Arvioita karakterisummille: Pólya–Vinogradovin epäyhtälö ja sen parannuksia

Jesse Jääsaari
Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Johdanto

Alkuluvut ovat analyyttisen lukuteorian keskeinen tutkimuskohde. Jo Eukleides todisti, että alkulukuja on äärettömän monta. Ensimmäinen huomio on, että lukua kaksi lukuunottamatta kaikki alkuluvut ovat parittomia. Yhdistettynä Eukleideen havaintoon niiden äärettömyydestä tämä tarkoittaa, että jonossa $\{2n+1\}_{n\geq 0}$ on äärettömän monta alkulukua. Tästä herää luonnollinen jatkokysymys: millä muilla aritmeettisilla jonoilla $\{an+b\}_{n\geq 0}$, jotka koostuvat positiivista kokonaisluvuista $b, a+b, 2a+b, 3a+b, ...$, on tämä ominaisuus? Mikäli lukujen a ja b suurin yhteinen tekijä d on aidosti suurempi kuin yksi, niin jokainen jonon termi on jaollinen luvulla d, ja siten jonossa on korkeintaan yksi alkuluku. Mutta mitä tapahtuu jos $d = 1$?

P. Dirichlet osoitti edistyneitä analyyttisen lukuteorian keinoja kayttën, että tässä tapauksessa jonosta $\{an+b\}_{n\geq 0}$ löytyy todella äärettömän monta alkulukua. Todistuksessa hän joutui erottamaan muista luvuista ne luvut, jotka antavat jakojäännöksen a luvulla n jaettaessa. Luonnollinen tapa tehdä tämä on muodostamaa joukon $\{x \in \mathbb{Z} \quad | x \equiv a \pmod{n}\}$ karakteristinen funktio eli sellainen funktio, joka saa arvon yksi tässä joukossa ja muualla arvon nolla. Valitettavasti tämä menetelmä ei kuitenkaan toimi. Sen sijaan Dirichlet määritteli toisenlaiset funktiot, joille myöhemmin löydettiin yhteyksiä myös muuhun matematiikkaan. Dirichlet'n määrittelemiä funktioita kutsutaan *Dirichlet'n karaktereiksi*, ja tämän artikkelin tarkoituksena on tarkastella niiden summan suuruusluokkaa.

Tarkemmin sanottuna tässä artikkelissa tarkastellaan karakterisummaa

$$\mathcal{S}_\chi(t) := \sum_{n\leq t} \chi(n),$$

missä χ on Dirichlet'n karakteri. Eräs syy tarkastella karakterisummia on esimerkiksi se, että ne liittyvät läheisesti alkulukujen jakautuneisuuteen aritmeettisissa jonoissa. Todistukset on yritetty kirjoittaa mahdollisimman yksityiskohtaisesti aiheen vaikeuden huomioiden, mutta silti joidenkin yksityiskohtien täydentäminen on jätetty lukijalle harjoitustehtäviksi.

Merkintöjä

Käydään nopeasti läpi käytettävät merkinnät. Olkoot $f, g : \mathbb{R} \longrightarrow \mathbb{C}$ funktioita. Vinogradovilta peräisin oleva merkintä $f \ll g$ tarkoittaa, että on olemassa vakio C siten, että $|f(x)| \leq C|g(x)|$ kaikilla $x \in \mathbb{R}$. Jos vakio C riippuu jostakin parametrista ε, niin merkitään $f \ll_\varepsilon g$.

Kuten tavallista, kompleksiluvun $z = x + iy$, $x, y \in \mathbb{R}$, konjugaattia merkintään $\overline{z} = x - iy$ ja reaaliosalle merkintää $\Re z = x$. Lisäksi positiivisten kokonaislukujen a ja b

suurinta yhteistä tekijää merkitään suureella (a, b). Merkintä $e(x)$ tarkoittaa samaa kuin $e^{2\pi ix}$, kun $x \in \mathbb{R}$.

Tarvitsemme vielä muutaman aritmeettisen funktion määritelmän. Möbiuksen funktio $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ määritellään seuraavasti: Jos luvulla n on alkutekijähajotelma $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, niin

$$\mu(n) = \begin{cases} (-1)^k & \text{jos } n \text{ on neliövapaa,} \\ 0 & \text{muuten.} \end{cases}$$

Esimerkiksi siis, $\mu(1) = 1$, $\mu(4) = 0$, ja $\mu(p) = -1$, kun p on alkuluku. Määrittelemme vielä Eulerin funktion $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ tulona

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right),$$

kun luvulla n on alkulukuhajotelma $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Lukijalle jätetään harjoitustehtäväksi osoittaa, että itse asiassa $\varphi(n)$ kertoo niiden välin $[1, n]$ kokonaislukujen lukumäärän, joilla ei ole yhteisiä tekijöitä luvun n kanssa. Lopuksi, summaustapa $\sum_{n \leq t}$ tarkoittaa, että summa otetaan niiden positiivisten kokonaislukujen yli, jotka ovat korkeintaan t.

Dirichlet'n karakterit

Olkoon q kiinnitetty positiivinen kokonaisluku. Määritellään funktio $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ seuraavilla kolmella ehdolla:

1. $\chi(n + q) = \chi(n)$ kaikilla $n \in \mathbb{Z}$.
2. Jos $(n, q) > 1$, niin $\chi(n) = 0$, ja muuten $\chi(n) \neq 0$.
3. $\chi(mn) = \chi(m)\chi(n)$, kaikilla $m, n \in \mathbb{Z}$.

Tällaista funktiota kutsutaan *Dirichlet'n karakteriksi modulo* q ja sitä merkitään $\chi \pmod q$. Jatkossa Dirichlet'n karaktereja kutsutaan yksinkertaisesti vain karaktereiksi[1].

Katsotaan seuraavaksi esimerkkejä karaktereista. Jos $q = 1$, niin löytyy vain yksi karakteri: $\chi(n) = 1$ kaikilla $n \in \mathbb{Z}$. Tätä kutsutaan *triviaalikarakteriksi*. Kun $q = 5$, karaktereita löytyy peräti neljä kappaletta, jotka on lueteltu alla olevassa taulukossa (vasemmanpuolimmaisessa sarakkeessa on karakteri ja ylimmällä rivillä on karakterin arvot $\chi(n)$; muut arvot saadaan 5-jaksollisuuden avulla, ts. $\chi(n) = \chi(n + 5)$ kaikilla kokonaisluvuilla n):

χ/n	0	1	2	3	4
χ_1	0	1	1	1	1
χ_2	0	1	i	$-i$	-1
χ_3	0	1	-1	-1	1
χ_4	0	1	$-i$	i	-1

Tässä luku i on imaginääriyksikkö eli kompleksiluku, jolla on ominaisuus $i^2 = -1$. Karaktereja modulo 5 on siis neljä kappaletta. Yleisemmin voidaan todistaa, että karaktereja modulo q on täsmälleen $\varphi(q)$ kappaletta ([1] s. $138 - 139$).

Siten myös karaktereja modulo 10 on $\varphi(10) = 4$ kappaletta. Yksi niistä on tietysti pääkarakteri ja toinen karakteri määräytyy arvoista $\chi(0) = 0$, $\chi(1) = 1$, $\chi(2) = 0$, $\chi(3) = i$, $\chi(4) = 0$, $\chi(5) = 0$, $\chi(6) = 0$, $\chi(7) = -i$, $\chi(8) = 0$, ja $\chi(9) = -1$. Lukijalle jätetään harjoitukseksi löytää puuttuvat kaksi karakteria (mod 10).

Esitetään sitten muutamia määritelmiä. Karakteri $\chi \pmod q$ on *pääkarakteri*, jos $\chi(n) = 1$, kun $(n, q) = 1$ ja $\chi(n) = 0$ muuten. Pääkarakterille varataan merkintä χ_1. Karakteri on *primitiivinen*, jos jokaisella luvun q aidolla tekijällä $d \neq q$ löytyy $0 \leq a \leq q - 1$ siten, että $a \equiv 1 \pmod d$ ja $\chi(a) \neq 1$. Karakterin *johtaja* puolestaan on pienin positiivinen kokonaisluku b, joka on luvun q tekijä, ja jolla on ominaisuus $\chi(n + b) = \chi(n)$ kaikilla n, joilla $(n, q) = (n, b) = 1$. Lopuksi, karakterin *kertaluku* on pienin positiivinen kokonaisluku n, jolla χ^n on pääkarakteri modulo q.

[1] Yleisesti näin ei tehdä, sillä matematiikassa on monia muitakin karaktereja.

Pólya–Vinogradovin arvio

Aloitetaan tarkastelu katsomalla millaisia arvioita suureelle $|\mathcal{S}_\chi(t)|$ saadaan vähällä vaivalla. Jos $\chi \pmod q$ on pääkarakteri, niin saadaan helposti

$$\mathcal{S}_\chi(t) = \left\lfloor \frac{t}{q} \right\rfloor \varphi(q) + \varphi\left(t - \left\lfloor \frac{t}{q} \right\rfloor q\right),$$

jos tulkitaan, että $\varphi(0) = 0$. Tämän todistus on harjoitustehtävä (vihje: kirjoita $t = kq + r$, missä $k \in \mathbb{Z}_+ \cup \{0\}$, $0 \leq r < q$ ja huomaa, että $(a, q) = 1$ jos ja vain jos $(a+q, q) = 1$). Erityisesti, jos q on alkuluku, niin $\mathcal{S}_\chi(q) = q - 1$.

Siten jätämme pääkarakterin pois tarkastelusta. Ensimmäistä arviota varten tarvitsemme seuraavan tuloksen.

Lemma 1. Olkoon $\chi \pmod q$ karakteri, joka ei ole pääkarakteri. Tällöin

$$\sum_{n=1}^{q} \chi(n) = 0.$$

Todistus. Koska χ ei ole pääkarakteri, niin löytyy kokonaisluku m siten, että $\chi(m) \neq 0, 1$. Koska $\chi(n) = 0$, kun $(n, q) > 1$, niin summaus voidaan ajatella yli lukujen $1 \leq n \leq q$, joilla $(n, q) = 1$. Kun n käy läpi nämä luvut, niin samoin käy $m' = mn \pmod q$. Siten karakterin täyden multiplikatiivisuuden nojalla

$$\begin{aligned}\chi(m) \sum_{n=1}^{q} \chi(n) &= \sum_{\substack{1 \leq n \leq q \\ (n,q)=1}} \chi(mn) \\ &= \sum_{\substack{1 \leq m' \leq q \\ (m',q)=1}} \chi(m') \\ &= \sum_{n=1}^{q} \chi(n).\end{aligned}$$

Koska $\chi(m) \neq 1$, niin väite seuraa. □

Koska karakterin itseisarvo on korkeintaan yksi, saadaan kolmioepäyhtälön nojalla

$$|\mathcal{S}_\chi(t)| \leq \sum_{n \leq t} |\chi(n)| \leq t.$$

Toisaalta, koska luvuista $\chi(0), \chi(1), ..., \chi(q-1)$ tasan $\varphi(q)$ kappaletta ovat nollasta poikkeavia, niin yllä olevan huomion ja Lemman 1 nojalla

$$|\mathcal{S}_\chi(t)| \leq \min(t, \varphi(q)).$$

Tämä tunnetaan *triviaaliestimaattina*. Yleisesti se on paras mahdollinen arvio, sillä pääkarakterilla $\chi_1 \pmod q$ pätee $|\mathcal{S}_{\chi_1}(q)| = \varphi(q)$. Tätä arviota on parannettu aikojen saatossa ei-pääkaraktereilla. Tässä artikkelissa todistetaan ensimmäinen epätriviaali arvio ei-pääkaraktereille, joka tunnetaan Pólya-Vinogradovin epäyhtälönä. Nimensä se on saanut G. Pólyalta ja I.M. Vinogradovilta, jotka todistivat kyseisen arvion toisistaan riippumatta vuonna 1918 [6], [7]. Tätä varten johdetaan ensin sarjaesitys primitiiviselle karakterille $\chi \pmod q$. Merkitään

$$\tau(\chi) := \sum_{a=1}^{q} \chi(a) e\left(\frac{a}{q}\right).$$

Suuretta $\tau(\chi)$ kutsutaan karakteriin $\chi \pmod q$ liittyväksi *Gaussin summaksi*.

Lemma 2. Olkoon $\chi \pmod q$ primitiivinen karakteri. Tällöin

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{m=1}^{q} \overline{\chi}(m) e\left(\frac{mn}{q}\right)$$

kaikilla kokonaisluvuilla n.

Todistus. Todistetaan väite ensin niille luvuille n, joille $(n, q) = 1$. Harjoitustehtävänä lukija voi todeta, että jokaisella $n \in \mathbb{Z}$, jolla $(n, q) = 1$, löytyy kokonaisluku $\tilde{n}$ siten, että $n\tilde{n} \equiv 1 \pmod q$, jolloin $\chi(\tilde{n}) = \overline{\chi}(n)$. Tällöin

$$\begin{aligned}\chi(n)\tau(\overline{\chi}) &= \chi(n)\sum_{m=1}^{q}\overline{\chi}(m)e\left(\frac{m}{q}\right)\\ &= \sum_{m=1}^{q}\overline{\chi}(\tilde{n}m)e\left(\frac{m}{q}\right)\\ &= \sum_{m=1}^{q}\overline{\chi}(m)e\left(\frac{mn}{q}\right). \qquad (1)\end{aligned}$$

Näytetään sitten, että $\tau(\overline{\chi}) \neq 0$. Osoitetaan, että itse asiassa $|\tau(\overline{\chi})| = \sqrt{q}$ primitiivisellä $\chi \pmod q$. Tätä tietoa tullaan tarvitsemaan myöhemmin.

Identiteetistä (1) seuraa, että

$$\begin{aligned}&|\chi(n)|^2|\tau(\overline{\chi})|^2\\ &= \sum_{m=1}^{q}\sum_{m'=1}^{q}\overline{\chi}(m)\chi(m')e\left(\frac{n(m-m')}{q}\right).\end{aligned}$$

Summaamalla yli lukujen $n = 1, ..., q$, käyttäen tietoa, että lukujen $|\chi(n)|^2$ summa näiden lukujen yli on $\varphi(q)$, sekä tietoa, että

$$\begin{aligned}&\overline{\chi}(m)\chi(m')e\left(\frac{n(m-m')}{q}\right)\\ &+\overline{\chi}(m')\chi(m)e\left(\frac{n(m'-m)}{q}\right) = 0,\end{aligned}$$

ellei $m \equiv m' \pmod q$, saadaan

$$\varphi(q)|\tau(\overline{\chi})|^2 = q\sum_{m=1}^{q}\overline{\chi}(m)\chi(m) = q\varphi(q),$$

mistä haluttu yhtälö $|\tau(\overline{\chi})| = \sqrt{q}$ seuraa. Huomautetaan vielä, että myös $|\tau(\chi)| = \sqrt{q}$, sillä $\chi \pmod q$ on primitiivinen jos ja vain jos karakteri $\overline{\chi} \pmod q$ on primitiivinen.

Jakamalla luvulla $\tau(\overline{\chi})$ saadaan

$$\chi(n) = \frac{1}{\tau(\overline{\chi})}\sum_{m=1}^{q}\overline{\chi}(h)e\left(\frac{mn}{q}\right), \qquad (2)$$

mikä oli lemman väite.

Osoitetaan sitten, että kaava (2) pätee myös niillä luvun n arvoilla, joilla $d := (n, q) > 1$. Tässä tapauksessa $\chi(n) = 0$ ja siksi riittää osoittaa, että

$$\sum_{m=1}^{q}\overline{\chi}(m)e\left(\frac{mn}{q}\right) = 0.$$

Kirjoitetaan $q = q'd$. Tarkastellaan lukuja $h = q' \cdot a + b$, missä $a = 0, 1, ..., d-1$ ja $b = 0, 1, ..., q'-1$. Kun a ja b käyvät läpi kaikki mahdolliset näiden lukujen yhdistelmät, niin m käy läpi kaikki joukon $\{0, 1..., q-1\}$ alkiot. Siten

$$\begin{aligned}&\sum_{m=1}^{q}\overline{\chi}(m)e\left(\frac{mn}{q}\right)\\ &= \sum_{b=0}^{q'-1}\sum_{a=0}^{d-1}\overline{\chi}(q'a+b)e\left(\frac{(q'a+b)n}{q}\right)\\ &= \sum_{b=0}^{q'-1}e\left(\frac{bn}{q}\right)\sum_{a=0}^{d-1}\overline{\chi}(q'a+b),\end{aligned}$$

koska $\frac{q'an}{q}$ on kokonaisluku.
Nyt riittää osoittaa, että kiinnitetyllä q' kaava

$$\sum_{a=0}^{d-1}\overline{\chi}(q'a+b) = 0 \qquad (3)$$

on voimassa jokaisella kokonaisluvulla b. Tarkastellaan yhtälön (3) vasenta puolta b:n funktiona. Tällöin se on q'-jaksollinen (tämä jätetään lukijalle harjoitustehtäväksi). Olkoon c sellainen kokonaisluku, että $(c, q) = 1$ ja $c \equiv 1 \pmod{q'}$. Käyttäen q'-jaksollisuutta saadaan

$$\begin{aligned}\overline{\chi}(c)\sum_{a=0}^{d-1}\overline{\chi}(q'a+b) &= \sum_{a=0}^{d-1}\overline{\chi}(cq'a+cb)\\ &= \sum_{a=0}^{d-1}\overline{\chi}(aq'+cb)\\ &= \sum_{a=0}^{d-1}\overline{\chi}(q'a+b). \qquad (4)\end{aligned}$$

Huomataan, että primitiivisellä $\chi \pmod q$ on voimassa $\chi(n+q') \neq \chi(n)$ jokaisella q:n aidolla tekijällä q', kaikilla n, joilla

$(n,q)>1$ (tämä on taas jätetty harjoitustehtäväksi lukijalle). Tästä seuraa, että on olemassa kokonaisluvut c_1 and c_2 siten, että $(c_1,q)=(c_2,q)=1$, $c_1\equiv c_2 \pmod{q'}$ ja $\chi(c_1)\neq\chi(c_2)$. Siten on olemassa kokonaisluku $c\equiv c_1\overline{c_2} \pmod{q'}$, jolla $\overline{\chi}(c)\neq 1$, $c\equiv 1 \pmod{q'}$ ja $(c,q)=1$. Valitsemalla tämän c:n yhtälössä (4) saadaan yhtälö (3). Näin ollen lemman todistus on viimein valmis. □

Nyt voidaan muotoilla ja todistaa Pólya–Vinogradovin lause. Seuraamme kirjan [1] todistusta. Huomionarvoista on, että tämä raja on huomattavasti parempi kuin triviaaliestimaatin antama yläraja, sillä logaritmi kasvaa paljon hitaamminen kuin neliöjuuri.

Lause 3. Olkoon $\chi \pmod q$ ei-pääkarakteri. Tällöin

$$\mathcal{S}_\chi(t) \ll \sqrt{q}\log q.$$

Todistus. Oletetaan ensin, että χ on primitiivinen. Lemman 2 perusteella sillä on esitys sarjana

$$\chi(n)=\frac{1}{\tau(\overline{\chi})}\sum_{m=1}^{q}\overline{\chi}(m)e\left(\frac{mn}{q}\right).$$

Summaamalla lukujen $n\le t$ yli saadaan

$$\mathcal{S}_\chi(t)=\frac{1}{\tau(\overline{\chi})}\sum_{m=1}^{q-1}\overline{\chi}(m)\sum_{n\le t}e\left(\frac{mn}{q}\right),$$

koska $\chi(q)=0$. Ottamalla itseisarvot puolittain, kertomalla luvulla $\sqrt{q}$ ja käyttämällä tietoa $|\tau(\chi)|=\sqrt{q}$ saadaan

$$\sqrt{q}\cdot|\mathcal{S}_\chi(t)|=\left|\sum_{m=1}^{q-1}\sum_{n\le t}e\left(\frac{mn}{q}\right)\right|,$$

mistä kolmioepäyhtälöön avulla saadaan

$$\sqrt{q}\cdot|\mathcal{S}_\chi(t)|\le\sum_{m=1}^{q-1}\left|\sum_{n\le t}e\left(\frac{mn}{q}\right)\right|. \qquad (5)$$

Merkitään

$$f(m):=\sum_{n\le t}e\left(\frac{mn}{q}\right).$$

Huomataan, että

$$\begin{aligned} f(q-m) &= \sum_{n\le t}e\left(\frac{n(q-m)}{q}\right)\\ &= \sum_{n\le t}e\left(-\frac{mn}{q}\right)\\ &= f(-m)=\overline{f}(m)\end{aligned}$$

ja näin ollen $|f(q-m)|=|\overline{f}(m)|=|f(m)|$. Siten (5) voidaan kirjoittaa muodossa

$$\begin{aligned}\sqrt{q}\cdot|\mathcal{S}_\chi(t)| &\le 2\sum_{m<q/2}|f(m)| \qquad (6)\\ &+ \frac{(-1)^q+1}{2}\left|f\left(\frac{q}{2}\right)\right|.\end{aligned}$$

Erityisesti jos q on pariton, niin jälkimmäinen termi katoaa.

Koska lausekkeen $f(m)$ termit muodostavat geometrisen sarjan, niin lukiosta tutun summakaavan avulla voidaan laskea, että luvun $f(m)$ itseisarvo on

$$\begin{aligned}|f(m)| &= \left|e\left(\frac{m\lfloor t+1\rfloor}{2q}\right)\frac{e\left(-\frac{\lfloor t\rfloor m}{2q}\right)-e\left(\frac{\lfloor t\rfloor m}{2q}\right)}{e\left(-\frac{m}{2q}\right)-e\left(\frac{m}{2q}\right)}\right|\\ &= \left|\frac{\sin\frac{\pi\lfloor t\rfloor m}{q}}{\sin\frac{\pi m}{q}}\right|\le\frac{1}{\sin\frac{\pi m}{q}}.\end{aligned}$$

Nyt käyttämällä epäyhtälöä $\sin t\ge\frac{2t}{\pi}$ (mikä pätee kun $t\in[0,\pi/2]$, todistus harjoitustehtävänä), arvolla $t=\frac{\pi m}{q}$ saadaan

$$|f(m)|\le\frac{q}{2m}.$$

kun $m\le\frac{q}{2}$. Jos q on pariton, niin kaava (6) antaa

$$\begin{aligned}\sqrt{q}\cdot|\mathcal{S}_\chi(t)| &\le q\sum_{m<\frac{q}{2}}\frac{1}{m}\\ &< q\log q.\end{aligned}$$

Jos taas q on parillinen, niin $|f(q/2)|\le 1$ ja siten (6) antaa

$$\sqrt{q}\cdot|\mathcal{S}_\chi(t)|\le q\left(\sum_{m<\frac{q}{2}}\frac{1}{m}+\frac{1}{q}\right)<q\log q.$$

Molemmissa tapauksissa

$$|\mathcal{S}_\chi(t)| < \sqrt{q}\log q,$$

kuten haluttiinkin.

Oletetaan seuraavaksi, että $\chi \pmod q$ on ei-primitiivinen karakteri ja olkoon c sen johtaja. Tällöin

$$\chi(m) = \psi(m)\chi_1(m),$$

missä χ_1 on pääkarakteri modulo q ja ψ on jokin primitiivinen karakteri modulo c (tämän tarkistaminen jätetään lukijalle).

Käyttämällä edellistä kaavaa saadaan

$$\begin{aligned}
\mathcal{S}_\chi(t) &= \sum_{\substack{n\le t\\(n,q)=1}} \psi(n)\\
&= \sum_{n\le t}\psi(n)\sum_{d\mid(n,q)}\mu(d)\\
&= \sum_{n\le t}\sum_{\substack{d\mid q\\ d\mid n}}\mu(d)\psi(n)\\
&= \sum_{d\mid q}\mu(d)\sum_{q\le \frac{t}{d}}\psi(qd)\\
&= \sum_{d\mid q}\mu(d)\psi(d)\sum_{x\le\frac{t}{d}}\psi(x).
\end{aligned}$$

Koska Pólya–Vinogradovin epäyhtälö on voimassa primitiiviselle karakterille $\psi \pmod c$, niin

$$\begin{aligned}
|\mathcal{S}_\chi(t)| &\le \sum_{d\mid q}|\mu(d)\psi(d)|\left|\sum_{x\le\frac{t}{d}}\psi(x)\right| \qquad (7)\\
&< \sqrt{c}\log c\left|\sum_{d\mid q}\mu(d)\psi(d)\right|\\
&\le \sqrt{c}\log c\sum_{d\mid q}|\mu(d)\psi(d)|.
\end{aligned}$$

Huomataan sitten, että $|\mu(d)\psi(d)|$ on joko 0 tai 1. Se on yksi jos ja vain jos $|\mu(d)| = 1$ ja $|\psi(d)| = 1$. Siis täsmälleen silloin, kun d on neliövapaa ja $(d, c) = 1$. Silloin luku d voidaan kirjoittaa erisuurten alkulukujen tulona $d = p_1p_2\cdots p_l$. Silloin yksikään alkuluku p_i ei jaa lukua c. Siten jokainen alkuluku p_i jakaa luvun $\frac{q}{c}$ ja siten erityisesti d jakaa tämän luvun. Näin ollen

$$\begin{aligned}
\sum_{d\mid q}|\mu(d)\psi(d)| &\le \sum_{d\mid\frac{q}{c}}1\\
&\le 2\sum_{\substack{d\le\sqrt{\frac{q}{c}}\\ d\mid\frac{q}{c}}}1\\
&\le 2\sqrt{\frac{q}{c}}\\
&\ll \sqrt{\frac{q}{c}}.
\end{aligned}$$

Siten kaavasta (7) seuraa, että

$$\begin{aligned}
|\mathcal{S}_\chi(t)| &\ll \sqrt{\frac{q}{c}}\cdot\sqrt{c}\log c\\
&\ll \sqrt{q}\log c\\
&\ll \sqrt{q}\log q,
\end{aligned}$$

mikä toditaa väitteen. □

Käyttämällä osittaissummauskaavaa

$$\sum_{n\le x}a_nf(n) = A(x)f(x) - \int_1^x A'(t)f'(t)\mathrm{d}t,$$

missä $a_1, ..., a_n$ ovat reaalilukuja, $A(x) = \sum_{n\le x}a_n$ ja f välillä $[1, x]$ derivoituva funktio (tätä voi ajatella diskreettinä osittaisintegrointina), saadaan alaraja primitiivisten karakterien summalle:

$$\begin{aligned}
\sqrt{q} &= |\tau(\chi)|\\
&\le \frac{2\pi}{q}\int_1^q|\mathcal{S}_\chi(t)|dt\\
&\le 2\pi\max_{t\le q}|\mathcal{S}_\chi(t)|
\end{aligned}$$

eli

$$|\mathcal{S}_\chi(t)| \gg \sqrt{q}.$$

Näin ollen Pólya–Vinogradovin epäyhtälöstä voitaisiin parhaimmillaan pudottaa tekijä $\log q$ pois.

Parannuksia

Tässä luvussa tarkastellaan Lauseen 3 mahdollisia vahvennuksia muutamassa eri tilanteessa. Ensinnäkin, Pólya–Vinogradovin epäyhtälöä voidaan parantaa olettamalla eräs merkittävä lukuteoreettinen väite. Määritellään Dirichlet'n L-funktio ja yleistetty Riemannin hypoteesi. Olkoon $\chi \pmod q$ karakteri ja $s \in \mathbb{C}$ sellainen, että $\Re s > 1$. Tällöin Dirichlet'n L-sarja on

$$L(s,\chi) := \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s}.$$

Tämän voi laajentaa meromorfiseksi funktioksi koko kompleksitasoon, jolloin siitä tulee Dirichletin L-funktio, jolle käytetään edelleen merkintää $L(s,\chi)$. Yleistetty Riemannin hypoteesi (YRH) sanoo seuraavaa.

Konjektuuri (YRH): Olkoon $\chi \pmod q$ karakteri ja $L(s,\chi)$ siihen liittyvä L-funktio. Jos $s \in \mathbb{C}$ on sellainen, että $0 \leq \Re s \leq 1$ ja $L(s,\chi) = 0$, niin itse asiassa $\Re s = 1/2$.

Riemannin hypoteesi, joka on yksi matematiikan tärkeimmistä avoimista ongelmista, on erikoistapaus yllä olevasta, kun χ on triviaalikarakteri.

Jos YRH on totta, niin seuraava vahvennos Pólya–Vinogradovin epäyhtälölle on voimassa.

Lause 4. Oletetaan YRH. Tällöin eipääkarekterilla $\chi \pmod q$ pätee

$$\mathcal{S}_\chi(t) \ll \sqrt{q} \log\log q.$$

Tämän todistivat H. Montgomery ja R.C. Vaughan vuonna 1977 [5].

Tarkastellaan sitten millaisia parannuksia on olemassa tietynlaisille karaktereille. Erityisesti tarkastelemme paritonta kertalukua olevia karaktereita. A. Granville, K. Soundararajan ja L. Goldmakher osoittivat seuraavan tuloksen.

Lause 5. Jos $\chi \pmod q$ on paritonta kertalukua $g \geq 3$ oleva karakteri, niin

$$|\mathcal{S}_\chi(t)| \ll_g \sqrt{q}(\log q)^{1-\delta_g+o(1)}, \qquad (8)$$

missä $\delta_g = 1 - \frac{g}{\pi}\sin\frac{\pi}{g}$ ja $o(1)$ on termi, joka lähestyy nolla, kun $g \longrightarrow \infty$.

Voidaan esimerkiksi laskea, että $1-\delta_2 = 0.636619...$, $1-\delta_3 = 0.8269933...$, $1-\delta_4 = 0.9003163...$, ja $1-\delta_5 = 0.935489...$ jne. Lisäksi lukija voi helposti todeta, että $1-\delta_g \longrightarrow 1$, kun $g \longrightarrow \infty$. Näin ollen parannukset suurilla g:n arvoilla ovat melko pieniä.

Alunperin Granville ja Soundararajan osoittivat arvion (9) muuttujalla $\delta_g/2$ [4], ja lopulta Goldmakher, Soundararajanin oppilaana, paransi muuttujan δ_g:een väitöskirjassaan [2, 3]. Arvion (4) todistus on pitkä ja se käyttää pitkälle meneviä analyysin menetelmiä ja siksi se sivuutetaan.

Keskustellaan vielä yhdestä parannuksesta. Montgomeryn ja Vaughanin tulokselle (Lause 4) on parannus YRH:n vallitessa. Tämäkin tulos on peräisin Granvillelta, Soundararajanilta ja Goldmakherilta [3, 4].

Lause 6. Oletetaan YRH. Jos $\chi \pmod q$ on paritonta kertalukua $g \geq 3$ oleva karakteri, niin

$$|\mathcal{S}_\chi(t)| \ll_g \sqrt{q}(\log\log q)^{1-\delta_g+o(1)} \qquad (9)$$

Ainoa ero lauseiden $3,5$ ja $4,6$ välillä on siis se, että $\log q$:n paikalla on $\log\log q$. Lauseiden 5 ja 6 väitteet ovat vahvempia kuin lauseiden 3 ja 4, sillä $\log\log x$ kasvaa hitaammin kun $\log x$. Pitää kuitenkin muistaa, että Lause 5 on todistettu vain tietynlaisille karaktereille ja, että lauseet 4 ja 6 eivät välttämättä pidä paikkaansa mikäli YRH ei päde.

References

[1] Apostol, T. M.: Introduction to Analytic Number Theory. Undergraduate Texts in Mathematics. Springer (1976).

[2] Goldmakher, L.: Multiplicative Mimicry and Improvements of the Pólya-Vinogradov Inequality. (2009), Phd-Thesis, University of Michigan.

[3] Goldmakher, L.: Multiplicative mimicry and improvements of the Pólya-Vinogradov inequality. Algebra and Number Theory Vol. 6 (2012), No. 1, s. 123 – 163.

[4] Granville, A. & Soundararajan, K.: Large character sums: Pretentious characters and the Pólya-Vinogradov theorem. J. Amer. Math. Soc. 20 (2007), no. 2, s. 357 – 384.

[5] Montgomery, H. & Vaughan, R.C.: Exponential sums with multiplicative coefficients. Invent. Math. 43 (1): s. 69 – 82.

[6] Pólya, G.: Über die Verteilung der quadratischen Reste und Nichtreste, Göttinger Nachrichten (1918), s. 21-29.

[7] Vinogradov, I.M.: Sur la distribution des résidus et des nonrésidus des puissances. J. Phys.-Mat. ob-va Permsk Univ. 1 (1918) s. 94-98.