Debreceni Egyetem
Természettudományi Kar
Matematikai Intézet

Diplomamunka/Szakdolgozat

Diszkrét logaritmus

készítette:

Vasenszki Zoltán

témavezető: Dr. Tengely Szabolcs

Debrecen, 2010.10.23.

Tartalomjegyzék

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani a szüleimnek, akik a kezdetektől fogva családi és anyagi hátteret biztosítottak számomra tanulmányaim sikeres befejezéséhez.

1. Bevezetés

A következő bevezető részben az algebra néhány alapvető, a csoportokkal foglalkozó eredményei kerülnek bemutatásra. A fejezet Bódi Béla Algebra [1] című könyvének a felhasználásával készült.

1.1. A csoport fogalma és néhány alapvető tulajdonságai

1.1.1. Definíció. Az A és a B adott halmazok $A \times B$ **direkt szorzat**a (vagy Descartes-féle szorzata) az

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

halmaz, ahol az (a, b) rendezett pár.

1.1.2. Definíció. Egy $A \times A \longrightarrow A$ leképezést **kétváltozós művelet**nek (vagy binér műveletnek) nevezünk.

Egy kétváltozós művelet egy adott A halmazon annak bármely két eleméhez egy harmadikat rendel: $\forall a, b \in A : (a, b) \in A$.

1.1.3. Definíció. (Műveletek tulajdonságai) Egy (kétváltozós) $* : A \times A \longrightarrow A$ művelet

1. **asszociatív**, ha:

$$\forall a, b, c \in A : (a * b) * c = a * (b * c)$$

2. **kommutatív**, ha:

$$\forall a, b \in A : a * b = b * a$$

Példák:

- A $\mathbb{Z}$ egész számok halmazán az azon definiált $+$ összeadás és $\cdot$ szorzás kommutatív és asszociatív, de a $-$ kivonásra egyik sem igaz.
- Az a, b $\mathbb{R}^n$-beli vektorok $< a, b > \in \mathbb{R}$ skaláris szorzatára igaz, hogy

$$< a, b > = < b, a >$$

tehát ez a kétváltozós művelet kommutatív.

- A mátrixok körében definiált szorzás asszociatív, hiszen ha $A \in \mathcal{M}_{m\times n}$, $B \in \mathcal{M}_{n\times p}$, $C \in \mathcal{M}_{p\times r}$, $D = A \cdot B$, $G = B \cdot C$, $F = (A \cdot B) \cdot C$ és $H = A \cdot (B \cdot C)$, akkor a mátrixok szorzásának definíciója szerint

$$d_{i,j} = \sum_k a_{i,k} \cdot b_{k,j}$$

$$g_{i,j} = \sum_k b_{i,k} \cdot c_{k,j}$$

és így

$$\begin{aligned} f_{i,j} &= \sum_k (\sum_l a_{i,l} \cdot b_{l,j}) \cdot c_{k,j} = \sum_k \sum_l a_{i,l} \cdot b_{l,k} \cdot c_{k,j} = \\ &= \sum_l a_{i,l} \cdot (\sum_k b_{l,k} \cdot c_{k,j}) = \sum_l a_{i,l} \cdot g_{l,j} = h_{i,j} \end{aligned}$$

viszont nem kommutatív, hiszen

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 3 \end{pmatrix} \neq \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

1.1.4. Definíció. $(G, *)$ neve **félcsoport**, ha $*$ egy kétváltozós asszociatív művelet a G halmazon.

Megjegyzés: ha $\exists e \in G$:

$$\forall a \in G : a * e = e * a = a$$

akkor G neve **egységelemes félcsoport**, e a $*$ műveletre nézve **neutrális elem**.

Például az $n \times n$-es $\mathbb{R}$ feletti mátrixok a mátrixszorzás művelettel félcsoportot alkotnak.

1.1.5. Definíció. G **csoport** a $*$ műveletre nézve, ha félcsoport és

$$\forall a \in G : \exists a^{-1} : a * a^{-1} = a^{-1} * a = e$$

Ha a $*$ művelet kommutatív, akkor **kommutatív csoport**(Abel-csoport).

Az a^{-1} elemet az a elem **inverzének** nevezzük.

Példák:

- A $\mathbb{Z}$ egész számok halmaza a rajtuk értelmezett $+$ összeadás műveletre tekintve kommutatív-csoport.
- az $n \times n$-es $\mathbb{R}$ feletti invertálható mátrixok a mátrixszorzás művelettel (nem kommutatív) csoport.

A csoportok néhány egyszerű tulajdonságai:

1.1.1. Tétel. *Bármely $(G,*)$ csoportra igazak a következők:*

1. *G neutrális eleme egyértelmű*
2. *G minden elemének inverze egyértelmű*
3. *$\forall a \in G$-re $(a^{-1})^{-1} = a$*
4. *$\forall a,b \in G$-re $(a*b)^{-1} = b^{-1} * a^{-1}$*

Bizonyítás. 1. Legyenek e és f neutrális elemei a csoportnak, ekkor a neutrális elem definícióját felhasználva

$$e = e * f = f * e = f$$

nyerhető, így a neutrális elem valóban egyértelmű.

2. Legyenek $a,b,c \in G$, b,c egyaránt az a elem inverzei. Ekkor

$$c = c * e = c * (a * b) = (c * a) * b = e * b = b$$

adódik, a $*$ művelet asszociativitása miatt, tehát a csoport tetszőleges elemének inverze egyértelmű.

3. A harmadik állítás következik a másodikból, hiszen ha egy elem inverzének az inverze egy harmadik elem lenne, nem állna fenn az egyértelműség.

4.

$$(a*b)*(b^{-1}*a^{-1}) = a*(b*(b^{-1}*a^{-1})) = a*((b*b^{-1})*a^{-1}) = a*(e*a^{-1}) = e$$

□

1.2. A csoportok és elemeik rendje, részcsoportok

1.2.1. Definíció. Egy G csoport **véges**, ha elemeinek száma véges, ez a szám a **csoport rendje**.
Jele: $ord(G)$
Nem véges elemszámú csoport rendje végtelen.

1.2.2. Definíció. Legyen $a \in (G,*)$. Ha $a^m = 1$, $m \in \mathbb{Z}$ (a hatványozása a $*$ művelet ismételt végrehajtása önmagával), akkor a **véges rendű**, ha $\nexists n : n < m, a^n = 1$, akkor m az a rendje. Ha nem létezik ilyen véges szám, akkor a **végtelen rendű** elem.
Jele: $ord(a)$

1.2.1. Tétel. *Ha $a \in G$ rendje n, akkor $a^m = 1$-ből $n|m$ következik.*

Bizonyítás. Az m szám maradékos osztással előáll $m = n \cdot q + r$ alakban, ahol $0 \leq r < n$, ebből pedig

$$a^m = a^{n \cdot q + r} = (a^n)^q \cdot a^r = a^r = 1$$

miatt $r = 0$. □

1.2.3. Definíció. Legyen $(G, *)$ csoport, $H \subseteq G$. Ha $(H, *)$ csoport, akkor a H csoport **részcsoport**ja a G-nek.

1.2.2. Tétel. *Egy $H \subseteq G$ halmaz akkor és csak akkor részcsoport, ha $\forall a, b \in H$: $a^{-1} * b \in H$.*

Bizonyítás. Ha H részcsoport, akkor minden $a, b \in H$ esetén $a^{-1} * b \in H$ teljesül.

A másik irány belátásának feltéltele, hogy $a^{-1} * b \in H$ igaz minden $a, b \in H$-re. Kell, hogy a csoportművelet asszociatív legyen a H halmazon, ez a tulajdonság öröklődik G-ből. Kell továbbá a neutrális elem és az inverz elemek létezése. A feltevés szerint $\forall c \in H : e = c * c^{-1} \in H$ és ebből $c^{-1} * e \in H$, tehát létezik neutrális elem, és minden elemnek létezik az inverze is, tehát H részcsoportja G-nek.

□

1.2.4. Definíció. Legyen G csoport, $u \in G$, $H \subseteq G$ részcsoportja. Ekkor az

$$uH = \{u * h | \forall h \in H\}$$

$$Hu = \{h * u | \forall h \in H\}$$

halmazokat a G csoport H részcsoport szerinti **baloldali** és **jobboldali mellékosztály**ainak nevezzük.

Megjegyzés: Abel-csoportok esetén uH és Hu megegyeznek $\forall u$ esetén.

Példa: $n > 1$ esetén $n\mathbb{Z}$ az n-el osztható számok halmaza. A $(\mathbb{Z}, +)$ csoport $n\mathbb{Z}$ szerinti mellékosztályai a modulo n maradékosztályok.

1.2.3. Tétel. *Legyen $H \subseteq G$ részcsoport. Ekkor:*

1. $c \in bH \Longrightarrow cH = bH$
2. $bH \cap cH = \emptyset$ *és* $bH = cH$

közül pontosan az egyik igaz.

Bizonyítás. 1. $c \in H$ miatt c írható $b * h_1$ alakban, ahol $h_1 \in H$. Tetszőleges $c * h \in cH$ elemre

$$c * h = (b * h_1) * h = b * (h_1 * h) \Longrightarrow c * h \in bH \Longrightarrow cH \subseteq bH$$

Hasonlóan belátható a másik irányú tartalmazás.

2. Tegyük fel, hogy $c \in aH \cap bH$. Ekkor $cH = aH$ és $cH = bH \Longrightarrow aH = bH$

□

Megjegyzés: ebből a két tulajdonságból következik, hogy a G csoport H szerinti baloldali mellékosztályai G-nek egy osztályozását adják.

1.2.4. Tétel. ***(Lagrange-tétel)*** *Ha $H \subseteq G$ részcsoportja és G véges, akkor $ord(H)|ord(G)$.*

Bizonyítás. Legyen a G egy osztályozása $a_1H, a_2H, \ldots, a_sH$. Ekkor $G = a_1H \cup a_2H \cup \ldots \cup a_sH$, ahol $i \neq j$ esetén $a_iH \cap a_jH = \emptyset$.
$ord(a_iH) = ord(H)$, emiatt

$$|G| = |a_1H| + |a_2H| + \ldots + |a_sH| = s|H|$$

□

1.2.5. Definíció. A G csoport egy M részhalmazát a csoport **generátorrendszer**ének nevezzük, ha az őt tartalmazó legszűkebb részhalmaz G.

1.2.6. Definíció. Az egy elemmel generált csoport neve **ciklikus csoport**.

Példa: $\mathbb{Z}/p\mathbb{Z}$ ciklikus.

1.2.5. Tétel. *Ha egy véges csoport rendje prím, akkor a csoport ciklikus.*

Bizonyítás. Legyen a G csoport rendje p prím, $a \in G$ a neutrális elemtől különböző. Az a által generált H részcsoport rendje Lagrange tétele miatt osztja G rendjét, p-t, tehát az is egyenlő p-vel, és így $H = G$ ciklikus csoport. □

2. Diszkrét logaritmus

Ezen fejezet célja a diszkrét logaritmus problémának (DLP) és annak egy lehetséges megoldásának, az index kalkulus módszernek a bemutatása. A fejezet Raminder Ruprai az interneten fellelhető Improvements in the Index-Calculus algorithm for Solving the Discrete Logarithm problem over $\mathbb{F}_p$ [3] című munkájából merít.

2.1. A diszkrét logaritmus probléma

A diszkrét logaritmus probléma (DLP) a következő módon értelmezhető:

$$a^x = b$$

ahol $a, b \in G$ valamilyen G csoportra, $b \in < a >$ (b az a által generált részcsoport eleme), a hatványozás a csoportművelet ismételt végrehajtását jelöli, és az $x \in \mathbb{Z}$ meghatározása a feladat.

A DLP legjobban $\mathbb{Z}/p\mathbb{Z}$ fölött szemléltethető, ezért a továbbiakban csak ez a speciális eset kerül tárgyalásra.

2.1.1. Definíció. Legyenek $a, b \in \mathbb{Z}/p\mathbb{Z}$, p prím, a pedig generátora $\mathbb{Z}/p\mathbb{Z}$-nek. Ekkor a diszkrét logaritmus problémája olyan $x \in \mathbb{Z}$ keresése, melyre

$$a^x \equiv b \pmod{p}$$

teljesül.

2.1.2. Definíció. Legyen $n, p \in \mathbb{N}$. Az n **p-sima**, ha n kanonikus alakjában fellépő összes prímtényező nem nagyobb, mint p.

Példa: A 84 szám $84 = 2^2 \cdot 3 \cdot 7$ miatt 7-sima.

2.2. Az index kalkulus módszer

Legyen B egy halmaz, melynek tagjai néhány pozitív prím. Ekkor B neve **faktorbázis**.

2.2.1. Definíció. Egy $n \in \mathbb{N}$ szám **F-sima**, ha az n kanonikus alakjában fellépő prímek mind elemei az F faktorbázisnak:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_l^{r_l}$$

$$F = \{\dots, p_1, p_2, \dots, p_l, \dots\}$$

Az eljárás elején választunk egy véletlenszerű $t \in (1 \dots p-1)$ számot, és erre kiszámítjuk

$$a^t \equiv c \pmod{p}$$

értékét, és c-t mint egész számot faktorizájuk.
Ekkor c kanonikus alakja:

$$c = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_l^{r_l}$$

Amennyiben c B-sima, úgy a kanonikus alakjának logaritmusát véve adódik a

$$t \equiv r_1 \log_a p_1 + r_2 \log_a p_2 + \dots + r_l \log_a p_l \pmod{p-1}$$

egyenlet, melyben a logaritmus értékek az ismeretlenek. Ha legalább l darab ilyen véletlenszerűen választott t számot találunk, akkor egy olyan egyenletrendszer nyerhető, melyből a p_i prímek diszkrét logaritmusa meghatározható.

Megjegyzés: A különböző egyenletek együtthatóiból kapott szám l-esek mint vektorok közül legalább l darab vektor lineáris függetlensége szükséges a megoldhatósághoz.

Ezzel megkaptuk a B minden elemének a diszkrét logaritmusát.

A következő lépésben véletlenszerű q számokra vizsgáljuk, hogy $a^q \cdot b$ B-sima-e modulo p. Ha igen, akkor

$$a^q \cdot b \equiv p_1^{d_1} \cdot p_2^{d_2} \cdot \dots \cdot p_n^{d_n} \pmod{p}$$

alakban írható, ahol $p_i,\ i \in \{1 \dots n\}$ a B faktorbázis elemei. Ennek a logaritmusát véve

$$q + \log_a b \equiv d_1 \log_a p_1 + d_2 \log_a p_2 + \dots + d_n \log_a p_n \pmod{p}$$

adódik, melyből csak a $x = \log_a b$ nem ismert, ennek értéke (mely a probléma megoldása) átrendezéssel nyerhető.

2.3. Példa az algoritmus működésére

A feladat: $19^k = 4 \pmod{5209}$.
A faktorbázis $\{2, 3, 5\}$.
Ekkor:

$$\begin{aligned} 19^{30} &\equiv 2 \cdot 3 \cdot 5 \pmod{5209} \\ 19^{180} &\equiv 2 \cdot 3^2 \cdot 5^2 \pmod{5209} \\ 19^{274} &\equiv 2^4 \cdot 3^2 \cdot 5 \pmod{5209} \end{aligned}$$

melynek logaritmusát véve

$$\begin{aligned} 30 &\equiv \log_{19} 2 + \log_{19} 3 + \log_{19} 5 \pmod{5208} \\ 180 &\equiv \log_{19} 2 + 2 \cdot \log_{19} 3 + 2 \cdot \log_{19} 5 \pmod{5208} \\ 274 &\equiv 4 \cdot \log_{19} 2 + 2 \cdot \log_{19} 3 + \log_{19} 5 \pmod{5208} \end{aligned}$$

adódik.
Az egyenletrendszert megoldva a választott prímek logaritmusai:

$$\begin{aligned} \log_{19} 2 &\equiv 5088 \pmod{5208} \\ \log_{19} 3 &\equiv 604 \pmod{5208} \\ \log_{19} 5 &\equiv 4754 \pmod{5208} \end{aligned}$$

Ebből, és a $19^{60} \cdot 4 \equiv 2^4 \cdot 3^2 \cdot 5^2 \pmod{5209}$ kongruenciából

$$\begin{aligned} 60 + \log_{19} 4 \equiv 4 \cdot \log_{19} 2 + 2 \cdot \log_{19} 3 + 2 \cdot \log_{19} 5 \equiv \\ 4 \cdot 5088 + 2 \cdot 3208 + 2 \cdot 4754 \equiv 31008 \equiv 4968 \pmod{5208} \end{aligned}$$

az eredmény $k = 4968$.

2.4. Faktorbázis és a kiválasztás módszere

A definícióban azt mondtuk, hogy a t érték véletlenszerűen választott, de érdemes megvizsgálni, hogy hogyan változik a lefutási idő (lépésszámokban mérve), ha ehelyett egyesével lépegetünk végig az $[1 \dots p-1]$-beli egész számokon, valamint azt, hogy ha az algoritmus bemeneténél egy adott faktorbázis helyett egy nagyobb, például a kétszerese szerepel.

Ennek megfelelően egy partikuláris problémát négyféleképpen fogunk megoldani,

egyszer a t véletlenszerűen kerül kiválasztásra, egyszer pedig befutja az $[1 \dots p-1]$-beli egészeket mindaddig, amíg meg nem lesz a megoldáshoz elegendő számú egyenelet. Mindkét módszert alkalmazzuk egy kisebb és egy kétszer akkora számosságú faktorbázisra.

Legyen a probléma $47^k \equiv 126 \pmod{25219}$.

Első eset: t véletlenszerű választása a $B = \{2, 3, 5, 7\}$ faktorbázissal:

A következő egyenletek adódtak:

$$\begin{aligned} 47^{10828} &\equiv 2 \cdot 3 \cdot 5 \pmod{25219} \\ 47^{11107} &\equiv 3^3 \cdot 5 \pmod{25219} \\ 47^{8299} &\equiv 2 \cdot 3^2 \cdot 5 \cdot 7 \pmod{25219} \\ 47^{11411} &\equiv 3 \cdot 5^4 \pmod{25219} \end{aligned}$$

ahol a baloldalon álló hatványkitevők a véletlen t értékek.

A rendszer logaritmusát véve

$$\begin{aligned} 10828 &\equiv \log_{47} 2 + \log_{47} 3 + \log_{47} 5 \pmod{25218} \\ 11107 &\equiv 3 \cdot \log_{47} 3 + \log_{47} 5 \pmod{25218} \\ 8299 &\equiv \log_{47} 2 + 2 \cdot \log_{47} 3 + \log_{47} 5 + \log_{47} 7 \pmod{25218} \\ 11411 &\equiv \log_{47} 3 + 4 \cdot \log_{47} 5 \pmod{25218} \end{aligned}$$

adódik.

Az egyenletrendszert megoldva a faktorbázis elemeinek logaritmusai:

$$\begin{aligned} \log_{47} 2 &\equiv 1139 \pmod{25219} \\ \log_{47} 3 &\equiv 709 \pmod{25219} \\ \log_{47} 5 &\equiv 8980 \pmod{25219} \\ \log_{47} 7 &\equiv 21980 \pmod{25219} \end{aligned}$$

A megoldás $k = 24537$.

Második eset: t véletlenszerű választása a $B = \{2, 3, 5, 7, 11, 13, 17, 19\}$ faktorbázissal:

A következő egyenletek adódtak:

$$
\begin{aligned}
47^{630} &\equiv 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \pmod{25219} \\
47^{24286} &\equiv 2^3 \cdot 3^3 \cdot 7^2 \pmod{25219} \\
47^{18342} &\equiv 2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 19 \pmod{25219} \\
47^{14901} &\equiv 2^3 \cdot 5^2 \cdot 7^2 \pmod{25219} \\
47^{14017} &\equiv 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \pmod{25219} \\
47^{17147} &\equiv 2 \cdot 3^4 \cdot 7 \cdot 11 \pmod{25219} \\
47^{3445} &\equiv 2^4 \cdot 3^3 \cdot 7 \pmod{25219} \\
47^{17009} &\equiv 2 \cdot 7^2 \cdot 17 \pmod{25219}
\end{aligned}
$$

ahol a baloldalon álló hatványkitevők a véletlen t értékek.

A rendszer logaritmusát véve

$$
\begin{aligned}
630 &\equiv 2 \cdot \log_{47} 2 + 2 \cdot \log_{47} 3 + \log_{47} 5 + \log_{47} 7 + \log_{47} 11 \pmod{25218} \\
24286 &\equiv 3 \cdot \log_{47} 2 + 3 \cdot \log_{47} 3 + 2 \cdot \log_{47} 7 \pmod{25218} \\
18342 &\equiv 2 \cdot \log_{47} 2 + \log_{47} 3 + \log_{47} 5 + \log_{47} 13 + \log_{47} 19 \pmod{25218} \\
14901 &\equiv 3 \cdot \log_{47} 2 + 2 \cdot \log_{47} 5 + 2 \cdot \log_{47} 7 \pmod{25218} \\
14017 &\equiv \log_{47} 2 + 2 \cdot \log_{47} 3 + \log_{47} 7 + \log_{47} 11 + \log_{47} 13 + \log_{47} 17 \pmod{25218} \\
17147 &\equiv \log_{47} 2 + 4 \cdot \log_{47} 3 + \log_{47} 7 + \log_{47} 11 \pmod{25218} \\
3445 &\equiv 4 \cdot \log_{47} 2 + 3 \cdot \log_{47} 3 + \log_{47} 7 \pmod{25218} \\
17009 &\equiv \log_{47} 2 + 2 \cdot \log_{47} 7 + \log_{47} 17 \pmod{25218}
\end{aligned}
$$

adódik.
Az egyenletrendszert megoldva a faktorbázis elemeinek logaritmusai:

$$
\begin{aligned}
\log_{47} 2 &\equiv 1139 \pmod{25219} \\
\log_{47} 3 &\equiv 709 \pmod{25219} \\
\log_{47} 5 &\equiv 8980 \pmod{25219} \\
\log_{47} 7 &\equiv 21980 \pmod{25219} \\
\log_{47} 11 &\equiv 16410 \pmod{25219} \\
\log_{47} 13 &\equiv 23506 \pmod{25219} \\
\log_{47} 17 &\equiv 22346 \pmod{25219} \\
\log_{47} 19 &\equiv 8087 \pmod{25219}
\end{aligned}
$$

A megoldás itt is $k = 24537$.

Harmadik eset: t sorban való próbálgatása 1-től 25218-ig, a $B = \{2, 3, 5, 7\}$ faktorbázissal:

A következő egyenletek adódtak:

$$\begin{aligned} 47^{28} &\equiv 2 \cdot 3^3 \cdot 7 \pmod{25219} \\ 47^{179} &\equiv 2^3 \cdot 7 \pmod{25219} \\ 47^{12623} &\equiv 2 \cdot 5^2 \cdot 7^2 \pmod{25219} \\ 47^{12676} &\equiv 2^2 \cdot 3^2 \cdot 5 \pmod{25219} \end{aligned}$$

ahol a baloldalon álló hatványkitevők a véletlen t értékek.

A rendszer logaritmusát véve

$$\begin{aligned} 28 &\equiv \log_{47} 2 + 3 \cdot \log_{47} 3 + \log_{47} 7 \pmod{25218} \\ 179 &\equiv 3 \cdot \log_{47} 2 + \log_{47} 7 \pmod{25218} \\ 12623 &\equiv \log_{47} 2 + 2 \cdot \log_{47} 5 + 2 \cdot \log_{47} 7 \pmod{25218} \\ 12676 &\equiv 2 \cdot \log_{47} 2 + 2 \cdot \log_{47} 3 + \log_{47} 5 \pmod{25218} \end{aligned}$$

adódik.
Az egyenletrendszert megoldva a faktorbázis elemeinek logaritmusai nem változtak:

$$\begin{aligned} \log_{47} 2 &\equiv 1139 \pmod{25219} \\ \log_{47} 3 &\equiv 709 \pmod{25219} \\ \log_{47} 5 &\equiv 8980 \pmod{25219} \\ \log_{47} 7 &\equiv 21980 \pmod{25219} \end{aligned}$$

Az eredmény természetesen ismét $k = 24537$.

Negyedik eset: t sorban való próbálgatása 1-től 25218-ig, a $B = \{2, 3, 5, 7, 11, 13, 17, 19\}$ faktorbázissal:

A következő egyenletek adódtak:

$$\begin{aligned} 47^{10} &\equiv 5^3 \cdot 13 \pmod{25219} \\ 47^{28} &\equiv 2 \cdot 3^3 \cdot 7 \pmod{25219} \\ 47^{136} &\equiv 2 \cdot 3 \cdot 13 \pmod{25219} \\ 47^{153} &\equiv 2^6 \cdot 3^3 \cdot 11 \pmod{25219} \\ 47^{12623} &\equiv 2 \cdot 5^2 \cdot 7^2 \pmod{25219} \\ 47^{12632} &\equiv 7^3 \cdot 17 \pmod{25219} \\ 47^{12643} &\equiv 2^4 \cdot 19 \pmod{25219} \\ 47^{12676} &\equiv 2^2 \cdot 3^2 \cdot 5 \pmod{25219} \end{aligned}$$

ahol a baloldalon álló hatványkitevők a véletlen t értékek.

A rendszer logaritmusát véve

$$\begin{aligned}
10 &\equiv 3 \cdot \log_{47} 5 + \log_{47} 13 \pmod{25218} \\
28 &\equiv \log_{47} 2 + 3 \cdot \log_{47} 3 + \log_{47} 7 \pmod{25218} \\
136 &\equiv \log_{47} 2 + \log_{47} 3 + \log_{47} 13 \pmod{25218} \\
153 &\equiv 6 \cdot \log_{47} 2 + 3 \cdot \log_{47} 3 + \log_{47} 11 \pmod{25218} \\
12623 &\equiv \log_{47} 2 + 2 \cdot \log_{47} 5 + 2 \cdot \log_{47} 7 \pmod{25218} \\
12632 &\equiv 3 \cdot \log_{47} 7 + \log_{47} 17 \pmod{25218} \\
12643 &\equiv 4 \cdot \log_{47} 2 + \log_{47} 19 \pmod{25218} \\
12676 &\equiv 2 \cdot \log_{47} 2 + 2 \cdot \log_{47} 3 + \log_{47} 5 \pmod{25218}
\end{aligned}$$

adódik.
Az egyenletrendszert megoldva a faktorbázis elemeinek logaritmusai:

$$\begin{aligned}
\log_{47} 2 &\equiv 1139 \pmod{25219} \\
\log_{47} 3 &\equiv 709 \pmod{25219} \\
\log_{47} 5 &\equiv 8980 \pmod{25219} \\
\log_{47} 7 &\equiv 21980 \pmod{25219} \\
\log_{47} 11 &\equiv 16410 \pmod{25219} \\
\log_{47} 13 &\equiv 23506 \pmod{25219} \\
\log_{47} 17 &\equiv 22346 \pmod{25219} \\
\log_{47} 19 &\equiv 8087 \pmod{25219}
\end{aligned}$$

A megoldás itt is $k = 24537$.

3. Magma kód

Itt a példák számításához használt programcsomag, a MAGMA [2] ingyenes, interneten elérhető változatához íródott kódok találhatóak.

Az alább látható lépegetős módszer kódjánál figyelembe kell venni azt, hogy az alguritmus mindenféleképpen $n \times n$-es együtthatómátrixot keres a faktorbázis elemeinek a logaritmusának megtalálásához (ahol n a faktorbázis számossága), pedig lehetséges, hogy az kevesebb egyenletből is nyerhető lenne.

```
IK:=function(a,b,p,FB)
   FBsub:={k: k in Subsets(SequenceToSet(FB))|#k gt 0};
   fac:=Factorization(p-1);
   facB:=[t[1]^t[2]: t in fac];
   kitevok:={};
   Lm1:=(p-1) div 2;
   s:=1;
   logMatrix:=ZeroMatrix(Integers(p-1),#FB,#FB);
   logVector:=Vector(Integers(p-1),[0: l in [1..#FB]]);
   k:=1;
   while not s eq #FB+1 do
      if not k in kitevok then
         pd:=PrimeDivisors(a^k mod p);
         pdm:=PrimeDivisors((-a^k) mod p);
         if SequenceToSet(pd) in FBsub then
            kitevo_vektor:=Vector(Integers(p-1),[Valuation(a^k mod p,FB[l]):
            l in [1..#FB]]);
            logmatrix:=logMatrix;
            logmatrix[s]:=kitevo_vektor;
            if &and[Rank(ChangeRing(logmatrix,GF(t))) eq s: t in facB] then
               logVector[s]:=k;
               logMatrix:=logmatrix;
               s:=s+1;
            end if;
         end if;
         if SequenceToSet(pdm) in FBsub and s lt #FB then
```

```
            kitevo_vektor:=Vector(Integers(p-1),[Valuation(-a^k mod p,FB[l]):
            l in [1..#FB]]);
            logmatrix:=logMatrix;
            logmatrix[s]:=kitevo_vektor;
            if &and[Rank(ChangeRing(logmatrix,GF(t))) eq s: t in facB] then
               logVector[s]:=k-Lm1;
               logMatrix:=logmatrix;
               s:=s+1;
            end if;
         end if;
         kitevok:=kitevok join {k};
      end if;
      k:=k+1;
   end while;
   time logSol:=Solution(Transpose(logMatrix),logVector);

   kitevok2:={};
   nyer:=false;
   k:=1;
   while not nyer do
      if not k in kitevok then
         pdb:=PrimeDivisors((a^k*b) mod p);
            if SequenceToSet(pdb) in FBsub then
               kitevo_vektor2:=Vector(Integers(p-1),[Valuation((a^k*b) mod p,
               FB[l]): l in [1..#FB]]);
               logeredmeny:=Integers(p-1)!((&+[kitevo_vektor2[t]*logSol[t]:
               t in [1..#FB]])-k);
               nyer:=true;
               print k;
            end if;
            kitevok2:=kitevok2 join {k};
         end if;
         k:=k+1;
   end while;

   return logMatrix,logVector,logeredmeny;
end function;
```

A másik, véletlenszerűen kereső algoritmus kódja:

```
IK:=function(a,b,p,FB)
   FBsub:={k: k in Subsets(SequenceToSet(FB))|#k gt 0};
```

```
fac:=Factorization(p-1);
facB:=[t[1]^t[2]: t in fac];
kitevok:={};
Lm1:=(p-1) div 2;
s:=1;
logMatrix:=ZeroMatrix(Integers(p-1),#FB,#FB);
logVector:=Vector(Integers(p-1),[0: l in [1..#FB]]);
while not s eq #FB+1 do
   k:=Random([1..p-1]);
   if not k in kitevok then
      pd:=PrimeDivisors(a^k mod p);
      pdm:=PrimeDivisors((-a^k) mod p);
      if SequenceToSet(pd) in FBsub then
         kitevo_vektor:=Vector(Integers(p-1),[Valuation(a^k mod p,FB[l]):
         l in [1..#FB]]);
         logmatrix:=logMatrix;
         logmatrix[s]:=kitevo_vektor;
         if &and[Rank(ChangeRing(logmatrix,GF(t))) eq s: t in facB] then
            logVector[s]:=k;
            logMatrix:=logmatrix;
            s:=s+1;
         end if;
      end if;
      if SequenceToSet(pdm) in FBsub and s lt #FB then
         kitevo_vektor:=Vector(Integers(p-1),[Valuation(-a^k mod p,FB[l]):
         l in [1..#FB]]);
         logmatrix:=logMatrix;
         logmatrix[s]:=kitevo_vektor;
         if &and[Rank(ChangeRing(logmatrix,GF(t))) eq s: t in facB] then
            logVector[s]:=k-Lm1;
            logMatrix:=logmatrix;
            s:=s+1;
         end if;
      end if;
      kitevok:=kitevok join {k};
   end if;
end while;
time logSol:=Solution(Transpose(logMatrix),logVector);

kitevok2:={};
nyer:=false;
```

```
   while not nyer do
      k:=Random([1..p-1]);
      if not k in kitevok then
         pdb:=PrimeDivisors((a^k*b) mod p);
            if SequenceToSet(pdb) in FBsub then
               kitevo_vektor2:=Vector(Integers(p-1),[Valuation((a^k*b) mod p,
               FB[l]): l in [1..#FB]]);
               logeredmeny:=Integers(p-1)!((&+[kitevo_vektor2[t]*logSol[t]:
               t in [1..#FB]])-k);
               nyer:=true;
               print k;
            end if;
            kitevok2:=kitevok2 join {k};
         end if;
   end while;

   return logMatrix,logVector,logeredmeny;
end function;
```

Irodalomjegyzék

[1] B. Bódi. *Algebra*. Kossuth Lajos Tudományegyetem Természettudományi Kar, 1997.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] R. Ruprai. Improvements in the index-calculus algorithm for solving the discrete logarithm problem over $\mathbb{F}_p$. 2007. Elérhető: http://www.isg.rhul.ac.uk/ prai175/ISGStudentSem07/IndexCalculus.pdf.