Exponenciális és karakterösszegek

Gyarmati Katalin

katalin.gyarmati@ttk.elte.hu

Sárközy András

andras.sarkozy@ttk.elte.hu

Eötvös Loránd Tudományegyetem

Egyetemi Jegyzet

ELTE TTK, Matematikai Intézet

2024

Tartalomjegyzék

Bevezetés 3

1. Jelölések 5

2. Parseval formula és Ramanujan összegek 9

3. Csoport karakterek 13

4. Additív karakterek 19

5. Gauss összegek 24

6. A Vinogradov lemma 31

7. Weyl összegek és Weil tétel 37

8. Erdős és Moser problémája 39

9. Kloosterman összegek 49

10. Multiplikatív karakterek 55

11. Gauss összegek (2. rész) 60

12. A Vinogradov lemma duálisa 64

13. Éles-e a Weil tétel? 73

14. Pólya-Vinogradov egyenlőtlenség 78

15. Rövid multiplikatív karakterösszegek 85

16. Nagy szita 92

17. A nagy szita megfordítása 111

Bevezetés

A jegyzetben szereplő kurzus az ELTE-n az MSc és PhD tanterv része, azon matematikus hallgatók számára készült, akik szeretnének a mélyebb számelmélet alapjaival is megismerkedni.

Az olvasóknak kellemes időtöltést kívánunk!

Könyvek, amelyre az anyag épül:

Hivatkozások

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967, 2., 5., 23. és 27. fejezet.

[2] S. W. Graham, G. Kolesnik, *Van der Corput's Method of Exponential Sums*, Cambridge University Press, 1991.

[3] A. Ivič, *The Riemann Zeta-Function: Theory and Applications*, Dover Publications, 2003, 55-83. oldal.

[4] H. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Springer Berlin, Heidelberg 2006, 1-49. oldal.

[5] R. C. Vaughan, *The Hardy-Littlewood Method*, Cambridge University Press, 1997.

[6] I. M. Vinogradov, *A Számelmélet Alapjai*, Tankönyvkiadó, Budapest, 1951.

[7] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Dover Publications, Revised edition 2004.

Az alapok ismertetése főként a [6] és [7] alapján történt. A nagy szita ismertetése pedig a [1], [4] könyvekre épül. A fentieken túl még pár cikkre is épül a jegyzet, ezek referenciáját az adott fejezet végén adtam meg.

További tanulmányok folytatásához, Weyl összegek, van-der Corput módszer, exponens párokhoz pedig [2]-t ajánljuk. Akik érdeklődnének folytatás iránt az [3], [5] könyveket is tanulmányozhatják még.

1. Jelölések

Mi is az, hogy exponenciális összeg?

Komplex számok trigonometrikus alakja:

$$z = r(\cos\alpha + i\sin\alpha) = re^{i\alpha}.$$

Exponenciális összeg: olyan összeg, melyben exponenciális alakban adott komplex számok vannak.

$$e^{i(\alpha_1+\alpha_2)} = e^{i\alpha_1}e^{i\alpha_2}$$
$$\left(e^{i\alpha}\right)^n = e^{in\alpha}.$$

Komplex függvénytan:

$$f(x) = e^x : \mathbb{R} \to \mathbb{R}$$

kiterjeszthető egyértelműen

$$f(z) = e^z : \mathbb{C} \to \mathbb{C}.$$

Itt z helyébe $i\alpha$-t írva, a fent definiált $e^{i\alpha}$-t kapjuk.

$$\overline{e^{i\alpha}} = e^{i(-\alpha)}.$$

Valós analízis:

$$f : \mathbb{R} \to \mathbb{R}.$$

Komplex analízis:

$$f : \mathbb{C} \to \mathbb{C}.$$

Analitikus számelmélet: komplex változós függvények.

Itt:

$$f : \mathbb{R} \to \mathbb{C},$$

azaz valós változós komplex függvények.

Majdnem ugyanaz mint a valós analízis

$$f(t) = g(t) + ih(t),$$

ahol g, h valós függvények, azaz f vizsgálata g-re, h-ra redukálható.

Folytonosság, differenciálhatóság, integrálhatóság definíciója a valós esetre redukálható.

$$f'(t) = g'(t) + ih'(t)$$
$$\int_a^b f(t)dt = \int_a^b g(t)dt + i\int_a^b h(t)dt$$

Differenciálhatósági, integrálhatósági szabályok ugyanazok.

Pl. $f(t) = e^{it}$ esetén

$$\begin{aligned} f'(t) &= (\cos t + i \sin t)' \\ &= (\cos t)' + i(\sin t)' \\ &= -\sin t + i \cos t \\ &= i(\cos t + i \sin t) \\ &= ie^{it}. \end{aligned}$$

Hasonlóan

$$\int_a^b e^{it}dt = \left[\frac{e^{it}}{i}\right]_a^b$$

$$= \frac{1}{i}\left(e^{ib} - e^{ia}\right).$$

Miért olyan fontos a számelméletben ez az $f(t) = e^{it}$ függvény?

Mert

$$f(t) = e^{it} = \cos t + i \sin t$$

periodikus 2π periódushosszal.

$\Rightarrow$

- $g(t) = e^{2\pi i t}$ periodikus 1 periódussal
- $g(t)$ értéke csak a t törtrészétől függ.

Olyan gyakran használjuk ezt a függvényt, hogy külön jelölést vezetünk be:

1.1 DEFINÍCIÓ. *Legyen* $e(\alpha) \overset{\text{def}}{=} e^{2\pi i\alpha}$. *Ekkor* $e(\alpha)$ *értéke csak* α *törtrészétől függ. Ezenkívül használjuk még az* $e_m(\alpha)$ *jelölést is, ahol* $e_m(\alpha) \overset{\text{def}}{=} e^{2\pi i\frac{\alpha}{m}} = e\left(\frac{\alpha}{m}\right)$.

Különösen fontos szerepet játszanak:

$$f(t) = \sum_{n=0}^{N} a_n e(nt)$$
$$= \sum_{n=0}^{N} a_n \left(e(t)\right)^n$$

exponenciális (trigonometrikus) polinomok, valamint

$$F(t) = \sum_{n=0}^{\infty} a_n e(nt)$$

hatványsorok; itt feltesszük, hogy ez abszolút konvergens:

$$\sum_{n=0}^{\infty} |a_n| < \infty.$$

Mint valósban, itt is, minden szakaszosan folytonos $F(t)$ függvény ilyen hatványsorba, ún. Fourier sorba fejthető.

Legyen

$$f(t) = \sum_{n=0}^{N} a_n e(nt).$$

Ekkor mivel egyenlő $f'(t)$ és $\int_a^b f(t)dt$?

Nyilván

$$f'(t) = \sum_{n=0}^{N} 2\pi i n a_n e(nt).$$

Itt $\int_0^1 f(t)dt$ helyett kicsit általánosabban nézzük, ha $0 \leq k \leq N$ egész szám, akkor

$$\begin{aligned}
\int_0^1 f(t)e(-kt)dt &= \sum_{n=0}^{N} a_n \int_0^1 e((n-k)t)dt \\
&= a_k \int_0^1 e(0)dt + \sum_{\substack{n=0,\\ n\neq k}}^{N} a_n \int_0^1 e((n-k)t)dt \\
&= a_k + \sum_{\substack{n=0,\\ n\neq k}}^{N} a_n \left[\frac{e((n-k)t)}{2\pi i(n-k)}\right]_0^1 \\
&= a_k.
\end{aligned}$$

Hasonlóan

$$\int_0^1 f(t)e(-kt)dt = 0 \text{ ha } k < 0 \text{ vagy } k > N.$$

2. Parseval formula és Ramanujan összegek

A következő tétel az egyik legalapvetőbb eszköz exponenciális összegek becslése során.

2.1 TÉTEL. (Parseval formula)

a) $f(t) = \sum_{n=0}^{N} a_n e(nt)$ *esetén*

$$\int_0^1 |f(t)|^2 \, dt = \sum_{n=0}^{N} |a_n|^2.$$

b) *Ha* $f(t) = \sum_{n=0}^{\infty} a_n e(nt)$ *és* $\sum_{n=0}^{\infty} |a_n|^2$ *abszolút konvergens, akkor*

$$\int_0^1 |f(t)|^2 \, dt = \sum_{n=0}^{\infty} |a_n|^2.$$

A 2.1 Tétel bizonyítása.

a)

$$\begin{aligned}
\int_0^1 |f(t)|^2 \, dt &= \int_0^1 f(t)\overline{f(t)}dt \\
&= \int_0^1 \sum_{n=0}^{N} a_n e(nt) \sum_{m=0}^{N} \overline{a_m} e(-mt) dt \\
&= \int_0^1 \sum_{n=0}^{N} \sum_{m=0}^{N} a_n \overline{a_m} e((n-m)t) dt \\
&= \sum_{n=0}^{N} \sum_{m=0}^{N} a_n \overline{a_m} \int_0^1 e((n-m)t) dt.
\end{aligned}$$

Itt az utolsó integrál 0, ha $n \neq m$ és 1, ha $n = m$, azaz

$$\int_0^1 |f(t)|^2 \, dt = \sum_{n=0}^{N} a_n \overline{a_n}$$

$$= \sum_{n=0}^{N} |a_n|^2 .$$

b) hasonlóan.

2.2 LEMMA. a) *Tetszőleges* $\alpha \in \mathbb{R}$*-re*

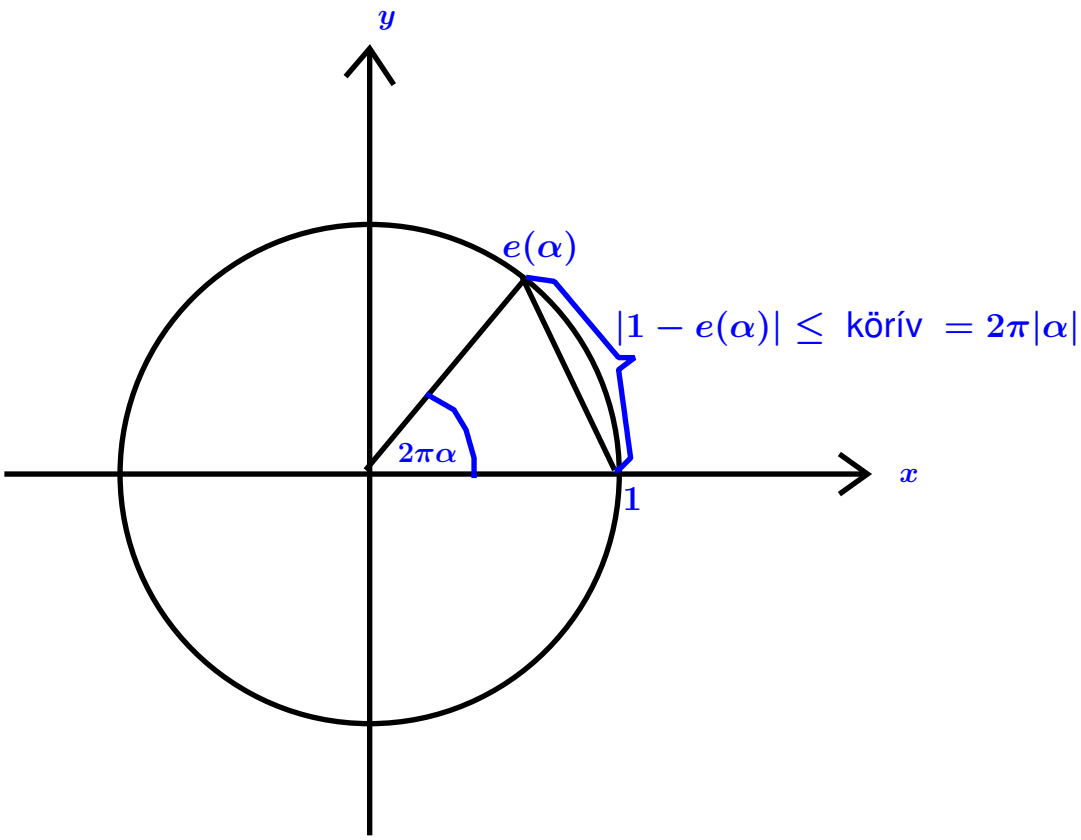
$$|1 - e(\alpha)| \leq 2\pi\,|\alpha| .$$

b) $|\alpha| \leq \frac{1}{2}$ *esetén*

$$|1 - e(\alpha)| \geq 4\,|\alpha| .$$

A 2.2 Lemma bizonyítása.

a)



b)

$$\begin{aligned}|1-e(\alpha)|^2 &= (1-e(\alpha))\,\overline{(1-e(\alpha))}\\ &= (1-e(\alpha))\,(1-e(-\alpha))\\ &= 1-e(\alpha)-e(-\alpha)+1\\ &= 2-2\mathrm{Re}\,e(\alpha)\\ &= 2(1-\cos 2\pi\alpha)\\ &= 2\cdot 2\sin^2\pi\alpha.\end{aligned}$$

Gyököt vonva:

$$|1-e(\alpha)| = 2|\sin\pi\alpha| = 2\sin\pi|\alpha|.$$

Mivel $\frac{\sin x}{x}$ a $[0,\pi/2]$-ben monoton fogyó:

$$\frac{\sin x}{x} \geq \frac{\sin \pi/2}{\pi/2} = \frac{2}{\pi},$$

így

$$\sin x \geq \frac{2}{\pi}x.$$

Azaz

$$|1-e(\alpha)| = 2\sin|\pi\alpha| \geq 2\cdot\frac{2}{\pi}\pi|\alpha| = 4\,|\alpha|\,.$$

Példa. $p\in\mathbb{Z}$, $q\in\mathbb{N}$

$$\begin{aligned}\sum_{n=0}^{q-1} e\left(n\frac{p}{q}\right) &= \sum_{n=0}^{q-1} e\left(\frac{p}{q}\right)^n\\ &= \begin{cases} q & \text{ha } q\mid p,\\ \frac{1-e\left(q\frac{p}{q}\right)}{1-e\left(\frac{p}{q}\right)} = \frac{1-1}{1-e\left(\frac{p}{q}\right)} = 0 & \text{ha } q\nmid p.\end{cases}\end{aligned}$$

2.3 TÉTEL. (Jensen-Ramanujan formula) *Ha $q \in \mathbb{N}$, akkor*

$$S = \sum_{\substack{0 \le p < q \\ (p,q)=1}} e\left(\frac{p}{q}\right) = \mu(q).$$

Azaz a primitív q-adik egységgyökök összege $\mu(q)$.

A 2.3 Tétel bizonyítása. Jelölje μ a Möbius-függvényt. A következőt használjuk:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{ha } n = 1 \\ 0 & \text{ha } n > 1. \end{cases}$$

Ekkor:

$$\begin{aligned} S &= \sum_{p=0}^{q-1} \left(\sum_{d|(p,q)} \mu(d) \right) e\left(\frac{p}{q}\right) \\ &= \sum_{d|q} \mu(d) \sum_{\substack{0 \le p \le q-1 \\ d|p}} e\left(\frac{p}{q}\right). \end{aligned}$$

Az utolsó szummában írjunk $p = kd$-t. Ekkor $kd \le q-1$, tehát $k \le \frac{q}{d} - 1$. Így:

$$S = \sum_{d|q} \mu(d) \sum_{k=0}^{\frac{q}{d}-1} e\left(k\frac{d}{q}\right).$$

Az első szummában különválasszuk a $d = q$ és $d < q$ eseteket. Ekkor

$$\begin{aligned} S &= \mu(q) + \sum_{\substack{d|q \\ d<q}} \mu(d) \sum_{k=0}^{\frac{q}{d}-1} e\left(k\frac{d}{q}\right) \\ &= \mu(q) + \sum_{\substack{d|q \\ d<q}} \mu(d) \frac{1 - e\left(\frac{q}{d} \cdot \frac{d}{q}\right)}{1 - e\left(\frac{d}{q}\right)} \qquad = \mu(q) + \sum_{\substack{d|q \\ d<q}} \mu(d) 0 \\ &= \mu(q). \end{aligned}$$

3. Csoport karakterek

Számelméletben karakteren általában multiplikatív karaktereket, esetleg additív karaktereket értünk, ezekről később lesz szó.

Először inkább általánosabban definiáljuk az ún. csoport karaktereket, minimális csoportelméletet használva (így jobban látszik, modernebb).

Először tehát, hogy az algebrában mit értünk csoport karakteren. Mi most csak a véges Ábel csoportok esetét nézzük (jóval egyszerűbb és nekünk elég).

3.1 DEFINÍCIÓ. *Legyen $\mathcal{G}$ véges Ábel csoport,*

$$\chi : \mathcal{G} \to \mathbb{C}$$

a következő tulajdonságokkal

1. $\chi(g) \not\equiv 0 \quad \mathcal{G}$*-n*
2. $\chi(g)$ *multiplikatív* $\mathcal{G}$*-n:*

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2) \quad \forall g_1, g_2 \in \mathcal{G}.$$

Ekkor χ-t ($\mathcal{G}$-n definiált) csoport karakternek nevezzük.

3.2 KÖVETKEZMÉNYEK.

(1) *Ha $\mathcal{G}$ egységeleme e, akkor $\chi(e) = 1$.*

(2) *$\forall\, g \in \mathcal{G}$-re $(\chi(g))^{|\mathcal{G}|} = 1$.*

(3) *Definiáljuk* $\chi_0 : \mathcal{G} \to \mathbb{C}$*-t úgy, hogy*

$$\chi_0(g) \equiv 1 \quad \forall\, g \in \mathcal{G}\text{-re.}$$

Ekkor χ_0 *karakter* $\mathcal{G}$*-n, ez az ún. főkarakter vagy triviális karakter.*

(4) *Ha* χ *karakter* $\mathcal{G}$*-n, akkor definiáljuk*

$$\overline{\chi} : \mathcal{G} \to \mathbb{C}\text{-t}$$
$$\overline{\chi}(g) \stackrel{\text{def}}{=} \overline{\chi(g)} \quad \forall g \in \mathcal{G}\text{-vel.}$$

Ekkor $\overline{\chi}$ *is karakter* $\mathcal{G}$*-n, ez az ún. konjugált karakter.*

(5) *Ha* $\chi_1,\ \chi_2$ *karakter* $\mathcal{G}$*-n, akkor definiáljuk* χ*-t*

$$\chi(g) \stackrel{\text{def}}{=} \chi_1(g)\chi_2(g) \quad \forall\, g \in \mathcal{G}\text{-vel.}$$

Ekkor χ *is karakter* $\mathcal{G}$*-n. (Tehát két karakter szorzata is karakter, sőt, a karakterek csoportot alkotnak.)*

(6) *Ha* $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$*, akkor* $\chi : \mathcal{G} \to \mathbb{C}$ *akkor és csak akkor karakter* $\mathcal{G}$*-n, ha* $\exists\ \chi_1$ *karakter* $\mathcal{G}_1$*-n,* χ_2 *karakter* $\mathcal{G}_2$*-n, hogy* $\forall\, g = g_1 g_2 \in \mathcal{G}$*-re*

$$\chi(g) = \chi(g_1 g_2) = \chi_1(g_1)\chi_2(g_2).$$

(7) *Ha* $\mathcal{G} = C_n = \{g\}_n$ *az* n*-edrendű ciklikus csoport, akkor* χ *akkor és csak akkor karakter* $\mathcal{G}$*-n, ha* $\exists$ *olyan* $a \in \{0, 1, 2, \ldots, n-1\}$ *hogy*

$$\chi(g^k) = e\left(k\frac{a}{n}\right) \quad \forall\, k \in \mathbb{Z}\text{-re.}$$

(8) *A* $\mathcal{G} = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r} = \{g_1\}_{n_1} \times \{g_2\}_{n_2} \times \cdots \times \{g_r\}_{n_r}$*-en definiált karakterek explicit alakja*

$$\chi(g_1^{k_1} \cdots g_r^{k_r}) = e\left(k_1 \frac{a_1}{n_1} + \cdots + k_r \frac{a_r}{n_r}\right),$$

ahol $a_i \in \{0, 1, 2, \ldots, n_i - 1\} \quad \forall\, 1 \leq i \leq r$*-re. Megjegyezendő* $\chi = \chi_0 \;\Leftrightarrow\; a_i = 0 \quad \forall i$*-re.*

(9) *A* $\mathcal{G}$*-n definiált (különböző) karakterek száma* $|\mathcal{G}|$*.*

A 3.2 Következmény bizonyítása.

(1) $\exists\, g:\ \chi(g) \neq 0$. Ekkor

$$\chi(e)\chi(g) = \chi(eg) = \chi(g) \qquad / : \chi(g)(\neq 0)$$
$$\chi(e) = 1.$$

(2)

$$(\chi(g))^{|\mathcal{G}|} = \chi\left(g^{|\mathcal{G}|}\right) = \chi(e) = 1$$
$$\uparrow \qquad\qquad \uparrow$$
2. miatt Lagrange t.

(3) Triviális.

(4) Triviális. Megjegyzés:

$$1 = \chi(e) = \chi(gg^{-1}) = \chi(g)\chi(g^{-1}) \quad / \cdot \overline{\chi}(g)$$
$$\overline{\chi}(g) = \left(\chi(g)\overline{\chi(g)}\right)\chi(g^{-1})$$

Itt (2) miatt $\chi(g)\overline{\chi(g)} = |\chi(g)|^2 = 1$. Tehát

$$\overline{\chi}(g) = \chi(g^{-1}).$$

(5), (6) Triviális, HF.

(7) Következik (2)-ből és $\chi(g^k) = \chi(g)^k$.

(8) Ez (7) következménye.

(9) Ez (8) következménye.

További tulajdonságok

3.3 Következmények.

(10) *Ha χ a $\mathcal{G}$-n definiált csoport karakter, akkor*

$$\sum_{g\in\mathcal{G}} \chi(g) = \begin{cases} |\mathcal{G}| & \text{ha } \chi = \chi_0 \\ 0 & \text{ha } \chi \neq \chi_0. \end{cases}$$

(11) *$\forall\, g \in \mathcal{G}$ esetén*

$$\sum_{\chi} \chi(g) = \begin{cases} |\mathcal{G}| & \text{ha } g = e \\ 0 & \text{ha } g \neq e. \end{cases}$$

A 3.3 Következmény bizonyítása. (10): Legyen $\mathcal{G} = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r} = \{g_1\}_{n_1} \times \{g_2\}_{n_2} \times \cdots \times \{g_r\}_{n_r}$. Ekkor $\forall g \in \mathcal{G}$ egyértelműen felírható $g_1^{k_1} \cdots g_r^{k_r}$ alakban, ahol $0 \leq k_i < n_i$. Mivel (8) szerint $\forall\, \chi$ explicit alakja

$$\chi(g_1^{k_1} \cdots g_r^{k_r}) = e\left(k_1\frac{a_1}{n_1} + \cdots + k_r\frac{a_r}{n_r}\right),$$

ahol $a_i \in \{0, 1, \ldots, n_i - 1\}$, ezért

$$\sum_{g\in\mathcal{G}} \chi(g) = \sum_{k_1=0}^{n_1-1} \cdots \sum_{k_r=0}^{n_r} e\left(k_1\frac{a_1}{n_1} + \cdots + k_r\frac{a_r}{n_r}\right).$$

Így:

$$\sum_{g\in\mathcal{G}}\chi(g)=\left(\sum_{k_1=0}^{n_1-1}e\left(k_1\frac{a_1}{n_1}\right)\right)\cdots\left(\sum_{k_r=0}^{n_r-1}e\left(k_r\frac{a_r}{n_r}\right)\right)$$
$$=\begin{cases}n_1 & \text{ha } a_1=0\\ 0 & \text{ha } a_1\neq 0\end{cases}\cdots\begin{cases}n_r & \text{ha } a_r=0\\ 0 & \text{ha } a_r\neq 0.\end{cases}$$

Vagyis

$$\sum_{g\in\mathcal{G}}\chi(g)=\begin{cases}n_1\cdots n_r=|C_1|\cdots|C_r|=|\mathcal{G}|, & \text{ha } a_1=\cdots=a_r=0,\\ & \Leftrightarrow\ \chi=\chi_0,\\ 0, & \text{ha } \exists\, a_i\neq 0\ \Leftrightarrow\ \chi\neq\chi_0.\end{cases}$$

11 bizonyítása:

Legyen $\mathcal{G}=C_{n_1}\times\cdots\times C_{n_r}=\{g_1\}_{n_1}\times\cdots\times\{g_r\}_{n_r}$. Továbbá írjuk fel a rögzített $g\in\mathcal{G}$ elemet $g=g_1^{k_1}\cdots g_r^{k_r}$ alakban, ahol $0\leq k_i<n_i$.

Megint 8 szerint:

$$\sum_{g\in\mathcal{G}}\chi(g)=\sum_{a_1=0}^{n_1-1}\cdots\sum_{a_r=0}^{n_r}e\left(k_1\frac{a_1}{n_1}+\cdots+k_r\frac{a_r}{n_r}\right).$$

Így:

$$\sum_{\chi}\chi(g)=\left(\sum_{a_1=0}^{n_1-1}e\left(a_1\frac{k_1}{n_1}\right)\right)\cdots\left(\sum_{a_r=0}^{n_r-1}e\left(a_r\frac{k_r}{n_r}\right)\right)$$
$$=\begin{cases}n_1 & \text{ha } k_1=0\\ 0 & \text{ha } k_1\neq 0\end{cases}\cdots\begin{cases}n_r & \text{ha } k_r=0\\ 0 & \text{ha } k_r\neq 0.\end{cases}$$

Vagyis

$$\sum_{\chi}\chi(g)=\begin{cases}n_1\cdots n_r=|\mathcal{G}|, & \text{ha } k_1=\cdots=k_r=0,\ \Leftrightarrow\ g=e,\\ 0, & \text{ha } \exists\, k_i\neq 0\ \Leftrightarrow\ g\neq e.\end{cases}$$

3.4 TÉTEL. *Legyen $\mathcal{G}$ tetszőleges véges Ábel csoport, $g \in \mathcal{G}$ és $g_1, g_2, \ldots, g_t \in \mathcal{G}$ elemek (ahol $g_i = g_j$ megengedett). Ekkor*

$$|\{i : \ 1 \le i \le t, \ g_i = g\}| = \frac{1}{|\mathcal{G}|} \sum_{\chi} \overline{\chi}(g) \sum_{i=1}^{t} \chi(g_i).$$

A 3.4 Tétel bizonyítása.

$$\begin{aligned}
\sum_{\chi} \overline{\chi}(g) \sum_{i=1}^{t} \chi(g_i) &= \sum_{i=1}^{t} \left(\sum_{\chi} \overline{\chi}(g)\chi(g_i) \right) \\
&= \sum_{i=1}^{t} \left(\sum_{\chi} \chi(g^{-1})\chi(g_i) \right) \\
&= \sum_{i=1}^{t} \left(\sum_{\chi} \chi(g^{-1}g_i) \right) \\
&= \sum_{i=1}^{t} \begin{cases} |\mathcal{G}| & \text{ha } g^{-1}g = e \ \Leftrightarrow \ g_i = g \\ 0 & \text{ha } g^{-1}g \neq e \ \Leftrightarrow \ g_i \neq g \end{cases} \\
&= \sum_{\substack{1 \le i \le t \\ g_i = g}} |\mathcal{G}| \\
&= |\mathcal{G}| \cdot |\{i : \ 1 \le i \le t, \ g_i = g\}| ,
\end{aligned}$$

ahonnan $|\mathcal{G}|$-vel osztva megkapjuk a tétel állítását.

Számelméletben két fontos speciális eset:

1. $\mathcal{G} =< \mathbb{Z}_m, + >$, a $\mod m$ maradékosztályok additív csoportja $\Rightarrow$ additív karakterek.

2. $\mathcal{G} =< Z_m^*, \times >$, ahol $\mathbb{Z}_m$ redukált maradékosztályainak csoportja Z_m^*, művelet a szorzás $\Rightarrow$ multiplikatív karakterek.

4. Additív karakterek

Rögzített $m, k \in \mathbb{Z}$ esetén jelöljük a k által reprezentált modulo m maradékosztályt $\overline{k}$-val:

$$\overline{k} = \{x : \ x \in \mathbb{Z}, \ x \equiv k \pmod{m}\}.$$

Ekkor a 3.2 Következmény (7) pontja szerint a $\mathbb{Z}_m$-en definiált karakterek:

$$\Psi(\overline{k}) = e\left(k\frac{a}{m}\right),$$

ahol $a \in \{0, 1, \ldots, m-1\}$. Ezentúl az egyszerűség kedvéért a felülvonást a k-ról elhagyjuk, tehát

$$\Psi(k) = e\left(k\frac{a}{m}\right).$$

Ezeket szokás újabban additív karaktereknek hívni. Ezekre a 3.2 és 3.3 Következmények (1)-(11) pontjai kimondhatóak, pl. az utolsó tételt specializálva kapjuk:

4.1 Tétel. *Ha $\mathcal{A} \subset \mathbb{Z}$ véges, $r \in \mathbb{Z}$, $m \in \mathbb{N}$, akkor*

$$f(t) = \sum_{a \in \mathcal{A}} e(at)$$

-t írva

$$|\{a : \ a \in \mathcal{A}, \ a \equiv r \pmod{m}\}| = \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{rk}{m}\right) f\left(\frac{k}{m}\right)$$
$$= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{rk}{m}\right) \sum_{a \in \mathcal{A}} e\left(\frac{ak}{m}\right).$$

A 4.1 Tétel bizonyítása. A 3.4 Tétel szerint

$$|\{i : \ 1 \le i \le t, \ g_i = g\}| = \frac{1}{|\mathcal{G}|}\sum_{\chi} \overline{\chi}(g) \sum_{i=1}^{t} \chi(g_i). \qquad (4.1)$$

Legyen ebben a tételben $\mathcal{G} = \mathbb{Z}_m$, $g \stackrel{\text{def}}{=} r$, $\mathcal{A} = \{a_1, a_2, \ldots, a_s\}$ (azaz $t = s$), $g_i \stackrel{\text{def}}{=} a_i$.

Ekkor ha χ karakter $\mathcal{G} = \mathbb{Z}_m$-en, akkor

$$\chi(1) = e\left(\frac{k}{m}\right),$$

ahol $0 \leq k \leq m-1$. Ekkor (4.1) alapján

$$\begin{aligned}
|\{a:\ a \in \mathcal{A},\ a \equiv r \pmod m\}| &= \frac{1}{m}\sum_{\chi}\overline{\chi}(r)\sum_{i=1}^{s}\chi(a_i) \\
&= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{kr}{m}\right)\sum_{i=1}^{s} e\left(\frac{ka_i}{m}\right) \\
&= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{kr}{m}\right)\sum_{a\in\mathcal{A}} e\left(\frac{ka}{m}\right) \\
&= \frac{1}{m}\sum_{k=0}^{m-1} e\left(-\frac{rk}{m}\right) f\left(\frac{k}{m}\right).
\end{aligned}$$

A 4.1 Tételben $f(t)$ az $\mathcal{A}$ halmaznak generátorfüggvénye, továbbá hívjuk még Fourier transzformáltnak is.

Most derül ki, hogy miért olyan fontos a számelméletben az $e(\alpha)$ függvény:

$e(\alpha)$ periodikus egy periódussal. Így $e\left(\frac{n}{m}\right)$ csak az n elem mod m maradék osztályától függ.

$e\left(a\frac{k}{m}\right)$ fix k-ra és m-re csak az a elem mod m maradék osztályától függ.

Tehát, ha az $\mathcal{A}$ sorozat $f(t) = f_{\mathcal{A}}(t)$ generátorfüggvényét (Fourier transzformáltját) tudjuk uralni, akkor a maradék osztályokban való eloszlása uralható.

Ezt az elvet fordított irányban is alkalmazhatjuk. Ismert eloszlás a maradék osztályokban $\Rightarrow f(t)$ generátorfüggvény kontrollja $\Rightarrow \mathcal{A}$ más aritmetikai tulajdonságai is vizsgálhatók.

Erre épül az additív karakterek alkalmazhatósága.

Persze a tételben szereplő formula direkt karakterekre való hivatkozás nélkül is kiszámolható lenne, de így jobban látszik.

4.1. Alkalmazások

4.2 TÉTEL. *Ha $\ell \in \mathbb{N}$, $f(x_1, \dots, x_\ell) \in \mathbb{Z}[x_1, \dots, x_\ell]$, akkor az*

$$f(x_1, \dots, x_\ell) \equiv 0 \pmod{p}$$

kongruencia megoldásszáma

$$N = \frac{1}{m} \sum_{k=0}^{m-1} \sum_{t_1=0}^{m-1} \cdots \sum_{t_\ell=0}^{m-1} e\left(f(t_1, \dots, t_\ell) \frac{k}{m} \right).$$

A 4.2 Tétel bizonyítása. Az előző tétel $r = 0$-val és

$$\mathcal{A} = \{ f(t_1, \dots, t_\ell) : \ (t_1, \dots, t_\ell) \in \{0, 1, \dots, m-1\}^\ell \}$$

-val. Ekkor

$$\begin{aligned} N = |\, \{ f(t_1, \dots, t_\ell) : \quad & (t_1, \dots, t_\ell) \in \{0, 1, \dots, m-1\}^\ell, \\ & f(t_1, \dots, t_\ell) \equiv 0 \pmod{m} \}\, | \\ = \frac{1}{m} \sum_{k=0}^{m-1} e\left(-\frac{0 \cdot k}{m} \right) & \sum_{t_1=0}^{m-1} \cdots \sum_{t_\ell=0}^{m-1} e\left(f(t_1, \dots, t_\ell) \frac{k}{m} \right). \end{aligned}$$

Itt $e\left(-\frac{0 \cdot k}{m}\right) = 1$, s ezzel megkaptuk a tétel állítását.

Lineáris kongruenciára specializálva:

4.3 TÉTEL. *Legyen* $\ell \in \mathbb{N}$, $a_1, a_2, \ldots, a_\ell, b \in \mathbb{Z}$ *és*

$$d \overset{\text{def}}{=} (a_1, a_2, \ldots, a_\ell, m).$$

Ekkor az

$$a_1 x_1 + \cdots + a_\ell x_\ell \equiv b \pmod{m}$$

kongruencia megoldásszáma:

$$N = \begin{cases} m^{\ell-1} d, & \text{ha } d \mid b \\ 0, & \text{ha } d \nmid b. \end{cases}$$

Megjegyzés. $\ell = 1$-re az $ax \equiv b \pmod{m}$ megoldására valóban azt kapjuk, hogy

$$N = \begin{cases} d = (a, m), & \text{ha } d \mid b \\ 0, & \text{ha } d \nmid b. \end{cases}$$

A 4.3 Tétel bizonyítása. Előző tétel $f(x_1, \ldots, x_\ell) = a_1 x_1 + \cdots + a_\ell x_\ell - b$-vel:

$$\begin{aligned} N &= \frac{1}{m} \sum_{k=0}^{m-1} \sum_{t_1=0}^{m-1} \cdots \sum_{t_\ell=0}^{m-1} e\left((a_1 t_1 + \cdots + a_\ell t_\ell - b) \frac{k}{m} \right) \\ &= \frac{1}{m} \sum_{k=0}^{m-1} e\left(-b\frac{k}{m}\right) \left(\sum_{t_1=0}^{m-1} e\left(a_1 t_1 \frac{k}{m}\right) \right) \ldots \left(\sum_{t_\ell=0}^{m-1} e\left(a_\ell t_\ell \frac{k}{m}\right) \right) \\ &\qquad \begin{cases} m, & \text{ha } m \mid a_1 k \\ 0, & \text{ha } m \nmid a_1 k \end{cases} \cdots \begin{cases} m, & \text{ha } m \mid a_\ell k \\ 0, & \text{ha } m \nmid a_\ell k \end{cases} \\ &= \frac{1}{m} \sum_{\substack{0 \le k < m \\ m \mid (a_1 k, \ldots, a_\ell k)}} e\left(-b\frac{k}{m}\right) m^\ell \\ &= \frac{1}{m} \sum_{\substack{0 \le k < m \\ m \mid (a_1, \ldots, a_\ell) k}} e\left(-b\frac{k}{m}\right) m^\ell. \end{aligned}$$

Legyen $d \stackrel{\text{def}}{=} (a_1, \ldots, a_\ell, m)$, továbbá $m = m^* d$, $(a_1, \ldots, a_\ell) = a^* d$, ahol $(m^*, a^*) = 1$.

Az utolsó szumma indexében $m \mid (a_1, \ldots, a_\ell)k$ szerepel, ezt elemezzük most kicsit:

$$\begin{aligned} m \mid (a_1, \ldots, a_\ell)k &\Leftrightarrow m^* d \mid a^* dk \\ &\Leftrightarrow m^* \mid a^* k \end{aligned}$$

ahol $(m^*, a^*) = 1$ miatt

$$\Leftrightarrow m^* \mid k.$$

Ezért a szumma indexében írhatunk $k = m^* t$-t, ahol t fut a $0, 1, \ldots, \frac{m}{m^*} - 1$ számokon, azaz a $0, 1, \ldots, d-1$ számokon. Ekkor $\frac{k}{m} = \frac{m^* t}{m^* d} = \frac{t}{d}$. Tehát

$$\begin{aligned} N &= \frac{1}{m} \sum_{t=0}^{d-1} e\left(-b\frac{t}{d}\right) m^\ell \\ &= \begin{cases} m^{\ell-1} d, & \text{ha } d \mid b \\ 0, & \text{ha } d \nmid b. \end{cases} \end{aligned}$$

Ezzel a tétel bizonyítását befejeztük.

Eddig olyan exponenciális összegeket néztünk, ahol a kitevő a változónak lineáris függvénye, azaz

$$e((r(n)),$$

ahol $r(n)$ az n-nek elsőfokú polinomja. A következő lépés, amikor másodfokú polinom van a kitevőben. Ezt az esetet a következő fejezetben nézzük meg.

5. Gauss összegek

5.1 Definíció. *Legyen* $m \in \mathbb{N},\ a \in \mathbb{Z}$. *Ekkor*

$$S(a,m) = \sum_{x=0}^{m-1} e\left(x^2 \frac{a}{m}\right)$$

összeget Gauss összegnek nevezzük.

5.2 Tétel. *Ha* $p > 2$ *prím,* $(a,p) = 1$, *akkor*

$$S(a,p) = \begin{cases} \pm\sqrt{p}, & \text{ha } p \equiv 1 \pmod 4 \\ \pm i\sqrt{p}, & \text{ha } p \equiv 3 \pmod 4 \end{cases}$$

Tehát $|S(a,p)| = \sqrt{p}$.

Az 5.2 Tétel bizonyítása. Először csak $|S(a,p)|$-t határozzuk meg.

$$\begin{aligned} |S(a,p)|^2 &= S(a,p)\overline{S(a,p)} \\ &= \sum_{x=0}^{p-1} e\left(x^2\frac{a}{p}\right) \sum_{y=0}^{p-1} e\left(-y^2\frac{a}{p}\right) \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e\left((x^2-y^2)\frac{a}{p}\right) \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e\left((x-y)(x+y)\frac{a}{p}\right). \end{aligned}$$

Most $x-y$ értéke szerint vezetünk be új változókat. Legyen

$$x - y \equiv t \pmod p,$$

ahol $0 \le t \le p-1$ feltehető. Most csak $x - y \equiv t \pmod p$ maradéka számít. Eredetileg a szummák x, y-n futnak. Az új változók: t, y. Így:

$$|S(a,p)|^2 = \sum_{t=0}^{p-1}\sum_{y=0}^{p-1} e\left(\frac{t(t+2y)a}{p}\right)$$

$$= \sum_{t=0}^{p-1} \sum_{y=0}^{p-1} e\left(\frac{t^2 a}{p}\right) e\left(\frac{2tya}{p}\right)$$
$$= \sum_{t=0}^{p-1} e\left(\frac{t^2 a}{p}\right) \sum_{y=0}^{p-1} e\left(\frac{2tya}{p}\right)$$
$$\begin{cases} 0, & \text{ha } p \nmid 2at, \text{ azaz } t > 0 \\ p, & \text{ha } p \mid 2at, \text{ azaz } t = 0. \end{cases}$$
$$= 1 \cdot p.$$

Ebből

$$S(a,p) = \sqrt{p}.$$

Ha $p \equiv 1 \pmod 4$, akkor -1 kvadratikus maradék. Azaz az összes kvadratikus maradékot kétszer soroljuk fel az alábbi kongruencia bal és jobboldalán:

$$\{1^2, 2^2, \ldots, (p-1)^2\} \equiv \{-1^2, -2^2, \ldots, -(p-1)^2\} \pmod p.$$

Így:

$$\overline{S(a,p)} = \overline{\sum_{x=0}^{p-1} e\left(x^2 \frac{a}{p}\right)}$$
$$= \sum_{x=0}^{p-1} e\left(-x^2 \frac{a}{p}\right)$$
$$= S(a,p).$$

Azaz $S(a,p)$ valós, abszolút értéke $\sqrt{p}$. Tehát $S(a,p) = \pm\sqrt{p}$.

Ha $p \equiv 3 \pmod 4$:

$$S(a,p) + \overline{S(a,p)} = \sum_{x=0}^{p-1} e\left(x^2\frac{a}{p}\right) + \sum_{y=0}^{p-1} e\left(-y^2\frac{a}{p}\right)$$

$$\uparrow \qquad\qquad \uparrow$$

kvadratikus maradékok $2\times$ és a 0 $1\times$ — kvadratikus nem-maradékok $2\times$ és a 0 $1\times$

$$= 2\sum_{z=0}^{p-1} e\left(z\frac{a}{p}\right)$$

$$= 0.$$

Azaz $\operatorname{Re} S(a,p) = 0$, de mivel $|S(a,p)| = \sqrt{p}$, így

$$S(a,p) = \pm i\sqrt{p}.$$

5.3 Tétel. *Ha $(a,p) = 1$, akkor*

$$S(a,p) = \left(\frac{a}{p}\right) S(1,p).$$

A 5.3 Tétel bizonyítása. A következő lemmát használjuk.

5.4 Lemma. *$a, b \in \mathbb{Z}_p^*$ esetén*

$$S(ab^2,p) = S(a,p).$$

A 5.4 Lemma bizonyítása. Valóban

$$S(a,p) = \sum_{x=0}^{p-1} e_p(ax^2) = \sum_{x=0}^{p-1} e(\frac{a}{p}x^2).$$

Amint x fut $\mathbb{Z}_p$-n, nyilván bx is fut $\mathbb{Z}_p$-n ezért

$$\begin{aligned} S(a,p) &= \sum_{x=0}^{p-1} e_p(a(bx)^2) \\ &= \sum_{x=0}^{p-1} e_p(ab^2x^2) \\ &= S(ab^2,p), \end{aligned}$$

ami éppen a lemma állítása.

Fixáljunk egy n kvadratikus nem-maradékot mod p. A lemma alapján:

$$S(a,p) = S(1,p),$$

ha a kvadratikus maradék. Ebből:

$$S(a,p) = \left(\frac{a}{p}\right) S(1,p)$$

azonnal következik, ha $\left(\frac{a}{p}\right) = 1$. Hiányzik a $\left(\frac{a}{p}\right) = -1$ eset. Szintén a lemma alapján:

$$S(a,p) = S(n,p),$$

ha a kvadratikus nem-maradék. Vizsgáljuk a

$$\sum_{a=0}^{p-1} S(a,p)$$

összeget. Egyrészt ez

$$S(0,p) + \frac{p-1}{2} S(1,p) + \frac{p-1}{2} S(n,p),$$

mivel $\frac{p-1}{2}$ kvadratikus maradék és $\frac{p-1}{2}$ kvadratikus nem-maradék létezik. Másrészt:

$$\sum_{a=0}^{p-1} S(a,p) = \sum_{a=0}^{p-1} \sum_{x=0}^{p-1} e_p(ax^2)$$

$$= \sum_{x=0}^{p-1} \underbrace{\sum_{a=0}^{p-1} e_p(ax^2)}_{\substack{\text{Ez 0 kivéve } x=0 \\ \text{esetet, amikor } p}}$$

$$= p.$$

Vagyis:

$$\underbrace{S(0,p)}_{\text{Ez } p} + \frac{p-1}{2} S(1,p) + \frac{p-1}{2} S(n,p) = p.$$

Ebből

$$S(n,p) = -S(1,p)$$

$$S(n,p) = \left(\frac{n}{p}\right) S(1,p).$$

Azaz $\left(\frac{a}{p}\right) = -1$ esetén is

$$S(a,p) = S(n,p) = -S(1,p) = \left(\frac{a}{p}\right) S(1,p)$$

teljesül.

A következő tétel megtalálható pl. a „kis” Vinogradov könyvben [6, 67. oldal, 11b β feladat]. Itt most nem bizonyítjuk.

5.5 TÉTEL. *$m > 2$, $(a,m) = 1$ esetén*

1.

$$|S(a,m)| = \begin{cases} \sqrt{m}, & \text{ha } m \equiv 1 \pmod 2 \\ 0, & \text{ha } m \equiv 2 \pmod 4 \\ \sqrt{2m}, & \text{ha } m \equiv 0 \pmod 4. \end{cases}$$

2.

$$S(1,m) = \begin{cases} (1+i)\sqrt{m}, & \text{ha } m \equiv 0 \pmod 4 \\ \sqrt{m}, & \text{ha } m \equiv 1 \pmod 4 \\ 0, & \text{ha } m \equiv 2 \pmod 4 \\ i\sqrt{m}, & \text{ha } m \equiv 3 \pmod 4. \end{cases}$$

Példaként tekintsük a következőt:

5.6 Tétel. *Az* $x^2+y^2 \equiv a \pmod{p}$ *kongruencia megoldásszáma*

$$N = \begin{cases} 2p-1, & \text{ha } a \equiv 0 \pmod{p},\ p \equiv 1 \pmod{4} \\ p-1, & \text{ha } a \not\equiv 0 \pmod{p},\ p \equiv 1 \pmod{4} \\ 1, & \text{ha } a \equiv 0 \pmod{p},\ p \equiv -1 \pmod{4} \\ p+1, & \text{ha } a \not\equiv 0 \pmod{p},\ p \equiv -1 \pmod{4} \end{cases}$$

Az 5.6 Tétel bizonyítása. Az $f(x_1,\dots,x_\ell) \equiv 0 \pmod{m}$ megoldásszámára a tanult tétel miatt

$$\begin{aligned} N &= \frac{1}{p}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\sum_{k=0}^{p-1} e\left((x^2+y^2-a)\frac{k}{p}\right) \\ &= \frac{1}{p}\sum_{k=0}^{p-1} e\left(-a\frac{k}{p}\right)\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e\left((x^2+y^2)\frac{k}{p}\right). \end{aligned}$$

A $k=0$ tagot különvéve:

$$N = \frac{1}{p^2}\cdot p^2 + \frac{1}{p}\underbrace{\sum_{k=1}^{p-1} S(k,p)^2}$$

Ez $\begin{cases} p, & \text{ha } p \equiv 1 \pmod{4} \\ -p, & \text{ha } p \equiv -1 \pmod{4} \end{cases}$

$$= \delta_p \cdot p, \text{ ahol } \delta_p = \begin{cases} 1 & \text{ha } p \equiv 1 \pmod{4} \\ -1 & \text{ha } p \equiv -1 \pmod{4}. \end{cases}$$

Így:

$$\begin{aligned} N &= p + \delta_p \sum_{k=1}^{p-1} e\left(-a\frac{k}{p}\right) \\ &= p + \delta_p \cdot \begin{cases} p-1, & \text{ha } a = 0 \\ -1, & \text{ha } a \neq 0 \end{cases} \end{aligned}$$

$$= \begin{cases} p + (p-1) = 2p - 1, & \text{ha } a \equiv 0 \pmod{p},\ p \equiv 1 \pmod{4} \\ p + 1 \cdot (-1) = p - 1, & \text{ha } a \not\equiv 0 \pmod{p},\ p \equiv 1 \pmod{4} \\ p - (p-1) = 1, & \text{ha } a \equiv 0 \pmod{p},\ p \equiv -1 \pmod{4} \\ p - 1 \cdot (-1) = p + 1, & \text{ha } a \not\equiv 0 \pmod{p},\ p \equiv -1 \pmod{4}. \end{cases}$$

5.7 KÖVETKEZMÉNY. *Bármely p prímre $\exists\, a, b \in \mathbb{Z}$ úgy, hogy*

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

Ez kellett a négynégyzetszám-tétel bizonyítása során.

Az 5.7 Következmény bizonyítása. Az

$$x^2 + y^2 \equiv -1 \pmod{p}$$

kongruencia megoldhatóságát állítjuk. Ez $p = 2$-re triviálisan megoldható ($x = 0,\ y = 1$ megoldás). Ha $p > 2$, akkor a tanult tétel szerint a megoldások száma:

$$N = \begin{cases} p - 1 > 0 & \text{ha } p \equiv 1 \pmod{4} \\ p + 1 > 0 & \text{ha } p \equiv -1 \pmod{4}. \end{cases}$$

6. A Vinogradov lemma

A következőkben egy rendkívül fontos, additív karakterekre vonatkozó egyenlőtlenségről lesz szó.

Roth a Vinogradov könyv [2] könyv előszavában írja, hogy Vinogradov módszerének a lényege az, hogy a kérdéses problémát

$$\sum_u \sum_v e(\alpha uv)$$

típusú összegek becslésére redukálja, és ilyen összegek becslésére van egy egyszerű technikája. Az első lépés ilyen irányban:

6.1 LEMMA. (Vinogradov) *Legyen* $(a,q)=1$, $q>1$ *és*

$$S \stackrel{\text{def}}{=} \sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \xi(x)\eta(y)e\left(xy\frac{a}{q}\right)$$

(azaz $\Psi(n) = e\left(\frac{a}{q}n\right) \mod q$ *additív karaktert írva,* $S = \sum_x \sum_y \xi(x)\eta(y)\Psi(xy)$*), és legyen*

$$\sum_{x=0}^{q-1} |\xi(x)|^2 = X_0, \qquad \sum_{y=0}^{q-1} |\eta(y)|^2 = Y_0.$$

Ekkor

$$|S| \le (X_0 Y_0 q)^{1/2}.$$

A 6.1 Lemma bizonyítása. A Cauchy-Schwarz egyenlőtlenség szerint:

$$|S|^2 = \left|\sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \xi(x)\eta(y)e\left(xy\frac{a}{q}\right)\right|$$
$$= \left|\sum_{x=0}^{q-1} \underbrace{\xi(x)}_{a(x)} \underbrace{\sum_{y=0}^{q-1} \eta(y)e\left(xy\frac{a}{q}\right)}_{b(x)}\right|$$

$$\leq \underbrace{\left(\sum_{x=0}^{q-1}|\xi(x)|^2\right)}_{X_0} \cdot \underbrace{\left(\sum_{x=0}^{q-1}\left|\sum_{y=0}^{q-1}\eta(x)e\left(xy\frac{a}{q}\right)\right|^2\right)}_{\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}\eta(y)e\left(xy\frac{a}{q}\right)\sum_{y'=0}^{q-1}\overline{\eta(y')}e\left(-xy'\frac{a}{q}.\right)}$$

Azaz

$$|S|^2 \leq X_0 \sum_{y=0}^{q-1}\sum_{y'=0}^{q-1}\eta(y)\overline{\eta(y')}\underbrace{\sum_{x=0}^{q-1}e\left(\frac{x(y-y')a}{q}\right)}_{=\begin{cases} q, & \text{ha } q \mid (y-y')a \Leftrightarrow y=y' \\ 0, & \text{ha } y \neq y' \end{cases}}$$

$$= X_0 \sum_{y=0}^{q-1}\sum_{y'=0}^{q-1}\eta(y)\overline{\eta(y')}q$$

$$= X_0 Y_0 q.$$

Ebből:

$$|S| \leq (X_0 Y_0 q)^{1/2}.$$

A következőkben egy alkalmazásról lesz szó. Ha $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ nagy, akkor az

$$a+b=cd, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}$$

egyenlet megoldható $\mathbb{Z}_p$-ben.

6.2 Tétel. (Sárközy [1], 2005) *Ha p prím, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ és az*

$$a+b=cd, \qquad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \tag{6.1}$$

megoldásszámát N-nel jelöljük, akkor

$$\left|N - \frac{|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|\cdot|\mathcal{D}|}{p}\right| \leq (|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|\cdot|\mathcal{D}|)^{1/2}\, p^{1/2}.$$

6.3 KÖVETKEZMÉNY. *Ha p prím, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ és*

$$|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}| > p^3, \tag{6.2}$$

akkor (6.1) *megoldható.*

Megjegyzés. A következmény, azaz (6.2) a lehető legjobb konstansszorzótól eltekintve: ha $\mathcal{A} = \mathcal{B} = \{n : 1 \leq n < p/2\}$, $\mathcal{C} = \mathbb{Z}_p$, $\mathcal{D} = \{0\}$, akkor

$$|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}| = \left(\frac{1}{4} + o(1)\right) p^3,$$

és (6.1) nem oldható meg.

A tétel nem terjeszthető ki prímmodulusról összetettre, azaz $\mathbb{Z}_p$-ről $\mathbb{Z}_m$-re: Ha $m = 2k$, $\mathcal{A} = \mathcal{C} = \{2, 4, \ldots, 2k\}$, $\mathcal{B} = \{1, 3, \ldots, 2k-1\}$, $\mathcal{D} = \mathbb{Z}_m$, akkor

$$|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}| = \left(\frac{1}{8} + o(1)\right) m^4,$$

és (6.1) nem oldható meg.

Sok érdekes következmény, pl.:

$$\mathcal{C} = \mathcal{D} = \{x^k : \ x \in \mathbb{Z}_p^*\}\text{-t}$$

véve

$$\{cd : \ c \in \mathcal{C}, \ d \in \mathcal{D}\} = \{z^k : \ z \in \mathbb{Z}_p^*\},$$

azaz $|\mathcal{A}| \cdot |\mathcal{B}| \geq \left(k^2 + o(1)\right) p$ esetén

$$a + b = x^k \qquad a \in \mathcal{A}, \ b \in \mathcal{B}$$

megoldható.

Így ha például, $\mathcal{A} = \{x^m : x \in \mathbb{Z}_p^*\}$, $\mathcal{B} = \{y^n : y \in \mathbb{Z}_p^*\}$, akkor azt kapjuk, hogy

$$x^m + y^n \equiv z^k \pmod{p}, \qquad xyz \not\equiv 0 \pmod{p}$$

megoldható. Speciálisan $x^n + y^n \equiv z^n \pmod{p}$, $xyz \not\equiv 0 \pmod{p}$ is (ez a Fermat-kongruencia).

Fontos még az alábbi következmények is: ha $\mathcal{C} = \mathcal{D} = \{z^2 : z \in \mathbb{Z}_p^*\}$ és $|\mathcal{A}| \cdot |\mathcal{B}| \geq (4 + o(1))p$, akkor

$$\left(\frac{a+b}{p}\right) = 1, \qquad a \in \mathcal{A},\ b \in \mathcal{B}$$

megoldható. Ebből persze az is következik, hogy ha $|\mathcal{A}| \cdot |\mathcal{B}| \geq (4 + o(1))p$, akkor

$$\left(\frac{a+b}{p}\right) = -1, \qquad a \in \mathcal{A},\ b \in \mathcal{B}$$

is megoldható. Sőt, összefügg a legkisebb kvadratikus nemmaradék problémájával.

A 6.2 Tétel bizonyítása. Legyen $F(a,b,c,d) = a + b - cd$. Ekkor

$$F(a,b,c,d) = a + b - cd \equiv 0 \pmod{p},$$

$a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}$ megoldásszáma a 4.2 Tétel alapján

$$N = \frac{1}{p} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{c\in\mathcal{C}} \sum_{d\in\mathcal{D}} \underbrace{\sum_{k=0}^{p-1} e\left((a+b-cd)\frac{k}{p}\right)}_{\begin{cases} p, & \text{ha } a,b,c,d \text{ megoldás} \\ 0, & \text{ha } a,b,c,d \text{ nem megoldás.} \end{cases}}$$

Rendszerint a főkarakter $k = 0$ adja a főtagot, a többi csak hiba. Ezért ezt különvesszük:

$$N = \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p} + \frac{1}{p} \sum_{k=1}^{p-1} \sum_{a \in \mathcal{A}} e\left(a\frac{k}{p}\right) \sum_{b \in \mathcal{B}} e\left(b\frac{k}{p}\right) \sum_{c \in \mathcal{C}} \sum_{d \in \mathcal{D}} e\left(-cd\frac{k}{p}\right).$$

Így

$$\left|N - \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p}\right| \leq \frac{1}{p} \sum_{k=1}^{p-1} \left|\sum_{a \in \mathcal{A}} e\left(a\frac{k}{p}\right)\right| \left|\sum_{b \in \mathcal{B}} e\left(b\frac{k}{p}\right)\right| \left|\sum_{c \in \mathcal{C}} \sum_{d \in \mathcal{D}} e\left(-cd\frac{k}{p}\right)\right|.$$

Itt a Vinogradov lemma miatt (ld. 6.1 Lemma):

$$\left|\sum_{c \in \mathcal{C}} \sum_{d \in \mathcal{D}} e\left(-cd\frac{k}{p}\right)\right| \leq (|\mathcal{C}||\mathcal{D}|p)^{1/2}.$$

Azaz

$$\left|N - \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p}\right| \leq \frac{1}{p^{1/2}} (|\mathcal{C}||\mathcal{D}|)^{1/2} \underbrace{\sum_{k=1}^{p-1} \left|\sum_{a \in \mathcal{A}} e\left(a\frac{k}{p}\right)\right| \left|\sum_{b \in \mathcal{B}} e\left(b\frac{k}{p}\right)\right|}_{\text{Cauchy-Schwarz}}$$

$$\leq \frac{1}{p^{1/2}} (|\mathcal{C}||\mathcal{D}|)^{1/2} \left(\sum_{k=1}^{p-1} \left|\sum_{a \in \mathcal{A}} e\left(a\frac{k}{p}\right)\right|^2\right)^{1/2} \left(\sum_{k=1}^{p-1} \left|\sum_{b \in \mathcal{B}} e\left(b\frac{k}{p}\right)\right|^2\right)^{1/2}$$

Tudjuk, hogy $F(\alpha) = \sum_{j=0}^{p-1} a_j e(j\alpha)$ esetén

$$\sum_{k=0}^{p-1} \left|F\left(\frac{k}{p}\right)\right|^2 = p \sum_{k=0}^{p-1} |a_k|^2. \tag{6.3}$$

(Parseval típusú egyenlőség, HF.) Így:

$$\left|N - \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p}\right| \leq \frac{1}{p^{1/2}} \left(|\mathcal{C}||\mathcal{D}|\right)^{1/2} \left(p|\mathcal{A}|\right)^{1/2} \left(p|\mathcal{B}|\right)^{1/2}$$
$$= p^{1/2} \left(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|\right)^{1/2}.$$

A 6.3 Következmény bizonyítása.

$$N \geq \frac{|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|}{p} - p^{1/2} \left(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|\right)^{1/2}$$
$$= p^{1/2} \left(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|\right)^{1/2} \left(\frac{\left(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{C}| \cdot |\mathcal{D}|\right)^{1/2}}{p^{3/2}} - 1\right)$$
$$> 0.$$

Hivatkozások

[1] A. Sárközy, *On sums and products of residues modulo p*, Acta Arith. 118 (4) (2005), 403-409.

[2] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Dover Publications, Revised edition 2004.

7. Weyl összegek és Weil tétel

Volt

$$\underbrace{\left|\sum_{x=0}^{p-1} e\left(\frac{ax^2}{p}\right)\right|}_{\text{Gauss összeg}} = \sqrt{p}$$

A bizonyítás módszerével:

$$\begin{aligned}\left|\sum_x e\left(\frac{f(x)}{p}\right)\right|^2 &= \sum_x e\left(\frac{f(x)}{p}\right)\overline{\sum_y e\left(\frac{f(y)}{p}\right)} \\ &= \sum_x \sum_y e\left(\underbrace{(f(x)-f(y))}_{\underbrace{(x-y)}_{t}\, g(x,y)}/p\right) \\ &= \sum_t \sum_y e\left(tg(t+y,y)/p\right),\end{aligned}$$

itt $g(t+x,y)$ foka y-ban eggyel kisebb mint f foka, s ezzel eggyel kisebb fokú polinomokra redukáltuk a becslést. A $\sum_{x=M}^{N} e\left(f(x)\right)$ típusú összegeket Weyl összegeknek nevezzük.

Ezzel az ötlettel Weyl [3] pl. a következőt igazolta:

7.1 Tétel. *Ha M, N, a és q egész számok, ahol $(a,q)=1$, $q>0$ és f valós együtthatós k-adfokú polinom, amelynek a_k főegyütthatójára teljesül az*

$$\left|a_k - \frac{a}{q}\right| \leq \frac{t}{q^2},$$

egyenlőtlenség valamilyen $t \geq 1$-gyel, akkor $\forall\ \varepsilon > 0$-ra igaz lesz, hogy

$$\sum_{x=M}^{M+N} e(f(x)) = O\left(N^{1+\varepsilon}\left(\frac{t}{q}+\frac{1}{N}+\frac{t}{N^{k-1}}+\frac{q}{N^k}\right)^{2^{1-k}}\right)$$

amint $N \to \infty$.

A fenti becslés csak akkor nem triviális, ha $q < N^k$.

Van egy másik kapcsolódó általános tétel:

7.2 TÉTEL. (Weil [2], 1941) *Legyen* p *prím,* $f(x) \in \mathbb{F}_p[x]$, d*-edfokú polinom, ahol* $1 \leq d < p$. *Ekkor*

$$\left| \sum_{x=0}^{p-1} e\left(\frac{f(x)}{p}\right) \right| \leq (d-1)\sqrt{p}.$$

Pontos: ha $f(x) = x^2$.

Nem bizonyítjuk a tételt, nagyon mély algebrai geometriával. (Később: Sztyepanov + Schmidt [1] elemileg, de hosszasan.)

Hivatkozások

[1] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Mathematics, Vol. 536, Springer, 2006.

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

[3] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Ann. 77 (1916).

8. Erdős és Moser problémája

Még egy illusztráció. Diophantosz kérdezte a következőt:

Hány $a_1, a_2, \ldots, a_t$ egész szám adható meg úgy, hogy $a_i a_j + 1$ mindig négyzetszám, ha $i \neq j$?

Euler, Fermat, Dujella és sokan mások dolgoztak a problémán (én is).

Erdős, illetve Moser kérdezték az alábbi problémát egymástól függetlenül 1963-ban:

Legyen $\mathcal{A} = \{a_1, a_2, \ldots, a_t\}$ olyan, hogy

$$a_i + a_j$$

mindig négyzetszám, ha $i \neq j$. (Különböző a_i-k összege mindig négyzetszám.) Mekkora lehet t? Lehet-e tetszőlegesen nagy?

Megjegyzés: az, hogy i és j különböző azért kell, mert különben

$$a_i + a_i = 2a_i = n^2$$
$$a_i = \frac{n^2}{2}$$

esetén túl erős, tulajdonképpen pitagoraszi számhármas-szerű problémát kapnánk. Lagrange [4] és Nicolas [5] példát adott meg $t = 6$-tal:

$$\mathcal{A} = \{-15863902, 17798783, 21126338, 49064546, 82221218, 447422978\}.$$

Azóta sincs másik példa $t = 6$-tal.

Lehetséges, hogy $\max t = 6$, és nagyon valószínű, hogy $\max t = O(1)$, de ez reménytelennek tűnik. Ezért inkább az $[1, x]$ intervallumbeli halmazok esetén x függvényében becsüljük t értékét.

8.1 Tétel. (Rivat, Stewart, Sárközy [6]) *Létezik egy x_0 egész szám, hogyha $x_0 < x \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, 3, \dots, x\}$, és tudjuk, hogy $a, a' \in \mathcal{A}$ esetén $a + a'$ mindig négyzetszám, akkor*

$$|\mathcal{A}| < 37 \log x.$$

A 8.1 Tétel bizonyítása. Most itt a lemma, ami a lényeges rész, a többi könnyű (szita alkalmazása)... Tehát a lemma, ami talán független érdekességű:

8.2 Lemma. *Ha p prím, $p > 2$, $\mathcal{B} \subseteq \mathbb{Z}_p$ és $b, b' \in \mathcal{B}$, $b \not\equiv b' \pmod p$ esetén*

$$\left(\frac{b + b'}{p}\right) = 1 \quad \textit{vagy} \quad b + b' \equiv 0 \pmod p,$$

akkor

$$|\mathcal{B}| \leq 6\sqrt{p}.$$

Mielőtt bebizonyítanánk, ez miért visz előbbre?

Tekintsünk egy „jó” $\mathcal{A}$ sorozatot. Ha $a, a' \in \mathcal{A}$, $a \neq a'$, akkor

$$a + a' = n^2,$$

vagyis

$$\left(\frac{a + a'}{p}\right) = 1 \quad \textit{vagy} \quad a + a' \equiv 0 \pmod p,$$

Így a lemma miatt $\forall\ p$-re csak kevés $< 6p^{1/2}$ maradékosztályban helyezkedik el.

Ebből szitával kijön, hogy $\mathcal{A} \subseteq \{1, 2, \dots, x\}$ „ritka” ($|\mathcal{A}|$ „kicsi”) x függvényében.

A 8.2 Lemma kijön Sárközy tételéből (6.2 Tétel) is, de most lássuk az eredeti bizonyítást.

A 8.2 Lemma bizonyítása. Legyen

$$\mathcal{G}(h,p) = \sum_{x=0}^{p-1} e\left(\frac{hx^2}{p}\right) \quad \text{(Gauss összeg)}$$

$$\mathcal{G}_0 = \mathcal{G}(1,p), \qquad |\mathcal{G}_0| = \sqrt{p}.$$

Ekkor az 5.3 Tétel miatt

$$\mathcal{G}(h,p) = \left(\frac{h}{p}\right)\mathcal{G}(1,p), \qquad \text{ha } (h,p)=1.$$

Szóval

$$\mathcal{G}(h,p) = \begin{cases} \mathcal{G}_0, & \text{ha } \left(\frac{h}{p}\right) = 1 \\ -\mathcal{G}_0, & \text{ha } \left(\frac{h}{p}\right) = -1 \\ p, & \text{ha } p \mid h. \end{cases} \tag{8.1}$$

Tekintsük most

$$S \stackrel{\text{def}}{=} \sum_{x=0}^{p-1} \left(\sum_{b\in\mathcal{B}} e\left(\frac{bx^2}{p}\right)\right)^2.$$

Ekkor $|S|$-re alsó felső becslést adva adódik a lemma állítása.

Először nézzük az alsó becslést.

$$\begin{aligned} |S| &= \left| \sum_{x=0}^{p-1} \sum_{b\in\mathcal{B}} \sum_{b'\in\mathcal{B}} e\left(\frac{(b+b')x^2}{p}\right)\right| \\ &= \left| \sum_{b\in\mathcal{B}} \sum_{b'\in\mathcal{B}} \mathcal{G}(b+b',p)\right| \\ &= \left| \sum_{b\in\mathcal{B}} \sum_{b'\in\mathcal{B}} \mathcal{G}_0 + \sum_{b\in\mathcal{B}} \sum_{b'\in\mathcal{B}} (G(b+b',p) - \mathcal{G}_0)\right| \end{aligned}$$

Itt a második tagban $\mathcal{G}(b+b',p)-\mathcal{G}_0$ majdnem mindig 0, hiszen $b+b'$ különböző b,b'-kre kvadratikus maradék vagy 0, és itt használhatjuk (8.1)-t. Kivételt jelent, ha $b\equiv b' \pmod p$ vagy $p\mid b+b'$.

Így a háromszög-egyenlőtlenség alapján:

$$\begin{aligned}
|S| &\geq |\mathcal{B}|^2\,|\mathcal{G}_0| - \sum_{b\in\mathcal{B}} |\mathcal{G}(2b,p)-\mathcal{G}_0| - \sum_{\substack{b,b'\in\mathcal{B},b\neq b'\\ p\mid b+b'}} |\mathcal{G}(0,p)-\mathcal{G}_0| \\
&\geq |\mathcal{B}|^2\sqrt{p} - \sum_{b\in\mathcal{B}} 2p - \sum_{\substack{b,b'\in\mathcal{B},b\neq b'\\ p\mid b+b'}} 2p \\
&\qquad\qquad\qquad\qquad \uparrow \\
&\qquad\qquad\qquad\qquad \forall\ b\text{-hez legfeljebb egy } b' \\
&\geq |\mathcal{B}|^2\sqrt{p} - \sum_{b\in\mathcal{B}} 2p - \sum_{b\in\mathcal{B}} 2p \\
&\geq |\mathcal{B}|^2\sqrt{p} - 4p|\mathcal{B}|.
\end{aligned}$$

Másrészt:

$$|S| \leq \sum_{x=0}^{p-1} \left|\sum_{b\in\mathcal{B}} e\left(\frac{bx^2}{p}\right)\right|^2.$$

Ahogy x fut a $0,1,\dots,p-1$ mod p maradékosztályokon x^2 minden maradékosztályt legfeljebb 2-szer vesz fel. Tehát:

$$\begin{aligned}
|S| &\leq 2\sum_{y=0}^{p-1} \left|\sum_{b\in\mathcal{B}} e\left(\frac{by}{p}\right)\right|^2 \\
&\leq 2\sum_{y=0}^{p-1} \sum_{b\in\mathcal{B}} \sum_{b'\in\mathcal{B}} e\left(\frac{(b-b')y}{p}\right) \\
&= 2\sum_{b\in\mathcal{B}} \sum_{b'\in\mathcal{B}} \sum_{y=0}^{p-1} e\left(\frac{(b-b')y}{p}\right) \\
&= 2 \sum_{\substack{b,b'\in\mathcal{B}\\ b-b'\equiv 0 \pmod p\\ \uparrow\\ \text{csak } b=b'\text{-re}}} p
\end{aligned}$$

$$= 2|\mathcal{B}|p.$$

Így:

$$|\mathcal{B}|^2\sqrt{p} - 4p|\mathcal{B}| \leq |S| \leq 2|\mathcal{B}|p$$
$$|\mathcal{B}|^2\sqrt{p} \leq 6|\mathcal{B}|p$$
$$|\mathcal{B}| \leq 6\sqrt{p}.$$

A következőkben a másik alkalmazott eszközt, Gallagher nagyobb szitáját [2] ismertetjük.

A jelen változatot Erdős, Stewart és Sárközy [1] mondta ki 1994-ben.

8.3 TÉTEL. (Gallagher nagyobb szitája) *Tegyük fel, hogy* $m, n \in \mathbb{N}$, $\mathcal{A} \subset \{m+1, m+2, \ldots, m+n\}$ *és* $\mathcal{P} \subset \mathbb{N}$ *egy véges halmaz, amelynek elemei páronként relatív prímek. Minden* $p \in \mathcal{P}$*-re jelölje* $\nu(p)$ *azon* $\mod b$ *maradékosztályok számát, amelyek metszik* $\mathcal{A}$*-t. Ekkor*

$$|\mathcal{A}| \leq \frac{\sum\limits_{p\in\mathcal{P}} \log p - \log n}{\sum\limits_{p\in\mathcal{P}} \frac{\log p}{\nu(p)} - \log n}, \tag{8.2}$$

feltéve, hogy a nevező pozitív.

Gallagher az állítást először abban az esetben fogalmazta meg, amikor $\mathcal{P}$ csak prímeket tartalmazott.

Miért hívunk egy ilyen tételt szitának? Ebben az esetben az $\mathcal{A}$ halmaz elemszámát a $\nu(p)$ függvények segítségével becsüljük. Ha $\mathcal{A}$ sok $\mod p$ maradékosztályból nem tartalmaz elemet, akkor $\nu(p)$ kicsi, így (8.2) nevezőjében szereplő tört nagy, ami $|\mathcal{A}|$ elemszámára erős felső becslést ad.

A tételt a „Kombinatorikus Számelmélet” előadáson [3] bizonyítottuk.

Gallagher nagyobb szitájából következik a tétel.

Legyen $m = 1$, $n = x$,

$$\mathcal{P} = \{p : \ p \text{ prím és } p < 36(\log x)^2\}.$$

Jelölje $\mathcal{B}_p \subseteq \mathbb{Z}_p$ azon maradékosztályok halmazát, mod p, amelyekre létezik vele kongruens $a \in \mathcal{A}$:

$$\mathcal{B}_p \stackrel{\text{def}}{=} \{b \in \mathbb{Z}_p : \ \exists a \in \mathcal{A}, b \equiv a \pmod{p}\}.$$

Mivel $a + a'$ mindig négyzetszám, így $b, b' \in \mathcal{B}_p$-re:

$$\left(\frac{b + b'}{p}\right) = 1 \quad \textit{vagy} \quad b + b' \equiv 0 \pmod{p}.$$

A 8.2 lemma miatt

$$\mu(p) = |\mathcal{B}_p| \leq 6p^{1/2}.$$

Ezt alkalmazva:

$$|\mathcal{A}| \leq \frac{\sum\limits_{p \leq 36(\log x)^2} \log p - \log x}{\sum\limits_{p \leq 36(\log x)^2} \frac{\log p}{6\sqrt{p}} - \log x}. \tag{8.3}$$

A fenti képletben szummákat kiszámolva a következő becslés

$$|\mathcal{A}| \leq 37 \log x.$$

De vajon, hogyan kezelhető a fenti képletben a $\sum\limits_{p \leq 36(\log x)^2} \log p$ és $\sum\limits_{p \leq 36(\log x)^2} \frac{\log p}{6\sqrt{p}}$ prímeken futó szummák?

Prímeken futó szummák kezelésére két lehetőség is kínálkozik:

1. Lehetőség: Lebesgue-Stieltjes integrállal (a két lehetőség közül ez ad pontosabb becslést), erről a fejezet végén lesz egy két szó. Most a 2. Lehetőség szerint fogunk haladni.

2. Lehetőség: Prímszámtétellel. Eszerint a számlálóban lévő kifejezés:

$$\sum_{p\leq 36(\log x)^2} \log p - \log x = \log\left(\prod_{p\leq 36(\log x)^2} p\right) - \log x.$$

A „Primorial” című Wikipédia oldal [7] szerint $\prod_{p\leq n} = e^{(1+o(1))n}$, így

$$\begin{aligned}\sum_{p\leq 36(\log x)^2} \log p - \log x &= \log\left(e^{(1+o(1))36(\log x)^2} - \log x\right)\\ &= (1+o(1))36\left(\log x\right)^2 - \log x\\ &= (1+o(1))36\left(\log x\right)^2.\end{aligned}$$

Sajnos, a nevezőnél nincs olyan szerencsénk, hogy a szóban forgó prímeken futó szummát megtaláljuk a Wikipédián. Ezt bizony ki kell számolni...

Következzen tehát a nevező becslése. Amit lehet rögtön beleolvasztunk az $o(1)$-be. A szummánk:

$$\sum_{p\leq 36(\log x)^2} \frac{\log p}{6\sqrt{p}} - \log x.$$

Az $[1, 36(\log x)^2]$ intervallumban a prímek növekvő sorrendben: $p_1 = 2,\ p_2 = 3, p_3 = 5, \ldots, p_t$. Ekkor

$$\begin{aligned}t &= \pi(36\left(\log x\right)^2)\\ &= (1+o(1))\frac{36(\log x)^2}{\log\left(36(\log x)^2\right)}\\ &= (1+o(1))18\frac{\left(\log x\right)^2}{\log\log x}.\end{aligned}$$

A nevezőben a szumma

$$\sum_{i=1}^{t} \frac{\log p_i}{6\sqrt{p_i}} - \log x = \sum_{i=1}^{(1+o(1))18\frac{(\log x)^2}{\log\log x}} \frac{\log p_i}{6\sqrt{p_i}} - \log x.$$

A prímszámtétel miatt:

$$p_i = (1+o(1))i\log i$$
$$\log p_i = (1+o(1))\log i$$
$$\sqrt{p_i} = (1+o(1))\sqrt{i\log i}.$$

Így a nevezőben a szumma

$$\sum_{i=1}^{(1+o(1))18\frac{(\log x)^2}{\log\log x}} (1+o(1))\frac{\sqrt{\log i}}{6\sqrt{i}} - \log x.$$

Közelítjük integrállal:

$$\int_{i=1}^{(1+o(1))18\frac{(\log x)^2}{\log\log x}} (1+o(1))\frac{\sqrt{\log i}}{6\sqrt{i}} - \log x.$$

$(1+o(1))\frac{\sqrt{\log i}}{6\sqrt{i}}$ primitív függvénye $(1+o(1))\frac{1}{3}\sqrt{i\log i}$ (ez nem pontos érték, hanem olyan, amiben megengedünk egy ordós hibatagot. Deriváljuk le az utóbbi függvényt és megkapjuk az előbbi függvényt, amennyiben a főtagot megtartjuk, a többi tag meg mehet az ordóba.)

Most tehát ott tartunk

$$\sum_{p\le 36(\log x)^2} \frac{\log p}{6\sqrt{p}} - \log x$$
$$= (1+o(1))\frac{1}{3}\sqrt{i\log i}\Big]_2^{(1+o(1))18\frac{(\log x)^2}{\log\log x}} - \log x$$
$$= (1+o(1))\frac{1}{3}\sqrt{18\frac{(\log x)^2}{\log\log x}\cdot 2\log\log x} - \log x$$

$$= 2(1+o(1))\log x - \log x$$
$$= (1+o(1))\log x.$$

Vagyis

$$|\mathcal{A}| \leq \frac{(1+o(1))36(\log x)^2}{(1+o(1))\log x} < 37\log x.$$

Említettük, hogy (8.3) becslése történhet másképp is (az említett 2 lehetőség közül ez volt az első), nevezetesen Lebesgue-Stieltjes integrállal. Ezeknek a becsléseknek az alapja:

$$\sum_{p\leq x} f(p) = \int_2^x f(t)d\,pi(t)$$
$$= f(t)\pi(t)\Big|_2^x - \int_2^x f'(t)\pi(t)dt$$

Ennek a módszernek a további kidolgozása HF. Az érdeklődők ennek kapcsán megnézhetik még a következő linket is: link.

Következne:

$$\sum_{x=1}^{q} e\left(\frac{x^k a}{q}\right), \sum_{x=1}^{q} e\left(f(x)\frac{a}{q}\right), \sum_{x=m}^{n} e\left(f(x)\frac{a}{q}\right),$$

Waring, Weil összeg... Majd valamikor... Most azonban a következő fejezetben még egy additív karakteres összeg, utána rátérünk a multiplikatív karakterekre.

Hivatkozások

[1] P. Erdős, A. Sárközy, C.L. Stewart, *On prime factors of subset sums*, Journal of the London Math. Soc. 49 (2) (1994), 209-218.

[2] P. X. Gallagher, *A larger sieve*, Acta Arithmetica 18 (1971), 77-81.

[3] K. Gyarmati, *Elemi Módszerek a Kombinatorikus Számelméletben*, előzetes változat.

[4] J. Lagrange, *Six entiers dont les sommes deux à deux sont des carrés*, Acta Arithmetica, 40 (1981), 91–96.

[5] J.-L. Nicolas, *Six nombres dont les sommes deux à deux sont des carrés*, in Utilisation des calculateurs en mathématiques pures (1975, Limoges), Mémoires de la Société Mathématique de France 49-50 (1977), 141-143.

[6] J. Rivat, A. Sárközy and C.L. Stewart, *Congruence properties of the Omega-function on sumsets*, Illinois J. Math., 43 (1999), 1-18.

[7] Wikipedia, *Primorial*, link.

9. Kloosterman összegek

Két definíció:

9.1 DEFINÍCIÓ. *Ha* $q \in \mathbb{N}$, $q > 1$, $a, b \in \mathbb{Z}$, *akkor az*

$$U(a,b;q) \stackrel{\text{def}}{=} \sum_{\substack{0 \le x < q \\ (x,q)=1}} e\left(\frac{ax + bx^*}{q}\right)$$

(ahol x^**-ra az* $xx^* \equiv 1 \pmod{q}$ *teljesül) összeget Kloosterman-összegnek nevezzük.*

9.2 DEFINÍCIÓ. *Egy*

$$\sum_{x=1}^{q} e\left(f(x)\frac{a}{q}\right) \quad \text{vagy} \quad \sum_{\substack{1 \le x \le q \\ (x,q)=1}} e\left(f(x)\frac{a}{q}\right)$$

típusú összeget teljesnek (angolul „complete”-nak), egy

$$\sum_{u<x<v} e\left(f(x)\frac{a}{q}\right) \quad \text{vagy} \quad \sum_{\substack{u<x<v \\ (x,q)=1}} e\left(f(x)\frac{a}{q}\right)$$

típusú összeget nem teljesnek (angolul „incomplete”-nak) nevezünk.

Eddig csupa teljes összeggel (Ramanujan összegek, Gauss összegek) foglalkoztunk; a fenti Kloosterman összegek is teljesek, de lehet nem teljes összeget is definiálni a

$$U(a,b;q) \stackrel{\text{def}}{=} \sum_{\substack{u<x<q \\ (x,q)=1}} e\left(\frac{ax + bx^*}{q}\right)$$

képlettel. Nem teljes Kloosterman összegekről később lesz szó.

Először teljes Kloosterman összegek. Néhány alaptulajdonság (ld. „Kis” Vinogradov [2, 51. oldal] vagy Hooley [1]):

9.3 TÉTEL.

a) $U(a,b;q)$ $\forall\, a,b,q$-ra valós.

b) $U(a,b;q) = U(b,a;q)$ $\forall\, a,b,q$-ra.

c) Ha $(h,q) = 1$ akkor

$$U(a,bh;q) = U(ah,b;q).$$

d) *Multiplikatív tulajdonság:* Ha $q_1, q_2 \in \mathbb{N}$, $q_1, q_2 > 1$, $(q_1,q_2) = 1$ és adott a, b, q_1, q_2 mellett b_1, b_2 olyan, hogy

$$b_1 q_2^2 + b_2 q_1^2 \equiv b \pmod{q_1 q_2} \tag{9.1}$$

akkor

$$U(a,b;q_1q_2) = U(a,b;q_1)U(a,b;q_2).$$

A 9.3 Tétel bizonyítása.

a) Elég: $\overline{U(a,b;q)} = U(b,a;q)$.

Valóban:

$$\begin{aligned}
\overline{U(a,b;q)} &= \sum_{\substack{0\le x<q\\(x,q)=1}} \overline{e\left(\frac{ax+bx^*}{q}\right)} \\
&= \sum_{\substack{0\le x<q\\(x,q)=1}} e\left(\frac{a(-x)+b\overbrace{(-x^*)}^{(-x)^*}}{q}\right) \\
&= \sum_{\substack{0\le y<q\\(y,q)=1}} e\left(\frac{ay+by^*}{y}\right) \\
&= U(a,b;q)
\end{aligned}$$

b), c) Hasonlóan könnyű, HF.

d) Itt a lényeg: Ezzel a d) tulajdonsággal a Kloosterman összegek vizsgálata a $q = p^\alpha$ esetre redukálható.

A bizonyítás során a következőből indulunk ki: ha

$$x(u,v) \stackrel{\text{def}}{=} uq_2 + vq_1$$

és u redukált maradékrendszeren fut mod q_1, valamint v redukált maradékrendszeren fut mod q_2, akkor $x(u,v)$ redukált maradékrendszeren fut mod q_1q_2.

Így a baloldalon

$$U(a,b;q) = \sum_{\substack{1\le x\le q\\(x,q)=1}} e\left(\frac{ax+bx^*}{q}\right)$$

szerepel, ahol az x-re vonatkozó összegzés $\bmod q_1q_2$ redukált maradékrendszeren való összegzést jelent. Ehelyett: $x \to x(u,v)$, ahol u,v fut mint fent:

$$U(a,b;q_1q_2) = \sum_{\substack{1\le u\le q_1\\(u,q_1)=1}} \sum_{\substack{1\le v\le q_2\\(v,q_2)=1}} e\left(\frac{ax(u,v)+bx(u,v)^*}{q_1q_2}\right)$$

Itt $*$ definíciója miatt $x^*(u,v)$ olyan, hogy

$$\begin{aligned} \underbrace{x(u,v)}_{uq_2+vq_1}\ x^*(u,v) &\equiv 1 \pmod{q_1q_2}\\ uq_2x^*(u,v) + vq_1x^*(u,v) &\equiv 1 \pmod{q_1q_2}\\ uq_2x^*(u,v) &\equiv 1 \pmod{q_1}\\ vq_1x^*(u,v) &\equiv 1 \pmod{q_2}. \end{aligned} \tag{9.2}$$

Így ezt és $b \equiv b_1 q_2^2 + b_2 q_1^2 \pmod{q_1 q_2}$-t használva

$$e\left(\frac{ax(u,v) + bx(u,v)^*}{q_1 q_2}\right) = \\ = e\left(\frac{a(uq_2 + vq_1) + (b_1 q_2^2 + b_2 q_1^2)x^*(u,v)}{q_1 q_2}\right) \\ = e\left(\frac{au}{q_1} + \frac{av}{q_2} + \frac{b_1 q_2 x^*(u,v)}{q_1} + \frac{b_2 q_1 x^*(u,v)}{q_2}\right).$$

Itt (9.2) alapján:

$$q_2 x^*(u,v) \equiv u^* \pmod{q_1}$$
$$q_1 x^*(u,v) \equiv v^* \pmod{q_2},$$

vagyis

$$e\left(\frac{ax(u,v) + bx(u,v)^*}{q_1 q_2}\right) = e\left(\frac{au}{q_1} + \frac{av}{q_2} + \frac{b_1 u^*}{q_1} + \frac{b_2 v^*}{q_2}\right) \\ = e\left(\frac{au + b_1 u^*}{q_1}\right) e\left(\frac{av + b_1 v^*}{q_2}\right).$$

Azaz

$$U(a,b;q_1 q_2) = \sum_{\substack{0 \le u < q_1 \\ (u,q_1)=1}} e\left(\frac{au + b_1 u^*}{q_1}\right) \sum_{\substack{0 \le v < q_2 \\ (v,q_2)=1}} e\left(\frac{av + b_2 v^*}{q_2}\right) \\ = U(a,b;q_1)U(a,b;q_2).$$

Ezek után, mit lehet tudni egy Kloosterman összeg abszolút értékéről tudni?

9.4 TÉTEL.

a) $(a,p) = (b,p) = 1$ *esetén* $|U(a,b;p)| \le 2\sqrt{p}$.

b) $\forall\, a,b$*-re* $|U(a,b;p)| \le 2\sqrt{p(b,p)}$.

c) $\alpha \in \mathbb{N}$, $\alpha > 1$, $(a,p) = (b,p) = 1$ *esetén*

$$|U(a,b;p^\alpha)| \leq 3\sqrt{p^\alpha}.$$

d) $\forall\, a,b$*-re:*

$$|U(a,b;p^\alpha)| \leq d(p^\alpha)\sqrt{p(b,p^\alpha)}.$$

e) $\forall\, a,b,q$*-ra:*

$$|U(a,b;q)| \leq d(q)\sqrt{p(b,q)}.$$

A 9.4 Tétel bizonyítása.

a) A. Weiltől származik, nagyon mély, algebrai geometriával, nem bizonyítjuk.

b) 3 eset:

1. $(a,p) = (b,p) = 1$: a)-val azonos.
2. $p \mid b$: Ekkor $|U(a,b;p)| \leq p$ triviálisan. Jobboldal $2\sqrt{p(b,p)} = 2p$.
3. $p \mid a$, $(b,p) = 1$:

$$\begin{aligned} U(a,b;p) &= \left| \sum_{\substack{0 \leq x < p \\ (x,p)=1}} e\left(\frac{bx^*}{p}\right) \right| \\ &= \left| \sum_{y=1}^{p-1} e\left(\frac{y}{p}\right) \right| \\ &= 1. \end{aligned}$$

c) Salié, elemileg, nem bizonyítjuk.

d) Ez b)-ből és c)-ből következik. HF.

e) Az utolsó tétel multiplikatív tulajdonsága + d). HF.

Eddig teljes (komplett) Kloosterman összegekről beszéltünk. Általában nem teljes exponenciális összegek kezelése, becslése jóval nehezebb; rendszerint csak jóval gyengébb becslések adhatók. 2 fontos kivétel: Gauss-összegek (visszatérünk) valamint a Kloosterman összegek; részben ebben áll a jelentőségük.

9.5 TÉTEL. *Ha* $\varepsilon > 0$, $q \in \mathbb{N}$, $q > q_0(\varepsilon)$, $a, b \in \mathbb{Z}$ *és* $0 \leq v - u \leq 2q$, *akkor*

$$\left| \sum_{\substack{u \leq x \leq v \\ (x,q)=1}} e\left(\frac{ax + bx^*}{q}\right) \right| < q^{1/2+\varepsilon}\sqrt{(b,q)}.$$

A 9.5 Tétel bizonyítása. Előző tételből lehet levezetni; A Pólya-Vinogradov egyenlőtlenségnél fogunk hasonlót csinálni; visszatérünk. (Egyébként Hooley [1, 36. oldal].)

Hivatkozások

[1] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, (Cambridge Tracts in Mathematics, Series Number 70, Cambridge University Press, 1976.

[2] I. M. Vinogradov, *A Számelmélet Alapjai*, Tankönyvkiadó, Budapest, 1951.

10. Multiplikatív karakterek

Láttuk a számelméletben két fontos véges csoport létezik: $\mathbb{Z}_m$ és Z_m^* (= mod m redukált maradékosztályok multiplikatív csoportja.)

Előbbit tárgyaltuk; jön az utóbbin definiált csoport karakterek. De technikai okokból kicsit módosítjuk (kiterjesztjük a definíciót.)

10.1 Definíció. *Ha $m \in \mathbb{N}$, akkor egy $\chi(n) : \mathbb{Z} \to \mathbb{C}$ függvényt akkor nevezünk multiplikatív karakternek, ha $\exists$ olyan Z_m^*-en definiált χ_1 csoportkarakter, hogy*

$$\chi(n) = \begin{cases} \chi_1(n), & \text{ha } (n,m) = 1 \\ 0, & \text{ha } (n,m) > 1. \end{cases}$$

(Tehát tulajdonképpen csak annyi különbség, hogy $(n,m) > 1$ esetén $\chi(n)$-t 0-nak vesszük.)

Lehetne csoport karakterek nélkül is definiálni:

10.2 Definíció. *$m \in \mathbb{N}$ esetén egy $\chi(n) : \mathbb{Z} \to \mathbb{C}$ függvényt, akkor nevezünk multiplikatív karakternek, ha*

a) $u, v \in \mathbb{Z}$, $u \equiv v \pmod{m} \Rightarrow \chi(u) = \chi(v)$.

b) $u, v \in \mathbb{Z} \Rightarrow \chi(uv) = \chi(u)\chi(v)$.

c) $(n,m) > 1 \Rightarrow \chi(n) = 0$.

d) $\chi(n) \not\equiv 0$.

A két definíció ekvivalenciája HF.

Példa. Legyen p prím. Ekkor

$$\chi(n) = \begin{cases} \left(\frac{a}{p}\right), & \text{ha } (a,p) = 1 \\ 0, & \text{ha } p \mid a. \end{cases}$$

A csoport karakterekre mondottakból következnek a mod m multiplikatív karakterek alábbi alaptulajdonságai (ld. 3.2 Következmények).

1. $\chi(1) = 1$.
2. $(a, m) = 1$ esetén $\chi(a)$ az $\varphi(m)$ $(= |Z_m^*|)$-edik egységgyök.
3. $$\chi_0(a) = \begin{cases} 1, & \text{ha } (a, n) = 1 \\ 0, & \text{ha } (a, n) > 1 \end{cases}$$
   karakter az ún. főkarakter.
   χ karakter $\Rightarrow \overline{\chi}$ is, ahol $\overline{\chi}(a) = \overline{\chi(a)}$ $(= \chi(a^{-1}))$
   χ_1, χ_2 karakter $\Rightarrow \chi_1\chi_2$ is, ahol $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$.
4. A mod m karakterek száma $\varphi(m)$.
5. $$\sum_{a=1}^{m} \chi(a) = \begin{cases} \varphi(m), & \text{ha } \chi = \chi_0 \\ 0, & \text{ha } \chi \neq \chi_0. \end{cases}$$
6. $$\sum_{\chi \pmod m} \chi(a) = \begin{cases} \varphi(m), & \text{ha } a = 1 \\ 0, & \text{ha } a \neq 1. \end{cases}$$

10.3 Tétel. *Ha* $a, n_1, n_2, \ldots, n_t \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$, *akkor*

$$|\{i : 1 \leq i \leq t,\ n_i \equiv a \pmod m\}| = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a) \sum_{i=1}^{t} \chi(n_i).$$

Csoportkarakterekről tanultak miatt elég $\mathbb{Z}_m^*$-ot ciklikus csoportok direkt szorzataként felírni. A kínai maradéktétel miatt, ha $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ esetén

$$\mathbb{Z}_m^* = \mathbb{Z}_{p_1^{\alpha_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}^*.$$

Ha $\mathbb{Z}^*_{p_i^{\alpha_i}}$ mindig ciklikus lenne, azaz, $\forall\ p_i^{\alpha_i}$-re lenne primitív gyök, készen is lennénk. Sajnos, nem ez a helyzet. Két számelméleti tétel:

10.4 Tétel. *Akkor és csak akkor $\exists$ mod m primitív gyök, ha $m = 2, 4, p^\alpha$ vagy $2p^\alpha$, ahol $p > 2$ prím.*

10.5 Tétel. *$\alpha > 2$ esetén*

$$\mathbb{Z}^*_{2^\alpha} = \{-1\}_2 \times \{5\}_{2^{\alpha-2}}$$

A 10.4 és 10.5 Tételek bizonyítása. Ld. „kis” Vinogradov [2, 76-78. oldal].

E két számelméleti segédtételt felhasználva következik, hogy a mod m multiplikatív karakterek explicit alakja az alábbi:

10.6 Tétel. *Legyen $m = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, ahol $2 < p_1 < \cdots < p_k$, $0 \le \beta$, $0 < \beta_1, \ldots, \beta_k$. Legyen továbbá g_i primitív gyök mod $p_i^{\alpha_i}$. Ekkor $\chi : \mathbb{Z}_m \to \mathbb{C}$, akkor és csak akkor multiplikatív karakter modulo m, ha léteznek olyan $a_1, a_2, b_1, \ldots, b_k$ egész számok, hogy*

$$0 \le a_1 < c_1 \overset{\text{def}}{=} \begin{cases} 1, & \text{ha } \alpha = 0 \text{ vagy } 1 \\ 2, & \text{ha } \alpha \ge 2, \end{cases}$$

$$0 \le a_2 \le c_2 \overset{\text{def}}{=} \begin{cases} 1, & \text{ha } \alpha = 0 \text{ vagy } 1 \\ 2^{\alpha-2}, & \text{ha } \alpha \ge 2 \end{cases}$$

és

$$0 \le b_i \le \varphi(p_i^{\alpha_i}) - 1,$$

továbbá

a) $(n, m) = 1$ esetén a $k_1, k_2, \ell_1, \ldots, \ell_k$ egész számokat az

$$n \equiv (-1)^{k_1} 5^{k_2} \pmod{2^\beta}, \quad 0 \le k_1 < c_1,\ 0 \le k_2 < c_2$$

$$n \equiv g_i^{\ell_i} \pmod{p_i^{\alpha_i}}, \quad 0 \le \ell_i < \varphi(p_i^{\alpha_i})$$

feltételekkel definiálva

$$\chi(n) = e\left(k_1\frac{a_1}{c_1} + k_2\frac{a_2}{c_2} + \ell_1\frac{b_1}{\varphi(p_1^{\alpha_1})} + \cdots + \ell_k\frac{b_k}{\varphi(p_k^{\alpha_k})}\right)$$

b) $(n, m) > 1$ *esetén* $\chi(n) = 0$.

A 10.6 Tétel bizonyítása. Davenport [1, 29. oldal], „kis” Vinogradov [2, 80. oldal].

10.7 DEFINÍCIÓ. *A* χ mod m *karaktert primitívnek mondjuk, ha* $\nexists$ *olyan* m_1 *szám és* χ_1 *karakter* mod m_1*, hogy* $m_1 \mid m$, $m_1 < m$ *és* $n \in \mathbb{Z}$, $(n, m) = 1$ *esetén* $\chi(n) = \chi_1(n)$*. Ha viszont létezik ilyen* m_1, χ_1*, akkor* χ*-t nem primitívnek, és a legkisebb ilyen* m_1*-et* χ *„conductor”-ának,* χ*-t magát a legkisebb* m_1*-hez tartozó (egyértelmű)* χ_1 *karakter által indukáltnak mondjuk.*

Megjegyzés.

1. χ_0 Davenport szerint sem primitív, sem nem primitív.
2. Ha p prím, akkor mod p minden $\chi \neq \chi_0$ karakter primitív.
3. Másik lehetséges definíció: χ nem primitív, ha $\exists\ m_1 \mid m$, $1 < m_1 < m$, hogy $\chi(n)$ értékei az $(n.m) = 1$-et kielégítő n-ekre periodikusak m_1 periódussal.

Hivatkozások

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967.

[2] I. M. Vinogradov, *A Számelmélet Alapjai*, Tankönyvkiadó, Budapest, 1951.

11. Gauss összegek (2. rész)

11.1 DEFINÍCIÓ. *Ha $q \in \mathbb{N}$, χ karakter mod m, akkor a*

$$\tau(\chi) = \sum_{m=0}^{q-1} \chi(m) e\left(\frac{a}{m}\right)$$

összeget is Gauss összegnek nevezzük.

Miért?

Eredetileg beláttuk, hogy ha p prím és $(a,p) = 1$, akkor az

$$S(a,p) = \sum_{x=0}^{p-1} e\left(x^2 \frac{a}{p}\right)$$

Gauss összeg abszolút értéke

$$|S(a,p)| = \sqrt{p}.$$

Tekintsük rá egy kicsit erre az $S(a,p)$ Gauss összegre:

$$\begin{aligned} S(a,p) &= \sum_{x=0}^{p-1} e\left(x^2 \frac{a}{p}\right) \\ &= 1 + \sum_{x=1}^{p-1} \underbrace{e\left(x^2 \frac{a}{p}\right)}_{\substack{x^2 \equiv (-x)^2 \equiv y\text{-t 2x számoltuk,} \\ \text{ha } \left(\frac{y}{p}\right)=1,\ 0\text{-szor, ha} \left(\frac{y}{p}\right)=-1}} \\ &= 1 + \sum_{y=1}^{p-1} \left(\left(\frac{y}{p}\right) + 1\right) e\left(y \frac{a}{p}\right) \\ &= \underbrace{\sum_{y=0}^{p-1} e\left(y \frac{a}{p}\right)}_{=0,\ (a,p)=1 \text{ miatt}} + \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) e\left(y \frac{a}{p}\right) \end{aligned}$$

$$= \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) e\left(y\frac{a}{p}\right)$$

Legyen

$$\chi(n) = \begin{cases} \left(\frac{n}{p}\right), & \text{ha } (n,p)=1 \\ 0 & \text{ha } (n,p)>1. \end{cases}$$

Ekkor

$$S(a,p) = \sum_{y=0}^{p-1} \chi(y) e\left(\frac{ya}{p}\right)$$

típusú összeg. Itt $ya \equiv t \pmod p$-t helyettesítve $y \equiv ta^* \pmod p$, ahol a^* az a multiplikatív inverze. Vagyis:

$$\begin{aligned} S(a,p) &= \sum_{t=0}^{p-1} \chi(ta^*) e\left(\frac{t}{p}\right) \\ &= \chi(a^*) \sum_{t=0}^{p-1} \chi(t) e\left(\frac{t}{p}\right) \\ &= \overline{\chi(a)} \underbrace{\sum_{t=0}^{p-1} \chi(t) e\left(\frac{t}{p}\right)}_{\substack{\text{Ezt nézve lesz} \\ \text{világos a definíció.}}} \end{aligned}$$

11.2 TÉTEL. *Ha $m \in \mathbb{N}$, χ primitív karakter mod m, akkor*

$$|\tau(\chi)| = \sqrt{m}.$$

A 11.2 Tétel bizonyítása. Csak abban az esetben bizonyítjuk, ha m egy p prím. Ekkor az, hogy χ primitív, azt jelenti $\chi \neq \chi_0$. Ekkor

$$\begin{aligned} |\tau(\chi)|^2 &= \sum_{a=1}^{p-1} \chi(a) e\left(\frac{a}{p}\right) \overline{\sum_{b=1}^{p-1} \chi(b) e\left(\frac{b}{p}\right)} \\ &= \sum_{a=1}^{p-1} \chi(a) e\left(\frac{a}{p}\right) \sum_{b=1}^{p-1} \underbrace{\overline{\chi(b)}}_{\chi(b^*)} e\left(-\frac{b}{p}\right) \end{aligned}$$

$$= \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \chi(ab^*) e\left(\frac{a-b}{p}\right)$$

Legyen $ab^* \equiv t \pmod{p}$, azaz $a \equiv tb \pmod{p}$. Ekkor

$$\begin{aligned}
|\tau(\chi)|^2 &= \sum_{t=1}^{p-1} \sum_{b=1}^{p-1} \chi(t) e\left(\frac{bt-b}{p}\right) \\
&= \sum_{t=1}^{p-1} \left(\underbrace{\sum_{b=0}^{t-1} e\left(\frac{b(t-1)}{p}\right)}_{\begin{cases} p, & \text{ha } t=1 \\ 0, & \text{ha } t \neq 1 \end{cases}} - 1 \right) \\
&= \chi(1)(p-1) + \sum_{t=2}^{p-1} \chi(t)(-1) \\
&= p - 1 + \sum_{t=1}^{p-1} \chi(t) + \chi(1) \\
&= 0.
\end{aligned}$$

A következőkben egy áttérési formulát tanulunk multiplikatív karakterről additívra.

11.3 TÉTEL. *Ha $q \in \mathbb{N}$, $n \in \mathbb{Z}$, χ multiplikatív karakter mod p és*

a) $(n, q) = 1$

vagy

b) χ *primitív karakter, akkor*

$$\chi(n)\tau(\overline{\chi}) = \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(n\frac{h}{p}\right).$$

A 11.3 Tétel bizonyítása. a)

$$\begin{aligned}\chi(n)\tau(\overline{\chi}) &= \underbrace{\chi(n)}_{\overline{\chi}(n^*)} \sum_{m=0}^{q-1} \overline{\chi}(m) e\left(\frac{m}{q}\right) \\ &= \sum_{m=0}^{q-1} \overline{\chi}(mn^*) e\left(\frac{m}{q}\right) \\ &= \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(\frac{hn}{q}\right),\end{aligned}$$

ahol az utolsó sorban $h \equiv mn^* \pmod{q} \Leftrightarrow m \equiv hn \pmod{q}$. b) Komplikáltabb, ld. Davenport [1, 65. oldal].

Hivatkozások

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967.

12. A Vinogradov lemma duálisa

Az előző fejezetben tanult áttérési formulát, azaz a 11.3 Tételt alkalmazva bebizonyítjuk a Vinogradov lemma (6.1 Lemma) egy dualisát.

Ugyanis, az alábbiak szerint létezik egy dualitás elv, mely szerint, bizonyos tételek esetén, az additív karakterek helyettesíthetőek multiplikatív karakterekkel, a szorzatok pedig összegekkel, és vice versa, a bizonyítások pedig gyakran konvertálhatóak. Erre látunk most példát.

A 6. fejezetben a 6.1 Lemmában a következőt bizonyítottuk:

12.1 TÉTEL. (Vinogradov lemma) *Legyen* $(a,q)=1$, $q>1$ *és*

$$S \stackrel{\text{def}}{=} \sum_{x=0}^{q-1}\sum_{y=0}^{q-1} \xi(x)\eta(y)e\left(xy\frac{a}{q}\right)$$

azaz $\Psi(n)=e\left(\frac{a}{q}n\right) \mod q$ *additív karaktert írva,*

$$S=\sum_{x}\sum_{y}\xi(x)\eta(y)\Psi(xy),$$

és legyen

$$\sum_{x=0}^{q-1}|\xi(x)|^2=X_0, \qquad \sum_{y=0}^{q-1}|\eta(y)|^2=Y_0.$$

Ekkor

$$|S|\le (X_0Y_0q)^{1/2}.$$

Speciálisan, ha $q=p$ prím, akkor a tételben az $(a,q)=(a,p)=1$ feltétel azt mondja ki, hogy $\Psi\neq\Psi_0$ (ugyanis itt $\Psi(n)=e\left(\frac{a}{q}n\right)$). Így ebben a speciális esetben a következőt kapjuk:

12.2 TÉTEL. *Ha p prím és $\Psi \neq \Psi_0$ egy additív karakter modulo p, akkor*

$$|S| = \left| \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x)\eta(y)\Psi(xy) \right| \leq (X_0 Y_0 p)^{1/2},$$

ahol

$$\sum_{x=0}^{p-1} |\xi(x)|^2 = X_0, \qquad \sum_{y=0}^{p-1} |\eta(y)|^2 = Y_0.$$

A fenti tétel duálisa a következő:

12.3 TÉTEL. (Gyarmati - Sárközy [7]) *Ha p prím és $\chi \neq \chi_0$ egy multiplikatív karakter modulo p, akkor*

$$|S| = \left| \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x)\eta(y)\chi(x+y) \right| \leq (X_0 Y_0 p)^{1/2},$$

ahol

$$\sum_{x=0}^{p-1} |\xi(x)|^2 = X_0, \qquad \sum_{y=0}^{p-1} |\eta(y)|^2 = Y_0.$$

Megjegyzés. Mind a Vinogradov lemma, mind a fenti duálisa könnyen kiterjeszthető $\mathbb{F}_p$-ről tetszőleges véges testre.

12.4 KÖVETKEZMÉNY. *Amennyiben p prím és $\xi(x)$ és $\eta(y)$ karakterisztikus függvénye bizonyos $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ halmazoknak, azaz*

$$\xi(x) = \begin{cases} 1, & \text{ha } x \in \mathcal{A} \\ 0, & \text{ha } x \notin \mathcal{A} \end{cases} \qquad \eta(y) = \begin{cases} 1, & \text{ha } y \in \mathcal{B} \\ 0, & \text{ha } y \notin \mathcal{B}, \end{cases}$$

akkor

$$\left| \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(a+b) \right| \leq (|\mathcal{A}||\mathcal{B}|p)^{1/2}.$$

Ezt a tételt először Erdős és Shapiro [4] bizonyította be 1957-ben.

Megjegyezzük, hogy ha χ a kvadratikus karaker, azaz $\chi(n) = \left(\frac{n}{p}\right)$ ha $(n,p) = 1$ és $\chi(n) = 0$, ha $(n.p) > 1$, akkor az alábbit kapjuk:

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{a+b}{p}\right)\right| \leq (|\mathcal{A}||\mathcal{B}|p)^{1/2}.$$

A 12.3 Tétel bizonyítása. Mivel p prím és $\chi \neq \chi_0$, ezért χ primitív karakter. Így a transzformációs formula, azaz 11.3 Tétel alkalmazható:

$$\chi(n)\tau(\overline{\chi}) = \sum_{h=0}^{p-1}\overline{\chi}(h)e\left(n\frac{h}{p}\right).$$

Mivel χ primitív $\tau(\overline{\chi}) = \sqrt{p} \neq 0$, ezért leoszthatunk vele:

$$\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{h=0}^{p-1}\overline{\chi}(h)e\left(n\frac{h}{p}\right).$$

Azaz $|S|$ a következőképpen becsülhető:

$$\begin{aligned}
|S| &= \left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\left(\frac{1}{\tau(\overline{\chi})}\sum_{h=0}^{p-1}\overline{\chi}(h)e\left((x+y)\frac{h}{p}\right)\right)\right| \\
&= \frac{1}{|\tau(\overline{\chi})|}\left|\sum_{h=0}^{p-1}\overline{\chi}(h)\sum_{x=0}^{p-1}\xi(x)e\left(x\frac{h}{p}\right)\sum_{y=0}^{p-1}\eta(y)e\left(y\frac{h}{p}\right)\right| \\
&\leq \frac{1}{\sqrt{p}}\sum_{h=0}^{p-1}\left|\sum_{x=0}^{p-1}\xi(x)e\left(x\frac{h}{p}\right)\right|\left|\sum_{y=0}^{p-1}\eta(y)e\left(y\frac{h}{p}\right)\right|
\end{aligned}$$

A Cauchy-Schwarz egyenlőtlenség szerint:

$$|S| \leq \frac{1}{\sqrt{p}}\left(\sum_{h=0}^{p-1}\left|\sum_{x=0}^{p-1}\xi(x)e\left(x\frac{h}{p}\right)\right|^2\right)^{1/2}\left(\sum_{h=0}^{p-1}\left|\sum_{y=0}^{p-1}\eta(y)e\left(y\frac{h}{p}\right)\right|^2\right)^{1/2}$$

Egy előzőleg tanult Parseval-formula szerint (ld. (6.3)):

$$\begin{aligned}|S| &\le \frac{1}{\sqrt{p}}\left(p\sum_{x=0}^{p-1}|\xi(x)|^2\right)^{1/2}\left(p\sum_{y=0}^{p-1}|\eta(y)|^2\right)^{1/2}\\ &= \frac{1}{\sqrt{p}}\left(pX_0\right)^{1/2}\left(pY_0\right)^{1/2}\\ &= \left(pX_0Y_0\right)^{1/2}.\end{aligned}$$

Ahogy azt pl. Diofantosz problémájához kapcsolódóan láttuk (8. fejezet) egy multiplikatív problémának (pl. $aa'+1$ mindig négyzetszám, ha $a \neq a'$ és $a, a' \in \mathcal{A}$) van additív analogonja ($a+a'$ mindig négyzetszám, ha $a \neq a'$ és $a, a' \in \mathcal{A}$), és vice versa.

Ha tehát van egy állításunk $a+b$ típusú összegekre, érdekes kérdés, hogy vajon hasonló mondható-e $ab+1$-re.

Így például érdekes kérdés, hogy a 12.3 Tételben vizsgált $\left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\chi(x+y)\right|$ kifejezés becslése átvihető-e $\left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\chi(xy+1)\right|$ alakú összegre? Erre a kérdésre, a válasz megerősítő, azaz igaz a következő:

12.5 Következmény. (Gyarmati - Sárközy) *Ha p prím és $\chi \neq \chi_0$ egy multiplikatív karakter modulo p, akkor*

$$|S| = \left|\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\eta(y)\chi(xy+1)\right| \le \left(pX_0\right)^{1/2}\left(Y_1^{1/2}+|\eta(0)|\right),$$

ahol

$$\sum_{x=0}^{p-1}|\xi(x)|^2 = X_0, \qquad \sum_{y=1}^{p-1}|\eta(y)|^2 = Y_1.$$

A 12.5 Következmény bizonyítása. A bizonyítás lényegében, csak annyi, hogy a 12.3 Tételt alkalmazzuk $\eta(y)$-et $\eta(y^{-1})\chi(y^{-1})$-gyel

helyettesítve, majd a szummában a $z = x^{-1}$ új változót bevezetve megkapjuk a kívánt eredményt:

$$
\begin{aligned}
|S| &= \left| \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x)\eta(y)\chi(xy+1) \right| \\
&\le \left| \sum_{x=0}^{p-1} \sum_{y=1}^{p-1} \xi(x) \underbrace{\eta(y)\chi(y)}_{=\eta'(y^{-1})=\eta'(z)} \chi(x+\underbrace{y^{-1}}_{=z}) \right| + \left| \sum_{x=0}^{p-1} \xi(x)\eta(0) \underbrace{\chi(1)}_{=1} \right| \\
&\le \left(pX_0 \underbrace{\sum_{z=1}^{p-1} |\eta'(z)|^2}_{} \right)^{1/2} + \underbrace{\left| \sum_{x=0}^{p-1} \xi(x) \right|}_{\text{Cauchy-Shwarz}} |\eta(0)| \\
&\qquad \sum_{z=1}^{p-1} |\eta(z^{-1})|^2 \underbrace{\left|\chi(z^{-1})\right|^2}_{=1} = Y_1 \\
&\le (pX_0Y_1)^{1/2} + |\eta(0)| \, (X_0 p)^{1/2} \\
&= (pX_0)^{1/2} \left(Y_1^{1/2} + |\eta(0)| \right).
\end{aligned}
$$

12.6 KÖVETKEZMÉNY. *Amennyiben p prím, $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$, $0 \notin \mathcal{B}$, $\xi(x)$ és $\eta(y)$ az $\mathcal{A}$ és $\mathcal{B}$ halmazok karakterisztikus függvénye, akkor a következőt kapjuk:*

$$\left| \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \chi(ab+1) \right| \le (|\mathcal{A}||\mathcal{B}|p)^{1/2}.$$

Ezt az utóbbi következményt [6]-ben igazoltam, illetve még előbb Vinogradov vizsgálta a $\chi(n) = \left(\frac{n}{p}\right)$ esetet.

Ha már szóba kerültek additív és multiplikatív analógiák ($a+b$ illetve $ab+1$ eset), megemlítjük, hogy Sárközy a 6.2 Tételben az

$$a + b = cd,\ a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \qquad (12.1)$$

egyenlet megoldhatóságát vizsgálta, amennyiben $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ nagy halmazok.

Érdekes kérdés a fenti problémának a multiplikatív analogonja:

12.7 TÉTEL. (Sárközy [9], 2005) *Ha p prím, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ és az*

$$ab + 1 = cd, \quad a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D} \tag{12.2}$$

megoldásszámát N-nel jelöljük, akkor

$$\left| N - \frac{|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}|}{p} \right| \leq 8\left(|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}|\right)^{1/2} p^{1/2} + 4p^2.$$

12.8 KÖVETKEZMÉNY. *Ha p prím, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{Z}_p$ és*

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}| > 100p^3,$$

akkor (12.2) *megoldható.*

A 12.7 Tétel bizonyítása. A bizonyítás HF, csak annyit mondunk róla, hogy hasonló a 6.2 Tétel bizonyításhoz, azzal a különbséggel, hogy $|\sum_a \sum_b \chi(ab+1)|$ becsléséhez a 12.6 Következményt használjuk.

Megjegyzés. Mind (12.1) és (12.2) speciális esete az

$$f(a_1, a_2, \ldots, a_k) = 0, \quad a_1 \in \mathcal{A}_1,\ a_2 \in \mathcal{A}_2, \ldots,\ a_k \in \mathcal{A}_k$$

típusú algebrai egyenletnek, ahol $f(a_1, \ldots, a_k) \in \mathbb{Z}_p[a_1, \ldots, a_k]$ és $\mathcal{A}_1, \ldots, \mathcal{A}_k$ pedig nagy részhalmazai $\mathbb{Z}_p$-nek. Sárközy Andrással közösen fenti típusú egyenletek megoldhatóságát vizsgáltuk [8]-ben.

Ezekben az eredményekben a Weil tétel kulcsszerepet játszik. Az alábbiakban a Weil tétel multiplikatív karakterekre vonatkozó alakját ismertetjük:

12.9 TÉTEL. (Weil) *Ha p prím, χ egy d-ed rendű multiplikatív karakter modulo p, ahol $d > 1$ és $f(x) \in \mathbb{F}_p[x]$ polinomnak s különböző*

gyöke van $\mathbb{F}_p$ algebrai lezártja felett, továbbá $f(x)$ nem $cg(x)^d$ alakú, ahol $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$, akkor

$$\left|\sum_{x\in\mathbb{F}_p} \chi(f(x))\right| \leq (s-1)p^{1/2} \leq (\deg f - 1)p^{1/2}.$$

12.10 DEFINÍCIÓ. *Egy karakter rendje akkor d, ha d a legkisebb pozitív egész, amelyre $\chi^d = \chi_0$.*

Az Euler-Fermat tételből következik, hogy ha χ tetszőleges karakter modulo m és $(n,m)=1$, akkor

$$\chi(n)^{\varphi(m)} = \chi(n^{\varphi(m)}) = \chi(1) = 1 = \chi_0(n).$$

Míg $(n,m) > 1$ esetén is $\chi(n) = 0 = \chi_0(n)$. Vagyis $\chi^{\varphi(m)} = \chi_0$, azaz egy karakter rendje mindig $\leq \varphi(m)$.

Weil tételében az $f(x) \neq cg(x)^d$ feltétel fontos, ugyanis, ha $f(x) = cg(x)^d$ és χ egy d-ed rendű karakter, akkor

$$\begin{aligned}\left|\sum_{x\in\mathbb{F}_p} \chi(f(x))\right| &= \left|\sum_{x\in\mathbb{F}_p} \chi(cg(x)^d)\right| \\ &= \left|\sum_{x\in\mathbb{F}_p} \chi(c)\chi^d(g(x))\right| \\ &= \left|\sum_{\substack{x\in\mathbb{F}_p \\ g(x)\neq 0}} \chi(c)\right| \\ &\geq p - \deg g.\end{aligned}$$

Megjegyezzük azt is, hogy Weil tételében az $f(x)$ polinom helyettesíthető egy $\frac{f(x)}{g(x)}$ törtfüggvénnyel, ugyanis, ha $g(x) \neq 0$, akkor

$\frac{1}{g(x)} \overset{\text{def}}{=} g^*(x) = g(x)^{p-2}$, s így

$$\left| \sum_{\substack{x \in \mathbb{F}_p \\ g(x) \neq 0}} \chi\left(\frac{f(x)}{g(x)}\right) \right| = \left| \sum_{x \in \mathbb{F}_p} \chi\left(f(x)g(x)^{p-2}\right) \right|$$

$$\leq (\#\text{különböző gyökök száma } f(x)g(x)\text{-ben})\, p^{1/2},$$

feltéve, hogy $f(x)g(x)^{p-2}$ nem $ch(x)^d$ alakú, ami $(f,g) = 1$ esetén azzal ekvivalens, hogy $f(x)$ vagy $g(x)$ valamelyike nem $ch(x)^d$ alakú.

Sárközy Andrással közös cikkeinkben [7] és [8] a következő karakterösszegek becslésére volt szükségünk: $|\sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \Psi(f(x,y))|$, ahol Ψ additív karakter, illetve $|\sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \chi(f(x,y))|$, ahol χ multiplikatív karakter, f pedig két változós polinom.

Ilyen típusú összegeket legerősebben Delinge [2], [3], majd Fouvry és Katz [5] becsült, azonban a becslések során van egy feltétel, miszerint $f(x,y)$ nem szinguláris, amely történetesen a mi alkalmazásaink során sajnos nem mindig teljesült... Így akkor be kellett érnünk gyengébb becslésekkel.

Megjegyezzük még, hogy Csikvárival közös hármas cikkünkben [1] kiterjesztettük a problémát $\mathbb{F}_p$-ről $\mathbb{N}$, $\mathbb{Z}$ és $\mathbb{Q}$-ra, de ezekben az esetekben a kombinatorikai eszközök dominálnak.

Hivatkozások

[1] P. Csikvári, A. Sárközy, K. Gyarmati, *Density and Ramsey type results on algebraic equations with restricted solution sets*, Combinatorica 32 (2012), 425-449,

[2] P. Delinge, *La conjecture de Weil, I*, Pub. Math. I. H. E. S. 43 (1974), 273-307.

[3] P. Delinge, *La conjecture de Weil, II*, Pub. Math. I. H. E. S. 43 (1980), 137-250.

[4] P. Erdős, N. H. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. 7 (1957), 861-865.

[5] E. Fouvry, N. Katz, *A general stratification theorem for exponential sums, and applications*, J. Reine Angew. Math. 540 (2001), 115-166.

[6] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97 (1) (2001), 53-65.

[7] K. Gyarmati, A. Sárközy, *Equations in finite fields with restricted solution sets, I. (Character sums.)*, Acta Math. Hungar. 118 (2008), 129-148.

[8] K. Gyarmati, A. Sárközy, *Equations in finite fields with restricted solution sets, II. (Algebraic equations.)*, Acta Math. Hungar. 119 (2008), 259-280.

[9] A. Sárközy, *On sums and products of residues modulo p*, Acta Arith. 118 (4) (2005), 403-409.

13. Éles-e a Weil tétel?

Winterhof (a fentinél kicsit általánosabban) a következőt igazolta [1, Lemma 2]-ben:

13.1 Lemma. *Legyen $\mathcal{A} \subseteq \mathbb{F}_p$ tetszőleges halmaz. Ekkor*

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathcal{A}}\chi(x+a)\right|^2 = p|\mathcal{A}| - |\mathcal{A}|^2.$$

A 13.1 Lemma bizonyítása. Valóban,

$$\begin{aligned}
\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathcal{A}}\chi(x+a)\right|^2 &= \sum_{x\in\mathbb{F}_p}\sum_{a,b\in\mathcal{A}}\chi(x+a)\overline{\chi}(x+b)\\
&= \sum_{x\in\mathbb{F}_p}\sum_{a\in\mathcal{A}}\underbrace{\left|\chi(x+a)\right|^2}_{\begin{cases}1, & \text{ha } x\neq -a\\ 0, & \text{ha } x=-a\end{cases}} + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{x\in\mathbb{F}_p}\chi(x+a)\overline{\chi}(x+b)\\
&= (p-1)|\mathcal{A}| + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{x\in\mathbb{F}_p}\chi(x+a)\overline{\chi}(x+b)\\
&= (p-1)|\mathcal{A}|\sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{\substack{x\in\mathbb{F}_p\\ x\neq -b}}\chi\left(\frac{x+a}{x+b}\right).
\end{aligned}$$

Könnyű látni, hogy ahogy x fut az $\mathbb{F}_p\setminus\{b\}$ halmaz elemein $\frac{x+a}{x+b}$ minden értéket felvesz kivéve a 1-t. Ezért:

$$\begin{aligned}
\sum_{x\in\mathbb{F}_p}\left|\sum_{a\in\mathcal{A}}\chi(x+a)\right|^2 &= (p-1)|\mathcal{A}| + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}\sum_{\substack{y\in\mathbb{F}_p\\ y\neq 1}}\chi(y)\\
&= (p-1)|\mathcal{A}| + \sum_{\substack{a,b\in\mathcal{A}\\ a\neq b}}(-1)
\end{aligned}$$

$$= (p-1)|\mathcal{A}| - |\mathcal{A}|\left(|\mathcal{A}| - 1\right)$$
$$= p|\mathcal{A}| - |\mathcal{A}|^2.$$

A fenti lemmának azonnal van egy érdekes következménye. Vegyük a 13.1 Lemmában az $\mathcal{A}$ halmazt egymást követő számoknak: $\mathcal{A} = \{1, 2, \ldots, N\}$. Ekkor a 13.1 Lemma szerint:

$$\sum_{x \in \mathbb{F}_p} \left| \sum_{a=1}^{N} \chi(x+a) \right|^2 = pN - N^2.$$

Vagyis létezik egy $x \in \mathbb{F}_p$, mondjuk $x = M$, amire

$$\left| \sum_{a=1}^{N} \chi(M+a) \right|^2 \geq N - \frac{N^2}{p}$$
$$\left| \sum_{a=1}^{N} \chi(M+a) \right| \geq \sqrt{N - \frac{N^2}{p}}$$
$$\left| \sum_{x=M+1}^{M+N} \chi(x) \right| \geq \sqrt{N - \frac{N^2}{p}}.$$

Ha $p \geq 3$, akkor N-et $(p-1)/2$-nek választva, a következő adódik:

13.2 KÖVETKEZMÉNY. *Ha $p \geq 3$ prím, akkor $\exists\, M \in \mathbb{F}_p$, amelyre*

$$\left| \sum_{x=M+1}^{M+(p-1)/2} \chi(x) \right| \geq \sqrt{\frac{p-1}{2} - \frac{1}{4p}} > \frac{\sqrt{p}}{\sqrt{2}} - 1.$$

Hogy ez mennyire éles, arról a következő fejezetben lesz szó.

Van egy még izgalmasabb alkalmazás, amikor azt firtatjuk, hogy a Weil tétel multiplikatív karakterekre vonatkozó alakja (12.9 Tétel) mennyire éles.

Az egyszerűség kedvéért legyen most a χ karakter rendje $p-1$ és $f(x) = x^k + m$ alakú, ahol a polinom fokszámára $k \mid p-1$ és

$k < p-1$ teljesül. Ekkor $f(x)$ nyilván nem $cg(x)^{p-1}$ alakú polinom. A következőt fogjuk bizonyítani:

13.3 Következmény. *Legyen p páratlan prím, $k \mid p-1$, $k < p-1$ és χ egy $p-1$-ed rendű multiplikatív karakter. Ekkor $\exists\ m \in \mathbb{F}_p^*$, hogy az $f(x) = x^k + m$ polinomra*

$$\sum_{x \in \mathbb{F}_p} \chi(f(x)) > \sqrt{(k-1)p}.$$

A bizonyításhoz csak kicsit szükséges módosítani a 13.1 Lemma bizonyítását.

A 13.3 Következmény bizonyítása. Vizsgáljuk most a $\sum_{x \in \mathbb{F}_p} \left| \sum_{a \in \mathbb{F}_p^*} \chi(x + a^k) \right|^2$ összeget.

$$\sum_{x \in \mathbb{F}_p} \left| \sum_{a \in \mathbb{F}_p^*} \chi(x + a^k) \right|^2 = \sum_{x \in \mathbb{F}_p} \sum_{a,b \in \mathbb{F}_p^*} \chi(x + a^k)\overline{\chi}(x + b^k)$$

$$= \sum_{x \in \mathbb{F}_p} \sum_{\substack{a,b \in \mathbb{F}_p^* \\ a^k = b^k}} \underbrace{\left| \chi(x + a^k) \right|^2}_{\begin{cases} 1, & \text{ha } x \neq -a^k \\ 0, & \text{ha } x = -a^k \end{cases}} + \sum_{\substack{a,b \in \mathbb{F}_p^* \\ a^k \neq b^k}} \sum_{x \in \mathbb{F}_p} \chi(x + a^k)\overline{\chi}(x + b^k)$$

Rögzített $b \not\equiv 0 \pmod p$-re mindig pont k darab a létezik, amelyre $a^k \equiv b^k \pmod p$. (Itt azt használjuk, hogy $(c, p) = 1$ esetén $x^k \equiv c \pmod p$ kongruencia akkor oldható meg, ha $c^{(k-1)/(k-1,p)} \equiv 1 \pmod p$ és ekkor a megoldások száma $(k, p-1)$.) Így:

$$\sum_{x \in \mathbb{F}_p} \left| \sum_{a \in \mathbb{F}_p^*} \chi(x + a^k) \right|^2 = (p-1)^2 k + \sum_{\substack{a,b \in \mathbb{F}_p^* \\ a^k \neq b^k}} \sum_{x \in \mathbb{F}_p} \chi(x + a^k)\overline{\chi}(x + b^k)$$

$$= (p-1)^2 k + \sum_{\substack{a,b \in \mathbb{F}_p^* \\ a^k \neq b^k}} \sum_{\substack{x \in \mathbb{F}_p \\ x \neq -b^k}} \chi\left(\frac{x+a^k}{x+b^k}\right).$$

Könnyű látni, hogy ahogy x fut az $\mathbb{F}_p \setminus \{-b^k\}$ halmaz elemein $\frac{x+a^k}{x+b^k}$ minden értéket felvesz kivéve a 1-t. Ezért:

$$\begin{aligned}
\sum_{x \in \mathbb{F}_p} \left| \sum_{a \in \mathbb{F}_p^*} \chi(x+a^k) \right|^2 &= (p-1)^2 k + \sum_{\substack{a,b \in \mathbb{F}_p^* \\ a^k \neq b^k}} \sum_{\substack{y \in \mathbb{F}_p \\ y \neq 1}} \chi(y) \\
&= (p-1)^2 k - (p-1)(p-1-k) \\
&= (p-1)(pk-p+1) \\
&\geq (p-1)p(k-1) + 2. \qquad (13.1)
\end{aligned}$$

Vegyük észre, hogy $x = 0$ esetén

$$\sum_{a \in \mathbb{F}_p^*} \chi(x+a^k) = \sum_{a \in \mathbb{F}_p^*} \chi(a^k) = \sum_{a \in \mathbb{F}_p^*} \chi^k(a) = -1,$$

mivel χ^k is egy multiplikatív karakter. Ezért (13.1)-ből adódóan:

$$\sum_{x \in \mathbb{F}_p^*} \left| \sum_{a \in \mathbb{F}_p^*} \chi(x+a^k) \right|^2 \geq (p-1)p(k-1) + 1.$$

Vagyis létezik egy $x \in \mathbb{F}_p^*$, mondjuk $x = m$, amire

$$\begin{aligned}
\left| \sum_{a \in \mathbb{F}_p^*} \chi(m+a^k) \right|^2 &> (k-1)p \\
\sum_{a \in \mathbb{F}_p^*} \chi(m+a^k) &> \sqrt{(k-1)p}.
\end{aligned}$$

Ez utóbbiba a helyébe x-et írva azonnal adódik a 13.3 Következmény állítása.

Hivatkozások

[1] A. Winterhof, *Some estimates for character sums and applications*, Designs, Codes and Cryptography 22 (2001), 123-131.

14. Pólya-Vinogradov egyenlőtlenség és Vinogradov módszere nem teljes karakterösszegek becslésére

1918-ban Pólya és Vinogradov egymástól függetlenül a következőt igazolta:

14.1 Tétel. (Pólya-Vinogradov egyenlőtlenség) *$\exists$ egy c pozitív abszolút konstans úgy, hogy ha $m \in \mathbb{N}$, $m > 2$ és χ multiplikatív karakter* mod m*, $\chi \neq \chi_0$, $M \in \mathbb{Z}$ és $N \in \mathbb{N}$, akkor*

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < c\sqrt{m} \log m.$$

Megjegyzés. A triviális felső becslés a szummára N. Így a Pólya-Vinogradov egyenlőtlenség akkor nem triviális, ha $N \gg \sqrt{m} \log m$.

A tételt Vinogradov törvényét alkalmazva bizonyítjuk be, amely nem teljes összegek becslését teljes összegek becslésére vezeti vissza.

14.2 Tétel. (Vinogradov) *Ha $m \in \mathbb{N}$, $x, y \in \mathbb{N}$, $(0 <) x < y \leq m$ és $a_1, a_2, \ldots, a_m \in \mathbb{C}$, akkor*

$$F(t) = \sum_{j=1}^{m} a_j e\left(\frac{jt}{m}\right)$$

-et írva, és

$$A = \sum_{j=1}^{m} a_j$$

-et véve kapjuk, hogy

$$\left| \sum_{n=x}^{y} a_n - \frac{y-x+1}{m} A \right| \leq \frac{1}{2m} \sum_{\ell=1}^{m-1} \frac{|F(\ell)|}{\left|\left|\frac{\ell}{m}\right|\right|},$$

ahol $||s||$ az s-nek a legközelebbi egésztől való távolságát jelöli.

14.3 KÖVETKEZMÉNY. (Vinogradov)

$$\left|\sum_{n=x}^{y} a_n - \frac{y-x+1}{m}A\right| \le (\log m + 1) \max_{1\le \ell \le m-1} |F(\ell)|.$$

A 14.2 Tétel bizonyítása.

$$\begin{aligned} S &= \sum_{n=x}^{y} a_n \\ &= \sum_{n=x}^{y}\sum_{j=1}^{m}\frac{1}{m}\sum_{\ell=0}^{m-1} e\left(\frac{\ell(j-n)}{m}\right)a_j \\ &= \frac{1}{m}\sum_{\ell=0}^{m-1}\sum_{n=x}^{y}\sum_{j=1}^{m}\underbrace{a_j e\left(\frac{\ell(j-n)}{m}\right)}_{a_j e\left(-\frac{\ell n}{m}\right)e\left(\frac{\ell j}{m}\right)} \underbrace{=}_{\substack{\ell=0 \text{ tagot}\\ \text{külön vesszük}}} \\ &= \underbrace{\frac{1}{m}\sum_{n=x}^{y}\overbrace{\sum_{j=1}^{m} a_j}^{A}}_{\frac{y-x+1}{m}A} + \frac{1}{m}\sum_{\ell=1}^{m}\left(\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right)\underbrace{\left(\sum_{j=1}^{m} a_j e\left(\frac{\ell j}{m}\right)\right)}_{F(\ell)}. \end{aligned}$$

Így:

$$\left|S - \frac{y-x+1}{m}A\right| \le \frac{1}{m}\sum_{\ell=1}^{m}\left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| |F(\ell)|\,.$$

Itt:

$$\left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| = \left|\frac{1-e\left(-\frac{(y-x+1)\ell}{m}\right)}{1-e\left(-\frac{\ell}{m}\right)}\right| \le \frac{2}{\left|1-e\left(\frac{\ell}{m}\right)\right|}.$$

↑ számtani sorozat $e\left(-\frac{\ell}{n}\right)$ kvócienssel

Ekkor $|1-e(\alpha)| \geq 4\,||\alpha||$-t használva (ld. 2.2 Lemma):

$$\left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| \geq \frac{2}{4\,||\frac{\ell}{m}||} = \frac{1}{2\,||\frac{\ell}{m}||}.$$

Azaz

$$\begin{aligned}\left|S - \frac{y-x+1}{m}A\right| &\leq \frac{1}{m}\sum_{\ell=1}^{m}\left|\sum_{n=x}^{y} e\left(-\frac{\ell n}{m}\right)\right| |F(\ell)| \\ &\leq \frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{|F(\ell)|}{||\frac{\ell}{m}||},\end{aligned}$$

ami éppen a tétel állítása.

A 14.3 Következmény bizonyítása.

$$\frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{|F(\ell)|}{||\frac{\ell}{m}||} \leq \left(\max_{1\leq\ell\leq m-1}|F(\ell)|\right)\frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{1}{||\frac{\ell}{m}||}. \qquad (14.1)$$

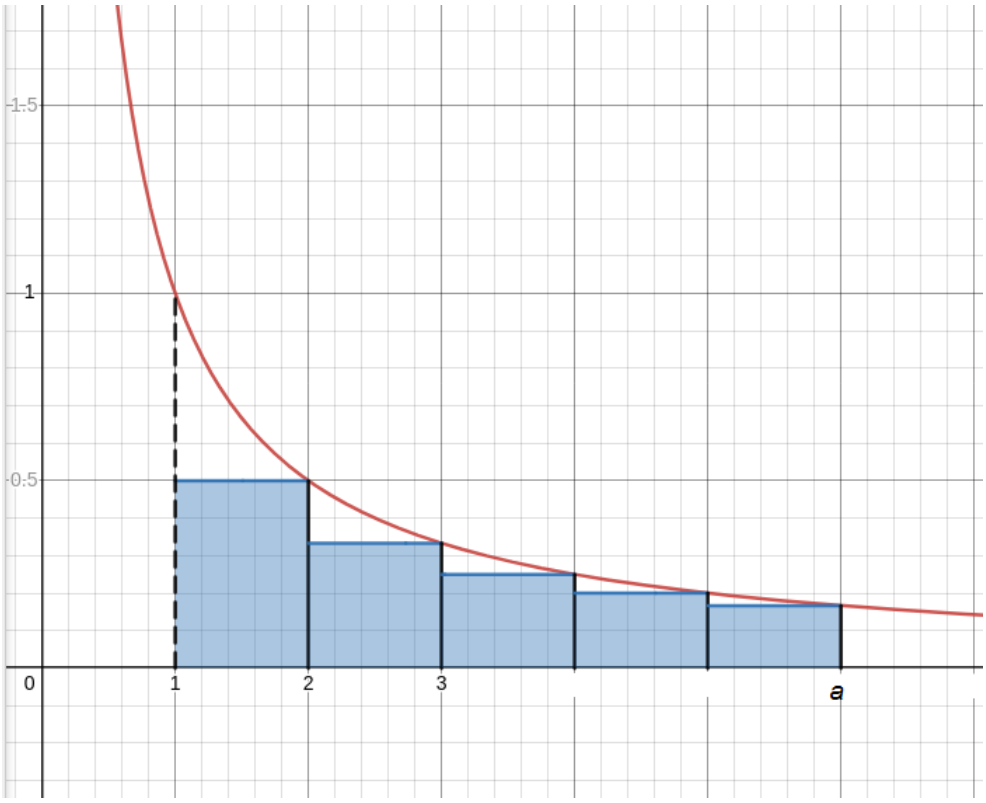
Itt:

$$\sum_{\ell=1}^{m-1}\frac{1}{||\frac{\ell}{m}||} \leq 2\sum_{1\leq\ell\leq[m/2]}\frac{1}{\frac{\ell}{m}} = 2m\sum_{1\leq\ell\leq[m/2]}\frac{1}{\ell}, \qquad (14.2)$$

ahol

$$\sum_{1\leq\ell\leq a}\frac{1}{\ell} = 1 + \sum_{2\leq\ell\leq a}\frac{1}{\ell} \leq 1 + \int_1^a \frac{1}{x}dx = 1 + \log a.$$

Ez utóbbi egyenlőtlenség a következő ábrával szemléltethető:



Ezt (14.2)-be írva:

$$\sum_{\ell=1}^{m-1} \frac{1}{\left|\left|\frac{\ell}{m}\right|\right|} \leq 2m(1+\log[m/2]) \leq 2m(1+\log m).$$

Így (14.1) alapján:

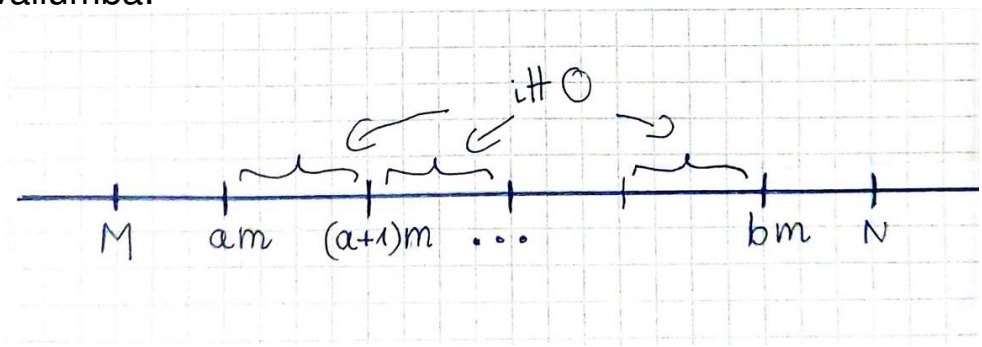
$$\begin{aligned}\frac{1}{2m}\sum_{\ell=1}^{m-1}\frac{|F(\ell)|}{\left|\left|\frac{\ell}{m}\right|\right|} &\leq \left(\max_{1\leq\ell\leq m-1}|F(\ell)|\right)\frac{1}{2m}\cdot 2m(1+\log m)\\ &= (\log m+1)\left(\max_{1\leq\ell\leq m-1}|F(\ell)|\right).\end{aligned}$$

A 14.1 Tétel bizonyítása.

A eset. Tegyük fel, hogy χ primitív karakter mod m. Tekintsük azokat az n-eket, amelyre

$$M \leq n \leq M+N.$$

$\sum_{n=1}^{m} \chi(n) = 0$ és a periodicitás miatt a szumma az alábbi intervallumokon 0, míg az első és utolsó rövid intervallum eltolható a $(0, p]$ intervallumba:



Így egy

$$\left| \sum_{n=x}^{y} \chi(n) \right|$$

$0 \le x \le y$, $y - x \le p$ típusú összeg becslése a feladat. (Szükség esetén, ha a $(0, p]$ intervallumnak az legelején és legvégén is van egy-egy diszjunkt részintervallum, akkor a komplementer intervallumon becsüljük az összeget, míg, ha a fenti két intervallum metszi egymást, akkor elég a metszeten becsülni az összeget, hiszen $\sum_{n=1}^{m} \chi(n) = 0$.)

A 14.3 Következményt $a_n = \chi(n)$-nel használva kapjuk, hogy

$$A = \sum_{n=1}^{m} \chi(n) = 0$$

és

$$\left| \sum_{n=x}^{y} \chi(n) \right| \le (\log m + 1) \max |F(\ell)| ,$$

ahol a Gauss összegekről tanultak alapján (ld. 5. fejezet):

$$|F(\ell)| = \left| \sum_{j=1}^{m} \chi(j) e\left(\frac{j\ell}{m}\right) \right| = |\overline{\chi}(\ell)\tau(\chi)| \le \sqrt{m}.$$

Így valóban:

$$\left|\sum_{n=x}^{y}\chi(n)\right| \leq (\log m + 1)\sqrt{m}$$
$$\left|\sum_{n=M+1}^{M+N}\chi(n)\right| \leq (\log m + 1)\sqrt{m}.$$

B eset. Nem primitív χ-kre: az A esetre redukálható, lásd Davenport [1, 136. oldal].

Megjegyzések. A Pólya-Vinogradov majdnem éles: a $\log m$ nem hagyható el teljesen (ld. pl. 13.2 Következmény), a legjobb esetben egy $\log\log m$-mel helyettesíthető. Az első eredményt Schur érte el 1918-ban, miszerint minden χ primitív karakterre

$$\max_{M,N}\left|\sum_{n=N}^{N+M}\chi(N)\right| > \frac{1}{2\pi}\sqrt{m}.$$

Itt az $\frac{1}{2\pi}$ konstanst sikerült levinnünk közel $\frac{1}{\sqrt{2}}$-re prímmodulus esetén a 13.2 Következményben.

Végtelen sok karakter létezik még élesebb becsléssel. Payley [3] 1932-ben a következőt igazolta:

14.4 Tétel. (Payley) *Végtelen sok m és $\chi \neq \chi_0 \bmod m$ karakter létezik, amelyre*

$$\max_{M,N}\left|\sum_{n=N}^{N+M}\chi(N)\right| > c\sqrt{m}\log\log m.$$

Montgomery és Vaughan [2] 1977-ben feltétezve az általánosított Riemann hipotézist a következőt igazolta:

14.5 Tétel. (Montgomery-Vaughan) *$\exists$ egy c pozitív abszolút konstans úgy, hogy ha igaz az általánosított Riemann hipotézis,*

$m, N \in \mathbb{N}$, $m > 2$ *és* χ *multiplikatív karakter* mod m, $\chi \neq \chi_0$, $M \in \mathbb{Z}$, *akkor*

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < c\sqrt{m} \log \log m.$$

Hivatkozások

[1] H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics 74, Springer New York, 2013, Originally published by Markham Publishing Co., 1967.

[2] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math.43 (1) (1977), 69–82.

[3] R. E. A. C. Paley, *A theorem on characters*, J. Lond. Math. Soc. 7 (1932), 28–32.

15. Rövid multiplikatív karakterösszegek és a legkisebb kvadratikus nem maradék.

A Pólya-Vinogradov egyenlőtlenség: ha $\chi \neq \chi_0$ egy multiplikatív karakter mod m és $M \in \mathbb{Z}$, $N \in \mathbb{N}$, akkor

$$\left| \sum_{n=M+1}^{N} \chi(n) \right| < c\sqrt{m} \log m. \tag{15.1}$$

Triviálisan

$$\left| \sum_{n=M+1}^{N} \chi(n) \right| < N$$

(mivel minden tag abszolút értékben ≤ 1 és M tag van összesen). Így (15.1) csak akkor nem triviális, ha az (15.1)-ben a felső becslés $< N$, azaz

$$c\sqrt{m} \log m < M.$$

Mi történik akkor, ha ez nem teljesül, vagyis rövid karakterösszegeket tekintünk

$$N = o(\sqrt{m} \log m)$$

-mel? Nagyon fontos, hogy ekkor is tudjunk nem triviális becslést adni, mondjuk egy

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| = o(N)$$

típusú becslést igazolni.

A következőkben bemutatunk egy alkalmazását egy ilyen jellegű becslésnek, nevezetesen a legkisebb kvadratikus nem maradék becslését vizsgáljuk. Ez az egyik az $5-6$ legfontosabb probléma közül a számelméletben.

15.1 DEFINÍCIÓ. *Ha p prím, akkor a legkisebb pozitív egész $q = q(p)$-t, ahol $\left(\frac{q}{p}\right) = -1$ a legkisebb kvadratikus nem-maradéknak nevezzük.*

A Pólya-Vinogradov egyenlőtlenség azonnal ad egy becslést $q(p)$-ra. Valóban (15.1)-et alkalmazva $\chi(n) = \left(\frac{n}{p}\right)$, $M = 0$, $N = q(p) - 1$-re kapjuk, hogy

$$\left| \sum_{n=1}^{q(p)-1} \left(\frac{n}{p}\right) \right| \leq c\sqrt{p}\log p,$$

de $1 \leq n \leq q(p) - 1$ esetén $\left(\frac{n}{p}\right) = 1$, így

$$q(p) - 1 < c\sqrt{p}\log p$$
$$q(p) = O(\sqrt{p}\log p).$$

Ez a becslés Burgess tételével [1] javítható tovább. De mielőtt ezt megnéznénk, érdemes meggondolni, hogy elemileg vajon milyen becslés adható $q(p)$-re.

Tegyük fel, hogy $q(p) \geq \sqrt{p}+1$. Ekkor $\left\lceil \frac{p}{q(p)} \right\rceil \leq \frac{p}{q(p)}+1 < q(p)$, vagyis $\left\lceil \frac{p}{q(p)} \right\rceil$ kvadratikus maradék, hiszen minden $q(p)$-nél kisebb pozitív egész érték kvadratikus maradék mod p.

Tehát $\left\lceil \frac{p}{q(p)} \right\rceil q(p)$ kvadratikus nem-maradék. Viszont

$$p = \frac{p}{q(p)}q(p) < \left\lceil \frac{p}{q(p)} \right\rceil q(p) < \left(\frac{p}{q(p)} + 1\right) q(p) = p + q(p)$$

(itt használtuk, hogy $\frac{p}{q(p)}$ nem egész azaz $\left\lceil \frac{p}{q(p)} \right\rceil$ szigorúan $\frac{p}{q(p)}$ és $\frac{p}{q(p)} + 1$ között van).

Vagyis $\left\lceil \frac{p}{q(p)} \right\rceil q(p)$ kvadratikus nem maradék p-vel vett osztási maradéka kisebb mint $q(p)$, ami ellentmond $q(p)$ definíciójának. Azaz

$$q(p) < \sqrt{p} + 1.$$

Ennél egy picit még lejjebb tudunk menni elemileg is akár, ha azt is tudjuk, hogy p egy $4k+1$ alakú prím. Ehhez legyen

$$\mathcal{A} = \{0, 1, 2, \ldots, q(p) - 1\},$$

n pedig egy rögzített kvadratikus nem-maradék. Ekkor az

$$\mathcal{A} + n\mathcal{A} = \{a + na' : \ a, a' \in \mathcal{A}\}$$

halmazban minden elem csak egyszer van reprezentálva. Ugyanis, ha

$$\begin{aligned} a_1 + na_1' &\equiv a_2 + na_2' \pmod{p} \\ a_1 - a_2 &\equiv n(a_2' - a_1') \pmod{p}. \end{aligned}$$

Itt viszont

$$a_1 - a_2,\ a_2' - a_1' \in \{-q(p)+1, -q(p)+2, \ldots, q(p)-2, q(p)-1\},$$

amely halmazban a 0-t kivéve minden szám kvadratikus maradék.

A Legendre szimbólum multiplikativitása miatt

$$\begin{aligned} \left(\frac{a_1 - a_2}{p}\right) &= \left(\frac{n}{p}\right)\left(\frac{a_2' - a_1'}{p}\right) \\ 1 &= (-1) \cdot 1, \end{aligned}$$

ami ellentmondás. Egyetlen kivétel van, ha $a_1 - a_2 = 0$ és $a_2' - a_1' = 0$, amikor is $a_1 = a_2$ és $a_1' = a_2'$.

Vagyis valóban az

$$\mathcal{A} + n\mathcal{A} = \{a + na' : \ a, a' \in \mathcal{A}\}$$

halmazban minden elem csak egyszer van reprezentálva. Azaz $|\mathcal{A} + n\mathcal{A}| = |\mathcal{A}|^2$. Másrészt

$$\mathcal{A} + n\mathcal{A} \subseteq \mathbb{Z}_p^2,$$

tehát

$$\begin{aligned} |\mathcal{A}|^2 &\leq p \\ |\mathcal{A}| &\leq \sqrt{p} \\ q(p) &\leq \sqrt{p}. \end{aligned}$$

Ezzel a legkisebb kvadratikus nem-maradék elemi becslésére vonatkozó részt befejeztük. De vajon mondható-e több a fentieknél az eleminél mélyebb eszközökkel? Ekkor Burgess tétele segít:

15.2 TÉTEL. (Burgess) *$\exists\ c > 0$, amelyre, ha p prím, $N, r \in \mathbb{N}$, $N \in \mathbb{Z}$, akkor*

$$\left| \sum_{n=M+1}^{M+N} \chi(n) \right| < cN^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}}.$$

A tételt itt nem bizonyítjuk. A bizonyítás Weil tételén, azaz $\left|\sum_{x \in \mathbb{F}_p} \chi(x)\right|$ becslésén alapul.

Ebből a tételből:

$$\begin{aligned} q(p) - 1 &< cq(p)^{1-1/r} p^{(r+1)/4r^2} (\log p)^{1/r} \\ q(p)^{1/r} &\ll p^{(r+1)/4r^2} (\log p)^{1/r} \end{aligned}$$

$$q(p) \ll p^{(r+1)/4r} \log p)$$

következik, azaz $\forall\, \varepsilon > 0$-ra

$$q(p) = o\left(p^{1/4+\varepsilon}\right).$$

Ezen a becslésen Vinogradov módszerével [3] lehet javítani.

15.3 TÉTEL. (Vinogradov) *Ha* $\left|\sum_{n=M+1}^{M+N} \chi(n)\right| = o(N)$ *fennáll valamilyen* N*-re, akkor* $\varepsilon > 0$, $M > M_0(\varepsilon)$ *esetén, akkor*

$$q(p) < M^{\frac{1}{4\sqrt{e}}}.$$

15.4 KÖVETKEZMÉNY.

Pólya-Vinogradov: $M = p^{1/2+\delta} \;\Rightarrow\; q(p) \ll p^{\frac{1}{2\sqrt{e}}+\varepsilon}.$

Burgess: $M = p^{1/4+\delta} \;\Rightarrow\; q(p) \ll p^{\frac{1}{4\sqrt{e}}+\varepsilon}$

minden $\varepsilon > 0$*-ra.*

A 15.3 Tétel bizonyítása.

15.5 LEMMA.

$$\sum_{p \le x} \frac{1}{p} = \log\log x + c + o(1),$$

ahol c *a Meissel–Mertens konstans.*

A 15.5 Lemma bizonyítása. A lemma Mertens második tétele [2], itt nem ismertetjük.

A Pólya-Vinogradov egyenlőtlenséghez hasonlóan rövid karakter összeget becsülünk a

$$\chi(n) \begin{cases} \left(\frac{n}{p}\right) & \text{ha } (n,p) = 1 \\ 0 & \text{ha } p \mid n \end{cases}$$

választással. A tétel feltételei szerint

$$
\begin{aligned}
o(M) &= \sum_{n=1}^{M} \left(\frac{n}{p}\right) \\
&= \sum_{n=1}^{M} 1 + \sum_{n=1}^{M} \left(\left(\frac{n}{p}\right) - 1\right) \\
&= M - 2\Big|\underbrace{\{n:\ 1 \le n \le M,\ \left(\frac{n}{p}\right) = -1\}}_{\substack{\exists \text{ egy } r \text{ prím, hogy } r \le n,\\ \left(\frac{r}{p}\right) = -1,\ r \mid n,\\ q(p) \text{ definíciója miatt}\\ q(p) \le r \le n \le M}}\Big| \\
&\ge M - 2 \sum_{\substack{q(p) \le r \le n \\ r \text{ prím}}} |\{n:\ 1 \le n \le M,\ r \mid n\}| \\
&\ge M - 2 \sum_{\substack{q(p) \le r \le n \\ r \text{ prím}}} \frac{M}{r} \\
&= M\left(1 - 2\left(\sum_{\substack{r \le M \\ r \text{ prím}}} \frac{1}{r} - \sum_{\substack{r < q(p) \\ r \text{ prím}}} \frac{1}{r}\right)\right) \\
&= 2M\left(\frac{1}{2} - (\log\log M + c + o(1)) + (\log\log q(p) + c + o(1))\right) \\
&= 2M\left(\frac{1}{2} - \log\frac{\log M}{\log q(p)} + o(1)\right).
\end{aligned}
$$

Ezután indirekten bizonyítjuk a tételt. Feltesszük, hogy

$$q(p) \ge M^{1/\sqrt{e}+\varepsilon}.$$

Ekkor

$$o(M) \ge 2M\left(\frac{1}{2} - \log\frac{\log M}{\log q(p)} + o(1)\right)$$

$$
\begin{aligned}
&\geq 2M \left(\frac{1}{2} - \log \frac{\log M}{\log q(p)} \right) \\
&\geq 2M \left(\frac{1}{2} - \log \frac{\log M}{\log M^{1/\sqrt{e}+\varepsilon}} \right) \\
&\geq 2M \left(\frac{1}{2} - \log \frac{1}{1/\sqrt{e}+\varepsilon} \right) \\
&\geq 2M \left(\frac{1}{2} + \log \left(1/\sqrt{e}+\varepsilon\right) \right) \\
&\geq 2M \left(\frac{1}{2} + \log(1/\sqrt{e}) + \log \left(1+\varepsilon\sqrt{e}\right) \right) \\
&= 2M \underbrace{\log \left(1+\varepsilon\sqrt{e}\right)}_{\text{konstans} >0} \\
&\neq o(M).
\end{aligned}
$$

Hivatkozások

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. 12 (3) (1962), 179–192.

[2] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine angew. Math. 78 (1874), 46–62.

[3] I. M. Vinogradov, *Sur la distribution des résidus et des non-résidus des puissances*, Journal Physico-Math. Soc. Univ. Perm, (1)(1918), 94–96.

16. Nagy szita

Ezt a módszert Linnik fedezte fel 1941-ben, miközben kvadratikus nem-maradékok eloszlását tanulmányozta. Később Rényi (1947-1950) általánosította Linnik módszerét, szisztematikusan vizsgálta, és a következő híres eredményt bizonyította:

16.1 TÉTEL. (Rényi) *$\exists$ egy k szám, hogy $\forall\, n \in \mathbb{N}$ felírható*

$$p + P_k = n$$

alakban, ahol p prím, P_k pedig legfeljebb k prím szorzata.

Ez a tétel részeredmény a Goldbach sejtés megoldásához vezető úton. Rényi nem számolta ki egy explicit k-t, de később meghatározták: Barban $k = 4$, Bombieri $k = 3$, végül Chen [3] $k = 2$ $\forall\, n > n_0$-ra.

A nagy szita kifejlesztése során ekkor Roth, Bombieri, Davenport, Halberstam, Montgomery és Gallagher jelentős előrelépést tett.

A nagy szitát mint analitikus állítást Davenport és Halberstam fogalmazta meg először.

16.2 TÉTEL. (Nagy szita analitikus alakja) *Tegyük fel, hogy $M \in \mathbb{Z}$, $N \in \mathbb{N}$, $a_{M+1}, a_{M+2}, \ldots, a_{M+N} \in \mathbb{C}$, $\mathbf{X} = \{x_1, \ldots, x_R\} \in \mathbb{R}$ olyan, hogy $1 \leq i < j \leq R$ esetén $||x_i - x_j|| \geq \delta > 0$. Legyen*

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha). \tag{16.1}$$

Ekkor

$$\sum_{i=1}^{R} |S(x_i)|^2 \leq \left(\frac{1}{\delta} + \pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2. \tag{16.2}$$

Megjegyzések. Ha az $\{x_i\}$-k egyenletesen vannak eloszolva a $[0,1]$ intervallumon úgy, hogy $\delta = \frac{1}{R}$ és $N \ll R$, akkor (16.2) a következőt mondja:

$$\underbrace{\frac{1}{R}\sum_{i=1}^{R}|S(x_i)|^2}_{\substack{\text{Riemann összeg az}\\ \int_0^1|S(\alpha)|^2d\alpha\text{-hoz}}} \ll \underbrace{\sum_{n=M+1}^{M+N}|a_n|^2}_{\substack{\text{A Parseval formula szerint}\\ =\int_0^1|S(\alpha)|^2d\alpha}} .$$

A tétel a következőt mondja ki: egy „elég finom” Riemann összeg felülről becsülhető az integrál konstansszorosával.

Selberg (ld. pl. [8]) konstans szorzót javított a nagy szita becslésén, belátva, hogy

$$\sum_{i=1}^{R}|S(x_i)|^2 \le \left(\frac{1}{\delta}+N-1\right)\sum_{n=M+1}^{M+N}|a_n|^2. \tag{16.3}$$

is igaz.

A 16.2 Tétel bizonyítása. Gallagher ötlete [5] a következő: $|S(\alpha)|^2$ közel van $\frac{1}{\delta}\int_{\alpha-\delta/2}^{\alpha+\delta/2}|S(\beta)|^2\,d\beta$-hoz.

A két kifejezés közötti összefüggés $S(\beta)$ és $S'(\beta)$ segítségével fejezhető ki. E célból „Sobolev típusú” egyenlőtlenséget [10] használunk:

16.3 Lemma. *Ha $f(x):\ [0,1]\to\mathbb{C}$-nek van folytonos első deriváltja, akkor $0\le x\le 1$ esetén*

$$|f(x)| \le \int_0^1 \left(|f(y)|+|f'(y)|\right)dy \tag{16.4}$$

és

$$\left|f\left(\frac{1}{2}\right)\right| \le \int_0^1 \left(|f(x)|+\frac{1}{2}|f'(x)|\right)dx \tag{16.5}$$

A 16.3 Lemma bizonyítása.

1. Állítás:

$$f(x) = \int_0^1 f(u)du + \int_0^x uf'(u)du + \int_x^1 (u-1)f'(u)du.$$

Valóban a jobboldalon az utolsó integrált szétbontva:

$$\int_0^1 f(u)du + \underbrace{\int_0^x uf'(u)du + \int_x^1 uf'(u)du}_{\int_0^1 uf'(u)du = [uf(u)]_0^1 - \int_0^1 f(u)du} - \int_x^1 f'(u)du$$

$$= \int_0^1 f(u)du + [uf(u)]_0^1 - \int_0^1 f(u)du - \int_x^1 f'(u)du$$

$$= [uf(u)]_0^1 - \int_x^1 f'(u)du$$

$$= f(1) - (f(1) - f(x))$$

$$= f(x).$$

(16.4) bizonyításához:

$$|f(x)| \le \left|\int_0^1 f(u)du\right| + \left|\int_0^x uf'(u)du\right| + \left|\int_x^1 (u-1)f'(u)du\right|$$

$$\le \int_0^1 |f(u)|\,du + \int_0^x |u|\,|f'(u)|\,du + \int_x^1 |u-1|\,|f'(u)|\,du. \tag{16.6}$$

Először is megjegyezzük, hogy a $[0,1]$ intervallumon $|u|$ és $|u-1| \le 1$, így (16.6)-ból adódóan

$$|f(x)| \le \int_0^1 |f(u)|\,du + \int_0^x |f'(u)|\,du + \int_x^1 |f'(u)|\,du$$

$$= \int_0^1 |f(u)|\,du + \int_0^1 |f'(u)|\,du,$$

ami igazolja (16.4)-t.

(16.5) bizonyításához helyettesítsünk (16.6)-ben $x = \frac{1}{2}$-t. Ekkor

$$\left| f\left(\frac{1}{2}\right)\right| \leq \int_0^1 |f(u)|\,du + \int_0^{1/2} \frac{1}{2}\,|f'(u)|\,du + \int_{1/2}^1 \frac{1}{2}\,|f'(u)|\,du$$
$$= \int_0^1 |f(u)|\,du + \int_0^1 \frac{1}{2}\,|f'(u)|\,du.$$

Ezzel a lemma állítását beláttuk.

A 16.2 Tétel bizonyításban feltehetjük, hogy $M = \left[-\frac{1}{2}(N+1)\right]$.

Ugyanis legyen $M' \overset{\text{def}}{=} \left[-\frac{1}{2}(N+1)\right]$, és $a'_{M'+i} \overset{\text{def}}{=} a_{M+i}$. Ekkor

$$|S(x_r)| = \left|\sum_{n=M+1}^{M+N} a_n e(nx_r)\right|$$
$$= \left|\sum_{i=1}^{N} a_{M+i} e((M+i)x_r)\right|$$
$$= \left|\sum_{i=1}^{N} a_{M+i} e((M'+i)x_r)\right|$$
$$= \left|\sum_{i=1}^{N} a'_{M'+i} e((M'+i)x_r)\right|$$
$$= \left|\sum_{n=M'+1}^{M'+N} a'_n e(nx_r)\right|.$$

Továbbá:

$$\sum_{n=M+1}^{M+N} |a_n|^2 = \sum_{n=M'+1}^{M'+N} |a'_n|^2$$

Vagyis, ha a fenti $M' = \left[-\frac{1}{2}(N+1)\right]$ -re és tetszőleges a'_n-ekre igazoljuk a tételt, abból a fenti átindexelés miatt az összes M-re és a_n számokra is igazoltuk.

Ezután először $|S(x_i)|^2$-t akarjuk becsülni az $I_r = [x_r - \delta/2, x_r + \delta/2]$ intervallumon. Legyen

$$g(x) : [x_r - \delta/2, x_r + \delta/2] \to \mathbb{C}$$

függvény, amelynek van folytonos első deriváltja. Írjuk

$$f(x) = g(\delta x + (x_r - \delta/2)),$$

ahol $x \in [0,1]$. Ekkor

$$\begin{aligned}\left|f\left(\frac{1}{2}\right)\right| &= \left|g\left(\frac{\delta}{2} + \left(x_r - \frac{\delta}{2}\right)\right)\right| = g(x_r) \\ &\leq \int_0^1 |f(x)|\,dx + \int_0^1 \frac{1}{2}\,|f'(x)|\,dx \\ &= \int_0^1 \left|g\left(\delta x + x_r - \frac{\delta}{2}\right)\right| dx + \int_0^1 \frac{1}{2}\left|\delta g'\left(\delta x + x_r - \frac{\delta}{2}\right)\right| dx.\end{aligned}$$

Helyettesítsünk $y = \delta x + x_r - \frac{\delta}{2}$-t:

$$\frac{dy}{dx} = \delta, \quad dx = \frac{dy}{\delta}.$$

Az integrandus határai:

$$\begin{aligned}x = 0 \Rightarrow\ y &= x_r - \frac{\delta}{2} \\ x = 1 \Rightarrow\ y &= x_r + \frac{\delta}{2}.\end{aligned}$$

Így:

$$\begin{aligned}g(x_r) &\leq \int_{x_r-\delta/2}^{x_r+\delta/2} |g\,(y)|\,\frac{1}{\delta}dy + \int_{x_r-\delta/2}^{x_r+\delta/2} \frac{1}{2}\,|\delta g'\,(y)|\,\frac{1}{\delta}dy \\ &= \frac{1}{\delta}\int_{x_r-\delta/2}^{x_r+\delta/2} |g\,(y)|\,dy + \frac{1}{2}\int_{x_r-\delta/2}^{x_r+\delta/2} |\delta g'\,(y)|\,dy.\end{aligned}$$

A fenti egyenlőtlenséget alkalmazzuk $g(x) = S^2(x)$ függvényre:

$$|S(x_r)|^2 \leq \frac{1}{\delta}\int_{x_r-\delta/2}^{x_r+\delta/2} |S(\alpha)|^2\,d\alpha + \int_{x_r-\delta/2}^{x_r+\delta/2} |S(\alpha)S'(\alpha)|\,d\alpha. \tag{16.7}$$

A tétel feltétele szerint az $[x_r - \delta/2, x_r + \delta/2]$ intervallumok nem fedik le egymást modulo 1. Még azt is használva, hogy $S(\alpha)$ periodikus 1 periódussal kapjuk, hogy

$$\sum_{r=1}^{R}\left(\frac{1}{\delta}\int_{x_r-\delta/2}^{x_r+\delta/2}|S(\alpha)|^2\,d\alpha+\int_{x_r-\delta/2}^{x_r+\delta/2}|S(\alpha)S'(\alpha)|\,d\alpha\right)$$
$$\leq\frac{1}{\delta}\int_0^1|S(\alpha)|^2\,d\alpha+\int_0^1|S(\alpha)S'(\alpha)|\,d\alpha.$$

Azaz a (16.7) egyenlőtlenséget összeadva:

$$\sum_{r=1}^{R}|S(x_r)|^2\leq\frac{1}{\delta}\underbrace{\int_0^1|S(\alpha)|^2\,d\alpha}_{\text{Parseval formula}}+\underbrace{\int_0^1|S(\alpha)S'(\alpha)|\,d\alpha}_{\text{Cauchy-Schwarz}}$$
$$\leq\frac{1}{\delta}\sum_{n=M+1}^{M+N}|a_n|^2+\left(\underbrace{\int_0^1|S(\alpha)|^2\,d\alpha}_{\text{Parseval formula}}\right)^{1/2}\left(\underbrace{\int_0^1|S'(\alpha)|^2\,d\alpha}_{\text{Parseval formula}}\right)^{1/2}$$
$$\leq\frac{1}{\delta}\sum_{n=M+1}^{M+N}|a_n|^2+\left(\sum_{n=M+1}^{M+N}|a_n|^2\right)^{1/2}\left(\sum_{n=M+1}^{M+N}|2\pi i n a_n|^2\right)^{1/2}.$$

Itt használjuk, hogy feltehető, hogy $M=\left[-\frac{1}{2}(N+1)\right]$. Ekkor ugyanis $n\in[M+1,M+N]\subseteq[-N/2,N/2]$ miatt $|n|\leq N/2$, így az utolsó zárójelben:

$$\sum_{n=M+1}^{M+N}|2\pi i n a_n|^2\leq\sum_{n=M+1}^{M+N}|2\pi|^2\left|\frac{N}{2}\right|^2|a_n|^2$$
$$=\pi^2N^2\sum_{n=M+1}^{M+N}|a_n|^2,$$

azaz

$$\sum_{r=1}^{R}|S(x_r)|^2\leq\frac{1}{\delta}\sum_{n=M+1}^{M+N}|a_n|^2+\left(\sum_{n=M+1}^{M+N}|a_n|^2\right)^{1/2}\left(\pi^2N^2\sum_{n=M+1}^{M+N}|a_n|^2\right)^{1/2}$$

$$\leq \left(\frac{1}{\delta} + \pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2 .$$

Ezzel a tétel állítását beláttuk.

16.4 Következmény. *Definiáljuk $S(\alpha)$-t úgy, ahogy a 16.2 Tételben. Ekkor minden $Q \in \mathbb{N}$, $Q \geq 2$-re*

$$\sum_{q \leq Q} \sum_{1 \leq a \leq q} |S(a/q)|^2 \leq (Q^2 + \pi N) \sum_{n=M+1}^{M+N} |a_n|^2 .$$

A 16.4 Következmény bizonyítása. Bebizonyítjuk, hogy a tétel feltételei teljesülnek az

$$\mathbf{X} = \left\{ \frac{a}{q} : \ a, q \in \mathbb{N}^+, \ q \leq Q, \ 1 \leq a \leq q, \ (a, q) = 1 \right\}$$

halmazra és $\delta = \frac{1}{Q^2}$-re ugyanis ez a halmaz $\delta = \frac{1}{Q^2}$-"spaced": azaz, legyen $\frac{a}{q}, \frac{b}{r} \in \mathbf{X}$, $(a, q) = (b, r) = 1$, $\frac{a}{q} \neq \frac{b}{r}$. Ekkor tudjuk, hogy

$$0 < \left| \frac{a}{q} - \frac{b}{r} \right|$$

és $0 < \frac{a}{q}, \frac{b}{r} \leq 1$, így

$$\left| \frac{a}{q} - \frac{b}{r} \right| < 1.$$

Másrészről definiáljuk $c \in \mathbb{Z}$-t

$$\left| \frac{a}{q} - \frac{b}{r} \right| = \frac{|ar - qb|}{qr} = \frac{c}{qr}$$

-rel, ekkor

$$\left| \frac{a}{q} - \frac{b}{r} \right| \in \left\{ \frac{1}{qr}, \frac{2}{qr}, \frac{3}{qr}, \cdots \frac{qr-1}{qr}, \right\} .$$

Tehát

$$\left|\left|\frac{a}{q}-\frac{b}{r}\right|\right| = \left|\left|\left|\frac{a}{q}-\frac{b}{r}\right|\right|\right| \in \left\{\frac{1}{qr}, \frac{2}{qr}, \frac{3}{qr}, \cdots \frac{qr-1}{qr}, \right\}$$

így

$$\left|\left|\frac{a}{q}-\frac{b}{r}\right|\right| \geq \frac{1}{qr} \geq \frac{1}{QQ} = \frac{1}{Q^2}.$$

A tételt $\mathbf{X}$-re és δ-ra alkalmazva kapjuk, hogy

$$\begin{aligned}\sum_{x\in\mathbf{X}} |S(x)|^2 &= \sum_{q\leq Q} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \left|S\left(\frac{a}{q}\right)\right|^2 \\ &\leq \left(\frac{1}{\delta}+\pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2 \\ &\leq \left(Q^2+\pi N\right) \sum_{n=M+1}^{M+N} |a_n|^2 .\end{aligned}$$

16.5 Tétel. (A nagy szita aritmetikai alakja) *Legyen* $M \in \mathbb{Z}$, $Q, N \in \mathbb{N}$, $\mathcal{M} \subseteq \{1, 2, \ldots, Q\}$ *olyan, hogy* $m, m' \in \mathcal{M}$, $m \neq m' \Rightarrow (m, m') = 1$, $\mathcal{A} \subseteq \{M+1, M+2, \ldots, M+N\}$, $Z \stackrel{\text{def}}{=} |\mathcal{A}|$,

$$Z(m,h) = \sum_{\substack{a\equiv h \pmod m\\ a\in\mathcal{A}}} 1.$$

Ekkor

$$\sum_{m\in\mathcal{M}} m\left(\sum_{h=1}^{m} Z(m,h) - \frac{Z}{m}\right) \leq (Q^2+\pi N)Z.$$

Ha $\mathcal{M} = \{p : \ p \text{ prím}, p \leq Q\}$-t választunk a tételben, akkor a következőt kapjuk:

16.6 Következmény. *Ha* $M \in \mathbb{Z}$, $Q, N \in \mathbb{N}$, $\mathcal{A} \subseteq \{M+1, M+2, \ldots, M+N\}$, Z, $Z(m,h)$ *mint a 16.5 Tételben akkor*

$$\sum_{p\leq Q} p\left(\sum_{h=1}^{p} Z(p,h) - \frac{Z}{p}\right) \leq (Q^2+\pi N)Z.$$

Megjegyzés. Tegyük fel, hogy a $p \leq Q$ prímek egy pozitív százalékára igaz, hogy a modulo p maradékosztályok egy pozitív százaléka tiltott.

Ha h egy tiltott maradékosztály modulo p, akkor

$$\left(Z(p,h) - \frac{Z}{p} \right) = \frac{Z^2}{p^2},$$

amiből adódóan

$$\begin{aligned} \sum_{p \leq Q} p \left(\sum_{h=1}^{p} Z(p,h) - \frac{Z}{p} \right) &\gg \sum_{p \leq Q}^{*} p \sum_{h}^{*} \frac{Z^2}{p^2} \\ &\gg \sum_{p \leq Q}^{*} p \frac{Z^2}{p} \\ &\gg Z^2 \sum_{p \leq Q}^{*} 1 \\ &\gg Z^2 \pi(Q). \end{aligned}$$

Így a 16.6 Következményből adódik, hogy

$$\begin{aligned} Z^2 \pi(Q) &\ll (Q^2 + \pi N) Z \\ z &\ll \frac{Q^2 + \pi N}{\pi(Q)} \ll \frac{Q^2 + N}{\pi(Q)}. \end{aligned}$$

Montgomery [7] egy kicsit élesebb formáját bizonyította a nagy szitának.

16.7 Tétel. (Montgomery, 1968) *Legyen $M \in \mathbb{Z}$, $Q, N \in \mathbb{N}$, $Q \geq 2$ $\mathcal{A} \subseteq \{M+1, M+2, \ldots, M+N\}$, és legyen $|\mathcal{A}| = Z$. Tegyük fel, hogy $\forall\, p \leq Q$-ra $\exists\, \omega(p)$ maradékosztály, amely nem metszi $\mathcal{A}$-t. Tegyük fel, hogy $\omega(p) < p$. Ekkor*

$$Z \leq \frac{Q^2 + \pi N}{L},$$

ahol

$$L = \sum_{q \le Q} \mu^2(q) \prod_{p \le Q} \frac{\omega(p)}{p - \omega(p)}.$$

A 16.7 Tételt nem, de a 16.5 Tételt viszont bebizonyítjuk.

A 16.5 Tétel bizonyítása. A következő Parseval típusú azonosságot fogjuk használni.

16.8 Lemma. *Ha* $m \in \mathbb{N}$, $b_1, b_2, \dots, b_m \in \mathbb{C}$, $F(\alpha) = \sum_{h=1}^{m} b_h e(h\alpha)$, *akkor*

$$\sum_{k=1}^{m} \left| F\left(\frac{k}{m}\right) \right|^2 = m \sum_{h=1}^{m} |b_h|^2.$$

A 16.8 Lemma bizonyítása.

$$\begin{aligned}
\sum_{k=1}^{m} \left| F\left(\frac{k}{m}\right) \right|^2 &= \sum_{k=1}^{m} \sum_{h=1}^{m} b_h e\left(h\frac{k}{m}\right) \sum_{j=1}^{m} \overline{b_j} e\left(-j\frac{k}{m}\right) \\
&= \sum_{h=1}^{m} \sum_{j=1}^{m} b_h \overline{b_j} \underbrace{\sum_{k=1}^{m} e\left((h-j)\frac{k}{m}\right)}_{\begin{cases} m, & \text{ha } h = j \\ 0, & \text{ha } h \neq j \end{cases}} \\
&= m \sum_{h=1}^{m} |b_h|^2,
\end{aligned}$$

ami a bizonyítandó volt.

Alkalmazzuk a lemmát $b_h = Z(m,h) - \frac{Z}{m}$-mel, és legyen $S(\alpha) = \sum_{a \in \mathcal{A}} e(a\alpha)$. Ekkor a lemma szerint

$$m \sum_{h=1}^{m} \left(Z(m,h) - \frac{Z}{m} \right)^2 = \sum_{k=1}^{m} \left| F\left(\frac{k}{m}\right) \right|^2. \tag{16.8}$$

Itt

$$\begin{aligned} F\left(\frac{k}{m}\right) &= \sum_{h=1}^{m}\left(Z(m,h)-\frac{Z}{m}\right)e\left(h\frac{k}{m}\right) \\ &= \sum_{h=1}^{m} Z(m,h)e\left(h\frac{k}{m}\right) - \frac{Z}{m}\sum_{h=1}^{m} e\left(h\frac{k}{m}\right) \\ &= \sum_{a\in\mathcal{A}} e\left(a\frac{k}{m}\right) - \frac{Z}{m}\begin{cases} m, & \text{ha } m \mid k \\ 0, & \text{ha } m \nmid k \end{cases} \\ &= \begin{cases} |\mathcal{A}| - Z = 0, & \text{ha } m \mid k \\ S\left(\frac{k}{m}\right), & \text{ha } m \nmid k. \end{cases} \end{aligned}$$

Így (16.8) a következőképp alakul:

$$m\sum_{h=1}^{m}\left(Z(m,h)-\frac{Z}{m}\right)^2 = \sum_{m\in\mathcal{M}}\sum_{k=1}^{m-1}\left|S\left(\frac{k}{m}\right)\right|^2. \qquad (16.9)$$

Mivel ha $m \neq m' \in \mathcal{M}$ esetén $(m,m') = 1$, azért ha $m \neq m'$ vagy $k \neq k'$ akkor $\frac{k}{m} \neq \frac{k'}{m'}$. Így (16.9) jobboldalán $\frac{k}{m}$-et $\frac{a}{q}$ alakra hozva, ahol $(a,q) = 1$ kapjuk, hogy

$$m\sum_{h=1}^{m}\left(Z(m,h)-\frac{Z}{m}\right)^2 \leq \sum_{q\leq Q}\sum_{\substack{1\leq a\leq q\\(a,q)=1}}|S(a/q)|^2$$

A 16.4 Következmény szerint

$$m\sum_{h=1}^{m}\left(Z(m,h)-\frac{Z}{m}\right)^2 \leq (Q^2+\pi N)\sum_{n=M+1}^{M+n}|a_n|^2,$$

ahol most

$$a_n = \begin{cases} 1, & \text{ha } a_n \in \mathcal{A} \\ 0, & \text{ha } a_n \notin \mathcal{A}. \end{cases}$$

Így

$$m\sum_{h=1}^{m}\left(Z(m,h)-\frac{Z}{m}\right)^2 \leq (Q^2+\pi N)Z,$$

ami éppen a bizonyítandó állítás.

Selbergnek (16.3) becsléséből levezethető, hogy a π-es szorzó a 16.4, 16.5, 16.6 és 16.7 Tételekből és Következményekből elhagyható. Azonban mi a jegyzet keretein belül maradtunk az ugyan kicsit gyengébb, de rövidebben bizonyítható változatoknál.

Egy egyszerű alkalmazás: legyen

$$P(n) \stackrel{\text{def}}{=} \max_{\substack{p|n \\ p \text{ prím}}} p.$$

16.9 Tétel. (Balog-Sárközy [2]) *Ha* $N > N_0$, $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ *és*

$$|\mathcal{A}| > 33N^{1/2} \log N, \tag{16.10}$$

akkor $\exists\, a, a' \in \mathcal{A}$, *hogy*

$$P(a + a') > \frac{|\mathcal{A}|}{33 \log N}. \tag{16.11}$$

Megjegyzés. Mit mond ki a tétel? Egy ilyen $a + a'$ esetén írjunk $P(a + a') = p$, $\frac{a+a'}{p} = m$. Ekkor

$$m = \frac{a + a'}{p} < \frac{N + N}{\frac{|\mathcal{A}|}{33 \log N}} = 66 \frac{N}{|\mathcal{A}|} \log N.$$

Ha mondjuk (16.10) a sokkal élesebb formában igaz, azaz $|\mathcal{A}| > \varepsilon N$, akkor

$$m < 66 \frac{N}{|\mathcal{A}|} \log N < \frac{66}{\varepsilon} \log N$$

és

$$p > \frac{|\mathcal{A}|}{33 \log N} > \frac{\varepsilon}{33} \frac{N}{\log N}.$$

Vagyis ekkor $a + a' = mp$, ahol p „nagyon nagy”, m pedig „nagyon kicsi”, így az $a + a'$ összeg „közel” van egy prímhez.

Érdekes kérdés esetleg, hogy $a + a' =$ prím, ilyen tétel nincs, legyen $\mathcal{A} = \{n : \ n \text{ páros}, \ n \leq N\}$. Ekkor $\forall\, a+a'$ páros, $\forall\, a+a'$ összetett.

A 16.9 Tétel bizonyítása. Indirekten bizonyítunk. Tegyük fel, hogy ellentétben (16.11)-zel, $\forall\, a + a'$-re

$$P(a + a') \leq \left\lceil \frac{|\mathcal{A}|}{33 \log N} \right\rceil \overset{\text{def}}{=} t.$$

Ekkor $\forall\, p > t$-re $a, a' \in \mathcal{A}$ esetén $p \nmid a + a'$, azaz

$$a + a' \not\equiv 0 \pmod{p} \qquad (\forall a, a' \in \mathcal{A}, \ p > t)$$
$$a \not\equiv -a' \pmod{p}.$$

Jelölje $\nu(p)$ az $\mathcal{A}$-t metsző mod p maradékosztályok számát:

$$\nu(p) = \left|\{r : \ 0 \leq r < p, \ \exists a \in \mathcal{A}, \text{ ahol } a \equiv r \pmod{p}\}\right|.$$

Ekkor

$$\left.\begin{array}{ll} \mathcal{A}: & \nu(p) \text{ különböző maradékosztály} \\ -\mathcal{A}: & \nu(p) \text{ különböző maradékosztály} \end{array}\right\} \begin{array}{l} \text{Ezek együttesen} \\ \text{is mind különbözők.} \end{array}$$

Így

$$\nu(p) + \nu(p) \leq p$$
$$\nu(p) \leq \frac{p}{2}.$$

Tehát $\mathcal{A}$ nem metsz legalább $p - \nu(p) \geq \frac{p}{2}$ maradékosztályt mod p. Így $\forall\, p > t$-re:

$$S = \sum_{t < p \leq 2t} p \sum_{h=1}^{p} \left(Z(p, h) - \frac{Z}{p} \right)^2$$

$$\geq \sum_{t<p\leq 2t} p \sum_{\substack{1\leq h\leq p\\ Z(p,h)=0}} \left(0-\frac{Z}{p}\right)^2$$

$$= \sum_{t<p\leq 2t} p\frac{Z^2}{p^2} \underbrace{\sum_{\substack{1\leq h\leq p\\ Z(p,h)=0}} 1}_{\geq \frac{p}{2}} \tag{16.12}$$

$$\geq \frac{Z^2}{2} \sum_{t<p\leq 2t} 1$$

$$= \frac{Z^2}{2}\left(\pi(2t)-\pi(t)\right). \tag{16.13}$$

Itt (16.10) miatt

$$t = \left\lceil \frac{|\mathcal{A}|}{33\log N} \right\rceil > \frac{33N^{1/2}\log N}{33\log N} = N^{1/2} \to \infty,$$

amint $N \to \infty$.

A prímszámtétel szerint $\pi(x) \sim \frac{x}{\log x}$, amint $x \to \infty$. Tehát

$$\pi(2t)-\pi(t) = (1+o(1))\frac{2t}{\log 2t} - (1+o(1))\frac{t}{\log t}$$
$$= (1+o(1))\frac{t}{\log t},$$

vagyis

$$\pi(2t)-\pi(t) > \frac{t}{2\log t}, \qquad \text{ha } N > N_0. \tag{16.14}$$

Ekkor (16.13) és (16.14) miatt

$$S > \frac{Z^2}{2}\cdot\frac{t}{2\log t}. \tag{16.15}$$

Másrészt a nagy szita aritmetikai alakja miatt (ld. 16.5 Tétel):

$$\begin{aligned} S &= \sum_{t<p\le 2t} p \sum_{h=1}^{p} \left(Z(p,h) - \frac{Z}{p} \right)^2 \\ &\le \sum_{p\le 2t \overset{\text{def}}{=} Q} p \sum_{h=1}^{p} \left(Z(p,h) - \frac{Z}{p} \right)^2 \\ &\le (Q^2 + \pi N) Z \\ &< 4(t^2 + N) Z. \end{aligned} \tag{16.16}$$

Ekkor (16.15) és (16.16) alapján:

$$\begin{aligned} \frac{1}{4} Z^2 \frac{t}{\log t} < S < 4(t^2 + N) Z \\ Z < 16 \frac{\log N}{t} (t^2 + N). \end{aligned} \tag{16.17}$$

Ekkor (16.10) szerint:

$$t^2 = \left\lceil \frac{|\mathcal{A}|}{33 \log N} \right\rceil^2 \ge \left\lceil \frac{1}{33} \frac{33 N^{1/2} \log N}{\log N} \right\rceil^2 = \left\lceil N^{1/2} \right\rceil^2 = N \tag{16.18}$$

(16.17) és (16.18) szerint

$$\begin{aligned} Z < 16 \frac{\log N}{t} \cdot 2t^2 = 32 t \log N = 32 \left\lceil \frac{|\mathcal{A}|}{33 \log N} \log N \right\rceil \\ < 32 \left(1 + \frac{|\mathcal{A}|}{33 \log N} \log N \right) = \frac{32}{33} |\mathcal{A}| + \log N < |\mathcal{A}| = Z, \end{aligned}$$

ami ellentmondás.

Megjegyzés. A tétel $a + a'$ összegekről kifejezhető $a + b$ összegekre, és hasonló jellegű tétel bizonyítható. A következő eredmények szintén Balogtól és Sárközytől [1], [2] származnak:

Ha $\varepsilon > 0$, $N > N_0(\varepsilon)$, $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \dots, N\}$, $|\mathcal{A}|, |\mathcal{B}| > \varepsilon N$, akkor $\exists a \in \mathcal{A},\ b \in \mathcal{B}$, hogy

1. $P(a+b) > c(\varepsilon)N \quad (\Rightarrow\ a+b = pO(1))$.

2. $\exists p:\ p^2 \mid a+b,\ p^2 > c'(\varepsilon)N$

3. $P(a+b) < \exp\left(c''(\varepsilon)\sqrt{\log N \log\log N}\right)$ azaz „kicsi” $= N^{o(1)}$.

Sok hasonló jellegű tétel létezik sűrű $\mathcal{A}$, $\mathcal{B}$ halmazokra, ahol található olyan $a+b$ összeg, amely rendelkezik bizonyos aritmetikai tulajdonságokkal.

Emlékeztetőül felírjuk a nagy szita analitikus formájának a következményét:

$$\sum_{q\le Q}\sum_{1\le a\le q}{}^{*}\ \Big|\ \underbrace{S(a/q)}_{\sum_n a_n e\left(n\frac{a}{q}\right)}\ \Big|^2 \le (Q^2+\pi N)\sum_{n=M+1}^{M+N}|a_n|^2\,. \tag{16.19}$$

Mivel létezik dualitás additív és multiplikatív karakterek között, azt reméljük, hogy $\exists$ a fenti következménynek multiplikatív analogonja. Valóban:

16.10 TÉTEL. (Gallagher [6]) *Ha $Q \in \mathbb{N}$, $Q \ge 2$*

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sum_{\substack{\chi \text{ primitív}\\ \text{karakter mod} q}}^{*}\left|\sum_{n=M+1}^{M+N}a_n\chi(n)\right|^2 \le (Q^2+\pi N)\sum_{n=M+1}^{M+N}|a_n|^2. \tag{16.20}$$

A 16.10 Tétel bizonyítása. Szeretnénk (16.20)-t levezetni (16.19)-ből. Így additív karakterekről kell áttérnünk multiplikatív karakterekre, amihez egy áttérési formulát használunk, ld. 11.3 Tétel. Eszerint, ha χ primitív karaker mod q, akkor

$$\chi(n)\tau(\overline{\chi}) = \sum_{h=0}^{q-1}\overline{\chi}(h)e\left(n\frac{h}{q}\right), \tag{16.21}$$

ahol $\tau(\chi)$ Gauss összeg:

$$\tau(\chi) = \sum_{1 \le a \le q} \chi(a) e\left(\frac{a}{q}\right).$$

Szintén tanultuk (ld. 11.2 Tétel), hogy primitív karakterre

$$|\tau(\chi)| = \sqrt{q}.$$

Azaz (16.21)-ból adódóan

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(n\frac{h}{q}\right).$$

Így primitív χ karakterek esetén

$$\begin{aligned}\sum_{n=M+1}^{M+N} a_n \chi(n) &= \sum_{n=M+1}^{M+N} a_n \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) e\left(n\frac{h}{q}\right) \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) \sum_{n=M+1}^{M+N} a_n e\left(n\frac{h}{q}\right) \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{h=0}^{q-1} \overline{\chi}(h) S\left(\frac{h}{q}\right).\end{aligned}$$

Azaz (16.20) baloldala

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \text{ primitív} \\ \text{karakter mod} q}}^{*} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2$$

$$= \sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \text{ primitív} \\ \text{karakter mod} q}}^{*} \underbrace{\frac{1}{|\tau(\overline{\chi})|^2}}_{\substack{=q \text{ mivel} \\ \chi \text{ primitív}}} \left| \sum_{h=0}^{q-1} \overline{\chi}(h) S\left(\frac{h}{q}\right) \right|^2.$$

Itt a jobboldalon $\forall$ tag ≥ 0, így felső becslést kapunk, ha vesszük a nem primitív karaktereket is, azaz

$$\sum_{q \le Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \text{ primitív} \\ \text{karakter mod} q}}^{*} \left| \sum_{n=M+1}^{M+N} a_n \chi(n) \right|^2$$

$$\leq \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\chi}\left|\sum_{h=0}^{q-1}\overline{\chi}(h)S\left(\frac{h}{q}\right)\right|^2$$

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\chi}\sum_{h=0}^{q-1}\overline{\chi}(h)S\left(\frac{h}{q}\right)\sum_{k=0}^{q-1}\chi(k)\overline{S\left(\frac{k}{q}\right)}$$

mivel $\chi(k)=0$, ha $(k,q)=1$ és $\overline{\chi}(h)=0$, ha $(h,q)=1$ így

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\chi}\sum_{\substack{0\leq h<q\\(h,q)=1}}\sum_{\substack{0\leq k<q\\(k,q)=1}}\underbrace{\overline{\chi}(h)\chi(k)}_{\chi(h^*k)}S\left(\frac{h}{q}\right)\overline{S\left(\frac{k}{q}\right)}$$

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\substack{0\leq h<q\\(h,q)=1}}\sum_{\substack{0\leq k<q\\(k,q)=1}}S\left(\frac{h}{q}\right)\overline{S\left(\frac{k}{q}\right)}\underbrace{\sum_{\chi}\chi(h^*k)}$$

$$\begin{cases}\varphi(q), & \text{ha } h^*k\equiv 1\ (q)\\ & \Leftrightarrow h=k\\ 0, & \text{ha } h\neq k.\end{cases}$$

$$= \sum_{q\leq Q}\frac{1}{\varphi(q)}\sum_{\substack{0\leq h<q\\(h,q)=1}}\left|S\left(\frac{h}{q}\right)\right|^2\varphi(q)$$

$$= \sum_{q\leq Q}\sum_{\substack{0\leq h<q\\(h,q)=1}}\left|S\left(\frac{h}{q}\right)\right|^2$$

$$\leq (Q^2+\pi N)\sum_{n=M+1}^{M+N}.$$

Ezzel a tétel állítását beláttuk.

Hivatkozások

[1] A. Balog, A. Sárközy, *On sums of sequences of integers I.*, Acta Arithmetica 44 (1984), 73-84.

[2] A. Balog, A. Sárközy, *On sums of sequences of integers II.*, Acta Math. Acad. Sci.Hungar. 44 (1984), 169-179.

[3] J. R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica. 16 (1973) 157–176.

[4] H. Davenport, H. Halberstam, *The values of a trigonometric polynomial at well spaced points*, Mathematika 13 (1966), 91-96. *Corrigendum and addendum*, Mathematika 14 (1967), 229-232.

[5] P. X. Gallagher, *The large sieve*, Mathematika 14 (1967), 14-20.

[6] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. 11, 329-339 (1970).

[7] H. L. Montgomery, *A note on the large sieve*, J. London Math. Soc. 43 (1968), 93-98.

[8] H. L. Montgomery, *The analytic principle of the large sieve*, Bulletin of the American Mathematical Society 84 (4) (1978), 547-567.

[9] A. Rényi, *On the representation of an even number as the sum of a prime and an almost prime*. Izvestiya Akademii Nauk SSSR Seriya Matematicheskaya 12 (1948), 57–78 (oroszul).

[10] S. L. Sobolev, *Applications of functional analysis in mathematical physics*, TransL Math. Monographs, vol. 7, 1963.

17. A nagy szita megfordítása

Emlékeztető a nagy szitáról: Egy egészekből álló sűrű halmaz egyenletesen oszlik el majdnem minden maradékosztályban majdnem minden modulusra nézve.

Másrészt Roth [4] bebizonyította, hogy ez az eloszlás nem lehet túlzottan uniform, vagyis $\exists$ egy maradékosztály, amelyhez tartozó elemek vagy sokkal többen vagy sokkal kevesebben vannak mint amit várunk.

Később Roth [5] a következőt is igazolta:

17.1 TÉTEL. *Legyen k pozitív egész, és tegyük fel, hogy $N > (10k)^7$. Ekkor az $s_1, s_2, \dots, s_N$ valós számokból álló sorozatra $\exists n, q \in \mathbb{Z}^+$, amelyre*

$$1 \leq n \leq n + (k-1)q \leq N$$

és

$$\left| \sum_{i=0}^{k-1} s_{n+iq} \right| \geq \left(\frac{k}{10N} \sum_{j=1}^{N} |s_j|^2 \right)^{1/2}.$$

Sárközy [6]-ban kidolgozta Roth néhány általános eredményének moduláris analogonját is. Ehhez azonban többek közt a fenti tételnek egy kissé módosított és pontosabb formájára volt szükség. Ez a következő:

17.2 TÉTEL. *Legyen $N, Q \in \mathbb{N}$, $Q \geq 2$, $s_1, s_2, \dots, s_N \in \mathbb{C}$. Legyen továbbá $Q_1 = \left[\frac{Q}{2}\right]$ és $s_j \overset{\text{def}}{=} 0$ ha $j \leq 0$ vagy $j > N$, valamint $\forall n \in \mathbb{Z}$, $q, k \in \mathbb{Z}^+$*

$$D(n, q, k) \overset{\text{def}}{=} s_n + s_{n+q} + s_{n+2q} + \cdots + s_{n+(k-1)q}.$$

Ekkor

$$\sum_{q=1}^{Q}\sum_{n=1-(Q_1-1)q}^{N}|D(n,q,Q_1)|^2\geq\left(\frac{2}{\pi}Q_1\right)^2\sum_{m=1}^{N}|s_m|^2. \qquad (17.1)$$

Jelen fejezetben Sárközy számolásait követve bebizonyítjuk a 17.2 Tételt, és megnézzük azt is, hogyan következik ebből Roth eredeti első kérdése (ld. később 17.5 Következmény). De előtte egy megjegyzés és pár következmény.

Megjegyzés. Tipikusan $s_1+s_2+\cdots+s_N=0\ \Rightarrow s_n+s_{n+q}+\cdots+s_{n+(k-1)q}$ szintén 0 várhatóan, vagy legalább „kicsi” $\Rightarrow |D(n,q,k)|$ méri az eltérését a várható értéktől, ez a diszkrepancia. Tehát a tétel azt mondja ki: a szórása a diszkrepanciának nagy.

Néhány következmény:

17.3 Következmény. *$\exists\, n\in\mathbb{Z},\ q\in\mathbb{N}$, hogy $q\leq Q$ és*

$$|D(n,q,Q_1)|\geq\frac{2}{\pi}\left[\frac{Q}{2}\right]Q^{-1/2}\left(N+\frac{Q^2}{4}\right)^{-1/2}\left(\sum_{m=1}^{N}|s_m|^2\right)^{1/2}. \qquad (17.2)$$

A 17.3 Következmény bizonyítása. Írjunk

$$M\overset{\text{def}}{=}\max_{m,q}|D(n,q,Q_1)|$$

-t. Itt azt kell bizonyítanunk, hogy $M\geq$ jobboldala (17.2)-nek.

Az (17.1) baloldalára:

$$\leq\sum_{q=1}^{Q}\sum_{n=1-(Q_1-1)q}^{N}M^2$$

$$
\begin{aligned}
&= M^2 \sum_{q=1}^{Q} \sum_{n=1-(Q_1-1)q}^{N} 1 \\
&= M^2 \sum_{q=1}^{Q} (N + (Q_1 - 1)q) \\
&= M^2 \left(NQ + (Q_1 - 1) \sum_{q=1}^{Q} q \right) \\
&= M^2 \left(NQ + \left(\left[\frac{Q}{2} \right] - 1 \right) \frac{Q(Q+1)}{2} \right) \\
&\leq M^2 Q \left(N + \left(\frac{Q}{2} - \underbrace{1}_{>\frac{1}{2}} \right) \left(\frac{Q}{2} + \frac{1}{2} \right) \right) \\
&< M^2 Q \left(N + \frac{Q^2}{4} - \frac{1}{4} \right) \\
&< M^2 Q \left(N + \frac{Q^2}{4} \right). \qquad (17.3)
\end{aligned}
$$

(17.1) és (17.3):

$$
M^2 Q \left(N + \frac{Q^2}{4} \right) \geq \frac{2}{\pi} \left[\frac{Q}{2} \right]^2 \sum_{m=1}^{N} |s_m|^2 .
$$

Ezt $Q \left(N + \frac{Q^2}{4} \right)$-gyel osztva és gyököt vonva megkapjuk (17.2)-t.

Akkor kapjuk a legjobb becslést $\max_{n,q,Q} |D(n, q, Q_1)|$-re, ha $Q \asymp \sqrt{N}$. Nevezetesen, ha $Q = \left[\sqrt{N} \right]$, akkor a 17.3 Következmény szerint:

17.4 Következmény. *Ha* $\varepsilon > 0$, $N > N_0(\varepsilon)$, $N \in \mathbb{N}$, $s_1, s_2, \ldots, s_N \in \mathbb{C} \Rightarrow \exists\, n \in \mathbb{Z},\ q \in \mathbb{Z}^+$, *hogy* $q \leq \sqrt{N}$ *és*

$$
|D(n, q, [\sqrt{N}/2])| \geq \left(\frac{2}{\pi\sqrt{5}} - \varepsilon \right) \left(\frac{\sum_{m=1}^{N} |s_m|^2}{N} \right)^{1/2} N^{1/4}. \qquad (17.4)
$$

A 17.4 Következmény bizonyítása. Most $Q = \left[\sqrt{N}\right]$. Ekkor (17.2) jobboldala a 17.3 Következményben:

$$(1+o(1))\left(\frac{2}{\pi}\frac{\sqrt{N}}{2}N^{-1/4}\left(N+\frac{N}{4}\right)^{-1/2}\left(\sum_{m=1}^{N}|s_m|^2\right)\right)^{1/2}$$
$$=(1+o(1))\left(\frac{1}{\pi}\left(\frac{4}{5}\right)^{1/2}N^{1/4}\left(\frac{\sum_{m=1}^{N}|s_m|^2}{N}\right)^{1/2}\right)$$
$$\geq\left(\frac{2}{\pi\sqrt{5}}-\varepsilon\right)N^{1/4}\left(\frac{\sum_{m=1}^{N}|s_m|^2}{N}\right)^{1/2}. \qquad (17.5)$$

Ekkor (17.2)-ből és (17.4)-ből következik (17.5).

Ezek után azt a speciális esetet nézzük, amelyet Roth [4] eredetileg tanulmányozott.

17.5 Következmény. *Ha* $\varepsilon > 0$, $N > N_0(\varepsilon)$, $\mathcal{A} \subseteq \{1,2,\dots,N\}$, *akkor írjunk* $\eta = \frac{|\mathcal{A}|}{N}$*-t és* $\mathcal{A}(u,q,t) \stackrel{\text{def}}{=} |\{u,u+q,\dots,u+(t-1)q\}\cap\mathcal{A}|$, $\exists\, u,q,t$, *hogy* $\{u,u+q,\dots,u+(t-1)q\}\subseteq\{1,2,\dots,N\}$, $q\leq N$ *és*

$$|\mathcal{A}(u,q,t)-\eta t|\geq\left(\frac{2}{\pi\sqrt{5}}-\varepsilon\right)\sqrt{\eta(1-\eta)}N^{1/4}. \qquad (17.6)$$

Megjegyzés. Ez úgy tekinthető mint a nagy szita megfordítása: $\exists$ legalább egy számtani sorozat $\sqrt[4]{N}$ nagyságrendű irregularitással.

A 17.5 Következmény bizonyítása. A 17.4 Következményt alkalmazzuk

$$s_n=\begin{cases}\eta, & \text{ha } n\notin\mathcal{A},\ 1\leq n\leq N\\ -(1-\eta), & \text{ha } n\in\mathcal{A},\ 1\leq n\leq N\\ 0, & \text{ha } n<1 \text{ vagy } n>N.\end{cases}$$

Ekkor a 17.4 Következmény miatt $\exists\, n,\ q,\ q \le N$, amelyre

$$|D(n,q,[\sqrt{N}/2])| = |s_n + s_{n+q} + \cdots + s_{n+([\sqrt{N}/2]-1)q}| \\ \ge \left(\frac{2}{\pi\sqrt{5}} - \varepsilon\right)\left(\frac{\sum_{m=1}^{N}|s_m|^2}{N}\right)^{1/2} N^{1/4}. \tag{17.7}$$

Elvileg itt előfordulhat, hogy az $n, n+q, \ldots, n+([\sqrt{N}/2]-1)q$ számtani sorozatunk túl nyúlik az $[1,N]$ intervallumon, ekkor eldobjuk azokat az s_i-ket, amelyre $i \notin [1,N]$, hiszen ekkor $s_i = 0$, azaz csak 0-kat dobunk el. A metszetet megtartjuk:

$$\{u, u+q, \ldots, u+(t-1)q\} \overset{\text{def}}{=} \\ \{n, n+q, \ldots, n+([\sqrt{N}/2]-1)q\} \cap \{1,2,\ldots,N\}.$$

Ekkor

$$\begin{aligned} D(n,q,[\sqrt{N}/2]) &= \sum_{j=0}^{[\sqrt{N}/2]-1} s_{n+jq} \\ &= \sum_{j=0}^{t-1} s_{u+jq} \\ &= \sum_{\substack{0\le j<t \\ u+jq\notin\mathcal{A}}} \eta + \sum_{\substack{0\le j<t \\ u+jq\in\mathcal{A}}} -(1-\eta) \\ &= \eta t - A(u,q,t). \end{aligned} \tag{17.8}$$

Míg (17.7) jobboldala

$$\frac{1}{N}\sum_{m=1}^{N}|s_m|^2 = \frac{1}{N}\left(\sum_{\substack{n\notin\mathcal{A} \\ 1\le n\le N}} \eta^2 + \sum_{\substack{n\in\mathcal{A} \\ 1\le n\le N}} (1-\eta)^2\right) \\ = \frac{1}{N}\left(\eta^2(N-\eta N) + (1-\eta)^2\eta N\right)$$

$$= \eta(1-\eta)\left(\eta + (1-\eta)\right)$$
$$= \eta(1-\eta). \tag{17.9}$$

Így (17.7), (17.8) és (17.9)-ből következik (17.6).

A 17.2 Tétel bizonyítása. Generátorfüggvény módszert fogunk alkalmazni, amelyet még Euler vezetett be.

A generátorfüggvény módszerek esetében, általában, egy $s_1, s_2, \dots$ sorozathoz hozzárendelünk egy $S(\alpha)$ függvényt (itt $S(\alpha)$ tipikusan egy polinom vagy hatványsor). Ezután $S(\alpha)$ analitikus tulajdonságait vizsgáljuk, és ebből vezetjük le az eredeti sorozat bizonyos aritmetikai tulajdonságait:

$$\text{sorozat} \to \text{generátor függvény} \overset{\text{analízis}}{\to} \text{analitikus tulajdonságok} \to$$
$$\to \text{ aritmetikai tulajdonságai a sorozatnak}$$

Nézzük tehát a konkrét tételbeli sorozatot: $s_1, s_2, \dots, s_N$-et, és rendeljük hozzá az

$$S(\alpha) \overset{\text{def}}{=} \sum_{n=1}^{N} s_n e(n\alpha)$$

polinomot. Ezután az ún. Fejér mag komplex változatát használjuk: legyen $M \in \mathbb{N}$ esetén

$$F_M(\alpha) \overset{\text{def}}{=} \sum_{j=0}^{M-1} e(j\alpha).$$

Ekkor a (komplex) Fejér mag $|F_M(\alpha)|^2$.

17.6 Lemma. *Ha $\alpha \in \mathbb{R}$, $|\alpha| \le \frac{1}{2M}$, akkor $|F_M(\alpha)| \ge \frac{2}{\pi}M$.*

A 17.6 Lemma bizonyítása. Ha $\alpha = 0$, akkor a lemma triviális, hiszen $F_M(0) = M > \frac{2}{\pi}M$.

Tudjuk továbbá, hogy $F_M(-\alpha) = \overline{F_M(\alpha)}$, azaz $|F_M(-\alpha)| = |F_M(\alpha)|$. Tehát a bizonyítás során feltehetjük, hogy $0 < \alpha \leq \frac{1}{2M}$. Ekkor $F_M(\alpha)$ egy mértani sorozat $e(\alpha) \neq 1$ hányadossal, tehát

$$|F_M(\alpha)|^2 = \left|\frac{1 - e(M\alpha)}{1 - e(\alpha)}\right|^2.$$

Itt mind a nevező, mind a számláló $|1 - e(\beta)|^2$ alakú, ahol

$$\begin{aligned} |1 - e(\beta)|^2 &= (1 - e(\beta))\overline{(1 - e(\beta))} \\ &= (1 - e(\beta))(1 - e(-\beta)) \\ &= 2 - (e(\beta) + e(-\beta)) \\ &= 2 - 2\mathrm{Re}\, e(\beta) \\ &= 2 - 2\cos 2\pi\beta \\ &= 4\sin^2 \pi\beta, \end{aligned}$$

azaz

$$|F_M(\alpha)|^2 = \frac{4\sin^2 M\pi\alpha}{4\sin^2 \pi\alpha} = \left|\frac{\sin M\pi\alpha}{\sin \pi\alpha}\right|^2.$$

A következőkben írjunk

$$f(x) = \frac{\sin Mx}{\sin x}$$

-et (ahol most M fix).

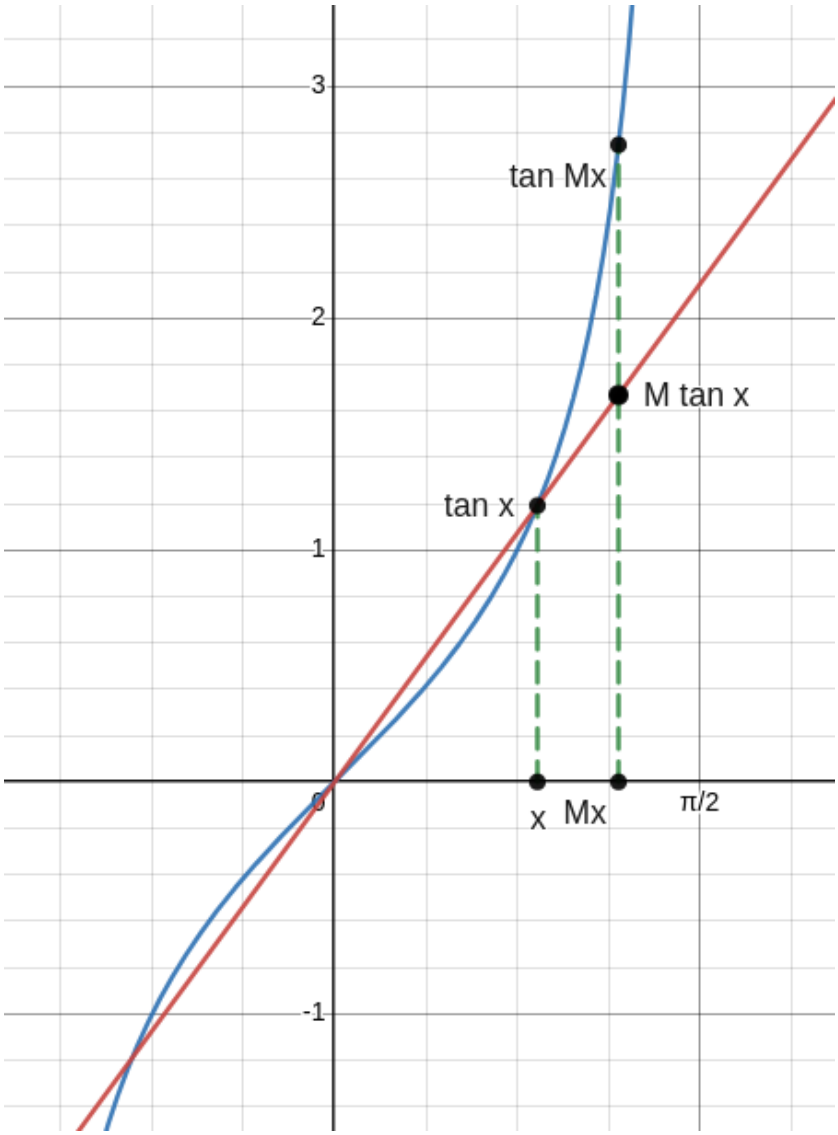
Állítás. Az $f(x)$ függvény monoton csökkenő a $\left(0, \frac{\pi}{2M}\right]$ intervallumon.

Ekkor azt kell megmutatnunk, hogy $f'(x) < 0$. Valóban $x = \frac{\pi}{2M}$-re ez nyilvánvalóan teljesül, $0 < x < \frac{\pi}{2M}$ esetén pedig:

$$f'(x) = \frac{M\cos Mx \sin x - \sin Mx \cos x}{\sin^2 x}$$

$$= \frac{\cos x \cos Mx}{\sin^2 x} \left(M \frac{\sin x}{\cos x} - \frac{\sin Mx}{\cos Mx} \right)$$
$$= \frac{\cos x \cos Mx}{\sin^2 x} \left(M \tan x - \tan Mx \right).$$

Itt az első szorzótényező $\frac{\cos x \cos Mx}{\sin^2 x} > 0$, mert $0 < x \leq Mx < \frac{\pi}{2}$, míg $M \tan x - \tan Mx < 0$, hiszen ha ábrázoljuk a tangens függvényt a következő ábrát kapjuk:



A konvexitás miatt az $x = \tan x$ függvény (kék görbe) felette van az origót $(x, \tan x)$ ponttal összekötő egyenesnek (piros egyenes)

az $\left[x, \frac{\pi}{2}\right)$ intervallumon. (Ez azért van így, mert a konvexitás miatt $\frac{\tan x - \tan 0}{x-0} \leq \tan' x \leq \frac{\tan Mx - \tan x}{Mx - x}$.)

Vagyis $M \tan x < \tan Mx$, amivel az állításunkat igazoltuk.

Állításunkból adódóan $0 < x \leq \frac{\pi}{2M}$ esetén

$$f(x) \geq f\left(\frac{\pi}{2M}\right) = \frac{\sin M\frac{\pi}{2M}}{\sin \frac{\pi}{2M}} = \frac{1}{\sin \frac{\pi}{2M}} > \frac{1}{\frac{\pi}{2M}} = \frac{2}{\pi}M.$$

$$\uparrow$$

$$\sin x < x$$

Vagyis

$$|F_M(\alpha)| = |f(\underbrace{\pi|\alpha|}_{\text{itt } 0 \leq \pi|\alpha| \leq \frac{\pi}{2M}})| \geq \frac{2}{\pi}M,$$

amivel a 17.6 Lemmát igazoltuk.

Legyen a továbbiakban $Q_1 \overset{\text{def}}{=} \left[\frac{Q}{2}\right]$ (ahogy a tételben definiáltuk) és

$$G(\alpha) \overset{\text{def}}{=} \sum_{q=1}^{Q} |F_{Q_1}(q\alpha)|^2 . \tag{17.10}$$

17.7 LEMMA. *Minden $\alpha \in \mathbb{R}$ esetén*

$$G(\alpha) \geq \left(\frac{2}{\pi}Q_1\right)^2 .$$

A 17.7 Lemma bizonyítása. Dirichlet approximációs tétele szerint, ha $\alpha \in \mathbb{R}$, $Q \in \mathbb{N}$, akkor $\exists\, p \in \mathbb{Z}$, $q \in \mathbb{N}$, melyekre $q \leq Q$, $(p, q) = 1$ és

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ},$$

amiből adódóan

$$|q\alpha - p| < \frac{1}{Q} \leq \frac{1}{2[Q/2]} = \frac{1}{2Q_1}. \tag{17.11}$$

Ekkor

$$G(\alpha) = \sum_{q=1}^{Q} |F_{Q_1}(q\alpha)|^2 .$$

A szummából egyetlen q-t tartunk meg, azt amelyikre (17.11) fennáll:

$$G(\alpha) \geq |F_{Q_1}(q\alpha)|^2 = |F_{Q_1}(q\alpha - p)|^2 .$$

Itt használhatjuk a 17.6 Lemmát $M = Q_1$-gyel, hiszen $|q\alpha - p| < \frac{1}{2Q_1}$. Azaz:

$$G(\alpha) \geq \left(\frac{2}{\pi} Q_1\right)^2 .$$

Ezután tekintsük a

$$\mathcal{J} \stackrel{\text{def}}{=} \int_0^1 |S(\alpha)|^2 G(\alpha) d\alpha$$

függvényt, ahol $|S(\alpha)|^2$ a Jensen függvény, $G(\alpha)$ pedig a (17.10)-ben definiált súlyfüggvény. Ekkor $\mathcal{J}$-re a következő alsó becslést tudjuk adni:

$$\mathcal{J} \geq \underbrace{(\min G(\alpha))}_{\text{17.7 Lemma}} \int_0^1 |S(\alpha)|^2 d\alpha \geq \left(\frac{2}{\pi} Q_1\right)^2 \sum_{m=1}^{N} |s_m|^2. \tag{17.12}$$

Másrészt, $\mathcal{J}$-t kiszámolhatjuk a Parseval formulával:

$$\mathcal{J} = \int_0^1 |S(\alpha)|^2 G(\alpha) d\alpha$$

$$= \int_0^1 |S(\alpha)|^2 \sum_{q=1}^{Q} |F_{Q_1}(q\alpha)|^2 \, d\alpha$$
$$= \sum_{q=1}^{Q} \int_0^1 |S(\alpha) F_{Q_1}(q\alpha)|^2 \, d\alpha$$
$$= \sum_{q=1}^{Q} \int_0^1 \left| \sum_{n=1}^{N} s_n e(n\alpha) \sum_{j=0}^{Q_1-1} e(jq\alpha) \right|^2 d\alpha$$
$$= \sum_{q=1}^{Q} \int_0^1 \left| \sum_{n=1}^{N} s_n \sum_{j=0}^{Q_1-1} e((n+jq)\alpha) \right|^2 d\alpha.$$

Helyettesítsünk a fenti képletbe $m = (n+jq)$-t. Ekkor $n = m-jq$, azaz

$$\mathcal{J} = \sum_{q=1}^{Q} \int_0^1 \left| \sum_{m=1}^{N+(Q_1-1)q} \underbrace{\left(\sum_{j=0}^{Q_1-1} s_{m-jq} \right)}_{D(m-q(Q_1-1),q,Q_1)} e(m\alpha) \right|^2 d\alpha.$$

A Parseval formula szerint:

$$\mathcal{J} = \sum_{q=1}^{Q} \sum_{m=1}^{N+(Q_1-1)q} |D(m-q(Q_1-1),q,Q_1)|^2 .$$

Ezután $n = m - q(Q_1-1)$-t helyettesítünk:

$$\mathcal{J} = \sum_{q=1}^{Q} \sum_{n=1-q(Q_1-1)}^{N} |D(n,q,Q_1)|^2 .$$

Azaz (17.12) alapján:

$$\sum_{q=1}^{Q} \sum_{n=1-q(Q_1-1)}^{N} |D(n,q,Q_1)|^2 \geq \left(\frac{2}{\pi} Q_1 \right)^2 \sum_{m=1}^{N} |s_m|^2, \qquad (17.13)$$

amivel a tétel állítását beláttuk.

Kérdés. Milyen messze van Roth egyenlőtlensége, azaz (17.13) a lehető legjobb becsléstől?

Az egyszerűség kedvéért, tekintsük a 17.4 Következményt abban az esetben, amikor $s_1, s_2, \dots, s_N \in \{-1, +1\}$. Ekkor tudjuk, hogy $\exists\, n \in \mathbb{Z},\ q \in \mathbb{Z}^+$, amelyre

$$\left|D(n, q, [\sqrt{N}/2)]\right| \gg N^{1/4}.$$

A másik irányból Roth észrevette, hogy valószínűségi módszereket használva, belátható, hogy van olyan N-hosszú ± 1 sorozat, amelyre $\max |D(n, q, k)| \ll N^{1/2}(\log N)^{1/2}$, és azt sejtette, ez az eredmény nem javítható lényegesen, azaz

$$\max |D(n, q, k)| \gg N^{1/2-\varepsilon}.$$

minden N-hosszú ± 1 sorozatra és pozitív ε-ra fennáll (ahol $\gg$-nál az alkalmazott konstans szorzó csak ε-tól függ).

Ezt a sejtést Sárközy ([2, §8]) megcáfolta, bebizonyítva olyan sorozat létezését, amelyre

$$\max |D(n, q, k| \ll N^{1/3}(\log N)^{2/3}. \tag{17.14}$$

Beck [1] még lejjebb vitte a becslést $N^{1/4}(\log N)^{5/2}$-re. Matoušek és Spencertől [3] pedig igazolta a lehető legélesebb becslést is, azaz megmutatták olyan sorozat létezését, amelyre

$$\max |D(n, q, k)| \ll N^{1/4}.$$

Itt mi csak (17.14)-t igazoljuk, azaz a következőt:

17.8 Tétel. (Sárközy) *Minden N természetes számra $\exists\, s_1, s_2, \dots, s_N \in \{-1, +1\}$ sorozat, amelyre*

$$\max_{n,q,t} \left|s_n + s_{n+q} + \dots + s_{n+(t-1)q}\right| \ll N^{1/3}(\log N)^{2/3}.$$

A 17.8 Tétel bizonyítása. Csebisev tétele szerint tudjuk, hogy n és $2n$ közé mindig esik prím, így rögzítsük most p prímet úgy, hogy

$$\left(\frac{N}{\log N}\right)^{2/3} < p < 2\left(\frac{N}{\log N}\right)^{2/3}.$$

Definiáljuk az s_n sorozatot a következővel

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

Ekkor $D = \sum_{j=0}^{t-1} s_{n+jq}$ a következőképpen becsülhető:

I. eset: $p \mid q$. Ekkor

$$\begin{aligned} n + (t-1)q &\le N \\ (t-1)q &\le N - n \le N - 1 \\ t &\le \frac{N-1}{q} + 1 \le \frac{N-1}{p} + 1 \ll \frac{N}{\left(\frac{N}{\log N}\right)^{2/3}} \\ t &\ll N^{1/3}(\log N)^{2/3}. \end{aligned}$$

Vagyis a számtani sorozat differenciájára $t \ll N^{1/3}(\log N)^{2/3}$ fennáll, s ekkor a tétel triviális.

II. eset: $p \nmid q$. Jelölje χ a kvadratikus karaktert, azaz

$$\chi(n) = \begin{cases} \left(\frac{n}{p}\right), & \text{ha } p \nmid n, \\ 0, & \text{ha } p \mid n, \end{cases}$$

azaz ekkor

$$s_n = \begin{cases} \chi(n), & \text{ha } p \nmid n, \\ 0, & \text{ha } p \mid n. \end{cases}$$

Ekkor

$$|D| = \left| \sum_{j=0}^{t-1} \chi(n+jq) + \sum_{\substack{0 \le j \le t \\ p \mid n+jq}} 1 \right|.$$

A háromszög-egyenlőtlenség szerint:

$$|D| \le \left| \sum_{j=0}^{t-1} \chi(n+jq) \right| + \left| \sum_{\substack{0 \le m \le N \\ p \mid m}} 1 \right|.$$

Ebben az esetben $p \nmid q$, azaz létezik q^*, amelyre $qq^* \equiv 1 \pmod{p}$. Így

$$\begin{aligned} |D| &\le \left| \chi(q^*) \sum_{j=0}^{t-1} \chi(n+jq) \right| + \left[\frac{N}{p} \right] \\ &\le \left| \sum_{j=0}^{t-1} \chi(nq^*+j) \right| + \frac{N}{p}. \end{aligned}$$

A Pólya-Vinogradov egyenlőtlenség szerint (14.1 Tétel):

$$\begin{aligned} |D| &\le \sqrt{p} \log p + \frac{N}{p} \\ &\ll \left(\frac{N}{\log N} \right)^{1/3} \log \left(\frac{N}{\log N} \right)^{2/3} + \frac{N}{\left(\frac{N}{\log N} \right)^{2/3}} \\ &\ll N^{1/3} (\log N)^{2/3}. \end{aligned}$$

Így a tétel állítását mindkét esetben beláttuk.

Hivatkozások

[1] J. Beck, *Roth's estimate of the discrepancy of integer sequences is nearly sharp*, Combinatorica 1 (4) (1981), 319-325.

[2] P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Akadémiai Kiadó, Budapest, 1974.

[3] J. Matoušek, J. Spencer, *Discrepancy in arithmetic progression*, Jornal of the American Mathematical Society 9 (1) (1996), 195-204.

[4] K. F. Roth, *Remark concerning integer sequences*, Acta Arithmetica, 9 (1964), 257-260.

[5] K. F. Roth, *Irregularities of sequences relative to arithmetic progressions, I*, Math. Ann., 169 (1967), 1-25.

[6] A. Sárközy, *Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions. IV*, Acta Math. Academiae Scientiarum Hungaricae 30 (1977), 155–162.