EÖTVÖS LORÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR

Becslések pszeudovéletlen sorozatok kombinált mértékére

SZAKDOLGOZAT

Gologi Sarolta
Matematika BSc, elemző szakirány

Témavezető

Dr. Gyarmati Katalin
egyetemi docens

2021

NYILATKOZAT

Név: Gologi Sarolta

ELTE Természettudományi Kar, szak: matematika BSc

NEPTUN azonosító: E94FT0

Szakdolgozat címe:
Becslések pszeudovéletlen sorozatok kombinált mértékére

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2021.05.18

Gológi Sarolta

a hallgató aláírása

Tartalomjegyzék

1. Köszönetnyilvánítás **3**

2. Bevezetés **4**

3. Bináris sorozatok pszeudovéletlenségének mérése **5**

4. A Legendre szimbólum pszeudovéletlensége **8**

5. A Legendre szimbólumhoz kapcsolódó további konstrukció **9**

6. Elfogadhatóság, "jó" prímek **15**

7. Következmények, algoritmus **15**

8. Karakterösszeg becslések a pq modulusra **18**

8.1. Multiplikatív karakterösszeg becslések 18

8.2. Additív karakterösszeg becslések 20

9. A Legendre szimbólum konstrukciójának kiterjesztése a Jacobi szimbólumra **23**

9.1. A (13) konstrukció kiterjesztése 30

9.2. A (15) konstrukció kiterjesztése 31

10. Saját programok eredményei adott mértékekre **33**

10.1. Eredmények (1) konstrukcióval 34

10.2. Eredmények (3) konstrukcióval 37

1. Köszönetnyilvánítás

Ezúton köszönöm témavezetőmnek, Dr. Gyarmati Katalinnak a szakdolgozat megírásához adott iránymutatását, illetve a szakirodalmak rendelkezésemre bocsátását.

2. Bevezetés

Számos cikk jelent meg a pszeudovéletlen sorozatokról, melyek célok, megközelítések és eszközök széles skáláját mutatják be és melyek még a pszeudovéletlenséget is különbözőképpen értelmezik. Ezek többségében matematikusok a pszeudovéletlen sorozatok konstrukcióit adják meg és/vagy tesztelik a pszeudovéletlenség szempontjából. Több másik, a kriptográfia által inspirált cikkben, a matematikai logika módszereit, a valószínűségi elméletet és a kombinatorikát használják fel a pszeudovéletlenség vizsgálatára (például [1], [2], [3]).

A pszeudovéletlen sorozat fogalma három különböző módon értelmezhető:

1. $[0,1)$ sorozatok,

2. az $1,\ldots,N$ halmazból vett egészek pszeudovéletlen sorozatai,

3. pszeudovéletlen bináris, vagy általánosabban, b-edrendű sorozatok.

Knuth [4] nem tesz éles különbséget e három koncepció között, hiszen szorosan összefüggenek. Ennek ellenére vannak bizonyos eltérések; a különböző pszeudovéletlenségi fogalmak tanulmányozása különböző megközelítéseket és konstrukciós elveket inspirálhat.

Christian Mauduit és Sárközy András [5] a konstrukciók elemzése, összehasonlítása valamint a korábbi módszerek bizonyos hiányosságainak kiküszöbölése érdekében a pszeudovéletlenség új mértékét (vagy mértékeit) vezették be. Céljuk volt minél jobb konstrukciók keresése, olyanoké, melyek legalább bizonyos speciális esetekben jobbak az előzőeknél. A legtöbb konstrukciójuk esetén sikerrel jártak, mind közül a Goubin-Mauduit-Sárközy [6] cikkében megadott bizonyult a legjobbnak, amelyet az **5.** fejezetben ismertetek. Emellett a számelméletben és a matematika más területein fontos szerepet játszó speciális bináris sorozatok véletlenszerű tulajdonságairól is új információkat gyűjtöttek.

3. Bináris sorozatok pszeudovéletlenségének mérése

Az elvárás az, hogy ez a mérték tükrözze a legfontosabb és intenzíven tanulmányozott véletlenszerű tulajdonságokat, mint például

1. normailtás;
2. a számtani progressziókhoz viszonyított jó eloszlás;
3. kis többszörösű összefüggések.

Mauduit és Sárközy [5] az $E = (e_1, e_2, \ldots) \in \{-1,1\}^\infty$ végtelen bináris sorozatok esetében ezeket a véletlen tulajdonságokat a következő módon definiálják:
$k \in \mathbb{N},\ \ M \in \mathbb{N},\ \ X = (x_1, \ldots, x_k) \in \{-1,1\}^k,\ \ a \in \mathbb{Z},\ \ b \in \mathbb{N},\ \ D = (d_1, \ldots, d_k) \in \mathbb{N}^k$, $d_1 < \ldots < d_k$-ra

$$T(E,M,X) = |\{n : 0 \le n \le M, (e_{n+1}, e_{n+2}, \ldots, e_{n+k}) = X\}|,$$

$$U(E,M,a,b) = \sum_{j=1}^{M} e_{a+jb}$$

és

$$V(E,M,D) = \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k}.$$

Ekkor az E sorozat normális, ha

$$|T(E,M,X) - M/2^k| = o(M)$$

minden rögzített k-ra és X-re, ahogy $M \to \infty$, míg a második és harmadik véletlen tulajdonság a következőképpen fejezhető ki:

$$U(E,M,a,b) = o(M),$$

illetve

$$V(E,M,D) = o(M)$$

minden rögzített a, b és D-re, ahogy $M \to \infty$.

A véletlen tulajdonságok véges analógiájának megfogalmazása előtt további két különböző természetű követelményt állítanak elő.

Hogy megmagyarázzák a következő követelményt, szemléltetésül először megfontolják a véges bináris sorozatok pszeudovéletlenségének Knuth [4] által adott definícióját:

3.1. Definíció (*Knuth*)**.** Egy $E_N = (e_1, \ldots, e_N) \in \{-1,1\}^N$ véges halmazt pszeudovéletlennek nevezünk, ha minden $k \in \mathbb{N}$-re, ahol

$$k \leq \frac{\log N}{\log 2},$$

és minden $X \in \{-1,1\}^k$-ra létezik

$$\left| T(E_N, N+1-k, X) - \frac{N+1-k}{2^k} \right| \leq \frac{1}{\sqrt{N}}.$$

A fenti definíció csupán két lehetőséget enged: a sorozat vagy "jó" vagy "rossz", azaz vagy pszeudovéletlen vagy nem az.

4. A bináris sorozatok pszeudovéletlenségét jellemeznie kell egy az összes véges bináris sorozat halmazán meghatározott valós értékű függvénynek (így össze kell tudnia hasonlítani két azonos hosszúságú sorozatot).

5. Meg kell tudnia becsülni ezt a pszeudovéletlenségi mértéket legalább bizonyos "szép" sorozatokra.

Gyakorlatilag reménytelen definiálni egy értéket, ami viszonylag jól becsülhető a sorozatok többségére, így az utolsó feltétel, hogy:

6. Ez a pszeudovéletlen mérték különböző szintekkel kell, hogy rendelkezzen és az egyiknek képesnek kell lennie legalább alacsony szintű mértékeket becsülnie, hogy a kapott eredményt egy "trendként", "részeredményként" értelmezze a pszeudovéletlenség irányában.

Mauduit és Sárközy [5] egy ilyen pszeudovéletlenségi mérték definiálásához először az első három véletlen tulajdonságot jellemző pszeudovéletlenségi mértéket mutatják be. Ezen tulajdonságok mindegyikéhez létezik egy meglehetősen természetes módja annak, hogy egy pszeudovéletlenségi mértéket bármilyen adott $E_N = (e_1, \ldots, e_N) \in \{-1,1\}^N$ sorozathoz hozzárendeljük:

3.2. Definíció (*Mauduit-Sárközy*)**.** k-adrendű normalitás mérték:

$$N_k(E_N) = \max_{X \in \{-1,1\}^k} \max_{0 < M \leq N+1-k} |T(E_N, M, X) - M/2^k|.$$

3.3. Definíció (*Mauduit-Sárközy*)**.** Normalitás mérték:

$$N(E_N) = \max_{k \leq (\log N)/\log 2} N_k(E_N).$$

3.4. Definíció (*Mauduit-Sárközy*)**.** Egyenletes eloszlás mértéke:

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

ahol a maximumot minden olyan a-ra, b-re és t-re tekintjük, ahol $a,b,t \in \mathbb{N}$ és $1 \leq a+b \leq a+tb \leq N$.

3.5. Definíció (*Mauduit-Sárközy*)**.** k-adrendű korrelációs mérték:

$$C_k(E_N) = \max_{M,D} |V(E_N,M,D)| = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \right|,$$

ahol a maximumot minden olyan $D = (d_1, \dots, d_k)$-ra és M-re tekintjük, ahol $M + d_k \leq N$.

3.6. Definíció (*Mauduit-Sárközy*)**.** Korrelációs mérték:

$$C(E_N) = \max_{k \leq (\log N)/\log 2} C_k(E_N).$$

Ekkor az E_N sorozat N szempontjából "jó" pszeudovéletlen sorozatnak számít, ha a $W(E_N)$ és $C_k(E_N)$ mértékek is "kicsik" (legalább kis k értékekre).

3.7. Definíció (*Mauduit-Sárközy*)**.** Kombinált (egyenletes eloszlású-korrelációs) k-adrendű mérték:

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right| = \max_{a,b,t,D} |Z(a,b,t,D)|,$$

ahol

$$|Z(a,b,t,D)| = \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k}$$

definiált minden olyan $a,b,t,D = (d_1, d_2, \dots, d_k)$-ra, ahol minden $a + jb + d_l$ index az $\{1, \dots, N\}$-hez tartozik.

3.8. Definíció (*Mauduit-Sárközy*)**.** Kombinált mérték:

$$Q(E_N) = \max_{k \leq (\log N)/\log 2} Q_k(E_N)$$

4. A Legendre szimbólum pszeudovéletlensége

A Q_k és Q kombinált pszeudovéletlenségi mértékek rendelkeznek az 1-4. és 6. tulajdonságokkal. Azt kell még megmutatni, hogy ezek a mértékek az 5. tulajdonsággal is rendelkeznek, melyhez Mauduit és Sárközy [5] a Legendre szimbólumot tesztelik:

4.1. Tétel (*Mauduit-Sárközy*)**.** *Létezik egy p_0 szám úgy, hogy ha $p > p_0$ prímszám, $k \in \mathbb{N}$, $k < p$ és*

$$E_{p-1} = \left(\left(\frac{1}{p} \right), \left(\frac{2}{p} \right), \ldots, \left(\frac{p-1}{p} \right) \right),$$

akkor

$$Q_k(E_{p-1}) \leq 9kp^{1/2} \log p$$

így $N = p-1$-re

$$Q(E_N) = \max_{k \leq (\log N)/\log 2} Q_k(E_N) \leq 27N^{1/2} (\log N)^2$$

továbbá

$$Q^*(E_N) = \sum_{k=1}^{\infty} Q_k(E_N)/2^k \leq 33N^{1/2} \log N.$$

A tétel bizonyítása az [5] cikkben megtalálható.

Mauduit és Sárközy [5] megmutatták, hogy a Legendre szimbólum "jó" pszeudovéletlen sorozatot alkot.

Legyen p egy páratlan prím és

$$N = p-1, \quad e_n = \left(\frac{n}{p} \right), \quad E_N = \{e_1, \ldots, e_N\}. \tag{1}$$

Ekkor az előző tétel alapján létezik

$$W(E_N) \ll p^{1/2} \log p \ll N^{1/2} \log N$$

és

$$C_k(E_N) \ll kp^{1/2} \log p \ll kN^{1/2} \log N.$$

Számos bináris sorozat tesztelésre került már sor pszeudovéletlenségi szempontból, azonban továbbra is az (1) konstrukció a legjobb. Az eddigi "jó" pszeudovéletlen bináris sorozatot adó konstrukciók csak "keveset" állítanak elő, míg egyes alkalmazásokban (például a kriptográfiában) ezek "nagy" családjára van szükség. Goubin, Mauduit és Sárközy a [6]-os cikkben erős pszeudovéletlen tulajdonságokkal rendelkező bináris sorozatok egy nagy családját adták meg, melyet a következő fejezetben ismertetek.

5. A Legendre szimbólumhoz kapcsolódó további konstrukció

Az $\left(\frac{n}{p}\right)$ Legendre szimbólum pszeudovéletlen tulajdonságait számos cikkben tanulmányozták (például [8]). Mauduit és Sárközy [9] kibővítették az (1)-es konstrukciót e_n definíciójának általánosításával:

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

ahol $f(n)$ egy permutációs polinom $\mathbb{F}_p$ felett (a modulo p maradékosztályok mezője).

Bár nagyon keveset tudunk a permutációs polinomokról és csak nagyon kevesüket ismerjük, a "jó" polinomok egy sokkal nagyobb családját tudjuk használni, de ezek leírása előtt ismerkedjünk meg a következő két definícióval:

5.1. Definíció (*Goubin-Mauduit-Sárközy*)**.** Ha $m, M \in \mathbb{N}$, $\mathscr{A}, \mathscr{B} \subset \mathbb{Z}_m$ (gyűrűje a modulo m maradékosztájainak), és $\mathscr{A} + \mathscr{B}$ reprezentálja $\mathbb{Z}_m$ minden elemét multiplicitásokkal együtt, azaz minden $c \in \mathbb{Z}_m$ esetén

$$a + b = c, \quad a \in \mathscr{A},\ b \in \mathscr{B} \tag{2}$$

páros számú megoldással rendelkezik (beleértve azt az esetet, amikor nincs megoldása), akkor $\mathscr{A} + \mathscr{B}$ összegét P tulajdonságúnak mondjuk.

5.2. Definíció (*Goubin-Mauduit-Sárközy*)**.** Ha $k, \ell, m \in \mathbb{N}$ és $k, \ell \leq m$, akkor azt mondjuk, hogy (k, ℓ, m) egy elfogadható hármas, ha nincs $\mathscr{A}, \mathscr{B} \subset \mathbb{Z}_m$ úgy, hogy $|\mathscr{A}| = k$, $|\mathscr{B}| = \ell$, és $\mathscr{A} + \mathscr{B}$ rendelkezik a P tulajdonsággal.

Jelölje $\mathbb{F}_p$ algebrai berekesztését $\overline{\mathbb{F}}_p$.

5.3. Tétel (*Goubin-Mauduit-Sárközy*)**.** *Ha p egy prím, $f(x) \in \mathbb{F}_p[x]$ foka $k(>0)$, $f(x)$ nem tartalmaz több nullát $f(x) \in \mathbb{F}_p$-ben, és az $E_p = \{e_1, \ldots, e_p\}$ bináris sorozatot az*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & ha\ (f(n), p) = 1 \\ +1 & ha\ p \mid f(n) \end{cases} \tag{3}$$

által definiáljuk, akkor létezik

$$W(E_p) < 10\, kp^{1/2} logp$$

. Továbbá tegyük fel, hogy $\ell \in \mathbb{N}$ és a következő feltételek egyike áll:

(i) $\ell = 2$*;*

(ii) $\ell < p$ *és* 2 *primitív gyök modulo* p*;*

(iii) $(4k)^\ell < p$*;*

Ekkor

$$C_\ell(E_p) < 10\, k\ell p^{1/2} \log p.$$

A fenti tétel bizonyítása, melyet Goubin, Mauduit és Sárközy [6] cikkében találunk, a következő lemmán alapul, melyet Mauduit és Sárközy Weil [7] tételéből vezetett le Vinogradov módszerét használva. A legtöbb konstrukció esetén a pszeudovéletlen mértékek becslése Weil ezen híres tételére vezetődik vissza.

1. Lemma (*Goubin-Mauduit-Sárközy*)**.** *Tegyük fel, hogy p prím, χ nem főkarakter d-ed rendben modulo p (így $d \mid p-1$), $f(X) \in \mathbb{F}_p[X]$ foka k és egy faktorizációja $f(X) = b(X-X_1)_1^d \ldots (X-X_s)_s^d$ (legyen $X_i \neq X_j \quad i \neq j$-re) $\overline{\mathbb{F}}_p$-ben, ahol*

$$(d, d_1, \ldots, d_s) = 1. \tag{4}$$

Legyenek X, Y valós számok úgy, hogy $0 < Y \leq p$. Ekkor

$$\left| \sum_{X < n \leq X+Y} \chi(f(n)) \right| < 9kp^{1/2} \log p.$$

Az **5.3.** tétel felhasználásához szükséges kritérium, hogy a (k, ℓ, p) hármas elfogadható legyen.
Goubin, Mauduit és Sárközy [6] a következő tételben fogalmazzák meg az elfogadhatóság feltételeit:

5.4. Tétel (*Goubin-Mauduit-Sárközy*). *(i) Minden p prímre és $k \in \mathbb{N}$, $k < p$ a $(k, 2, p)$ hármas elfogadható.*

(ii) Ha p prím, k, $\ell \in \mathbb{N}$ és

$$(4\ell)^k < p, \tag{5}$$

akkor (k, ℓ, p) elfogadható.

(iii) Ha p olyan prím, melynek 2 primitív gyöke modulo p, akkor minden k, $\ell \in \mathbb{N}$ párosra, ahol $k < p$, $\ell < p$, a (k, ℓ, p) hármas elfogadható.

Bizonyítás. (*Goubin-Mauduit-Sárközy*)

(i) Az állítással ellentétesen tegyük fel, hogy létezik egy p prímszám és egy $k \in \mathbb{N}$, ahol

$$k < p \tag{6}$$

úgy, hogy a $(k, 2, p)$ hármas nem elfogadható, azaz létezik $\mathscr{A}, \mathscr{B} \subset \mathbb{Z}_p$ úgy, hogy $|\mathscr{A}| = k$, $|\mathscr{B}| = 2$ és (2)-nek páros számú megoldása van minden $c \in \mathbb{Z}_p$-re. $\mathscr{B} = \{b, b+d\}$ (ahol $d \neq 0$).
$\mathscr{A} + b$ minden tagjának (legalább) 2 ábrázolása van (2)-es alakban, amiből könnyen következik, hogy $\mathscr{A} + b = \mathscr{A} + b + d$. Következésképpen $\mathscr{A} + b = \mathscr{A} + b + rd$ bármely r-re, és így $\mathscr{A} + b = \mathscr{A} + b + s$ bármely $s \in \mathbb{Z}_p$-re, különösen bármely $s \in \mathscr{A} + b$-re. Ennél fogva $\mathscr{A} + b$ additív alcsoportja $\mathbb{Z}_p$-nek, és így $\mathscr{A} + b = \mathbb{Z}_p$.

(ii) Tegyük fel, hogy k, ℓ, p kielégíti (5)-öt és van $\mathscr{A}$, $\mathscr{B} \subset \mathbb{Z}_p$, $|\mathscr{A}| = k$, $|\mathscr{B}| = \ell$.
Ez elegendő, hogy megmutassa, létezik $c \in \mathbb{Z}_p$, amire (2)-nek pontosan egy megoldása van. Ráadásul, ha $m \in \mathbb{N}$, $(m, p) = 1$, akkor (2)-nek és az alábbinak:

$$ma + mb = mc, \quad a \in \mathscr{A},\ b \in \mathscr{B}$$

ugyanazok a megoldásai és ha c a $\mathbb{Z}_p$ elemein fut, akkor itt $c' = mc$ ugyanazt csinálja. Így elegendő megmutatni, hogy van olyan $m \in \mathbb{N}$, $c' \in \mathbb{Z}_p$, hogy $(m,p) = 1$, és a következőnek ugyanaz a megoldása:

$$ma + mb = c', \quad a \in \mathscr{A}, \quad b \in \mathscr{B} \tag{7}$$

Jelölje $r(a)$ az $a \mod p$ abszolút legkisebb maradékát $a \in \mathbb{Z}$-re, azaz $r(a) \in \mathbb{Z}$-t határozzák meg

$$r(a) \equiv a \mod p, \quad |r(a)| \leq \frac{p-1}{2}.$$

A következő lemma szükséges:

2. Lemma (*Goubin-Mauduit-Sárközy* [6]). *Ha k, ℓ, p, $\mathscr{A}$ a fentiek szerint vannak definiálva, és $\mathscr{A}$-ban a maradékosztályokat $a_1, \ldots, a_k$ reprezentálja, akkor létezik $m \in \mathbb{N}$ úgy, hogy $(m,p) = 1$ és*

$$|r(ma_i)| \leq \frac{1}{2}\left[\frac{p}{\ell}\right] \quad \textit{ahol } i = 1,2,\ldots,k. \tag{8}$$

Bizonyítás. (*Goubin-Mauduit-Sárközy*) Tekintsük a p k értéksorokat.

$$\underline{u}_j = (r(ja_1),\ \ldots,\ r(ja_k)), \quad j = 1,2,\ldots,p. \tag{9}$$

Legyen $D = \frac{1}{2}\left[\frac{p}{\ell}\right] + 1$ és $Z = \left[\frac{p}{D}\right] + 1$. Ekkor $DZ > p$ és így minden k hármasra (9)-ben egyedileg meghatározott nemnegatív egészek $t_1 = t_1(j)$, …, $t_k = t_k(j)$ úgy, hogy

$$r(ja_i) \in \left\{-\frac{p-1}{2} + t_i D,\ -\frac{p-1}{2} + t_i D + 1,\ \ldots,\ -\frac{p-1}{2} + (t_i+1)D - 1\right\}$$
$$i = 1,2,\ldots,k \text{ esetén}$$

és ezen t_i egészekre egyértelműen létezik

$$t_i \in 0,1,\ldots,Z-1, \quad \text{ahol } i = 1,2,\ldots,k. \tag{10}$$

A lehetséges k értéksorok száma $t_1,\ldots,t_k$ (10) szerint, (5) által,

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

és így létezik legalább egy k értéksor $t_1, \ldots, t_k$, amely legalább két különböző j-hez j_1, j_2 van rendelve:

$$t_1 = t_1(j_1) = t_1(j_2), \ldots, t_k = t_k(j_1) = t_k(j_2). \tag{11}$$

Ekkor

$$-\frac{p-1}{2} + t_i D \leq r(j_1 a_i), \quad r(j_2 a_i) < -\frac{p-1}{2} + (t_i + 1)D,$$

ahonnan

$$|r(j_1 a_i) - r(j_2 a_i)| < D \quad i = 1,\ 2,\ \ldots,\ k \text{ esetén.} \tag{12}$$

Most definiáljuk m-et $m = |j_1 - j_2|$ által, így $1 \leq j_1,\ j_2 \leq p$-re és $j_1 \neq j_2$-re $(m, p) = 1$. Ezután (12)-ből következik, hogy

$$|r(ma_i)| = |r((j_1 - j_2)a_i)| \leq |r(j_1 a_i) - r(j_2 a_i)| < D \quad i = 1,\ 2,\ \ldots,\ k \text{ esetén,}$$

amivel teljesül a 2. Lemma bizonyítása. □

A (ii) rész bizonyításának befejezése, illetve a (iii) rész bizonyítása a [6] cikkben található. □

Bár két olyan konstrukció is megjelent, melyek csak kissé alacsonyabbrendűek az **5.3.** tételbelinél, továbbra is (3) a legjobb konstrukció erős pszeudovéletlen tulajdonságú bináris sorozatok nagy családjának előállítására.
Az elsőt Mauduit, Rivat és Sárközy adta meg a [10] cikkben:

5.5. Tétel (*Mauduit-Rivat-Sárközy*)**.** *Legyen p egy páratlan prím, $f(x) \in \mathbb{F}_p[x]$ d fokú, és $E_p = \{e_1, \ldots, e_p\}$ bináris sorozatot az*

$$e_n = \begin{cases} +1 & \text{ha } 0 \leq r_p(f(n)) < p/2 \\ -1 & \text{ha } p/2 \leq r_p(f(n)) < p, \end{cases} \tag{13}$$

definiálja, ahol r_p jelöli az egyedi $r \in \{0, \ldots, p-1\}$-t, melyre $n \equiv r \mod p$. Ekkor

$$W(E_p) \ll d p^{1/2} (\log p)^2$$

és

$$2 \leq \ell \leq d - 1 \tag{14}$$

esetén

$$C_\ell(E_p) \ll dp^{1/2}(\log p)^{\ell+1}.$$

Ennek hátránya, hogy amennyiben (14) nem áll fenn, $C_\ell(E_p)$ nagy lehet.

Bár az előbbi két konstrukció (3) és (13) egymástól nagyon távolinak tűnnek, nem teljesen azok, ahogy Rivat és Sárközy [12] következő megfigyelése mutatja:

legyen $g(x) \in \mathbb{F}_p[x]$, és vegyük a (13) konstrukciót $g(n)^{(p-1)/2}$-re $f(n)$ helyett. Euler lemmájából

$$e_n = +1, \text{ ha } p \mid g(n) \text{ vagy } g\left(n^{(p-1)/2}\right) \equiv 1 \mod p, \text{ azaz } \left(\frac{g(n)}{p}\right) = 1$$

és

$$e_n = -1, \text{ ha } g\left(n^{(p-1)/2}\right) \equiv -1 \mod p, \text{ azaz } \left(\frac{g(n)}{p}\right) = -1$$

így megkapjuk a (3) konstrukciót $g(n)$-nel $f(n)$ helyett, ami a (13) konstrukció speciális esetének tekinthető. Természetesen ez nem jelenti azt, hogy bármilyen kapcsolat lenne az **5.3.** és **5.5.** tétel között.

A másik konstrukciót, amely a modulo p multiplikatív inverz fogalmán alapul, Mauduit és Sárközy [13] adták meg:

5.6. Tétel (*Mauduit-Sárközy*)**.** *Legyen p prím, $f(x) \in \mathbb{F}_p[x]$ k fokú $(1 < k < p)$, és nincs többszörös nulla $\overline{\mathbb{F}}_p$-ben. $(a,p) = 1$-re jelölje a multiplikatív inverzét a^{-1}:*

$$aa^{-1} \equiv 1 \mod p$$

Az $E_p = \{e_1, \ldots, e_p\}$ bináris sorozatot definiáljuk a következő módon:

$$e_n = \begin{cases} +1 & \text{ha } (f(n),p) = 1,\ r_p(f(n)^{-1}) < p/2; \\ -1 & \text{ha } (f(n),p) = 1,\ r_p(f(n)^{-1}) \geq p/2 \text{ vagy } p \mid (f(n)), \end{cases} \tag{15}$$

*ahol r_p az **5.5.** tétel szerint definiált. Ekkor*

$$W(E_p) \ll kp^{1/2}(\log p)^2.$$

Továbbá tegyük fel, hogy $\ell \in \mathbb{N}$, és a következő feltételek közül egy áll:

(i) $\ell = 2$;

(ii) $(4k)^\ell < p$.

Ekkor

$$C_\ell(E_p) \ll k\ell p^{1/2}(\log p)^{\ell+1}.$$

Figyeljük meg, hogy mindhárom konstrukció $\mathbb{F}_p$ feletti, vagyis p modulusú moduláris konstrukciók. Még nem találtak más természetű konstrukciót hasonló minőségben, így vannak, akik más típusúakat keresnek, összetett m modulusú moduláris konstrukciókat. Rivat és Sárközy [12] célja megtenni az első lépést ebbe az irányba a három konstrukció kiterjesztésével olyan összetett m modulusú speciális esetre, ahol m "RSA típusú", azaz két egymástól nem távoli prím szorzata:

$$m = pq, \quad p, q \text{ prímek, } (2 <)p < q < 2p. \tag{16}$$

6. Elfogadhatóság, "jó" prímek

Goubin, Mauduit és Sárközy [6] a következő definíciót adták:

6.1. Definíció (*Goubin-Mauduit-Sárközy*)**.** Egy pozitív m egész számot jónak tekintünk, ha bármely k, $\ell \in \mathbb{N}$-re, melyre $k < m$ és $\ell < m$ a (k, ℓ, m) hármas elfogadható.

A következő tételük bizonyítása a [6] cikkükben olvasható:

6.2. Tétel (*Goubin-Mauduit-Sárközy*)**.** *Egy p páratlan prím akkor és csakis akkor jó, ha a 2 primitív gyöke modulo p.*

7. Következmények, algoritmus

Az **5.3.** tétel és az **5.5.** tétel (i) részének kombinálásával Goubin, Mauduit és Sárközy [6] a következőket kapták:

7.1. Következmény (*Goubin-Mauduit-Sárközy*)**.** Ha p, f, k, E_p a **5.3.** tétel szerint vannak definiálva, akkor létezik

$$W(E_p) < 10kp^{1/2}\log p; \tag{17}$$

és

$$C_2(E_p) < 20kp^{1/2}\log p.$$

Vagyis az egyenletes eloszlás mérték és a másodrendű korrelációs mérték mindig kicsi. Magasabb rendű korrelációk vizsgálatára is van lehetőség, amennyiben a rend k és p szempontjából nem "nagyon nagy". Az **5.3.** tétel és az **5.5.** tétel (ii) részét kombinálva megkapjuk:

7.2. Következmény (*Goubin-Mauduit-Sárközy*)**.** Ha p, f, k, E_p a **5.3.** tétel szerint vannak definiálva, akkor

(i) 2 primitív gyök modulo p és $\ell < p$, vagy

(ii)
$$\ell < \frac{p^{1/4}}{4},$$

(iii) mind a (17) és
$$C_\ell(E_p) < 20k\ell_p^{1/2}\log p \tag{18}$$

áll.

A **7.2.** következmény alapján az alábbi algoritmus ajánlott az adott p hosszúságú pszeudovéletlen bináris sorozatok előállításához (ahol p prím) [6]:

7.3. Algoritmus (*Goubin-Mauduit-Sárközy*)**.** Tegyük fel, hogy egy p prím és egy $L \in \mathbb{N}$ egész szám adottak úgy, hogy

$$L < \begin{cases} p & \text{minden } p\text{-re} \\ \frac{p}{4} & \text{ha 2 nem primitív gyök modulo } p. \end{cases} \tag{19}$$

(L jellemzően $p/4$-nél "sokkal kisebb", például $L < p^{1/4}$). Tegyük fel, hogy ellenőrizni szeretnénk az ℓ-edrendű korrelációt minden $\ell \leq L$-re.

Legyen $L \in \mathbb{N}$ "nagy" szám úgy, hogy

$$k < \frac{\log p}{\log(4L)}, \quad \text{ha 2 nem primitív gyök modulo } p. \tag{20}$$

Legyen $t = [k/2]$, majd tekintsük $g(X) \in \mathbb{F}_p[X]$ polinomokat a következő alakban:

$$g(X) = X^k + \sum_{i=0}^{t} a_i X^i, \tag{21}$$

ahol bármely a_i együttható megválasztható a következőképpen:

$$a_i \in \mathbb{Z}_p \quad i = 0, 1, \ldots, t-1\text{-re és } a_t \in \mathbb{Z}_p \setminus 0. \tag{22}$$

Jelölje $d(X)$ a $g(X)$ és $g'(X)$ polinomok legnagyobb közös osztóját, és számítsuk ki:

$$f(X) = \frac{g(X)}{d(X)} = \frac{g(X)}{(g(X), g'(X))}. \tag{23}$$

Ez után az **5.3.** tétel szerint definiált E_p sorozat kiszámításával egy "jó" E_p pszeudovéletlen sorozahoz jutunk.
(23)-ból következik, hogy $f(X)$ nem tartalmaz több nullát. $f(X)$ foka

$$\deg f(X) \leq \deg g(X) = k.$$

Ezenfelül (19) és (20) által minden $\ell \leq L$-re létezik

$$\ell \leq L < \begin{cases} p & \text{minden } p\text{-re} \\ \frac{1}{4}p^{1/4} & \text{ha 2 nem primitív gyök modulo } p, \end{cases}$$

így a **7.2.** következmény feltételei teljesülnek, amiből következik, hogy mind (17), mind (18) (minden $\ell \leq L$-re) fenn áll. Minden így definiált E_p sorozat rendelkezik a kívánt tulajdonságokkal.
Jegyezzük meg, hogy a_0, a_1, …, a_t (21)-ben és (22)-ben $(p-1)p^{t-1} \geq \frac{1}{2}p^t = p^{[k/2]}$ féle különböző módon választható meg, így "sok" $g(X)$ polinom létezik (21) alakban, ráadásul minden $g(X)$-re van

$$d(X) \mid (kg(X) - X'g(X)) = (k-t)a_t X^t + \ldots$$

(ahol $(k-t)a_tX^t$ a legmagasabb kitevőjű tag) ahonnan $\deg d(X) \leq t$, így

$$\deg f(X) = \deg g(X) - \deg d(X) \geq k - t = k - [k/2] \geq k/2.$$

Ez megmutatja, hogy bár különböző $g(X)$ polinomok vezethetnek ugyanahhoz az $f(X)$ polinomhoz, erre kis esély van. Másrészt, amikor a $g(X)$ polinomokat redukáljuk az $f(X)$ polinomokra, a kapott polinomok általában nem lesznek "túl egyszerű", lineáris polinomok, Vagyis az E_p sorozatok ily módon definiált családja "nagy" és "magasan összetett".

8. Karakterösszeg becslések a pq modulusra

A moduláris exponenciális összegek klasszikus becslései (Weil [11]) teljes összegekkel foglalkoznak, vagyis minden maradékosztály felett összegeznek. A hiányos összegekre való áttéréshez legalább egy Vinogradov-elv szükséges, amely a következő egyenlőtlenségen alapul:

3. Lemma (*Rivat-Sárközy* [12]). *Ha $m \in \mathbb{N}$, a $g(x) : \mathbb{Z} \to \mathbb{C}$ függvény periodikus m periódussal és X, Y valós számok úgy, hogy $Y > 0$, akkor*

$$\left| \sum_{X<n\leq X+Y} g(n) \right| \leq \frac{Y+1}{m} \left| \sum_{n=1}^{m} g(n) \right| + \sum_{1\leq|h|\leq m/2} |h|^{-1} \left| \sum_{n=1}^{m} g(n) e\left(\frac{hn}{m}\right) \right|.$$

Implicit bizonyítás: Vinogradov [14].

8.1. Multiplikatív karakterösszeg becslések

A következő lemmák, propozíciók és tétel bizonyításai, illetve azok hivatkozásai Rivat és Sárközy [12] cikkében olvashatóak.

4. Lemma (*Rivat-Sárközy*). *Tegyük fel, hogy p prím, χ d-edrendben nem főkarakter modulo p (így $d \mid p-1$), $f(x) \in \mathbb{F}_p[x]$ k fokú, és*

$$f(x) \text{ nem állandó többszöröse egy } \mathbb{F}_p \text{ feletti polinom } d-th \text{ hatványának.} \tag{24}$$

Ekkor minden $a \in \mathbb{Z}$ esetén

$$\left|\sum_{x\in\mathbb{F}_p} \chi(f(x))e_p(ax)\right| \leq sp^{1/2}\left(\leq kp^{1/2}\right) \tag{25}$$

ahol s jelöli $f(x)$ különböző nulláinak számát ($\mathbb{F}_p$ algebrai zárásban, $\overline{\mathbb{F}_p}$-ben).

5. Lemma (*Rivat-Sárközy*)**.** *Legyenek p, χ, d és s a **4.** lemmában definiáltak és tegyük fel, hogy $f(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ egy olyan polinom, amely $\mathbb{F}_p$ felett egy $k(\leq \ell)$ fokú polinomra redukálódik úgy, hogy nem konstans többszöröse egy $\mathbb{F}_p$ feletti polinom $d-th$ hatványának. Legyenek X, Y valós számok, ahol $0 < Y \leq p$. Ekkor*

$$\left|\sum_{X<n\leq X+Y} \chi(f(n))\right| < 9sp^{1/2}\log p\left(\leq 9\ell p^{1/2}\log p\right).$$

6. Lemma (*Rivat-Sárközy*)**.** *Legyenek p és q különböző prímek és $f(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$. Legyen χ primitív (multiplikatív) karakter modulo pq és $\chi = \chi_p\chi_q$, ahol χ_p karakter modulo p $d_p > 1$ rendben és χ_q karakter modulo q $d_q > 1$ rendben.*

Ha feltesszük, hogy $\mathbb{F}_p[x]$-ben $f(x)$ nem konstans többszöröse egy polinom $d_p - th$ hatványának és s_p különböző nullát tartalmaz $\overline{\mathbb{F}_p}$ felett, akkor

$$\left|\sum_{n=0}^{pq-1} \chi(f(n))e_{pq}(an)\right| \leq s_p p^{1/2} q. \tag{26}$$

Hasonlóan, ha feltesszük, hogy $\mathbb{F}_q[x]$-ben $f(x)$ nem konstans többszöröse egy polinom $d_q - th$ hatványának és s_q különböző nullát tartalmaz $\overline{\mathbb{F}_p}$-ben, akkor

$$\left|\sum_{n=0}^{pq-1} \chi(f(n))e_{pq}(an)\right| \leq s_q p q^{1/2}. \tag{27}$$

Ha mindkét feltétel teljesül, akkor az alábbi élesebb becslés áll:

$$\left|\sum_{n=0}^{pq-1} \chi(f(n))e_{pq}(an)\right| \leq s_p s_q p^{1/2} q^{1/2}. \tag{28}$$

7. Lemma (*Rivat-Sárközy*)**.** *Legyenek p és q különböző prímek és $f(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ és X, Y valós számok úgy, hogy $0 < Y \leq pq$. Legyen χ primitív (multiplikatív) karakter modulo pq és $\chi = \chi_p\chi_q$, ahol χ_p karakter modulo p $d_p > 1$ rendben*

és χ_q karakter modulo q $d_q > 1$ rendben. Tegyük fel, hogy $\mathbb{F}_p[x]$-ben $f(x)$ nem konstans többszöröse egy polinom $d_p - th$ hatványának és s_p különböző nullát tartalmaz $\overline{\mathbb{F}_p}$ felett, illetve $\mathbb{F}_q[x]$-ben $f(x)$ nem konstans többszöröse egy polinom $d_q - th$ hatványának és s_q különböző nullát tartalmaz $\overline{\mathbb{F}_q}$ felett. Ekkor

$$\left|\sum_{X<n\leq X+Y} \chi(f(n))\right| \ll s_p s_q p^{1/2} q^{1/2} \log(pq) \left(\leq \ell^2 p^{1/2} q^{1/2} \log(pq)\right). \tag{29}$$

8.2. Additív karakterösszeg becslések

8. Lemma (*Rivat-Sárközy*)**.** *Tegyük fel, hogy p egy prímszám és $f(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ egy polinom, ahol $0 < \ell < p$ és $(a_\ell, p) = 1$. Ekkor*

$$\left|\sum_{n=0}^{p-1} e_p(f(n))\right| \leq (\ell - 1)p^{1/2}.$$

9. Lemma (*Rivat-Sárközy*)**.** *Tegyük fel, hogy p egy prímszám és $f(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ egy polinom, ahol $2 < \ell < p$ és $(a_\ell, p) = 1$. Ekkor minden X és Y valós számra, ahol $0 < Y \leq p$*

$$\left|\sum_{X<n\leq X+Y} e_p(f(n))\right| \ll \ell p^{1/2} \log p.$$

1. Jelölés (Multiplikatív inverz)**.** Olyan $a \in \mathbb{Z}$-ra és $m \in \mathbb{N}$-re, ahol $(a, m) = 1$ jelöljük $i_m(a)$-val az olyan egyedi b egész számot, ahol $0 \leq b \leq m - 1$ és $ab \equiv 1 \bmod m$.

10. Lemma (*Rivat-Sárközy*)**.** *Legyenek p és q különböző prímszámok. Ekkor minden $f(x) \in \mathbb{Z}[x]$ polinomra létezik*

$$\left|\sum_{n=0}^{pq-1} e_{pq}(f(n))\right| = \left|\sum_{u=0}^{q-1} e_q(i_q(p) f(u))\right| \left|\sum_{v=0}^{p-1} e_p(i_p(q) f(v))\right|. \tag{30}$$

11. Lemma (*Rivat-Sárközy*)**.** *Legyenek p és q különböző prímszámok és $f(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, ahol $2 \leq \ell < \min(p, q)$ és $pq \nmid a_\ell$. Ekkor*

$$\left|\sum_{n=0}^{pq-1} e_{pq}(f(n))\right| \leq (\ell - 1)^2 p^{1/2} q^{1/2} \quad (a_\ell, pq) = 1 \text{ esetén}, \tag{31}$$

$$\left|\sum_{n=0}^{pq-1} e_{pq}(f(n))\right| \leq (\ell-1)pq^{1/2} \quad (a_\ell, q) = 1 \textit{ esetén}, \tag{32}$$

és

$$\left|\sum_{n=0}^{pq-1} e_{pq}(f(n))\right| \leq (\ell-1)p^{1/2}q \quad (a_\ell, p) = 1 \textit{ esetén}. \tag{33}$$

12. Lemma (*Rivat-Sárközy*)**.** *Legyenek p és q különböző prímszámok és $f(x) = a_\ell x^\ell + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, ahol $2 \leq \ell < \min(p,q)$, $pq \nmid a_\ell$ és X, Y valós számok úgy, hogy $0 < Y \leq pq$. Ekkor*

$$\left|\sum_{X<n\leq X+Y} e_{pq}(f(n))\right| \ll \ell^2 p^{1/2} q^{1/2} \log(pq) \quad (a_\ell, pq) = 1 \textit{ esetén}, \tag{34}$$

$$\left|\sum_{X<n\leq X+Y} e_{pq}(f(n))\right| \ll \ell pq^{1/2} \log(pq) \quad (a_\ell, q) = 1 \textit{ esetén}, \tag{35}$$

és

$$\left|\sum_{X<n\leq X+Y} e_{pq}(f(n))\right| \ll \ell p^{1/2} q \log(pq) \quad (a_\ell, p) = 1 \textit{ esetén}. \tag{36}$$

1. Propozíció (*Rivat-Sárközy*)**.** Legyenek p és q különböző prímszámok úgy, hogy $(p,q) = 1$. Ha $n \in \mathbb{Z}$, ahol $(n, pq) = 1$, akkor

$$i_{pq} \equiv p i_q(pn) + q i_p(qn) \bmod pq.$$

13. Lemma (*Rivat-Sárközy*)**.** *Legyen $p, q \in \mathbb{N}$ úgy, hogy $(p,q) = 1$ és $Q(x), R(x) \in \mathbb{Z}[x]$. Ekkor*

$$\begin{aligned}
&\sum_{\substack{1\leq n\leq pq \\ (R(n),pq)=1}} e_{pq}(Q(n) i_{pq}(R(n))) \\
&\quad = \sum_{\substack{1\leq u\leq q \\ (R(u),q)=1}} e_q(Q(u) i_q(pR(u))) \sum_{\substack{1\leq v\leq p \\ (R(v),p)=1}} e_p(Q(v) i_p(qR(v)))
\end{aligned}$$

2. Propozíció (*Rivat-Sárközy*)**.** Legyen p prímszám és Q/R egy nem konstans valós függvény $\mathbb{F}_p$ felett, továbá tegyük fel, hogy $\deg(Q) < p$ és $\deg(R) < p$. Ekkor Q/R nem $A^p - A$ alakú, ahol $A \in \overline{\mathbb{F}_p}(x)$ ($\overline{\mathbb{F}_p}(x)$ jelöli a valós függvény terét $\mathbb{F}_p$ algebrai zárására, $\overline{\mathbb{F}_p}$ felett).

14. Lemma (*Rivat-Sárközy*). *Legyen Q/R valós függvény $\mathbb{F}_q$ felett nem $A^p - A$ alakban, ahol $A \in \overline{\mathbb{F}_q}(x)$ és p az $\mathbb{F}_q$ karakterisztikája. Legyen s az R polinom különböző gyökeinek száma $\overline{\mathbb{F}_q}$-ban. Ha ψ egy nemtriviális additív karaktere $\mathbb{F}_q$-nak, akkor*

$$\left| \sum_{\substack{n \in \mathbb{F}_q \\ R(n) \neq 0}} \psi\left(\frac{Q(n)}{R(n)}\right) \right| \leq (\max(\deg(Q), \deg(R)) + s - 1)\sqrt{q}.$$

15. Lemma (*Rivat-Sárközy*). *Legyen p prímszám és Q/R egy nem konstans valós függvény $\mathbb{F}_p$ felett. Legyen s az R polinom különböző gyökeinek száma $\overline{\mathbb{F}_p}$-ben. Ha ψ egy nemtriviális additív karaktere $\mathbb{F}_p$-nek, akkor*

$$\left| \sum_{\substack{n \in \mathbb{F}_p \\ R(n) \neq 0}} \psi\left(\frac{Q(n)}{R(n)}\right) \right| \leq (\max(\deg(Q), \deg(R)) + s - 1)\sqrt{p}.$$

8.1. Tétel (*Rivat-Sárközy*). *Legyen p prímszám és ψ nemtriviális additív karakter modulo p. Legyen Q/R egy valós függvény $\mathbb{F}_p$ felett oly módon, hogy az R polinomnak s különböző gyöke van $\overline{\mathbb{F}_p}$ felett, és tegyük fel, hogy Q/R nem állandó vagy lineáris polinom. Legyen $d = \max(\deg(R), \deg(Q) - 1)$. Ekkor $1 \leq N \leq p$ esetén*

$$\left| \sum_{\substack{0 \leq n \leq N-1 \\ R(n) \neq 0}} \psi\left(\frac{Q(n)}{R(n)}\right) \right| \leq (d+s)\sqrt{p}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{N+0.64}{p}\right).$$

16. Lemma (*Rivat-Sárközy*). *Legyen p és q két különböző prímszám. Legyenek $Q, R \in \mathbb{Z}[x]$ polinomok úgy, hogy modulo p redukálva őket az így kapott Q_p és R_p polinomok egy Q_p/R_p nem konstans valós függvényt határoznak meg $\mathbb{F}_p$ felett. Ugyanezt feltesszük modulo q Q_q/R_q-ra. Ekkor*

$$\left| \sum_{\substack{1 \leq n \leq pq \\ (R(n), pq) = 1}} e_{pq}(Q(n) i_{pq}(R(n))) \right| \leq (d_p + s_p - 1)(d_q + s_q - 1)\sqrt{pq},$$

ahol $d_p = \max(\deg(Q_p, R_p))$ és s_p R_p különböző gyökeinek száma $\overline{\mathbb{F}_p}$ felett. Hasonlóan $d_q = \max(\deg(Q_q, R_q))$ és R_q különböző gyökeinek száma $\overline{\mathbb{F}_q}$ felett s_q.

17. Lemma (*Rivat-Sárközy*). *Legyenek p és q különböző prímszámok és $Q,R \in \mathbb{Z}[x]$ polinomok úgy, hogy modulo p redukálva őket az így kapott Q_p és R_p polinomok egy Q_p/R_p valós függvényt határoznak meg $\mathbb{F}_p$ felett, mely nem konstans vagy lineáris polinom. Ugyanezt feltesszük Q_q/R_q-ra modulo q. $D = \max(\deg(R), \deg(Q))$ és X,Y valós számok, ahol $0 < Y \leq pq$. Ekkor*

$$\left| \sum_{\substack{X<n\leq X+Y \\ (R(n),pq)=1}} e_{pq}(Q(n)i_{pq}(R(n))) \right| \ll d_p d_q \sqrt{pq} \log(pq) \ (\ll D^2 \sqrt{pq} \log(pq)).$$

9. A Legendre szimbólum konstrukciójának kiterjesztése a Jacobi szimbólumra

Számos tanulmány jelent meg, melyben pszeudovéletlen sorozatokat Jacobi szimbólummal állítanak elő (például [15], [16]). Érdemes ezeket a sorozatokat az általunk használt mértékekkel pszeudovéletlenségre tesztelni. Rivat és Sárközy [12] megmutatjuk, hogy a **5.3.** tételben szereplő (3) konstrukcióban a p prímet és a Legendre szimbólumot kicserélve a (16) formulájú m modulusra és a Jacobi szimbólumra olyan E_N bináris sorozatot kapunk, melyre $W(E_N)$ és $C_2(E_N)$ kicsi, de $C_4(E_N)$ (bármely $f(n)$-re) nagy:

9.1. Tétel (*Rivat-Sárközy*). *Tegyük fel, hogy $m \in \mathbb{N}$ (16) formulájú, $f(x) = a_d x^d + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$,*

$$(a_d, pq) = 1, \tag{37}$$

$$0 < d < p(< q), \tag{38}$$

$f(x)$, mint $\mathbb{F}_p$ feletti polinom (pontosabban egy d fokú polinom, melynek együtthatói az a_d, $\ldots$, a_1, illetve a_0 által reprezentált modulo m maradékosztályok) nem egy $\mathbb{F}_p$ feletti polinom négyzetének állandó többszöröse, és $f(x)$, mint $\mathbb{F}_q$ feletti polinom nem egy $\mathbb{F}_q$ feletti polinom négyzetének állandó többszöröse. Definiáljuk az $E_m = e_1, \ldots, e_m$ bináris sorozatot a következőképpen:

$$e_n = \begin{cases} \left(\frac{f(n)}{m}\right) & ha\ (f(n),m) = 1, \\ +1 & ha\ (f(n),m) > 1, \end{cases}$$

ahol $\left(\frac{f(n)}{m}\right)$ *jelöli a Jacobi szimbólumot. Ekkor*

$$W(E_p) \ll d^2 m^{1/2} logm, \tag{39}$$

$$C_2(E_p) \ll dm^{3/4} \tag{40}$$

és

$$C_4(E_p) \geq m - 35dm^{1/2} (= (1+o(1))m). \tag{41}$$

Bizonyítás. (*Rivat-Sárközy*) Tegyük fel, hogy $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ és

$$1 \leq a \leq a + (t-1)b \leq m, \tag{42}$$

és legyen $g(x) = f(a+bx) = a_d b^d x^d + (a_d dab^{d-1} + a_{d-1} b^{d-1}) x^{d-1} + \dots$ úgy, hogy $g(x) \in \mathbb{Z}[x]$, és ($b \in \mathbb{N}$-re) $\deg g(x) = d$.

Tegyük fel, hogy

$$(b,m) = 1. \tag{43}$$

Ekkor mind $g(x) \equiv 0 \bmod p$-nek és $g(x) \equiv 0 \bmod q$-nak legfeljebb d megoldása van, így $p \mid g(x)$-hez legfeljebb dq, míg $q \mid g(x)$-hez legfeljebb dp inkongruens x érték van modulo $m (= pq)$. Ebből következik, hogy $(a,m) > 1$-re $\left(\frac{a}{m}\right)$-t 0-ként definiálva

$$\begin{aligned} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| &\leq \left| \sum_{j=0}^{t-1} \left(\frac{f(a+jb)}{m} \right) \right| + \sum_{\substack{0 \leq j \leq t-1 \\ (f(a+jb),m)>1}} 1 \\ &\leq \left| \sum_{j=0}^{t-1} \left(\frac{g(j)}{m} \right) \right| + dp + dq. \end{aligned} \tag{44}$$

(37) és (43) alapján az x^d kifejezés $a_d b^d$ együtthatója (ami a legmagasabb fokú tag) a $g(x)$-ben m-hez relatív prím. Ebből következik, hogy a **7.** lemmát felírhatjuk $g(x)$, $\left(\frac{a}{m}\right)$, 2, 2, d-vel és $f(n)$, $\chi(n)$, d_p, d_q, s_p, s_q helyett d-vel. Ezt követően az **5.** lemma felhasználásával (44)-ből kapjuk, hogy

$$\left| \sum_{j=0}^{t-1} e_{a+jb} \right| \ll d^2 m^{1/2} \log m + dm^{1/2} + dm^{1/2} \ll d^2 m^{1/2} \log m. \tag{45}$$

Most tegyük fel, hogy $p \mid b$. Ekkor (16) és (42) alapján

$$pq = m \geq a + (t-1)b \geq 1 + (t-1)p > (t-1)p$$

ahonnan

$$t - 1 < q,$$
$$t \leq q < 2m^{1/2}$$

így

$$\left| \sum_{j=0}^{t-1} e_{a+jb} \right| \leq \sum_{j=0}^{t-1} 1 = t < 2m^{1/2} \quad (p \mid b\text{-re}). \tag{46}$$

Ha $q \mid b$, ugyanúgy megkapjuk, hogy

$$\left| \sum_{j=0}^{t-1} e_{a+jb} \right| \leq t \leq p < m^{1/2} \quad (q \mid b\text{-re}). \tag{47}$$

(45), (46) és (47)-ből következik (39).

(40) bizonyításához vegyük a d_1, d_2 egész számokat és $M \in \mathbb{N}$-t úgy, hogy

$$0 \leq d_1 < d_2, \quad M + d_2 \leq m.$$

Legyen $\delta = d_2 - d_1$. Először tegyük fel, hogy

$$(\delta, m) = 1. \tag{48}$$

Ahogy (44)-ben, $(a,m) > 1$-re $\left(\frac{a}{m}\right) = 0$, és felhasználjuk, hogy

$$f(n + d_i) \equiv 0 \bmod m$$

$i = 1$, 2-re legfeljebb $dp + dq$ inkongruens megoldással rendelkezik modulo m. Megkapjuk, hogy

$$\begin{aligned}
&\left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \right| \\
&\quad \leq \left| \sum_{n=1}^{M} \left(\frac{f(n+d_1)}{m} \right) \left(\frac{f(n+d_2)}{m} \right) \right| + \sum_{\substack{1 \leq n \leq M \\ (f(n+d_1)f(n+d_2),m) > 1}} 1 \\
&\quad \leq \left| \sum_{n=1}^{M} \left(\frac{f(n+d_1)f(n+d_2)}{m} \right) \right| + 2d(p+q).
\end{aligned} \tag{49}$$

Most megmutatjuk, hogy $\mathbb{F}_p$-ben a $h(x) = f(n+d_1)f(n+d_2)$ polinom nem állandó többszöröse egy polinom négyzetének. Írjuk fel $f(x)$-et $\mathbb{F}_p$ felett egy $r(x) \in \mathbb{F}_p[x]$ polinom négyzete és egy négyzetmentes $s(x) \in \mathbb{F}_p[x]$ polinom szorzataként: $f(x) = r^2(x)s(x)$ ($\mathbb{F}_p$ felett). Az $f(x)$-re vonatkozó feltevéseink szerint $s(x)$ nem állandó polinom $\mathbb{F}_p$ felett. Írjuk fel $s(x)$-et különböző irreducibilis polinomok szorzataként $\mathbb{F}_p[x]$ felett, és jelölje $\varphi(x)$ ezen irreducibilis faktorok egyikét. Ekkor

$$\varphi(x+d_1) \mid s(x+d_1) \mid f(x+d_1).$$

A következő polinomok mind irreducibilisek: $\varphi(x+d_1)$, $\varphi(x+d_1+\delta)$, $\varphi(x+d_1+2\delta)$, ..., $\varphi(x+d_1+(p-1)\delta)$ és (48)-ból következik, hogy modulo p különbözőek. Ha mindegyik polinom osztója $s(x+d_1)$-nek, akkor

$$\begin{aligned} d = \deg f(x) = \deg f(x+d_1) &\geq \deg s(x+d_1) \\ &\geq \deg \varphi(x+d_1)\varphi(x+d_1+\delta)\dots\varphi(x+d_1+(p-1)\delta) = p\deg\varphi(x) \\ &\geq p \end{aligned}$$

ami ellentmond (38)-nak. Jelölje t a legkiebb pozitív egész számot melyre $\varphi(x+d_1+(t-1)\delta) \mid s(x+d_1)$, $\varphi(x+d_1+t\delta) \nmid s(x+d_1)$ (így $0<t<p$). Ekkor egyértelműen $\varphi(x+d_1+t\delta) \mid s(x+d_1+\delta)$, így $f(x+d_1)$ osztható $\varphi(x+d_1+t\delta)$ egy páros hatványával, míg $f(x+d_1+\delta) = f(x+d_2)$ egy páratlan hatványával. Ekkor $h(x) = f(x+d_1)f(x+d_2)$ valóban osztható $\varphi(x+d_1+t\delta)$ egy páratlan hatványával, ezért nem lehet egy $\mathbb{F}_p$ feletti polinom négyzetének állandó többszöröse. (48)-ból ugyanígy következik, hogy $h(x) = f(x+d_1)f(x+d_2)$ nem lehet egy $\mathbb{F}_q$ feletti polinom négyzetének állandó többszöröse. Következésképpen a (49)-beli összeg becsléséhez a **7.** lemmát $f(x+d_1)f(x+d_2)$-vel használjuk $f(n)$ helyett. valamint $\chi(n) = \left(\frac{n}{m}\right)$, $\chi_p(n) = \left(\frac{n}{p}\right)$ $\left(\left(\frac{n}{p}\right) = 0 \quad p \mid n\text{-re}\right)$, $\chi_q(n) = \left(\frac{n}{q}\right)$, $d_p = d_q = 2d$, $s_p, s_q \leq \deg f(x+d_1)f(x+d_2) \leq 2\deg f(n) \leq 2d$. Azt kapjuk, hogy

$$\begin{aligned} \left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\right| &\ll d^2m^{1/2}\log m + dm^{1/2} \\ &\ll d^2m^{1/2}\log m \quad (\delta,m) = 1\text{-re}. \end{aligned} \tag{50}$$

Tegyük fel, hogy

$$(\delta,m) = p. \tag{51}$$

Ekkor, ahogy (49)-ben

$$\begin{aligned}
&\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\right| \\
&\quad\le \left|\sum_{n=1}^{M}\left(\frac{f(n+d_1)f(n+d_2)}{m}\right)\right| + 2d(p+q) \\
&\quad= \left|\sum_{n=1}^{M}\left(\frac{f(n+d_1)f(n+d_1+\delta)}{p}\right)\left(\frac{f(n+d_1)f(n+d_2)}{q}\right)\right| + 2d(p+q) \\
&\quad= \left|\sum_{n=1}^{M}\left(\frac{f^2(n+d_1)}{p}\right)\left(\frac{f(n+d_1)f(n+d_2)}{q}\right)\right| + 2d(p+q) \\
&\quad\le \left|\sum_{n=1}^{M}\left(\frac{f(n+d_1)f(n+d_2)}{q}\right)\right| + \sum_{\substack{1\le n\le m\\ p\mid f(n+d_1)}} 1 + 2d(p+q) \\
&\quad\le \left|\sum_{n=1}^{M}\left(\frac{f(n+d_1)f(n+d_2)}{q}\right)\right| + dq + 2d(p+q) \\
&\quad\le \sum_{i=1}^{\lfloor M/q\rfloor}\left|\sum_{n=(i-1)q+1}^{iq}\left(\frac{f(n+d_1)f(n+d_2)}{q}\right)\right| \\
&\quad+ \left|\sum_{n=\lfloor M/q\rfloor q+1}^{M}\left(\frac{f(n+d_1)f(n+d_2)}{q}\right)\right| + 3d(p+q). \qquad (52)
\end{aligned}$$

(51)-et felhasználva a (49)-hez hasonló módon megmutatható, hogy $\mathbb{F}_p$-ben az $f(n+d_1)f(n+d_2)$ polinom nem állandó többszöröse egy polinom négyzetének, így felhasználhatjuk a **4.** lemmát (p, χ, d, $f(x)$ és a helyett q, $\left(\frac{n}{q}\right)$, 2, $f(x+d_2)f(x+d_2)$ és 0), illetve az **5.** lemmát (p, χ, d és $f(x)$ helyett q, $\left(\frac{n}{q}\right)$, 2 és $f(x+d_2)f(x+d_2)$) az (52)-es szumma felső becsléséhez.

$$\begin{aligned}
\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\right| &\ll \left\lfloor\frac{M}{q}\right\rfloor dq^{1/2} + dq^{1/2}\log q + d(p+q) \qquad (53)\\
&\ll dpq^{1/2} \ll dm^{3/4} \quad ((\delta,m)=p\text{-re}).
\end{aligned}$$

Ugyanígy megmutatható, hogy

$$\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\right| \ll dm^{3/4} \quad ((\delta,m)=q\text{-ra}). \qquad (54)$$

(50), (53), (54)-ből következik (40) $\quad (\delta < m$-re $(\delta, m) = 1$, p vagy $q)$.

9.2. Megjegyzés (*Rivat-Sárközy*)**.** Ez a bizonyítás megmutatja, hogy a felső határ (40)-ben a lehető legjobb (eltekintve az implicit konstans faktor értékétől). Könnyű látni, hogy ha $f(n) = n$, akkor az összegek (52)-ben $\gg pq^{1/2} \gg dm^{3/4}$ nagyságúak lehetnek. Másrészről, ha "rövidtávú korrelációra" korlátozzuk magunkat, pontosabban olyan összegekre, ahol $(0 <)\ d_2 - d_1 < p$, akkor (51) és $(\delta, m) = q$ nem fordulhat elő, így mindig (50) érvényes:

$$\left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \right| \ll d^2 m^{1/2} \log m \quad (0 < d_2 - d_1 < p\text{-re}). \tag{55}$$

Végül, ha $g(n,p,q) = f(n)f(n+p)f(n+q)f(n+p+q)$, megkapjuk, hogy

$$\begin{aligned} C_4(E_N) &\geq \left| \sum_{n=1}^{m-p-q} e_n e_{n+p} e_{n+q} e_{n+p+q} \right| \qquad (56) \\ &\geq \sum_{n=1}^{m-p-q} 1 - \sum_{\substack{1 \leq n \leq m-p-q \\ (g(n,p,q),m)=1}} |e_n e_{n+p} e_{n+q} e_{n+p+q} - 1| \\ &- \sum_{\substack{1 \leq n \leq m-p-q \\ (g(n,p,q),m)>1}} |e_n e_{n+p} e_{n+q} e_{n+p+q} - 1| \\ &\geq (m-p-q) - \sum_{\substack{1 \leq n \leq m-p-q \\ (g(n,p,q),m)=1}} \left| \left(\frac{g(n,p,q)}{m} \right) - 1 \right| \\ &-2 \left(\sum_{\substack{1 \leq n \leq m-p-q \\ (f(n),m)>1}} 1 + \sum_{\substack{1 \leq n \leq m-p-q \\ (f(n+p),m)>1}} 1 + \sum_{\substack{1 \leq n \leq m-p-q \\ (f(n+q),m)>1}} 1 + \sum_{\substack{1 \leq n \leq m-p-q \\ (f(n+p+q),m)>1}} 1 \right). \end{aligned}$$

Ha $(g(n,p,q),m) = 1$, akkor

$$\begin{aligned} \left(\frac{g(n,p,q)}{m} \right) &= \left(\frac{g(n,p,q)}{p} \right) \left(\frac{g(n,p,q)}{q} \right) \\ &= \left(\frac{f^2(n) f^2(n+q)}{p} \right) \left(\frac{f^2(n) f^2(n+p)}{q} \right) = 1, \end{aligned}$$

így (56) alsó határának első összege 0. Továbbá

$$\begin{aligned}\sum_{\substack{1\le n\le m-p-q\\(f(n),m)>1}} 1 &\le \sum_{\substack{1\le n\le m-p-q\\p|f(n)}} 1+\sum_{\substack{1\le n\le m-p-q\\q|f(n)}} 1\\ &\le \left(\left\lfloor\frac{m-p-q}{p}\right\rfloor+1\right)d+\left(\left\lfloor\frac{m-p-q}{q}\right\rfloor+1\right)d\\ &\le \frac{m}{p}d+\frac{m}{q}d\le 2\frac{m}{p}d\le 4dm^{1/2},\end{aligned}$$

és ugyanez a felső határ adható az utolsó három összegre (56)-ban, így (56)-ból következik, hogy

$$C_4(E_m)\ge (m-p-q)-32dm^{1-2}\ geqm-35dm^{1-2},$$

amely teljesíti a **9.1.** tétel bizonyítását.

□

További feltételek mellett (55) kiterjeszthető magasabb rendű "rövidtávú" korrelációra. Rivat és Sárközy következő tételeinek bizonyítása [12] cikkben található.

9.3. Tétel (*Rivat-Sárközy*)**.** *Legyenek p, q, m, $f(x)$, d és $E_m=\{e_1,\dots,e_m\}$ a **9.1.** tételben definiáltak. Tegyük fel továbbá, hogy $\ell\in\mathbb{N}$ és a következő feltételek egyike áll:*

(i) $\ell<p$, *és* 2 *primitív gyök modulo* p *és* q*;*

(ii) $(4d)^\ell<p\ (<q)$.

Ekkor, ha $d_1<d_2<\ldots<d_l$ pozitív egészek és

$$d_i\not\equiv d_j \bmod p,\ d_i\not\equiv d_j \bmod q,\quad \text{ahol } 1\le i<j\le\ell, \tag{57}$$

akkor minden $M\in\mathbb{N}$, $1\le M\le N-d_\ell$ esetén

$$\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\dots e_{n+d_\ell}\right|\ll d\ell m^{1/2}\log m$$

(ahol az implicit konstans tényező egy abszolút konstans).

Vegyük észre, hogy $d_\ell<p$-ből következik (57), így az előző tételből:

9.4. Tétel (*Rivat-Sárközy*)**.** *Legyenek p, q, m, $f(x)$, d és $E_m = \{e_1, \ldots, e_m\}$ a **9.1.** tételben definiáltak és tegyük fel, hogy 2 primitív gyök modulo p. Ekkor*

$$N_k(E_m) \ll k2^k m^{1/2} \log m \quad k \in \mathbb{N},\ 2 \leq k \text{ esetén}$$

és

$$N(E_m) \ll m^{3/4} \log m.$$

9.1. A (13) konstrukció kiterjesztése

9.5. Tétel (*Rivat-Sárközy*)**.** *Tegyük fel, hogy $m \in \mathbb{N}$ (16) alakú, $f(x) = a_d x^d + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$,*

$$(a_d, pq) = 1, \tag{58}$$

$$2 \leq d < p\ (< q). \tag{59}$$

Legyen $E_m = e_1, \ldots, e_m$ bináris sorozat a következőképpen definiálva

$$e_n = \begin{cases} +1 & \text{ha } 0 \leq r_m(f(n)) < m/2, \\ -1 & \text{ha } m/2 \leq r_m(f(n)) < m, \end{cases}$$

ahol $r_m(n)$ jelöli az egyetlen $r \in \{0, \ldots, m-1\}$-t $n \equiv r$ mod m-re. Ekkor

$$W(E_m) \ll d^2 m^{1/2} (\log m)^2. \tag{60}$$

9.6. Tétel (*Rivat-Sárközy*)**.** *Legyenek p, q, m, $f(x)$, d és $E_m = \{e_1, \ldots, e_m\}$ a **9.5.** tételben definiáltak. Továbbá tegyük fel, hogy*

$$2 \leq k \leq d-1, \tag{61}$$

és $d_1 < d_2 < \cdots < d_k$ és M pozitív egészek, ahol

$$d_i \not\equiv d_j \text{ mod } p,\ d_i \not\equiv d_j \text{ mod } q \quad 1 \leq i < j \leq k\text{-ra}, \tag{62}$$

és $M \leq m - d_k$. Ekkor

$$\left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k} \right| \ll d^2 m^{1/2} (\log m)^{k+1}.$$

9.7. Tétel (*Rivat-Sárközy*). *Legyenek p, q, m, $f(x)$, d és $E_m = \{e_1, \ldots, e_m\}$ a **9.5.** tételben definiáltak. Továbbá tegyük fel, hogy*

$$d \geq 3. \tag{63}$$

Ekkor

$$C_2(E_m) \ll dm^{3/4}(\log m)^3. \tag{64}$$

9.8. Tétel (*Rivat-Sárközy*). *Legyenek p, q, m, $f(x)$, d és $E_m = \{e_1, \ldots, e_m\}$ a **9.5.** tételben definiáltak. Ekkor $k \in \mathbb{N}$-re,*

$$2 \leq k \leq \min(d-1, p-1)$$

létezik

$$N_k(E_m) \ll d^2 2^k m^{1/2}(\log m)^{k+1}. \tag{65}$$

9.9. Tétel (*Rivat-Sárközy*). *Legyenek p, q, m, $f(x)$, d és $E_m = \{e_1, \ldots, e_m\}$ a **9.5.** tételben definiáltak és tegyük fel, hogy $d < m^{1/8}$. Ekkor létezik*

$$N(E_m) = \begin{cases} \ll m2^{-d} & \text{ha } d^2 2^{2d}(\log m)^{d+1} \leq m^{1/2}, \\ < m\exp\left(-\left(\frac{\log 2}{16} + o(1)\right)\frac{\log m}{\log\log m}\right) & \text{ha } d^2 2^{2d}(\log m)^{d+1} > m^{1/2}. \end{cases} \tag{66}$$

9.2. A (15) konstrukció kiterjesztése

9.10. Tétel (*Rivat-Sárközy*). *Tegyük fel, hogy $m \in \mathbb{N}$ (16) alakú, $f(x) = a_k x^k + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$,*

$$(a_k, pq) = 1 \tag{67}$$

és

$$1 \leq k < p(< q). \tag{68}$$

Definiáljuk az $E_m = \{e_1, \ldots, e_m\}$ bináris sorozatot a következőképpen:

$$e_n = \begin{cases} +1 & \text{ha } (f(n), m) = 1,\ r_m(i_m(f(n))) < m/2, \\ -1 & \text{ha } (f(n), m) = 1,\ r_m(i_m(f(n))) \geq m/2, \text{ vagy } (f(n), m) > 1, \end{cases}$$

*ahol $r_m(n)$ a **9.5.** tételben definiáltak szerinti. Ekkor*

$$W(E_m) \ll k^2 m^{1/2}(\log m)^2. \tag{69}$$

9.11. Tétel (*Rivat-Sárközy*)**.** *Legyenek p, q, m, $f(x)$, k és $E_m = \{e_1, \dots, e_m\}$ a* ***9.10.*** *tételben definiáltak. Tegyük fel továbbá, hogy $\ell \in \mathbb{N}$, és a következő feltételek egyike teljesül:*

(i) $\ell = 2$;

(ii) $(4k)^\ell < p \ (< q)$.

Ekkor $d_1 < d_2 < \cdots < d_\ell$ és M pozitív egészek esetén, ha

$$d_i \not\equiv d_j \bmod p,\ d_i \not\equiv d_j \bmod q \quad \text{ahol } 1 \le i \le j \le \ell$$

és $M \le m - d_\ell$, akkor

$$\left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right| \ll k^4 \ell^2 m^{1/2} (\log m)^{\ell+1}.$$

9.12. Tétel (*Rivat-Sárközy*)**.** *Legyenek p, q, m, $f(x)$, k és $E_m = \{e_1, \dots, e_m\}$ a* ***9.10.*** *tételben definiáltak. Ekkor*

$$C_2(E_m) \ll k^2 \ell m^{3/4} (\log m)^k.$$

9.13. Tétel (*Rivat-Sárközy*)**.** *Legyenek p, q, m, $f(x)$, k és $E_m = \{e_1, \dots, e_m\}$ a* ***9.10.*** *tételben definiáltak, továbbá tegyük fel, hogy $r \in \mathbb{N}$, és a következő feltételek egyike teljesül:*

(i) $r = 2$;

(ii) $(4k)^r < p \ (< q)$.

Ekkor

$$N_r(E_m) \ll k^4 r^2 2^r m^{1/2} (\log m)^{k+1}.$$

9.14. Tétel (*Rivat-Sárközy*)**.** *Legyenek p, q, m, $f(x)$, k és $E_m = \{e_1, \dots, e_m\}$ a* ***9.10.*** *tételben definiáltak, továbbá tegyük fel, hogy*

$$8k^4 (\log m)^{k+1} < m^{1/2}$$

(amiből következik, hogy $4k < p$). Jelölje R a legnagyobb pozitív egész számot, melyre $(4k)^R < p$. Ekkor

$$N(E_m) \ll \frac{m}{2^R} \quad \text{ha } k^4 R^2 2^{2R} (\log m)^{k+1} \le m^{1/2},$$

míg ha $k^4R^2 2^{2R}(\log m)^{k+1} > m^{1/2}$, *akkor*

$$N(E_m) \ll \frac{m}{2^L},$$

ahol L a legnagyobb egész, melyre

$$k^4L^2 2^{2L}(\log m)^{k+1} \leq m^{1/2}.$$

10. Saját programok eredményei adott mértékekre

Két programot írtam pszeudovéletlen mértékek kiszámítására:
Az első program (*1konstr.cbp*) egy bemenő paraméterként kapott p prímhez ($p > 2$) kiszámítja a Legendre szimbólumot használó (1) konstrukcióval kapott bináris sorozathoz a következő mértékeket: egyenletes eloszlás mértéke, elsőrendű kombinált mérték, másodrendű korrelációs mérték, másodrendű kombinált mérték, harmadrendű korrelációs mérték és harmadrendű kombinált mérték.
A második program (*3konstr.cbp*) bemenő paraméterként egy p prímet ($p > 2$), illetve egy polinomot vár, melynek először a fokát kéri be, majd ennek megfelelően minden tag együtthatóját. A beolvasott adatokból a (3) konstrukcióval kapott bináris sorozatra számítja ki az első programnál felsorolt pszeudovéletlen mértékeket.

A következő táblázatokban ezen programok eredményeit foglalom össze.

10.1. Eredmények (1) konstrukcióval

p	$W(E_p)$	$Q_1(E_p)$	$\sqrt{p * \log p}$
3	1	1	$1,1964$
5	2	1	$1,86945$
7	2	2	$2,43222$
11	3	3	$3,38457$
13	4	4	$3,80543$
17	3	3	$4,57358$
19	4	4	$4,92913$
23	5	5	$5,5964$
31	6	6	$6,79943$
47	8	8	$8,86502$
79	10	10	$12,2439$
113	10	10	$15,2315$
173	18	17	$23,061$
211	18	18	$22,1455$
271	22	22	$25,6775$
317	26	25	$28,1573$
373	32	32	$30,9717$
457	14	14	$34,8652$

1. táblázat. Az egyenletes eloszlás és a kombinált elsőrendű eloszlás mértéke

A fenti eredményeim alapján az egyenletes eloszlás és a kombinált elsőrendű eloszlás mértéke közel azonos; a kapott értékekre teljesülnek a következők:
$0 \leq W(E_p) - Q_1(E_p) \leq 1$, illetve
$W(E_p) \leq \frac{5}{4}\sqrt{p * \log p}$ és $Q_1(E_p) \leq \frac{5}{4}\sqrt{p * \log p}$.

p	$C_2(E_p)$	$Q_2(E_p)$	$\sqrt{p * \log p}$
3	1	0	$1,1964$
5	2	0	$1,86945$
7	2	2	$2,43222$
11	4	4	$3,38457$
13	4	4	$3,80543$
17	6	6	$4,57358$
19	5	5	$4,92913$
23	5	5	$5,5964$
31	8	8	$6,79943$
47	9	9	$8,86502$
79	14	14	$12,2439$
113	16	17	$15,2315$
173	18	17	$23,061$
211	21	21	$22,1455$
271	26	26	$25,6775$
317	30	32	$28,1573$
373	31	33	$30,9717$
457	42	44	$34,8652$

2. táblázat. Másodrendű korrelációs mérték és a kombinált másodrendű eloszlás mértéke

A másodrendű korrelációs mértékre és a kombinált másodrendű eloszlás mértékre kapott eredményeim azt mutatják, hogy $|C_2(E_p)$ - $Q_2(E_p)| \leq 2$, illetve
$C_2(E_p) \leq \frac{3}{2}\sqrt{p * \log p}$ és $Q_2(E_p) \leq \frac{3}{2}\sqrt{p * \log p}$ teljesül.

p	$C_3(E_p)$	$Q_3(E_p)$	$\sqrt{p * \log p}$
3	0	0	$1,1964$
5	2	0	$1,86945$
7	3	2	$2,43222$
11	4	4	$3,38457$
13	6	5	$3,80543$
17	8	8	$4,57358$
19	7	7	$4,92913$
23	10	10	$5,5964$
31	10	10	$6,79943$
47	15	15	$8,86502$
79	14	14	$12,2439$
113	16	17	$15,2315$
173	38	38	$23,061$
211	42	42	$22,1455$
271	47	47	$25,6775$
317	51	51	$28,1573$
373	56	56	$30,9717$
457	68	68	$34,8652$

3. táblázat. Harmadrendű korrelációs mérték és a kombinált harmadrendű eloszlás mértéke

A harmadrendű korrelációs mértékre és a kombinált harmadrendű eloszlás mértékre kapott eredményeim ugyanazt mutatják, mint amit az imént láthattunk ezen mértékek másodrendű változatainál: $|C_3(E_p)$ - $Q_3(E_p)| \leq 2$.
Felső becslésre ebben az esetben $C_3(E_p) \leq 2\sqrt{p * \log p}$ és $Q_3(E_p) \leq 2\sqrt{p * \log p}$ teljesül.

10.2. Eredmények (3) konstrukcióval

p	$W(E_p)$	$Q_1(E_p)$	$\sqrt{p * \log p}$
3	2	1	$1,1964$
5	2	2	$1,86945$
7	4	4	$2,43222$
11	3	3	$3,38457$
13	3	3	$3,80543$
17	4	4	$4,57358$
19	5	5	$4,92913$
23	9	9	$5,5964$
31	7	6	$6,79943$
47	10	10	$8,86502$
79	8	8	$12,2439$
113	16	16	$15,2315$
173	21	21	$19,6769$
211	40	40	$22,1455$
271	77	77	$25,6775$

4. táblázat. Az egyenletes eloszlás és a kombinált elsőrendű eloszlás mértéke $f(n) = n^4 - 4n^2 + 3n - 2$ polinomra

A **10.1** fejezetben leírtakhoz hasonlóan az egyenletes eloszlás és a kombinált elsőrendű eloszlás mértékére itt is teljesül, hogy $0 \leq W(E_p) - Q_1(E_p) \leq 1$;
most azonban nem bizonyul megfelelő felső becslésnek az $\frac{5}{4}\sqrt{p * \log p}$,
$W(E_p) \leq 3\sqrt{p * \log p}$ és $Q_1(E_p) \leq 3\sqrt{p * \log p}$ ellenben már teljesül.

p	$W(E_p)$	$Q_1(E_p)$	$\sqrt{p * \log p}$
3	2	1	$1,1964$
5	2	2	$1,86945$
7	4	4	$2,43222$
11	4	4	$3,38457$
13	6	6	$3,80543$
17	5	5	$4,57358$
19	8	8	$4,92913$
23	5	5	$5,5964$
31	13	13	$6,79943$
47	13	13	$8,86502$
79	11	11	$12,2439$
113	14	14	$15,2315$
173	16	15	$19,6769$
211	13	13	$22,1455$
271	26	26	$25,6775$

5. táblázat. Az egyenletes eloszlás és a kombinált elsőrendű eloszlás mértéke $f(n) = -3n^3 + 4n^2 - 3$ polinomra

$0 \leq W(E_p) - Q_1(E_p) \leq 1$ most is teljesül; felső becslésre ennél a polinomnál azonban már $2\sqrt{p * \log p}$ is alkalmas:
$W(E_p) \leq 2\sqrt{p * \log p}$ és $Q_1(E_p) \leq 2\sqrt{p * \log p}$.

p	$C_2(E_p)$	$Q_2(E_p)$	$\sqrt{p * \log p}$
3	0	0	$1,1964$
5	1	0	$1,86945$
7	3	3	$2,43222$
11	4	4	$3,38457$
13	8	8	$3,80543$
17	6	6	$4,57358$
19	6	6	$4,92913$
23	8	8	$5,5964$
31	12	12	$6,79943$
47	11	11	$8,86502$
79	17	17	$12,2439$
113	29	29	$15,2315$
173	32	32	$19,6769$
211	44	44	$22,1455$
271	86	86	$25,6775$

6. táblázat. Másodrendű korrelációs mérték és a kombinált másodrendű eloszlás mértéke $f(n) = n^4 - 4n^2 + 3n - 2$ polinomra

A másodrendű korrelációs mértékre és a kombinált másodrendű eloszlás mértékre kapott eredményeim ebben az esetben azt mutatják, hogy $|C_2(E_p)$ - $Q_2(E_p)| \leq 1$, illetve $C_2(E_p) \leq \frac{7}{2}\sqrt{p * \log p}$ és $Q_2(E_p) \leq \frac{7}{2}\sqrt{p * \log p}$ teljesül.

p	$C_2(E_p)$	$Q_2(E_p)$	$\sqrt{p * \log p}$
3	0	0	$1,1964$
5	2	2	$1,86945$
7	3	3	$2,43222$
11	3	3	$3,38457$
13	6	6	$3,80543$
17	7	7	$4,57358$
19	9	9	$4,92913$
23	5	6	$5,5964$
31	12	12	$6,79943$
47	11	11	$8,86502$
79	27	27	$12,2439$
113	21	21	$15,2315$
173	40	40	$19,6769$
211	26	27	$22,1455$
271	45	45	$25,6775$

7. táblázat. Másodrendű korrelációs mérték és a kombinált másodrendű eloszlás mértéke $f(n) = -3n^3 + 4n^2 - 3$ polinomra

$|C_2(E_p)$ - $Q_2(E_p)| \leq 1$ ebben az esetben is teljesül, felső becslésre pedig $\frac{9}{4}\sqrt{p * \log p}$ alkalmas: $C_2(E_p) \leq \frac{9}{4}\sqrt{p * \log p}$ és $Q_2(E_p) \leq \frac{9}{4}\sqrt{p * \log p}$.

p	$C_3(E_p)$	$Q_3(E_p)$	$\sqrt{p * \log p}$
3	0	0	$1,1964$
5	1	0	$1,86945$
7	2	2	$2,43222$
11	4	4	$3,38457$
13	3	5	$3,80543$
17	8	8	$4,57358$
19	8	8	$4,92913$
23	9	9	$5,5964$
31	12	12	$6,79943$
47	16	16	$8,86502$
79	25	25	$12,2439$
113	33	33	$15,2315$
173	41	41	$19,6769$
211	51	51	$22,1455$
271	97	97	$25,6775$

8. táblázat. Harmadrendű korrelációs mérték és a kombinált harmadrendű eloszlás mértéke $f(n) = n^4 - 4n^2 + 3n - 2$ polinomra

A harmadrendű korrelációs mértékre és a kombinált harmadrendű eloszlás mértékre kapott eredményeim itt is ugyanazt mutatják, mint a **10.1** fejezetben: $|C_3(E_p)$ - $Q_3(E_p)| \leq 2$; felső becslésre azonban ebben az esetben $2\sqrt{p * \log p}$ nem alkalmas, ellenben $C_3(E_p) \leq 4\sqrt{p * \log p}$ és $Q_3(E_p) \leq 4\sqrt{p * \log p}$ teljesül.

p	$C_3(E_p)$	$Q_3(E_p)$	$\sqrt{p * \log p}$
3	0	0	$1,1964$
5	1	0	$1,86945$
7	2	2	$2,43222$
11	4	4	$3,38457$
13	5	5	$3,80543$
17	7	7	$4,57358$
19	7	7	$4,92913$
23	10	10	$5,5964$
31	14	14	$6,79943$
47	19	19	$8,86502$
79	23	23	$12,2439$
113	35	35	$15,2315$
173	47	47	$19,6769$
211	46	46	$22,1455$
271	54	54	$25,6775$

9. táblázat. Harmadrendű korrelációs mérték és a kombinált harmadrendű eloszlás mértéke $f(n) = -3n^3 + 4n^2 - 3$ polinomra

A fent vizsgált polinomra már $|C_3(E_p)$ - $Q_3(E_p)| \leq 1$ is teljesül; felső becslésre pedig az $\frac{5}{2}\sqrt{p * \log p}$ alkalmas: $C_3(E_p) \leq \frac{5}{2}\sqrt{p * \log p}$ és $Q_3(E_p) \leq \frac{5}{2}\sqrt{p * \log p}$.

Hivatkozások

[1] F. K. R. Chung and P. Tetali: *Communication complexity and quasirandomness*, SIAM J. Discrete Math. 6, 1993, 110-123.

[2] A. N. Kolmogorov: *On table of random numbers*, Sankhya A 25, 1963, 369-376.

[3] P. Martin-Löf: *The definition of random sequences*, Inform. and Control (Shenyang) 6, 1966, 602-619.

[4] D. E. Knuth: *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

[5] C. Mauduit and A. Sárközy: *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arithmetica 82, 1997, 365-377.

[6] L. Goubin, C. Mauduit, and A. Sárközy: *Construction of large families of pseudorandom binary sequences*, Journal of Number Theory 106, 2004, 56-69.

[7] A. Weil: *Sur les courbes algébriques et les variétés qui s'en déduisent*, Acta Sci Ind. Vol. 1041, Hermann, Paris, 1948.

[8] A. Sárközy: *Number Theory and Its Applications*, Műszaki Könyvkiadó, Budapest, 1978.

[9] C. Mauduit and A. Sárközy: *On finite pseudorandom binary sequences II: the Champernowne, Rudin-Shapiro, and Thue-Morse sequences. A further construction*, Journal of Number Theory 73, 1998, 256-276.

[10] C. Mauduit, J. Rivat and A. Sárközy: *Construction of pseudorandom binary sequences using additive characters*, Monatshefte für Mathematik 141, no. 3, 2004, 197-208.

[11] A. Weil: *On some exponential sums*, Proc. Natl. Acad. Sci. USA 34, 1948, 204-207.

[12] J. Rivat and A. Sárközy: *Modular constructions of pseudorandom binary sequences with composite moduli*, Periodica Mathematica Hungarica Vol. 51 (2), 2005, 75-107.

[13] C. Mauduit and A. Sárközy: *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Mathematica Hungarica 108, 2005, 239-252.

[14] I. M. Vinogradov: *Elements of number theory*, Dover, 1954.

[15] I. B. Damgård: *On the randomness of Legendre and Jacobi sequences*, Advances in cryptology - CRYPTO '88 (Santa Barbara, CA, 1988), Lecture Notes in Comput. Sci., Vol. 403, Springer, Berlin, 1990, 163-172.

[16] H. Delfs and H. Knebl: *Introduction to cryptography*, Information Security and Cryptography, Springer-Verlag, Berlin, 2002, Principles and applications.