas ir Birutė susitaria, kad naudos didelį pirminį skaičių p ir kitą skaičių $2 \leq g \leq p-2$.

2. Antanas atsitiktinai pasirenka savo skaičių $a \in \{1, \ldots, p-2\}$, apskaičiuoja

$$A = g^a \mod p$$

ir nusiunčia jį Birutei.

3. Birutė atsitiktinai pasirenka savo skaičių $b \in \{1, \ldots, p-2\}$, apskaičiuoja

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

ir nusiunčia jį Antanui.

4. Antanas apskaičiuoja slaptąjį raktą

$$K = B^a \mod p = g^{ba} \mod p.$$

Birutė apskaičiuoja slaptąjį raktą

$$K = A^b \mod p = g^{ab} \mod p.$$

Taigi jie nesaugiu kanalu saugiai pasikeitė slaptu raktu.

Atlikite skaičiavimus, kai $p = 17$, $g = 3$, $a = 7$, $b = 4$. Turite parodyti, kad $K = 4$.

DH algoritmo saugumas grindžiamas šios dienos matematikos žiniomis, kad multiplikatyviosioms liekanų klasių grupėms neegzistuoja greitieji diskrečiojo logaritmo skaičiavimo algoritmai. $a = \mathrm{d}\log_g A$ gali būti surandamas tik sprendžiant uždavinį

$$g^a = A \mod p.$$

Tokio uždavinio sprendimui turime tik pilno perrinkimo algoritmą (greitesnės modifikacijos grindžiamos sveikųjų skaičių faktorizavimu).

Situacija yra visai kitokia, kai naudojame adityviąją liekanų klasių grupę. Tada diskretųjį logaritmą labai efektyviai skaičiuojame klasikiniu Euklido algoritmu.
Turime rasti uždavinio

$$g \cdot a = A \mod p$$

sprendinį. Kadangi p yra pirminis skaičius, tai $\gcd(p, g) = 1$. Euklido algoritmu apskaičiuojame $x, y \in \mathbb{Z}$:

$$g \cdot x + p \cdot y = 1.$$

Tada

$$g \cdot x \cdot A - A = p \cdot (-y) \cdot A,$$

todėl skaičiaus A diskretųjį logaritmą surandame iš paprasto ekvivalentumo sąryšio:

$$a \equiv x \cdot A \mod p.$$

Su artėjančiomis Kalėdomis!