Pszeudovéletlen sorozatok és rácsok

Doktori (Ph.D.) értekezés

Mérai László

Matematikai Doktori Iskola
Vezető: Laczkovich Miklós

Elméleti Matematikai Doktori Program
Vezető: Szűcs András

Témavezető: Sárközy András, egyetemi tanár

Eötvös Loránd Tudományegyetem, Természettudományi Kar
Matematikai Intézet
Budapest, 2010.

Tartalomjegyzék

1. fejezet

Bevezetés

1.1. Véletlen sorozatok

Véletlen elemek generálása több alkalmazásban is központi szerepet játszik, különösen a kriptográfiában és a numerikus analízisben.

Véletlen bináris sorozatok alkalmazására jó példa a Vernam tipusú titkosítás: Legyen $A_N = \{a_1, \ldots, a_N\} \in \{0,1\}^N$ az üzenet bináris ábrázolása, és legyen $E_N = \{e_1, \ldots, e_N\} \in \{0,1\}^N$ egy az üzenet hosszával megegyező hosszúságú véletlen sorozat. Ezután az A_N üzenetet bitenként titkosítjuk úgy, hogy a véletlen E_N sorozat megfelelő elemét hozzáadjuk modulo 2:

$$\begin{array}{rcl} A_N & : & \{a_1, \ldots, a_N\} \\ \oplus\ E_N & : & \{e_1, \ldots, e_N\} \\ \hline F_N & : & \{f_1, \ldots, f_N\} \end{array}$$

Az üzenetet hasonló módon lehet dekódolni. Ha most a titkosított F_N üzenethez adjuk hozzá bitenként a véletlen sorozatot, visszakapjuk az eredeti üzenetet:

$$\begin{array}{rcl} F_N & : & \{f_1, \ldots, f_N\} \\ \oplus\ E_N & : & \{e_1, \ldots, e_N\} \\ \hline A_N & : & \{a_1, \ldots, a_N\} \end{array}$$

Ennek a titkosítási eljárásnak az előnye, hogy mind a titkosítás, mind a dekódolás egyszerűen végrehajtható. A rejtjelezés másik előnye, hogy tökéletes biztonságot garantál. Azaz, ha egy véletlen sorozatot csak egyetlen üzenet titkosítására használunk, akkor bizonyítható, hogy a támadó, erőforrástól függetlenül, nem képes semmilyen információt megtudni a rejtjelezett üzenetről.

A titkosítási rendszernek ezen erős tulajdonságát kihasználva, a második világháború és a hidegháború alatt előszeretettel alkalmazták azt. Például a Washington és Moszkva közötti forró drótot 1963-tól ezzel a titkosítással védték.

A rendszer hátránya, hogy megkívánja a véletlen sorozattól, hogy hossza megegyezzen az üzenet hosszával. Ez pedig megnehezíti a kulcsok szétosztását és kezelését. Annak érdekében, hogy a titkosítást hatékonyabbá tegyük, valódi véletlen sorozat helyett pszeudovéletlen sorozatot használhatunk, mely egy valódi ám jóval rövidebb véletlen sorozatból készül. Pontosabban:

1. definíció. *A pszeudovéletlen szám generátor egy olyan determinisztikus algoritmus, mely egy adott k hosszúságú valódi véletlen sorozatból egy k-nál hosszabb pszeudovéletlen sorozatot generál.*

Hogy a titkosítás biztonsága ne csökkenjen, megköveteljük, hogy az így legyártott pszeudovéletlen sorozatot ne lehessen megkülönböztetni egy valódi véletlen sorozattól. Persze ezt már feltétel nélkül nem tudjuk garantálni, így bizonyos módon korlátozzuk a támadót. Természetes feltétel, hogy megköveteljük, hogy a támadó csak polinomiális erőforrással rendelkezzen.

2. definíció. *Egy pszeudovéletlen bit generátor kielégíti a következő-bit tesztet, ha nem létezik olyan polinomiális idejű algorimus, amelynek segítségével meg lehetne jósolni az output sorozat első l bitjéből az $(l+1)$-ediket 1/2-nél lényegesen nagyobb valószínűséggel.*

A definíciónak több hiányossága is van. Pszeudovéletlen sorozatot nem, csak pszeudovéletlen generátort definiál. Az alkalmazásokban, mikor egy adott, N hosszú sorozattal dolgozunk, nem tudjuk eldönteni, hogy véletlennek tekintsük-e azt, vagy ne. Másrészről, annak bizonyítása, hogy nem létezik polinomiális algoritmus, szinte lehetetlen. Így a definíció a gyakorlatban alkalmazhatatlan.

Egy másik, alkalmazás-orientált megközelítés a lineáris komplexitás:

3. definíció. *Egy E_N sorozat $L(E_N)$ lineáris komplexitása a legkisebb lineáris feed back shift register (lineáris rekurzió $\mathbb{F}_2$ fölött) hossza, ami generálja az egész sorozatot.*

Valódi véletlen E_N sorozatok esetén $L(E_N) \sim \frac{N}{2}$. Tehát egy „jó” pszeudovéletlen sorozattól meg kell követelni, hogy nagy legyen a lineáris komplexitása. Azonban ez koránt sem elégséges feltétel.

További hátránya, hogy egy sorozat lineáris komplexitását apriori tesztként csak speciális esetekben lehet alkalmazni. A gyakorlatban általános sorozatok lineáris komplexitását aposteriori döntik el (ld Berlekamp-Massey algoritmus [23]), ami szintén felvet alkalmazhatósági kérdéseket .

Adódik, hogy újabb, elég erős definicióját adjuk a pszeudovéletlenségnek. Az új definiciótól elvárjuk, hogy tesztelhető legyen sorozatok egy elég nagy családjára

1.2. Pszeudovéletlenség mértékei

1997-ben Mauduit és Sárközy a pszeudovéletlenség új mértékeit vezette be [19]. A mértékek definiálásánál a véletlen sorozatok alábbi fontos tulajdonságait vették alapul:

- számtani sorozatok mentén egyenletes eloszlású (*well-distribution*);
- kis autokorreláció (*correlation*);
- normalitás (*normality*).

Adott $E_N = \{e_1, \dots, e_N\} \in \{+1, -1\}^N$ bináris sorozat esetén a fenti tulajdonságok „mérésére" a következő mértékeket vezették be:

4. definíció. *Az E_N sorozat eloszlás mértéke:*

$$W(E_N) = \max_{a,b,t} |U(E_N, a, b, t)| = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|,$$

ahol a maximum olyan $a, b, t \in \mathbb{N}$ számokra fut melyekre $1 \le a \le a + (t-1)b \le N$.

Az E_N sorozat ℓ-ed rendű korrelációs mértéke:

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right|,$$

ahol a maximum olyan $D = (d_1, \dots, d_\ell)$ ℓ-eseken és $M \in \mathbb{N}$ számokon fut, melyekre $d_1 < d_2 < \dots < d_\ell$, $M + d_\ell \le N$.

Az E_N sorozat ℓ-ed rendű normalitás mértéke:

$$N_\ell(E_N) = \max_{X \in \{+1,-1\}^\ell} \max_{0 < M \le N+1-\ell} \left| T(E_N, M, X) - \frac{M}{2^\ell} \right|,$$

ahol

$$T(E, M, X) = |\{n : \ 0 \le n < M, \ (e_{n+1}, \dots, e_{n+\ell}) = X\}|.$$

Megjegyezzük azonban, hogy a korrelációs és a normalitás mérték között erős összefüggés van, így általában elég az eloszlás és korrelációs mértékeket vizsgálni:

1. tétel (Mauduit, Sárközy, [19]). *Minden N, E_N és $\ell < N$ esetén*

$$N_\ell \le \max_{1 \le t \le \ell} |C_t(E_N)|$$

teljesül.

Egy E_N sorozatot pszeudovéletlennek tekinthetünk, ha mind az eloszlás, mind a korrelációs mértéke (legalább kis ℓ-re) kicsi N függvényében (kívánatosan mindkettő $o(N)$, ha $N \to \infty$).

Ezt a terminológiát támasztja alá a következő tétel:

2. tétel (Alon, Kohayakava, Mauduit, Moreira, Rödl [1]).
Minden $\varepsilon_1 > 0$ számhoz létezik $N_0(\varepsilon_1)$ és $\delta > 0$, hogy $N > N_0$ esetén

$$\delta\sqrt{N} < W(E_N) < \frac{1}{\delta}\sqrt{N}$$

$1 - \varepsilon_1$-nál nagyobb valószínűséggel.

Hasonlóan minden $\varepsilon_2 > 0$ számhoz létezik $N_0(\varepsilon_2)$, hogy $N > N_0$ esetén

$$\frac{2}{5}\sqrt{N \log \binom{N}{\ell}} < C_\ell(E_N) < \frac{7}{4}\sqrt{N \log \binom{N}{\ell}}$$

$1 - \varepsilon_2$-nál nagyobb valószínűséggel.

A tétel alapján tehát a következőképpen definiálhatjuk a pszeudovéletlen sorozatokat:

5. definíció. *Egy $E_N \in \{-1, +1\}^N$ sorozat jó pszeudovéletlen tulajdonságokkal rendelkezik, ha*

$$W(E_N) = N^{1/2}(\log N)^{O(1)}, \quad \text{illetve} \quad C_\ell(E_N) = N^{1/2}(\log N)^{O_\ell(1)}$$

legalább kis ℓ értékekre.

1.3. Korábbi konstrukciók

Régóta ismert, hogy a Legendre szimbólum erős pszeudovéletlen tulajdonságokkal rendelkezik. Mauduit és Sárközy [19] a pszeudovéletlenségi mértékek segítségével kvantitatív módon jellemzték a Legendre szimbólumot. Nevezetesen a Legendere szimbólum segítségével definiált az 5 definíciót kielégítő sorozatot:

1. konstrukció (Mauduit, Sárközy). *Legyen p egy prímszám és definiáljuk az $E_{p-1} = \{e_1, \ldots, e_{p-1}\}$ sorozatot a következőképpen:*

$$e_n = \left(\frac{n}{p}\right),$$

ahol $\left(\frac{\cdot}{p}\right)$ a Legendre szimbólum.

Mauduit és Sárkozy bizonyította, hogy az így konstruált sorozatra

$$W(E_N) \ll N^{1/2} \log N, \quad \text{illetve} \quad C_\ell(E_N) \ll \ell N^{1/2} \log N.$$

Mivel alkalmazásokban nem egy sorozatra, hanem sorozatok egy nagy családjára van szükség, Goubin, Mauduit és Sárközy [9] vizsgálta, milyen módon lehet az 1 konstrukciót kiterjeszteni. Azt találták, hogy ha a sorozat n-edik tagjánál az n-et lecserélik egy alkalmas polinom n helyen felvett értékére, akkor továbbra is jó pszeudovéletlen tulajdonságokkal rendelkező sorozatot kapnak. Pontosabban:

2. konstrukció (Goubin, Mauduit, Sárközy). *Legyen p egy prímszám, $f \in \mathbb{F}_p[x]$ és definiáljuk az $E_p = \{e_1, \dots, e_p\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right), & \text{ha } p \nmid f(n), \\ 1, & \text{ha } p \mid f(n), \end{cases}$$

ahol $\left(\frac{\cdot}{p}\right)$ a Legendre szimbólum.

Bizonyították, hogy ha az f polinom kielégít bizonyos (könnyen ellenőrizhető) tulajdonságokat, akkor

$$W(E_p) \ll \deg f p^{1/2} \log p, \quad \text{illetve} \quad C_\ell(E_p) \ll \ell \deg f p^{1/2} \log p.$$

A számítógépes számelméletben széles körben használják az index (diszkrét logaritmus) fogalmát. Az index erős pszeudovéletlen tulajdonságait használta ki Gyarmati [10] (Sárközy eredményét kiterjesztve [27]), hogy új pszeudovéletlen sorozatokat definiáljon:

3. konstrukció (Gyarmati). *Legyen p egy prímszám, $f \in \mathbb{F}_p[x]$, g primitív gyök mudulo p és legyen* ind *a g alapú index (diszkrét logaritmus) modulo p. Definiáljuk az $E_p = \{e_1, \dots, e_p\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } p \nmid f(n) \text{ és } 1 \le \operatorname{ind} f(n) < p/2, \\ -1, & \text{máskülönben.} \end{cases}$$

Gyarmati bizonyította, hogy ha az f polinom kielégít bizonyos feltételeket, akkor

$$W(E_p) \ll \deg f p^{1/2} (\log p)^2, \quad \text{illetve} \quad C_\ell(E_p) \ll 4^\ell \deg f p^{1/2} (\log p)^{\ell+1}.$$

Oon vizsgálta a 2 és 3 konstrukciók egy közös általánosítását javasolta:

4. konstrukció. *Legyen p egy prímszám, $f \in \mathbb{F}_p[x]$, χ multplikatív karakter mudulo p. Definiáljuk az $E_p = \{e_1, \dots, e_p\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } p \nmid f(n) \text{ és } \arg\left(\chi(f(n))\right) \in [0, \pi), \\ -1, & \text{máskülönben,} \end{cases}$$

ahol $\arg(z)$ *a komplex z szám argumentumát jelöli.*

Világos, hogy ha χ a kvadratikus karakter, akkor lényegében megkapjuk a 2 konstrukciót. Másrészről, ha a χ karaktert úgy választjuk, hogy $\chi(g) = e^{\frac{2\pi i}{p-1}}$, akkor a 3 konstrukciót kapjuk.

Oon [25] bebizonyította, hogy ha a karakter d rendje nagy ($d = \Omega(p^{1/2})$), akkor jó pszeudovéletlen tulajdonságokkal rendelkező sorozatot kapunk:

$$W(E_p) \ll \deg f p^{1/2} (\log p)^2 + \frac{p}{d}, \quad \text{illetve} \quad C_\ell(E_p) \ll \ell \deg f p^{1/2} (\log 8p)^{\ell+1} + 4\ell \frac{p}{d^\ell}.$$

Sajnos a bizonyítás nem fedi a legérdekesebb eseteket, nevezetesen, amikor a karakter rendje kicsi ($d = o(p^{1/2})$).

Az eddig felsorolt konstrukciók jó pszeudovéletlen tulajdonsággal rendelkeznek (leszámítva talán a 4 konstrukció bizonyos eseteit), azonban az implementációjuk komoly problémát okozhat. Ezért a következő cél jól számolható konstrukciók megtalálása volt, esetleg az erős pszeudovéletlenség gyengítése árán is.

Mauduit, Rivat és Sárközy [18] először a talán legegyszerűbben számolható konstrukciót vizsgálták:

5. konstrukció (Mauduit, Rivat, Sárközy). *Legyen p egy prímszám és $f \in \mathbb{F}_p[x]$. Definiáljuk az $E_p = \{e_1, \dots, e_p\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } f(n) \in \{1, 2, \dots, \frac{p-1}{2}\} \\ -1, & \text{máskülönben.} \end{cases}$$

Mauduit, Rivat és Sárközy [18] bizonyította, hogy a konstrukció csak erős megszorításokkal mondható pszeudovéletlennek:

$$W(E_p) \ll \deg f p^{1/2} \log p, \quad \text{illetve} \quad C_\ell(E_p) \ll \deg f p^{1/2} (\log p)^{\ell+1},$$

feltéve, hogy a korreláció rendje kicsi: $\ell < \deg f$. Megmutatták, hogy ha ez a feltétel nem teljesül (azaz $\ell \geq \deg f$), akkor $C_\ell(E_p) \gg p$.

Később Mauduit és Sárközy [20] megmutatta, hogy ha az 5 konstrukcióban polinom helyett annak multiplikatív inverzével számolunk, elkerülhetjük a fenti, fokszámra vonatkozó erős feltételt. Az $E_N = \{e_1, \dots, e_p\}$ sorozatot a következőképpen definiálták:

6. konstrukció (Mauduit, Sárközy). *Legyen p egy prímszám és $f \in \mathbb{F}_p[x]$. Definiáljuk az $E_p = \{e_1, \dots, e_p\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } f(n) \neq 0 \text{ és } f(n)^{-1} \in \{1, 2, \dots, \frac{p-1}{2}\} \\ -1, & \text{máskülönben,} \end{cases}$$

ahol a^{-1} ($a \neq 0$) az $a \in \mathbb{F}_p$ elem multiplikatív inverzét jelöli.

Mauduit és Sárközy [20] megmutatta, hogy ha f kielégít bizonyos tulajdonságokat, akkor az így definiált sorozat jó pszeudovéletlen tulajdonságokkal rendelkezik:

$$W(E_p) \ll \deg f p^{1/2} (\log p)^2, \quad \text{illetve} \quad C_\ell(E_p) \ll \ell \deg f p^{1/2} (\log p)^{\ell+1}.$$

2. fejezet

Felhasznált eszközök

A fejezetben a tételek bizonyításához felhasznált eszközöket foglalom össze.

2.1. Karakterösszegek

A pszeudovéletlen mértékek becslése különböző nemteljes karakterösszeg becslésekre vezethető vissza, ezért először összefoglalom a véges testek feletti karakter összeg becsléseket.

A fejezet folyamán a következő jelöléseket fogjuk használni:

$\mathbb{F}_q$ egy p karakterisztikájú véges test;
$F(x), Q(x) \in \mathbb{F}_q(x)$ racionális törtfüggvények;
$\deg \frac{f(x)}{g(x)} = \deg f(x) + \deg g(x)$;
$\deg^* \frac{f(x)}{g(x)} = \deg f(x) - \deg g(x)$;
$\mathcal{S}$ $F(x)$ és $Q(x)$ pólusainak és Q gyökeinek halmaza;
ψ additív, χ, γ multiplikatív karakterei $\mathbb{F}_q$-nek;
ψ_0, χ_0 a főkarakterek;
$e(\alpha) = e^{2\pi i \alpha}$, illetve $e_m(a) = e(a/m)$.

6. definíció. *Tekintsük a következő hibrid karakterösszeget:*

$$S(\psi, F; \chi, Q) = \sum_{n \notin \mathcal{S}} \psi\left(F(n)\right) \cdot \chi\left(Q(n)\right).$$

Azt mondjuk, hogy $S(\psi, F; \chi, Q)$ elfajuló ha

$$F(x) = G^p(x) - G(x) + b$$

valamely $b \in \mathbb{F}_q$ elemre és $G(x) \in \mathbb{F}_q(x)$ racionális törtfüggvényre és

$$Q(x) = cH^d(x)$$

valamely $c \in \mathbb{F}_q$ elemre és $H(x) \in \mathbb{F}_q(x)$ racionális törtfüggvényre.

Ha az $S(\psi, F; \chi, Q)$ karakterösszeg elfajuló, akkor az összeg összes tagja 1, így az összeget csak a triviális módon tudjuk becsülni. Másrészről Perel'muter bebizonyította, hogy ha $S(\psi, F; \chi, Q)$ nem elfajuló, akkor már lehet az összeget nemtriviális módon becsülni:

3. tétel (Perel'muter [26]). *Legyen $\mathbb{F}_q$ p karakterisztikájú véges test, $\psi \neq \psi_0$ additív, $\chi \neq \chi_0$ d-ed rendű multiplikatív karaktere $\mathbb{F}_q$-nak. Legyenek $F(x) = \frac{f(x)}{g(x)}$, $Q(x) = \frac{q(x)}{r(x)} \in \mathbb{F}_q(x)$ racionális törtfüggvények. Tegyük fel, hogy az $S(\psi, F; \chi, Q)$ nem elfajuló és a következő feltételek teljesülnek:*

1. *Ha $F = \frac{f}{g_1^{\lambda_1} \dots g_r^{\lambda_r}}$, akkor $p \nmid \lambda_i$, ahol $\lambda_i > 0$, $i = 1, \dots, r$ esetén és $\deg F > 0$ esetén $p \nmid \deg F$.*
2. *Ha $Q = \frac{q_1^{n_1} \dots q_u^{n_u}}{r_1^{m_1} \dots r_v^{m_v}}$, akkor $0 < n_i < d$, $0 < m_i < d$ minden i-re.*

Ekkor

$$\left| \sum_{n \notin \mathcal{S}} \psi(F(n)) \chi(Q(n)) \right| \leq \big(d_1 + d_2 - 2\big) q^{1/2} + d_1 + d_2 + 1 \tag{2.1}$$

ahol

$$d_1 = \max\{\deg f, \deg g\} + s + \lambda, \quad d_2 = z + \mu$$

és s g különböző gyökeinek számát jelöli, $\lambda = 0$ ha $\deg g \geq \deg f$ és $\lambda = 1$ máskülönben, z q és r különböző gyökeinek száma, végül $\mu = 0$ ha $d \mid \deg Q$ és $\mu = 1$ máskülönben.

A tétel segítségével adható nem triviális korlát nem teljes karakterösszegekre is.

4. tétel ([M3]). *Legyen p prímszám, $\psi \neq \psi_0$ additív, $\chi \neq \chi_0$ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek. Legyenek továbbá $F = \frac{f}{g}$, $Q = \frac{q}{r}$ nem nulla racionális törtfüggvények. Tegyük fel továbbá, hogy*

$$g(x) \nmid f(x) \tag{2.2}$$

vagy

$$Q(x) \neq bB^d(x) \quad \text{bármely } b \in \mathbb{F}_p \text{ és } B(x) \in \mathbb{F}_p(x) \text{ esetén.} \tag{2.3}$$

Ha $1 \leq N < p$, akkor

$$\left| \sum_{\substack{0 \leq n < N \\ n \notin \mathcal{S}}} \psi(F(n)) \chi(Q(n)) \right| \leq 9\big(\max\{\deg f, \deg g\} + s + z\big) p^{1/2} \log p, \tag{2.4}$$

ahol s g, z q és r különböző gyökeinek száma.

Bizonyítás. Ha a (2.3) feltétel teljesül, de a (2.2) feltétel nem, akkor nem teljes multiplikatív karakter összeg becslését kapjuk (ld. [19]).

Tekintsük most azt az esetet, amikor a (2.2) feltétel teljesül. A bizonyítás során feltehetjük, hogy az f, g, r, q polinomok p-nél kisebb fokúak (különben a tétel semmitmondó).

Mivel a ψ karakter nem a főkarakter, ezért az additív karakterek alapvető tulajdonságaiból következik, hogy

$$\sum_{r=0}^{N-1} \frac{1}{p} \sum_{u=0}^{p-1} \psi(u(n-r)) = \begin{cases} 1 & \text{ha } 0 \le n < N \\ 0 & \text{máskülönben.} \end{cases}$$

Jelöljük a (2.4)-ben szereplő összeget S_N-nel. Ekkor

$$\begin{aligned} S_N &= \sum_{n \notin \mathcal{S}} \psi(F(n))\chi(Q(n)) \sum_{r=0}^{N-1} \frac{1}{p} \sum_{u=0}^{p-1} \psi(u(n-r)) = \\ &= \frac{1}{p} \sum_{u=0}^{p-1} \left(\sum_{r=0}^{N-1} \psi(-ur) \right) \left(\sum_{n \notin \mathcal{S}} \psi(F(n)+un)\chi(Q(n)) \right) = \\ &= \frac{1}{p} \sum_{u=1}^{p-1} \left(\sum_{r=0}^{N-1} \psi(-ur) \right) \left(\sum_{n \notin \mathcal{S}} \psi(F(n)+un)\chi(Q(n)) \right) + \\ &\quad + \frac{N}{p} \sum_{n \notin \mathcal{S}} \psi(F(n))\chi(Q(n)), \end{aligned}$$

ahonnan

$$|S_N| \le \frac{1}{p} \sum_{u=1}^{p-1} \left| \sum_{r=0}^{N-1} \psi(ur) \right| \left| \sum_{n \notin \mathcal{S}} \psi(F(n)+un)\chi(Q(n)) \right| + \\ + \frac{N}{p} \left| \sum_{n \notin \mathcal{S}} \psi(F(n))\chi(Q(n)) \right|. \quad (2.5)$$

Rögzített u esetén legyen

$$F_u(x) = F(x) + ux = \frac{f(x)}{g(x)} + ux.$$

Annak érdekében, hogy megmutassuk, hogy az $F_u(x)$ racionális törtfüggvény kielégíti a 3 tétel feltételeit, elegendő megmutatni, hogy $F_u(x)$ nem írható $A(x)^p - A(x)$ alakba ahol $A(x) \in \overline{\mathbb{F}}_p(x)$. Indirekt tegyük fel, hogy léteznek $k(x), l(x) \in \overline{\mathbb{F}}_p[x]$ polinomok, hogy

$$(k(x), l(x)) = 1 \quad (2.6)$$

és

$$F_u(x) = \left(\frac{k(x)}{l(x)} \right)^p - \frac{k(x)}{l(x)}. \quad (2.7)$$

A nevezőkkel felszorozva kapjuk, hogy

$$l^p(x)(f(x)+uxg(x)) = (k^{p-1}(x)-l^{p-1}(x))k(x)g(x)$$

ahonnan (2.6) miatt

$$l^p(x) \mid g(x).$$

Mivel $\deg g < p$, az $l(x)$ polinom egy konstans polinom. Tehát

$$f(x)+uxg(x) = (\alpha k^p(x)+\beta k(x))g(x),$$

illetve

$$f(x) = (\alpha k^p(x)+\beta k(x)-ux)g(x),$$

valamely $\alpha, \beta \in \overline{\mathbb{F}}_p$, $\alpha\beta \neq 0$ értékekre. Mivel $g(x) \nmid f(x)$ és

$$\deg(\alpha k^p(x)+\beta k(x)-ux) \leq p$$

azt kapjuk, hogy (2.7) nem teljesülhet.

Mivel $F(x)+ux$, $F(x)$ és $Q(x)$ kielégíti a 3 tétel feltételét, alkalmazhatjuk a tételt (2.5)-beli karakter összegekre:

$$\begin{aligned} |S_N| \quad &\leq \quad \frac{1}{p}\left(\sum_{u=1}^{p-1}\left|\sum_{r=0}^{N-1}\psi(ur)\right| + N\right)\cdot \\ &\quad \cdot 2\big(\max\{\deg f, \deg g\}+s+z\big)p^{1/2}. \end{aligned}$$

ahonnan a kívánt becslés következik a

$$\sum_{u=0}^{p-1}\left|\sum_{r=0}^{N-1}\psi(ur)\right| < \frac{4}{\pi}p\log p + 0.38p + 0.64.$$

egyenlőtlenséget felhasználva (1. tétel, [6]). □

A következő tétel általános véges testek fölötti karakterösszegekre ad nemtriviális korlátot.

5. tétel (Winterhof, [28]). *Legyen p prím, és $q = p^n$, χ d-ed rendű multiplikatív karaktere $\mathbb{F}_q$-nak, $f(x) \in \mathbb{F}_q[x]$ nem konstans polinom, mely nem d-hatvány és melynek m különböző gyöke van a felbontási testben. $v_1, \ldots, v_n \in \mathbb{F}_q$ $\mathbb{F}_q$ egy $\mathbb{F}_p$ fölötti bázisa, $t_1, \ldots, t_n \in \mathbb{N}$ olyan egészek, melyre $0 < t_1, \ldots, t_n$. Legyen*

$$B = \left\{\sum_{i=1}^{n} a_i v_i : 0 \leq a_i \leq t_i,\ i = 1, \ldots, n\right\}$$

ekkor

$$\left|\sum_{x\in B}\chi(f(x))\right| < mq^{1/2}(1+\log p)^n.$$

Az alábbi két lemma segítségével a sorozat tagjait tudjuk majd felírni karakterek lineáris kombinációjaként :

7. lemma. *Legyen χ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek, $n \neq 0$. Ekkor*

$$\frac{2}{d}\sum_{\gamma^d=\chi_0}^{*} \frac{1-\bar{\gamma}(g)^{d/2}}{1-\bar{\gamma}(g)} \cdot \gamma(n) = \begin{cases} +1 & \text{ha } \arg\big(\chi(n)\big) \in [0,\pi) \\ -1 & \text{máskülönben,} \end{cases} \tag{2.8}$$

ahol γ fut azon nemtriviális karaktereken, melynek d-edik hatványa a főkarakter, és g az a generátor, melyre $\chi(g) = e(1/d)$.

Bizonyítás. Jelölje $r_m(c)$ a c legkisebb nem negatív maradékát modulo m. Ekkor, ha $n \neq 0$, akkor

$$\chi(n) = \chi(g^{\operatorname{ind} n}) = \chi(g)^{\operatorname{ind} n},$$

ahol ind a g alapú diszkrét logaritmus. Ekkor

$$\arg\big(\chi(n)\big) \in [0,\pi) \Longleftrightarrow r_d(\operatorname{ind} f(nG)) < \frac{d}{2}.$$

Felhasználva az

$$\frac{1}{p-1}\sum_{\gamma}\gamma(a) = \begin{cases} 1 & \text{ha } a = 1 \\ 0 & \text{máskülönben,} \end{cases}$$

összefüggést, azt kapjuk hogy a (2.8) jobb oldala

$$2\sum_{\substack{0\le k<p-1 \\ r_d(k)<d/2 \\ g^k=f(nG)}} 1 - 1 = 2\frac{1}{p-1}\sum_{\gamma}\sum_{i=0}^{\frac{p-1}{d}-1}\sum_{0\le k<d/2}\bar{\gamma}(n)\gamma(g^{k+id}) - 1$$

$$= 2\frac{1}{p-1}\sum_{\gamma}\bar{\gamma}(n)\sum_{i=0}^{\frac{p-1}{d}-1}\gamma(g^d)^i\sum_{0\le k<d/2}\gamma(g)^k - 1.$$

Mikor $\gamma = \chi_0$, akkor

$$2\frac{1}{p-1}\sum_{i=0}^{\frac{p-1}{d}-1}\sum_{0\le k<d/2} 1 = 1.$$

Hasonlóan, ha $\gamma^d \neq \chi_0$, akkor

$$\sum_{i=0}^{\frac{p-1}{d}-1}\gamma(g^d)^i = 0.$$

Végül, ha $\gamma^d = \chi_0$ (de $\gamma \neq \chi_0$), akkor

$$\sum_{i=0}^{\frac{p-1}{d}-1}\gamma(g^d)^i = \frac{p-1}{d}.$$

Végül az állítás következik a

$$\sum_{0\le k<d/2} \gamma(g)^k = \frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)}$$

összefüggésből.

□

Az előbbi lemma additív analogonja:

8. lemma. *Legyen $m \in \mathbb{N}$. Ekkor*

$$\frac{1}{m} \sum_{-[m/2]<k\le[m/2]} v_m(k) e_m(ak) = \begin{cases} +1 & ha\ -\frac{\pi}{2} \le \arg(e_m(a)) < \frac{\pi}{2} \\ -1 & másképpen, \end{cases}$$

ahol $v_m(k)$ egy m szerinti periodikus függvény, melyre

$$v_m(0) = 1,$$

és ha m páratlan, akkor

$$v_m(k) = i^k \left(1 + i\frac{(-1)^k - \cos(\pi k/m)}{\sin(\pi k/m)}\right), \quad \text{ha } 1 \le |k| < m/2,$$

ha m páros, akkor

$$v_m(k) = \begin{cases} 0 & \text{ha } k \text{ páros}, \\ i^k \left(2 - 2i\frac{\cos(k\pi/m)}{\sin(k\pi/m)}\right) & \text{ha } k \text{ páratlan}, \end{cases} \qquad \text{ha } 1 \le |k| \le m/2.$$

Továbbá mindkét esetben

$$v_m(k) \ll \frac{m}{k} \qquad ha\ k \neq 0.$$

Bizonyítás. Páratlan m-re a lemmát Mauduit, Rivat és Sárközy bizonyította [18], páros m-re a bizonyítás hasonló. □

9. lemma. *Legyen g az $\mathbb{F}_q$ egy generátora. Ekkor*

$$\sum_{\chi^d=\chi_0}^{*} \frac{1}{|1-\chi(g)|} < d\log d.$$

Bizonyítás. Abban az esetben, mikor $q = p$ és $d = p - 1$ a bizonyítás megtalálható [27]-ben. Az általános eset hasonlóan bizonyítható. □

2.2. Megengedhetőség

Annak érdekében, hogy leírhassuk azon polinomokat, melyekre az adott konstrukció jó pszeudovéletlen tulajdonságokkal rendelkező sorozatot generál, bevezetjük a megengedhetőség fogalmát.

10. definíció. *Legyen $m, d \in \mathbb{Z}$ egész számok, $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ olyan multihalmazok, hogy az elemek multiplicitása kisebb, mint d, és $\mathcal{A}$ minden elemének multiplicitása relatív prím d-hez. Azt mondjuk, hogy az $\mathcal{A}, \mathcal{B}$ pár $P(d)$ tulajdonságú, ha az $\mathcal{A}+\mathcal{B}$ összegben minden elem d-szeresen van reprezentálva. Azaz a*

$$a + b = c, \quad a \in \mathcal{A}, b \in \mathcal{B} \tag{2.9}$$

egyenletnek a megoldásszáma minden c esetén osztható d-vel.

Jelölje egy adott $\mathcal{A}$ multihalmaz különböző elemeinek a számát $|\mathcal{A}|$.

11. definíció. *A (k, ℓ, m) számhármas d-megengedhető (d-admissible) ($k, \ell < m$), ha nem létezik olyan $\mathcal{A}, \mathcal{B}$ multihalmaz, hogy $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$, és $\mathcal{A}, \mathcal{B}$ $P(d)$ tulajdonságú.*

A következőkben elégséges feltételeket adunk d-megengedhetőségre.

6. tétel ([M7]). *Egy m szám legkisebb prímosztóját jelölje $p(m)$. Ekkor*

(i) Ha $k, m, d \in \mathbb{N}$, $k < p(m)$, akkor a $(k, 2, m)$ hármas d-megengedhető.

(ii) Ha $k, m, d \in \mathbb{N}$, $k < p(m)$, továbbá

$$(4\ell)^k < p(m), \tag{2.10}$$

akkor a (k, ℓ, m) hármas d-megengedhető.

(iii) Ha m egy prímszám, d minden prímosztója primitív gyök modulo m, akkor minden $k, \ell < m$ esetén a (k, ℓ, m) hármas d-megengedhető.

A következő lemma miatt elég a tételt abban az esetben bebizonyítani, ha d prímszám. A lemma (és a tétel) bizonyításában egy $\mathcal{A}$ multihamaz adott a elemének a multiplicitását $m_{\mathcal{A}}(a)$-val fogjuk jelölni.

12. lemma. *Ha d minden p prímosztójára a (k, ℓ, m) hármas p-megengedhető, akkor a (k, ℓ, m) hármas d-megengedhető.*

Bizonyítás. Tegyük fel, hogy létezik egy $P(d)$ tulajdonságú $\mathcal{A}, \mathcal{B}$ multihalmaz pár.

Legyen $d = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, és legyen p_i olyan prímosztó, hogy $p_i^{\alpha_i}$ nem osztja az összes $m_{\mathcal{B}}(b)$ multiplicitást.

Ha van olyan $b \in \mathcal{B}$ elem, melyre $p_i \nmid m_{\mathcal{B}}(b)$, akkor gyűjtsük $\mathcal{A}'$-be az $\mathcal{A}$ elemeit $m_{\mathcal{A}}(a) \pmod{p_i}$ multiplicitással, hasonlóan $\mathcal{B}'$-be a $\mathcal{B}$ elemeit $m_{\mathcal{B}}(b) \pmod{p_i}$ multiplicitással. Ekkor sem $\mathcal{A}'$, sem $\mathcal{B}'$ nem üres (hiszen nem minden $m_{\mathcal{A}}(a)$, $m_{\mathcal{B}}(b)$ multiplicitás osztható p_i-vel) és az $\mathcal{A}', \mathcal{B}'$ pár $P(p_i)$ tulajdonságú.

Ha minden $m_{\mathcal{B}}(b)$ multiplicitás osztható p_i-vel, akkor legyen β_i az a kitevő, melyre

$$p_i^{\beta_i} \mid\mid \text{lnko}\{m_{\mathcal{B}}(b) : \ b \in \mathcal{B}\}.$$

Ekkor $\beta_i < \alpha_i$. Legyen $\mathcal{A}' = \mathcal{A}$ és $\mathcal{B}'$ multihalmaza a $b \in \mathcal{B}$ elemeknek $m_{\mathcal{B}}(b)p_i^{-\beta_i}$ multiplicitással. Ezzel a választással nem minden $m_{\mathcal{B}'}(b')$ multiplicitás osztható p_i-vel ($b' \in \mathcal{B}'$), és az $\mathcal{A}', \mathcal{B}'$ pár $P(d/p_i^{\beta_i})$ tulajdonságú. Így az előző gondolatmenet alapján létezik olyan $\mathcal{A}''$, $\mathcal{B}''$ pár, ami $P(p_i)$ tulajdonságú. □

A 6 tétel bizonyítása. A 12 lemma alapján elég a tételt prím d-re bizonyítani.

A 6 tétel (i) pontjának bizonyítása. Az állítást indirekt módon bizonyítjuk. Tegyük fel, hogy léteznek $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ multihalmazok, hogy $|\mathcal{A}| = k$, $|\mathcal{B}| = 2$ és minden $c \in \mathbb{Z}$ esetén a (2.9) egyenlet megoldásszáma d-vel osztható.

Legyen a $\mathcal{B}$ két különböző eleme $r, r+s$ (ahol most $s \neq 0$). $\mathcal{A}+r$ minden elemének legalább két előállítása van a (2.9) alakban, tehát $\{a+r \mid a \in \mathcal{A}\} = \{a+r+s \mid a \in \mathcal{A}\}$ mint halmazok. Hasonlóan $\{a + r \mid a \in \mathcal{A}\} = \{a + r + st \mid a \in \mathcal{A}\}$ minden $t \in \mathbb{N}$ esetén, azaz $\mathcal{A}+r$ tartalmazza $\mathbb{Z}_m$ egy nemtriviális részcsoportjának mellékosztályát, ami ellentmond a $|\mathcal{A}| < p(m)$ feltételnek.

A 6 tétel (ii) pontjának bizonyítása. Tegyük fel, hogy k, ℓ, m kielégíti a (2.10) egyenlőtlenséget, $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_m$ olyan multihalmazok, melyekre $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$.

Ha $s \in \mathbb{N}$, $(s, m) = 1$, akkor a (2.9) és az

$$sa + sb = sc, \quad a \in \mathcal{A}, \ b \in \mathcal{B}$$

egyenlet megoldásai megegyeznek, ha c végigfutja $\mathbb{Z}_m$ elemeit. Tehát elég megmutatni, hogy van olyan $s \in \mathbb{N}$ és $c \in \mathbb{Z}_m$, hogy $(s, m) = 1$ és az

$$sa + sb = c, \quad a \in \mathcal{A}, \ b \in \mathcal{B} \tag{2.11}$$

egyenlet megoldásszáma nem osztható d-vel.

Adott $a \in \mathbb{Z}$ esetén legyen $r(a)$ a-nak az abszolút legkisebb maradéka modulo m, azaz

$$r(a) \equiv a \mod m, \quad -\frac{m}{2} < r(a) \leq \frac{m}{2}.$$

A tétel bizonyítása során a következő lemmát használjuk:

13. lemma. *Ha $k, \ell, m, \mathcal{A}$ eleget tesz a fenti követelményeknek és $a_1, \ldots, a_k$ az $\mathcal{A}$ különböző elemei, akkor létezik olyan s szám, melyre $(s, m) = 1$ és*

$$|r(sa_i)| \leq \frac{1}{2}\left[\frac{m}{\ell}\right] \quad i = 1, \ldots, k \text{ esetén.} \tag{2.12}$$

Bizonyítás. Legyen $\mathcal{J} = \{1, \ldots, p(m)\}$. Világos, hogy ha $i, j \in \mathcal{J}$, akkor $(i-j, m) = 1$. Tekintsük a következő $p(m)$ darab k-ast:

$$\mathbf{u}_j = (r(ja_1), \ldots, r(ja_k)), \quad j \in \mathcal{J}. \tag{2.13}$$

Legyen $D = \frac{1}{2}\left[\frac{m}{\ell}\right] + 1$ és $Z = \left[\frac{m}{D}\right] + 1$. Ekkor $DZ > m$, így minden $j \in \mathcal{J}$ esetén léteznek $t_1 = t_1(j), \ldots, t_k = t_k(j)$ egészek, hogy

$$r(ja_i) \in \left\{-\left[\frac{m}{2}\right] + t_i D, -\left[\frac{m}{2}\right] + t_i D + 1, \ldots, -\left[\frac{m}{2}\right] + (t_i + 1)D - 1\right\}$$

ahol

$$t_i \in \{0, 1, \ldots, Z - 1\} \tag{2.14}$$

$i = 1, \ldots, k$ esetén.

A lehetséges $(t_1, \ldots, t_k)$ k-asok száma, melyekre (2.14) teljesül

$$Z^k = \left(\left[\frac{m}{D}\right] + 1\right)^k < \left(2\frac{m}{D}\right)^k < \left(2\frac{m}{m/2\ell}\right)^k = (4\ell)^k < p(m),$$

(2.10) miatt. Tehát létezik legalább két index $j_1, j_2 \in \mathcal{J}$, melyekre

$$t_1 = t_1(j_1) = t_1(j_2), \ldots, t_k = t_k(j_1) = t_k(j_2),$$

azaz

$$-\left[\frac{m}{2}\right] + t_i D \leq r(j_1 a_i), r(j_2 a_i) < -\left[\frac{m}{2}\right] + (t_i + 1)D$$

ahonnan azt kapjuk, hogy

$$|r(j_1 a_i) - r(j_2 a_i)| < D \quad i = 1, \ldots, k.$$

Legyen $s = |j_1 - j_2|$. Ezzel a választással

$$|r(sa_i)| = |r((j_1 - j_2)a_i)| \leq |r(j_1 a_i) - r(j_2 a_i)| < D.$$

□

A tétel (ii) pontjának bizonyításához válasszunk egy olyan s elemet, ami kielégíti (2.12)-et. Legyenek $b_1 \ldots, b_\ell$ $\mathcal{B}$ különböző elemei. Legyen i, j olyan indexpár melyre

$$sb_l \notin \{sb_i + 1, \ldots, sb_j - 1\}, \quad l = 1, \ldots, \ell$$

(itt az sb_l elemeket ciklikusan, azaz modulo m soroljuk fel). A skatulyaelv miatt a maximális távolság két egymást követő sb_l között legalább $[m/\ell]+1$.

Legyen $r_1,\dots,r_k$ az $r(sa_1),\dots,r(sa_k)$ változók értéke nagyság szerint rendezve:

$$-\frac{1}{2}\left[\frac{m}{\ell}\right] \le r_1 \le \dots \le r_k \le \frac{1}{2}\left[\frac{m}{\ell}\right].$$

(2.12) alapján

$$(sb_j + r_1) - (sb_i + r_k) = (sb_j - sb_i) + r_1 - r_k \ge$$
$$\ge \left(\left[\frac{m}{\ell}\right]+1\right) - \frac{1}{2}\left[\frac{m}{\ell}\right] - \frac{1}{2}\left[\frac{m}{\ell}\right] = 1 > 0.$$

Legyenek u, v azon indexek, melyre $r(sa_u) = r_1$, $r(sa_v) = r_k$. Ekkor a

$$sa_v + sb_i \quad \text{és} \quad sa_u + sb_j$$

elemek különböző reprezentációinak száma a $(a,b) = (a_v, b_i)$ illetve a $(a',b') = (a_u, b_j)$ párok száma, ami $m_{\mathcal{A}}(a_v)m_{\mathcal{B}}(b_i)$ és $m_{\mathcal{A}}(a_u)m_{\mathcal{B}}(b_j)$ mely számok nem oszthatók d-vel.

A 6 tétel (iii) pontjának bizonyítása. Adott $\mathcal{C} \subset \mathbb{Z}_m$ multihalmaz esetén definiáljuk a $P_{\mathcal{C}}(x) \in \mathbb{Z}_d[x]$ polinomot a következőképpen:

$$P_{\mathcal{C}}(x) = \sum_{c\in\mathcal{C}} x^{r_m(c)},$$

ahol $r_m(c)$ a c legkisebb nem negatív maradékát jelöli modulo m.

Megjegyezzük, hogy ha $u \in \mathbb{Z}_m$, akkor

$$P_{\mathcal{C}+u}(x) \equiv x^u P_{\mathcal{C}}(x) \mod x^m - 1.$$

Következésképpen egy $\mathcal{A},\mathcal{B}$ pár pontosan akkor $P(d)$ tulajdonságú, ha

$$P_{\mathcal{A}}(x)P_{\mathcal{B}}(x) \equiv 0 \mod x^m - 1$$

$\mathbb{Z}_d$ fölött, azaz $x^m - 1 \mid P_{\mathcal{A}}(x)P_{\mathcal{B}}(x)$.

Ha a $x^{m-1}+\dots+1$ polinom reducibilis $\mathbb{Z}_d[x]$ fölött, például $P_1(x)P_2(x) = x^{m-1}+\dots+1$, akkor definiáljuk az $\mathcal{A}$ illetve $\mathcal{B}$ multihalmazt a $P_1(x) = \sum_{a\in\mathcal{A}} x^{r_m(a)}$ illetve $P_2(x)(x-1) = \sum_{b\in\mathcal{B}} x^{r_m(b)}$ összefüggéssel. Ekkor az $\mathcal{A},\mathcal{B}$ pár $P(d)$ tulajdonágú.

Megfordítva, ha $x^{m-1}+\dots+1$ irreducibilis $\mathbb{Z}_d[x]$ fölött, és az $\mathcal{A},\mathcal{B}$ pár $P(d)$ tulajdonságú, akkor $x^{m-1}+\dots+1$ osztja vagy a $P_{\mathcal{A}}(x)$, vagy a $P_{\mathcal{B}}(x)$ polinomot, tehát $\mathcal{A}$ vagy $\mathcal{B}$ tartalmazza $\mathbb{Z}_d$-t.

Végül megjegyezzük, hogy a [16]-beli 2.47 tétel alapján az $x^{m-1}+\dots+1$ polinom pontosan akkor irreducibils $\mathbb{Z}_d[x]$ fölött, ha m prím és d primitív gyök modulo m. □

A 6 tétel (iii) pontja nem csak elégséges, de bizonyos szempontból szükséges és elégséges feltételt ad számunkra a megengedhetőségre:

14. definíció. *Adott d szám esetén az $m \in \mathbb{N}$ szám jó, ha minden $k, \ell \in \mathbb{N}$ párra, melyre $k < m$, $\ell < m$ a (k, ℓ, m) hármas d-megengedhető.*

15. Következmény. *Az adott d szám esetén az $m \in \mathbb{N}$ szám pontosan akkor jó, ha m prím, és d minden prímosztója primitív gyök modulo m.*

Bizonyítás. Azt kell megmutatni, hogy minden $k, \ell \in \mathbb{N}$ pár esetén, melyre a (k, ℓ, m) hármas d-megengedhető, akkor d minden p prímosztójára és $k', \ell' \in \mathbb{N}$ párra a (k', ℓ', m) hármas p-megengedhető.

Legyenek $\mathcal{A}, \mathcal{B}$ multihalmazok, melyek $P(p)$ tulajdonságúak. Ekkor legyen $\mathcal{A}' = \mathcal{A}$ és legyen $\mathcal{B}'$ az a multihalmaz, mely $\mathcal{B}$ elemeit tartalmazza $m_{\mathcal{B}}(b) \cdot \frac{d}{p}$ multiplicitása. Ekkor a $\mathcal{A}', \mathcal{B}'$ pár $P(d)$ tulajdonságú. □

Megjegyezzük, hogy abban a speciális esetben, mikor az $\mathcal{A}$, $\mathcal{B}$ multihamlazokba minden elem multiplicitása legfeljebb egy (azaz $\mathcal{A}$ és $\mathcal{B}$ halmazok), akkor az (i) és (ii) pontokban a megengedhetőségnél erősebb dolgot bizonyítunk:

16. Következmény. *Ha k, ℓ eleget tesz a 6 tétel (i) és (ii) pontjainak feltételének, akkor minden $\mathcal{A}, \mathcal{B}$ halmaz esetén, melyre $|\mathcal{A}| \leq k$, $|\mathcal{B}| \leq \ell$ létezik olyan $c \in \mathbb{Z}_m$ elem, hogy az*

$$a + b = c \quad a \in \mathcal{A},\ b \in \mathcal{B}$$

egyenletnek pontosan egy megoldása van.

A következőkben a 16 következmény általánosítását nézzük, mikor a (2.9) egyenletet tetszőleges Abel csoport felett vizsgáljuk.

17. definíció. *A (k, ℓ, G) hármas megengedhető, ha minden $\mathcal{A}, \mathcal{B} \subset G$ halmaz esetén melyre $|\mathcal{A}| \leq k$, $|\mathcal{B}| \leq \ell$ létezik olyan $c \in G$ elem, hogy az*

$$a + b = c \quad a \in \mathcal{A},\ b \in \mathcal{B}$$

egyenletnek pontosan egy megoldása van.

7. tétel ([M6]). *Legyen $G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}$ tetszőleges véges Abel csoport, és $p(G)$ a csoport rendjének legkisebb prímosztója. Legyen $k, \ell \in \mathbb{N}$ melyek az alábbi feltételek valamelyikét teljesítik:*

(i) $k < p(G)$ $\ell = 2$;

(ii)

$$4^{s(k+\ell)} < p(G). \tag{2.15}$$

Ekkor a (k, ℓ, G) hármas megengedhető.

Bizonyítás. A tétel (i) pontjának bizonyítása hasonló a 6. tétel (i) pontjának bizonyításához, így azt az olvasóra bizom.

A (ii) pontjának bizonyításához felhasználjuk a 13 lemma analogonját:

18. lemma. *Ha $d_1, \dots, d_s \in \mathbb{N}$, p a legkisebb prímosztója a $\prod d_j$ szorzatnak, és $t \in \mathbb{N}$ olyan egész, melyre*

$$4^{st} < p, \tag{2.16}$$

akkor adott $\mathbf{h}_1, \dots, \mathbf{h}_t \in \mathbb{Z}^n$ esetén létezik egy olyan $0 < r < p$ egész, melyre

$$|m_{d_j}(r \cdot (\mathbf{h}_i)_j)| \leq \frac{d_j}{4}.$$

Bizonyítás. Adott $h \in \mathbb{Z}$ esetén legyen $y_j(h)$ az a nem negatív egész, melyre h kongruens az $\left(y_j(h)\left(\left[\frac{d_j}{4}\right]+1\right), (y_j(h)+1)\left(\left[\frac{d_j}{4}\right]+1\right)\right]$ intervallum valamelyik elemével modulo d_j. Ekkor $y_j(h) \in \{0,1,2,3\}$ teljesül. Adott $u = 1, \dots, p$ esetén tekintsük a következő $\mathbf{y}_i(u) = \big(y_1\left(u \cdot (\mathbf{h}_i)_1\right)), \dots, y_s\left(u \cdot (\mathbf{h}_i)_s\right)\big) \in \{0,1,2,3\}^s$ s-eseket, ahol $i = 1, \dots, t$. A $(\mathbf{y}_1(u), \dots, \mathbf{y}_t(u)) \in (\{0,1,2,3\}^s)^t$ t-esek száma p, amely a feltétel szerint nagyobb az összes különböző $(\{0,1,2,3\}^s)^t$-beli t-esek számánál. Következésképp a skatulyaelv alapján létezik legalább kettő t-es, melyre

$$(\mathbf{y}_1(u), \dots, \mathbf{y}_t(u)) = (\mathbf{y}_1(v), \dots, \mathbf{y}_t(v)), \qquad u < v.$$

Legyen $r = v - u$, ekkor a $y_j\big(u \cdot (\mathbf{h}_i)_j\big) = y_j\big(v \cdot (\mathbf{h}_i)_j\big)$ feltételből következik, hogy

$$|m_{d_i}(r \cdot (\mathbf{h}_i)_j)| = |m_{d_i}((v-u) \cdot (\mathbf{h}_i)_j)| \leq |m_{d_i}((v \cdot (\mathbf{h}_i)_j - u \cdot (\mathbf{h}_i)_j)| \leq \frac{d_i}{4},$$

minden $i = 1, \dots, t$ és $j = 1, \dots, s$ indexre. □

A lemma segítségével a következőképpen bizonyíthatjuk a tétel (ii) pontját: Legyen $x_i(a)$ az i-edik komponense a-nak a $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}$-beli reprezentációban, és alkalmazzuk a lemmát a $(x_1(a), \dots, x_s(a))$, $(a \in \mathcal{A})$ és $(x_1(b), \dots, x_s(b))$, $(b \in \mathcal{B})$ s-esekre, ahol most $t = k + \ell$. Ekkor a (2.16) feltétel a tételben megfogalmazott (2.15) feltétel miatt teljesül, így a lemma szerint van olyan r egész, melyre $0 < r < p(G)$ és

$$|m_{d_i}(r \cdot x_i(a))|,\ |m_{d_i}(r \cdot x_i(b))| \leq \frac{d_i}{4}, \quad i = 1, \dots, s,\ a \in \mathcal{A},\ b \in \mathcal{B}. \tag{2.17}$$

Definiáljuk most az $\mathbf{A}, \mathbf{B}$ halmazokat a következő módon:

$$\mathbf{A} = \{(m_{d_1}(r \cdot x_1(a)), \dots, m_{d_s}(r \cdot x_s(a))) :\ a \in \mathcal{A}\}$$

és

$$\mathbf{B} = \{(m_{d_1}(r \cdot x_1(b)), \dots, m_{d_s}(r \cdot x_s(b))) : \ b \in \mathcal{B}\}.$$

Legyen $\mathbf{w}_\mathcal{A}$ és $\mathbf{w}_\mathcal{B}$ az $\mathbf{A}$ és $\mathbf{B}$ halmazok maximális eleme a lexikografikus elrendezés szerint, és legyenek $\overline{a} \in \mathbf{A}$ és $\overline{b} \in \mathbf{B}$ azon elemek melyekre

$$\mathbf{w}_\mathcal{A} = (m_{d_1}(r \cdot x_1(\overline{a})), \dots, m_{d_s}(r \cdot x_s(\overline{a})))$$

és

$$\mathbf{w}_\mathcal{B} = (m_{d_1}(r \cdot x_1(\overline{b})), \dots, m_{d_s}(r \cdot x_s(\overline{b}))).$$

Ekkor a $\mathbf{w}_\mathcal{A}$ és $\mathbf{w}_\mathcal{B}$ maximalitása miatt a $\mathbf{w}_\mathcal{A} + \mathbf{w}_\mathcal{B}$ összegnek nincs más előállítása a

$$\mathbf{w} + \mathbf{w}', \quad \mathbf{w} \in \mathbf{A},\, \mathbf{w}' \in \mathbf{B}. \tag{2.18}$$

formában.

A (2.17) miatt az i-edik koordinátája az összegnek a

$$\left(-2\left[\frac{d_i}{4}\right], 2\left[\frac{d_i}{4}\right]\right] \subset \left(-\left[\frac{d_i}{2}\right], \left[\frac{d_i}{2}\right]\right]$$

intervallumban van. Tehát minden $a \in \mathcal{A}$ és $b \in \mathcal{B}$ esetén

$$\begin{aligned}&\big(m_{d_1}(r \cdot x_1(\overline{a})), \dots, m_{d_s}(r \cdot x_s(\overline{a}))\big) + \big(m_{d_1}(r \cdot x_1(\overline{b})), \dots, m_{d_s}(r \cdot x_s(\overline{b}))\big)\\ \neq &\big(m_{d_1}(r \cdot x_1(a)), \dots, m_{d_s}(r \cdot x_s(a))\big) + \big(m_{d_1}(r \cdot x_1(b)), \dots, m_{d_s}(r \cdot x_s(b))\big),\end{aligned}$$

amiből következik, hogy

$$r\overline{a} + r\overline{b} \neq ra + rb, \quad a \in \mathcal{A},\, b \in \mathcal{B}$$

és a $(r, \prod d_i) = 1$ tulajdonságot felhasználva, hogy

$$\overline{a} + \overline{b} \neq a + b, \quad a \in \mathcal{A},\, b \in \mathcal{B}.$$

□

3. fejezet

Pszeudovéletlen bináris sorozatok konstrukciója véges testek fölött

A fejezetben az 1.2 részben tárgyalt konstrukciók egy közös általánosítását tanulmányozom. A 2.1 rész jelöléseit felhasználva a következő módon definiálhatjuk az általános konstrukciót.

7. konstrukció. *Legyen p prímszám, ψ additív, χ multiplikatív karaktere $\mathbb{F}_p$-nek, $F(x)$, $Q(x) \in \mathbb{F}_p(x)$ racionális törtfüggvények. Ekkor definiáljuk az E_p sorozatot a következő módon:*

$$e_n = \begin{cases} +1 & \text{ha } \arg\left(\psi\left(F(n)\right) \cdot \chi\left(Q(n)\right)\right) \in [0, \pi) \text{ és } n \notin S \\ -1 & \text{máskülönben.} \end{cases}$$

Világos, hogy ha az F függvényt konstansnak és a χ karaktert a kvadratikus karakternek választjuk, akkor visszakapjuk a 2 konstrukciót. Másrészről, ha a χ karaktert úgy választjuk, hogy $\chi(g) = e^{\frac{2\pi i}{p-1}}$, ahol g generátor $\mathbb{F}_p$-ben akkor a 3 konstrukciót kapjuk. Végül általános χ multiplikatív karakter esetén a 4 konstrukciót kapjuk.

Másrészről, ha a Q függvény konstans, akkor visszakapjuk az 5 illetve a 6 konstrukciót, amennyiben az F függvény egy polinom vagy annak multiplikatív inverze.

Pszeudovéletlen bináris sorozatok konstrukcióját ilyen általánosságban először Oon tanulmányozta [24, 25]. Vizsgálta a 4 konstrukciót, és bebizonyította, hogy a konstrukció jó, ha a karakter rendje nagy: $\Omega(p^{1/2})$. Abban az esetben, amikor a karakter rendje kicsi (nagyságrendileg $o(p^{1/2})$) és páratlan, akkor nem várhatunk nemtriviális korlátot, amit a következő példa is mutat:

1. példa. *Ha χ egy harmad rendű multiplikatív karakter, és az E_p sorozatot a 4*

konstrukció definiálja $f(n) = n$ polinommal, akkor

$$U(E_p, p, 0, 1) = \sum_{j=0}^{p-1} e_j = \Big| |\{j : \chi(j) = 1\}| - |\{j : \chi(j) \neq 1\}| \Big| \gg \left| \frac{p}{3} - \frac{2p}{3} \right| = \frac{p}{3}.$$

Ezek alapján külön vizsgáljuk azt az esetet, amikor az F függvény konstans és a multiplikatív karakter rendje páros illetve azt az esetet, mikor az F függvény nem konstans.

3.1. Pszeudovéletlen bináris sorozatok konstrukciója multiplikatív karakter segítségével

8. tétel ([M1]). *Legyen p prím, χ multiplikatív karaktere $\mathbb{F}_p$-nek, melynek d rendje páros, $q \in \mathbb{F}_p[x]$ polinom, ami nem d-hatvány. Ha az E_p sorozatot a 4 konstrukció definiálja, akkor*

$$W(E_p) \leq 36sp^{1/2} \log p \log d + s, \tag{3.1}$$

ahol s az q gyökeinek számát jelöli.

Ha továbbá az q minden gyökének multiplicitása vagy relatív prím d-hez, vagy azzal osztható, és az (s, ℓ, p) hármas d megengedhető, akkor

$$C_\ell(E_p) \leq 9\, 4^\ell \ell s p^{1/2} \log p (\log d)^\ell + \ell s. \tag{3.2}$$

Megjegyezzük, hogy a tétel alkalmazható abban az általános esetben is, mikor a multiplikatív karakter argumentumában nem polinom, hanem általános racionális törtfüggvény szerepel. Adott q/r függvényhez tekintsük a $q \cdot r^{p-1}$ polinomot. Ekkor (legszámítva r gyökeit) a két függvény minden ponton megegyezik, azonban ebben az esetben az s paraméter az q/r gyökeinek és pólusainak számát fogja jelölni.

A 8 tetel bizonyítása. A (3.1) bizonyításához legyenek $a \in \mathbb{Z}$ és $b, t \in \mathbb{N}$ olyan számok, melyekre

$$1 \leq a \leq a + (t-1)b \leq t.$$

Ekkor a 7 lemma alapján

$$\begin{aligned}|U(E_T,t,a,b)| &= \left|\sum_{j=0}^{t-1} e_{a+jb}\right| \\ &\le \left|\sum_{\substack{0\le j<t\\ q(a+jb)\neq 0}} \frac{2}{d}\sum_{\gamma^d=\chi_0}^{*} \frac{1-\bar\gamma(g)^{\frac{d}{2}}}{1-\bar\gamma(g)}\cdot\gamma(q(a+jb))\right| + s \\ &\le \frac{2}{d}\sum_{\gamma^d=\chi_0}^{*}\left|\sum_{\substack{0\le j<t\\ q(a+jb)\neq 0}} \gamma(q(a+jb))\right|\left|\frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)}\right| + s.\end{aligned}$$

Mivel q nem d-hatvány, ezért a 4 tétel alkalmazható, így a 9 lemma alapján

$$\begin{aligned}&\frac{2}{d}\sum_{\gamma^d=\chi_0}\left|\sum_{\substack{0\le j<t\\ q(a+jb)\neq 0}} \gamma(q(a+jb))\right|\left|\frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)}\right| \le \\ &\qquad\le \frac{2}{d}9sp^{1/2}\log p\sum_{\gamma^d=\chi_0}^{*}\frac{2}{|1-\gamma(g)|} \\ &\qquad\le 36sp^{1/2}\log p\log d.\end{aligned}$$

A (3.2) bizonyításához legyenek $M\in\mathbb{N}$ és $D=(d_1,\dots,d_\ell)$ olyanok, hogy $0\le d_1<\dots<d_\ell\le p-M$. Ekkor a 7 lemma alapján

$$\begin{aligned}|V(E_T,M,D)| &= \left|\sum_{n=1}^{M} e_{n+d_1}\dots e_{n+d_\ell}\right| \le \\ &\le \left|\sum_{\substack{1\le n\le M:\\ q(n+d_i)\neq 0\\ i=1,\dots,\ell}} \frac{2^\ell}{d^\ell}\sum_{\gamma_1^d=\chi_0}^{*}\frac{1-\bar\gamma_1(g)^{\frac{d}{2}}}{1-\bar\gamma_1(g)}\cdot\gamma_1(q(n+d_1))\cdots\right. \\ &\qquad\left.\cdots\sum_{\gamma_\ell^d=\chi_0}^{*}\frac{1-\bar\gamma_\ell(g)^{\frac{d}{2}}}{1-\bar\gamma_\ell(g)}\cdot\gamma_\ell(q(n+d_\ell))\right| + \ell s \\ &\le \frac{2^\ell}{d^\ell}\sum_{\gamma_1^d=\chi_0}^{*}\cdots\sum_{\gamma_\ell^d=\chi_0}^{*}\left|\frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)}\cdots\frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)}\right|\cdot \\ &\qquad\cdot\left|\sum_{\substack{1\le n\le M:\\ q(n+d_i)\neq 0\\ i=1,\dots,\ell}}\gamma_1(q(n+d_1))\dots\gamma_\ell(q(n+d_\ell))\right| + \ell s.\end{aligned}$$

Adott γ_u $(u=1,\dots,\ell)$ karakter esetén legyen δ_u az az egész, melyre

$$\gamma_u=\chi^{\delta_u},\quad 0\le\delta_u<d,\quad u=1,\dots,\ell. \tag{3.3}$$

A jelölést használva kapjuk, hogy

$$\sum_{\substack{1\le n\le M:\\ q(n+d_i)\neq 0\\ i=1,\dots,\ell}} \gamma_1(q(n+d_1))\dots\gamma_\ell(q(n+d_\ell)) =$$

$$= \sum_{\substack{1\le n\le M:\\ q(n+d_i)\neq 0\\ i=1,\dots,\ell}} \chi\left(q^{\delta_1}(n+d_1)\dots q^{\delta_\ell}(n+d_\ell)\right).$$

Legyen $F_{\gamma_1,\dots,\gamma_\ell}(x) = F_{\delta_1,\dots,\delta_\ell}(x) = q^{\delta_1}(x+d_1)\cdot\ldots\cdot q^{\delta_\ell}(x+d_\ell)$. Hogy alkamazni tudjuk a 4 tételt, szükséges, hogy az $F_{\gamma_1,\dots,\gamma_\ell}(x)$ polinom ne legyen d-hatvány. Ezt garantálja nekünk a következő lemma:

19. lemma. *Legyen p prím, $q\in\mathbb{F}_p[x]$, mely nem d-hatvány, és minden gyökének multiplicitása vagy osztható d-vel, vagy ahhoz relatív prím. Ha s jelöli a q polinom különböző gyökeinek számát, és az (s,ℓ,p) d-megengedhető, akkor az $F_{\delta_1,\dots,\delta_\ell}(x) = q^{\delta_1}(x+d_1)\cdot\ldots\cdot q^{\delta_\ell}(x+d_\ell)$ polinom $(0<\delta_1\dots,\delta_\ell<d)$ nem d-hatvány.*

A lemma bizonyítása előtt megmutatom, hogy ez elég a tétel bizonyításához. Valóban, a 4 tétel és a 9 lemma alapján azt kapjuk, hogy

$$\begin{aligned}
|V(E_T,M,D)| &\le \frac{2^\ell}{d^\ell}\sum_{\gamma_1^d=\chi_0}^{*}\dots\sum_{\gamma_\ell^d=\chi_0}^{*}\left|\frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)}\dots\frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)}\right|\cdot\\
&\qquad\cdot\left|\sum_{\substack{1\le n\le M:\\ q(n+d_i)\neq 0\\ i=1,\dots,\ell}} F_{\gamma_1,\dots,\gamma_\ell}(n)\right| + \ell s.\\
&\le \frac{2^\ell}{d^\ell}\ell s p^{1/2}\log p\left(\sum_{\gamma^d=\chi_0}^{*}\frac{2}{|1-\gamma(g)|}\right)^\ell + \ell s\\
&\le \frac{2^\ell}{d^\ell}\ell s p^{1/2}\log p(2d\log d)^\ell + \ell s\\
&\le 4^\ell \ell s p^{1/2}\log p(\log d)^\ell + \ell s.
\end{aligned}$$

Végül a 19 lemma bizonyítása:

Bizonyítás. A bizonyításhoz bevezetünk $\mathbb{F}_p[x]$-en egy ekvivalencia relációt: két polinomot $\rho(x),\sigma(x)\in\mathbb{F}_p[x]$ azonos ekvivalencia osztályba sorolunk ($\rho(x)\sim\sigma(x)$), ha létezik olyan $c\in\mathbb{F}_p$ érték, hogy $\rho(x)=\sigma(x+c)$.

Bontsuk fel a q polinomot irreducibilis polinomok szorzatára, és a faktorokat csoportosítsuk az ekvivalencia osztályoknak megfelelően. A q-ra vonatkozó feltételek alapján van legalább egy olyan tényezője a szorzatnak, mely nem d-hatvány. Legyen ez a tényező:

$$\rho^{\alpha_1}(x+a_1)\dots\rho^{\alpha_t}(x+a_t),$$

ahol $d \nmid \alpha_1$ és $t \leq s$.

Indirekt tegyük fel, hogy a 19 lemma nem teljesül, azaz az $F_{\gamma_1,\ldots,\gamma_\ell}(x)$ polinom d-hatvány. Ekkor, ha ezt a polinomot is hasonló módon felbontjuk, az előbb kiválasztott ekvivalencia osztályba pontosan a $\rho(x + a_i + d_j)$ alakú polinomok fognak tartozni, ahol $i = 1, \ldots, t$, $j = 1, \ldots, \ell$.

Hogy ellentmondásra jussunk, legyen $\mathcal{A}$ az a_i $(i = 1, \ldots, t)$ elemekből álló multihalmaz, ahol az adott a_i elem multiplicitása α_i, és $\mathcal{B}$ a d_j $(j = 1, \ldots, \ell)$ elemekből álló multihalmaz, ahol most az adott d_j elem multiplicitása δ_j. Ha tehát az adott osztályba eső faktor d-hatvány, minden elem d-szeresen van reprezentálva az

$$a_i + b_j, \qquad i = 1, \ldots, t,\ j = 1, \ldots, \ell$$

formában, azaz az $\mathcal{A}, \mathcal{B}$ pár $P(d)$ tulajdonságú. □

□

3.2. Pszeudovéletlen bináris sorozatok általános konstrukciója

Az előző részben a 7 konstrukció azon speciális esetét néztük, mikor az additív karakter argumentumában a konstans függvény szerepel, és a multiplikatív karakter rendje páros. Ebben a részben azon általános esetet tanulmányozzuk, mikor az F függvény nem polinom, és a multiplikatív karakter tetszőleges.

9. tétel ([M3]). *Legyen $\psi \neq \psi_0$ additív, $\chi \neq \chi_0$ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek, $F(x) = \frac{f(x)}{g(x)}, Q(x) = \frac{q(x)}{r(x)} \in \mathbb{F}_p(x)$ olyan racionális törtfüggvények, melyre $(g(x), f(x)) = 1$, $(q(x), r(x)) = 1$ és sem f-nek, sem g-nek nincs többszörös gyöke, Q pedig nem d-hatvány. Ha az E_p sorozatot a 7 konstrukció definiálja, akkor*

$$W(E_p) \ll (\deg^* F + z) \cdot p^{1/2} (\log p)^2, \tag{3.4}$$

ahol z q és r különböző gyökeinek számát jelöli.

Továbbá, ha $\ell \in \mathbb{N}$ teljesíti az alábbi feltételek valamelyikét:

(i) $\ell = 2$;

(ii) $(4 \cdot \deg g)^\ell < p$, $(4 \cdot \deg^* Q)^\ell < p$;

(iii) $g(x) = (x + a_1)(x + a_2) \ldots (x + a_k)$ ($a_i \neq a_j$, $i \neq j$) és $\ell \cdot \deg g < \frac{p}{2}$, $(4 \cdot \deg^* Q)^\ell < p$,

akkor

$$C_\ell(E_p) \ll (\ell + 1)(\deg^* F + d \cdot \deg^* Q) \cdot p^{1/2} (\log p)^{\ell+1}. \tag{3.5}$$

Megjegyezem, hogy hasonló módszerekkel lehet azt az esetet is kezelni, mikor a Q függvény konstans [M2], ekkor a tételben szereplő korlátok megfelelői érvényesek.

Bizonyítás. A 3.4 bizonyításához legyenek $a \in \mathbb{Z}$ és $b, t \in \mathbb{N}$ olyan számok, melyekre

$$1 \le a \le a + (t-1)b \le t.$$

Ekkor a 8 lemma alapján

$$\begin{aligned} U(E_p, t, a, b) &= \sum_{j=0}^{t-1} e_{a+jb} = \\ &= \frac{1}{dp} \sum_{-[dp/2]<h\le[dp/2]} v_{dp}(h) \sum_{\substack{0\le j\le t-1 \\ a+jb\notin\mathcal{S}}} \psi\left(F(a+jb)\right)^h \chi\left(Q(a+jb)\right)^h + \mathcal{O}\left(\mathcal{S}\right) \\ &= \frac{1}{dp} \sum_{\substack{-[dp/2]<h\le[dp/2] \\ h\neq 0}} v_{dp}(h) \sum_{\substack{0\le j\le t-1 \\ a+jb\notin\mathcal{S}}} \psi\left(F(a+jb)\right)^h \chi\left(Q(a+jb)\right)^{r_d(h)} + \mathcal{O}\left(\mathcal{S}\right) + \frac{t}{dp}. \end{aligned}$$

Mivel $(p, d) = 1$, a $0 < |h| \le dp/2$ feltételből következik, hogy $h \nmid p$ vagy $h \nmid d$ (ekkor persze $r_d(h) \nmid d$), így alkamazhatjuk a 4 tételt:

$$|U(E_p, t, a, b)| \le 9\left(\deg^* F + s + z\right)p^{1/2}\log p \cdot \frac{1}{dp} \sum_{\substack{-[dp/2]<h\le[dp/2] \\ h\neq 0}} v_{dp}(h) + \mathcal{O}\left(\mathcal{S}\right) + \frac{t}{dp},$$

ahol s g különböző gyökeinek számát jelöli. Itt a 8 lemma miatt

$$\frac{1}{dp} \sum_{-[dp/2]<h\le[dp/2]} v_{dp}(h) \ll \frac{1}{dp} \sum_{0<|h|\le[dp/2]} v_{dp}(h) \ll \frac{1}{dp} \sum_{0<|h|\le[dp/2]} \frac{dp}{h} \ll \log p.$$

A 3.5 bizonyításához legyenek $M \in \mathbb{N}$ és $D = (d_1, \ldots, d_\ell)$ olyanok, hogy $0 \le d_1 < \cdots < d_\ell \le p - M$. Ekkor az előzőekhez hasonlóan

$$\begin{aligned} V(E_p, M, D) &= \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_\ell} = \\ &= \frac{1}{(dp)^\ell} \sum_{\substack{1\le n\le M \\ n+d_1,\ldots,\, n+d_\ell\notin\mathcal{S}}} \prod_{i=1}^{\ell} \cdot \\ &\quad \cdot \sum_{-[dp/2]<h_i\le[dp/2]} v_{dp}(h_i)\left(\psi\left(F(n+d_i)\right)\chi\left(Q(n+d_i)\right)\right)^{h_i} + \\ &\quad + \mathcal{O}\left(\ell\,\mathcal{S}\right) = \end{aligned}$$

$$= \frac{1}{(dp)^\ell} \sum_{-[dp/2]<h_1\le[dp/2]} \cdots \sum_{-[dp/2]<h_\ell\le[dp/2]} v_{dp}(h_1)\dots v_{dp}(h_\ell)$$
$$\sum_{\substack{1\le n\le M \\ n+d_1,\dots,\, n+d_\ell\notin\mathcal{S}}} \prod_{i=1}^{\ell} \left(\psi\left(F(n+d_i)\right)\chi\left(Q(n+d_i)\right)\right)^{h_i}$$
$$+ \frac{1}{(dp)^\ell} M + \mathcal{O}\left(\ell\,\mathcal{S}\right)$$

Tekintsük most a legbelső összeget (ahol most nem minden $h_i = 0$), és legyenek $h_{i_1} \le \dots \le h_{i_t}$ a (nem nulla) h_i-k ($i = 1, \dots, \ell$). Ekkor

$$\begin{aligned}
&\sum_{\substack{1\le n\le M \\ n+d_1,\dots,\, n+d_\ell\notin\mathcal{S}}} \prod_{i=1}^{\ell} \left(\psi\left(F(n+d_i)\right)\chi\left(Q(n+d_i)\right)\right)^{h_i} = \\
&= \sum_{\substack{1\le n\le M \\ n+d_1,\dots,\, n+d_\ell\notin\mathcal{S}}} \psi\left(\sum_{i=1}^{\ell} h_i F(n+d_i)\right)\chi\left(\prod_{i=1}^{\ell} Q(n+d_i)^{h_i}\right) = \\
&= \sum_{\substack{1\le n\le M \\ n+d_{i_1},\dots,\, n+d_{i_r}\notin\mathcal{S}}} \psi\left(\sum_{j=1}^{r} h_{i_j} F(n+d_{i_j})\right)\chi\left(\prod_{j=1}^{r} Q(n+d_{i_j})^{r_d(h_{i_j})}\right) = \\
&= \sum_{\substack{1\le n\le M \\ n+d_{i_1},\dots,\, n+d_{i_r}\notin\mathcal{S}}} \psi\left(\frac{f_{h_1,\dots,h_\ell}(n)}{g_{h_1,\dots,h_\ell}(n)}\right)\chi\left(\frac{q_{h_1,\dots,h_\ell}(n)}{r_{h_1,\dots,h_\ell}(n)}\right),
\end{aligned} \tag{3.6}$$

ahol

$$\begin{aligned}
f_{h_1,\dots,h_\ell}(x) &= \sum_{t=1}^{r} h_{i_t} f(x+d_{i_t}) \prod_{\substack{1\le j\le r \\ j\ne t}} g(x+d_{i_j}), \\
g_{h_1,\dots,h_\ell}(x) &= \prod_{j=1}^{r} g(x+d_{i_j}), \\
q_{h_1,\dots,h_\ell}(x) &= \prod_{j=1}^{r} q(x+d_{i_j})^{r_d(h_{i_j})}, \\
r_{h_1,\dots,h_\ell}(x) &= \prod_{j=1}^{r} r(x+d_{i_j})^{r_d(h_{i_j})},
\end{aligned}$$

ahol

$$\begin{aligned}
\deg f_{h_1,\dots,h_\ell} &\le \deg f + (r-1)\cdot\deg g \le \deg f + (\ell-1)\cdot\deg g, \\
\deg g_{h_1,\dots,h_\ell} &= r\cdot\deg g \le \ell\cdot\deg g \\
\deg^*\left(\frac{q_{h_1,\dots,h_\ell}}{r_{h_1,\dots,h_\ell}}\right) &\le \sum_{j=1}^{r} r_d(h_{i_j})\deg^* Q \le \ell d\cdot\deg^* Q.
\end{aligned}$$

Hogy megmutassuk, hogy a (3.6) karakterösszeg nem elfajuló, két esetet különböztetünk meg: Először tegyük fel, hogy az összes nem nulla h_i indexek nem oszthatóak p-vel. Ekkor a következő lemma alapján a karakter összeg nem elfajuló (7. lemma ld: [M3])

20. lemma. *Ha p, $f(x), g(x)$ és ℓ kielégíti a 9 tétel feltételeit és $p \nmid h_{i_j}$, $j = 1, \dots, r$, akkor $g_{h_1,\dots,h_\ell}(x) \nmid f_{h_1,\dots,h_\ell}(x)$.*

Ha valamely i-re $p \mid h_i$, akkor $d \nmid h_i$, így alkalmazható a következő lemma (8. lemma ld: [M3])

21. lemma. *Ha p, $q(x), r(x)$ és ℓ kielégíti a 9 tétel feltételeit, valamint van olyan j index melyre $d \nmid h_{i_j}$, akkor*

$$\frac{q_{h_1,\dots,h_\ell}(x)}{r_{h_1,\dots,h_\ell}(x)} = bB^d(x)$$

nem teljesül semmilyen $b \in \mathbb{F}_p$ és $B(x) \in \mathbb{F}_p(x)$ esetén.

Ekkor mindkét esetben

$$\left| \sum_{\substack{1 \le n \le M \\ n+d_{i_1},\dots,n+d_{i_r} \notin \mathcal{S}}} \psi\left(\frac{f_{h_1,\dots,h_\ell}(n)}{g_{h_1,\dots,h_\ell}(n)}\right) \chi\left(\frac{q_{h_1,\dots,h_\ell}(n)}{r_{h_1,\dots,h_\ell}(n)}\right) \right| \le$$

$$\le 9\left(\deg^*\left(\frac{f_{h_1,\dots,h_\ell}(x)}{g_{h_1,\dots,h_\ell}(x)}\right) + \deg^*\left(\frac{q_{h_1,\dots,h_\ell}(x)}{r_{h_1,\dots,h_\ell}(x)}\right)\right) p^{1/2} \log p \le$$

$$\le 9(\ell+1)\left(\deg^*(F(x)) + d \cdot \deg^*(Q(x))\right) p^{1/2} \log p, \quad (3.7)$$

ugyanis

$$\begin{aligned} \max\{\deg f_{h_1,\dots,h_\ell}, \deg g_{h_1,\dots,h_\ell}\} + s_{h_1,\dots,h_\ell} &\le \deg f + (\ell+1) \cdot \deg g \\ &\le (\ell+1) \cdot \deg^* F \end{aligned}$$

ahol $s_{h_1,\dots,h_\ell}$ a $g_{h_1,\dots,h_\ell}$ különböző gyökeinek számát jelöli.

Ekkor a (3.4) rész bizonyításához hasonlóan kapjuk, hogy

$$
\begin{aligned}
&|V(E_p, M, D)| \ll \\
&\ll \frac{1}{(dp)^\ell} \left| \sum_{\substack{-[dp/2]<h_1\le[dp/2] \\ (h_1,\dots,h_\ell)\neq(0,\dots,0)}} \cdots \sum_{-[dp/2]<h_\ell\le[dp/2]} v_{dp}(h_1)\dots v_{dp}(h_\ell) \right| \cdot \\
&\cdot \left| \sum_{\substack{1\le n\le M \\ n+d_1,\dots,\, n+d_\ell\notin\mathcal{S}}} \psi\left(\prod_{i=1}^{\ell} h_i F(n+d_i)\right) \chi\left(\sum_{i=1}^{\ell} Q(n+d_i)^{h_i}\right) \right| + \\
&+ \mathcal{O}(\ell\,|\mathcal{S}|) \\
&\ll \frac{1}{(dp)^\ell}(\ell+1)\left(\deg^* F + d\cdot\deg^* Q\right) p^{1/2}\log p \left(\sum_{|h|<dp/2} |v_{dp}(h)|\right)^{\ell} + \\
&+ \mathcal{O}(|\mathcal{S}|\ell) + \mathcal{O}\left(\ell\cdot\deg f\right) \\
&\ll (\ell+1)\left(\deg^*(F(x)) + d\cdot\deg^*(Q(x))\right) p^{1/2}(\log p)^{\ell+1}.
\end{aligned}
$$

□

4. fejezet

Pszeudovéletlen bináris rácsok

Az alkalmazásokban a pszeudovéletlen sorozatok mellet komoly igény mutatkozott pszeudovéletlen rácsok iránt is, például szteganográfiában, több dimenziós képek titkosításában, vízjelkészitésben. Ezért Hubert, Mauduit és Sárközy kiterjesztette a pszeudovéletlen bináris sorozatok fogalmát több dimenzióra [14]. Legyen I_N^n az olyan n-dimenziós vektorokból álló halmaz, mely vektorok koordinátái a $\{0, 1, \ldots, N-1\}$ halmazból kerülnek ki:

$$I_N^n = \big\{\mathbf{x} = (x_1, \ldots, x_n) : \, x_1, \ldots, x_n \in \{0, 1, \ldots, N-1\}\big\}.$$

Ekkor a bináris rács mint az I_N^n halmazon értelmezett bináris függvény van definiálva:

$$\eta : I_N^n \to \{-1, +1\}.$$

Az egydimenziós esethez hasonlóan definiálhatjuk a mértékeket. Ehhez legyen először $\mathbf{u}_1, \ldots, \mathbf{u}_n$ n darab lineárisan független vektor, melyeknek $n-1$ koordinátája nulla. Legyenek $t_1, \ldots, t_n$ olyan egészek, melyekre $0 \leq t_1, \ldots, t_n < N$. Ekkor B_N^n (vagy röviden B) *tégla rácsot* (box lattice) a következőképpen definiáljuk:

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u}_1 + \cdots + x_n\mathbf{u}_n : \, 0 \leq x_i|\mathbf{u}_i| \leq t_i, \; i = 1, \ldots, n\}\,.$$

22. definíció. *Az η sorozat ℓ-ed rendű véletlenségi mértéke a*

$$Q_\ell(\eta) = \max_{B, \mathbf{d}_1, \ldots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d}_1) \ldots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|,$$

ahol a maximum az összes $\mathbf{d}_1, \ldots, \mathbf{d}_\ell \in I_N^n$ és B téglarácsra vétetik, melyre $B + \mathbf{d}_1, \ldots, B + \mathbf{d}_\ell \subseteq I_N^n$.

Huber, Mauduit és Sárközy szintén vizsgálta, hogy hogyan viselkednek ezen mértékek a valódi véletlen esetben [14]:

10. tétel (Huber, Mauduit és Sárközy). *Ha $\ell \in \mathbb{N}$, $\varepsilon > 0$, akkor létezik olyan $N_0 = N_0(\ell, \varepsilon)$ és $\delta = \delta(\ell, \varepsilon) > 0$, hogy ha $N > N_0$, akkor*

$$\delta N^{n/2} < Q_\ell(\eta) < (81\ell\, N^n \log N^n)^{1/2}$$

teljesül $1 - \varepsilon$-nál nagyobb valószínűséggel.

Mauduit és Sárközy [21] (kiterjesztve a [14]-ben található konstrukciót) példát mutatott jó pszeudovéletlen tulajdonságokkal rendelkező rácsra:

8. konstrukció (Mauduit és Sárközy). *Legyen $q = p^n$ prímhatvány, γ a kvadratikus karaktere $\mathbb{F}_q$-nak, $f(x) \in \mathbb{F}_q[x]$. Ekkor definiáljuk az η rácsot a következőképpen:*

$$\eta(\mathbf{x}) = \begin{cases} \gamma(f(x_1b_1 + \cdots + x_nb_n)) & \text{ha } f(x_1b_1 + \cdots + x_nb_n) \neq 0, \\ 1 & \text{máskülönben,} \end{cases}$$

ahol $b_1, \ldots, b_n$ $\mathbb{F}_q$ egy bázisa $\mathbb{F}_p$ fölött és $\mathbf{x} = (x_1, \ldots, x_n)$.

Bebizonyították továbbá, hogy ha f kielégít bizonyos feltételeket, akkor ez a konstrukció jó:

$$Q_\ell(\eta) < \deg f\, \ell(q^{1/2}(1 + \log p)^n + 2).$$

További jó konstrukciókat ld: [11], [12], [22].

Megjegyezem, hogy mind a bináris rács fogalmát, mind a mértékeket ki lehet terjeszteni több szimbólumú esetre, ld [M5].

4.1. Pszeudovéletlen bináris rácsok konstrukciója multiplikatív karakter segítségével

A 4 konstrukcióhoz hasonlóan kiterjeszthetjük a 8 konstrukciót általános multiplikatív karakterre:

9. konstrukció. *Legyen $q = p^n$ prímhatvány, $f(x) \in \mathbb{F}_q[x]$, χ multiplikatív karaktere $\mathbb{F}_q$-nak. Ekkor definiáljuk az η rácsot a következőképpen:*

$$\eta(\mathbf{x}) = \begin{cases} +1 & \text{ha } \arg\left(\chi(f(x_1b_1 + \cdots + x_nb_n))\right) \in [0, \pi), \\ -1 & \text{máskülönben,} \end{cases}$$

ahol $b_1, \ldots, b_n$ $\mathbb{F}_q$ egy bázisa $\mathbb{F}_p$ fölött és $\mathbf{x} = (x_1, \ldots, x_n)$.

A következő tétel alapján ez egy jó konstrukció:

11. tétel ([M4]). *Legyen $q = p^n$ egy páratlan prímhatvány, χ multiplikatív karaktere $\mathbb{F}_q$-nak, melynek d rendje páros, $f(x) \in \mathbb{F}_q[x]$ olyan polinom mely nem d-hatvány, és minden gyökének multiplicitása vagy osztható d-vel, vagy ahhoz relatív prím. Tegyük fel továbbá, hogy a $(\deg f, \ell, \mathbb{F}_q)$ hármas megengedhető. Ekkor*

$$Q_\ell(\eta) \le 4^\ell \ell \deg f (\log d)^\ell q^{1/2} (1+\log p)^n \ell \deg f.$$

1. megjegyzés.. *Hasonló módszerekkel kezelhetjük azt az esetet is, mikor a karakter rendje páratlan [M4]. Ekkor hasonlóan az egydimenziós esethez, a konstrukció csak nagy d-re használható:*

$$Q_\ell(\eta) \ll_\ell \deg f (\log d)^\ell q^{1/2} (1+\log p)^n + \frac{q}{d^\ell}.$$

Bizonyítás. Azonosítsuk az $\mathbb{F}_p^n$ vektorteret $\mathbb{F}_q$-val az $\mathbf{x} \leftrightsquigarrow x = x_1 b_1 + \cdots + x_n b_n$ megfeleltetéssel. Ekkor $\eta(\mathbf{x}) = \eta(x)$.

A bizonyításhoz tekintsünk egy B téglarácsot, $d_1, \dots d_\ell \in \mathbb{F}_q$ elemeket, hogy $B + d_1, \dots, B + d_\ell \in I_p^n$. Legyen $\mathcal{N}$ a lehetséges gyökök halmaza:

$$\mathcal{N} = \{x \in B : f(x+d_1) \cdot \ldots \cdot f(x+d_\ell) = 0\}.$$

Ekkor a 7 lemma alapján

$$\begin{aligned}
&\left| \sum_{x \in B} \eta(x+d_1) \dots \eta(x+d_\ell) \right| \le \\
&\le \left| \sum_{x \in B \setminus \mathcal{N}} \frac{2^\ell}{d^\ell} \sideset{}{^*}\sum_{\gamma_1^d = \chi_0} \frac{1-\bar{\gamma_1}(g)^{\frac{d}{2}}}{1-\bar{\gamma_1}(g)} \cdot \gamma_1(f(x+d_1)) \cdots \right. \\
&\qquad \left. \cdots \sideset{}{^*}\sum_{\gamma_\ell^d = \chi_0} \frac{1-\bar{\gamma_\ell}(g)^{\frac{d}{2}}}{1-\bar{\gamma_\ell}(g)} \cdot \gamma_\ell(f(x+d_\ell)) \right| + \ell \deg f \\
&\le \frac{2^\ell}{d^\ell} \sideset{}{^*}\sum_{\gamma_1^d = \chi_0} \cdots \sideset{}{^*}\sum_{\gamma_\ell^d = \chi_0} \left| \frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)} \cdots \frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)} \right| \cdot \\
&\qquad \cdot \left| \sum_{x \in B \setminus \mathcal{N}} \gamma_1(f(x+d_1)) \dots \gamma_\ell(f(x+d_\ell)) \right| + \ell \deg f.
\end{aligned}$$

Ha adott γ_u $(u = 1, \dots, \ell)$ karakter esetén δ_u egészet a 3.3-hoz hasonlóan definiáljuk, akkor

$$\begin{aligned}
&\sum_{x \in B \setminus \mathcal{N}} \gamma_1(f(x+d_1)) \dots \gamma_\ell(f(x+d_\ell)) = \\
&= \sum_{x \in B \setminus \mathcal{N}} \chi\big(f^{\delta_1}(x+d_1) \dots f^{\delta_\ell}(x+d_\ell)\big) = \sum_{x \in B \setminus \mathcal{N}} \chi(F_{\delta_1,\dots,\delta_\ell}(x)).
\end{aligned}$$

A 19 lemmához hasonlóan igazolhatjuk [M4]:

23. lemma. *Ha a 11 tétel feltételei teljasülnek, és* $0 < \delta_1, \dots, \delta_\ell < d$, *akkor az* $F_{\delta_1,\dots,\delta_\ell}(x)$ *függvény nem* d*-hatvány.*

A lemma alapján a fenti karakterösszeg nem triviális, így alaklmazható az 5 tétel:

$$\begin{aligned}
&\left|\sum_{x\in B}\eta(x+d_1)\dots\eta(x+d_\ell)\right| \leq \\
&\leq \frac{2^\ell}{d^\ell}\sum_{\gamma_1^d=\chi_0}^{*}\dots\sum_{\gamma_\ell^d=\chi_0}^{*}\left|\frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)}\dots\frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)}\right|\cdot\left|\sum_{x\in B\setminus\mathcal{N}}F_{\delta_1,\dots,\delta_\ell}(x)\right|+\ell\deg f \\
&\leq \frac{2^\ell}{d^\ell}\ell\deg f q^{1/2}(1+\log p)^n\left(\sum_{\gamma^d=\chi_0}^{*}\left|\frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)}\right|\right)^\ell+\ell\deg f \\
&\leq 4^\ell\ell\deg f(\log d)^\ell q^{1/2}(1+\log p)^n+\ell\deg f
\end{aligned}$$

a 9 lemma miatt. □

5. fejezet

Pszeudovéletlen bináris sorozatok és rácsok elliptikus görbék felett

Kriptográfiai alkalmazásokban előszeretettel használnak elliptikus görbéket, azok véletlen viselkedése miatt. Elliptikus görbék segítségével először Hallgren definiált sorozatot [13]. Nevezetesen definiálta az *elliptikus görbe fölötti lineáris kongruencia generátort*: Adott $\mathcal{E}$ elliptikus görbe és $P, P_0 \in \mathcal{E}$ pont esetén a sorozatot az $s_0 = P_0$ és az

$$s_n = P \oplus s_{n-1} = nP \oplus P_0 \tag{5.1}$$

rekurzió definiálja.

Chen [3], illetve később Chen, Li, és Xiao [4] tanulmányozta az ebből a sorozatból származtatható bináris sorozatokat, ahol a bináris sorozatot a Legendre szimbólum, illetve véges testek fölötti diszkrét logaritmus segítségével származtatták. A fejezetben ezt az elméletet terjesztem ki, illetve vizsgálom az elliptikus görbék alkalmazhatóságát pszeudovéletlen bináris rácsok generálásra.

5.1. Elliptikus görbék és karakterösszegek

Ebben a részben összefoglalom az elliptikus görbékre vonatkozó alapvető jelöléseket és karakterösszeg becsléseket.

Legyen $p > 3$ prímszám, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ felett, melyet a Weierstrass egyenlet definiál:

$$y^2 = x^3 + Ax + B,$$

ahol $A, B \in \mathbb{F}_p$ és a diszkrimináns nem nulla (ld [8]).

Az $\mathbb{F}_p$-racionális pontok $\mathcal{E}(\mathbb{F}_p)$ Abel csoportot alkotnak, ahol a művelet az összeadás: $\oplus$ (és ennek inverze: $\ominus$). Egy R pont esetén nR legyen $nR = \bigoplus_{i=1}^{n} R$.

$\mathcal{E}(\mathbb{F}_p)$ mint csoport izomorf két ciklikus csoport direkt szorzatával: $\mathcal{E}(\mathbb{F}_p) \cong \mathbb{Z}_M \times \mathbb{Z}_L$ adott $L \mid M$ egészekre. A P, Q elempár egy bázis, ha P rendje M, Q rendje L és minden elem egyértelműen írható fel $mP \oplus lQ$ alakban, ahol $0 \leq m < M$ és $0 \leq l < L$

Legyen $\mathbb{F}_p(\mathcal{E})$ az $\mathcal{E}$ függvényteste $\mathbb{F}_p$ fölött. Az $f \in \mathbb{F}_p(\mathcal{E})$ függvény *divizora* a

$$\mathrm{Div}(f) = \sum_{R \in \mathcal{E}(\overline{\mathbb{F}}_p)} \mathrm{ord}_R(f)[R],$$

formális összeg, ahol $\mathrm{ord}_R(f)$ az f rendje R-ben.

Az f gyökeinek és pólusainak halmaza

$$\mathrm{Supp}(f) = \{R \in \mathcal{E}(\overline{\mathbb{F}}_p) \mid \mathrm{ord}_R(f) \neq 0\}$$

az f divizorának tartója.

Az f foka a függvény divizorának nemnegatív együtthatóinak összege:

$$\deg f = \sum_{\mathrm{ord}_R(f) > 0} \mathrm{ord}_R(f).$$

Például $\deg x = 2$, $\deg y = 3$.

τ_W a $W \in \mathcal{E}(\mathbb{F}_p)$ elemmel történő eltolás:

$$\begin{aligned} \tau_W : \mathcal{E}(\mathbb{F}_p) &\to \mathcal{E}(\mathbb{F}_p), \\ P &\mapsto P \oplus W. \end{aligned}$$

Az $\mathcal{E}(\mathbb{F}_p)$, mint Abel csoport karakterei:

$$\Omega = \{\omega_{ab} : \ \omega_{ab}(mP \oplus lQ) = e_M(am)e_L(bl) \ \ 0 \leq m < M \text{ éa } 0 \leq l < L\}$$

ahol P és Q egy fix bázis)

Adott χ $\mathbb{F}_p$ fölötti multiplikatív karakter, ψ additív karakter, $\omega \in \Omega$ $\mathcal{E}(\mathbb{F}_p)$ fölötti karakter és $f \in \mathbb{F}_p(\mathcal{E})$ függvény esetén legyen:

$$S(\omega, \chi, f) = \sum_{\substack{P \in \mathcal{E}(\mathbb{F}_p) \\ f(P) \neq 0, \infty}} \omega(P)\chi(f(P)),$$

és

$$S(\omega, \psi, f) = \sum_{\substack{P \in \mathcal{E}(\mathbb{F}_p) \\ f(P) \neq \infty}} \omega(P)\psi(f(P)),$$

illetve adott $\mathcal{H} \leq \mathcal{E}(\mathbb{F}_p)$ részcsoport esetén legyen

$$S_{\mathcal{H}}(\omega, \chi, f) = \sum_{\substack{P \in \mathcal{H} \\ f(P) \neq 0, \infty}} \omega(P)\chi(f(P)).$$

és

$$S_{\mathcal{H}}(\omega, \chi, f) = \sum_{\substack{P \in \mathcal{H} \\ f(P) \neq \infty}} \omega(P)\psi(f(P)).$$

Ha az összeg nem triviális, akkor a karakterösszeg becsülhető [3]:

12. tétel. *Legyen $\chi \neq \chi_0$ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek, $\omega \in \Omega$ karaktere $\mathcal{E}(\mathbb{F}_p)$-nek. Ha $f \in \mathbb{F}_p(\mathcal{E})$ nem d-hatvány, akkor*

$$|S(\omega, \chi, f)| \leq 2|\operatorname{Supp}(f)|\sqrt{p}.$$

A tétel egy következménye [M6]:

24. Következmény. *Ha χ, ω és f mint előbb, $\mathcal{H} \leq \mathcal{E}(\mathbb{F}_p)$ részcsoport, akkor*

$$|S_{\mathcal{H}}(\omega, \chi, f)| \leq 2|\operatorname{Supp}(f)|\sqrt{p}.$$

Az additív esetben hasonló bizonyítható:

13. tétel (Kohel, Shparlinski [15]). *Legyen $\psi \neq \psi_0$ additív karaktere $\mathbb{F}_p$-nek, $\omega \in \Omega$ karaktere $\mathcal{E}(\mathbb{F}_p)$-nek. Ha $f \in \mathbb{F}_p(\mathcal{E})$ nem konstans, akkor*

$$|S(\omega, \psi, f)| \leq 2\deg(f)\sqrt{p}.$$

A fönti eredmények segítségével bizonyíthatunk nem triviális korlátot nemteljes karakterösszegekre is:

25. lemma (Chen, Li, Xiao [4]). *Legyen $Q \in \mathcal{E}(\mathbb{F}_p)$ N-ed rendű pont, $\chi \neq \chi_0$ multiplikatív karaktere $\mathbb{F}_p$-nek, $f \in \mathbb{F}_p(\mathcal{E})$ olyan függvény, melyre $f(x, y) \neq z^d(x, y)$ minden $z \in \overline{\mathbb{F}}_p(\mathcal{E})$ esetén. Ekkor minden $a, b, t \in \mathbb{N}$ számra, melyre $1 \leq a \leq a + (t-1)b \leq N$, a következő teljesül:*

$$\left|\sum_{x=0}^{t-1} \chi(f((a+bx)Q))\right| < |\operatorname{Supp}(f)|p^{1/2}(1 + \log N).$$

Illetve az additív esetben:

26. lemma (Chen, Xiao [5]). *Legyen $Q \in \mathcal{E}(\mathbb{F}_p)$ N-ed rendű pont, $f \in \mathbb{F}_p(\mathcal{E})$ nem konstans függvény. Ekkor minden $a, b, t \in \mathbb{N}$ számra, melyre $1 \leq a \leq a + (t-1)b \leq N$, a következő teljesül:*

$$\left|\sum_{i=0}^{t-1} e_p(f((a+bi)G))\right| \ll \deg f p^{1/2} \log N.$$

A következőkben bizonyítom az 5 tétel megfelelőjét. A tétel kimondásához szükségünk lesz a gyenge függetlenség fogalmára.

27. definíció. *A $P_1, \dots, P_n$ elemek gyengén függetlenek, ha*

$$a_1P_1 \oplus \cdots \oplus a_nP_n = \mathcal{O} \quad \Longrightarrow \quad a_iP_i = \mathcal{O},\ i = 1, \dots, n.$$

Megjegyezem, hogy ha a $P_1, \dots, P_n$ elemek gyengén függetlenek, akkor a $P_1, \dots, P_n, P_{n+1} = \mathcal{O}$ is azok, azonban ezt a triviális esetet (amikor valamely elem a $\mathcal{O}$) a továbbiakban kizárjuk.

14. tétel ([M6]). *Legyen χ d-ed rendű multiplikatív karakter, $f \in \mathbb{F}_p(\mathcal{E})$, mely nem d-hatvány $\overline{\mathbb{F}}_p(\mathcal{E})$ fölött. Legyenek $P_1, \dots, P_n \in \mathcal{E}(\mathbb{F}_p)$ gyengén független pontok, és $t_1, \dots, t_n \in \mathbb{N}$ olyan egészek, melyekre $t_i < |P_i|$.*

Legyen

$$B = \{i_1P_1 \oplus \cdots \oplus i_nP_n : i_1 \le t_1, \dots, i_n \le t_n\},$$

ekkor

$$\sum_{Q \in B} \chi(f(Q)) \le 2 \cdot 3^n \deg(f) p^{1/2} \left(\log |\mathcal{E}(\mathbb{F}_p)|\right)^n.$$

A tétel bizonyítása során felhasználom a következő lemmát:

28. lemma ([M4]). *Legyen $P \in \mathcal{E}(\mathbb{F}_p)$ és $t \in \mathbb{N}$ olyan egész, melyre $t < |P|$. Ekkor*

$$\sum_{\omega \in \Omega} \left| \sum_{i=0}^{t} \omega(iP) \right| \le 3|\mathcal{E}(\mathbb{F}_p)| \log |\mathcal{E}(\mathbb{F}_p)|.$$

A 14 tétel bizonyítása. A csoportkarakterek alapvető tulajdonságai alapján

$$\begin{aligned}
&\sum_{Q \in B} \chi(f(Q)) = \sum_{i_1=0}^{t_1} \cdots \sum_{i_n=0}^{t_n} \chi(f(i_1P_1 \oplus \cdots \oplus i_nP_n)) \\
&= \frac{1}{|\mathcal{E}(\mathbb{F}_p)|^n} \sum_{i_1=0}^{t_1} \cdots \sum_{i_n=0}^{t_n} \sum_{\omega_1, \dots, \omega_n} \sum_{j_1=1}^{|P_1|} \cdots \sum_{j_n=1}^{|P_n|} \chi(f(j_1P_1 \oplus \cdots \oplus j_nP_n)) \cdot \\
&\qquad \cdot \omega_1(j_1 - i_1) \dots \omega_n(j_n - i_n) \\
&= \frac{1}{|\mathcal{E}(\mathbb{F}_p)|^n} \sum_{\omega_1, \dots, \omega_n} \sum_{j_1=1}^{|P_1|} \cdots \sum_{j_n=1}^{|P_n|} \chi(f(j_1P_1 \oplus \cdots \oplus j_nP_n)) \omega_1(j_1P_1) \dots \omega_n(j_nP_n) \\
&\qquad \cdot \sum_{i_1=0}^{t_1} \cdots \sum_{i_n=0}^{t_n} \omega_1(-i_1P_1) \dots \omega_n(-i_nP_n) = \\
&= \frac{1}{|\mathcal{E}(\mathbb{F}_p)|^n} \sum_{\omega_1, \dots, \omega_n} \sum_{j_1=1}^{|P_1|} \cdots \sum_{j_n=1}^{|P_n|} \chi(f(j_1P_1 \oplus \cdots \oplus j_nP_n)) \omega_1(j_1P_1) \dots \omega_n(j_nP_n) \\
&\qquad \cdot \prod_{\nu=1}^{n} \left(\sum_{i_\nu=0}^{t_\nu} \omega_\nu(-i_\nu P_\nu) \right).
\end{aligned}$$

Ahonnan a háromszög egyenlőtlenség alapján

$$\left|\sum_{Q\in B}\chi(f(Q))\right| \leq$$
$$\leq \frac{1}{|\mathcal{E}(\mathbb{F}_p)|^n}\sum_{\omega_1,\ldots,\omega_n}\left|\sum_{j_1=1}^{|P_1|}\cdots\sum_{j_n=1}^{|P_n|}\chi(f(j_1P_1\oplus\cdots\oplus j_nP_n))\omega_1(j_1P_1)\cdots\omega_n(j_nP_n)\right|\cdot$$
$$\cdot\prod_{\nu=1}^{n}\left|\sum_{i_\nu=0}^{t_\nu}\omega_\nu(-i_\nu P_\nu)\right|. \tag{5.2}$$

□

Legyen most $\mathcal{H}\leq\mathcal{E}(\mathbb{F}_p)$ a $P_1,\ldots,P_n$ elemek által generált részcsoport. Mivel a $P_1,\ldots,P_n$ elemek gyengén függetlenek, ezért

$$\tilde{\omega}:\left\{\begin{array}{rcl}\mathcal{H} & \longrightarrow & \mathbb{C}^*\\ j_1P_1\oplus\cdots\oplus j_nP_n & \longmapsto & \omega_1(j_1P_1)\cdot\ldots\cdot\omega_n(j_nP_n)\end{array}\right.$$

jól definiált, és ez $\mathcal{H}$ egy karaktere. Legyen ω az a karaktere $\mathcal{E}(\mathbb{F}_p)$-nek, melyre $\tilde{\omega}=\omega\ \mathcal{H}-n$

Ezzel a választással

$$\begin{aligned}&\left|\sum_{j_1=1}^{|P_1|}\cdots\sum_{j_n=1}^{|P_n|}\chi(f(j_1P_1\oplus\cdots\oplus j_nP_n))\omega_1(j_1P_1)\cdots\omega_n(j_nP_n)\right|\\ &=\left|\sum_{P\in\mathcal{H}}\chi(f(P))\omega(P)\right|\leq 2\deg(f)p^{1/2}\end{aligned} \tag{5.3}$$

a 24 következmény miatt. Az (5.2), (5.3) és a 28 lemma alapján

$$\begin{aligned}\left|\sum_{Q\in B}\chi(f(Q))\right| &\leq 2\deg(f)p^{1/2}\frac{1}{|\mathcal{E}(\mathbb{F}_p)|^n}\prod_{\nu=1}^{n}\sum_{\omega}\left|\sum_{i=0}^{t_\nu}\omega(iP_\nu)\right|\\ &\leq 2\deg(f)p^{1/2}\frac{1}{|\mathcal{E}(\mathbb{F}_p)|^n}\left(3|\mathcal{E}(\mathbb{F}_p)|\log|\mathcal{E}(\mathbb{F}_p)|\right)^n\\ &=2\cdot 3^n\deg(f)p^{1/2}\left(\log|\mathcal{E}(\mathbb{F}_p)|\right)^n.\end{aligned}$$

5.2. Pszeudovéletlen sorozatok elliptikus görbék fölött

Elliptikus görbék felett pontok egy sorozatát a már említett (5.1)-beli lineáris kongruencia generátor segítségével lehet generálni. Persze, ha ismerjük a sorozat két

korábbi elemét, akkor könnyen ki tudjuk számítani a rákövetkező elemeket is, így a gyakorlatban még a pontokra egy $\mathbb{F}_p(\mathcal{E})$-beli függvényt is alkalmaznak:

$$n \mapsto f(nP). \tag{5.4}$$

A sorozat pszeudovéletlenségi tulajdonságainak vizsgálatához, az ebből a sorozatból képzett bináris sorozatokat vizsgáljuk a már eddig is használt mértékekkel. A sorozatot legegyszerűbben a Legendre szimbólummal tudjuk bináris sorozattá transzformálni:

10. konstrukció (Chen). *Legyen p prímszám, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ fölött, $G \in \mathcal{E}(\mathbb{F}_p)$ T-ed rendű elem, $f \in \mathbb{F}_p(\mathcal{E})$. Ekkor definiáljuk az $E_T = \{e_1, \ldots, e_T\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} \left(\frac{f(nG)}{p}\right) & \text{ha } nG \notin \mathrm{Supp}(f) \\ -1 & \text{máskülönben.} \end{cases}$$

Chen [3] vizsgálta a konstrukció eloszlás mértékét, illetve lineáris komplexitását. Azonban nyitott probléma maradt, hogy a konstrukció korrelációs mértéke milyen esetekben lesz kicsi. Amint az alábbi példa mutatja, bizonyos görbék esetén, még a legegyszerűbb konstrukció, mikor $f(x, y) = x$, is rossz sorozatot generál:

2. példa. *Tekintsük a következő elliptikus görbét $\mathbb{F}_{19}$ fölött.*

$$y^2 = x^3 - 2x.$$

A görbének 20 pontja van, és a $G = (2, 2)$ pont egy generátor. Legyen $f(x, y) = x$, és tekintsük a 10 konstrukció által definiált sorozatot:

n	nG	e_n	n	nG	e_n
1	(2,2)	-1	11	(18 ,1)	-1
2	(7,14)	+1	12	(16 ,6)	+1
3	(15,1)	-1	13	(10,12)	-1
4	(11,6)	+1	14	(5,18)	+1
5	(13,10)	-1	15	(13,9)	-1
6	(5 ,1)	+1	16	(11,13)	+1
7	(10 ,7)	-1	17	(15,18)	-1
8	(16 ,13)	+1	18	(7,5)	+1
9	(18 ,18)	-1	19	(2,17)	-1
10	(0 ,0)	-1	20	$\mathcal{O}$	-1

A másodrendű korreláció nagy:

$$e_n \cdot e_{n+10} = \left(\frac{f(nG)}{19}\right) \cdot \left(\frac{f((n+10)G)}{19}\right) = \left(\frac{f(nG) \cdot f(nG+10G)}{19}\right)$$
$$= \left(\frac{f(nG) \cdot f(nG+(0,0))}{19}\right) = \left(\frac{x \cdot \left(\left(\frac{y}{x}\right)^2 - x\right)}{19}\right) = 1,$$

ugyanis a $x \cdot \left(\left(\frac{y}{x}\right)^2 - x\right)$ *függvény konstans a görbén.*

A példában szereplő sorozat magas korrelációjának következménye, hogy már az eredeti $f(nG)$ sorozat sem pszeudovéletlen. Ugyanis, ha ismerjük az első felét, akkor tudni fogjuk, hogy a sorozat második felében mikor kapunk olyan pontot, aminek első koordinátája kvadratikus maradék, és mikor nem.

A 4 konstrukcióhoz hasonlóan általánosíthatjuk a 10 konstrukciót:

11. konstrukció. *Legyen* p *prímszám,* $\mathcal{E}$ *elliptikus görbe* $\mathbb{F}_p$ *fölött,* $G \in \mathcal{E}(\mathbb{F}_p)$ T*-ed rendű elem,* $f \in \mathbb{F}_p(\mathcal{E})$*,* χ d *multiplikatív karaktere* $\mathbb{F}_p$*-nek. Ekkor definiáljuk az* $E_T = \{e_1, \ldots, e_T\}$ *sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } nG \notin \operatorname{Supp}(f) \text{ és } \arg\left(\chi(f(nG))\right) \in [0, \pi), \\ -1, & \text{máskülönben.} \end{cases}$$

Hasonlóan a korábbiakhoz, ha χ a Legendre szimbólum, akkor visszakapjuk a 10 konstrukciót, másrészről, ha χ $p-1$-ed rendű karakter, akkor megkapjuk Chen, Li és Xiao diszkrét logaritmuson alapuló konstrukcióját [4].

15. tétel ([M7]). *Legyen* p *prímszám,* χ *olyan* d*-ed rendű multiplikatív karaktere* $\mathbb{F}_p$*-nek, melynek rendje páros,* $\mathcal{E}$ *elliptikus görbe* $\mathbb{F}_p$ *fölött,* $f \in \mathbb{F}_p(\mathcal{E})$ *olyan függvény, mely nem* d*-hatvány* $\overline{\mathbb{F}}_p(\mathcal{E})$*-ben. Ha* G T*-ed rendű pont, és az* $E_T = \{e_1, \ldots, e_T\}$ *sorozatot a 11 konstrukció definiálja, akkor*

$$W(E_T) \leq 4|\operatorname{Supp}(f)|p^{1/2}(1+\log T)\log d + |\operatorname{Supp}(f)|. \tag{5.5}$$

Továbbá, ha f *gyökeinek és pólusainak multiplicitása vagy* d*-vel osztható, vagy ahhoz relatív prím,* $\ell \in \mathbb{N}$ *olyan egész, melyre a* $(|\operatorname{Supp}(f)|, \ell, T)$ *hármas* d*-megengedhető, akkor*

$$C_\ell(E_T) \leq 4^\ell|\operatorname{Supp}(f)|p^{1/2}(1+\log T)(\log d)^\ell + \ell|\operatorname{Supp}(f)|. \tag{5.6}$$

2. megjegyzés.. *Abban az esetben, mikor a karakter rendje páratlan, a következő korlátokat lehet bizonyítani:*

$$W(E_T) \ll_{\ell,f} p^{1/2}\log T \log d + \frac{T}{d}, \quad C_\ell(E_T) \ll_{\ell,f} p^{1/2}\log T(\log d)^\ell + \frac{M}{d^\ell}.$$

Bizonyítás. Legyen g $\mathbb{F}_p$ egy olyan generátora, melyre $\chi(g) = e(1/d)$. Ekkor a 7 lemma alapján

$$e_n = \frac{2}{d} \sum_{\gamma^d=\chi_0}^{*} \frac{1-\bar{\gamma}(g)^{d/2}}{1-\bar{\gamma}(g)} \cdot \gamma(f(nG)).$$

Legyen $a \in \mathbb{Z}$ és $b, t \in \mathbb{N}$ olyan egészek, melyekre

$$1 \le a \le a + (t-1)b \le T, \quad b < T.$$

Ekkor

$$\begin{aligned} |U(E_T, t, a, b)| &= \left| \sum_{j=0}^{t-1} e_{a+jb} \right| \\ &\le \left| \sum_{\substack{0 \le j < t \\ a+jb \in \mathcal{N}}} \frac{2}{d} \sum_{\gamma^d=\chi_0}^{*} \frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)} \cdot \bar{\gamma}(f((a+jb)G)) \right| + |\operatorname{Supp}(f)| \\ &\le \frac{2}{d} \sum_{\gamma^d=\chi_0}^{*} \left| \sum_{\substack{0 \le j < t \\ a+jb \in \mathcal{N}}} \gamma(f((a+jb)G)) \right| \left| \frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)} \right| + |\operatorname{Supp}(f)|. \end{aligned}$$

Mivel f nem d-hatvány, a 9 és 25 lemmák alapján

$$\begin{aligned} \frac{2}{d} \sum_{\gamma^d=\chi_0}^{*} \left| \sum_{\substack{0 \le j < t \\ a+jb \in \mathcal{N}}} \gamma(f((a+jb)G)) \right| \left| \frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)} \right| &\le \\ &\le \frac{2}{d} |\operatorname{Supp}(f)| p^{1/2} (1+\log t) \sum_{\gamma \ne \chi_0} \frac{2}{|1-\gamma(g)|} \\ &\le 2 |\operatorname{Supp}(f)| p^{1/2} (1+\log t) \log d. \end{aligned}$$

Hasonlóan, az (5.6) bizonyításához legyen $M < T$ és $D = (d_1, \dots, d_\ell)$ olyanok,

hogy $0 \le d_1 < \cdots < d_\ell \le T - M$. Ekkor

$$
\begin{aligned}
|V(E_T, M, D)| &= \left| \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_\ell} \right| \le \\
&\le \Bigg| \sum_{\substack{1 \le n \le M: \\ n+d_i \in \mathcal{N} \\ i=1,\dots,\ell}} \frac{2^\ell}{d^\ell} \sum_{\gamma_1^d = \chi_0}^{*} \frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)} \cdot \bar{\gamma_1}(f((n+d_1)G)) \cdots \\
&\qquad\qquad \cdots \sum_{\gamma_\ell^d = \chi_0}^{*} \frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)} \cdot \bar{\gamma_\ell}(f((n+d_\ell)G)) \Bigg| + \ell |\operatorname{Supp}(f)| \\
&\le \frac{2^\ell}{d^\ell} \sum_{\gamma_1^d = \chi_0}^{*} \cdots \sum_{\gamma_\ell^d = \chi_0}^{*} \left| \frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)} \cdots \frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)} \right| \cdot \\
&\qquad\qquad \cdot \left| \sum_{\substack{1 \le n \le M: \\ n+d_i \in \mathcal{N} \\ i=1,\dots,\ell}} \gamma_1(f((n+d_1)G)) \dots \gamma_\ell(f((n+d_\ell)G)) \right| \\
&\quad + \ell |\operatorname{Supp}(f)|.
\end{aligned}
$$

Adott γ_u karakter esetén $(u = 1, \dots, \ell)$ definiáljuk a δ_u egészeket a (3.3)-hoz hasonlóan. így

$$
\begin{aligned}
&\sum_{\substack{1 \le n \le M: \\ n+d_i \in \mathcal{N} \\ i=1,\dots,\ell}} \gamma_1(f((n+d_1)G)) \dots \gamma_\ell(f((n+d_\ell)G)) = \\
&= \sum_{\substack{1 \le n \le M: \\ n+d_i \in \mathcal{N} \\ i=1,\dots,\ell}} \chi\left(f^{\delta_1}((n+d_1)G)) \dots f^{\delta_\ell}((n+d_\ell)G)\right) \\
&= \sum_{\substack{1 \le n \le M: \\ n+d_i \in \mathcal{N} \\ i=1,\dots,\ell}} \chi\left(f^{\delta_1} \circ \tau_{d_1 G}(nG) \dots f^{\delta_\ell} \circ \tau_{d_\ell G}(nG)\right).
\end{aligned}
$$

Legyen $F_{\gamma_1,\dots,\gamma_\ell} = F_{\delta_1,\dots,\delta_\ell} = f^{\delta_1} \circ \tau_{d_1 G} \cdot \ldots \cdot f^{\delta_\ell} \circ \tau_{d_\ell G}$. Ekkor elég megmutatni a következő lemmát:

29. lemma. *A 15 tétel feltételeinek teljesülése esetén a $F_{\delta_1,\dots,\delta_\ell}$ függvény nem d-havány.*

Valóban, a 9 és 25 lemmák alapján

$$
\begin{aligned}
|V(E_T,M,D)| &\le \frac{2^\ell}{d^\ell}\sum_{\gamma_1^d=\chi_0}^{*}\cdots\sum_{\gamma_\ell^d=\chi_0}^{*}\left|\frac{1-\gamma_1(g)^{\frac{d}{2}}}{1-\gamma_1(g)}\cdots\frac{1-\gamma_\ell(g)^{\frac{d}{2}}}{1-\gamma_\ell(g)}\right|\left|\sum_{\substack{1\le n\le M:\\ n+d_i\in\mathcal{N}\\ i=1,\dots,\ell}}\chi\left(F_{\delta_1,\dots,\delta_\ell}\right)\right|+\\
&\quad+\ell|\operatorname{Supp}(f)|\\
&\le \frac{2^\ell}{d^\ell}\ell|\operatorname{Supp}(f)|p^{1/2}(1+\log M)\left(\sum_{\gamma^d=\chi_0}\frac{2}{|1-\gamma(g)|}\right)^\ell\\
&\quad+\ell|\operatorname{Supp}(f)|\\
&\le \frac{2^\ell}{d^\ell}\ell|\operatorname{Supp}(f)|p^{1/2}(1+\log M)(2d\log d)^\ell+\ell|\operatorname{Supp}(f)|\\
&\le 4^\ell|\operatorname{Supp}(f)|p^{1/2}(1+\log M)(\log d)^\ell+\ell|\operatorname{Supp}(f)|.
\end{aligned}
$$

□

Végül a 29 lemma bizonyítása:

Bizonyítás. Megmutatom, hogy az $F_{\delta_1,\dots,\delta_\ell}$ függvény divizorának nem minden együtthatója osztható d-vel. Ha $\mathcal{R}$ egy mellékosztálya $\langle G\rangle$-nek $\mathcal{E}(\overline{\mathbb{F}}_p)$-ban, akkor

$$\mathcal{R}=\{S\oplus aG\mid a=1,\dots,T\}$$

valamely $S\in\mathcal{R}$ esetén. Bontsuk fel f divizorát a mellékosztályoknak megfelelően:

$$\operatorname{Div}_{\mathcal{R}}(f)=\sum_{R\in\mathcal{R}}\operatorname{ord}_R(f)[R],$$

ahol

$$\operatorname{Div}(f)=\sum_{\mathcal{R}}\operatorname{Div}_{\mathcal{R}}(f).$$

Ha $R\in\mathcal{R}$ egy gyöke vagy egy pólusa f-nek, akkor az összes gyöke és pólusa $F_{\delta_1,\dots,\delta_\ell}$-nek $\mathcal{R}$-ben $R\oplus aG\ominus d_iG$ alakú ($a\in\{1,\dots,T\}, i\in\{1,\dots,\ell\}$). Ekkor $F_{\delta_1,\dots,\delta_\ell}$ divizorának $\mathcal{R}$-be eső része

$$
\begin{aligned}
\operatorname{Div}_{\mathcal{R}}(F_{\delta_1,\dots,\delta_\ell})&=\operatorname{Div}_{\mathcal{R}}(f^{\delta_1}\circ\tau_{d_1G}\dots f^{\delta_\ell}\circ\tau_{d_\ell G})=\sum_{R\in\mathcal{R}}\sum_{i=1}^{\ell}\delta_i\operatorname{ord}_R(f)[R\ominus d_iG]\\
&=\sum_{a=1}^{T}\sum_{i=1}^{\ell}\delta_i\operatorname{ord}_{S\oplus aG}(f)[S\oplus aG\ominus d_iG],
\end{aligned}
$$

ahol S $\mathcal{R}$ egy rögzített eleme.

Rögzítsünk most egy $\mathcal{R}$ mellékosztályt, mely tartalmaz f-nek

legalább egy olyan gyökét vagy pólusát, melynek rendje relatív prím d-hez. Legyen $\mathcal{A}$ az a elemekből álló multihalmaz ($a = 1, \ldots, T$), ahol minden elem multiplicitása $\mathrm{ord}_{R \oplus aG}(f)$ modulo d, és legyen $\mathcal{B}$ a $-d_i$ elemek multihalmaza, ahol minden elem multiplicitása δ_i ($i = 1, \ldots, \ell$). $\mathcal{A}$ minden elemének multiplicitása relatív prim d-hez, $\mathcal{A}$ különböző elemeinek száma legfeljebb $|\operatorname{Supp}(f)|$, $\mathcal{B}$ különböző elemeinek száma legfeljebb ℓ, a $(|\operatorname{Supp}(f)|, \ell, T)$ hármas d-megengedhető, így létezik olyan Q elem, mely multiplicitása $\mathcal{A} + \mathcal{B}$-ben nem osztható d-vel. Így ennek az elemnek az együtthatója $F_{\delta_1, \ldots, \delta_\ell}$ divizorában nem osztható d-vel. □

Az eddig használt eszközökkel az (5.4) sorozatnak nem csak a multiplikatív, de az additív tulajdonságait is vizsgálni tudjuk. Másszóval a sorozatot nem csak a 11 konstrukció segítségével tudjuk bináris sorozattá transzformálni, hanem a következő módon is:

12. konstrukció. *Legyen p prímszám, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ fölött, $G \in \mathcal{E}(\mathbb{F}_p)$ T-ed rendű elem, $f \in \mathbb{F}_p(\mathcal{E})$. Ekkor definiáljuk az $E_T = \{e_1, \ldots, e_T\}$ sorozatot a következőképpen:*

$$e_n = \begin{cases} +1, & \text{ha } f(nG) \in \{0, 1, \ldots, \frac{p-1}{2}\}, \\ -1, & \text{máskülönben.} \end{cases}$$

Ezt a konstrukciót először Chen és Xiao vizsgálta abban a speciális esetben, mikor $f(x, y) = x, y, x/2$ vagy $y/2$ [5]. Később Liu, Wang és Zhang [17] kiterjesztette a konstrukciót arra az általánosabb esetre, mikor f polinom (amikor a függvény egyetlen pólusa $\mathcal{O}$), vagy mikor f egy polinom multiplikatív inverze. Azonban mint az alábbi példa mutatja, könnyű olyan egyszerű racionális törtfüggvényeket adni, mikor a konstrukcióval kapott bináris sorozat nem pszeudovéletlen. Így érdemes vizsgálni, hogy a konstrukció mikor terjeszthető ki ily módon és mikor nem.

3. példa. *Tekintsük a 2 példában használt ellipttikus görbét, és legyen megint $G = (2, 2)$ a generátor. Legyen $f(x, y) = 9x + \frac{1}{x}$ és tekintsük a 12 konstrukció által definiált sorozatot:*

n	nG	$f(nG)$	e_n	n	nG	$f(nG)$	e_n
1	(2,2)	9	+1	11	(18 ,1)	9	+1
2	(7,14)	17	-1	12	(16 ,6)	17	-1
3	(15,1)	16	-1	13	(10,12)	16	-1
4	(11,6)	11	-1	14	(5,18)	11	-1
5	(13,10)	6	+1	15	(13,9)	6	+1
6	(5 ,1)	11	-1	16	(11,13)	11	-1
7	(10 ,7)	16	-1	17	(15,18)	16	-1
8	(16 ,13)	17	-1	18	(7,5)	17	-1
9	(18 ,18)	9	+1	19	(2,17)	9	+1
10	(0 ,0)	∞	-1	20	$\mathcal{O}$	∞	-1

Amint látszik, $e_n = e_{n+10}$, azaz a $C_2(E_{20})$ másodrendű korreláció nagy.

16. tétel ([M8]). *Legyen $p > 3$ prímszám, $G \in \mathcal{E}(\mathbb{F}_p)$ T-ed rendű elem, $f \in \mathbb{F}_p(\mathcal{E})$ nem konstans függvény. Ha az $E_T = \{e_1, \dots, e_T\}$ sorozatot a 12 konstrukció definiálja, akkor*

$$W(E_T) << \deg f \, p^{1/2} \log p \log T.$$

Ha feltesszük továbbá, hogy

(i) $\deg f < p(T)$ *és* $\ell = 2$;

(ii) $\deg f < p(T)$ *és* $(4 \deg f)^\ell < p(T)$,

ahol $p(T)$ a T legkisebb primosztója, akkor

$$C_\ell(E_T) << \ell \deg f p^{1/2} (\log p)^\ell \log T.$$

Bizonyítás. Legyen

$$\mathcal{N} = \{n : 1 \le n \le T : f(nG) = \infty\},$$

és tekintsünk $a, b, t \in \mathbb{N}$ olyan egészeket, melyekre

$$1 \le a \le a + (t-1)b \le T, \quad b < T. \tag{5.7}$$

A 8 lemma alapján

$$U(E_T, t, a, b) = \sum_{j=0}^{t-1} e_{a+jb} =$$

$$= \frac{1}{p} \sum_{|h|<p/2} v_p(h) \sum_{\substack{0 \le j \le t-1 \\ a+jb \notin \mathcal{N}}} e_p\left(hf((a+jb)G)\right) + \mathcal{O}\left(\sum_{\substack{0 \le j \le T \\ a+jb \in \mathcal{N}}} 1 \right). \tag{5.8}$$

Ha $h \neq 0$, akkor alkalmazhatjuk a 26 lemmát:

$$|U(E_T, a, b, t)| \ll |v_p(0)| + \frac{1}{p} \sum_{1<|h|<p/2} |v_p(h)| \deg f p^{1/2} \log T + \deg f. \tag{5.9}$$

Mivel

$$|v_p(h)| \ll \frac{p}{h}$$

minden $h \neq 0$ esetén, így

$$|U(E_T, a, b, t)| \ll \deg f p^{1/2} \log T \sum_{1<|h|<p/2} \frac{1}{h} + \deg f \ll \deg f p^{1/2} \log p \log T.$$

A második rész bizonyításához legyen $D = (d_1, d_2, \ldots, d_\ell)$ és M olyanok, hogy $0 \leq d_1 < d_2 < \cdots < d_\ell \leq p - M$. Ekkor szintén a 8 lemma alapján

$$\begin{aligned} V(E_T, M, D) &= \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_\ell} = \\ &= \frac{1}{p^\ell} \sum_{\substack{1 \leq n \leq M \\ n+d_1, \ldots, n+d_\ell \notin \mathcal{N}}} \prod_{i=1}^{\ell} \sum_{|h_i|<p/2} v_p(h_i) e_p\left(h_i f((n+d_i)G)\right) + \\ &\quad + \mathcal{O}\left(\sum_{\substack{1 \leq n \leq M \\ n+d_1 \in \mathcal{N}}} 1 + \cdots + \sum_{\substack{1 \leq n \leq M \\ n+d_\ell \in \mathcal{N}}} 1 \right). \end{aligned}$$

A $h_1 = \cdots = h_\ell = 0$ főtagot leválasztva

$$\begin{aligned} V(E_T, M, D) &= \frac{1}{p^\ell}(M + \mathcal{O}(\ell \deg f)) + \\ &\quad + \frac{1}{p^\ell} \sum_{\substack{|h_1|<p/2 \\ (h_1,\ldots,h_\ell) \neq (0,\ldots,0)}} \cdots \sum_{|h_\ell|<p/2} v_p(h_1) \ldots v_p(h_\ell) \cdot \\ &\quad \cdot \sum_{\substack{1 \leq n \leq M \\ n+d_1, \ldots, n+d_\ell \notin \mathcal{N}}} e_p\left(h_1 f((n+d_1)G) + \cdots + h_\ell f((n+d_\ell)G)\right) + \\ &\quad + \mathcal{O}(\ell \deg f) \\ &= \frac{1}{p^\ell} \sum_{\substack{|h_1|<p/2 \\ (h_1,\ldots,h_\ell) \neq (0,\ldots,0)}} \cdots \sum_{|h_\ell|<p/2} v_p(h_1) \ldots v_p(h_\ell) \cdot \\ &\quad \cdot \sum_{\substack{1 \leq n \leq M \\ n+d_1, \ldots, n+d_\ell \notin \mathcal{N}}} e_p\left(h_1 f((n+d_1)G) + \cdots + h_\ell f((n+d_\ell)G)\right) + \\ &\quad + \mathcal{O}(\ell \deg f). \end{aligned} \tag{5.10}$$

Tekintsük most a legbelső tagot, és jelöljék a nem nulla h_i együtthatókat a $h_{i_1} \leq \dots \leq h_{i_r}$ számok. Ekkor

$$\begin{aligned}
&\sum_{\substack{1\leq n\leq M\\ n+d_1,\dots,n+d_\ell\notin\mathcal{N}}} e_p\left(h_1 f((n+d_1)G)+\dots+h_\ell f((n+d_\ell)G)\right)\\
&=\sum_{\substack{1\leq n\leq M\\ n+d_1,\dots,n+d_\ell\notin\mathcal{N}}} e_p\left(h_{i_1} f((n+d_{i_1})G)+\dots+h_{i_r} f((n+d_{i_r})G)\right)\\
&=\sum_{\substack{1\leq n\leq M\\ n+d_{i_1},\dots,n+d_{i_r}\notin\mathcal{N}}} e_p\left(h_{i_1} f((n+d_{i_1})G)+\dots+h_{i_r} f((n+d_{i_r})G)\right)+\mathcal{O}\left(\ell\deg f\right).
\end{aligned}$$

Legyen $F_{h_1,\dots,h_\ell}=h_{i_1}f\circ\tau_{d_{i_1}G}+\dots+h_{i_r}f\circ\tau_{d_{i_r}G}$. Ekkor ez nem konstans függvény:

30. lemma. *Ha a 16 tétel feltételei teljesülnek, és $(h_1,\dots,h_\ell)\neq(0,\dots,0)$, akkor az $F_{h_1,\dots,h_\ell}$ függvény nem konstans.*

A lemma alapján az előző összeg becsülhető a 26 lemma segítségével:

$$\begin{aligned}
&\sum_{\substack{1\leq n\leq M\\ n+d_1,\dots,n+d_\ell\notin\mathcal{N}}} e_p\left(h_1 f((n+d_1)G)+\dots+h_\ell f((n+d_\ell)G)\right)\\
&\leq \deg F_{h_1,\dots,h_\ell}p^{1/2}\log T+\mathcal{O}\left(\ell\deg f\right)\\
&\ll \ell\deg f p^{1/2}\log T.
\end{aligned}\tag{5.11}$$

A 8 lemma, és az (5.10), (5.11) alapján

$$\begin{aligned}
V(E_T,M,D)&\ll\frac{1}{p^\ell}\sum_{\substack{|h_1|<p/2\\(h_1,\dots,h_\ell)\neq(0,\dots,0)}}\dots\sum_{|h_\ell|<p/2}|v_p(h_1)|\dots|v_p(h_\ell)|\ell\deg f p^{1/2}\log T\\
&\quad+\mathcal{O}\left(\ell\deg f\right)\\
&\leq \ell\deg f p^{1/2-\ell}\log T\left(\sum_{|h|<p/2}|v_p(h)|\right)^\ell+(\ell\deg f)\\
&\ll \ell\deg f p^{1/2-\ell}\log T\left(1+\sum_{0<|h|<p/2}\frac{p}{h}\right)^\ell+(\ell\deg f)\\
&\ll \ell\deg f p^{1/2}\log T(\log p)^\ell.
\end{aligned}$$

□

Végül bebizonyítom a 30 lemmát:

Bizonyítás. Megmutatom, hogy az $F_{h_1,\dots,h_\ell}$ függvénynek legalább egy pólusa van.

A 29 lemmához hasonlóan tekintsük $\langle G\rangle$ mellékosztályait $\mathcal{E}(\overline{\mathbb{F}}_p)$-ban.

Legyen $\mathcal{R} = \{S + aG : \ a = 1, \dots, T\}$ egy olyan mellékosztály, mely tartalmazza f legalább egy pólusát, és legyen $\mathcal{A}$ azon a elemek halmaza, melyre $S \oplus aG$ pólusa f-nek, és legyen $\mathcal{B}$ a $-d_{i_j}$ számok halmaza. $S \oplus aG \ominus d_{i_j}G$ ($a \in \mathcal{A}$, $-d_{i_j} \in \mathcal{B}$) az $F_{h_1,\dots,h_\ell}$ összes $\mathcal{R}$-be eső pólusa. Másrészről

$$|\mathcal{A}| \le \deg f \quad \text{és} \quad |\mathcal{B}| = r \le \ell,$$

így a 16 következmény miatt létezik olyan c, melynek pontosan egy előállítása van a

$$a - d_{i_j} = c, \quad a \in \mathcal{A}, -d_{i_j} \in \mathcal{B}.$$

formában. Ezen a és d_{i_j} számokra $S \oplus aG$ pólusa $h_{i_j} f \circ \tau_{d_{i_j}G}$-nek, de nem a $h_{i_l} f \circ \tau_{d_{i_l}G}$ ($j \neq l$) tényezőknek, így ez valóban pólusa $F_{h_1,\dots,h_\ell}$-nek. □

5.3. Pszeudovéletlen rácsok elliptikus görbék felett

Ebben a részben a 11 konstrukció többdimenziós változatát vizsgálom.

13. konstrukció. *Legyen p prímszám, χ multiplikatív karaktere $\mathbb{F}_p$-nek, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ fölött, $f \in \mathbb{F}_p(\mathcal{E})$ és $P_1, \dots, P_n \in \mathcal{E}(\mathbb{F}_p)$ olyan gyengén független pontok, melyek rendje nem nagyobb N-nél. Ekkor definiáljuk a $\eta : I_N^n \to \{-1, +1\}$ rácsot a következő módon:*

$$\eta(x_1, \dots, x_n) = \begin{cases} +1 & \text{ha } x_1P_1 \oplus \dots \oplus x_nP_n \notin \operatorname{Supp}(f) \\ & \quad \text{és } \arg\left(\chi(f(x_1P_1 \oplus \dots \oplus x_nP_n))\right) \in [0, \pi), \\ -1 & \text{máskülönben.} \end{cases}$$

17. tétel ([M6]). *Legyen $p > 3$ prímszám, χ d-ed rendű multiplikatív karaktere $\mathbb{F}_p$-nek, melynek rendje páros, $\mathcal{E}$ elliptikus görbe $\mathbb{F}_p$ fölött. Legyen továbbá $f \in \mathbb{F}_p(\mathcal{E})$, mely nem d-hatvány $\overline{\mathbb{F}}_p(\mathcal{E})$-ben, és az f gyökeinek és pólusainak rendje vagy osztható d-vel, vagy d-hez relatív prím. Legyenek $N \in \mathbb{N}$, $P_1, \dots, P_n \in \mathcal{E}(\mathbb{F}_p)$ olyan gyengén független pontok, melyek rendje nem nagyobb N-nél. Ha az $\eta : I_N^n \to \{-1, +1\}$ rácsot a 13 konstrukció definiálja, és a $(|\operatorname{Supp}(f)|, \ell, \mathcal{E}(\mathbb{F}_p))$ hármas megengedhető, akkor*

$$Q_\ell(\eta) \le 2 \cdot 3^n (2d)^\ell \ell d \deg(f) p^{1/2} (\log |\mathcal{E}(\mathbb{F}_p)|)^n (\log d)^\ell + \ell |\operatorname{Supp}(f)|.$$

3. megjegyzés.. *Ha a karakter rendje páros, akkor a Q_ℓ mértékre a következő korlát adható:*

$$Q_\ell(\eta) \ll_{n,\ell} d \deg(f) p^{1/2} (\log |\mathcal{E}(\mathbb{F}_p)|)^n (\log d)^\ell + \frac{|\mathcal{E}(\mathbb{F}_p)|}{d^\ell}$$

Bizonyítás. A tétel bizonyításához legyenek $\mathbf{u}_i$ $(i = 1, \dots, n)$ az n dimenziós egységvektorok, $b_1, \dots, b_n \in \mathbb{F}_p^*$, $\mathbf{d}_1, \dots, \mathbf{d}_\ell \in \mathbb{F}_p^n$ nem nulla vektorok, és $t_1, \dots, t_\ell$ olyan pozitív egészek, melyekre

$$B = \{\mathbf{x} = j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n : 0 \le j_i \le t_i,\ i = 1, \dots, n\}$$

esetén

$$B + \mathbf{d}_1, \dots, B + \mathbf{d}_\ell \subseteq I_N^n.$$

Legyen $\mathbf{d}_i = (d_1^{(i)}, \dots, d_n^{(i)})$ és

$$\mathcal{N} = \{\mathbf{x} = (x_1, \dots, x_n) : x_1 P_1 \oplus \cdots \oplus x_n P_n \in \mathrm{Supp}(f)\}$$

A 7 lemma alapján $\mathbf{x} \notin \mathcal{N}$ esetén

$$\eta(\mathbf{x}) = \frac{2}{d} \sum_{\substack{\gamma^d = \chi_0 \\ \gamma \neq \chi_0}} \frac{1 - \gamma(g)^{\frac{d}{2}}}{1 - \gamma(g)} \cdot \bar{\gamma}(f(x_1 P_1 \oplus \cdots \oplus x_n P_n)).$$

Legyen

$$\Omega(\eta, B, \mathbf{d}_1, \dots, \mathbf{d}_\ell) = \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d}_1) \cdots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|,$$

Ekkor ha $j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_i \notin \mathcal{N}$ $(i = 1, \dots, n)$, akkor az általános tag az összegben a következő módon írható:

$$\begin{aligned}
&\eta(j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_1) \cdots \eta(j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_\ell) = \\
&= \eta\big((j_1 b_1 + d_1^{(1)}, \dots, j_n b_n + d_n^{(1)})\big) \cdots \eta\big((j_1 b_1 + d_1^{(\ell)}, \dots, j_n b_n + d_n^{(\ell)})\big) \\
&= \left(\frac{2}{d}\right)^\ell \prod_{i=1}^{\ell} \sum_{\gamma_i^d = \chi_0}^{*} \frac{1 - \gamma_i(g)^{\frac{d}{2}}}{1 - \gamma_i(g)} \cdot \bar{\gamma}_i\Big(f\big((j_1 b_1 + d_1^{(i)}) P_1 \oplus \cdots \oplus (j_n b_n + d_n^{(i)}) P_n\big)\Big).
\end{aligned}$$

Így megkapjuk, hogy

$$
\begin{aligned}
&\Omega(\eta, B, \mathbf{d}_1, \dots, \mathbf{d}_\ell) = \\
&\le \Bigg| \sum_{\substack{j_1 b_1 \mathbf{u}_1 + \dots + j_n b_n \mathbf{u}_n + \mathbf{d}_i \notin \mathcal{N} \\ i=1,\dots,\ell}}^{t_1} \cdots \sum_{j_n=0}^{t_n} \left(\frac{2}{d}\right)^\ell \prod_{i=1}^{\ell} \\
&\qquad \sum_{\gamma_i^d = \chi_0}^{*} \frac{1-\gamma_i(g)^{\frac{d}{2}}}{1-\gamma_i(g)} \cdot \bar{\gamma_i}\Big(f\big((j_1 b_1 + d_1^{(i)})P_1 \oplus \dots \oplus (j_n b_n + d_n^{(i)})P_n\big)\Big) \Bigg| \\
&\qquad + \ell |\operatorname{Supp}(f)| \\
&\le \left(\frac{2}{d}\right)^\ell \sum_{\gamma_1^d = \chi_0}^{*} \cdots \sum_{\gamma_\ell^d = \chi_0}^{*} \prod_{i=1}^{\ell} \left| \frac{1-\gamma_i(g)^{\frac{d}{2}}}{1-\gamma_i(g)} \right| \cdot \\
&\qquad \cdot \Bigg| \sum_{\substack{j_1 b_1 \mathbf{u}_1 + \dots + j_n b_n \mathbf{u}_n + \mathbf{d}_i \notin \mathcal{N} \\ i=1,\dots,\ell}}^{t_1} \cdots \sum_{j_n=0}^{t_n} \prod_{i=1}^{\ell} \gamma_i\big(f\big((j_1 b_1 + d_1^{(i)})P_1 \oplus \dots \oplus (j_n b_n + d_n^{(i)})P_n\big)\big) \Bigg| \\
&\qquad + \ell |\operatorname{Supp}(f)|.
\end{aligned}
\tag{5.12}
$$

Definiáljuk a δ_i számokat a 3.3-hoz hasonló módon. Ekkor

$$
\begin{aligned}
&\prod_{i=1}^{\ell} \gamma_i\big(f\big((j_1 b_1 + d_1^{(i)})P_1 \oplus \dots \oplus (j_n b_n + d_n^{(i)})P_n\big)\big) \\
&= \prod_{i=1}^{\ell} \chi^{\delta_i}\big(f\big((j_1 b_1 + d_1^{(i)})P_1 \oplus \dots \oplus (j_n b_n + d_n^{(i)})P_n\big)\big) \\
&= \chi\left(\prod_{i=1}^{\ell} f^{\delta_i}\big((j_1 b_1 + d_1^{(i)})P_1 \oplus \dots \oplus (j_n b_n + d_n^{(i)})P_n\big)\right).
\end{aligned}
$$

Legyen most $Q = j_1 b_1 P_1 \oplus \dots \oplus j_n b_n P_n$ az általános pont, ami a $B' = \{i_1(b_1 P_1) \oplus \dots \oplus i_n(j_n P_n) : i_1 \le t_1, \dots, i_n \le t_n\}$ halmazon fut végig. Mivel

$$
b_\nu \le t_\nu b_\nu \le N \le |P_\nu|,
$$

így a $(b_1 P_1), \dots, (b_n P_n)$ pontok szintén gyengén függetlenek, ezért az (5.12)-beli abszolútérték a következőképpen írható:

$$
\begin{aligned}
&\left| \sum_{Q \in B'}^{*} \chi\left(\prod_{i=1}^{\ell} f^{\delta_i}(Q \oplus d_1^{(i)} P_1 \oplus \dots \oplus d_n^{(i)} P_n)\right) \right| \\
&= \left| \sum_{Q \in B'}^{*} \chi\left(\prod_{i=1}^{\ell} \left(f \circ \tau_{d_1^{(i)} P_1 \oplus \dots \oplus d_n^{(i)} P_n}\right)^{\delta_i}(Q)\right) \right|,
\end{aligned}
$$

ahol az összeg minden olyan $Q \in B'$ elemre vétetik, melyre $Q \oplus d_1^{(i)} P_1 \cdots \oplus d_n^{(i)} P_n \notin \mathrm{Supp}(f)$. Legyen $F_{\gamma_1,\ldots,\gamma_\ell} = F_{\delta_1,\ldots,\delta_\ell} = \prod_{i=1}^{\ell} \left(f \circ \tau_{d_1^{(i)} P_1 \oplus \cdots \oplus d_n^{(i)} P_n} \right)^{\delta_i}$. Ekkor az (5.12) a következőképpen írható:

$$\left(\frac{2}{d}\right)^{\ell} \sum_{\gamma_1^d=\chi_0}^{*} \cdots \sum_{\gamma_\ell^d=\chi_0}^{*} \prod_{i=1}^{\ell} \left| \frac{1-\gamma_i(g)^{\frac{d}{2}}}{1-\gamma_i(g)} \right| \left| \sum_{Q \in B'}^{*} \chi\left(F_{\gamma_1,\ldots,\gamma_\ell}(Q)\right) \right| + \ell |\,\mathrm{Supp}(f)|. \tag{5.13}$$

A következő lemma miatt a fenti kifejezésben szereplő karakterösszeg nem triviális:

31. lemma. *Ha f, ℓ, és χ kielégíti a 11 tétel feltételeit, és ha nem minden δ_i nulla, akkor az $F_{\gamma_1,\ldots,\gamma_\ell}$ nem d-hatvány.*

A lemma segítségével a következőképpen fejezhetjük be a bizonyítást:

$$\begin{aligned}
&\left(\frac{2}{d}\right)^{\ell} \sum_{\gamma_1^d=\chi_0}^{*} \cdots \sum_{\gamma_\ell^d=\chi_0}^{*} \prod_{i=1}^{\ell} \left| \frac{1-\gamma_i(g)^{\frac{d}{2}}}{1-\gamma_i(g)} \right| \left| \sum_{Q \in B'}^{*} \chi\left(F_{\gamma_1,\ldots,\gamma_\ell}(Q)\right) \right| \\
&\leq 2 \cdot 3^n \deg(F_{\gamma_1,\ldots,\gamma_\ell}) p^{1/2} (\log |\mathcal{E}(\mathbb{F}_p)|)^n \sum_{\gamma_1^d=\chi_0}^{*} \cdots \sum_{\gamma_\ell^d=\chi_0}^{*} \prod_{i=1}^{\ell} \left| \frac{1-\gamma_i(g)^{\frac{d}{2}}}{1-\gamma_i(g)} \right| \qquad (5.14) \\
&\leq 2 \cdot 3^n \ell d \deg(f) p^{1/2} (\log |\mathcal{E}(\mathbb{F}_p)|)^n \left(\sum_{\gamma^d=\chi_0}^{*} \left| \frac{1-\gamma_i(g)^{\frac{d}{2}}}{1-\gamma_i(g)} \right| \right)^{\ell},
\end{aligned}$$

ahol

$$\left(\sum_{\gamma^d=\chi_0}^{*} \left| \frac{1-\gamma(g)^{\frac{d}{2}}}{1-\gamma(g)} \right| \right)^{\ell} = \left(\sum_{\gamma^d=\chi_0}^{*} \frac{2}{|1-\gamma(g)|} \right)^{\ell} \leq (2d \log d)^{\ell}, \tag{5.15}$$

Az (5.13), (5.14) és (5.15)-ból következik, hogy

$$\Omega(\eta, B, \mathbf{d}_1, \ldots, \mathbf{d}_\ell) \leq 2 \cdot (2d)^{\ell} 3^n \ell d \deg(f) p^{1/2} (\log |\mathcal{E}(\mathbb{F}_p)|)^n (\log d)^{\ell} + \ell |\,\mathrm{Supp}(f)|.$$

□

Végül a 31 lemma bizonyítása:

Bizonyítás. A bizonyítás lényegében megegyezik a 29 lemma bizonyításával, azzal a különbséggel, hogy nem a $\langle G \rangle$, hanem a $\langle P_1, \ldots, P_n \rangle$ mellékosztályai szerint kell felbontani a függvények divizorát. □

Irodalomjegyzék

[M1] L. Mérai, Construction of large families of pseudorandom binary sequences, The Ramanujan Journal 18 (2009), 341–349.

[M2] L. Mérai, A construction of pseudorandom binary sequences using rational functions, Unif. Distrib. Theory, 4 (2009), no. 1, 35–49.

[M3] L. Mérai, A construction of pseudorandom binary sequences using both additive and multiplicative characters, Acta Arith. 139 (2009), 241–252.

[M4] L. Mérai, Construction of pseudorandom binary lattices based on multiplicative characters, Periodica Math. Hungar. 59 (2009) 43–51.

[M5] L. Mérai, On finite pseudorandom lattices of k symbols, Monatsh. Math. 161 (2010), no. 2, 173–191.

[M6] L. Mérai, Construction of pseudorandom binary lattices using elliptic curves, Proc. Amer. Math. Soc. 139 (2011), 407-420

[M7] L. Mérai, Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters, beküldve

[M8] L. Mérai, Construction of pseudorandom binary sequences over elliptic curves, beküldve

Irodalomjegyzék

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, Measures of pseudorandomness for finite sequences: typical values, Proc. Lond. Math. Soc. (3) 95 (2007) no. 3, 778–812.

[2] J. Cassaigne, C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences VII: The measures of pseudorandomness, Acta Arith.103 (2002), 97-118.

[3] Z. Chen, Elliptic curve analogue of Legendre sequences, Monatsh. Math. 154 (2008) no. 1, 1–10.

[4] Z. Chen, S. Li, G. Xiao, G. Construction of pseudorandom binary sequences from elliptic curves by using discrete logarithm, Lecture Notes in Comput. Sci., 4086, Springer, Berlin, (2006) 285-294.

[5] Z. Chen, G. Xiao, 'Good' Pseudo-random binary sequences from elliptic curves. Cryptology ePrint Archive, Report 2007/275, http://eprint.iacr.org/

[6] T. Cochrane, *On a trigonometric inequality of Vinogradov*, J. Number Theory 27 (1987), 9–16.

[7] J. Eichauer-Herrmann and H. Niederreiter, *Bounds for exponential sums and their applications to pseudorandom numbers*, Acta Arith. 67 (1994), 269–281.

[8] A. Enge: Elliptic Curves and Their Application to Cryptography: an introduction. Kluwer Academic Publisher, Dordrecht 1999.

[9] L. Goubin, C. Mauduit, and A. Sárközy, Construction of large families of pseudorandom binary sequences, J. Number Theory 106 (2004), 56–69.

[10] K. Gyarmati, On a family of pseudorandom binary sequences, Periodica Math. Hungar. 49 (2004) 45-63.

[11] K. Gyarmati; C. Mauduit; A. Sárközy: Constructions of pseudorandom binary lattices. Unif. Distrib. Theory 4 (2009), no. 2, 59–80.

[12] K. Gyarmati; A. Sárközy; C. L. Stewart: On Legendre symbol lattices. Unif. Distrib. Theory 4 (2009), no. 1, 81–95.

[13] S. Hallgren, Linear congruential generators over elliptic curves, Tech. Report CS-94-143, Carnegie Mellon Unv., 1994.

[14] P. Hubert, C. Mauduit and A. Sárközy, On pseudorandom binary lattices, *Acta Arith.* **125** (2006), 51–62.

[15] D. Kohel and I. E. Shparlinski: On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields. Proc Algorithmic Number Theory Symposium, Leiden. 2000. *Lecture Notes in Comput. Sci.*, 1838. Springer-Verlag, Berlin Heidelberg New York (2000), pp. 395–404.

[16] R. Lidl and H. Niederreiter, Finite Fields, second ed., Cambridge University Press, 1997.

[17] H. Liu, T. Zhan, X. Wang, Large families of elliptic curve pseudorandom binary sequences, Acta Arith. **140** (2009), 135–144

[18] C. Mauduit, J. Rivat and A. Sárközy, *Construction of pseudorandom binary sequence using additive characters*, Monatshefte Math. 141 (2004), 197–208

[19] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol, Acta Arith. 82 (1997), 365–377.

[20] C. Mauduit, A. Sárközy, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239–252.

[21] C. Mauduit, A. Sárközy, On large families of pseudorandom binary lattices, *Unif. Distrib. Theory* **2** (2007), no. 1, 23–37.

[22] C. Mauduit; A. Sárközy: Construction of pseudorandom binary lattices by using the multiplicative inverse. Monatsh. Math. 153 (2008), no. 3, 217–231.

[23] Massey, J. 1969. Shift-Register Synthesis and BCH Decoding. IEEE Transactions on Information Theory. IT-15(1): 122-127.

[24] S. M. Oon, *Construction des suites binaires pseudo-aléatories*, PhD dolgozat, Nancy, 2005.

[25] S. M. Oon, *On pseudo-random properties of certain Dirichlet series*, Ramanujan J. 15 (2008), no. 1, 19–30

[26] G. I. Perel'muter, *On certain character sums*, Uspehi Mat. Nauk 18 no. 2 110 (1963) 145–149.

[27] A. Sárközy, A finite pseudorandom binary sequence, Studia Sci. Math. Hungar. 38 (2001), 377-384.

[28] A. Winterhof, Some estimates for character sums and applications, *Des. Codes Crytogr.* **22** (2001), 123–131.

Összefoglaló

Véletlen elemek generálása több alkalmazásban is központi szerepet játszik, különösen a kriptográfiában és a numerikus analízisben.

1997-ben Mauduit és Sárközy pszeudovéletlenség új mértékeit vezette be, hogy *véges* sorozatok pszeudovéletlen tulajdonságát vizsgálhassák kvantitatív módon [19]. Megközelítésük szerint, ha egy sorozatot pszeudovéletlennek akarunk tekintetni, akkor a sorozat mértékeinek hasonló módon kell viselkedniük, mint a valódi véletlen sorozat mértékeinek.

Később több sorozatot is teszteltek a pszeudovéletlenségi mértékekkel, mint például a Legendre szimbólum által generált sorozatot [9, 19], a diszkrét logaritmuson alapuló sorozatot [10, 27], vagy például polinomoknak, illetve polinomok multiplikatív inverzének maradékaival generált sorozatot [18, 20].

Kiderült azonban, hogy az eddig vizsgált sorozatok pszeudovéletlensége, mind a

$$n \mapsto \psi(F(n))\chi(G(n)),$$

függvény erős pszeudovéletlen tulajdonságain alapulnak, ahol ψ additív, χ multiplikatív karaktere $\mathbb{F}_p$-nek, $F, Q \in \mathbb{F}_p(x)$ pedig racionális törtfüggvények.

A 3. fejezetben ezt az általános konstrukciót tanulmányozom, megkülönböztetve azt az esetet, mikor a χ multiplikatív karakter rendje páros, és az F függvény konstans, és azt az esetet, mikor az F függvény tetszőleges.

A 4. fejezetben kiterjesztem a konstrukciót több dimenzióra, és megmutatom, hogy az így definiált bináris rács erős pszeudovéletlen tulajdonságokkal rendelkezik.

Végül az 5. fejezetben tanulmányozom a fenti konstrukciók elliptikus görbék felett definiált megfelelőit. Az 5.2. részben definiálom az általános sorozat-konstrukciót kiterjesztve Chen [3], Chen, Li és Xiao [4] végül Liu, Wang és Zhan [17] konstrukcióját. Az 5.3. részben megmutatom hogyan lehet jó pszeudovéletlen rácsot definiálni elliptikus görbék segítségével.

Megjegyzem végül, hogy a felhasznált eszközöket a 2. fejezetben és az 5.1. részben foglalom össze.

Summary

Pseudorandom sequences play a crucial role in many areas such as cryptography and communication systems. There are many definitions to pseudorandomness depending on specific application. In order to study the pseudorandomness of *finite* binary sequences, Mauduit and Sárközy introduced several measures of pseudorandomness in [19]. The sequences can be considered as pseudorandom, if its measures behave as the measures of a real random sequence.

Later several sequences have been tested with this measures, such as the Legendre symbol sequences [9, 19], sequences based on the notion of discrete logarithm [10, 27], or on residues of polynomial or the multiplicative inverse of a polynomial [18, 20].

However, it turns out that the pseudorandomness of each sequences based on the pseudorandom behavior of the following function:

$$n \mapsto \psi(F(n))\chi(G(n)),$$

where ψ is additive, χ is multiplicative character of $\mathbb{F}_p$, $F, Q \in \mathbb{F}_p(x)$ are rational functions.

In Chapter 3, I study this general construction distinguishing the case, when the function F is constant and the order of the multiplicative character is even, and the case, when the function F is not a constant function.

In Chapter 4, I extend the general construction to several dimension defining pseudorandom binary lattice, following the approach developed by Hubert, Mauduit and Sárközy [14].

Finally, in Chapter 5, I study the application of elliptic curves to generate pseudorandom binary sequences and lattices. In Section 5.2, I define the general construction of pseudorandom sequences, extend the construction of Chen [3], Chen, Li and Xiao [4] and Liu, Wang and Zhan [17]. In Section 5.3, I define a construction of pseudorandom binary lattice over elliptic curve.

Finally, I remark that I summarize the used tool in Chapter 2 and Section 5.1.