

Debreceni Egyetem
Természettudományi és Technológiai Kar
Matematikai Intézet

Szakdolgozat

Kriptográfiai eljárások implementálása a SageMath programcsomagba

készítette:

Dsupin Krisztián

témavezető: Dr. Tengely Szabolcs

Debrecen, 2018

Tartalomjegyzék

1	Bevezetés	3
1.1	Diszkrét logaritmus probléma	3
1.2	Diszkrét logaritmus probléma véges csoportokban	4
2	Gyenge GDLP két speciális generátorral	5
2.1	Gyenge GDLP SageMath-ben	8
2.2	A megoldást végző program forráskódja	10
3	Gyenge GDLP két tetszőleges generátorral	12
3.1	Gyenge GDLP SageMath-ben	15
3.2	Az általános megoldást végző program forráskódja	17

Köszönetnyilvánítás

Szeretnék köszönetet mondani témavezetőmnek Dr. Tengely Szabolcsnak a sok segítségért, biztatásért és a hasznos tanácsokért, amikkel nagyban hozzájárult e szakdolgozat létrejöttéhez. Köszönettel tartozom a családomnak és barátaimnak a támogatásukért, amivel segítették, hogy ez a dolgozat elkészülhessen.

1 Bevezetés

Több ma ismert kriptorendszer biztonsága egy matematikailag nehezen számítható problémán alapszik, mint például a diszkrét logaritmus probléma, egész számok faktorizációja, Diffie-Hellman probléma, stb. Ebben a dolgozatban a diszkrét logaritmus probléma kap kiemelt figyelmet [1].

1.1 Diszkrét logaritmus probléma

Tekintsük az α elem által generált véges ciklikus G csoportot, továbbá legyen $\beta \in G$ egy további elem. A tradicionális diszkrét logaritmus probléma (DLP) egy nem negatív x egész szám keresése, melyre $\alpha^x = \beta$.

A DLP-re épülő kriptográfiai modellek építésekor fontos követelmény a probléma nehezen kezelhetősége. A diszkrét logaritmus probléma számára gyakorlatban használatos csoportok $\mathbb{F}_q$ multiplikatív csoportja, továbbá nagyméretű ciklikus részcsoporthai megfelelően választott $\mathcal{E}$ elliptikus görbének $\mathbb{F}_q$ felett.

A probléma kezelhetősége függ a csoport reprezentációján. Például $\mathbb{Z}_n$ -ben DLP kérdése könnyen megoldható. Egy adott $\beta \in \mathbb{Z}_n$ és $\alpha \in \mathbb{Z}_n$ generátor esetén egyszerű olyan nemnegatív x megadása, melyre $x\alpha = \beta$. Mivel $\gcd(n, \alpha) = 1$, a kiterjesztett euklideszi algoritmus segítségével α multiplikatív inverze kiszámolható, amely DLP megoldását jelenti.

A diszkrét logaritmus probléma megoldására szolgáló algoritmusokat három csoportra oszthatjuk:

1. Algoritmusok melyek tetszőleges csoportban működnek [2].
Például: Brute-force keresés, Baby-step giant-step, Pollard-féle rho algoritmus.
2. Algoritmusok melyek tetszőleges csoportban működnek, és hatékonyok kis prímfaktor rendű csoportokban [3].
Például: Pohlig-Hellman algoritmus.
3. Algoritmusok melyek csak speciális csoportban működnek [3].
Például: index-kalkulus algoritmus.

1.2 Diszkrét logaritmus probléma véges csoportokban

Ahogy [4]-ban definiált általános diszkrét logaritmus probléma (GDLP) tetszőleges véges csoportra a következő: Legyen G véges véges csoport $\alpha_1, \dots, \alpha_t$ generátorokkal, továbbá adott $\beta \in G$. Határozzunk meg egy pozitív egész k -t és egészekből álló $(x_{11}, \dots, x_{1t}, \dots, x_{k1}, \dots, x_{kt})$ szám kt -st melyre:

$$\beta = \prod_{i=1}^k (\alpha_1^{x_{i1}} \dots \alpha_t^{x_{it}}).$$

Az $(x_{11}, \dots, x_{1t}, \dots, x_{k1}, \dots, x_{kt})$ szám kt -st az $\alpha_1, \dots, \alpha_t$ -re vonatkozó β általános diszkrét logaritmusnak nevezzük.

Ha

$$S_k = \left\{ \prod_{i=1}^k (\alpha_1^{x_{i1}} \dots \alpha_t^{x_{it}}) \mid x_{ij} \in \mathbb{Z}_{n_j} \right\}$$

ahol n_j jelöli α_j rendjét. A legkisebb pozitív egész k_0 , melyre $\forall k > k_0, G \subseteq S_k$ -t a G csoport $(\alpha_1, \dots, \alpha_t)$ -re vonatkozó mélységének nevezzük.

Adott $\mathbb{F}_q$ test és n rögzített természetes szám. Az $n \times n$ reguláris mátrixok csoportját a mátrixszorzás műveletével n fokú általános lineáris csoportként ismert $\mathbb{F}_q$ felett, jelölése $GL(n, q)$. Könnyen látható, hogy $|GL(n, q)| = \prod_{i=0}^{n-1} (q^n - q^i)$. Az 1 determinánsú mátrixok hamaza $GL(n, q)$ -ban részcsoportot alkot, melyet speciális lineáris csoportnak nevezünk, jelölése $SL(n, q)$. $SL(n, q)$ a $\det : GL(n, q) \rightarrow \mathbb{F}_q^*$ homorfizmus magja, és ennél fogva $|SL(n, q)| = |GL(n, q)| / (q - 1)$. $GL(n, q)$ centruma a $\{\lambda I \mid \lambda \in \mathbb{F}_q^*\}$ alakú, $SL(n, q)$ centruma $\{\lambda I \mid \lambda^n = 1\}$ alakú mátrixokból áll. Az n rendű projektív lineáris csoport alatt $\mathbb{F}_q$ felett $PSL(n, q) = SL(n, q) / Z(SL(n, q))$ -t értjük. Itt csak az $n = 2$ esettel foglalkozunk majd, ahol q páratlan, tehát $|PSL(2, q)| = (q^2 - 1)q/2$.

2 Gyenge GDLP két speciális generátorral

Tekintsük $G = PSL(2, p)$ csoport, ahol p páratlan prím. Legyen α, β két teszőleges, nem felcserélhető, p rendű eleme a G csoportnak, továbbá legyenek $H, K \leq G$ részcsoporthok α , illetve β generátorral. [5]-ben a szerző megmutatja, hogy G -t generálja α és β , továbbá $G = HKHK$. Ezenfelül G mélysége α és β generátorokkal egyenlő kettővel.

A továbbiakban feltesszük, hogy G csoportot $SL(2, p)$ -beli mátrixok reprezentálják, $-I$ faktorig, ahol I a 2×2 -es egységmátrix.

Tekintsünk A, B mátrixokat az alábbi módon:

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

Ekkor A és B p rendű, nem felcserélhető, és G -t generálja. Megmutatjuk, hogy az általános diszkrét logaritmus probléma a G csoportban hatékonyan megoldható.

Feltéve, hogy $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in G$, $m_{11}, m_{12}, m_{21}, m_{22} \in \mathbb{F}_p$. Mivel G kettő mélységű, ezért M reprezentálható $M = A^i B^j A^k B^l$ módon, ahol i, j, k, l nemnegatív egészek. Az általános diszkrét logaritmus probléma megoldása, egy nemnegatívokból álló rendezett (i, j, k, l) négyes megtalálását jelenti, ahol $M = A^i B^j A^k B^l$.

Vegyük észre, hogy

$$A^i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}, \quad \text{és} \quad B^j = \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix}.$$

Amiből következik

$$A^i B^j A^k B^l = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ l & 1 \end{pmatrix}.$$

Emiatt

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} 1 + ij + l((1 + ij)k + i) & (1 + ij)k + i \\ j + l(jk + 1) & jk + 1 \end{pmatrix}.$$

A mátrix egyes elemeinek kiszámolásával az alábbi négy egyenletből álló és (i, j, k, l) ismeretlenes egyenletrendszerhez jutunk:

$$\begin{aligned} 1 + ij + l((1 + ij)k + i) &= m_{11} \\ (1 + ij)k + i &= m_{12} \\ j + l(jk + 1) &= m_{21} \\ jk + 1 &= m_{22} \end{aligned}$$

Az egyenletrendszer megoldható i, j, k, l -ra Gröbner bázist használva. Legyen I ideál

$$\begin{aligned} I = \langle & 1 + ij + l((1 + ij)k + i) - m_{11}, \\ & (1 + ij)k + i - m_{12}, \\ & j + l(jk + 1) - m_{21}, \\ & jk + 1 - m_{22} \rangle. \end{aligned}$$

I ideál GB Gröbner bázisa a racionális számok halmaza felett:

$$\begin{aligned} GB = [& l - jim_{21} + jm_{11} - m_{21}, \\ & k + im_{22} - m_{12}, \\ & jim_{12}m_{21} + ji + jm_{11}m_{12} - m_{11} + m_{12}m_{21} + 1, \\ & jim_{22} - jm_{12} + m_{22} - 1, \\ & m_{11}m_{22} - m_{12}m_{21} - 1]. \end{aligned}$$

Tehát az általános diszkrét logaritmus probléma megoldása $PSL(2, p)$ -ben, ekvivalens az alábbi egyenletrendszer megoldásával.

$$\begin{aligned} l - jim_{21} + jm_{11} - m_{21} &= 0 \\ k + im_{22} - m_{12} &= 0 \\ jim_{22} - jm_{12} + m_{22} - 1 &= 0. \end{aligned}$$

Az egyenletrendszernek általában több megoldása létezik. Az alábbi állítás módszert biztosít megoldáskereséshez, ha $M \in G$.

Állítás 2.1. Legyenek A, B és M mátrixok az előbb használt értékekkel. Ekkor létezik $n < p$ nemnegatív egész, hogy $nm_{22} - m_{12} \neq 0$ és olyan (i, j, k, l)

számnégyes, hogy $i = n$, $j = (1 - m_{22})(nm_{22} - m_{12})^{-1}$, $k = m_{12} - nm_{22}$, $l = (1 - m_{22})(nm_{21} - m_{11})(nm_{22} - m_{12})^{-1} + m_{21}$ mely megoldás $M = A^i B^j C^k D^l$ problémára.

Bizonyítás. Direkt számítással igazolható, hogy (i, j, k, l) kielégítik a fenti egyenletrendszer. n létezését $M \in PSL(2, p)$ biztosítja és emiatt b, d nem lehet egyszerre nulla. $\square$

Példa 2.1. Az alábbi példa szemlélteti a módszert: Tekintsük $G = PSL(2, 7)$ csoportot $SL(2, 7)$ -beli mátrixokkal reprezentálva modulo $\pm I$. Legyenek $A, B, M \in G$ az alábbiak:

$$M = \begin{pmatrix} 5 & 2 \\ 6 & 4 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Az M, A, B mátrix által meghatározott általános diszkrét logaritmus kiszámítása megfelel (i, j, k, l) nemnegatív számnégyes meghatározásának, melyre

$$M = A^i B^j C^k D^l.$$

Az egyenletrendszer melyet korábban meghatároztunk így alakul:

$$\begin{aligned} 1 + ij + l((i + ij)k + i) &= 5 \\ (i + ij)k + i &= 2 \\ j + l(jk + 1) &= 6 \\ jk + 1 &= 4. \end{aligned}$$

2.1 miatt $(i, j, k, l) = (0, 5, 2, 2)$. $\mathbb{F}_7$ -beli mátrix szorzásból adódik, hogy $M = A^0 B^5 C^2 D^2$.

2.1 Gyenge GDLP SageMath-ben

A fenti példa megoldása SageMath [6] programcsomagban:

$$p = \boxed{7} \quad \blacksquare$$

$$M = \begin{array}{|c|c|} \hline 5 & 2 \\ \hline 6 & 4 \\ \hline \end{array} \quad \blacksquare$$

Legyenek adottak az alábbi mátrixok:

$$M = \begin{pmatrix} 5 & 2 \\ 6 & 4 \end{pmatrix}, A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Célunk olyan (i, j, k, l) számnégyes megtalálása, ahol:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^i \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^j \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^l = \begin{pmatrix} 5 & 2 \\ 6 & 4 \end{pmatrix}$$

A mátrix egyes elemeinek kiszámolásával az alábbi (i, j, k, l) ismeretlenes egyenletrendszerhez jutunk:

$$\begin{aligned} ijk + i + j + kl + 1 &= 5 \\ ijk + i + k &= 2 \\ jkl + j + l &= 6 \\ jk + 1 &= 4 \end{aligned}$$

Az egyenletrendszer megoldását könnyíti a Gröbner bázis megadása, amelyhez legyen I ideál az alábbi:

$$[ijk + i + j + kl + 3, ijk + i + k + 5, jkl + j + l + 1, jk + 4]$$

A keresett Gröbner bázis:

$$[kl + 2k + 6, i + 2k + 3, j + 4l + 1]$$

Az eredeti egyenletrendszer megoldása ekvivalens az Gröbner bázis segítségével konstruált egyenletrendszer megoldásával:

$$\begin{aligned} kl + 2k + 6 &= 0 \\ i + 2k + 3 &= 0 \\ j + 4l + 1 &= 0 \end{aligned}$$

Az egyenletrendszer megoldásai az alábbi (i, j, k, l) számnégyesek:

$$\begin{aligned} (0, 5, 2, 2) \\ (1, 2, 5, 1) \\ (2, 3, 1, 6) \\ (3, 6, 4, 0) \\ (5, 1, 3, 3) \\ (6, 4, 6, 4) \end{aligned}$$

Interaktív megvalósítás SageMath-ben.

Másik példának tekintsük az $M = \begin{pmatrix} 8 & 13 \\ 16 & 7 \end{pmatrix} \in PSL(2, 17)$ mátrixot. Az így adódó GDLP megoldásai SageMath segítségével a következők:

$p =$

$M =$

8	13
16	7

Legyenek adottak az alábbi mátrixok:

$$M = \begin{pmatrix} 8 & 13 \\ 16 & 7 \end{pmatrix}, A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Célunk olyan (i, j, k, l) számnégyes megtalálása, ahol:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^i \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^j \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^l = \begin{pmatrix} 8 & 13 \\ 16 & 7 \end{pmatrix}$$

A mátrix egyes elemeinek kiszámolásával az alábbi (i, j, k, l) ismeretlenes egyenletrendszerhez jutunk:

$$\begin{aligned} ijk + i + il + kl + 1 &= 8 \\ ijk + i + k &= 13 \\ jkl + j + l &= 16 \\ jk + 1 &= 7 \end{aligned}$$

Az egyenletrendszer megoldását könnyíti a Gröbner bázis megadása, amelyhez legyen I ideál az alábbi:

$$[ijk + i + il + kl + 10, ijk + i + k + 4, jkl + j + l + 1, jk + 11]$$

A keresett Gröbner bázis:

$$[kl + 5k + 13, i + 5k + 3, j + 7l + 1]$$

Az eredeti egyenletrendszer megoldása ekvivalens az Gröbner bázis segítségével konstruált egyenletrendszer megoldásával:

$$\begin{aligned} kl + 5k + 13 &= 0 \\ i + 5k + 3 &= 0 \\ j + 7l + 1 &= 0 \end{aligned}$$

Az egyenletrendszer megoldásai az alábbi (i, j, k, l) számnégyesek:

$$\begin{aligned} (0, 7, 13, 11) \\ (1, 1, 6, 7) \\ (2, 11, 16, 8) \\ (3, 12, 9, 3) \\ (4, 3, 2, 14) \\ (5, 9, 12, 1) \\ (6, 8, 5, 6) \\ (7, 14, 15, 10) \\ (8, 5, 8, 4) \\ (9, 6, 1, 16) \\ (10, 16, 11, 0) \\ (11, 10, 4, 13) \\ (12, 15, 14, 5) \\ (13, 13, 7, 15) \\ (15, 4, 10, 9) \\ (16, 2, 3, 2) \end{aligned}$$

2.2 A megoldást végző program forráskódja

```
1 @interact(layout=[['Pmx','M']])
2 def _(Pmx=input_grid(1,1, default = [[7]], label='$p$'),
3     M=input_grid(2,2, default = [[5,2],[6,4]],
4         ↪ label='$M$')):
5     p=Pmx[0][0]; M=matrix(GF(p),2,2,M)
6     if M not in SL(2,p):
7         pretty_print(html(r'<center>$$s \notin SL(2,%s)
8             ↪ '$(latex(M),latex(p))$'))
9     else:
10         P.<i,j,k,l>=PolynomialRing(GF(p),4)
11         Ptmp.<X1,X2,X3,X4>=PolynomialRing(ZZ,4)
12         A=matrix(GF(p),[[1,1],[0,1]])
13         B=matrix(GF(p),[[1,0],[1,1]])
14         pretty_print('Legyenek adottak az alábbi mátrixok:')
15         pretty_print('M=',M,', A=',A,', B=',B);print
16         pretty_print ('\\nCélunk olyan $(i,j,k,l)$ számnégyes
17             ↪ megtalálása, ahol:')
18         html(r'<center>$$s^i s^j s^k s^l = s$'
19             ↪ '$(latex(A),latex(B),latex(A),latex(B),latex(M))$');print
20         pretty_print ('\\nA mátrix egyes elemeinek
21             ↪ kiszámolásával az alábbi $(i,j,k,l)$ ismeretlenes
22             ↪ egyenletrendszerhez jutunk:')
23         Ai=matrix(P,[[1,i],[0,1]]); Ak=matrix(P,[[1,k],[0,1]])
24         Bj=matrix(P,[[1,0],[j,1]]); Bl=matrix(P,[[1,0],[1,1]])
25         Mi=Ai*Bj*Ak*Bl
26
27         I=ideal(Mi[v][w]-M[v][w] for v in [0..1] for w in
28             ↪ [0..1])
29         for v in [0..3]:
30             pretty_print(Mi.list()[v], '=',M[v//2][v%2])
31         print
32         pretty_print('Az egyenletrendszer megoldását könnyíti a
33             ↪ Gröbner bázis megadása, amelyhez legyen $I$ ideál
34             ↪ az alábbi:')
35         IList=[Mi.list()[w]-M[w//2][w%2] for w in [0..3]]
36         pretty_print(IList);print
37         pretty_print('A keresett Gröbner bázis:')
38         GB=I.groebner_basis()
```

```

30     pretty_print(GB);print
31     pretty_print('Az eredeti egyenletrendszer megoldása
    ↪     ekvivalens az Gröbner bázis segítségével konstruált
    ↪     egyenletrendszer megoldásával:')
32     for z in [0..len(GB)-1]:
33         pretty_print(GB[z], '=', 0)
34     print
35     var('x1,x2,x3,x4')
36     S=[Ptmp(g(i=X1,j=X2,k=X3,l=X4))
    ↪     (X1=x1,X2=x2,X3=x3,X4=x4)==0 for g in GB]
37     pretty_print('Az egyenlerszer megoldásai az alábbi
    ↪     $(i,j,k,l)$ számnégyesek:')
38     Sol=solve_mod(S,p)
39     for t in [0..len(Sol)-1]:
40         pretty_print(Sol[t])

```

3 Gyenge GDLP két tetszőleges generátorral

Tegyük fel, hogy C, D két nem felcserélhető, p rendű elem $G = PSL(2, p)$ -ben, továbbá tekintsük A és B mátrixokat az előző fejezetben definiált módon. Bármely adott $M \in G$ esetén a célunk i, j, k, l egészek meghatározása, melyre:

$$M = C^i D^j C^k D^l.$$

Olyan $g \in G = PSL(2, p)$ elemet keresünk, mely teljesíti a következőket valamely nemnegatív $s, t < p$ egészekre:

$$C = g^{-1} A^s g \quad \text{és} \quad D = g^{-1} B^t g.$$

Ezzel ekvivalens módon valamely $g \in G$ esetén $gC = A^s g$ és $gD = B^t g$, valamely $s, t < p$ egészekre. Mivel $g = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$, így egy g_1, g_2, g_3, g_4 változókkal adott egyenletrendszerhez jutunk, amiből g meghatározható.

Amennyiben $g \in G$ elemet már meghatároztuk.

$$\begin{aligned} M &= C^i D^j C^k D^l \\ &= (g^{-1} A^s g)^i (g^{-1} B^t g)^j (g^{-1} A^s g)^k (g^{-1} B^t g)^l \\ &= (g^{-1} A^{si} g) (g^{-1} B^{tj} g) (g^{-1} A^{sk} g) (g^{-1} B^{tl} g) \\ &= g^{-1} A^{si} B^{tj} A^{sk} B^{tl} g. \end{aligned}$$

Legyenek $x = si, y = tj, v = sk, w = tl$. Ekkor:

$$\begin{aligned} M &= g^{-1} A^x B^y A^v B^w g \\ gMg^{-1} &= A^x B^y A^v B^w. \end{aligned}$$

Jelölje $M_1 = gMg^{-1}$. Természetesen $M_1 \in G$, továbbá:

$$M_1 = A^x B^y A^v B^w.$$

Így visszavezettük a tetszőleges C, D generátorokkal adott általános diszkrét logaritmus problémát, az előző részben már megoldott két speciális A, B generátorokkal adott problémára.

Mivel esetünkben minden nemnulla elemnek létezik inverze, így i, j, k, l elemek a következő módon számolhatók ki:

$$i = xs^{-1}, \quad j = yt^{-1}, \quad k = vs^{-1}, \quad l = wt^{-1}$$

ahol minden művelet modulo p értendő.

Végezetül az $s = 0$ vagy $t = 0$ eset nem fordulhat elő, mivel $C = g^{-1}A^s g$ és $D = g^{-1}B^t g$. Amennyiben $s = 0$, abból A^s megegyezik az egységmátrixszal, vagyis C úgyszintén az egységmátrixszal egyenlő, ami ellentmondana C p -rendűségének. Hasonlóan adódik, hogy $t \neq 0$.

Példa 3.1. Feltéve, hogy a $G = PSL(2, p)$ csoportok $SL(2, 7)$ -beli mátrixokkal reprezentálhatók $-I$ faktorig. Legyenek adottak C, D nem felcserélhető 7 rendű mátrixok, és $M \in G$ az alábbi módon adottak:

$$M = \begin{pmatrix} 3 & 5 \\ 2 & 6 \end{pmatrix}, \quad C = \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}, \quad D = \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix}.$$

Célunk kiszámolni M általános diszkrét logaritmus problémáját tekintettel (C, D) -re, vagyis olyan nemnegatív i, j, k, l egészek találása, mely esetén $M = C^i D^j C^k D^l$.

Olyan $g = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$ elemet keresünk, mely teljesíti a következőket valamely nem negatív $s, t < p$ egészekre, $C = g^{-1}A^s g$ és $D = g^{-1}B^t g$. Vagyis:

$$\begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix} = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}^{-1} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}.$$

Az egyenleteket rendezve, majd a mátrix elemeit tekintve az alábbi egyenletrendszerhez jutunk:

$$\begin{aligned} g_1 + 4g_2 &= 0 \\ 5g_1 - g_2 &= 0 \\ -g_1 t + g_3 - g_4 &= 0 \\ -g_2 t + 5g_3 - g_4 &= 0 \\ -g_3 s + 4g_1 + g_2 &= 0 \\ -g_4 s + 4g_1 + 3g_2 &= 0 \\ 4g_3 + 5g_4 &= 0 \\ g_3 + 3g_4 &= 0. \end{aligned}$$

A Gröbner bázis meghatározásával a GDLP megoldása a következőképpen egyszerűsödik:

$$\begin{aligned} g_4 s + g_2 &= 0 \\ g_2 t + 2g_4 &= 0 \\ g_1 + 4g_2 &= 0 \\ g_3 + 3g_4 &= 0. \end{aligned}$$

Az egyenletekből az egyes változókat g_1 segítségével kifejezve $g_4 = -\frac{g_2}{s}$, $g_1 = -4g_2$, $g_3 = -3g_4$. Ezeket a g mátrixba visszahelyettesítve

$$g \cdot C - A^s \cdot g = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{és} \quad g \cdot D - B^t \cdot g = \begin{pmatrix} 0 & 0 \\ \frac{4g_2 st - g_2}{s} & \frac{-g_2 st + g_2}{s} \end{pmatrix}$$

adódik. Ezek segítségével s, t lehetséges értékei meghatározhatók, melyek a most tárgyalt példa esetében

$$(s, t) \in \{(1, 2), (6, 5), (3, 3), (5, 6), (4, 4), (2, 1)\}$$

lehetnek. Ezek közül tetszőleges megoldáshoz vezet, válasszuk ki például $s = 1, t = 2$ értékeket további számoláshoz. Ezeket visszahelyettesítve $G \cdot C - A^s \cdot G$ és $g \cdot D - B^t \cdot g$ mátrixba, négyismeretlenes egyenletrendszerhez jutunk meghatározhatóak g_1, g_2, g_3, g_4 értékei, amik az előbb kiválasztott s, t értékek esetén az alábbiak lehetnek:

$$(g_1, g_2, g_3, g_4) \in \{(6, 2, 6, 5), (1, 5, 1, 2), (14, 6, 4, 1), (5, 4, 5, 3), (2, 3, 2, 4), (3, 1, 3, 6)\}.$$

Ismét egy tetszőleges megoldást választva, például $(6, 2, 6, 5)$ számnégyest $g = \begin{pmatrix} 6 & 2 \\ 6 & 5 \end{pmatrix}$ mátrix adódik. Kiszámolva $M_1 = G \cdot M \cdot G^{-1} = \begin{pmatrix} 3 & 3 \\ 1 & 6 \end{pmatrix}$ mátrixot, vagyis az olyan (x, y, v, w) számnégyeseket keresünk, melyek kielégítik $M_1 = A^x B^y A^v B^w$ egyenletet. A 2 részben mutatott módszer segítségével

$$(x, y, v, w) \in \{(0, 4, 3, 3), (1, 3, 4, 2), (2, 1, 5, 0), (3, 2, 6, 1), (5, 5, 1, 4), (6, 6, 2, 5)\}.$$

Az $M = C^i D^j C^k D^l$ GDLP probléma megoldásai tehát a következő:

$$(i, j, k, l) \in \{(0, 2, 3, 5), (1, 5, 4, 1), (2, 4, 5, 0), (3, 1, 6, 4), (5, 6, 1, 2), (6, 3, 2, 6)\}.$$

3.1 Gyenge GDLP SageMath-ben

Tekintsük az előző példa megoldását SageMath programcsomagban.

$p =$

7

 $M =$

3	5
2	6

 $C =$

5	1
5	4

 $D =$

2	5
4	0

Legyenek adottak az alábbi mátrixok:

$$M = \begin{pmatrix} 3 & 5 \\ 2 & 6 \end{pmatrix}, C = \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}, D = \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix}, G = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$$

Célunk olyan (i, j, k, l) számnégyes megtalálása, ahol:

$$\begin{pmatrix} 3 & 5 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}^i \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix}^j \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}^k \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix}^l$$

A korábbi fejezetben definiált A, B mátrixok segítségével. A probléma megoldható egy G mátrix segítségével melyre:

$$\begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix} = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \quad \text{és} \quad \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$$

Ehhez az alábbi egyenletrendszer megoldása szükséges:

$$\begin{aligned} g_1 + 4g_2 &= 0 \\ 5g_1 - g_2 &= 0 \\ -g_1t + g_3 + 4g_4 &= 0 \\ -g_2t + 5g_3 - g_4 &= 0 \\ -g_3s + 4g_1 + 5g_2 &= 0 \\ -g_4s + g_1 + 3g_2 &= 0 \\ 4g_3 + 5g_4 &= 0 \\ g_3 + 3g_4 &= 0 \end{aligned}$$

Az egyenletrendszer megoldását megkönnyíti a Gröbner bázis megadása, amelyhez ez esetben:

$$[g_4s + g_2, g_2t + 2g_4, g_1 + 4g_2, g_3 + 3g_4]$$

A Gröbner bázisból g_1, g_2, g_3, g_4 változók kifejezése g_2 segítségével:

$$[x_4 = -\frac{g_2}{s}, x_1 = -4x_2, x_3 = -3x_4]$$

A G mátrixba visszahelyettesítve az imént kiszámolt g_1, g_2, g_3, g_4 értékeket, majd kiszámolva $G1 = G \cdot C - A^s \cdot G$, $G2 = G \cdot D - B^t \cdot G$ adódik:

$$G1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{és} \quad G1 = \begin{pmatrix} 0 & 4g_2st - g_2 \\ 0 & -g_2st + 2g_2 \end{pmatrix}$$

$G1$ és $G2$ elemet figyelembe véve s és t -re adódó feltételek:

$$\{(1, 2), (6, 5), (3, 3), (5, 6), (4, 4), (2, 1)\}$$

A lehetséges s, t értékek közül válasszul például $s = 1, t = 2$

Ezeket visszahelyettesítve $G1$ és $G2$ mátrixokba, majd az adódó négyismeretlenes egyenletrendszert megoldva g_1, g_2, g_3, g_4 értékei az alábbiak lehetnek

$$\begin{aligned} (6, 2, 6, 5) \\ (1, 5, 1, 2) \\ (4, 6, 4, 1) \\ (5, 4, 5, 3) \\ (2, 3, 2, 4) \\ (3, 1, 3, 6) \end{aligned}$$

Egy szabadon választott megoldást kiválasztva, például $(6, 2, 6, 5)$, a g_1, g_2, g_3, g_4 elemek közül, adódik az alábbi G mátrix

$$G = \begin{pmatrix} 6 & 2 \\ 6 & 5 \end{pmatrix}$$

Alkalmazzuk a speciális generátorokkal használt módszert $M_1 = G * M * G^{-1}$ -re, ahol:

$$M_1 = \begin{pmatrix} 3 & 3 \\ 1 & 6 \end{pmatrix} = \begin{pmatrix} 6 & 2 \\ 6 & 5 \end{pmatrix} \begin{pmatrix} 3 & 5 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

Az eredeti egyenletrendszer megoldásai az alábbi (i, j, k, l) számnégyesek:

$$\begin{aligned} (0, 2, 3, 5) \\ (1, 5, 4, 1) \\ (2, 4, 5, 0) \\ (3, 1, 6, 4) \\ (5, 6, 1, 2) \\ (6, 3, 2, 6) \end{aligned}$$

Vagyis az $(0, 2, 3, 5)$ megoldása a GDLP problémának, ugyanis:

$$\begin{pmatrix} 3 & 5 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}^0 \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix}^2 \begin{pmatrix} 5 & 1 \\ 5 & 4 \end{pmatrix}^3 \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix}^5$$

Másik példának tekintsük az $M = \begin{pmatrix} 3 & 3 \\ 11 & 7 \end{pmatrix}, C = \begin{pmatrix} 5 & 6 \\ 6 & 10 \end{pmatrix}, D = \begin{pmatrix} 7 & 10 \\ 12 & 8 \end{pmatrix}$ $PSL(2, 13)$ -beli mátrixokat. Az így adódó GDLP megoldásai SageMath segítségével a következők:

$$p = \begin{array}{|c|} \hline 13 \\ \hline \end{array} \quad M = \begin{array}{|c|c|} \hline 3 & 3 \\ \hline 11 & 7 \\ \hline \end{array} \quad C = \begin{array}{|c|c|} \hline 5 & 6 \\ \hline 6 & 10 \\ \hline \end{array} \quad D = \begin{array}{|c|c|} \hline 7 & 10 \\ \hline 12 & 8 \\ \hline \end{array}$$

Legyenek adottak az alábbi mátrixok:

$$M = \begin{pmatrix} 3 & 3 \\ 11 & 7 \end{pmatrix}, C = \begin{pmatrix} 5 & 6 \\ 6 & 10 \end{pmatrix}, D = \begin{pmatrix} 7 & 10 \\ 12 & 8 \end{pmatrix}, G = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$$

Célunk olyan (i, j, k, l) számnégyes megtalálása, ahol:

$$\begin{pmatrix} 3 & 3 \\ 11 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 6 & 10 \end{pmatrix}^i \begin{pmatrix} 7 & 10 \\ 12 & 8 \end{pmatrix}^j \begin{pmatrix} 5 & 6 \\ 6 & 10 \end{pmatrix}^k \begin{pmatrix} 7 & 10 \\ 12 & 8 \end{pmatrix}^l$$

A korábbi fejezetben definiált A, B mátrixok segítségével. A probléma megoldható egy G mátrix segítségével melyre:

$$\begin{pmatrix} 5 & 6 \\ 6 & 10 \end{pmatrix} = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \quad \text{és} \quad \begin{pmatrix} 7 & 10 \\ 12 & 8 \end{pmatrix} = \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$$

Ehhez az alábbi egyenletrendszer megoldása szükséges:

$$\begin{aligned} 6g_1 - g_2 &= 0 \\ 10g_1 + 7g_2 &= 0 \\ -g_1t + 6g_3 - g_4 &= 0 \\ -g_2t + 10g_3 + 7g_4 &= 0 \\ -g_3s + 4g_1 + 6g_2 &= 0 \\ -g_4s + 6g_1 + 9g_2 &= 0 \\ 4g_3 + 6g_4 &= 0 \\ 6g_3 + 9g_4 &= 0 \end{aligned}$$

Az egyenletrendszer megoldását megkönnyíti a Gröbner bázis megadása, amelyhez ez esetben:

$$[g_4s + 3g_2, g_2t + 8g_4, g_1 + 2g_2, g_3 + 8g_4]$$

A Gröbner bázisból g_1, g_2, g_3, g_4 változók kifejezése g_2 segítségével:

$$[x_4 = -\frac{3x_2}{S}, x_1 = -2x_2, x_3 = -8x_4]$$

A G mátrixba visszahelyettesítve az imént kiszámolt g_1, g_2, g_3, g_4 értékeket, majd kiszámolva $G1 = G \cdot C - A^s \cdot G$, $G2 = G \cdot D - B^t \cdot G$ adódik:

$$G1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{és} \quad G1 = \begin{pmatrix} 0 & 0 \\ \frac{2g_2st+4g_2}{s} & \frac{-g_2st+11g_2}{s} \end{pmatrix}$$

$G1$ és $G2$ elemet figyelembe véve s és t -re adódó feltételek:

$$\{(6, 4), (10, 5), (5, 10), (4, 6), (12, 2), (8, 3), (3, 8), (11, 1), (2, 12), (7, 9), (1, 11), (9, 7)\}$$

A lehetséges s, t értékek közül válasszul például $s = 6, t = 4$

Ezeket visszahelyettesítve $G1$ és $G2$ mátrixokba, majd az adódó négyismeretlenes egyenletrendszert megoldva g_1, g_2, g_3, g_4 értékei az alábbiak lehetnek

$$\begin{aligned} (3, 5, 7, 4) \\ (11, 1, 4, 6) \\ (10, 8, 6, 9) \\ (2, 12, 9, 7) \\ (5, 4, 3, 11) \\ (8, 9, 10, 2) \\ (4, 11, 5, 1) \\ (7, 3, 12, 5) \\ (12, 7, 2, 3) \\ (1, 6, 11, 10) \\ (9, 2, 8, 12) \\ (6, 10, 1, 8) \end{aligned}$$

Egy szabadon választott megoldást kiválasztva, például $(3, 5, 7, 4)$, a $g1, g2, g3, g4$ elemek közül, adódik az alábbi G mátrix

$$G = \begin{pmatrix} 3 & 5 \\ 7 & 4 \end{pmatrix}$$

Alkalmazzuk a speciális generátorokkal használt módszert $M_1 = G * M * G^{-1}$ -re, ahol:

$$M_1 = \begin{pmatrix} 0 & 11 \\ 7 & 10 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 7 & 4 \end{pmatrix} \begin{pmatrix} 3 & 3 \\ 11 & 7 \end{pmatrix} \begin{pmatrix} 10 & 7 \\ 2 & 1 \end{pmatrix}$$

Az eredeti egyenlenszer megoldásai az alábbi (i, j, k, l) számnégyesek:

(0, 7, 4, 5)
(11, 12, 11, 11)
(9, 3, 5, 8)
(7, 11, 12, 2)
(5, 9, 6, 10)
(1, 4, 7, 4)
(12, 2, 1, 12)
(10, 10, 8, 6)
(8, 1, 2, 3)
(6, 6, 9, 9)
(4, 5, 3, 0)
(2, 8, 10, 1)

Vagyis az $(0, 7, 4, 5)$ megoldása a GDLP problémának, ugyanis:

$$\begin{pmatrix} 3 & 3 \\ 11 & 7 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 6 & 10 \end{pmatrix}^0 \begin{pmatrix} 7 & 10 \\ 12 & 8 \end{pmatrix}^7 \begin{pmatrix} 5 & 6 \\ 6 & 10 \end{pmatrix}^4 \begin{pmatrix} 7 & 10 \\ 12 & 8 \end{pmatrix}^5$$

3.2 Az általános megoldást végző program forráskódja

```

1  def sortfv(L):#sort by first variable
2      SL=[]
3      TL=[L[i][0] for i in range(0,len(L)-1)]
4      for j in range(0,len(L)-1):
5          SL.append(L[TL.index(max(TL))])
6          L.remove(L[TL.index(max(TL))])
7          TL.remove(TL[TL.index(max(TL))])
8      return SL
9
10 @interact(layout=[['Pmx','M','C','D']])
11 def sortfv(L):#sort by first variable
12     SL=[]
13     TL=[L[i][0] for i in range(0,len(L)-1)]
14     for j in range(0,len(L)-1):
15         SL.append(L[TL.index(max(TL))])
16         L.remove(L[TL.index(max(TL))])
17         TL.remove(TL[TL.index(max(TL))])
18     return SL
19
20 @interact(layout=[['Pmx','M','C','D']])
21 def _ (Pmx=input_grid(1,1, default = [[7]], label='$p=$'),
22       M=input_grid(2,2, default = [[3,5],[2,6]], label='$M=$'),
23       C=input_grid(2,2, default = [[5,1],[5,4]], label='$C=$'),
24       D=input_grid(2,2, default = [[2,5],[4,0]],
25       ↪ label='$D=$')):
```

```

25 p=Pmx[0][0]; M=matrix(GF(p),2,2,M); C=matrix(GF(p),2,2,C);
    ↪ D=matrix(GF(p),2,2,D)
26 if C.multiplicative_order()!=p or
    ↪ D.multiplicative_order()!=p:
27     pretty_print('Adjon meg másik mátrixokat, a megadott
        ↪ rangfeltételekkel')
28 else:
29     P.<g1,g2,g3,g4,s,t>=PolynomialRing(GF(p),6)
30     P.<i,j,k,l>=PolynomialRing(GF(p),4)
31     Ptmp.<X1,X2,X3,X4,Y1,Y2>=PolynomialRing(ZZ,6)
32     GVar=[g1,g2,g3,g4,s,t]
33     var('x1,x2,x3,x4,S,T')
34     G=matrix([[g1,g2],[g3,g4]])
35     As=matrix([[1,s],[0,1]])
36     Bt=matrix([[1,0],[t,1]])
37     N=matrix(2)
38
39     pretty_print('Legyenek adottak az alábbi mátrixok:')
40     pretty_print('M=',M,', C=',C,', D=',D,', G=',G)
41     html('<br><center>Célunk olyan $(i,j,k,l)$ számnégyes
        ↪ megtalálása, ahol:')
42     html(r'<center>$$s=%s^i%s^j%s^k%s^l$'%
        ↪ (latex(M),latex(C),latex(D),latex(C),latex(D)))
43     html('<br><center>A korábbi fejezetben definiált $A,B$
        ↪ mátrixok segítségével. A probléma megoldható egy
        ↪ $$ mátrix segítségével melyre:')
44     html(r'<center>$$s=%s%s%s \quad$ és $ \quad$
        ↪ $s=%s%s%s$'%(latex(C),latex(G),
        ↪ latex(As),latex(G),latex(D),latex(G),latex(Bt),latex(G)))
45     html('<br><center>Ezzel ekvivalens módon megoldandó:')
46     html(r'<center>$$s=%s%s-s%s^{ -1} \quad$ és $ \quad$
        ↪ $s=%s%s-s%s$'%(latex(N),latex(G),latex(C),latex(As),
        ↪ latex(G),latex(N),latex(G),latex(D),latex(Bt),latex(G)))
47
48     W1=G*D-Bt*G; W2=G*C-As*G
49     iw=ideal([W1[0,0],W1[0,1],W1[1,0],W1[1,1],W2[0,0],
        ↪ W2[0,1],W2[1,0],W2[1,1]])
50     html('<br><center>Ehhez az alábbi egyenlentsrendszer
        ↪ megoldásása szükséges:')
51     for y in [0..1]:
52         for z in [0..1]:

```

```

53         pretty_print(W1[y][z], '=', 0)
54     for y in [0..1]:
55         for z in [0..1]:
56             pretty_print(W2[y][z], '=', 0)
57
58     html('<br><center>Az egyenletrendszer megoldását
    ↳ megkönnyíti a Gröbner bázis megadása, amelyhez ez
    ↳ esetben:')
59     GB=iw.groebner_basis()
60     pretty_print(GB)
61     GBList=[] #GB with symbolic variables
62     for i in GB:
63         ↳ GBList.append(Ptmp(i(g1=X1,g2=X2,g3=X3,g4=X4,s=Y1,t=Y2))
64         ↳ (X1=x1,X2=x2,X3=x3,X4=x4,Y1=S,Y2=T))
65     XVar=[x1,x2,x3,x4]
66
67     #V1:variables in GB parts, V2:amount of variables,
68     ↳ V3:V2 sorted
69     V1=[y.variables() for y in GBList]
70     V2=[]
71     for y in [0..len(XVar)-1]:
72         n=0 #number for index
73         for z in [0..len(GBList)-1]:
74             if XVar[y] in V1[z]:
75                 n+=1
76                 V2.append((n,XVar[y]))
77     V3=sortfv(copy(V2));
78     x=V3[0][1];
79     ↳ g=Ptmp(x(x1=X1,x2=X2,x3=X3,x4=X4))(X1=g1,X2=g2,X3=g3,X4=g4)
80     ↳ #x:special xi element, g: x in GF(p)
81
82     PrevC=[] #PreviouslyChecked
83     ESol=[] #EquationSolutions
84     for y in [0..len(GBList)-1]:
85         VarT=list(V1[y])
86         z=0
87         lh=len(VarT)-1 #length
88         while z<=lh:
89             if bool(VarT[z]==x) or (VarT[z] in PrevC) or
90             ↳ (VarT[z] not in XVar):
91                 r=VarT.index(VarT[z]) #removable item

```

```

86         VarT.remove(VarT[r])
87         lh-=1
88     else:
89         z+=1
90     if len(VarT)!=0:
91         ESol.append((solve(GBList[y],VarT[0]))[0])
92     if len(VarT)!=0:
93         PrevC.append(VarT[0])
94 html('<br><center>A Gröbner bázisból $g1,g2,g3,g4$
    ↳ vátozók kifejezése $%s$ segítségével:%'(latex(g)))
95 pretty_print(ESol)
96
97 X=matrix(2,2,[x1,x2,x3,x4])
98 for i in [1..3]:
99     for y in ESol:
100         X=X.substitute({y.lhs():y.rhs()})
101
102
103     ↳ H=[Ptmp(a.numerator()(x1=X1,x2=X2,x3=X3,x4=X4,S=Y1,T=Y2))
104     ↳ (X1=g1,X2=g2,X3=g3,X4=g4,Y1=s,Y2=t)
105     ↳ /Ptmp(a.denominator()(x1=X1,x2=X2,x3=X3,x4=X4,S=Y1,T=Y2))
106     ↳ (X1=g1,X2=g2,X3=g3,X4=g4,Y1=s,Y2=t) for a in
107     ↳ copy(X.list())]
108 V=matrix(2,2,H)
109 G1=V*C-As*V; G2=V*D-Bt*V;
110 GmatList=[G1,G2]
111 html('<br><center> A $G$ mátrixba visszahelyettesítve
112     ↳ az imént kiszámolt $g1,g2,g3,g4$ értékeket, majd
113     ↳ kiszámolva $G1=G\cdot C-A^s\cdot G, \ G2=G\cdot
114     ↳ D-B^t\cdot G$ adódik:')
115 html('<center>$G1=%s \quad$ és $ \quad$
116     ↳ $G1=%s$'%(latex(G1),latex(G2)))
117 N=[]
118
119 for I in GmatList:
120     if I!=matrix(2):
121         for y in [0..1]:
122             for w in [0..1]:

```

```

114         if I[y][w] != 0: N.append(solve_mod(Ptmp
        ↪ ((I[y][w].numerator()/g)
        ↪ (g1=X1,g2=X2,g3=X3,g4=X4,s=Y1,t=Y2))
        ↪ (X1=x1,X2=x2,X3=x3,X4=x4,Y1=S,Y2=T),p))

115
116     for i in [0..len(N)-1]:
117         N[i]=Set(N[i])
118     ST=N[0]
119     for y in [1..len(N)-1]:
120         ST=ST.intersection(N[y])
121     html('<br><center>$G1$ és $G2$ elemet figyelembe véve
        ↪ $$ és $t$-re adódó feltételek:')
122     pretty_print(ST)
123
124     T1=W1(s=ST[0][0],t=ST[0][1]).list()
125     for y in [0..len(T1)-1]:
        ↪ T1[y]=Ptmp(T1[y](g1=X1,g2=X2,g3=X3,g4=X4,s=Y1,t=Y2))
        ↪ (X1=x1,X2=x2,X3=x3,X4=x4,Y1=S,Y2=T)
126     S1=Set(solve_mod(T1,p))
127     T2=W2(s=ST[0][0],t=ST[0][1]).list()
128     for y in [0..len(T2)-1]:
        ↪ T2[y]=Ptmp(T2[y](g1=X1,g2=X2,g3=X3,g4=X4,s=Y1,t=Y2))
        ↪ (X1=x1,X2=x2,X3=x3,X4=x4,Y1=S,Y2=T)
129     S2=Set(solve_mod(T2,p))
130     GEm=(S1.intersection(S2)).list() #GElements
131     if (0,0,0,0) in GEm:
132         GEm.remove((0,0,0,0))
133     html('<br><center>A lehetséges $s,t$ értékek közül
        ↪ válasszul például $s=%s$,
        ↪ $t=%s$'%(latex(ST[0][0]),latex(ST[0][1])))
134     html('<br><center>Ezeket visszahelyettesítve $G1$ és
        ↪ $G2$ mátrixokba, majd az adódó négyismeretlenes
        ↪ egyenletrendszert megoldva $g1,g2,g3,g4$ értékei az
        ↪ alábbiak lehetnek')
135     for y in GEm:
136         pretty_print(y)
137     G=matrix(GF(p),2,2,GEm[0])
138     html('<br><center>Egy szabadon választott megoldást
        ↪ kiválasztva, például $%s$, a $g1,g2,g3,g4$ elemek
        ↪ közül, adódik az alábbi $G$
        ↪ mátrix'%(latex(GEm[0])))

```

```

139     html('<center>$G=%s$'%(latex(G)))
140     W1=G*D-Bt*G
141     W2=G*C-As*G
142
143     P.<i,j,k,l>=PolynomialRing(GF(p),4)
144     M1=G*M*G.inverse(); MOr=M; M=M1
145
146     html('<center>Alkalmazzuk a speciális generátorokkal
147     ↪ használt módszert $M_1=G*M*G^{-1}$-re, ahol:')
148     html(r'<center>$M_1=%s=%s %s
149     ↪ %s$'%(latex(M1), latex(G), latex(MOr), latex(G.inverse()))))
150     Ai=matrix(P, [[1,i],[0,1]]); Ak=matrix(P, [[1,k],[0,1]])
151     Bj=matrix(P, [[1,0],[j,1]]); Bl=matrix(P, [[1,0],[1,1]])
152     Mi=Ai*Bj*Ak*Bl
153
154     I=ideal(Mi[v][w]-M[v][w] for v in [0..1] for w in
155     ↪ [0..1])
156     IList=[Mi.list()[w]-M[w//2][w%2] for w in [0..3]]
157     GB=I.groebner_basis()
158     LIS=[Ptmp(g(i=X1,j=X2,k=X3,l=X4))
159     ↪ (X1=x1,X2=x2,X3=x3,X4=x4)==0 for g in GB]
160     Sol=solve_mod(LIS,p)
161     s=ST[0][0]; t=ST[0][1]
162     SolFn=[]
163     for y in [0..len(Sol)-1]:
164         SolFn.append((Sol[y][0]*inverse_mod(int(s),p),
165         ↪ Sol[y][1]*inverse_mod(int(t),p),
166         ↪ Sol[y][2]*inverse_mod(int(s),p),
167         ↪ Sol[y][3]*inverse_mod(int(t),p)))
168     html('<br><center>Az eredeti egyenlerszer megoldásai az
169     ↪ alábbi $(i,j,k,l)$ számnégyesek:')
170     for t in [0..len(Sol)-1]:
171         pretty_print(SolFn[t])
172     html('<br><center>Vagyis az $s$ megoldása a GDLP
173     ↪ problémának, ugyanis:'%(latex(SolFn[0])))
174     html(r'<center>$s=%s^{%s}%s^{%s}%s^{%s}%s^{%s}$'
175     ↪ %(latex(MOr), latex(C), latex(SolFn[0][0]), latex(D),
176     ↪ latex(SolFn[0][1]), latex(C), latex(SolFn[0][2]),
177     ↪ latex(D), latex(SolFn[0][3])))

```

Irodalomjegyzék

- [1] Ivana Ilic. *The Discrete Logarithm Problem in Non-abelian Groups*. PhD thesis, Boca Raton, FL, USA, 2010.
- [2] Andrew V Sutherland. *Order Computations in Generic Groups*. PhD thesis, Cambridge, MA, USA, 2007.
- [3] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.
- [4] Lee C. Klingler, Spyros Magliveras, Fred Richman, and Michal Sramka. Discrete logarithms for finite groups. 85:3–19, 06 2009.
- [5] Michal Sramka. *New Results in Group Theoretic Cryptology*. PhD thesis, Boca Raton, FL, USA, 2006. AAI3239161.
- [6] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.1)*, 2018. <http://www.sagemath.org>.
- [7] Ivana Ilic and Spyros Magliveras. Weak discrete logarithms in non-abelian groups. 74, 08 2010.