Kokonaislukujen superpolynomiset laatoitukset

LuK Antti J. V. Tuominen

Pro gradu -tutkielma
Joulukuu 2021

Tarkastajat:
Prof. Jarkko Kari
Prof. Vesa Halava

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Antti J. V. Tuominen: Kokonaislukujen superpolynomiset laatoitukset
Pro gradu -tutkielma, 38 s., 0 liites.
Matematiikka
Joulukuu 2021

Kokonaislukujen laatoituksilla tarkoitetaan kaikkien kokonaislukujen peittämistä, jonkin tietyn joukon translaatioilla ilman päälekkäisyyksiä. Tällaisia laatoituksia on tutkittu pitkään, mutta erityisesti kiivaasti 1990-luvulta alkaen niiden tutkimus on edennyt paljon. Vaikka tutkimusala ei ole enää yhtä vilkas kuin 2000-luvun alussa, edelleen julkaistaan uusia tuloksia siitä millaiset laatat voivat laatoittaa kokonaisluvut.

Laatoituksien jaksonpituuden tutkiminen on erityisen kiintoisaa siksi, että voidaan todistaa, että kaikki laatoitukset ovat jaksollisia ja jaksonpituus on ylhäältä rajoitettu. Tähän liittyen on löydetty erilaisia laatoituksia, joiden jaksonpituus on erittäin pitkiä niihin käytettävän laatan pituuteen verraten.

Tässä tutkielmassa tarkastellaan kokonaislukujen laatoituksiin liittyviä tuloksia. Aluksi tutustutaan muutamiin tuloksiin siitä millaiset laatoitukset ovat mahdollisia, jonka jälkeen syvennytään tuloksiin laatoituksien jaksonpituuksista. Lopuksi esitellään esimerkkejä muutamista pitkäjaksoisista laatoituksista.

Asiasanat: laatoitukset, jaksollisuus, jaksonpituus, kokonaisluvut

Sisältö

1 Johdanto

Laatoituksella tarkoitetaan matematiikassa sitä, että jokin tila käytetään kokonaan erilaisilla tai samanlaisilla laatoilla, siten, että yhtään tilaa ei jää yli, mutta toisaalta laatat eivät myöskään mene keskenään päälekkäin. Esimerkiksi jos kuvitellaan, että $(2 \times n)$-kokoinen lauta ruutuja peitettäisiin dominoilla, tämä olisi kyseisen laudan laatoitus. Voidaan kuitenkin ajatella laatoituksia myös paljon laajemmin, kolmessa tai vaikka kymmenessä ulottuvuudessa. Nämä ovat usein hankalia tapauksia ratkaista, koska meillä ei ole niitä varten yhtä hyvää intuitiota. Tässä matematiikka ja formalismi voi kuitenkin auttaa.

Erilaisia laatoitusongelmia on tutkittu ahkerasti jo ainakin 1900-luvun alkupuolelta lähtien. Kuuluisat matemaatikot kuten Nicolaas G. de Bruijn (1918-2012), Donald J. Newman (1930-2007) ja Robert Tijdeman (1943-) ovat tutkineet niitä, sillä niillä on läheiset yhteydet joukkojen summiin, jaksollisuuteen, syklotomisiin polynomeihin ja laskettavuuteen liittyviin ongelmiin. Monasti itse laatoitusongelma ei olekaan se mikä tutkijoita on aluksi kiinnostanut, vaan se mitä muuta sen avulla voidaan todistaa.

Edelleen monet laatoitusongelmat ovat avoimia. Vasta viime vuosituhannen lopulla on esimerkiksi onnistuttu todistamaan kriteerejä laatan muodolle, jotka takaavat laatan laatoittavan kokonaisluvut. Ei kuitenkaan olla pystytty todistamaan, että ne ovat kattavat.[12] Moniulotteisesta tapauksesta tiedetään vieläkin vähemmän. Samat ongelmat on myös laajennettu tutkimuksessa koskemaan reaalilukuja ja niiden laatoittamista erilaisilla funktioilla.

Tässä tutkimuksessa keskitytään kokonaislukujen laatoituksiin ja erityisesti niiden jaksonpituuteen. Ala on kehittynyt paljon 2000-luvun ensimmäisen vuosikymmenen aikana, mikä tekee tutkielmasta ajankohtaisen. Kokonaislukujen laatoitukset ovat kiinnostavia monille tutkijoille erikoistapauksena, mutta niiden ymmärtämisellä on myös käytännön sovelluksia. Laatoitukset ovat jo muutamia vuosikymmeniä olleet tärkeä osa kaanonien teoriaa matemaattisen musiikkiteorian parissa ja saatua ymmärrystä ja erityisesti laatoitusten luokittelua voidaan soveltaa erilaisten musiikin ohjelmistojen kehityksessä.

2 Polynomien jaollisuuden teoriaa

Laatoitusten teoriassa on tapana rinnastaa laatat polynomeihin. Siksi monissa todistuksissa, varsinkin jaksonpituuksiin liittyvien lauseiden yhteydessä, on hyödyllistä tuntea joitain lauseita asiaan liittyen. Erityisen hyödyllinen käsite on jaoton polynomi, jota voidaan verrata laatoitukseen, joka ei koostu lyhyemmistä alijaksoista.

Määritelmä 2.1. Polynomi $P(x) \in \mathbb{Q}[x]$ on *jaoton*, jos kaikille mahdollisille hajotelmille $P(x) = Q(x)R(x)$, $Q(x), R(x) \in \mathbb{Q}[x]$ pätee, että joko $Q(x) \in \mathbb{Q}$ tai $R(x) \in \mathbb{Q}$. Muulloin polynomia sanotaan *jaolliseksi*.

2.1 Primitiiviset polynomit

Eräs tapa käsitellä ja tutkia polynomien jaollisuutta on käyttää primitiivisen polynomin käsitettä.

Määritelmä 2.2. Polynomi $P(x) \in \mathbb{Z}[x]$ on *primitiivinen*, jos sen kertoimien suurin yhteinen tekijä on 1.

Esimerkki 2.3. Olkoon polynomi $P(x) = \sum_{i=0}^{n} a_i x^i$ sellainen, että jokin kerroin $a_j = 1$. Tällöin pätee $\text{syt}_{0 \leq i \leq n}(a_i) = 1$, eli polynomi $P(x)$ on primitiivinen.

Mainitaan muutamia hyödyllisiä primitiivisiin polynomeihin liittyviä tuloksia. Todistukset lemmoille 2.4 ja 2.5 voi löytää esimerkiksi Magidinin ja McKinnonin tutkimuksesta.[15]

Lemma 2.4. *Jokainen polynomi $P(x) \in \mathbb{Q}[x]$ voidaan kirjoittaa muodossa $P(x) = cP^*(x)$, missä $c \in \mathbb{Q}$ on vakio ja $P^*(x)$ on jokin primitiivinen polynomi joukossa $\mathbb{Z}[x]$.*

Eräs kuuluisa ja monikäyttöinen lemma polynomien jaollisuudesta on niin kutsuttu Gaussin lemma primitiivisyydestä. Se on nimetty Carl Gaussin mukaan. Gauss esitti ja todisti vuonna 1801, kirjassaan *Disquisitiones Arithmeticae*, lemman joka on käytännössä yhtäpitävä[1] seuraavaksi esitettävän modernin muotoilun kanssa. Gauss oli tulloin vain 24 vuotias.[6]

Lemma 2.5. *Olkoot $P(x), Q(x) \in \mathbb{Z}[x]$ primitiivisiä polynomeja. Tällöin polynomi $P(x)Q(x)$ on myös primitiivinen polynomi.*

Erityisesti András Birón todistuksessa on hyödyllistä pitää mielessä seuraava lemma.

Lemma 2.6. *Olkoot $P_1(x), P_2(x) \in \mathbb{Z}[x]$ kaksi polynomia siten, että $P_1(x) | P_2(x)$ renkaassa $\mathbb{Q}[x]$ ja polynomin $P_1(x)$ ensimmäisen termin kerroin on 1. Tällöin $\frac{P_2(x)}{P_1(x)} \in \mathbb{Z}[x]$.*

Todistus. Polynomi $P_1(x)$ on primitiivinen, koska sen ensimmäinen termi on 1 ja siis kaikkien kertoimien suurin yhteinen tekijä on myös 1.

Tutkitaan nyt polynomia $Q(x) = \frac{P_2(x)}{P_1(x)} \in \mathbb{Q}[x]$. Lemman 2.4 mukaan tämä polynomi voidaan kirjoittaa muodossa $Q(x) = cQ^*(x)$, missä $c \in \mathbb{Q}$ on vakio ja $Q^*(x)$ on jokin primitiivinen polynomi joukossa $\mathbb{Z}[x]$.

Gaussin lemman 2.5 mukaan polynomi $P_1(x)Q^*(x)$ on primitiivinen ja nyt voidaankin kirjoittaa

$$P_2(x) = cP_1(x)Q^*(x) := cP_2^*(x),$$

missä $P_2^*(x)$ on lemman 2.4 mukainen primitiivinen polynomi polynomille $P_2(x)$.

[1] Gaussin muotoilun mukaan kahden polynomin $P(x), Q(x) \in \mathbb{Q}[x]$, joiden kertoimet eivät kaikki ole kokonaislukuja ja joiden suurimman asteisen termin kerroin on 1, tulolle pätee $P(x)Q(x) \in \mathbb{Q}[x]$ ja sen suurimman asteisen termin kerroin on 1, mutta toisaalta $P(x)Q(x) \notin \mathbb{Z}[x]$.

Koska $P_2(x) \in \mathbb{Z}[x]$ on selvää, että $c \in \mathbb{Z}$. Tällöin, kun $c \in \mathbb{Z}, Q^*(x) \in \mathbb{Z}[x]$, saadaan

$$Q(x) = cQ^*(x) \in \mathbb{Z}[x],$$

mikä todistaa väitteen. □

2.2 Syklotomiset polynomit

Määritelmä 2.7. *Syklotominen polynomi* on sellainen yksikäsitteinen kokonaislukukertoiminen polynomi $\Phi_s(x)$, $s \in \mathbb{N}$, että se jakaa polynomin $x^s - 1$, muttei jaa yhtään polynomia $x^k - 1$, kun $k < s$. Syklotomisen polynomin juuret ovat siis primitiiviset ykkösenjuuret $e^{2i\pi\frac{k}{s}}$, joille $\text{syt}(s,k) = 1$, eli

$$\Phi_s(x) = \prod_{\substack{k=1 \\ \text{syt}(k,s)=1}}^{s} \left(x - e^{2i\pi\frac{k}{s}}\right)$$

Laatoituksien parissa työskennellessä on erityisen hyödyllistä muistaa syklotomisten polynomien yhteys polynomiin $x^s - 1$.

Lemma 2.8. *Syklotomiset polynomit $\Phi_s(x)$, $s \in \mathbb{N}$, toteuttavat ehdon*

$$\prod_{s|n} \Phi_s(x) = x^n - 1$$

kaikilla $n \in \mathbb{N}$.

Todistus. Kirjoitetaan

$$\begin{aligned} x^n - 1 &= \prod_{k=1}^{n} \left(x - e^{2i\pi\frac{k}{n}}\right) \\ &= \prod_{s|n} \prod_{\substack{k=1 \\ \text{syt}(k,n)=s}}^{n} \left(x - e^{2i\pi\frac{k}{n}}\right) \\ &= \prod_{s|n} \Phi_{\frac{n}{s}}(x) \\ &= \prod_{s|n} \Phi_s(x). \end{aligned}$$

Tämä todistaa väitteen. □

Lause 2.9. *Olkoon p jokin alkuluku. Tällöin syklotominen polynomi $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ on jaoton renkaassa $\mathbb{Q}[x]$.*

Todistus. Lauseen voi todistaa suoraan Gaussin mukaan hieman yleisemmän lauseen nojalla.[7] Modernilla notaatiolla todistuksen on Gaussin mukaan esittänyt esimerkiksi Weintraub.[24] □

Monissa polynomien jaollisuuden todistuksissa, erityisesti syklotomisten polynomien yhteydessä, käytetään Eulerin totienttifunktiota, jonka Leonhard Euler (1707-1783) kehitti 1750-luvun lopulla ja julkaistiin hänen tutkielmassaan *Theoremata arithmetica nova methodo demonstrata.*[10] Funktio kuvaa niiden lukujen lukumäärää, joiden suurin yhteinen tekijä luvun n kanssa on 1.

Määritelmä 2.10. Funktio $\phi : \mathbb{N} \to \mathbb{N}$ määritellään

$$\phi(n) = \sum_{\substack{d=1 \\ \text{syt}(d,n)=1}}^{n} 1$$

ja sitä nimitetään **Eulerin totienttifunktioksi**.

Tälle on olemassa muutamia eri muotoiluja, joista seuraava lienee meille hyödyllisin.

Lause 2.11. *Eulerin totienttifunktio on*

$$\phi(n) = n \prod_{\substack{p=2 \\ p\in\mathbb{P}, p|n}}^{n} \left(1 - \frac{1}{p}\right),$$

jossa $\mathbb{P}$ on alkulukujen joukko.

Tästä seuraa suoraan seuraava lemma, jonka todistus on jokseenkin triviaali.

Lemma 2.12. *Olkoot $\phi(n)$ Eulerin totienttifunktio ja $k \in \mathbb{N}$. Nyt pätee*

1. $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.
2. $\phi(p) = p - 1$.
3. $\phi(p^k) \geq \frac{1}{2}p^k$.

Gauss on todistanut kuuluisan tuloksen Eulerin totienttifunktioiden summasta jo vuonna 1798.[5]

Lemma 2.13. *Eulerin totienttifunktiolle pätee*

$$\sum_{d=2, d|n}^{n} \phi(d) = n.$$

Lisäksi Eulerin totienttifunktiolla on seuraavat ominaisuudet.

Lause 2.14. *Olkoot $n, m \in \mathbb{N}$, $d = syt(m, n)$ ja $\phi(n)$ Eulerin totienttifunktio. Nyt pätee seuraavat lauseet.*

1. $\phi(mn) = \phi(n)\phi(m)\frac{d}{\phi(d)}$
2. $\phi(2m) = \begin{cases} 2\phi(m), & \text{jos } m \text{ on parillinen} \\ \phi(m), & \text{jos } m \text{ on pariton} \end{cases}$
3. $\phi(n^m) = n^{m-1}\phi(n)$

Todistus. Käyttäen lausetta 2.11

$$\phi(nm) = nm \prod_{\substack{p=2 \\ p\in\mathbb{P}, p|nm}}^{mn} \left(1 - \frac{1}{p}\right) = nm \frac{\prod^{n}_{\substack{p=2 \\ p\in\mathbb{P}, p|n}} \left(1 - \frac{1}{p}\right) \prod^{m}_{\substack{p=2 \\ p\in\mathbb{P}, p|m}} \left(1 - \frac{1}{p}\right)}{\prod^{d}_{\substack{p=2 \\ p\in\mathbb{P}, p|d}} \left(1 - \frac{1}{p}\right)} = \phi(n)\phi(m)\frac{d}{\phi(d)}.$$

Nyt, jos m on parillinen $d = \text{syt}(2, m) = 2$ eli

$$\phi(2m) = \phi(2)\phi(m)\frac{2}{\phi(2)} = 2\phi(m)$$

ja jos m on pariton, niin $d = \text{syt}(2, m) = 1$ eli

$$\phi(2m) = \phi(2)\phi(m)\frac{1}{\phi(2)} = \phi(m).$$

Lisäksi, kohdassa 3, kun $d = \text{syt}(n, n) = n$ saadaan

$$\phi(n^m) = \phi(n)\phi(n^{m-1})\frac{n}{\phi(n)} = \cdots = \phi(n)\phi(n)\frac{n^{m-1}}{\phi(n)} = n^{m-1}\phi(n).$$

□

3 Kokonaislukujen laatoitusten teoriaa

3.1 Hyödyllisiä määritelmiä

”Kokonaislukujen laatoitus” voi käsitteenä olla hieman oudolta kuulostava. Miten lukuja voi laatoittaa? Intuitiota parantaa kokonaislukujen kuvitteleminen äärettömänä nauhana ruutuja. Näitä ruutuja peitetään ”laatoilla”, esimerkiksi dominoilla eli (1×2)-laatoilla. Hyväksyttävä laatoitus on sellainen, että dominot eivät mene päälekkäin toistensa kanssa ja peittävät kaikki luvut, kuten kuvassa 1.

Kuva 1: Kuvassa on määritelmän 3.1 mukaan laatoitus $\{0, 1\} \oplus 2\mathbb{Z} = \mathbb{Z}$ laatalla $\{0, 1\}$ eli ”dominoilla”. Kuvassa on merkitty erikseen kokonaisluvut, jotka dominot peittävät, ja eri väreillä eri dominot.

Tämä on kuitenkin vain hyödyllinen intuitio, eikä sellaisenaan ole hyödyllinen meille. Tarvitaan siis muutamia tarkkoja määritelmiä, jotta voimme todistaa asioita laatoitusten rakenteesta.

Määritelmä 3.1. Olkoon $A \subset \mathbb{Z}$ äärellinen joukko kokonaislukuja. Olkoon $B \subset \mathbb{Z}$ sellainen kokonaislukujen joukko, että jokainen kokonaisluku $n \in \mathbb{Z}$ voidaan kirjoittaa yksikäsitteisesti muodossa $a+b$, jossa $a \in A, b \in B$. Merkitään tällöin $A \oplus B = \mathbb{Z}$ ja kutsutaan joukkoa A *laataksi*, joka *laatoittaa kokonaisluvut*.

Määritelmä 3.2. Jos A on laatta, olkoon *laatan pituus* $\text{diam}(A) = \max A - \min A$.

Määritelmä 3.3. Jos A on laatta, olkoon *laatan koko* $|A|$.

Määritellään vielä tarkemmin käytettävät jaksollisuuden käsitteet.

Määritelmä 3.4. Olkoot $t, n \in \mathbb{N} \setminus \{0\}$ ja $B \subset \mathbb{Z}$ tai $B \subset \mathbb{Z}_n$. Jos $B = B \oplus \{t\}$ sanotaan, että se on *jaksollinen* osajoukkona.

Määritelmä 3.5. Olkoot $t \in \mathbb{N} \setminus \{0\}$ ja $A \oplus B$ kokonaislukujen laatoitus siten, että $B = B \oplus \{t\}$. Tällöin t on laatoituksen *jaksonpituus* eli *jakso*.

Määritelmä 3.6. Laatalle A olkoon $\mathcal{K}(A)$ pisin mahdollinen A-laatoituksen jakso. Jos A ei laatoita kokonaislukuja, määritellään $\mathcal{K}(A) = 0$.

Määritelmä 3.7. Määritellään, että $\mathcal{D}(n) = \max\{\mathcal{K}(A) \mid \operatorname{diam}(A) \leq n\}$.

Toisin sanoen funktio $\mathcal{D}(n)$ kuvaa pisintä mahdollista n pituisten laattojen laatoituksen jaksoa.

3.2 Välin laatoituksen jaksollisuus

Tässä tutkimuksessa tullaan käymään läpi pitkäjaksoisia kokonaislukujen laatoituksia. Lukijaa ei kuitenkaan ole tarkoitus johtaa harhaan. Onkin mainittava, että tähän mennessä ei ole löydetty yhtään laattaa, joka laatoittaisi vain pitkäjaksoisesti. Lisäksi on muistettava, että välin laatoittaminen pitkäjaksoisesti (tässä: siten, että jaksonpituus on suurempi kuin $2n$ jos laatan pituus on n) ei ole mahdollista. Mihail Kolountzakis muotoili tämän lauseeksi vuonna 2002[13] seuraavasti:

Lause 3.8. *Jos* $0 \in A \cap B, n > 1, A \oplus B = \{0, 1, \ldots, n-1\}, A, B \subset \mathbb{Z}$ *ja* $\max A > \max B$ *niin* A *on jaksollinen joukon* $\mathbb{Z}_n$ *osajoukkona.*

Hän todisti lauseen viittaamalla Calvin Longin vuonna 1967 todistamaan tulokseen.[14]

Lemma 3.9. *Olkoot joukot* $A, B, C, D \subseteq \{0, 1, \ldots, n-1\}$ *sellaiset joukot, että jollekin kokonaisluvulle* $m \geq 2$ *pätee* $A = mC + \{0, 1, \ldots, m-1\}$ *ja* $B = mD$. *Olkoon* $p \geq 1$ *jokin kokonaisluku. Tällöin* $A \oplus B = \{0, 1, \ldots, mp-1\}$ *jos ja vain jos* $C \oplus D = \{0, 1, \ldots, p\}$.

Lisäksi Kolountzakis todisti[13] seuraavan lemman, joka seuraa lauseesta 3.8.

Lemma 3.10. *Jos* $A \subseteq \{0, \ldots, n\}, 0 \in A \cap B, A \oplus B = \{0, 1, \ldots, k-1\}$ *on laatoitus joukossa* $\mathbb{Z}$ *ja* $k > 2n$ *on olemassa sellainen* $t < k$ *siten että* $t|k$ *ja* $A \oplus (B \cap \{0, 1, \ldots, t-1\}) = \{0, 1, \ldots, t-1\}$ *on myös laatoitus joukossa* $\mathbb{Z}$.

Todistus. Koska $k - 1 = \max A + \max B$ seuraa, että $\max B > \max A$. Nyt lauseen 3.8 nojalla $B = B + t$ joukossa $\mathbb{Z}_k$ jollekin $t \in \{1, \ldots, k-1\}, t|k$. Tästä seuraa, että $A \oplus (B \cap \{0, \ldots, t-1\}) = \{0, 1, \ldots, t-1\}$ on myös laatoitus joukossa $\mathbb{Z}$. □

Itse asiassa pitkäjaksoisia laatoituksia voidaan Kolountzakiksen mukaan parhaiten kuvailla siten, että pitkä äärellisen pituinen sykli laatoitetaan epäjaksoisesti.[13] Tätä kuvailee seuraava lemma

Lemma 3.11. *Olkoon laatta* $A \subseteq \{0, 1, \ldots, M-1\}$, *jossa* M *on positiivinen kokonaisluku. Olkoon lisäksi* $B \subseteq \mathbb{Z}$ *joukko, jonka jaksonpituus on* M *eli* $B = B' \oplus M\mathbb{Z}$, *jossa* $B' \subseteq \{0, 1, \ldots, M-1\}$ *ja toisaalta* $B' \subseteq \mathbb{Z}_M$. *Tällöin* $A \oplus B = \mathbb{Z}$ *ja* M *on joukon* B *pienin jaksonpituus jos ja vain jos* $A \oplus B' = \mathbb{Z}_M$ *ja* B' *ei ole jaksollinen joukossa* $\mathbb{Z}_M$.

Todistus. Oletetaan ensin, että $A \oplus B = \mathbb{Z}$. Tästä seuraa, että $A \oplus (B' \oplus M\mathbb{Z}) = \mathbb{Z}$. Tällöin $A \oplus B' = \mathbb{Z}/M\mathbb{Z} = \mathbb{Z}_M$. Jos nyt $t \in \{1, \ldots, M-1\}$ ja $B' = B' + t$ joukossa $\mathbb{Z}_M$ niin $B = (B' + t) + M\mathbb{Z} = B + t$, mikä on ristiriita sen kanssa, että M on pienin B jaksonpituus.

Oletetaan nyt käänteisesti, että $A \oplus B' = \mathbb{Z}_M$ ja, että B' ei ole jaksollinen joukko joukossa $\mathbb{Z}_M$. Tällöin $A \oplus B = A \oplus B' \oplus M\mathbb{Z} = \{0, \ldots, M-1\} \oplus M\mathbb{Z} = \mathbb{Z}$ on M-jaksoinen kokonaislukujen laatoitus. Lisäksi, kuten edellä, jos joukolla B on pienempi jaksonpituus $t = \{1, \ldots, M-1\}$ seuraa, että joukon B' jaksonpituus on t joukossa $\mathbb{Z}_M$, mikä on ristiriita. □

3.3 Mahdolliset laatoitukset

Mielenkiintoinen on toki myös kysymys millaiset laatoitukset ovat mahdollisia. Tämä ei ole lainkaan triviaali kysymys, sillä edelleenkin kriteerit sille millainen laatan täytyy olla, jotta se laatoittaisi kokonaisluvut tunnetaan vain niille laatoille joiden koolla on hyvin pieni määrä alkulukutekijöitä. Donald Newman ratkaisi ongelman yhden alkuluvun potensseille vuonna 1977 julkaisemassaan artikkelissa.[16]

Lause 3.12. ***Newmanin lause*** *- Olkoot $a_1, a_2, \ldots, a_k$ eri kokonaislukuja, siten että $k = p^\alpha$, jossa p on alkuluku ja $\alpha \in \mathbb{N}$. Jokaiselle parille a_i, a_j, $i \neq j$, $i, j \in \{0, 1, \ldots, k\}$, merkitään, että $p^{e_{ij}}$ on korkein alkuluvun p potenssi, joka jakaa luvun $a_i - a_j$. Laatta $A = \{a_1, a_2, \ldots, a_k\}$ laatoittaa kokonaisluvut jos ja vain jos on olemassa korkeintaan α erilaista lukua e_{ij}.*

Lause voi olla tällaisenään hieman hankalaselkoinen, joten annetaan siitä esimerkki.

Esimerkki 3.13. Olkoon laatan A koko $k = 3$. Nyt, koska luku 3 on alkuluku, on selvää, että $\alpha = 1$. Olkoon laatta $A = \{0, a, b\}$, jossa $a \equiv 1 \mod 3$ ja $b \equiv 2 \mod 3$. Nyt selvästi

$$\begin{aligned} a - 0 &\equiv 1 \mod 3 \\ 0 - a &\equiv 2 \mod 3 \\ b - 0 &\equiv 2 \mod 3 \\ 0 - b &\equiv 1 \mod 3 \\ b - a &\equiv 1 \mod 3 \\ a - b &\equiv 2 \mod 3 \end{aligned}$$

eli vain 3^0 jakaa nämä luvut. Toisin sanoen, lukuja e_{ij} on yksi, jolloin lauseen 3.12 nojalla tällainen laatta laatoittaa kokonaisluvut.

Koska Newmanin lause kattaa vain laatat joiden koko on alkulukujen potenssi, edes laatojen joiden koko on 6 laatoituksia ei voitu karakterisoida kattavasti. Tilannetta ovat parantaneet matemaatikot Ethan Coven ja Aaron Meyerowitz vuonna 1999, todistamalla kriteerit kaikille laatoille, joiden koko on muotoa $|A| = p_1^{\alpha_1} p_2^{\alpha_2}$.[4] Tämä karakterisoi kaikki laatoitukset, joiden koko on alle $30 = 2 \cdot 3 \cdot 5$ lukua. Tässä esitetään Franck Jedrzejeweskin muotoilu lauseesta.[12]

Lause 3.14. ***Covenin-Meyerowitzin lause*** *- Olkoot A äärellinen joukko positiivisia kokonaislukuja ja $A(x) = \sum_{a \in A} x^a$ sellainen polynomi, että $|A| = A(1)$. Olkoon lisäksi S_A alkulukupotenssien $s = p^\alpha$ joukko, siten että niitä vastaavat syklotomiset polynomit $\Phi_s(x)$ jakavat polynomin $A(x)$. Kutsutaan seuraavia kahta ehtoa* ***Covenin-Meyerowitzin ehdoiksi****:*

(T1)

$$A(1) = \prod_{s \in S_A} \Phi_s(1)$$

(T2) Jos $s_1, s_2, \ldots, s_m \in S_A$ ovat eri alkulukujen potensseja, niin $\Phi_{s_1 s_2 \cdots s_m}(x)$ jakaa polynomin $A(x)$.

Näille ehdoille pätee

1. *Jos polynomille $A(x)$ pätevät ehdot (T1) ja (T2), niin A laatoittaa kokonaisluvut.*
2. *Jos A laatoittaa kokonaisluvut, niin polynomille $A(x)$ pätee ehto (T1).*
3. *Jos A laatoittaa kokonaisluvut ja luvulla $|A|$ on korkeintaan kaksi alkulukutekijää niin ehto (T2) pätee.*

Triviaalisti voidaan tiivistää lause lyhyempään muotoon.

Lemma 3.15. *Olkoot laatta A, $|A| = p_1^{\alpha_1} p_2^{\alpha_2}$. A laatoittaa kokonaisluvut jos ja vain jos sille pätevät molemmat Covenin-Meyerowitzin ehdot.*

Andrew Granville, Izabella Laba ja Yang Wang todistivat vuonna 2001 tuloksen laatoituksista joissa laatan koko on muotoa $|A| = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$, joille he paransivat Covenin-Meyerowitzin ehtoa (T2).[8]

Lause 3.16. *Olkoot A ja B kaksi laattaa siten, että $|A| = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$, $|B| = p_1 p_2 p_3$ ja $A \oplus B = \mathbb{Z}_M$, jossa $M = |A||B|$. Nyt jos syklotomiset polynomit $\Phi_{p_1}(x)$, $\Phi_{p_2}(x)$ ja $\Phi_{p_3}(x)$ jakavat polynomin $A(x)$ niin myös syklotomiset polynomit $\Phi_{p_1 p_2}(x)$, $\Phi_{p_1 p_3}(x)$, $\Phi_{p_2 p_3}(x)$ ja $\Phi_{p_1 p_2 p_3}(x)$ jakavat sen.*

Tämä karakterisoi monet kokoa $210 = 2 \cdot 3 \cdot 5 \cdot 7$ pienemmät laatoitukset.

Lisäksi Emmanuel Amiot vuonna 2005 [1] ja Franck Jedrzejewski vuonna 2009 [12] ovat todistaneet vastaavia tuloksia tietyille kaanoneille musiikkiteorian kontekstissa. Kaanon viittaa musiikkiin, jossa sama melodia toistuu useasti eri aikoina. Musiikkiteoriassa kaanonit on 1990-luvulta Dan Tudor Vuzan (1955-) pohjatyöstä lähtien analysoitu samalla tavalla kuten laatoitusten kontekstissa on analysoitu laatoitukset eli hajottamalla ne melodioiksi (laatoiksi) ja niiden toistoajoiksi (laattojen paikat määräävä ryhmä).[12] Jedrzejewski käyttää lisäksi apuna käsitettä Hajósin ryhmä, jonka György Hajós (1912-1972) esitteli vuonna 1942.[11]

Määritelmä 3.17. [1] Olkoot $A, B \subset \mathbb{N}$ äärellisiä joukkoja ja n kokonaisluku. Olkoon kyseessä **kaanon**, jos sisärytmille A, ulkorytmille B ja jaksonpituudelle n pätee

$$A \oplus B \oplus n\mathbb{Z} = \mathbb{Z}.$$

Määritelmä 3.18. [12] Abelin ryhmä G on **Hajósin joukko**, jos kaikilla jaoilla joukoiksi A ja B, siten että $A \oplus B = G$, ainakin toinen joukoista on jaksollinen.

Jos joukko G on muotoa $\mathbb{Z}_n$, on selvitetty kaikki joukot, jotka ovat Hajós joukkoja. Tämän on osoittanut muun muassa Arthur Sands vuonna 1962.[18]

Lause 3.19. *$\mathbb{Z}_n$ on Hajósin joukko jos ja vain jos n on muotoa: p^k kaikille $k \geq 0$, $p^k q$ kaikille $k \geq 1$, p^2q^2, pqr, p^2qr tai $pqrs$ neljälle eri alkuluvulle p, q, r ja s.*

Amiot todisti, että kaikkille $\mathbb{Z}_n$, jotka ovat Hajósin joukkoja pätee seuraava tulos.[1]

Lause 3.20. *Jos laatta A laatoittaa jaksonpituudella n ja $\mathbb{Z}_n$ on Hajósin juokko, niin Covenin-Meyerowitzin ehto (T2) pätee.*

Jedrzejewski osoitti lisäksi, että ei-jaksollisille kaanoneille pätee puolestaan lause.[12]

Lause 3.21. *Olkoon $n = p_1p_2n_1n_2n_3$ sellainen kokonaisluku, että $\mathbb{Z}_n$ ei ole Hajósin joukko. Olkoot K_1 ja K_2 joukot*

$$K_1 = n_2n_3(\{0, 1, \ldots, p_2 - 1\} \oplus \{0, p_2n_1, 2p_2n_1, \ldots, (p_1 - 1)p_2n_1\}),$$
$$K_2 = n_1n_3(\{0, 1, \ldots, p_1 - 1\} \oplus \{0, p_1n_2, 2p_1n_2, \ldots, (p_2 - 1)p_1n_2\}).$$

Olkoon lisäksi $T_j(K_2) = \{j\} \oplus K_2$ joukon K_2 translaatio luvulla j. Olkoot joukot A ja B sellaiset, että $|A| = n_1n_2$, $|B| = p_1p_2p_3$ ja

$$A = n_3(\{0, p_2n_2, \ldots, (n_1 - 1)p_2n_2\} \oplus \{0, p_1n_1, \ldots, (n_2 - 1)p_1n_1\}),$$
$$B = \bigcup_{j=0}^{n_3-1} T_j(K_2).$$

*Näiden joukkojen kaanon on ei-jaksollinen kaanon jota kutsutaan **kesyksi kaanoniksi**.*

Kuten huomataan, ei olla pystytty todistamaan, että kaikille laatoituksille pätee myös Covenin-Meyerowitzin ehto (T2), joka karakteroisi kaikki laatoitukset, tai esittämään vastaesimerkkiä, jolle se ei päde. Vaikka on pystytty lausumaan paljon eri joukkojen rakenteesta, ilman tätä yhteyttä laatoitusten jaksonpituuden tutkimus joutuukin kulkemaan eri teitä.

4 Jakson maksimipituuden ylärajat

Kun tiedetään minkä tahansa kokonaislukujen laatoituksen olevan lopulta jaksollinen, on järkevää kysyä mikä on pisin mahdollinen laatoituksen jakso. Tätä kysymystä on tutkittu jo kauan ja vastaus on tiedetty äärelliseksi jo 1970-luvulta lähtien.

Useimmat jakson ylärajoihin liittyvät todistukset pohjautuvat kuitenkin siihen, että todistetaan jaksonpituuden äärellisyys jollain keinolla. Newmanille riitti naiivi kyyhkyslakkaperiaate, mutta myöhemmät tutkijat lähestyvät lähes aina kysymystä samaistamalla laatoitukset polynomeihin. Soveltamalla polynomien jaollisuuteen liittyviä seikkoja he pystyvät todistamaan, että ne implikoivat ylärajan jakson pituudelle.

4.1 Newmanin triviaali yläraja

Donald J. Newman (1930-2007) julkaisi vuonna 1977 tutkimuksen *Tesselation of Integers*, jossa hän tutki millaiset laatoitukset ovat mahdollisia.[16] Lähes kaikki nykytutkijat viittaavat hänen ratkaisuunsa ensimmäiselle tunnetulle ylärajalle, joten tässäkin esityksessä lähdetään samasta artikkelista. Newmanin triviaalina ylärajana tunnetaan nykyään seuraava toteamus.

Lause 4.1. *Kaikille $n \in \mathbb{N}$ pätee*

$$\mathcal{D}(n) \leq 2^n.$$

Tämä ei varsinaisesti ole Newmanin tulos, mutta seuraa kuitenkin jokseenkin triviaalisti havainnosta, että $\mathcal{K}(A) \leq 2^{\mathrm{diam}(A)}$. Näin on käytännössä kaikkien muidenkin ylärajojen laita.

Todistus. Olkoon A_{max} sellainen laatta, että $\mathrm{diam}(A_{max}) \leq n$ ja $\mathcal{K}(A_{max}) = \mathcal{D}(n)$. Tällöin selvästi

$$\mathcal{D}(n) = \mathcal{K}(A_{max}) \leq 2^{\mathrm{diam}(A_{max})} \leq 2^n.$$

□

Newmanin tarkoitus ei tutkimuksessaan ollut tutkia laatoitusten jaksonpituuksia, vaan tämä havainto esitettiin erään toisen todistuksen osana. Newmanin tarkoitus oli todistaa, että jos $|A|$ on jonkin alkuluvun p potenssi, se laatoittaako A kokonaisluvut riippuu siitä kuinka monella alkuluvun p potenssilla A jäsenten erotukset ovat jaollisia. Tätä varten hän tarvitsi aputuloksen

Lause 4.2. *Olkoot $a_1, a_2, \ldots, a_k$ jotkin tietyt kokonaisluvut. Seuraavat väitteet ovat yhtäpitäviä.*

(I) On olemassa joukko $X = \{x_j\}$ jolla on tiheys $\frac{1}{k}$, siten että jokainen kokonaisluku voidaan ilmaista muodossa $a_i + x_j$.

(II) On olemassa joukko $X = \{x_j\}$ siten että jokainen kokonaisluku voidaan yksikäsitteisesti ilmaista muodossa $a_i + x_j$.

(III) On olemassa $N \in \mathbb{N}$ ja jäännösluokat $x_1, x_2, \ldots, x_N$ mod $(N \cdot k)$, siten että jokainen jäännösluokka mod $(N \cdot k)$ voidaan yksiselitteisesti ilmaista muodossa $a_i + x_j$.

Tässä esitetään vain tarpeellinen osa, jossa Newman todistaa halutun rajan, eli (II)→(III). Todistus etenee samoin kuin Newmanin tutkimuksessa, mutta sitä laajennetaan sanallisesti selkeyden vuoksi. Itse asiassa alkuperäisessä meille tärkeä yläraja ilmaistiin ohimennen sanomalla ”selvästi on vain 2^τ erilaista blokkia”, joten se, että tutkimukseen viitataan siten kuin Newman olisi käsitellyt ylärajaa tarkemminkin on minusta kyseenalaista.

Todistus. Oletetaan, että (II) pätee ja olkoon

$$C_n = \begin{cases} 1, & \text{kun } n \text{ on jokin } x_j, \\ 0, & \text{muulloin} \end{cases}$$

Olkoot x_1, $x_2 \in X$ ja oletetaan, että $n - a_1 = x_1, n - a_2 = x_2$. Tällöin selvästi

$$\begin{cases} n - a_1 = x_1 \\ n - a_2 = x_2 \end{cases} \Rightarrow n = a_1 + x_1 = a_2 + x_2,$$

mikä on ristiriita, koska jokaisella kokonaisluvulla n on yksikäsitteinen esitys muotoa $a_i + x_j$. Toisaalta, koska näin on, on olemassa sellaiset i ja j, että $n - a_i = x_j$. Saadaan siis erotusyhtälö $C_{n-a_1} + C_{n-a_2} + \ldots + C_{n-a_k} = 1$. Toisin sanoen jokainen peitetty luku määrää yhden edeltävän peitetyn luvun.

Tarkastellaan nyt arvoja $C_{m+1}, C_{m+2}, \ldots, C_{m+\tau}$, jossa

$$\tau = \max_{1 \leq i \leq k} a_i - \min_{1 \leq i \leq k} a_i.$$

ja $m \in \mathbb{Z}$. Jokaiselle luvulle $l \in \{m+1, \ldots, m+\tau\}$ pätee, että C_l voi olla joko 0 tai 1. Siksi mahdollisia sarjoja $C_{m+1}, C_{m+2}, \ldots, C_{m+\tau}$ on 2^τ erilaista.

Koska määrä on rajallinen on kyyhkyslakkaperiaatteen nojalla olemassa kaksi blokkia $C_{n_1+1}, C_{n_1+2}, \ldots, C_{n_1+\tau}$ ja $C_{n_2+1}, C_{n_2+2}, \ldots, C_{n_2+\tau}$, jotka ovat identtiset. Koska τ:n blokki C_n:iä määrää koko sarjan, voidaan päätellä, että C_n on identtisesti yhtäsuuri $C_{n+n_2-n_1}$:n kanssa eli C_n on *jaksollinen*. Toisin sanoen x_j:t ovat jaksollisia ja muodostavat jäännösluokat ja (III) seuraa helposti. □

Newmanin yläraja ei ole enää rajoista paras, eikä sitä sellaiseksi oletettukaan. Se on kuitenkin rajoista ainoa, jolla ei ole yleisiä rajoituksia ja joka pätee myös pienillä laatan pituuksilla, ei eksponentiaalisesti kasvavilla arvoilla. Tämän takia Newmanin raja on relevantti vielä nykyäänkin.

4.2 Ruzsan yläraja

Imre Z. Ruzsan (1953-) kuuluisa parannus esitettiin ensi kerran Rob Tijdemanin artikkelin *Periodicity and Almost-Periodicity* liitteessä vuonna 2002.[22] Artikkelissaan Tijdeman laajentaa Budapestissa 10.6.2002 pitämäänsä esitelmää, ja esittää oman jaksollisuuden parissa tekemänsä työn hedelmiä ja avoimia kysymyksiä.

Näistä ongelmista toinen kuuluu: ”Mikä on jaksonpituuden paras yläraja laatan pituuden diam(A) funktiona?”. Ruszan hänelle lähettämää osittaista ratkaisua Tijdeman kuvailee jälkiruoaksi, hänen itsensä tarjoileman pääruoan jälkeen. Seuraavaksi esitettävä todistus seuraa Ruzsan todistusta.

Lause 4.3. *On olemassa vakio $c > 0$ siten, että*

$$\mathcal{D}(n) \leq e^{c\sqrt{n \ln(n)}}$$

kaikille tarpeeksi suurille n.

Todistus. Olkoon $A \subset \mathbb{Z}$ laatta, jonka pituus on n, ja $B \subset \mathbb{Z}$ sellainen joukko, että $A \oplus B = \mathbb{Z}$. Yleisyyttä menettämättä voidaan olettaa, että $\min_{a \in A} a = 0$. Olkoon $B^+ = B \cap [0, \infty)$ ja $C = \{n \in \mathbb{Z} : n \geq 0, n = a + b, a \in A, b \in B, b < 0\}$.

Toisin sanoen B^+ on niiden positiivisten lukujen b joukko, jotka osoittavat ainoastaan positiivisia lukuja peittävien laattojen paikat. C on niiden positiivisten kokonaislukujen joukko, jotka tarvitsevat negatiivisia arvoja b hajotelmassaan eli se sisältää vain ne positiiviset kokonaisluvut, joita $A \oplus B^+$ ei peitä. Määritellään vielä kolme funktiota

$$f(x) = \sum_{a \in A} x^a, \ g(x) = \sum_{b \in B^+} x^b, \text{ ja } h(x) = \sum_{c \in C} x^c.$$

Nyt, koska jokainen summa $a + b$ on yksikäsitteinen kokonaisluku, saadaan

$$f(x)g(x) + h(x) = \sum_{i \in \mathbb{N} \setminus C} x^d + \sum_{c \in C} x^c = \sum_{i=0}^{\infty} x^i = \frac{1}{1-x}.$$

Tässä f ja h ovat äärellisen pituisia polynomeja. Kokonaisluku k on joukon B jaksonpituus jos $g(x)(1-x^k)$ on äärellinen polynomi. Koska laatoitukset ovat kaikki jaksollisia lauseen 4.1 nojalla, tällainen k on olemassa. Tässä halutaan osoittaa, että se voi olla pieni. Olkoon $n = \max_{a \in A} a$, jolloin selvästi $\deg f = n$. Nyt saadaan

$$g(x) = \frac{\frac{1}{1-x} - h(x)}{f(x)} = \frac{1 - (1-x)h(x)}{(1-x)f(x)} = \frac{p(x)}{q(x)},$$

jossa p ja q ovat keskenään jaottomia polynomeja. Tällöin voidaan kirjoittaa

$$g(x)(1-x^k) = \frac{p(x)(1-x^k)}{q(x)}.$$

Koska p ja q ovat keskenään jaottomia ja toisaalta $g(x)(1-x^k)$ on äärellinen polynomi jako menee tasan ja nähdään, että

$$q(x) | 1 - x^k = \prod_{d|k} \Phi_d(x),$$

jossa Φ_d on d:s syklotominen polynomi. Toisin sanoen

$$q(x) = \prod_{d \in D} \Phi_d(x)$$

jossa $D \subseteq \{d : d|k, d \in \mathbb{N}\}$ on jaksonpituuden k tekijöiden joukko. Käänteisesti, jos $q(x) = \prod_{d \in D} \Phi_d(x)$ ja määritellään $k = \text{pyj}_{d \in D} d$, niin $q(k) | 1 - x^k$, joten

$$g(x)(1-x^k) = \frac{p(x)(1-x^k)}{q(x)}$$

on äärellinen polynomi. Nyt saadaan

$$n + 1 \geq \deg q = \sum_{d \in D} \deg \Phi_d = \sum_{d \in D} \phi(d),$$

jossa ϕ on Eulerin totienttifunktio. Olkoot $p_1^{a_1}, \ldots, p_r^{a_r}$ luvun k jakavat alkulukupotenssit, jotka ovat aidosti suurempia kuin L. Oletetaan, että $L > 2$, jolloin $\phi\left(p_i^{a_i}\right) > 2$. Jokainen $p_i^{a_i}$ jakaa tasan jonkun $d \in D$. Käyttämällä toistuvasti epäyhtälöä $xy > x + y$, joka pätee kun $x, y > 2$, näemme, että

$$\begin{aligned}
\frac{1}{2}\sum_{i=1}^{r} p_i^{a_i} &\leq \sum_{i=1}^{r} p_i^{a_i}\left(1 - \frac{1}{p_i}\right) \\
&= \sum_{i=1}^{r} \phi\left(p_i^{a_i}\right) \\
&< \phi\left(p_1^{a_1}\right) \cdots \phi\left(p_r^{a_r}\right) \\
&= \phi\left(p_1^{a_1} \cdots p_r^{a_r}\right) \\
&\leq n + 1
\end{aligned}$$

Nyt $r \leq \frac{2(n+1)}{L}$ ja

$$\prod_{i=1}^{r} p_i^{a_i} \leq (n+1)^{\frac{2(n+1)}{L}} < n^{\frac{c_1 n}{L}}.$$

Tästä seuraa, että

$$k \leq \prod_{i=1}^{r} p_i^{a_i} \mathrm{pyj}_{1 \leq l \leq L-1} l < n^{\frac{c_1 n}{L}} e^{c_2 L} = e^{\ln n \frac{c_1 n}{L}} e^{c_2 L} = e^{\ln n \frac{c_1 n}{L} + c_2 L}.$$

Tehdään sijoitus $L = \sqrt{n \ln n}$. Nyt

$$k < e^{\ln n \frac{c_1 n}{L} + c_2 L} = e^{\ln n \frac{c_1 n}{\sqrt{n \ln n}} + c_2 \sqrt{n \ln n}} = e^{(c_1 + c_2)\sqrt{n \ln n}} < e^{c_3 \sqrt{n \ln n}}.$$

□

4.3 Kolountzakiksen yläraja

Mihail N. Kolountzakis todisti vuonna 2002 itsenäisesti seuraavan Ruzsan ylärajaa heikomman tuloksen. Kolountzakiksen ylärajan todistus on hyvin samanlainen kuin Ruzsan, mutta Ruzsan on saanut ylärajastaan terävämmän käyttämällä kriittisessä kohdassa tulon asemesta lukujen pienintä yhteistä jakajaa

Seuraavassa esitetään Kolountzakiksen todistus ylärajalleen, joka julkaistiin 2003 artikkelissa *Translational tilings of the integers with long periods.*[13]

Lause 4.4. *On olemassa sellaiset vakiot $c_1, c_2 > 0$, että*

$$\mathcal{D}(n) \leq c_1 e^{c_2 \sqrt{n} \ln n \sqrt{\ln \ln n}}$$

kaikille $n > 1$.

Todistus. Oletetaan, että $A \subseteq \{0, \ldots, n\}$, $n < M$ ja että $A \oplus B' = \mathbb{Z}_M$, jollekin $B' \subseteq \mathbb{Z}_M$. Riittää näyttää, että jos M on tarpeeksi suuri niin B' on jaksollinen. Tällöin lause seuraa lemmasta 3.11.

Jos joukko B' on jaksollinen, on olemassa $t \in \mathbb{Z}_M \setminus \{0\}$ siten, että $B' = B' + t$. Tämä on yhtäpitävä sen kanssa, että kun mille tahansa kokonaislukujen joukolle E määritellään polynomi

$$E(x) = \sum_{n \in E} x^n$$

pätee aina

$$B'(x) = x^t B'(x) \mod x^M - 1.$$

Tämä taas on yhtäpitävä sen kanssa että $x^M - 1 \mid (x^t - 1)B'(x)$. Tämä tarkoittaa, että kaikki syklotomiset polynomit $\Phi_d(x)$ siten, että $d \mid M$, $d > 1$ jakavat polynomin $x^t - 1$ tai polynomin $B'(x)$. Toisaalta, koska $A \oplus B'$ on joukon $\mathbb{Z}_M$ laatoitus

$$A(x)B'(x) = 1 + x + x^2 + \cdots + x^{M-1} \mod x^M - 1$$

mikä on ekvivalentti sen kanssa, että

$$x^M - 1 \mid A(x)B'(x) - \frac{x^M - 1}{x - 1},$$

joka tarkoittaa, että kaikille M:sille ykkösenjuurille paitsi luvulle 1 pätee, että ne ovat joko polynomin $A(x)$ tai polynomin $B'(x)$ juuria. Yhtäpitävästi jokaiselle $d \mid M$, $d > 1$, vastaava syklotominen polynomi $\Phi_d(x)$ jakaa joko polynomin $A(x)$ tai polynomin $B'(x)$.

Nyt, jos t on joukon B' jakso, riittää todistaa, että kaikki syklotomiset polynomit $\Phi_d(x)$, siten, että $d \mid M$, $d > 1$, jotka jakavat polynomin $A(x)$ jakavat myös polynomin $x^t - 1$. Olkoot $\Phi_{s_1}(x), \ldots, \Phi_{s_k}(x)$ kaikki syklotomiset polynomit $\Phi_s(x)$ siten, että $s > 1$, $1 < s_1 < s_2 < \ldots < s_k$ ja $\Phi_{s_i}(x) \neq \Phi_{s_j}(x)$, jotka jakavat polynomin $A(x)$. Koska $\deg \Phi_s(x) = \phi(s)$, jossa $\phi(s)$ on Eulerin totientti funktio, nähdään, että

$$\phi(s_1) + \ldots + \phi(s_k) \leq \deg A(x) \leq n.$$

Toisaalta on todistettu, että kaikille $n \geq n_0$ pätee

$$\phi(n) \geq c_3 \frac{n}{\ln \ln n},$$

jossa $c_3 = e^{-\gamma} - \varepsilon$ ja n_0 on luvusta $\varepsilon > 0$ käänteisesti riippuva vakio. Nyt

$$\begin{aligned} \phi(n) &\geq c_3 \frac{n}{\ln \ln n} \\ \phi(n) \ln \ln n &\geq c_3 n \\ \ln(\phi(n) \ln \ln n) &\geq \ln(c_3 n) \\ \ln \phi(n) + \ln \ln \ln n &\geq \ln c_3 + \ln n. \end{aligned}$$

Nyt jos valitaan sopiva vakio n_1 siten, että $n_0 < n_1 < n$ saadaan

$$\ln \phi(n) \leq \ln n \leq 2 \ln \phi(n).$$

Nyt saadaan

$$\begin{aligned}
\sum_{i=1}^{k} s_i = &\sum_{s_i \leq n_1} s_i + \sum_{s_i > n_1} s_i \\
\leq &n_1^2 + \sum_{s_i > n_1} (e^{-\gamma} + \varepsilon)\phi(s_i) \ln \ln s_i \\
\leq &n_1^2 + (e^{-\gamma} + \varepsilon) n \ln \ln s_k \\
\leq &n_1^2 + (e^{-\gamma} + \varepsilon) n (\ln 2 + \ln \ln n) \\
\leq &(e^{-\gamma} + 2\varepsilon) n \ln \ln n,
\end{aligned}$$

kaikille $n_2 < n$, jossa n_2 on positiivinen vakio. Nyt koska kaikki s_i ovat eri lukuja pätee

$$(e^{-\gamma} + 2\varepsilon) n \ln \ln n \geq \sum_{i=1}^{k} s_i.$$

Nyt, määritellään vakio $c_4 = \sqrt{2e^{-\gamma} + 4\varepsilon}$, saadaan helposti

$$k \leq \sqrt{(2e^{-\gamma} + 4\varepsilon) n \ln \ln n} = c_4 \sqrt{n \ln \ln n},$$

josta seuraa, että kaikille $n > n_3$ pätee

$$\begin{aligned}
\prod_{i=1}^{k} s_i \leq \left(\sum_{i=1}^{k} s_i \right)^k \leq &((e^{-\gamma} + 2\varepsilon) n \ln \ln n)^k \\
\leq &((e^{-\gamma} + 2\varepsilon) n \ln \ln n)^{c_4 \sqrt{n \ln \ln n}} \\
= &e^{c_4 \sqrt{n \ln \ln n} \ln((e^{-\gamma} + 2\varepsilon) n \ln \ln n)} \\
\leq &e^{c_4 \sqrt{n \ln \ln n} 2 \ln n}.
\end{aligned}$$

Nyt voidaan yksinkertaisesti määritellä, että jakso $t = \prod_{i=1}^{k} s_i$ siten, että kaikki syklotomiset polynomit, jotka jakavat polynomin $A(x)$ ovat myös polynomin $x^t - 1$ jakajia. Koska jaksonpituus on ylhäältä rajattu niin olemme itse asiassa todistaneet, että $x^M - 1 | (x^t - 1) B'(x)$, eli t on joukon B' jakso, vain jos $t < M$. Koska B' on kuitenkin ei-jaksollinen niin on oltava, että

$$M \leq c_1 e^{c_2 \sqrt{n} \ln n \sqrt{\ln \ln n}},$$

kuten haluttiinkin, jossa $c_2 = 2c_4$ ja $c_1 > 1$ on niin pieni, että lause pätee kaikille n. □

John Steinberger on jo vuonna 2004 todistanut, että Ruzsan yläraja on paras mahdollinen yläraja, jos kokonaislukujen laatoitukset laajennetaan koskemaan myös sellaisia yksiulotteisia laatoituksia, joissa on useampia rivejä kokonaislukuja, niin kutsuttuja monijoukkoja (*eng.* multiset). Tämä pätee kuitenkin vain monijoukkojen laatoituksille, jotka ovat hajoavia (*eng.* decomposable) ja joissa on hyvin suuri määrä rivejä.[19, 20]

4.4 Birón yläraja

Matemaatikko András Birón yläraja perustuu polynomien jaollisuuteen ja on tähän astisista ylärajoista paras. Kuten edellä todettiin, monijoukoilla voi olla pidempiä laatoituksia kuin Birón yläraja kertoo.

Vuonna 2005 julkaistussa tutkimuksessaan Biró kiittää Rob Tijdemania siitä, että tämä tutustutti hänet kokonaislukujen laatoitusongelmaan.[3] Seuraavassa esitetään Birón tuloksen todistus hänen esitystään mukaillen. Todistus on pitkä, mutta koska se on tämänhetkisistä tuloksista paras, on sen sisällyttäminen perusteltua.

Lause 4.5. *Olkoon laatan A maksimipituus $n \geq n_0$ ja $\varepsilon > 0$ n_0:sta riippuva positiivinen vakio. Tällöin*

$$\mathcal{D}(n) \leq e^{n^{\frac{1}{3}+\varepsilon}}$$

kaikille tarpeeksi suurille n.

Tämän todistamiseksi Biró tarvitsi joukon lemmoja ja käytti hyväksi äärellisten kuntien teoriaa.

Lemma 4.6. *Olkoon $p(x) \not\equiv 0$ kompleksiarvoinen polynomi, jonka aste on n ja jolle pätee $x^d - 1 \mid p(x)$. Olkoon $p^*(x) = \frac{p(x)}{x^d-1}$. Tällöin*

$$\|p^*(x)\| \leq n\|p(x)\|,$$

jossa $\|p(x)\|$ tarkoittaa polynomin vakiokertoimien absoluuttisten arvojen summaa.

Todistus. Merkitään

$$p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$
$$p^*(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{n-d}x^{n-d}.$$

Tarkastelemalla polynomien jakoalgoritmia nähdään suoraan, että

$$-b_j = \sum_{t=0}^{\lfloor j/d \rfloor} a_{j-td}.$$

Tässä summa laskee siis yhteen vakiokertoimet $a_j, a_{j-d}, \ldots, a_{j \mod d}$. Nyt nähdään, että kaikille $j \in \{0, 1, \ldots, n-d\}$ pätee

$$|b_j| = \Big| \sum_{t=0}^{\lfloor j/d \rfloor} a_{j-td} \Big| \leq \sum_{t=0}^{\lfloor j/d \rfloor} |a_{j-td}| \leq \sum_{t=0}^{n} |a_t| = \|p(x)\|,$$

jolloin

$$\|p^*(x)\| = \sum_{j=0}^{n} |b_j| \leq \sum_{j=0}^{n} \|p(x)\| = n\|p(x)\|.$$

□

Birón seuraavan lemman todistus käyttää kuuluisaa Möbiuksen funktiota $\mu(n)$, joka riippuu luvun n alkulukutekijöistä ja niiden määrästä. Tarvitaan lisäksi syklotomisen polynomin määritelmä.

Määritelmä 4.7. Olkoon *Möbiuksen funktio* $\mu : \mathbb{N} \to \{-1, 0, 1\}$, primitiivisten ykköstenjuurien summa, joka voidaan myös kirjoittaa muodossa

$$\mu(n) = \begin{cases} 0 & \text{jos luku ei ole neliö-vapaa} \\ -1 & \text{jos luvulla on pariton määrä alkulukutekijöitä, ja on neliö-vapaa} \\ 1 & \text{jos luvulla on parillinen määrä alkulukutekijöitä, ja on neliö-vapaa} \end{cases}$$

Esimerkki 4.8. $\mu(6) = \mu(2 \cdot 3) = 1$, $\mu(30) = \mu(2 \cdot 3 \cdot 5) = -1$ ja $\mu(18) = \mu(2 \cdot 3^2) = 0$.

Lemma 4.9. *Olkoon $\varepsilon > 0$ jonkin vakio ja olkoon $p(x) \not\equiv 0$ kompleksiarvoinen polynomi siten, että $\deg p(x) \leq n$, kun $n_0 \leq n$, jossa n_0 on vain vakiosta ε riippuva vakio. Jos m on positiivinen kokonaisluku siten, että $p^*(x) = \frac{p(x)}{\Phi_m(x)}$ ja $\Phi_m(x) \mid p(x)$, niin*

$$\|p^*(x)\| \leq e^{n^{\varepsilon}} \|p(x)\|.$$

Todistus. Syklotominen polynomi $\Phi_m(x)$ voidaan ilmaista muodossa

$$\begin{aligned} \Phi_m(x) &= \prod_{d \mid m} (x^d - 1)^{\mu(\frac{m}{d})} \\ &= \Big(\prod_{d \mid m, \mu(\frac{m}{d}) = 1} (x^d - 1) \Big) \Big(\prod_{d \mid m, \mu(\frac{m}{d}) = -1} (x^d - 1)^{-1} \Big) \\ &= \frac{\prod_{d \mid m, \mu(\frac{m}{d}) = 1} (x^d - 1)}{\prod_{d \mid m, \mu(\frac{m}{d}) = -1} (x^d - 1)} \\ &= \frac{\Phi_m^*(x)}{\Phi_m^{**}(x)}. \end{aligned}$$

Tällöin voidaan myös polynomi $p^*(x)$ kirjoittaa uudelleen muotoon

$$p^*(x) = \frac{p(x)}{\Phi_m(x)} = \frac{p(x)\Phi_m^{**}(x)}{\Phi_m^*(x)}.$$

Toisin sanoen $p(x)\Phi_m^{**}(x)$ on jaollinen polynomilla $\Phi_m^*(x)$. Olkoon funktio $\tau : \mathbb{N} \to \mathbb{N}$ kaikkien luvun $r \in \mathbb{N}$ jakajien lukumäärä. Lisäksi nähdään helposti, että

$$\deg \Phi_m^{**}(x) \leq \deg \prod_{d \mid m} (x^d - 1) \leq m\tau(m)$$

ja

$$\|\Phi_m^{**}(x)\| \leq \Big\| \prod_{d \mid m} (x^d - 1) \Big\| \leq \Big\| \sum_{i=0}^{\tau(m)} \binom{\tau(m)}{i} \Big\| \leq 2^{\tau(m)}.$$

Tällöin saadaan soveltamalla toistuvasti lemmaa 4.6

$$p^*(x) \leq (\|p(x)\|2^{\tau(m)})(n + m\tau(m))^{\tau(m)}$$

Kun lisäksi $\Phi_m(x)|p(x)$ niin luvun m ykköstenjuurten lukumäärä $\phi(m) \leq n$. Lisäksi tunnetusti $r^{1-\varepsilon} < \phi(r)$ sekä $\tau(r) < r^{\varepsilon}$ tarpeeksi suurille r, joten tämä todistaa lemman. □

Tarvitaan vielä seuraava lemma

Lemma 4.10. *Olkoon $\varepsilon > 0$ vakio ja K jonkin sellainen reaaliluku, että $K \geq K_0$, jossa K_0 on jokin tarpeeksi suuri vain vakiosta ε riippuva luku. Olkoon $C = 10^5 \log K$. Tällöin*

$$\sum_{1 \leq r \leq K} C^{\omega(r)} \leq K^{1+\varepsilon},$$

missä $\omega(r)$ on luvun r jakavien alkulukujen lukumäärä.

Todistus. Olkoon funktio

$$f(r) = \prod_{p|r, p>P} e^{\lambda},$$

jossa p kuuluu alkulukuihin ja parametrit λ ja P määritellään tarkemmin myöhemmin. Erityisesti jos p' on alkuluku

$$\begin{aligned} f(p') &= \begin{cases} \prod_{p|p', p>P} e^{\lambda} & \text{, kun } p' > P \\ \prod_{p|p', p>P} e^{\lambda} & \text{, kun } p' < P \end{cases} \\ &= \begin{cases} e^{\lambda} & \text{, kun } p' > P \\ 0 & \text{, kun } p' < P \end{cases} \end{aligned}$$

Tällöin

$$C^{\omega(r)} \leq e^{\lambda\pi(P)}(Ce^{-\lambda})^{\omega(r)} f(r)$$

kaikille $r \geq 1$, jossa π on alkulukujen kertymäfunktio. Koska jokaisella luvulla on yksikäsitteinen alkulukuhajotelma, on selvää että kaikilla $m, n \geq 1$ pätee

$$f(m)f(n) = \prod_{p|m, p>P} e^{\lambda} \prod_{p|n, p>P} e^{\lambda} \geq \prod_{p|mn, p>P} e^{\lambda} = f(mn)$$

joten voidaan lausua

$$\frac{1}{K} \sum_{1 \leq r \leq K} f(r) \leq \sum_{1 \leq r \leq K} \frac{f(r)}{r} \leq \prod_{p \leq K} \left(1 - \frac{f(p)}{p}\right)^{-1} \leq e^{2\sum_{p \leq K} \frac{f(p)}{p}}$$

joka pätee kun $\frac{f(p)}{p} \leq \frac{1}{2}$ kaikilla p, joka taas pätee kun $e^{\lambda} \leq \frac{P}{2}$. Nyt saadaan kaikille tarpeeksi suurille K, että

$$\sum_{p\le K}\frac{1}{p}\le 2\ln\ln K \text{ ja } \omega(r)\le 2\frac{\ln K}{\ln\ln K} \text{ kaikille } 1\le r\le K,$$

jolloin

$$\sum_{1\le r\le K} C^{\omega(r)}\le K(Ce^{-\lambda})^{2\frac{\ln K}{\ln\ln K}}e^{\lambda P+4e^{\lambda}\ln\ln K},$$

kaikille tarpeeksi suurille luvun K arvoille, jos $e^{\lambda}\le\frac{P}{2}$ ja $e^{\lambda}\le C$. Tehdään valinta $P=2e^{\lambda}$ ja $\lambda=\ln\ln K-2\ln\ln\ln K$, jolloin tulos seuraa. □

Lemma 4.11. *Olkoon $P\not\equiv 0$ sellainen n-asteinen polynomi, että jokainen sen kerroin on 0 tai 1. Olkoon $n\ge n_0$, jossa n_0 on jokin tarpeeksi suuri luku. Olkoon $d\in\mathbb{N}$. Tällöin, jos syklotominen polynomi $\Phi_d(x)^V|P(x)$, niin $V\le(100\ln n)^{\omega(d)}$.*

Todistus. Olkoon $d=d_1p^{\alpha}$, missä p on alkuluku, joka ei ole luvun d_1 tekijä, ja $\alpha\ge 1$. Kaikille kokonaisluvuille $U\ge 0$ saadaan

$$\Phi_d(x)^{V-U}|P^{(U)}(x),\ \|P^{(U)}\|\le n^U(n+1)\le n^{U+2},$$

missä $P^{(U)}$ on polynomin P kertaluvun U derivaatta. Tällöin

$$\Big(\prod_{\xi\in U(d_1)}\Phi_d(\xi)\Big)^{V-U}\Big|N:=\prod_{\xi\in U(d_1)}P^{(U)}(\xi).$$

Jossa $U(d_1)$ on kertaluvun d_1 primitiivisten ykköstenjuurten joukko. Tiedetään, että $N\in\mathbb{Z}$ ja $|N|\le(n^{U+2})^{\phi(d_1)}$ ja toisaalta

$$\prod_{\xi\in U(d_1)}\Phi_d(\xi)=\prod_{\xi_1,\xi_2\in U(d_1)}\prod_{\eta\in U(p^{\alpha})}(\xi_1-\xi_2\eta).$$

Tässä oikea puoli on jaollinen luvulla $p^{\phi(d_1)}$. Itse asiassa, kun $\xi_1=\xi_2$ ja muistetaan, että

$$\prod_{\eta\in U(p^{\alpha})}(1-\eta)=\Phi_{p^{\alpha}}(1)=p$$

tämä on triviaalisti selvää. Tällöin

$$(p^{\phi(d_1)})^{V-U}|N \text{ ja } |N|\le(n^{U+2})^{\phi(d_1)}.$$

Jos lisäksi $N\neq 0$ saadaan

$$2^{V-U}\le p^{V-U}\le n^{U+2}=e^{(U+2)\ln n}.$$

Jos valitaan $V\ge 100\ln n$ ja $U\le\frac{V}{100\ln n}$ tämä on selvästi ristiriita suurille n, joten luvun N on oltava 0.

Olemme nyt todistaneet, että jos $n \geq n_0$, $\Phi_d(x)^V | P(x)$, $V \geq 100 \ln n$ ja $U \leq \frac{V}{100 \ln n}$ pätee $\Phi_{d_1}(x)^{U+1} | P(x)$. Nyt jos $d = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ on luvun d alkulukuhajotelma, voimme yksinkertaisesti soveltaa edellistä tulosta t kertaa. Tällöin seuraa, että jos $V > (100 \ln n)^t$, niin $P(1) = 0$, mikä on ristiriita oletusten kanssa.

Tämä todistaa väitteen. □

Lause 4.12. *Olkoon $\varepsilon > 0$ jokin vakio ja olkoon $0 \not\equiv q(x) \in \mathbb{Z}[x]$, jonka suurimman asteen termin kerroin on 1. Oletetaan, että on olemassa polynomi $Q(x) \not\equiv 0$ siten, että kaikki polynomin $Q(x)$ kertoimet ovat 0 tai 1 ja $q(x) | (1-x)Q(x)$.*

Merkitään luvulla n polynomin $(1-x)Q(x)$ astetta ja oletetaan, että $n \geq n_0$, jossa n_0 on vain luvusta ε riippuva kokonaisluku. Jos on olemassa positiivinen kokonaisluku k siten, että $q(x) | x^k - 1$, tällöin pienimmälle tällaiselle k pätee

$$\ln k \leq n^{\frac{1}{3}+\varepsilon}.$$

Todistus. Birón mukaan: Jos $q(x) | x^k - 1$ jollekin k niin $q(x) = \prod_{d \in D} \Phi_d(x)$ jollekin joukolle D. Määritellään, että luku $k = \text{pyj}\{d : d \in D\}$. Arvioidaan nyt luvun k kokoa. Muistetaan, että

$$\deg q = \sum_{d \in D} \phi(d) \leq n$$

ja olkoot $n^{\frac{1}{3}} < M < \frac{1}{2} n^{\frac{1}{2}}$ ja $L > 2n^{\frac{1}{2}}$ parametreja, joiden arvot määritellään myöhemmin tarkemmin. Nyt saadaan neljä tapausta

1. Jos p on alkuluku, $\alpha \geq 1$, $p^\alpha \| k$ ja $p^\alpha \geq L$ ja $p^\alpha | d$ jollekin $d \in D$. Ei voi olla kahta alkuluvun potenssia $p_1^{\alpha_1}$ ja $p_2^{\alpha_2}$, jotka jakavat luvun $d \in D$, koska silloin

   $$\phi(d) \geq \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \geq \left(\frac{1}{2} p_1^{\alpha_1}\right) \left(\frac{1}{2} p_2^{\alpha_2}\right)$$

   ja, koska $p^\alpha \geq L$ ja $L > 2n^{\frac{1}{2}}$

   $$\left(\frac{1}{2} p_1^{\alpha_1}\right) \left(\frac{1}{2} p_2^{\alpha_2}\right) \geq \left(\frac{1}{2} L\right) \left(\frac{1}{2} L\right) \geq \left(\frac{1}{2} 2n^{\frac{1}{2}}\right) \left(\frac{1}{2} 2n^{\frac{1}{2}}\right) = n,$$

   mikä on ristiriita sen kanssa, että $\deg q = \sum_{d \in D} \phi(d) \leq n$. Täten jokainen alkuluvun potenssi jakaa eri luvun $d \in D$ ja jos $p^\alpha | d$ niin $\phi(d) \geq \phi(p^\alpha)$. Tällöin

   $$\frac{1}{2} \sum_{p^\alpha \| k, p^\alpha \leq L} L \geq \frac{1}{2} \sum_{p^\alpha \| k, p^\alpha \geq L} p^\alpha \leq \sum_{p^\alpha \| k, p^\alpha \geq L} \phi(p^\alpha) \leq \sum_{d \in D} \phi(d) \leq n.$$

   Tämä kertoo, että jokaiselle p^α pätee $p^\alpha \leq 2n$ ja sellaisia alkulukujen potensseja on enintään $\frac{2n}{L}$, jolloin

   $$\prod_{p^\alpha \| k, p^\alpha \geq L} p^\alpha \leq (2n)^{\frac{2n}{L}}.$$

2. Jos sen sijaan $p^\alpha \leq M$ niin selvästi

$$\prod_{p^\alpha \| k, p^\alpha \leq M} p^\alpha \leq \prod_{p^\alpha \leq M} p^\alpha \leq e^{c_1 M},$$

jossa c_1 on vakio.

3. Jos sen sijaan $M < p^\alpha < L$ ja lisäksi $\alpha \geq 2$, nähdään, että

$$\prod_{p^\alpha \| k, M < p^\alpha < L, \alpha \geq 2} p^\alpha \leq \prod_{p^\alpha < L, \alpha \geq 2} p^\alpha \leq e^{c_2 \sqrt{L}}$$

4. Jos taas $M < p^\alpha < L$ ja lisäksi $\alpha = 2$ on yksinkertaisesti kyseessä tapaus

$$\prod_{p^\alpha \| k, M < p^\alpha < L, \alpha = 1} p^\alpha = \prod_{p \| k, M < p < L} p.$$

Kuvitellaan ensin, että on kolme alkulukua p_1, p_2 ja p_3, jotka jakavat luvun $d \in D$ niin

$$\phi(d) \geq (p_1 - 1)(p_2 - 1)(p_3 - 1) \geq M^3 > \left(n^{\frac{1}{3}}\right)^3 = n,$$

koska $n^{\frac{1}{3}} < M$, mikä on ristiriita. Siis on korkeintaan kaksi alkulukua, jotka jakavat kunkin luvun $d \in D$ ja lisäksi $\phi(d) \geq (p_1 - 1)(p_2 - 1) \geq M^2$. Tästä seuraa, että

$$n \geq \sum_{d \in D} \phi(d) \geq \sum_{d \in D} M^2 = M^2 \sum_{d \in D} = M^2 |D| \Leftrightarrow |D| \leq \frac{n}{M^2}.$$

Tästä seuraa, että sellaisia alkulukuja p, jotka jakavat jonkin joukon D alkion d, mutta samalla jokin toinen alkuluku p' jakaa alkion d on korkeintaan $\frac{2n}{M^2}$. Tämä raja saavutetaan, jos jokaisella $\frac{n}{M^2}$ alkuluvulla on pari. Voidaankin sanoa, että

$$\prod_{p \| k, M < p < L} p \leq L^{\frac{2n}{M^2}} \prod_{p \in P} p,$$

jossa $P \subseteq \{p \| k : M < p < L\}$ on joukko, jonka alkioista korkeintaan yksi jakaa kunkin joukon D alkion d. Tällöin jokaiselle $p_i \in P$ on olemassa $d_{p_i} \in D$, siten, että jos $p_i \neq p_j$ niin $d_{p_i} \neq d_{p_j}$ ja lisäksi

$$n \geq \sum_{d \in D} \phi(d) \geq \sum_{p \in P} \phi(d_p).$$

Koska $p \| k$ kaikille $p \in P$, tiedetään, että $\text{syt}(p, \frac{d_p}{p}) = 1$. Tällöin

$$\phi(d_p) = \phi(p)\phi\left(\frac{d_p}{p}\right) = (p-1)\phi\left(\frac{d_p}{p}\right) \geq c_3(\varepsilon_1) M \left(\frac{d_p}{p}\right)^{1-\varepsilon_1},$$

missä ε_1 on vakio ja luku $c_3(\varepsilon_1)$ riippuu vain vakiosta ε_1. Olkoon lisäksi luku $K \geq K_0$, jossa K_0 on vain vakiosta ε_1 riippuva suuri luku. Jos $p \in P$ ja $\frac{d_p}{p} \geq K$, niin selvästi

$$\phi(d_p) \geq c_3(\varepsilon_1) M \left(\frac{d_p}{p}\right)^{1-\varepsilon_1} \geq c_3(\varepsilon_1) M K^{1-\varepsilon_1}.$$

Määritellään uusi joukko $P' = \{p : 1 \leq \frac{d_p}{p} < K, p \in P\} \subseteq P$. Tällöin voidaan nyt kirjoittaa

$$\prod_{p\in P} p \leq \Big(\prod_{p\in P'} p\Big) L^{\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}}.$$

Jaetaan joukko P' osajoukkoihin $P_r = \{p \in P' : d_p = rp\}$, jolloin $P' = \bigcup_{1\leq r<K} P_r$. Olkoon $V_r \geq 0$ suurin kokonaisluku, jolle pätee $\Phi_r(x)^{V_r} \mid Q(x)(1-x)$ ja olkoon

$$Q^*(x) = \frac{Q(x)(1-x)}{\Phi_r(x)^{V_r}}.$$

Nyt $Q^*(\xi) \neq 0$ kaikille $\xi \in U(r)$ ja lemman 4.9 mukaan $\|Q^*\| \leq 2ne^{V_r n^{\varepsilon_1}}$. Jos nyt määritellään

$$\nu := \prod_{\xi\in U(r)} Q^*(\xi)$$

saadaan $\nu \in \mathbb{Z}$, $\nu \neq 0$ ja $|\nu| \leq \|Q^*\|^{\phi(r)}$. Nyt joukon P_r määritelmän nojalla saadaan lisäksi, että $q(x) \mid Q(x)(1-x)$ ja

$$\prod_{p\in P_r} \Phi_{pr}(x) \;\Big|\; q(x) \quad \text{ja} \quad \operatorname{syt}\Big(\Phi_r(x), \prod_{p\in P_r} \Phi_{pr}(x)\Big) = 1.$$

Nyt polynomin Q^* määritelmän nojalla seuraa, että

$$\prod_{p\in P_r} \Phi_{pr}(x) \;\Big|\; Q^*(x),$$

jolloin luvun ν määritelmän mukaan

$$\prod_{p\in P_r} \Big(\prod_{\xi\in U(r)} \Phi_{pr}(\xi)\Big) \;\Big|\; \nu.$$

Selvästi $\operatorname{syt}(p, r) = 1$ kaikille $p \in P_r$, koska $p \| k$ kaikille p. Täten kaikille $p \in P_r$ pätee

$$\prod_{\xi\in U(r)} \Phi_{pr}(\xi) = \prod_{\xi_1,\xi_2\in U(r)} \prod_{\eta\in U(r)} (\xi_1 - \xi_2\eta),$$

jossa oikea puoli on selvästi jaollinen luvulla $p^{\phi(r)}$, joten niin on vasenkin. Koska tämä pätee kaikille $p \in P_r$, nähdään, että

$$\prod_{p\in P_r} \Big(\prod_{\xi\in U(r)} \Phi_{pr}(\xi)\Big) \;\Big|\; \nu \;\Rightarrow\; \prod_{p\in P_r} p^{\phi(r)} \;\Big|\; \nu.$$

Nyt voidaan kootusti lausua

$$\prod_{p\in P_r} p \leq \|Q^*\| \leq 2ne^{V_r n^{\varepsilon_1}}$$

ja koska $p \geq 2$ niin tarpeeksi suurille n pätee

$$|P_r| \leq c_5(V_r+1)n^{\varepsilon_1}.$$

Tosin sanoen

$$\begin{aligned}
\prod_{p^\alpha \| k, M<p^\alpha<L, \alpha=1} p^\alpha = & \prod_{p\|k, M<p<L} p \\
\leq & L^{\frac{2n}{M^2}} \prod_{p\in P} p \\
\leq & L^{\frac{2n}{M^2}+\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}} \Big(\prod_{p\in P'} p \Big) \\
\leq & L^{\frac{2n}{M^2}+\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}} \prod_{1\leq r<K} \Big(\prod_{p\in P_r} p \Big) \\
\leq & L^{\frac{2n}{M^2}+\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}} \prod_{1\leq r<K} \Big(\prod_{p\in P_r} L \Big) \\
= & L^{\frac{2n}{M^2}+\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}} \prod_{1\leq r<K} L^{|P_r|} \\
\leq & L^{\frac{2n}{M^2}+\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}} \prod_{1\leq r<K} L^{c_5(V_r+1)n^{\varepsilon_1}} \\
\leq & L^{\frac{2n}{M^2}+\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}} L^{\sum_{1\leq r<K} c_5(V_r+1)n^{\varepsilon_1}} \\
\leq & L^{\frac{2n}{M^2}+\frac{c_4(\varepsilon_1)n}{MK^{1-\varepsilon_1}}+c_5 n^{\varepsilon_1}\sum_{1\leq r<K}(V_r+1)}.
\end{aligned}$$

Nyt tapauksien 1.-4. perusteella voidaan kootusti sanoa

$$\begin{aligned}
\ln k \leq & \frac{2n}{L}\ln(2n) + c_1 M + c_2\sqrt{L} \\
& + c_6(\varepsilon_1)\ln(L)(Kn)^{\varepsilon_1}\Big(\frac{n}{M^2}+\frac{n}{MK}+\sum_{1\leq r<K}(V_r+1)\Big).
\end{aligned}$$

Jos valitaan $L = n^{\frac{2}{3}}$ niin $c_2\sqrt{L} = c_2 n^{\frac{1}{3}}$. Lemman 4.11 mukaan suurille luvun n arvoilla pätee $V_r + 1 \leq (200\ln n)^{\omega(r)}$. Jos lisäksi tehdään oletus $K \geq n^{\frac{1}{100}}$ ja käytetään lemmaa 4.10 saadaan

$$\ln k \leq c_7(\varepsilon_1)(Kn)^{2\varepsilon_1}\Big(n^{\frac{1}{3}}+M+\frac{n}{M^2}+\frac{n}{MK}+K\Big).$$

Jos valitaan, että $K = n^{\frac{1}{3}}$, $M = 2n^{\frac{1}{3}}$ ja $L = n^{\frac{2}{3}}$ saadaan

$$\begin{aligned}
\ln k \leq & c_7(\varepsilon_1)(Kn)^{2\varepsilon_1}\Big(n^{\frac{1}{3}}+M+\frac{n}{M^2}+\frac{n}{MK}+K\Big) \\
= & c_7(\varepsilon_1)(n^{\frac{1}{3}}\cdot n)^{2\varepsilon_1}\Big(n^{\frac{1}{3}}+2n^{\frac{1}{3}}+\frac{n}{n^{\frac{2}{3}}}+\frac{n}{2n^{\frac{1}{3}}\cdot n^{\frac{1}{3}}}+n^{\frac{1}{3}}\Big) \\
= & c_7(\varepsilon_1)n^{\frac{8\varepsilon_1}{3}}\Big(\frac{11}{2}n^{\frac{1}{3}}\Big) \\
= & c_8(\varepsilon_1)n^{\frac{1}{3}+\frac{8\varepsilon_1}{3}}.
\end{aligned}$$

Jos tehdään valinta $\varepsilon = 10\varepsilon_1$ niin tarpeeksi suurille n pätee

$$\ln k = c_8(\varepsilon_1) n^{\frac{1}{3}+\frac{8\varepsilon_1}{3}} \leq n^{\frac{1}{3}+10\varepsilon_1} = n^{\frac{1}{3}+\varepsilon},$$

mikä todistaa väitteen. □

Tämän jälkeen Biró voi viimeinkin todistaa lauseen, jota olemme etsineet. Lauseen 4.5 todistus kuuluu Birón mukaan:

Todistus. Voidaan yleisyyttä menettämättä olettaa, että laatan A pienin luku on 0 ja suurin luku on n. Määritellään seuraavat joukot

$$\begin{aligned} B^+ =& B \cap [0, \infty) \\ C =& \{n \in \mathbb{Z} : n \geq 0, n = a + b, a \in A, b \in B, b < 0\} \end{aligned}$$

sekä polynomit

$$\begin{aligned} f(x) &= \sum_{a \in A} x^a \\ g(x) &= \sum_{b \in B^+} x^b \\ h(x) &= \sum_{c \in C} x^c. \end{aligned}$$

Koska $A \oplus B = \mathbb{Z}$ on laatoitus seuraa

$$f(x)g(x) + h(x) = \sum_{i \in \mathbb{Z}} x^i = \frac{1}{1-x}.$$

Tällöin nähdään, että

$$g(x) = \frac{1 - (1-x)h(x)}{(1-x)f(x)} = \frac{p(x)}{q(x)},$$

missä polynomeilla $p(x)$ ja $q(x)$ ei ole yhteisiä tekijöitä joukosta $\mathbb{Z}[x]$. Erityisesti, polynomin $q(x)$ suurimman asteen termin kerroin on 1 ja $q(x)|(1-x)f(x)$.

Koska joukko B on aina jaksollinen, kuten Newman, Ruzsa ja Kolountzakis ovat osoittaneet, on olemassa sellainen k, että $g(x)(x^k - 1)$ on polynomi. Koska polynomeilla $p(x)$ ja $q(x)$ ei ole yhteisiä tekijöitä nähdään, että $q(x)|x^k - 1$.

Kun lisäksi polynomin $f(x)$ kertoimet ovat kaikki joko 0 tai 1, voidaan soveltaa lausetta 4.12. Koska $\deg f(x) = n$, on olemassa positiivinen kokonaisluku k siten, että

$$q(x)|x^k - 1, \text{ ja } \ln k \leq n^{\frac{1}{3}+\varepsilon}.$$

Riittää siis todistaa, että k on joukon B jaksonpituus. Kun tarkastellaan ääretöntä polynomia $g(x)$ ja äärellistä polynomia $g(x)(x^k - 1)$, voidaan nyt päätellä,

että k on jokin joukon B jaksonpituus. Nyt siis

$$\begin{aligned} \ln k &\leq n^{\frac{1}{3}+\varepsilon} \\ k &\leq e^{n^{\frac{1}{3}+\varepsilon}} \\ \Rightarrow \mathcal{D}(n) &\leq e^{n^{\frac{1}{3}+\varepsilon}}. \end{aligned}$$

□

5 Jakson maksimipituuden alarajat

Hyvin pitkään ainoa tunnettu alaraja oli tunnettu laattaa $\{0, n\}$ käyttäen saatu laatoitus, jonka jaksonpituus on $2n$. Vuonna 2002 Kolountzakis esittikin [13] tuon ajan tietämyksen muodossa:

Lemma 5.1. *Olkoon n laatan pituus. Tällöin*

$$2n \leq D(n) \leq 2^n$$

kaikilla $n \in \mathbb{N}$.

Tämä lemma johtuu lauseista 5.3 ja 4.1 ja onkin mielenkiintoinen nykyään lähinnä siksi, että se pätee kaikille laattojen pituuksille, ei vain hyvin pitkille laatoille.

Poiketen jaksonpituuden ylärajan tutkimusperinteestä alarajaa nostavat tutkimukset ovat poikkeuksetta esimerkkipohjaisia. Kukin tutkija pohjaa uuteen, joskus vanhaan perustuvaan, konstruktioon joka todistaa uuden pitkäjaksoisen laatoituksen olemassaolon. Usein helpoin tapa löytää tällainen laatoitus on samaistamalla ryhmäisomorfismilla n-ulotteisen avaruuden epäjaksoinen laatoitus kokonaislukuihin. Seuraavassa esitellään alarajaa koskevia tuloksia, jotka parantavat ylärajaa huomattavasti. Nykyajan tietämyksen voikin tiivistää lemmaan:

Lemma 5.2. *Olkoon laatan A maksimipituus $n \geq n_0$ ja $\varepsilon > 0$ luvusta n_0 riippuva positiivinen vakio. Tällöin*

$$e^{\frac{\ln(n)^2}{4 \ln \ln n}} \leq \mathcal{D}(n) \leq e^{n^{\frac{1}{3}+\varepsilon}}$$

kaikille tarpeeksi suurille $n \in \mathbb{N}$.

5.1 Välien alaraja

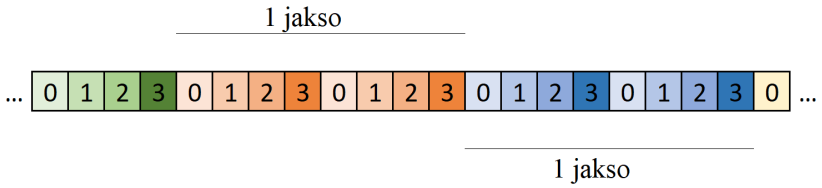
Yksinkertaisin mahdollinen alaraja jakson maksimipituudelle on $2n$, jota tässä kutsun välien alarajaksi, sillä sille ei kirjallisuudessa ole selkeää omaa nimeä. Pitkään oli avoin kysymys onko tätä pidempijaksoisia laatoituksia edes olemassa[4], mutta Mihail Kolountzakis todisti 2000-luvun alussa, että sellaisia laatoituksia todella voidaan konstruoida.[13] Välien alaraja on jossain määrin triviaali alaraja, joka pätee laattojen pituudesta riippumatta.

Lause 5.3. *Olkoon laatan A maksimipituus $n \in \mathbb{N}$. Tällöin pätee*

$$2n \leq D(n)$$

kaikille n.

Todistus. Olkoon laatta $A = \{j\} \oplus \{0, n\}$, jossa $j, n \in \mathbb{N}$. Tällöin $\operatorname{diam}(A) = n$. Nyt ja valitaan laattojen paikkoja kuvaavaksi joukoksi $T = \{0, 1, \ldots, n-1\} \oplus 2n\mathbb{Z}$ saadaan



Kuva 2: Laatoitus laatalla $\{0, 4\}$. Kuvassa yksittäiset jaksot ja laatat on korostettu käyttämällä numeroita ja värejä. Kokonaista jaksoa vastaa tietty väri, ja sen muodostavat laatat on väritetty eri sävyillä ja niihin on lisätty laatan numero.

$$\begin{aligned} A \oplus T &= \{j\} \oplus \{0, n\} \oplus \{0, 1, \ldots, n-1\} \oplus 2n\mathbb{Z} \\ &= \{j\} \oplus \{0, 1, \ldots, n-1, n, n+1, \ldots, 2n-1\} \oplus 2n\mathbb{Z} \\ &= \{j\} \oplus \mathbb{Z} \\ &= \mathbb{Z}. \end{aligned}$$

Koska $A \oplus T = \mathbb{Z}$ määritelmän mukaan A laatoittaa kokonaisluvut jaksolla $2n$, mikä todistaa väitteen. Kuva 2 selventää laatoituksen muotoa.

□

5.2 Kolountzakiksen alaraja

Vihdoin vuonna 2003 kreikkalaismatemaatikko Mihail N. Kolountzakis paransi alarajaa konstruoimalla neliöjaksoisen laatoituksen. Toisin sanoen, laatoituksen, jonka jaksonpituus on cn^2, kun laatan pituus on n.

Lause 5.4. *On olemassa sellainen $c > 0$, että kaikille $n > 1$ pätee*

$$cn^2 \leq \mathcal{D}(n)$$

Seuraavassa esitetään Kolountzakiksen todistus lauseelle.

Todistus. Lemman 3.11 nojalla riittää konstruoida kaikille $n \geq n_1$ sellainen joukko $A \subseteq \{0, \ldots, n\}$ ja ei-jaksollinen joukko $B \subseteq \mathbb{Z}_M$ siten, että $A \oplus B = \mathbb{Z}$ on laatoitus ja $M \geq c_6 n^2$, jossa $c_6 > 0$ on vakio joka määritellään tarkemmin myöhemmin. Vakioksi c valitaan niin pieni luku, että $cn^2 \leq \mathcal{D}(n)$ myös kun $n \leq n_1$.

Olkoon $n_1 = 10000$. Jos valitaan $m = \frac{n}{200}$, nähdään selvästi, että $[\frac{n}{200}, \frac{n}{50}] = [m, 2m] \cup [2m, 4m]$, jolloin Tšebyšovin lauseen mukaan välillä on ainakin kaksi

alkulukua.[2] Voidaan siis valita alkuluvut p ja q siten, että $p, q \in [\frac{n}{200}, \frac{n}{50}]$. Olkoon $M = 2 \cdot 3 \cdot 5 \cdot p \cdot q$, jolloin

$$M = 2 \cdot 3 \cdot 5 \cdot p \cdot q \geq 30 \left(\frac{n}{200}\right)^2 = \frac{30}{200^2} n^2.$$

Tehdään siis valinta $c_6 = \frac{30}{200^2}$.

Ryhmä $\mathbb{Z}_M$ on isomorfinen ryhmän $\mathbb{Z}_{3p} \times \mathbb{Z}_{5q} \times \mathbb{Z}_2$, joka voidaan visualisoida särmiönä Q, jossa x-akselin suuntainen pituus on $\mathbb{Z}_{3p}$, y-akselin suuntaien pituus on $\mathbb{Z}_{5q}$ ja z-akselin suuntainen pituus on $\mathbb{Z}_2$. Kolmiulotteinen avaruus voidaan helposti täyttää tällaisilla särmiöillä.

Olkoon suorakulmio $A = \{(i, j, 0) : 0 \leq i < 3, 0 \leq j < 5\}$. Käyttäen tätä suorakulmiota voimme täyttää joukon Q ei-jaksollisesti:

1. Laatoitetaan ensin jaksollisesti.
2. Siirrä tasossa jotakin riviä vektorin $(1, 0, 0)$ mukaisesti.
3. Siirrä seuraavassa tasossa jotain riviä vektorin $(0, 1, 0)$ mukaisesti.

Näin on siis selvää, että $B = L \cup U$, jossa $L = \{(i, j, 0)\}$ siten, että j saa kaikki arvot $< 5 > \subseteq \mathbb{Z}_{5q}$ ja i saa kaikki arvot $< 3 > \subseteq \mathbb{Z}_{3p}$, paitsi kun $j = 5$, jolloin i saa arvot $< 3 > +1 \subseteq \mathbb{Z}_{3p}$. Samoin $U = \{(i, j, 1)\}$ on joukko, jossa i saa kaikki arvot $< 3 > \subseteq \mathbb{Z}_{3p}$ ja j saa kaikki arvot $< 5 > \subseteq \mathbb{Z}_{5q}$, paitsi kun $i = 3$, jolloin j saa kaikki arvot $< 5 > +1 \subseteq \mathbb{Z}_{5q}$. Toisin sanoen:

$$L = \{(i, j, 0) : (3k, 0, 0), (3k + 1, 5, 0) \text{ ja } (3k, 5l, 0), \text{ jossa } 0 \leq k < p, 2 \leq l < q\}$$

ja

$$U = \{(i, j, 1) : (0, 5l, 1), (3, 5l + 1, 1), (3k, 5l, 1), \text{ jossa } 2 \leq k < p, 0 \leq l < q\}.$$

On triviaalisti selvää, että B is ole jaksollinen joukko. Muodostetaan nyt ryhmäisomorfismi $\psi : Q \to \mathbb{Z}_M$ ja määritellään joukot $X = \psi(A)$ ja $Y = \psi(B)$. Koska kyseessä on ryhmäisomorfismi, jotka eivät muuta jaksollisuutta, on selvää, että $X \oplus Y = \mathbb{Z}_M$ on laatoitus ja että Y ei ole jaksollinen joukko joukossa $\mathbb{Z}_M$. Nyt on enää laskettava joukon X pituus. Määritellään ryhmäisomorfismi ψ seuraavasti

$$\psi(i, j, k) = i(2 \cdot 5q) + j(2 \cdot 3) + k(3p5q) \bmod M,$$

jossa $i \in \{0, \ldots, 3p - 1\}$ $j \in \{0, \ldots, 5q - 1\}$ ja $k \in \{0, 1\}$. Tällöin saadaan joukko $X = \psi(A)$, joka on muotoa

$$\begin{aligned} X =& \psi(\{(i, j, 0) : 0 \leq i < 3, 0 \leq j < 5\}) \\ =& \{0, 10q, 20q, 6p, 12p, 18p, 24p, 10q + 6p, \ldots, 20q + 24p\}. \end{aligned}$$

[2] Tunnetaan myös nimellä Bertrandin postulaatti sen esittäjän Joseph Bertrandin mukaan. Lauseen mukaan kaikille $n > 1$ pätee, että välillä $[n, 2n]$ on ainakin yksi alkuluku. Bertrand esitti lauseen vuonna 1845 ja osoitti sen pitävän paikkansa, jos $\frac{n}{2} \leq 6000000$.[2] Pafnuti Tšebyšov todisti lauseen vuonna 1850[23]. Myöhemmin muutkin kuuluisat matemaatikot, kuten Srinivasa Ramanujan vuonna 1919[17] ja Paul Erdős vuonna 1932[9], ovat todistaneet lauseen eri tavoin.

Tämä tarkoittaa, että joukon läpimitta on $20q+24p \leq \frac{20n}{50} + \frac{24n}{50} = \frac{44}{50}n < n$. Kun samalla $\frac{30}{200^2}n^2 \leq M$, tämä todistaa väitteen. □

Joukon Y koko riippuu vakioiden p ja q valinnasta ja sen koko voidaan ilmaista muodossa $|Y| = 2pq$. Sen sijaan laatan X koko on vakio eli 15 alkiota.

Eräs todistuksesta huomattava seikka on, että vakio c on jossain määrin sattumanvarainen. Valinta tehdään vain siksi, että Kolountzakis haluaa lauseen pätevän kaikille kokonaisluvuille n. Olisi kuitenkin aivan mahdollista muotoilla lause kaikille kokonaislukua $n_1 = 10000$ suuremmille kokonaisluvuille.

Lemma 5.5. *Kaikille $n \geq 10000$ pätee*

$$\frac{30}{200^2}n^2 \leq \mathcal{D}(n)$$

Yhtä mielekästä olisi myös muotoilla lause myös tarpeeksi suurille n.

Lemma 5.6. *Kaikille $n \geq n'$ pätee*

$$n^2 \leq \mathcal{D}(n)$$

Kolountzakiksen konstruktiota mukailevalla k-ulotteisella Steinbergerin konstruktiolla saavutetaan lemman 5.6 mukainen laatoitus kun $n' = 335657$. Kolountzakiksen konstruktiolla tähän ei kuitenkaan vielä päästä.

5.3 Steinbergerin polynominen alaraja

John P. Steinberger julkaisi vuonna 2006 tutkimuksen, joka laajentaa Kolountzakiksen alarajaa n^k-pituisiin laatoituksiin asti.[21] Steinbergerin todistus on sinänsä ainutlaatuinen, että vaikka Steinberger haluaa nimenomaan todistaa, että tarpeeksi suurille n pätee $n^k \leq \mathcal{D}(n)$, hän ei muotoile sitä tutkimuksessaan lauseeksi. Poikkeamme tässä siis Steinbergerin tutkimuksessa sen verran, että toteamme lauseen spesifisesti.

Lause 5.7. *Olkoon A laatta ja $n = diam(A)$. Tällöin kaikille $n \geq n_1$ on olemassa sellainen laatoitus $A \oplus B = \mathbb{Z}$ että*

$$n^k \leq \mathcal{D}(n).$$

Karkeaksi arvioksi luvulle n_1 Steinberger ilmoittaa $n_1(k) \approx (k+1)^{k+1}K^k$, jossa K on kaikkien ensimmäisten $k+2$ alkuluvun tulo. Toisin sanoen $n_1(k)$ on erittäin nopeasti kasvava funktio. Steinberger kertoo löytäneensä lauseen toteuttavat laatoitukset siten, että $n_1(2) \leq 316673$ ja $n_1(3) \leq 783748556833$. Katso kuitenkin lukua 6.3, jossa esitän, että näissä arvioissa on virheitä ja oikeammin $n_1(2) \leq 335657$ ja $n_1(3) \leq 783749905213$.

Steinberger todistaa tutkimuksessaan lemman, joka on Kolountzakiksen käyttämän lemman 3.11 yleistys.

Lemma 5.8. *Olkoon $2 \leq k$ ja $A, B_1, \ldots, B_k \subseteq \mathbb{Z}_n$ joukkoja siten, että $B_i \neq B_j, A \oplus B_i = \mathbb{Z}_n$ kaikille $i \in \{1, \ldots, k\}$ ja jokaiselle alkuluvulle $p|n$ on jokin B_i, joka ei ole jaksollinen $\mod \frac{n}{p}$ joukossa $\mathbb{Z}_n$. Tällöin joukolla $p'A$ on laatoitus, jonka pienin jaksonpituus on $p'n$, jossa $p' \geq k$ on pienin alkuluku, joka ei jaa lukua n.*

Todistus. Näytetään ensin, että on olemassa joukko $B \subseteq \mathbb{Z}_{np'}$ siten, että $p'A \oplus B = \mathbb{Z}_{np'}$ ja B is ole jaksollinen $\mod \frac{p'n}{p}$ millekään alkuluvulle $p|p'n$.

Olkoon N pienin sellainen luvun n monikerta, että pätee $N \equiv 1 \mod p'$. Olkoon joukko B määritelty seuraavasti:

$$B = \left(\bigcup_{i=1}^{k} p'B_i + (i-1)N \right) \cup \left(\bigcup_{i=k}^{p'-1} p'B_k + iN \right) \mod p'n$$

Tässä jokainen osajoukko on erillinen, koska jokaisen osajoukon jäsenet ovat eri kongruenssiluokassa $\mod p'n$. Koska $p'A \oplus (p'B_i + c) = p'\mathbb{Z}_{p'n} + c$ ja joukot ovat erillisiä, on selvää, että

$$\begin{aligned}
p'A \oplus B &= p'A \oplus \left(\bigcup_{i=1}^{k} p'B_i + (i-1)N \right) \cup \left(\bigcup_{i=k}^{p'-1} p'B_k + iN \right) \\
&= \left(\bigcup_{i=1}^{k} p'A \oplus (p'B_i + (i-1)N) \right) \cup \left(\bigcup_{i=k}^{p'-1} p'A \oplus (p'B_k + iN) \right) \\
&= \left(\bigcup_{i=1}^{k} p'\mathbb{Z}_{p'n} + (i-1)N \right) \cup \left(\bigcup_{i=k}^{p'-1} p'\mathbb{Z}_{p'n} + iN \right) \\
&= \bigcup_{i=1}^{p'-1} p'\mathbb{Z}_{p'n} + iN \\
&= \mathbb{Z}_{p'n}.
\end{aligned}$$

On vielä tarkistettava, että B ei ole jaksollinen $\mod \frac{p'n}{p}$ joukossa $\mathbb{Z}_{p'n}$ kaikille alkuluvuille $p|p'n$. Jos $p' \neq p$ niin on olemassa jokin B_i siten, että se on ei-jaksollinen $\mod \frac{n}{p}$ joukossa $\mathbb{Z}_n$, joten $p'B_i$ on ei-jaksollinen $\mod \frac{p'n}{p}$ joukossa $\mathbb{Z}_{p'n}$.

Enää on tarkistettava, että B on ei-jaksollinen $\mod \frac{p'n}{p'} = n$ joukossa $\mathbb{Z}_{p'n}$. Koska $B_1 \neq B_2$ on jokin r siten, että $r \in B_1, r \notin B_2$. Tällöin $p'r \in B$, mutta $(p'r + N \mod p'n) \notin B$ vaikka $p'r$ ja $(p'r + N \mod p'n)$ eroavat luvun n monikerralla. Tällöin B ei voi olla jaksollinen modulo n, mikä todistaa väitteen. □

Tämän tuloksen todistettuaan Steinbergerin täytyi enää esitellä sopivat A ja B pystyäkseen todistamaan lause 5.7. Tässä erotetaan eksplisiittisesti osuus lauseen 5.7 todistukseksi, vaikka Steinberger ei niin itse teekkään.

Todistus. Analysoidaan kokonaislukujen joukkoa $\mathbb{Z}$ polynomien avulla ja merkitään $C(x) = \sum_{t \in \mathbb{Z}} x^t$. Jokaista kokonaislukujen joukkoa vastaa samoin yksikäsitteinen polynomi, jonka kertoimet ovat 1 tai 0. Tällöin huomataan, että $A \oplus B = \mathbb{Z}$ jos ja vain jos

$$A(x)B(x) \equiv 1 + x + x^2 + \cdots + x^{n-1} \mod 1 - x^n.$$

Erityisesti $A \oplus B = \mathbb{Z}_n$ jos ja vain jos $A(1)B(1) = n$ ja jokainen kertalukua n oleva ykkösenjuuri on joko polynomin $A(x)$ tai polynomin $B(x)$ juuri.

Olkoot nyt alkuluvut p_i, $i \in \{1, \ldots, k+1\}$ ensimmäiset $k+1$ alkulukua ja olkoot alkuluvut q_i, $i \in \{1, \ldots, k\}$ järjestyksessä k erilaista peräkkäistä alkulukua, jotka ovat kaikki (paljon) suurempia kuin p_{k+1}. Määritellään seuraavaksi luvut

$$\begin{aligned} P =& \prod_{i=1}^{k} p_i \\ Q =& \prod_{i=1}^{k} q_i \\ n =& \prod_{i=1}^{k} p_i q_i = PQ \\ L_j =& \frac{Pq_j}{p_j} \\ M_j =& \frac{PQ}{q_j} = \frac{n}{q_j}, \end{aligned}$$

jossa $j \in \{1, \ldots, k\}$. Näiden avulla määritellään seuraavaksi polynomit

$$\begin{aligned} A(x) =& \prod_{j=1}^{k} \left(1 + x^{L_j} + x^{2L_j} + \cdots + x^{(p_j-1)L_j}\right) \\ B_i'(x) =& \left(x^{\frac{n}{p_i}} + x^{M_i} + x^{2M_i} + \cdots + x^{(q_i-1)M_i}\right) \\ B_i(x) =& B_i'(x) \prod_{j=1, j\neq i}^{k} \left(1 + x^{M_j} + x^{2M_j} + \cdots + x^{(q_j-1)M_j}\right), \end{aligned}$$

joiden kaikkien ymmärretään tässä olevan modulo $1 - x^n$. Nämä kaikki vastaavat selkeästi kokonaislukujoukkoja, koska niiden kertoimet ovat joko 0 tai 1. Lisäksi nähdään, että $\frac{n}{p_i} \in B_i$, mutta $0 \notin B_i$, koska $x^{\frac{n}{p}}$ on ainoa termi polynomissa $B_i(x)$, joka on 0 modulo q_j kaikille indeksin j arvoille, joten B_i ei ole jaksollinen modulo $\frac{n}{p_i}$. Samoin, koska $M_i \in B_i, 0 \notin B_i$, nähdään, että B_i ei ole jaksollinen modulo M_i. Tämä tarkoittaa, että jokaiselle alkuluvulle $p|n$ on jokin B_i, joka ei ole jaksollinen modulo $\frac{n}{p}$.

On vielä näytettävä, että $A \oplus B_i = \mathbb{Z}_n$ kaikille $i \in \{1, \ldots, k\}$. Kun huomaamme, että $A(1) = P$ ja $B_i(1) = Q$ riittää todistaa, että jokainen kertaluvun n ykkösenjuuri paitsi 1 on joko polynomin $A(x)$ tai polynomin $B_i(x)$ juuri. Olkoon ζ jokin ykkösenjuuri kertalukua $m > 1$. Nyt, koska kaikille luvuille M ja luvuille $r|n$ pätee

$$\sum_{i=0}^{r-1} \zeta^{iM} = 0,$$

kaikille kertaluokille $m|rM$, mutta $m \nmid M$. Nyt, koska $m|n = q_j M_j$ saadaan $B_i(\zeta) = 0$, jos m ei jaa lukua M_j jollekin $j \neq i$, joten selvästi

$m|Pq_i = \text{syt}(M_j : j \neq i)$. Toisaalta, nyt nähdään, että luku m jakaa luvun $p_iL_i = Pq_i$ ja mikäli m ei jaa lukua L_i, niin $A(\zeta) = 0$, joten luvun m on jaettava $L_i = \frac{Pq_i}{p_i}$.

Jos luku q_i ei jaa lukua m niin m jakaa luvun P, joten alkuluku p_j on luvun m tekijä jollekin indeksille j ja m on luvun p_jL_j tekijä, ilman, että se on luvun L_j tekijä, joka tarkoittaa, että $A(\zeta) = 0$.

Voidaan siis olettaa, että $q_i|m$. Toisaalta, koska tällöin luku m ei ole luvun M_i tekijä ja $\zeta^{\frac{n}{p_i}} = 1$, koska m jakaa luvun L_i, saadaan, että $\zeta^{\frac{n}{p_i}} + \zeta^{M_i} + \cdots + \zeta^{(q_i-1)M_i} = 0$ ja siis $B_i(\zeta) = 0$, joka todistaa väitteen.

Näin ollaan todistettu joukkojen $A, B_1, B_2, \ldots, B_{k-1}$ ja B_k toteuttavan lemman 5.7 vaatimukset. Valitaan $p' = p_{k+1}$, jossa luku p_{k+1} on järjestysluvultaan alkuluku $k+1$. Jo aluksi määriteltiin, että kaikki alkuluvut q_i ovat eri alkulukuja kuin p_{k+1}. Olkoot lisäksi $n' = p'n, P' = p'P$ ja $A' = p'A$. Tällöin $\mathcal{K}(A') \geq n'$. Saadaan

$$\text{diam}(A') = p' \sum_{j=1}^{k} (p_j - 1)L_j \leq p' \sum_{j=1}^{k} Pq_j = P' \sum_{j=1}^{k} q_j \leq kP'q_k.$$

Olkoon $c > 1$ jokin vakio. Nyt, kun luvut q_i ovat peräkkäiset alkuluvut ja $q_1 \to \infty$, jotka ovat suurimpia kuin yksikäsitteisesti määritellyt alkuluvut $p_1, \ldots, p_{k+1}$.

Alkulukulause osoittaa, että kaikille tarpeeksi suurille q_1 pätee $q_k < cq_1$. Tällöin

$$\text{diam}(A')^k \leq k^k P'^k c^k q_1^k \leq (k^k P'^k c^k)n'.$$

Toisin sanoen $\text{diam}(A')^k$ on ylhäältä rajoitettu jollain luvun n' monikerralla kun $q_1 \to \infty$ eli $\mathcal{K}(A') \geq n'$ on alhaalta rajoitettu jollain luvun $\text{diam}(A')^k$ monikerralla. Koska tämä pätee kaikille $k \geq 2$ ja tapaus $k = 1$ on jo todistettu lauseessa 5.3, tämä todistaa lauseen 5.7. □

5.4 Granvillen eksponentiaalinen alaraja

Kun Steinberger kirjoitti tutkimustaan polynomisesta alarajasta, Andrew Granville käytti heidän konstruktiotaan luomaan eksponentiaalisen alarajan. Steinberger kertoi myös Birón ehdottaneen hänelle samaa, mutta Granvillen konstruktio on se, jonka Steinberger julkaisi oman tutkimuksensa lisänä.[21] Lauseeksi muotoiltuna Granville todisti, että

Lause 5.9. *Kaikille tarpeeksi suurille n pätee*

$$e^{\frac{\ln(n)^2}{4 \ln \ln n}} \leq \mathcal{D}(n).$$

Seuraavassa esitetään Granvillen todistus siinä yksinkertaisessa muodossa kuin se alun perin esitettiin Steinbergerin tutkimuksessa. Merkinnät ja käsitteet viittaavat osittain Steinbergerin lauseen todistukseen.

Todistus. Olkoon $R = k\prod_{i=1}^{k+1} p_i$, jossa alkuluvut p_i ovat ensimmäiset $k+1$ alkulukua. Alkulukulauseen nojalla

$$\begin{aligned} R &= \left(\frac{k\ln k}{e^{1+o(1)}}\right)^k \\ \ln R &= k(\ln k + \ln\ln k - 1 + o(1)) \\ \Rightarrow k &= \frac{\ln R}{\ln\ln R - 1 + o(1)} \end{aligned}$$

Valitaan ensimmäiset alkuluvut $q_1, \ldots, q_k$ jotka ovat suurempia tai yhtäsuuria kuin R. Alkulukulauseen mukaan ne kaikki ovat $(1+o(1))R$ eli $\mathrm{diam}A' = n = (1+o(1))R^2$. Nyt

$$\mathcal{K}(A') \geq \frac{R\prod_{i=1}^{k} q_i}{k} \geq \frac{R^{k+1}}{k} \geq e^{\frac{\ln(n)^2}{4\ln\ln n}}$$

kaikille tarpeeksi suurille n. □

6 Pitkiä laatoituksia

Lopuksi on hyvä vielä esitellä kootusti muutamia pitkiä laatoituksia käytännössä. Ikävä kyllä konstruktioiden luonteen vuoksi minkäänlainen kuvallinen esitys ei käytännössä ole mahdollinen. Verrattain pienilläkin laatoituksilla laattojen pituudet ovat useita tuhansia.

6.1 Lineaarinen vastaesimerkki

Luvussa 5.1 käytiin läpi esimerkki laatoituksesta, jonka jaksonpituus on $2n$ kun laatan pituus on n. Tässä esitellään vielä välien alarajan $2n \leq \mathcal{D}(n)$ ylittävä esimerkki. Esimerkin on kirjoittajalle esitellyt Jarkko Kari.

Tarkastellaan laattaa, jota kuvaa polynomi

$$A(x) = (1+x^9)(1+x^4+x^8) = 1 + x^4 + x^8 + x^9 + x^{13} + x^{17}$$

eli

$$A = \{0, 4, 8, 9, 13, 17\}.$$

Tämä polynomi löydettiin Steinbergerin konstruktiota seuraamalla valitsemalla alkuluvut $q_1 = 3$ ja $q_2 = 2$. Tämä laatta laatoittaa sekä jaksonpituudella 12 että jaksonpituudella 18. Näitä vastaavat joukot $B_{12} = \{0,2\} \oplus 12\mathbb{Z}$ ja $B_{18} = \{0,6,12\} \oplus 18\mathbb{Z}$. Laatoituksien rakennetta kuvataan kuvassa 3.

Määritellään nyt laatta $A' = 2A$ eli

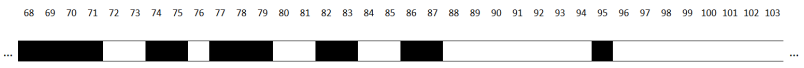
$$A' = \{0, 8, 16, 18, 26, 34\}.$$

Sijoitetaan parillisiin arvoihin laatat laatoituksen $A' \oplus 2B_{12}$ mukaisesti ja parittomiin arvoihin laatoituksen $A' \oplus 2B_{18} \oplus \{1\}$ mukaisesti. Nyt saadaan

Kuva 3: Laatoituksien $A \oplus B_{18}$ (yllä) ja $A \oplus B_{12}$ (alla) sisäiset rakenteet. Laatan $A = \{0, 4, 8, 9, 13, 17\}$ numerot on kirjattu laatoituksiin valkoisella. Mustalla ja vihreällä on merkitty isompien laattojen $A \oplus \{0, 6, 12\}$ ja $A \oplus \{0, 2\}$ translaatiot, joista laatoitukset koostuvat.

$$
\begin{aligned}
&(A' \oplus 2B_{12}) \cup (A' \oplus 2B_{18} \oplus \{1\}) \\
=&(A' \oplus 2(\{0, 2\} \oplus 12\mathbb{Z})) \cup (A' \oplus 2(\{0, 6, 12\} \oplus 18\mathbb{Z}) \oplus \{1\}) \\
=&(A' \oplus \{0, 4\} \oplus 24\mathbb{Z}) \cup (A' \oplus \{0, 12, 24\} \oplus 36\mathbb{Z} \oplus \{1\}) \\
=&(A' \oplus \{0, 4\} \oplus 24\mathbb{Z}) \cup (A' \oplus \{1, 13, 25\} \oplus 36\mathbb{Z}) \\
=&A' \oplus ((\{0, 4\} \oplus 24\mathbb{Z}) \cup (\{1, 13, 25\} \oplus 36\mathbb{Z})) \\
=&A' \oplus ((\{0, 4, 24, 28, 48, 52\} \oplus 72\mathbb{Z}) \cup (\{1, 13, 25, 37, 49, 61\} \oplus 72\mathbb{Z})) \\
=&A' \oplus \{0, 1, 4, 13, 24, 25, 28, 37, 48, 49, 52, 61\} \oplus 72\mathbb{Z} \\
=&A' \oplus B_{72},
\end{aligned}
$$

jossa $72 = \text{pyj}(24, 36)$. On siis olemassa laatoitus, jonka laatan pituus on 34 ja joka laatoittaa jaksonpituudella $72 = \frac{36}{17} \cdot 34 \approx 2{,}12 \cdot 34$. Laatoitus on siis riittävä todistamaan, että $\mathcal{D}(n) \neq 2n$. Kyseinen laatoitus on lyhin, jonka kirjoittaja tuntee tällä hetkellä. Katso myös kuvaa 4.



Kuva 4: Laatoituksen $A' \oplus B_{72}$ sisäistä rakennetta. Kuvassa on mustalla ja valkoisella merkitty isomman laatan $A' \oplus \{0, 1, 4, 13, 24, 25, 28, 37, 48, 49, 52, 61\}$ translaatiot. Kuva esittää ensimmäisen ja toisen tällaisen laatan rajaa. Muu osa laattaa koostuu peräkkäisistä luvuista 24-71.

6.2 Kolountzakiksen konstruktio

Luvut 53 ja 59 ovat pienimmät alkuluvut, jotka ovat suurempia kuin $\frac{10000}{200} = 50$. Tämä kertoo, että pienimmät Kolountzakiksen konstruktion mukaiset laatat ovat

$$\{0, 318, 590, 636, 908, 954, 1180, 1226, 1272, 1498, 1544, 1816, 1862, 2134, 2452\},$$

joka saadaan valinnoilla $p = 53$ ja $q = 59$ ja

$$\{0, 354, 530, 708, 884, 1060, 1062, 1238, 1414, 1416, 1592, 1768, 1946, 2122, 2476\},$$

joka saadaan valinnoilla $p = 59$ ja $q = 53$. Tällöin konstruktiossa jaksonpituus on $M = 2 \cdot 3 \cdot 5 \cdot 53 \cdot 59 = 93810$, joka on suurempi, kuin $\frac{30}{200^2} 2476^2 = 4597,932$.

Millainen on näistä Kolountzakiksen konstruktion mukainen siirtymien joukko Y? Käydään läpi jokin esimerkki. Kolountzakiksen konstruktiossa joukko Y on ryhmäisomorfismilla saatu joukosta B, joka on puolestaan kahden joukon unioini. Valinnoille $p = 53$ ja $q = 59$ nämä ovat

$$\begin{aligned} L =&\{(i,j,0) : (3k,0,0), (3k+1,5,0) \text{ ja } (3k,5l,0), \text{jossa } 0 \leq k < 53, 2 \leq l < 59\} \\ =&\{(0,0,0), (3,0,0), \ldots, (1,5,0), (4,5,0), \ldots, (0,10,0), \ldots, (156,290,0)\} \end{aligned}$$

ja

$$\begin{aligned} U =&\{(i,j,1) : (0,5l,1), (3,5l+1,1), (3k,5l,1), \text{jossa } 2 \leq k < 53, 0 \leq l < 59\} \\ =&\{(0,0,1), (0,5,1), \ldots, (3,1,1), (3,6,1), \ldots, (6,0,1), \ldots, (156,290,1)\}. \end{aligned}$$

Näiden kahden joukon muokkaamiseen tarvittava isomorfismi on näille valinnoille

$$\psi(i,j,k) = 590i + 318j + 46905k \mod 93810,$$

jossa $i \in \{0, \ldots, 158\}$, $j \in \{0, \ldots, 294\}$ ja $k \in \{0, 1\}$. Näin saadaan joukko Y, jonka koko on 6254 jäsentä:

$$Y = \{0, 15, 30, 45, 60, 75, 90, 105, \ldots, 93780, 93795\} \oplus 93810\mathbb{Z}.$$

Huomaa, että Y ei sisällä pelkästään luvun 15 monikertoja tai edes niitä kaikkia. Joukon Y osajoukoista $\psi(L)$ näyttää ensisilmäyksellä joukolta

$$L' = \{x \in \mathbb{Z} : x = 30k \mod 93810, k \in \mathbb{Z}\},$$

mutta tämä ei pidä paikkaansa. Esimerkiksi $410 \in \psi(L)$, mutta $410 \notin L'$. Toisaalta esimerkiksi luku $1590 \in L'$, mutta samalla $1590 \notin \psi(L)$. Samoin osajoukko $\phi(U)$ muistuttaa joukkoa

$$U' = \{x \in \mathbb{Z} : x = 30k + 15 \mod 93810, k \in \mathbb{Z}\},$$

mutta tämäkään ei pidä paikkaansa. Esimerkiksi luku $1293 \in \psi(U)$, vaikkei se selvästi ole joukon U' jäsen. Toisaalta luku $2565 \in U'$ ei kuulu joukkoon $\psi(U)$.

Nämä poikkeukset kumoavat määrällisesti toisensa, siten, että $|L'| = |\psi(L)| = 3127$ ja $|U'| = |\psi(U)| = 3127$. On selvää, että poikkeukset johtuvat Kolountzakiksen konstruktiossa tehdyistä "rivien siirroista", jotka tekevät joukosta Y ei-jaksollisen. Joukko Y voidaan kirjoittaa toisin

$$Y = (K' \cup M') \cup (Y' \setminus (K \cup M)) \oplus 93810\mathbb{Z},$$

jossa joukot Y', K, K', M ja M' ovat

$$\begin{aligned} Y' =&\{k \in \mathbb{Z} : k = 15m, m \in \{0, \ldots, 6253\}\} \\ K =&\{k \in \mathbb{Z} : k = 1590 + 1770m, m \in \{0, \ldots, 52\}\} \\ K' =&\{k \in \mathbb{Z} : k = 410 + 1770m, m \in \{0, \ldots, 52\}\} \\ M =&\{k \in \mathbb{Z} : k = 795 + 1590m, m \in \{0, \ldots, 58\}\} \\ M' =&\{k \in \mathbb{Z} : k = 1293 + 1590m, m \in \{0, \ldots, 58\}\}. \end{aligned}$$

6.3 Steinbergerin konstruktio

Steinbergerin konstruktiolla ei ole yhtä selkeitä rajoja sille, mikä on pienin mahdollinen laatta. Lisäksi konstruktiossa on erilaisia epäoptimaalisuuksia. Steinberger kertoo tutkimuksessaan [21] esimerkiksi, että potenssille n^k täytyy tosiasiassa soveltaa hänen konstruktiotaan asteelle $k+1$. Lisäksi, jos valitaan konstruktiossa alkuluvut $q_1, \ldots, q_k$ peräkkäisiksi aleneviksi alkuluvuiksi, eikä kasvaviksi alkuluvuiksi, tämä optimoi hieman tulosta. Jo edellä annetut arviot on saatu seuraavasti:

1. Konstruktiossa valittiin alkuluvut $q_1 = 773$, $q_2 = 769$ ja $q_3 = 761$, jolloin laatan pituus on 316673.[3]

2. Konstruktiossa valittiin alkuluvut $q_1 = 120151579$, $q_2 = 120151561$, $q_3 = 120151541$ ja $q_4 = 120151531$, jolloin laatan pituus on 783748556833.[4]

Käydään esimerkkinä läpi millainen laatta ensimmäisessä kohdassa on kyseessä. Jos käytetään konstruktiota kolmelle alkuluvulle, saadaan luvut

$$\begin{aligned} P =& 2 \cdot 3 \cdot 5 = 30 \\ L_1 =& \frac{30 \cdot 787}{2} = 11595 \\ L_2 =& \frac{30 \cdot 773}{3} = 7690 \\ L_3 =& \frac{30 \cdot 769}{5} = 4566. \end{aligned}$$

Tällöin laattaa A kuvaava polynomi on

$$\begin{aligned} A =& \left(1 + x^{11595}\right)\left(1 + x^{7690} + x^{2 \cdot 7690}\right)\left(1 + x^{4566} + \cdots + x^{4 \cdot 4566}\right) \\ =& 1 + x^{4566} + x^{7690} + x^{9132} + x^{11595} + x^{12256} + x^{13698} + x^{15380} \\ &+ x^{16161} + x^{16822} + x^{18264} + x^{19285} + x^{19946} + x^{20727} + x^{21388} \\ &+ x^{23851} + x^{24512} + x^{25293} + x^{25954} + x^{26975} + x^{28417} + x^{29078} \\ &+ x^{29859} + x^{31541} + x^{32983} + x^{33644} + x^{36107} + x^{37549} + x^{40673} \\ &+ x^{45239}, \end{aligned}$$

joka vastaa laattaa

$$\begin{aligned} A = \{&0, 4566, 7690, 9132, 11595, 12256, 13698, 15380, 16161, \\ &16822, 18264, 19285, 19946, 20727, 21388, 23851, 24512, \\ &25293, 25954, 26975, 28417, 29078, 29859, 31541, 32983, \\ &33644, 36107, 37549, 40673, 45239\}. \end{aligned}$$

Tämä laatta kerrotaan vielä neljännellä alkuluvulla eli seitsemällä, jolloin saa-

[3] Steinbergerin tutkimuksessa on virheellisesti alkuluvut 787, 773 ja 769. Näillä alkuluvuilla laatan pituus on 320047.

[4] Steinbergerin tutkimuksessa on virheellisesti alkuluvut 120151637, 120151579, 120151561 ja 120151541. Näillä alkuluvuilla laatan pituus on 783748708303.

daan laatta A'.

$$\begin{aligned} A' = \{&0, 31962, 53830, 63924, 81165, 85792, 95886, 107660, 113127 \\ &117754, 127848, 134995, 139622, 145089, 149716, 166957, \\ &171584, 177051, 181678, 188825, 198919, 203546, 209013, \\ &220787, 230881, 235508, 252749, 262843, 284711, 316673\} \end{aligned}$$

Tämän laatan konstruktion mukainen jaksonpituus on

$$\begin{aligned} p'n =& p' \prod_{i=1}^{3} p_i q_j = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 761 \cdot 769 \cdot 773 \\ =& 94996976970 \\ <& 316673^2. \end{aligned}$$

Tämä on ristiriidassa Steinbergerin väitteen kanssa, että 316673 on riittävä laatan pituus siten, että $n^2 \leq \mathcal{D}(n)$. Sain itse tämän tapahtumaan vasta valinnoilla $q_1 = 821$, $q_2 = 811$ ja $q_3 = 809$, jolloin laatan pituus on 335657 ja sen laatoituksen jaksonpituus on 113118028590. Jos konstruktiota seurataan tiukasti ja valitaan kasvavat alkuluvut, aikaisimmat sopivat valinnat ovat $q_1 = 811$, $q_2 = 821$ ja $q_3 = 823$, jolloin laatan pituus on 338359 ja sen laatoituksen jaksonpituus 115075571730.

Lisäksi, jos etsitään sellaista laattaa, että $n^3 \leq \mathcal{D}(n)$ ja käytetään konstruktiota Steinbergerin antamille luvuille $q_1 = 120151637$, $q_2 = 120151579$, $q_3 = 120151561$ ja $q_4 = 120151541$, saadaan laatan pituudeksi 783748708303 ei 783748556833. Saatavan laatan pituus on lisäksi liian pitkä verrattuna saatavan laatoituksen pituuteen 481426417007843810773622025392156130. Ensimmäiset valinnat, joilla itse sain laatoituksen onnistumaan, ovat alkuluvut $q_1 = 120151783$, $q_2 = 120151777$, $q_3 = 120151751$ ja $q_4 = 120151729$. Näillä saatavan laatan pituus on 783749905213 ja laatoituksen jaksonpituus 481429309942454744673152023249627590.

7 Yhteenveto

Kokonaislukujen laatoituksien ongelmien tutkijat ovat tiivis joukko ja heidän yhteistyönsä paistaa tutkimuksista läpi. Tutkijat kiittävät toisiaan tutkimuksissaan ja antavat kollegoilleen julkaistavaksi omia tuloksiaan. Tämä matematiikan ala onkin minusta malliesimerkki yhteistyön voimasta. Yhteistyön avulla edistyttiin hyvin nopeasti siihen pisteeseen asti, että laatoitusten jaksonpituuksien alarajan ja ylärajan tiedetään riippuvan eksponentiaalisesti laatan pituudesta, kun vielä 1990-luvulla tiedettiin vain, että totuus on jossain lineaarisen ja eksponentiaalisen välissä. Kenelle tahansa matemaatikolle tämän pitäisi olla inspiroivaa.

Edelleen on silti tutkittavaa. Monijoukkojen ja pelkkien kokonaislukujen alarajojen välinen ero on todettu, muttei täysin kvantifioitu eikä sen syistä olla varmoja. Mikä on paras approksimaatio funktiolle $\mathcal{D}(n)$? Voiko tässä esiteltyjä keinoja käyttää korkeamman asteen laatoitusongelmissa? Mahdollisuudet jatkotutkimukselle ovat lähes rajattomat.

Viitteet

[1] Amiot, Emmanuel, 2005, Rhythmic canons and Galois theory, *Colloquium on Mathematical Music Theory*, No. 347, pp. 1-25.

[2] Bertrand, Joseph, 1845, Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme., *Journal de l'École Royale Polytechnique* 18, No. 30, pp. 123–140.

[3] Biró, András, 2005, Divisibility of integer polynomials and tilings of the integers, *Acta Arithmetica* 2, No. 118, pp. 117-128.

[4] Coven, Ethan M. & Aaron Meyerowitz, 1999, Tiling the Integers with Translates of One Finite Set, *Journal of Algebra* 212, No. 1, pp. 161-174.

[5] Gauss, Carl Friedrich, 1801, Kohta 38, *Disquisitiones Arithmeticae*, Lipsiae, pp. 30-32.

[6] Gauss, Carl Friedrich, 1801, Kohta 42, *Disquisitiones Arithmeticae*, Lipsiae, pp. 36-38.

[7] Gauss, Carl Friedrich, 1801, Kohta 341, *Disquisitiones Arithmeticae*, Lipsiae, pp. 599-602.

[8] Granville, Andrew, Laba, Izabella & Wang, Yang, 2001, *A characterization of finite sets that tile the integers*, pre-print.

[9] Erdős, Paul, 1932, Beweis eines Satzes von Tschebyschef, *Acta Scientiarum Mathematicarum (Szeged)* 5, pp. 194-198.

[10] Euler, Leonhard, 1763, Theoremata arithmetica nova methodo demonstrata, *Novi Commentarii academiae scientiarum Petropolitanae* 8, pp. 74-104.

[11] Hajós, György, 1942, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Wurfelgitter, *Mathematische Zeitschrift* 47, pp. 427-467.

[12] Jedrzejewski, Franck, 2009, Tilings of the integers with aperiodic tiles, *Journal of Mathematics and Music* 3, No. 2, pp. 99-115.

[13] Kolountzakis, Mihail N., 2003, Translational Tilings of the Integers with Long Periods, *The Electronic Journal of Combinatorics* 10, R22.

[14] Long, Calvin T., 1967, Addition Theorems for Sets of Integers, *Pacific Journal of Mathematics* 23, No. 1, pp. 107-112.

[15] Magidin, Arturo & McKinnon, David, 2005, Gauss's Lemma for Number Fields, *The American Mathematical Monthly 112*, No. 5, pp. 387-388.

[16] Newman, Donald J., 1977, Tesselation of Integers, *Journal of Number Theory* 9, pp. 107-111.

[17] Ramanujan, Srinivasa, 1919, A proof of Bertrand's postulate, *Journal of the Indian Mathematical Society* 11, pp. 181-182.

[18] Sands, Arthur D., 1962, On the factorisation of finite abelian groups. II, *Acta Mathematica Academiae Scientiarum Hungarica* 13, pp. 153-169.

[19] Steinberger, John P., 2005, Multiple tilings of $\mathbb{Z}$ with long periods, and tiles with many-generated level semigroups, *New York Journal of Mathematics* 11, pp. 445-456.

[20] Steinberger, John P., 2005, Indecomposable Tilings of the Integers with Exponentially Long Periods, *The Electronic Journal of Combinatorics* 12, R36.

[21] Steinberger, John P., 2006, Tilings of the Integers Can Have Superpolynomial Periods, *Combinatorica* 29, No. 4, pp. 503-509.

[22] Tijdeman, Rob, 2006, Periodicity and Almost-Periodicity, *More Sets, Graphs and Numbers*, pp. 381-405.

[23] Tšebyšov, Pafnuti, 1852, Mémoire sur les nombres premiers., *Journal de mathématiques pures et appliquées, premiere série* 17, pp. 366–390.

[24] Weintraub, Steven H., 2000, A Proof of the Irreducibility of the p-th Cyclotomic Polynomial, Following Gauss, *Mathematics Subject Classification 2000*, 12E05, pp. 1-2.