# Diszkrét logaritmus probléma és a Diffie-Hellman kulcscsere

Tóth Kitti

2025. 06. 06.

# A diszkrét logaritmus probléma

A diszkrét logaritmus probláma az alábbi módon fogalmazható meg: legyen adott $G = \mathbb{Z}_p$ és legyen $g \in G$ egy generátorelem ebben a csoportban, valamint $c \in \mathbb{Z}_p^*$ egy tetszőleges másik elem. Keressük azt az $x$ egész számot, melyre teljesül az alábbi:

$$c \equiv g^x \pmod{p}.$$

Ezt a problámát röviden DLP-nek szokás hívni.

# Bébi-lépés-Óriás-lépés

Az algoritmus lépései röviden:

- Meghatározzuk $m = \lceil \sqrt{p} \rceil$ értékét
- Minden $i \in \{1, \ldots, m\}$ esetén kiszámoljuk $g^i$ értékét, és az $(i, g^i)$ párokat rögzítjük egy táblázatba
- A táblázat elemeit rendezzük növekvő sorrendbe $g^i$ értékei szerint
- Számítsuk ki $g^{-m}$ értékét
- Számítsuk ki az $cg^{-jm}$ értékeket, ahol $j \in \{1, \ldots, m-1\}$, majd ellenőrizzük, hogy ezek közül van-e olyan, amely szerepel a táblázatunkban
- Ha találunk olyen indexet, mellyel egyezést kapunk, akkor $cg^{-jm} = g^i$
- rendezve: $c = g^{jm+i}$

# Bébi-lépés-Óriás-lépés

Az algoritmus az alábbi egyszerű SageMath kóddal is leírható:

```
m=ceil(sqrt(n))
L=[(g^k)%n for k in [0..m-1]]
j=0
while not (a*g^(-m*j))%n in L:
    j=j+1
i=L.index((a*g^(-m*j))%n)
sol=(i+j*Nm)%(m-1)
print(sol)
```

# Index-kalkulus módszer

Három fő lépésből áll:

1. **Relációk gyűjtése:** Választunk egy faktorbázist $B = \{p_1, \ldots, p_t\}$ kis prímekből. Olyan $u$ kitevőket keresünk, hogy:
$$g^u \equiv p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_t^{\gamma_t} \mod p$$
Legalább $s \gg t$ lineárisan független relációra van szükség.
2. **Lineáris rendszer megoldása:** A kapott relációkból egy lineáris kongruenciarendszert állítunk fel, amelyből meghatározhatók az $\mathrm{ind}_g(p_i)$ értékek:
$$\sum_{j=1}^{t} \gamma_{ij} \mathrm{ind}_g(p_j) \equiv u_i \mod (p-1) \quad \forall i = 1, \ldots, s$$
3. **A keresett logaritmus meghatározása:** Keresünk $\alpha$-t, amire $cg^\alpha$ a faktorbázissal felírható. Ekkor:
$$\mathrm{ind}_g(c) \equiv -\alpha + \sum_{i=1}^{t} \gamma_i \mathrm{ind}_g(p_i) \mod p-1$$

# Pollard-$\rho$ módszer diszkrét logaritmusra

A **Pollard-$\rho$ algoritmus** egy véletlen séta segítségével oldja meg a diszkrét logaritmus problémát:

- Legyen $G = \mathbb{Z}_p$, ennek egy generátora $g$, és oldjuk meg $c = g^x$-re a DLP-t.
- Véletlen sétát konstruálunk: $x_i = c^{u_i} g^{v_i}$, ahol $u_i, v_i \in \mathbb{Z}_p$.
- A konstrukció miatt előbb-utóbb két azonos elem keletkezik: $x_i = x_j$ valamely $i \neq j$-re.
- Ebből következik:

$$c^{u_i - u_j} = g^{v_j - v_i} \Rightarrow (u_i - u_j)\,\mathrm{ind}_g(c) \equiv v_j - v_i \mod p$$

- Ha $\gcd(u_i - u_j, n) = 1$, akkor:

$$\mathrm{ind}_g(c) \equiv (v_j - v_i)(u_i - u_j)^{-1} \mod p$$

- A séta lépéseit egy jól megválasztott függvény $f : G \to G$ definiálja, amely meghatározza $x_{i+1}$-et $x_i$-ből.

# Pollard-$\rho$: a véletlen séta konstruálása

Kezdeti értékek:

$$x_0 = 1, \quad u_0 = 0, \quad v_0 = 0$$

A következő lépéseket az $x_i$ érték nagysága szerint határozzuk meg:

$$x_{i+1} = \begin{cases} ax_i & \text{ha } 0 \leq x_i < \frac{p}{3} \\ x_i^2 & \text{ha } \frac{p}{3} \leq x_i < \frac{2p}{3} \\ bx_i & \text{ha } \frac{2p}{3} \leq x_i < p \end{cases}$$

$$u_{i+1} = \begin{cases} u_i + 1 & \text{ha } 0 \leq x_i < \frac{p}{3} \\ 2u_i & \text{ha } \frac{p}{3} \leq x_i < \frac{2p}{3} \\ u_i & \text{ha } \frac{2p}{3} \leq x_i < p \end{cases} \qquad v_{i+1} = \begin{cases} v_i & \text{ha } 0 \leq x_i < \frac{p}{3} \\ 2v_i & \text{ha } \frac{p}{3} \leq x_i < \frac{2p}{3} \\ v_i + 1 & \text{ha } \frac{2p}{3} \leq x_i < p \end{cases}$$

# Diffie–Hellman kulcscsere

A **Diffie–Hellman kulcscsere** a diszkrét logaritmus probléma kriptográfiai alkalmazása, amely lehetővé teszi, hogy két fél biztonságosan megállapodjon egy közös titkos kulcsban nyilvános csatornán keresztül.

- Választott csoport: $G = \mathbb{Z}_p$, generátorelem: $g$
- **A fél**: választ egy titkos $a \in \{1, \ldots, p-1\}$ számot, elküldi $g^a$ mod $p$-t B-nek
- **B fél**: választ egy titkos $b \in \{1, \ldots, p-1\}$ számot, elküldi $g^b$ mod $p$-t A-nak
- Mindkét fél kiszámolja a közös kulcsot:

$$\text{A: } (g^b)^a \equiv g^{ab} \mod p, \quad \text{B: } (g^a)^b \equiv g^{ab} \mod p$$

A módszer biztonsága azon alapul, hogy a lehallgató fél nem tudja hatékonyan meghatározni $g^{ab}$ mod $p$-t csupán $g$, $g^a$, $g^b$ ismeretében. Ezt nevezzük **Diffie–Hellman problémának (DHP)**.

# Elliptikus görbe definíciója

(a) Legyen $K$ egy test, ahol $\text{char}(K) > 3$, és legyen $x^3 + ax + b$ egy harmadfokú polinom $a, b \in K$, amelynek nincs többszörös gyöke.
Ekkor egy $K$ feletti elliptikus görbe:

$$E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

ahol $\mathcal{O}$ a „végtelenben levő" pont.

(b) Ha $\text{char}(K) = 2$, akkor egy elliptikus görbe $K$ felett olyan pontok halmaza, ahol az $(x, y) \in K \times K$ pontokra teljesül:

$$y^2 + cy = x^3 + ax + b \quad \text{vagy} \quad y^2 + xy = x^3 + ax^2 + b$$

ahol $a, b, c \in K$, és az egyenlet jobb oldalán szereplő harmadfokú polinomnak lehet többszörös gyöke is.

(c) Ha $\text{char}(K) = 3$, akkor egy $K$ feletti elliptikus görbe az alábbi alakú:

$$y^2 = x^3 + ax^2 + bx + c$$

ahol $a, b, c \in K$, és a jobb oldali polinomnak nincs többszörös gyöke.

# Diffie–Hellman kulcscsere elliptikus görbéken

- A és B megállapodnak:
  - egy nyilvános $E$ elliptikus görbében az $\mathbb{F}_p$ test felett,
  - és egy $P \in E$ pontban, amelynek rendje egy nagy prím.
- A választ egy titkos $a \in \mathbb{N}$ számot, és kiszámolja $aP$-t.
- B választ egy titkos $b \in \mathbb{N}$ számot, és kiszámolja $bP$-t.
- Nyílt csatornán elküldik egymásnak $aP$ és $bP$ pontokat.
- A közös kulcs mindkettőjük számára:

$$abP = a(bP) = b(aP)$$

# A DLP és a DHP kapcsolata

- Ha valaki meg tudja oldani a diszkrét logaritmus problémát, akkor ki tudja számítani DHP-ban szereplő titkos kitevőket, azaz $a$-t és $b$-t, és így a közös kulcsot is: $g^{ab} \mod p$.
- Tehát:

$$\text{DLP} \Rightarrow \text{DHP}$$

- Az viszont, hogy a Diffie–Hellman probléma megoldása szükségszerűen maga után vonja a DLP megoldhatóságát is az jelenleg nyitott kérdés.

Köszönöm a figyelmet!