Polynomien yhteiset alkutekijät

TuKoKe 2019

Tiivistelmä

Kokonaislukukertoimisen polynomin P alkutekijöiksi kutsutaan niitä alkulukuja p, jotka jakavat jonkin luvuista $P(1), P(2), P(3), \ldots$. Osoitan työssä neljä polynomien alkutekijöitä käsittelevää lausetta käyttäen 21 apulausetta. Työn päätulos todistaa erään polynomin olemassaolon. Tämän polynomin etsimiseksi todistin algoritmin toimivuuden ja kirjoitin C++-ohjelmointikielellä ohjelman, joka implementoi algoritmin.

Lähtökohtina toimivat Schurin lause vuodelta 1912, Frobeniuksen lause vuodelta 1896 ja Nagellin todistama lause. Schurin lause osoittaa, että kaikilla kokonaislukukertoimislla epävakiolla polynomeilla on olemassa äärettömän monta alkutekijää. Tällaisiin polynomeihin viitataan vastedes lyhyesti sanalla "polynomi". Frobeniuksen lause osoittaa, että jokaisen polynomin alkutekijöiden tiheys alkulukujen joukossa on positiivinen. Useamman polynomin yhteisistä alkutekijöistä on vähemmän tutkimusta, vaikkakin Nagell on osoittanut, että kahdella polynomilla on äärettömästi yhteisiä alkutekijöitä.

Työn päätuloksena osoitin, että kaikilla polynomeilla A ja B on olemassa polynomi D, jonka alkutekijät ovat täsmälleen polynomien A ja B yhteiset alkutekijät. Yleistin väitteen useammalle kuin kahdelle polynomille sekä muillekin kuin alkulukutekijöille. Tuloksen avulla usean polynomin yhteisten alkutekijöiden tutkiminen voidaan palauttaa yhden polynomin tutkimiseen. Sovelluksena osoitan, että monen polynomin yhteisten alkutekijöiden tiheys on vähintään näiden polynomien asteiden tulon käänteisluku, ja että tämä raja on paras mahdollinen.

Osoitin, että polynomien A ja B yhteisten alkutekijöiden tiheys on polynomien A ja B alkutekijöiden tiheyksien tulo, kun polynomien A ja B juurikuntien leikkaus on rationaaliluvut. Tämäkin tulos yleistyy useammalle polynomille.

Tuloksen avulla osoitin, että kaikki rationaaliluvut nollan ja yhden välillä esiintyvät jonkin polynomin alkutekijöiden tiheytenä. Frobeniuksen lauseen nojalla muut kuin rationaaliluvut eivät esiinny tiheyksinä.

Päätuloksen todistus on konstruktiivinen, eli se antaa tavan löytää edellä kuvaillun polynomin D. Esitän työssä algoritmin tällaisen D löytämiseksi, kun oletetaan polynomeilla A, B olevan juuret a, b, joilla $[\mathbb{Q}(a, b) : \mathbb{Q}] = \deg(A)\deg(B)$. Osoitin algoritmin toimivuuden, yleistin sen monelle polynomille ja esitän algoritmin implementaation C++-ohjelmointikielellä.

Abstract

The prime divisors of a polynomial P with integer coefficients are those primes p which divide some of the numbers $P(1), P(2), P(3), \ldots$. I proved four theorems on the prime divisors of polynomials using 21 lemmas. Using C++, I implemented an algorithm which finds the polynomial described by the main theorem.

The basis of the work is Schur's theorem from 1912, Frobenius theorem from 1896, and a theorem by Nagell. Schur's theorem proves the infinitude of prime divisors for all non-constant polynomials with integer coefficients. These polynomials are referred as "polynomial"from now. Frobenius theorem proves that the prime divisors of polynomials have a positive, rational density in prime numbers. Nagell has proven the infinitude of the common prime divisors of two polynomials.

As the main theorem I proved that for all polynomials A and B, there exists a polynomial D whose prime divisors are exactly the common prime divisors of A and B. I generalized this for more than two polynomials, and for other divisors than prime divisors. Thus, questions on the common prime divisors of polynomials can be reduced to the case of a single polynomial.

I proved that the density of common prime divisors of A and B is the product of the density of prime divisors of A and B, when the intersection of their splitting fields is the rational numbers. This, too, generalizes for several polynomials. Using this I proved that all rationals between zero and one occur as the density of prime divisors of some polynomial.

I present an algorithm for determining the described polynomial D, assuming A and B have roots a and b such that $[\mathbb{Q}(a, b) : \mathbb{Q}] = \deg(A) \deg(B)$. I proved the correctness of the algorithm, generalized it for several polynomials and present an implementation with C++.

Sisältö

"Tähän menee varmaan 20 minuuttia"

-Kirjoittaja

1 Johdanto

Polynomit ovat laajasti tutkittuja matemaattisia objekteja, joita voidaan soveltaa suuressa osassa matematiikan alueita. Lukuteorian alalla kiinnostavimpia ovat polynomit, joiden kertoimet ovat kokonaislukuja. Tämän työn lähtökohtana toimii matemaatikko Issai Schurin mukaan nimetty **Schurin lause**:

Olkoon P kokonaislukukertoiminen polynomi, joka ei ole vakiopolynomi. On olemassa äärettömän monta alkulukua p niin, että p jakaa jonkin luvuista $P(1), P(2), P(3), \ldots$ [1].

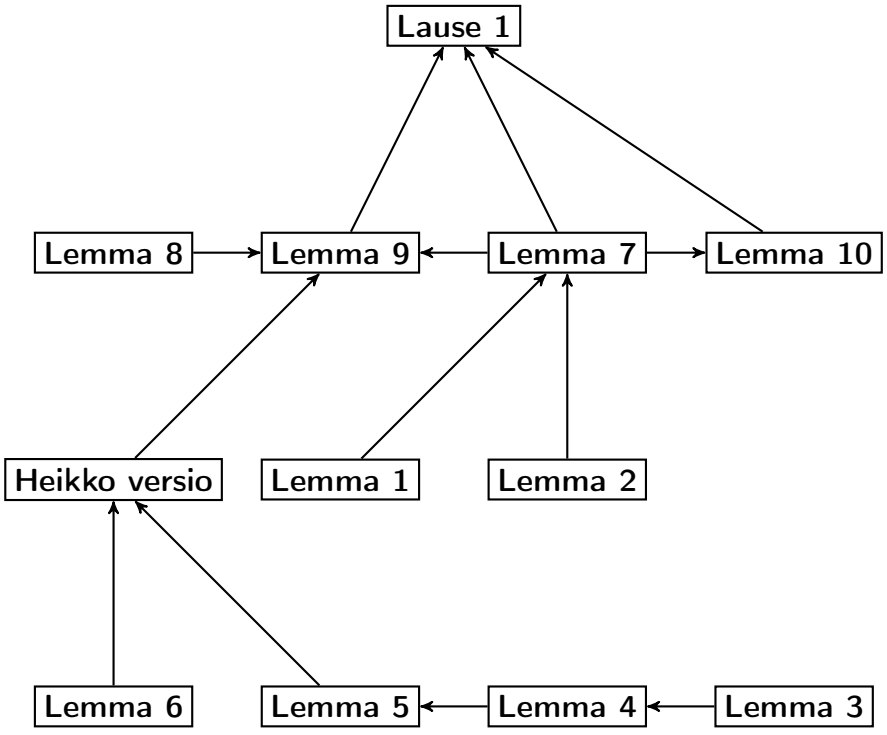
Lausetta voi yleistää seuraavilla kysymyksillä:

- Lause koskee yhtä polynomia P. Voidaanko vastaava lause todistaa kahdelle polynomille P ja Q: vaaditaan, että p jakaa luvut $P(n)$ ja $Q(m)$ jollain $n, m \in \mathbb{Z}_+$? Entä useampi polynomi?
- Päteekö väite, jos vaadittaisiin, että p^2 jakaa jonkin luvuista $P(n), n \in \mathbb{Z}_+$? Entä p^3, tai yleisesti p^k kaikilla $k \in \mathbb{Z}_+$?
- Kuinka suuri osuus alkuluvuista on halutunlaisia?

Työssä muotoillaan ja todistetaan Schurin lauseelle yleistys, joka yhdistää edelliset ideat. Tämä tehdään osoittamalla toinen aiheeseen liittyvä väite eräänlaisen polynomin olemassaolosta, jonka seurauksina saadaan tämä yleistys sekä muita tuloksia. Lopuksi esitetään algoritmi työn päätuloksen mukaisen polynomin löytämiseksi tietokoneella.

Kuvassa 1 on esitetty työn päätuloksen eli lauseen 1 todistuksen rakenne. Ensin osoitetaan lemmat 1-2 koskien työn matematiikan keskeisiä rakenteita. Tämän jälkeen osoitetaan heikompi versio lauseesta lemmojen 3-6 avulla. Lemmojen 7-10 avulla heikosta versiosta saadaan osoitettua koko väite.

Lause 2 osoittaa yleistyksen Schurin lauseelle. Lauseen todistuksessa esitellään Frobeniuksen lause, jota käytetään lauseen 3 todistuksessa. Lauseen 3 sovelluksena osoitetaan yhdessä kirjallisuudesta löytyvien tulosten kanssa lause 4.



Kuva 1: kuvaus työn päätuloksen todistuksen rakenteesta.

Polynomin $P \in \mathbb{Z}[x]$ tekijöiksi kutsutaan niitä $n \in \mathbb{Z}$, jotka jakavat jonkin luvuista $P(k), k \in \mathbb{Z}$, ja näiden joukkoa merkitään notaatiolla $S_d(P)$. P:n alkutekijät ovat ne alkuluvut p, jotka ovat P:n tekijöitä, ja näiden joukkoa merkitään $S(P)$. P:n vahvat alkutekijät ovat ne alkuluvut p, joilla $p^k \in S_d(P)$ kaikilla $k \in \mathbb{Z}_+$. Näiden joukkoa merkitään $S_v(P)$.

1.1 Aiempi tutkimus

Nagell on yleistänyt Schurin lausetta osoittamalla, että millä tahansa kahdella epävakiolla polynomilla $P_1, P_2 \in \mathbb{Z}[x]$ on äärettömän monta yhteistä alkutekijää. Tälle väitteelle on olemassa todistus käyttäen algebrallista lukuteoriaa [6] (lause 3). Yhden polynomin alkutekijöiden tiheyttä käsittelee Frobeniuksen lause, joka esitellään tässä työssä. Vahvojen alkutekijöiden tutkiminen vastaa polynomin nollakohdan etsimistä ns. p-adic luvuissa[*1] [7] [8]. Kirjallisuudesta ei löytynyt viitteitä näiden tulosten yhdistämisestä.

Alkutekijän määritelmää voidaan yleistää tutkimalla niitä alkulukuja p, joilla polynomilla P on täsmälleen k erisuurta nollakohtaa modulo p. Viitteessä [9] on tutkittu yleistettyyn määritelmään liittyviä kysymyksiä algebrallisen lukuteorian keinoin, mukaan lukien väitteitä tämäntyyppisten joukkojen leikkauksesta. Lisäksi artikkelissa on todistettu, että tietyntyyppisillä $f, g \in \mathbb{Z}[x]$ on olemassa sellainen $h \in \mathbb{Z}[x]$, jolla, muiden ominaisuuksien ohella, pätee $S(f) \cap S(g) = S(h)$ [*2]. Tässä työssä todistetaan viitteen tuloksia laajentaen, että kaikilla f, g on olemassa sellainen h, jolla $S_d(f) \cap S_d(g) = S_d(h)$.

Polynomien alkutekijöiden joukolle ei yleisessä tapauksessa ole löydetty yksinkertaista esitystapaa, mutta erikoistapauksia on ratkaistu. Viitteessä [10] on osoitettu, että polynomin P alkutekijät voidaan esittää kongruenssiehdoilla $p \in S(P) \Leftrightarrow p \equiv a_i \pmod{m}$ sopivilla $m, a_1, a_2, \ldots, a_k \in \mathbb{Z}_+$ jos P:n Galois'n ryhmä (määritelty lauseen 2 todistuksessa) on Abelin ryhmä. Viitteessä todetaan, että myös muunlaisia esitystapoja voidaan käyttää. Esimerkiksi polynomin $x^3 - 2$ alkutekijät ovat ne alkuluvut p, jotka ovat $2 \pmod 3$ tai muotoa $x^2 + 27y^2, x, y \in \mathbb{Z}$ [10]. Tämän työn tuloksilla saadaan palautettua monen polynomin yhteisten alkutekijöiden tutkiminen yhden polynomin tapaukseen.

Alkutekijöitä on tutkittu yhden muuttujan polynomien lisäksi muille joukoille. Vähintään kahden muuttujan polynomien alkutekijät ovat kaikki alkuluvut äärellisen montaa lukuun ottamatta [11] (lemma 2). Polynomien ohella muotoa $a_0 = a$, $a_{n+1} = P(a_n), P \in \mathbb{Z}[x]$ olevien lukujonojen alkutekijöiden tiheyttä on tutkittu [12][13]. Vastaavaa ongelmaa lineaarisesti rekursiivisille lukujonoille on myös käsitelty [14] [15].

Lopuksi mainitaan, että polynomien arvoista on paljon muuta tutkimusta. Luvun $P(n)$ suurimmalle alkutekijälle on esitetty rajoja [16] [17]. Niitä $P(n)$, jotka eivät ole jaollisia minkään alkuluvun neliöillä on tutkittu artikkeleissa [18] [19]. Polynomien alkulukuarvoihin liittyy avoimia ongelmia, kuten muotoa $n^2 + 1$ ja $p + 2$ olevien alkulukujen äärettömyys [20] [21].

1.2 Notaatiot ja esitietoja

Joukolla $\mathbb{Z}[x]$ viitataan kokonaislukukertoimisiin yhden muuttujan polynomeihin, ja $\mathbb{Z}_*[x]$ sisältää joukon $\mathbb{Z}[x]$ ei-vakiot polynomit. Vastaavasti määritellään $\mathbb{Q}[x]$ ja $\mathbb{Q}_*[x]$. Rationaalilukujen esitys muodossa $\frac{a}{b}$ valitaan aina niin, että murtoluku on supistetussa muodossa.

Kirjain p kuvaa aina alkulukua, ja kirjaimet n, m, k viittaavat kokonaislukuihin, useimmiten erityisesti positiivisiin kokonaislukuihin. Kreikkalaiset kirjaimet α, β, γ viittaavat algebrallisiin lukuihin, eli lukuihin, jotka ovat jonkin polynomin $P \in \mathbb{Q}_*[x]$ nollakohta.

Jokaisella algebrallisella luvulla α on olemassa yksikäsitteinen polynomi $P \in \mathbb{Q}_*[x]$, joka toteuttaa seuraavat ehdot:

- $P(\alpha) = 0$
- Ei ole olemassa sellaista polynomia $Q \in \mathbb{Q}_*[x]$, jonka aste olisi pienempi kuin P:n, ja jolla $Q(\alpha) = 0$.

[1] Englanninkielisellä termillä p-adic number ei ole vakiintunutta suomenkielistä käännöstä

[2] Viitteessä on osoitettu, että joukot $S(f) \cap S(g)$ ja $S(h)$ sisältävät samat alkuluvut äärellisen montaa poikkeusta lukuun ottamatta. Tämän työn lemman 7 muunnoksilla poikkeustapaukset voidaan korjata.

- P:n korkeimman asteen termin kerroin on 1. Tällaisia polynomeja kutsutaan pääpolynomeiksi (engl. monic polynomial).

Tätä P kutsutaan luvun α minimaaliseksi polynomiksi (kunnan $\mathbb{Q}$ yli). Vastaavasti voidaan määritellä minimaalisia polynomeja muiden kuntien yli.

Olkoon P luvun α minimaalinen polynomi kunnan $\mathbb{Q}$ yli. Jos $Q \in \mathbb{Q}_*[x]$ ja $Q(\alpha) = 0$, on Q jaollinen luvun α minimaalisella polynomilla. Tämän voi todistaa polynomien jakoyhtälöllä jakamalla polynomi Q polynomilla P: $Q = PT + R$, missä $\deg(R) < \deg(P)$. Tällöin $R(\alpha) = Q(\alpha) - P(\alpha)T(\alpha) = 0$, mikä on mahdollista minimaalisen polynomin määritelmän nojalla vain jos R on nollafunktio.

Merkinnällä $\mathbb{Q}(\alpha)$ tarkoitetaan pienintä kuntaa, joka sisältää sekä rationaaliluvut että luvun α, ja se sisältää luvut muotoa $Q(\alpha), Q \in \mathbb{Q}[x]$ [2] (lauseet 3.19 ja 3.15). Koska Q voitaisiin tarvittaessa jakaa jakokulmassa luvun α minimaalisella polynomilla P, voitaisiin edellisessä määritelmässä olettaa $\deg(Q) < \deg(P)$. Kunta $\mathbb{Q}(\alpha)$ voidaan siis tulkita $\mathbb{Q}$-vektoriavaruutena, jonka kanta on $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, missä n on α:n minimaalisen polynomin aste.

Kuntalaajennuksella tarkoitetaan kuntaparia A, B, joilla $A \subset B$ ja A:n laskutoimitukset ovat samat kuin B:n. Kuntalaajennusta merkitään B/A. Kuntalaajennuksen aste tarkoittaa A-vektoriavaruuden B ulottuvuutta. Esimerkiksi laajennuksen $\mathbb{Q}(\alpha) : \mathbb{Q}$ aste on luvun α minimaalisen polynomin aste n, ja tätä merkitään $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Kaikille kunnille $A \subset B \subset C$ pätee $[C : A] = [C : B][B : A]$ [2] (lause 4.7.).

Merkitään $a \mid b$, jos a jakaa luvun b, ja muuten $a \nmid b$. Notaatiolla $a \equiv b \pmod{m}$ tarkoitetaan, että $m|a - b$. Jos $a \equiv b \pmod{m}, a, b \in \mathbb{Z}$, niin pätee $P(a) \equiv P(b) \pmod{m}$ kaikilla $P \in \mathbb{Z}[x]$. Kaikilla luvun m kanssa yhteistekijättömillä b on olemassa sellainen c, jolla $bc \equiv 1 \pmod{m}$. Täten rationaaliluku $\frac{a}{b}$ voidaan ajatella kokonaislukuna ac tutkittaessa modulo m, missä c on luvun b käänteisluku modulo m. Merkitään $m|\frac{a}{b}$, jos $m|a$, ja lukujen b ja m suurin yhteinen tekijä on 1. Työssä käytetään vapaasti tätä jaollisuuden määritelmää rationaaliluvuille, mikä on vastaava kuin viitteessä [9] (sivu 253). Tavalliset jaollisuuden ominaisuudet toteutuvat myös rationaaliluvuilla, ja laajennettu määritelmä toteuttaa lisäksi ehdon $p|P(\frac{a}{b}) \implies p \in S(P)$, kun $p \nmid b$ [9]. Laajennettu määritelmä ei ole laajasti käytetty, mutta sitä käytetään todistusten helppolukuisuuden parantamiseksi. Kongruenssiyhtälöistä kokonaisluvuilla voi lukea lisää viitteen [3] luvuista 2 ja 3.

Työssä käytettäviä perustuloksia ovat kiinalainen jäännöslause, Bezout'n lemma ja Henselin lemma.

Kiinalainen jäännöslause

Olkoot $m_1, m_2, \ldots, m_k \in \mathbb{Z}_+$ sellaisia, joilla lukujen m_i, m_j suurin yhteinen tekijä on 1 kaikilla $i \neq j$. Olkoot $a_1, a_2, \ldots a_k$ mielivaltaisia kokonaislukuja. On olemassa sellainen $x \in \mathbb{Z}$, jolla $x \equiv a_i \pmod{m_i}$ kaikilla $1 \leq i \leq n$ [3] (sivu 31).

Bezout'n lemma

Olkoon $\mathbb{F}$ kunta, ja olkoot $A, B \in \mathbb{F}[x]$ yhteistekijättömiä kunnassa $\mathbb{F}$. On olemassa sellaiset polynomit $X, Y \in \mathbb{F}[x]$ ja $0 \neq f \in \mathbb{F}$, jolla $AX + BY = f$ [4].

Tutkitaan väitettä tapauksessa $\mathbb{F} = \mathbb{Q}$. Tällöin $AX + BY = n$ jollain $X, Y \in \mathbb{Q}[x]$, $n \in \mathbb{Q}$. Kertomalla yhtälön puolittain polynomien X, Y nimittäjien tulolla sekä luvun n nimittäjällä saadaan yhtälö $AX_* + BY_* = n_*$, missä $X_*, Y_* \in \mathbb{Z}[x]$ ja $0 \neq n_* \in \mathbb{Z}$. Täten väite on tosi myös valinnalla $\mathbb{F} = \mathbb{Z}$, vaikka $\mathbb{Z}$ ei ole kunta.

Henselin lemma

Olkoot $P \in \mathbb{Z}_*[x]$ ja $x \in \mathbb{Z}$ annettu. Oletetaan, että $P(x) \equiv 0 \pmod{p^k}$, ja $P'(x) \not\equiv 0 \pmod{p}$. Tällöin on olemassa luku $y \in \mathbb{Z}$, jolla $P(y) \equiv 0 \pmod{p^{k+1}}$, ja $x \equiv y \pmod{p}$.

Todistus. Todistetaan ensin, että kaikilla $a, b \in \mathbb{Z}$ pätee $P(a + bp^k) \equiv P(a) + bp^k P'(a) \pmod{p^{2k}}$. Olkoon $P(x) = c_0 + c_1 x + \ldots + c_d x^d$. Tällöin

$$P(a + bp^k) = c_0 + c_1(a + bp^k) + \ldots + c_d(a + bp^k)^d \equiv$$
$$\Big(c_0 + c_1 a + \ldots + c_d a^d\Big) + \Big(c_1 bp^k + 2c_2 abp^k + \ldots + dc_d a^{d-1} bp^k\Big) = P(a) + bp^k P'(a) \pmod{p^{2k}}$$

Olkoon $P(x) = np^k$ jollain $n \in \mathbb{Z}$. Edellisen nojalla pätee $P(x + bp^k) \equiv p^k(n + bP'(x)) \pmod{p^{2k}}$, joten $P(x + bp^k) \equiv p^k(n + bP'(x)) \pmod{p^{2k}}$. Koska $P'(x) \not\equiv 0 \pmod{p}$, on olemassa sellainen b, jolla $bP'(x) \equiv -n \pmod{p}$. Tällä b:n valinnalla pätee $P(x+bp^k) \equiv 0 \pmod{p^{k+1}}$. Tämä todistaa lemman valinnalla $y = x+bp^k$. □

Jaettaessa polynomeja tekijöihin käytetään seuraavaa tulosta:

Polynomien jakaantuminen

Olkoon $P \in \mathbb{Z}_*[x]$ rationaaliluvuissa jaollinen polynomi. Tällöin on olemassa polynomit $Q, R \in \mathbb{Z}_*[x]$, jolla $P = QR$ [5]. Tästä seuraa helpolla induktiolla, että mikä tahansa rationaaliluvuissa jaollinen P voidaan kirjoittaa jaottomien kokonaislukukertoimisten polynomien tulona.

Lopuksi määritellään alkuluvuista koostuvan joukon tiheys.

Tiheys

Jos S on alkulukujen $\mathbb{P}$ osajoukko, määritellään sen (luonnollinen) tiheys tavalliseen tapaan kaavalla

$$\delta(S) := \lim_{x\to\infty} \frac{|\{p \le x : p \in S\}|}{|\{p \le x : p \in \mathbb{P}\}|}$$

olettaen, että tämä raja-arvo on olemassa.

1.3 Tulokset

Olkoot $P_1, P_2, \ldots, P_n \in \mathbb{Z}_*[x]$.

Ensimmäisenä osoitetaan seuraava tulos:
Lause 1. *On olemassa sellainen $D \in \mathbb{Z}_*[x]$, jolla $S_d(D) = S_d(P_1) \cap S_d(P_2) \cap \ldots \cap S_d(P_n)$.*

Lause 1 mahdollistaa polynomien yhteisten alkutekijöiden tutkimisen redusoinnin yhden polynomin alkutekijöiden tutkimiseen. Tämä voidaan myös muotoilla niin, että yhtälöryhmä $P_i(x_i) \equiv 0 \pmod{m}$ kaikilla $1 \le i \le n$ on ratkeava jos ja vain jos yhtälö $D(x) \equiv 0 \pmod{m}$ on ratkeava.

Lauseen 1 todistus on konstruktiivinen. Konstruoidun D aste on enintään $\deg(P_1)\deg(P_2)\ldots\deg(P_n)$. Tämä on tiukka yläraja. Lauseen 1 ja sen todistukseen käytettyjen lemmojen avulla osoitetaan yleistys Schurin lauseelle.
Lause 2. *Tiheys $d := \delta(S_v(P_1) \cap S_v(P_2) \cap \ldots \cap S_v(P_n))$ on olemassa, ja*

$$d \ge \frac{1}{\deg(P_1)\ldots\deg(P_n)}$$

Lauseen 2 alaraja tiheydelle on tiukka.

Yhteisten alkutekijöiden tiheys voidaan tietyin lisäehdoin laskea.
Lause 3. *Olkoon polynomin P_i juuret $\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,d_i}$, ja olkoon $F_i := \mathbb{Q}(\alpha_{i,1}, \ldots, \alpha_{i,d_i})$ polynomin P_i juurikunta (engl. splitting field). Olkoon vielä $F := \mathbb{Q}(\alpha_{1,1}, \alpha_{1,2}, \ldots, \alpha_{1,d_1}, \alpha_{2,1}, \ldots, \alpha_{n,d_n})$ kunta, joka saadaan lisäämällä rationaalilukuihin kaikki juuret $\alpha_{i,j}$. Oletetaan, että $[F : \mathbb{Q}] = [F_1 : \mathbb{Q}][F_2 : \mathbb{Q}] \ldots [F_n : \mathbb{Q}]$. Tällöin*

$$\delta(S(P_1) \cap S(P_2) \cap \ldots \cap S(P_n)) = \delta(S(P_1))\delta(S(P_2))\ldots\delta(S(P_n))$$

Tapauksessa $n = 2$ tämä ehto on ekvivalenttia ehdon $F_1 \cap F_2 = \mathbb{Q}$ kanssa.

Frobeniuksen lauseen (esitetty lauseen 2 todistuksessa) nojalla $\delta(S(P))$ on aina rationaaliluku. Lause ei kuitenkaan kerro, esiintyvätkö kaikki rationaaliluvut (väliltä $[0, 1]$) jonkin polynomin alkutekijöiden tiheytenä. Lause 4 vastaa tähän kysymykseen.
Lause 4. *Olkoon $r \in \mathbb{Q} \cap [0, 1]$. On olemassa $P \in \mathbb{Z}[x]$, jolla $\delta(S(P)) = r$.*

Lauseiden todistuksissa käytettävät lemmat antavat enemmän tietoa alkutekijöistä kuin lauseet yksinään. Mielenkiintoisimmat alkeelliset lemmat ovat 1, 2 ja 10. 1 antaa tavan redusoida tekijöiden tutkiminen alkuluvun potensseihin tekijäjoukossa $S_d(P)$, 2 osoittaa väitteen $|S(P) \setminus S_v(P)| < \infty$, ja 10 osoittaa lauseen 1 variantin

joukkojen $S_d(P_i)$ yhdisteelle. Lauseen 2 todistuksessa esitetään kirjallisuudessa esitetty tulos $\delta(S(P)) \geq \frac{1}{\deg(P)}$ kaikilla $P \in \mathbb{Z}_*[x]$ [25]. Joukkojen $S(P_i)$ leikkauksien ja unionien yhdistelmien tiheyttä voidaan käsitellä lauseen 3 todistuksen menetelmillä samoin oletuksin kuin lauseessa 3.

Lopussa esitetään algoritmi lauseen 1 mukaisen D etsimiseksi tietokoneella, kun polynomeista P_i tehdään tietyt lisäoletukset.

Jatkotutkimuksena työn tuloksia voidaan soveltaa neliönjäännösten ja yleisten jäännösten tutkimiseen.

2 Lauseen 1 todistus

Lause 1 todistetaan vain tapauksessa $n = 2$, koska yleinen tapaus seuraa suoraan induktiolla. Ensiksi väite redusoidaan lemmojen 1-2 avulla vahvojen alkutekijöiden tutkimiseen, minkä jälkeen osoitetaan heikko versio lauseesta lemmojen 3-6 avulla. Tämän jälkeen esitetään lemmat 7-10, joiden avulla saadaan heikon version kanssa todistettua väite kokonaisuudessaan.

Lemma 1. *Olkoon $P \in \mathbb{Z}_*[x]$, ja olkoon $m = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, missä p_i ovat eri alkulukuja. $m \in S_d(P)$ jos ja vain jos $p_i^{a_i} \in S_d(P)$ kaikilla $1 \leq i \leq k$.*

Todistus. Jos $m \in S_d(P)$, pätee $p_i^{a_i} \in S_d(P)$ kaikilla i. Osoitetaan sitten väitteen toinen suunta. Oletetaan, että $p_i^{a_i} \in S_d(P)$ kaikilla i. Olkoon x_i sellainen, jolla $P(x_i) \equiv 0 \pmod{p_i^{a_i}}$. Kiinalaisen jäännöslauseen nojalla on olemassa sellainen x, jolla $x \equiv x_i \pmod{p_i^{a_i}}$ kaikilla i. Tällä x:n valinnalla pätee $P(x) \equiv P(x_i) \equiv 0 \pmod{p_i^{a_i}}$ kaikilla i, joten $m = p_1^{a_1} \ldots p_k^{a_k} \in S_d(P)$. Tämä todistaa väitteen toisen suunnan. □

Lemma 2. *Olkoon $D \in \mathbb{Z}_*[x]$. Tällöin on $p \in S(D) \implies p \in S_v(D)$ kaikilla paitsi äärellisen monella p.*

Todistus. Todistetään väite ensin, kun D ei jakaudu rationaaliluvuissa. Tällöin D:n derivaatalla D' ei ole yhteisiä tekijöitä D:n kanssa. Bezout'n lemman nojalla on olemassa $X, Y \in \mathbb{Z}[x]$ ja $N \in \mathbb{Z}_+$, joilla $DX + D'Y = N$.

Olkoon p mielivaltainen. Jos $p|D(n), D'(n)$ jollain p, tulee päteä $p|D(n)X(n) + D'(n)Y(n) = N$. Tämä tapahtuu vain äärellisen monessa tapauksessa. Poissuljetaan nämä p. Todistetaan, että lopuilla p pätee $p \in S(D) \implies p \in S_v(D)$.

Olkoon $p|D(x_1)$ jollain $x_1 \in \mathbb{Z}$, jolloin $p \nmid D'(x_1)$. Henselin lemman nojalla voidaan löytää sellainen x_2, jolla $p^2|D(x_2)$, ja $x_2 \equiv x_1 \pmod{p}$. Tällöin $D'(x_2) \equiv D'(x_1) \not\equiv 0 \pmod{p}$. Täten Henselin lemman nojalla voidaan löytää x_3, jolla $p^3|D(x_3)$, ja $x_3 \equiv x_1 \pmod{p}$. Jonoa voidaan jatkaa rajattoman pitkälle, joten p on D:n vahva alkutekijä. Tämä todistaa lemman jaottomilla D.

Olkoon nyt $D \in \mathbb{Z}_*[x]$ jaollinen polynomi. Kirjoitetaan $D = D_1 D_2 \ldots D_t$, missä $D_i \in \mathbb{Z}_*[x]$. Koska $p \in S(D) \implies p \in S(D_i)$ jollain i, pätee edellisen nojalla äärellisen montaa p lukuun ottamatta $p \in S(D_i) \implies p \in S_v(D_i) \implies p \in S_v(D)$. Täten lemman väite pätee myös jaollisilla polynomeilla D. □

Lemmat 1 ja 2 kertovat, että tärkeintä on tutkia vahvoja alkutekijöitä. Heikko versio keskittyy tähän. Heikon version esittämiseen ja myöhempiä todistuksia varten määritellään notaatio $\approx$ kahden joukon vertailemiselle.

Määritelmä 1. *Olkoot S_1 ja S_2 joukon $\mathbb{Z}_+$ osajoukkoja. Kirjoitetaan $S_1 \approx S_2$, jos on olemassa vain äärellisen monta p, jolla on olemassa k siten, että p^k kuuluu vain toiseen joukoista S_1, S_2.*

Todistettava heikompi versio on seuraava:

Heikko versio. *Olkoot $A, B \in \mathbb{Z}_*[x]$ jaottomia pääpolynomeja. On olemassa sellainen D, jolla $S_v(A) \cap S_v(B) \approx S_v(D)$ ja $S_v(A) \cap S_v(B) \subset S_v(D)$.*

2.1 Heikon version todistus

Lemma 3. *Olkoon $P \in \mathbb{Z}_*[x]$ jaoton, $P(\alpha) = 0$ ja $P(a) \equiv 0 \pmod{p^k}$ jollain $a \in \mathbb{Z}$. Oletetaan, että p ei jaa P:n korkeimman asteen termin kerrointa. Tällöin kaikilla $Q \in \mathbb{Z}_*[x]$, joilla $Q(\alpha) = 0$, pätee $Q(a) \equiv 0 \pmod{p^k}$.*

Todistus. Olkoon $0 \neq b \in \mathbb{Z}$ P:n korkeimman asteen termin kerroin. Koska P on jaoton, luvun α minimaalinen polynomi on $\frac{P}{b}$. Polynomilla Q on nollakohta α, joten se on jaollinen luvun α minimaalisella polynomilla, eli $\frac{P}{b}|Q$. Täten on olemassa $R \in \mathbb{Q}[x]$, jolla $Q = PR$. Osoitetaan vastaoletuksella, että polynomin R kertoimien nimittäjät eivät ole jaollisia p:llä.

Olkoot $P(x) = p_{d_P}x^{d_P} + \ldots + p_1x + p_0$, $Q(x) = q_{d_Q}x^{d_Q} + \ldots + q_0$, ja $R(x) = r_{d_R}x^{d_R} + \ldots + r_0$. Oletetaan, että on olemassa sellainen p, jolla p jakaa kertoimen r_i nimittäjän jollain i, ja valitaan näistä i suurin mahdollinen. Tutkitaan termin x^{d_P+i} kerrointa polynomissa Q. Tämä on määritelmän nojalla q_{d_P+i}, mikä on kokonaisluku. Toinen esitys kertoimelle saadaan ehdosta $Q = PR$, eli kerroin on myös

$$r_i p_{d_P} + r_{i+1} p_{d_P-1} + \ldots$$

Kirjoitetaan $r_{i+j}p_{d_P-j} = \frac{x_j}{y_j}$, missä $x_j, y_j \in \mathbb{Z}$ ovat yhteistekijättömiä. Oletusten nojalla pätee $p|y_0$, mutta $p \nmid y_i$ kun $i > 0$. Summa voidaan kirjoittaa muodossa

$$\frac{x_0}{y_0} + \frac{x_1}{y_1} + \ldots = \frac{x_0y_1y_2\cdots + x_1y_0y_2y_3\cdots + \ldots}{y_0y_1y_2\cdots}$$

Tämän rationaaliluvun nimittäjä on jaollinen luvulla y_0, joten se on jaollinen luvulla p. Osoittajan jokainen summattava termi lukuun ottamatta ensimmäistä on jaollinen luvulla y_0 eli myös p:llä. Mutta $p \nmid x_0y_1y_2\cdots$ luvun p ja indeksin i määritelmien nojalla, joten termin x^{d_P+i} kerroin ei ole kokonaisluku, mikä on ristiriita. Siis polynomin R kertoimet eivät ole jaollisia p:llä.

Yhtälön $Q = PR$ nojalla pätee $Q(a) = P(a)R(a)$. Luku $R(a)$ on rationaaliluku, jonka nimittäjä ei edellisen päättelyn nojalla ole jaollinen p:llä. On siis olemassa kokonaisluku $t \equiv R(a)^{-1} \pmod{p^k}$, jolla $Q(a)t \equiv P(a) \equiv 0 \pmod{p^k}$. Koska t ei ole jaollinen p:llä, pätee $Q(a) \equiv 0 \pmod{p^k}$. □

Olkoon $T = \{1, \alpha, \alpha^2, \ldots, \alpha^{\deg(D)-1}\}$ vektoriavaruuden $\mathbb{Q}(\alpha)$ kanta. Määritellään $\mathbb{Z}^p(\alpha)$ olemaan niiden $r \in \mathbb{Q}(\alpha)$ joukko, joiden esitys kannan T avulla sisältää vain rationaalilukuja, joiden nimittäjä ei ole jaollinen p:llä. Jos p ei jaa polynomin α minimaalisen polynomin minkään kertoimen nimittäjää, on $\mathbb{Z}^p(\alpha)$ rengas, koska α:n minimaalisen polynomin kertoimet voidaan tällöin tulkita kokonaislukuina renkaassa $\mathbb{Z}_p$. Lemma 4 käsittelee rengashomomorfismeja, jotka on määritelty viitteen [22] luvussa 3.

Lemma 4. *Olkoon $P \in \mathbb{Z}_*[x]$ jaoton. Olkoon $P(a) \equiv 0 \pmod{p^k}$ jollain $a \in \mathbb{Z}$, missä p ei jaa P:n korkeimman asteen termin kerrointa. Olkoon $P(\alpha) = 0$. On olemassa rengashomomorfismi $\phi : \mathbb{Z}^p(\alpha) \to \mathbb{Z}_{p^k}$, jolla $\phi(\alpha) = a$.*

Todistus. Määritellään $\phi(Q(\alpha)) \equiv Q(a) \pmod{p^k}$, kaikilla $Q \in \mathbb{Q}[x]$, joiden kertoimet eivät ole jaollisia p:llä. Tässä määritelmässä $Q(a)$ tulkitaan kokonaislukuna modulo p^k.

Selvästi ϕ on additiivinen ja multiplikatiivinen, sekä $\phi(1) \equiv 1 \pmod{p^k}$. Osoitetaan vielä, että ϕ on hyvin määritelty, eli jos $Q_1(\alpha) = Q_2(\alpha)$, niin $Q_1(a) \equiv Q_2 \pmod{p^k}$. Olkoon $Q := Q_1 - Q_2$. Tulee osoittaa $Q(\alpha) = 0 \implies Q(a) \equiv 0 \pmod{p^k}$. Q voidaan kertoa sen nimittäjien tulolla, jolloin todistettavana on ekvivalentti väite $Q_*(\alpha) = 0 \implies Q_*(a) \equiv 0 \pmod{p^k}$, missä $Q_* \in \mathbb{Z}[x]$. Tämä pätee lemman 3 nojalla. Täten lemman väite pätee. □

Olkoon α jokin polynomin A juuri. Kirjoitetaan $B = E_1E_2\ldots E_t$, missä $E_i \in \mathbb{Q}_*[x, \alpha]$ ovat kunnassa $\mathbb{Q}(\alpha)$ jaottomia pääpolynomeja, ja olkoon β_i polynomin E_i jokin juuri. Kaikilla $1 \leq i \leq t$ on olemassa sellainen $n_i \in \mathbb{Z}_+$, jolla $\mathbb{Q}(\alpha, \beta_i) = \mathbb{Q}(\alpha + n_i\beta_i)$ [23]. Olkoon D_i luvun $\alpha + n_i\beta_i$ minimaalinen polynomi kunnassa $\mathbb{Q}$. Luvut α, β_i ovat algebrallisia kokonaislukuja, toisin sanoen niiden minimaalisten polynomien kertoimet ovat kokonaislukuja. Koska algebralliset kokonaisluvut ovat rengas [24] (korollaari 1.4.), on myös D_i kokonaislukukertoiminen polynomi.

Valitaan $D = D_1D_2\ldots D_t$. Osoitetaan, että tällä D on heikon version väitteen ominaisuudet. Koska $D_i \in \mathbb{Z}_*[x]$, on $D \in \mathbb{Z}_*[x]$.

Lemma 5. $S_v(A) \cap S_v(B) \subset S_v(D)$.

Todistus. Olkoot $p \in S_v(A) \cap S_v(B)$ ja $k \in \mathbb{Z}_+$ mielivaltaisia. Olkoot $a_k, b_k \in \mathbb{Z}$ sellaisia, joilla $A(a_k) \equiv B(b_k) \equiv 0 \pmod{p^k}$, ja olkoon $\phi = \phi_k$ rengashomomorfismi $\mathbb{Z}^p(\alpha) \to \mathbb{Z}_{p^k}$, jolla $\phi(\alpha) = a_k$. Tällainen ϕ on olemassa lemman 4 nojalla.

Tutkitaan polynomia $D_i(\alpha + n_i x)$. Tämä on polynomi, jonka kertoimet ovat kunnassa $\mathbb{Q}(\alpha)$, ja jolla on juuri β_i. Täten se on jaollinen luvun β_i minimaalisella polynomilla (kunnassa $\mathbb{Q}(\alpha)$), eli polynomilla E_i. Siis on olemassa $F_i \in \mathbb{Q}(\alpha)[x]$, jolla $D_i(\alpha + n_i x) = E_i(x)F_i(x)$.

Olkoon $D_*(x) := \prod D_i(\alpha + n_i x)$, ja olkoon $F \in \mathbb{Q}(\alpha)[x]$ polynomien F_i tulo. Tällöin $D_*(x) = B(x)F(x)$. On olemassa sellainen $C \in \mathbb{Z}_+$, jolla polynomin $G(x) := CF(x)$ kertoimet kuuluvat renkaaseen $\mathbb{Z}^p(\alpha)$. Tällöin $CD_*(x) = B(x)G(x)$. Sijoitetaan tähän yhtälöön $x = b_k$ ja kuvataan molemmat puolet homomorfismilla ϕ, jolloin saadaan

$$0 \equiv \phi(B(b_k)) \equiv \phi(B(b_k))\phi(G(b_k)) \equiv \phi(CD_*(b_k)) \equiv C\prod \phi(D_i(\alpha + n_i b_k)) \equiv C\prod D_i(a_k + n_i b_k) \pmod{p^k}$$

Polynomien $D_i(\alpha + n_i x)$ kertoimet kuuluvat renkaaseen $\mathbb{Z}^p(\alpha)$ ja polynomin $D_i(x)$ kertoimet ovat kokonaislukuja, minkä vuoksi yhtälöketju $\phi(CD_*(b_k)) \equiv C\prod \phi(D_i(\alpha + n_i b_k)) \equiv C\prod D_i(a_k + n_i b_k) \pmod{p^k}$ pätee ja on hyvin määritelty.

Osoitetaan lemman väite vastaoletuksella. Oletetaan, että p ei ole polynomin D vahva alkutekijä, jolloin $p \notin S_v(D_i)$ kaikilla i. Täten kaikilla i on olemassa sellainen c_i, jolla $p^{c_i+1} \notin S_d(D_i)$. Olkoon vielä c suurin luvun p potenssi, joka jakaa luvun C. C ei riipu luvuista p, k, a_k, b_k, joten myös c on vakio. Valitaan $k = c + c_1 + c_2 + \ldots + c_t + 1$. Yhtälö $0 \equiv C\prod D_i(a_k + n_i b_k) \pmod{p^k}$ ei tällöin voi päteä, koska yhtälön oikea puoli on kokonaisluku, joka ei ole jaollinen luvulla p^k. Vastaoletus johtaa ristiriitaan, joten lemman väitteen tulee päteä. □

Osoitetaan vielä heikon version toinen osuus, eli $S_v(A) \cap S_v(B) \approx S_v(D)$. Tämän osoittaa seuraava lemma, joka on esitetty myös artikkelissa [9] (lause 2).

Lemma 6. *Olkoot $A, B \in \mathbb{Z}_*[x]$ jaottomia, ja olkoot α, β niiden juuria. Olkoon γ sellainen, jolla $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$, ja olkoon D luvun γ minimaalinen polynomi. Kaikilla paitsi äärellisen monella p pätee väite $p^k \in S_d(D) \implies p^k \in S_d(A) \cap S_d(B)$ kaikilla $k \in \mathbb{Z}_+$.*

Todistus. Osoitetaan ensin, että on olemassa polynomit $A_*, B_* \in \mathbb{Q}[x]$, joilla $D(x)|A(A_*(x)), B(B_*(x))$.

Olkoon $d = \deg(D)$. $\mathbb{Q}$-vektoriavaruudella $\mathbb{Q}(\gamma)$ on kanta $\{1, \gamma, \ldots, \gamma^{d-1}\}$. Jokainen vektoriavaruuden alkio voidaan esittää kannan alkioiden lineaarikombinaationa. Luku α kuuluu kuntaan $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$, joten on olemassa rationaaliluvut $a_0, a_1, \ldots, a_{d-1}$, joilla $\alpha = a_0 + a_1\gamma + \ldots + a_{d-1}\gamma^{d-1}$. Valitaan $A_*(x) = a_0 + a_1 x + \ldots + a_{d-1}x^{d-1}$. Tällöin polynomilla $A(A_*(x))$ on juuri γ, joten se on jaollinen luvun γ minimaalisella polynomilla D. Täten $D(x)|A(A_*(x))$. Vastaavasti voidaan löytää $B_*(x) \in \mathbb{Q}[x]$, jolla $D(x)|B(B_*(x))$.

Täten on olemassa polynomi $P \in \mathbb{Q}[x]$, joilla $A(A_*(x)) = D(x)P(x)$. Tutkitaan niitä p, jotka eivät jaa polynomien A_* ja P minkään kertoimen nimittäjää. Osoitetaan, että näillä p pätee $p^k \in S_d(D) \implies p^k \in S_d(A)$ kaikilla $k \in \mathbb{Z}_+$. Oletetaan, että $D(m) \equiv 0 \pmod{p^k}$. Tällöin $A(A_*(m)) \equiv D(m)P(m) \equiv 0 \pmod{p^k}$, koska $P(m)$ on rationaaliluku, jonka nimittäjä ei ole jaollinen p:llä. Täten yhtälöllä $A(x) \equiv 0 \pmod{p^k}$ on rationaalinen ratkaisu $x = A_*(m)$. $A_*(m)$:n nimittäjä ei ole jaollinen p:llä, minkä vuoksi se voidaan tulkita kokonaislukuna modulo p^k. Täten yhtälöllä $A(x) \equiv 0 \pmod{p^k}$ on kokonaislukuratkaisu, joten $p^k \in S_d(A)$.

Vastaavasti voidaan osoittaa, että poislukien äärellisen monta p pätee $p^k \in S_d(D) \implies p^k \in S_d(B)$. Tämä todistaa väitteen. □

Siispä jos $p \in S_v(D)$, pätee $p \in S_v(D_i)$ jollain i. Tällöin lemman 6 nojalla kaikilla paitsi äärellisen monella p pätee $p \in S_v(A) \cap S_v(B)$. Tämä todistaa osan $S_v(A) \cap S_v(B) \approx S_v(D)$ heikosta versiosta yhdessä lemman 5 kanssa.

2.2 Yleisen tapauksen todistus

Ensimmäisenä osoitetaan, että jos on olemassa melkein toimiva D, niin tämä voidaan muuttaa täysin toimivaksi polynomiksi. Tämän jälkeen osoitetaan lauseen väite jaottomille polynomeille, minkä jälkeen tulos laajennetaan kaikille polynomeille.

Lemma 7. *Olkoot $A, B \in \mathbb{Z}_*[x]$ polynomeja. Oletetaan, että on olemassa sellainen polynomi $D \in \mathbb{Z}_*[x]$, jolla $S_v(A) \cap S_v(B) \approx S_v(D)$, ja lisäksi $S_v(A) \cap S_v(B) \subset S_v(D)$. Tällöin on olemassa sellainen $D_* \in \mathbb{Z}_*[x]$, jolla $S_d(D_*) = S_d(A) \cap S_d(B)$.*

Todistus. Esitetään transformaatioita, joilla D voidaan muuttaa sellaiseksi D_*, jolla $S_d(D_*) = S_d(A) \cap S_d(B)$. Tutkitaan niitä p, joilla on olemassa jokin $k \in \mathbb{Z}_+$, jolla p^k kuuluu täsmälleen toiseen joukoista $S_d(A) \cap S_d(B)$ ja $S_d(D)$. Koska $S_v(A) \cap S_v(B) \approx S_v(D)$, lemmojen 1 ja 2 nojalla $S_d(A) \cap S_d(B) \approx S_d(D)$, joten näitä p on vain äärellisen monta. Jaetaan nämä p kahteen eri kategoriaan:

Tapaus 1. On olemassa sellainen k, jolla $p^k \in S_d(A) \cap S_d(B)$, mutta $p^k \notin S_d(D)$. Tällöin $p \notin S_v(D)$, joten ehdon $S_v(A) \cap S_v(B) \subset S_v(D)$ nojalla pätee $p \notin S_v(A) \cap S_v(B)$. Täten on olemassa sellainen $m \in \mathbb{Z}_+$, jolla $p^m \in S_d(A) \cap S_d(B)$, mutta $p^{m+1} \notin S_d(A) \cap S_d(B)$. Lisäksi on olemassa sellainen $t < m$, jolla $p^t \in S_d(D)$ ja $p^{t+1} \notin S_d(D)$. Muodostetaan nyt polynomi D_p asettamalla $D_p(x) := p^{m-t}D(x)$. Tällöin $p^m \in S_d(D_p)$, mutta $p^{m+1} \notin S_d(D_p)$.

Osoitetaan vielä, että polynomeilla D_p ja D on muuten samat alkulukujen potenssit tekijöinään, eli kaikilla alkuluvuilla $q \neq p$ pätee $q^s \in S_d(D_p) \Leftrightarrow q^s \in S_d(D)$. Oletetaan ensin, että pätee $q^s \in S_d(D)$ jollain q, s. Tällöin pätee $q^s \in S_d(D_p)$ polynomin D_p määritelmän nojalla. Oletetaan sitten, että pätee $q^s \in S_d(D_p)$. Tällöin on olemassa sellainen $y \in \mathbb{Z}$, jolla $D_p(y) \equiv 0 \pmod{q^s}$, joten $p^{m-t}D(y) \equiv 0 \pmod{q^s}$. Koska $p \neq q$, pätee nyt $D(y) \equiv 0 \pmod{q^s}$, eli $q^s \in S_d(D)$.

Tapaus 2. On olemassa sellainen k, jolla $p^k \notin S_d(A) \cap S_d(B)$, mutta $p^k \in S_d(D)$. Osoitetaan ensin, että on olemassa sellainen $D_p \in \mathbb{Z}_*[x]$, jolla $q^s \in S_d(D) \Leftrightarrow q^s \in S_d(D_p)$ kaikilla $s \geq 0$ ja alkuluvuilla $q \neq p$, ja jolla lisäksi pätee $p \notin S_d(D_p)$.

Koska D ei ole nollapolynomi, on olemassa $c \in \mathbb{Z}$, jolla $D(c) \neq 0$. Olkoon $D_c(x) = D(x + c)$. Tällöin $D_c(0) \neq 0$, ja $S_d(D) = S_d(D_c)$, koska yhtälöllä $D(x) \equiv 0 \pmod{m}$ on ratkaisu jos ja vain jos yhtälöllä $D_c(x) \equiv 0 \pmod{m}$ on ratkaisu. Muuttamalla D:n polynomiksi D_c joukko $S_d(D)$ ei muutu, ja voidaan olettaa, että $D(0) \neq 0$.

Olkoon $t \in \mathbb{Z}$ sellainen, jolla $p^t | D(0)$, mutta $p^{t+1} \nmid D(0)$. Määritellään nyt

$$D_p(x) := \frac{D(p^{t+1}x)}{p^t}$$

Osoitetaan, että $D_p \in \mathbb{Z}_*[x]$, ja lisäksi se, että kaikki polynomin D_p kertoimet ovat vakiotermiä lukuun ottamatta jaollisia luvulla p. Tutkitaan polynomin D yksittäistä termiä $d_i x^i$. Tässä $d_i \in \mathbb{Z}$, koska $D \in \mathbb{Z}_*[x]$. Tällöin polynomin D_p termin x^i kerroin on $p^{i(t+1)-t}d_i x^i$. Tämä on luvulla p jaollinen kokonaisluku kaikilla $i > 0$, mutta p:llä jaoton kokonaisluku, kun $i = 0$. Täten $D_p \in \mathbb{Z}_*[x]$, ja $p \notin S_d(D_p)$.

Todistetaan vielä, että $q^s \in S_d(D) \Leftrightarrow q^s \in S_d(D_p)$ kaikilla alkuluvuilla $q \neq p$. On selvää, että $q^s \in S_d(D_p) \implies q^s \in S_d(D)$. Oletetaan sitten, että $q^s \in S_d(D)$, ja olkoon x sellainen, jolla $D(x) \equiv 0 \pmod{q^s}$. Kiinalaisen jäännöslauseen nojalla on olemassa sellainen y, jolla $y \equiv x \pmod{q^s}$ ja $y \equiv 0 \pmod{p^{t+1}}$. Valitaan jokin tällainen y, ja kirjoitetaan $y = p^{t+1}z$, missä $z \in \mathbb{Z}$. Tällöin

$$0 \equiv p^{-t}D(x) \equiv p^{-t}D(y) = p^{-t}D(p^{t+1}z) = D_p(z) \pmod{q^s}$$

eli $0 \equiv D_p(z) \pmod{q^s}$, joten $q^s \in S_d(D_p)$.

Polynomi D_p voidaan nyt muuttaa sellaiseksi D_{p_*}, jolla $p^k \in S_d(A) \cap S_d(B) \Leftrightarrow p^k \in S_d(D_{p_*})$, ja jolla lisäksi $q^s \in S_d(D_{p_*}) \Leftrightarrow q^s \in S_d(D)$ kertomalla D_p sopivalla luvun p potenssilla kuten tapauksessa 1.

Suorittamalla tapausten 1 ja 2 esittämät muunnokset polynomille D kaikilla äärellisen monella tutkittavalla p saadaan muodostettua sellainen D_*, jolla $p^k \in S_d(A) \cap S_d(B) \Leftrightarrow p^k \in S_d(D_*)$ kaikilla p, k. Lemman 1 nojalla pätee $S_d(D_*) = S_d(A) \cap S_d(B)$, mikä todistaa lemman väitteen. □

Lemma 8. *Olkoon $P \in \mathbb{Z}_*[x]$ annettu. On olemassa pääpolynomi $Q \in \mathbb{Z}_*[x]$, jolla $S_d(P) \approx S_d(Q)$ ja $S_v(P) \subset S_v(Q)$.*

Todistus. Olkoon c_i polynomin P termiä x^i vastaava kerroin, ja olkoon $d = \deg(P)$. Valitaan

$$Q(x) := c_d^{d-1} P(\frac{x}{c_d})$$

Osoitetaan, että tämä Q toteuttaa lemman ehdot.

Osoitetaan ensin, että Q on kokonaislukukertoiminen pääpolynomi. Polynomin Q termiä x^i vastaavan termin kerroin on $c_d^{d-1-i} c_i$. Kun $i = d$, on tämä 1, joten Q on pääpolynomi. Muussa tapauksessa $i \leq d-1$, jolloin kerroin on kokonaisluku. Täten $Q \in \mathbb{Z}_*[x]$.

Osoitetaan sitten, että $S_v(P) \subset S_v(Q)$. Valitaan jokin $p \in S_v(P)$. Olkoon $k \in \mathbb{Z}_+$ mielivaltainen, ja olkoon x_k sellainen, jolla $P(x_k) \equiv 0 \pmod{p^k}$. Tällöin $Q(c_d x_k) = c_d^{d-1} P(x_k) \equiv 0 \pmod{p^k}$. Täten $p^k \in S_d(Q)$. Siis $p^k \in S_d(Q)$ mielivaltaisella $k \in \mathbb{Z}_+$, joten $p \in S_v(Q)$. Täten $S_v(P) \subset S_v(Q)$.

Lopuksi todistetaan, että $S_d(P) \approx S_d(Q)$. Tutkitaan vain niitä p, joilla $p \nmid c_d$. Edellä osoitettiin, että $p^k \in S_d(P) \implies p^k \in S_d(Q)$. Osoitetaan vielä, että $p^k \in S_d(Q) \implies p^k \in S_d(P)$. Olkoon $Q(x_k) \equiv 0 \pmod{p^k}$. Kiinalaisen jäännöslauseen nojalla on olemassa sellainen y_k, jolla $y_k \equiv x_k \pmod{p^k}$ ja $y_k \equiv 0 \pmod{c_d}$. Kirjoitetaan $y_k = c_d z_k$. Tällöin, $0 \equiv Q(x_k) \equiv Q(y_k) = Q(c_d z_k) = c_d^{d-1} P(z_k) \pmod{p^k}$. Koska $p \nmid c_d$, pätee $P(z_k) \equiv 0 \pmod{p^k}$. Täten $p^k \in S_d(P)$.

Edellisten huomioiden nojalla lemman ehdot täyttyvät valitulla Q. □

Osoitetaan sitten, että lauseen väite pätee jaottomilla $A, B \in \mathbb{Z}_*[x]$.

Lemma 9. *Olkoot $A, B \in \mathbb{Z}_*[x]$ jaottomia. Tällöin on olemassa sellainen D, jolla $S_d(A) \cap S_d(B) = S_d(D)$.*

Todistus. Jos A, B ovat pääpolynomeja, on heikon version nojalla olemassa sellainen D, jolla $S_v(A) \cap S_v(B) \approx S_v(D)$ ja $S_v(A) \cap S_v(B) \subset S_v(D)$. Lemman 7 nojalla on olemassa sellainen D_*, jolla $S_d(A) \cap S_d(B) = S_d(D_*)$. Väite siis pätee pääpolynomeilla A, B.

Olkoot A, B nyt mielivaltaisia jaottomia polynomeja. Olkoot A_*, B_* kuten lemmassa 8 polynomeille A, B. Edellisen nojalla on olemassa sellainen D_*, jolla $S_d(A_*) \cap S_d(B_*) = S_d(D_*)$. Polynomien A_*, B_* valinnan nojalla $S_d(A) \cap S_d(B) \approx S_d(A_*) \cap S_d(B_*) = S_d(D_*)$ ja $S_v(A) \cap S_v(B) \subset S_v(A_*) \cap S_v(B_*) = S_v(D_*)$. Täten lemman 7 ehdot täyttyvät polynomiparille A, B, joten on olemassa sellainen D, jolla $S_d(A) \cap S_d(B) = S_d(D)$. □

Todistetaan sitten, että lauseen väite pätee myös jaollisilla A, B. Tätä varten todistetaan ensin lausetta vastaava versio polynomien tekijäjoukkojen yhdisteelle.

Lemma 10. *Olkoot $P_1, P_2, \ldots, P_n \in \mathbb{Z}_*[x]$. On olemassa sellainen D, jolla $S_d(D) = S_d(P_1) \cup S_d(P_2) \cup \ldots \cup S_d(P_n)$.*

Todistus. Tapauksessa $n = 2$ voidaan valita $D = P_1 P_2$: on selvää, että $S_v(D) = S_v(P_1) \cup S_v(P_2)$, joten lemman 7 muunnoksilla D voidaan muuttaa halutunlaiseksi. Yleinen tapaus seuraa helposti induktiolla. □

Todistetaan nyt lause 1.

Todistus. Kirjoitetaan $A = A_1 A_2 \ldots A_t$, missä $A_i \in \mathbb{Z}_*[x]$ ovat jaottomia, ja vastaavasti $B = B_1 B_2 \ldots B_s$. Lemman 9 nojalla jokaisella parilla (i, j) on olemassa sellainen $D_{(i,j)}$, jolla $S_d(D_{(i,j)}) = S_d(A_i) \cap S_d(B_j)$.

Olkoon D sellainen, jolla

$$S_d(D) = \bigcup_{(i,j)} S_d(D_{(i,j)})$$

Tällainen on olemassa lemman 10 nojalla.

Osoitetaan, että $S_v(D) = S_v(A) \cap S_v(B)$. Jos $p \in S_v(A) \cap S_v(B)$, on olemassa sellaiset i, j, joilla $p \in S_v(A_i) \cap S_v(B_j) \implies p \in S_v(D_{(i,j)}) \implies p \in S_v(D)$. Täten $S_v(A) \cap S_v(B) \subset S_v(D)$. Vastaavasti jos $p \in S_v(D)$, niin $p \in S_v(D_{(i,j)})$ jollain i, j, joten $p \in S_v(A_i) \cap S_v(B_j) \implies p \in S_v(A) \cap S_v(B)$.

Täten $S_v(A) \cap S_v(B) = S_v(D)$. Lemman 7 nojalla on olemassa sellainen D_*, jolla $S_d(A) \cap S_d(B) = S_d(D_*)$. Tämä todistaa lauseen väitteen. □

Osoitetaan vielä yläraja polynomin D asteelle. Osoitetaan, että $\deg(D) \leq \deg(A)\deg(B)$, jolloin induktiolla saadaan osoitettua yleisen tapauksen raja $\deg(D) \leq \deg(P_1)\dots\deg(P_n)$. Osoitetaan ensin yläraja, kun A ja B ovat jaottomia. Lemmassa 9 muodostettu polynomi D on, käyttäen heikon version todistuksen notaatioita, asteeltaan enintään $\deg(D_1) + \deg(D_2) + \ldots + \deg(D_t)$. Polynomi D_i on luvun $\alpha + n_i\beta_i$ minimaalinen polynomi, joten sen aste on $[\mathbb{Q}(\alpha, \beta_i) : \mathbb{Q}] = [(\mathbb{Q}(\alpha)(\beta_i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(E_i)\deg(A)$. Täten $\deg(D) \leq \sum \deg(A)\deg(E_i) = \deg(A)\sum \deg(E_i) = \deg(A)\deg(B)$. Yleisen tapauksen todistuksessa esitetyt transformaatiot eivät muuta polynomin D astetta. Täten väite pätee jakautumattomilla A, B.

Lemmassa 10 luotu polynomi D, jolla $S_d(D) = S_d(A) \cup S_d(B)$ toteuttaa ehdon $\deg(D) = \deg(A) + \deg(B)$. Tämän avulla saadaan todistettua yläraja jaollisten polynomien tapauksessa: jos $A = A_1A_2\dots A_t$ ja $B = B_1B_2\dots B_s$, todistuksessa esitetyn D aste on

$$\deg(D) \leq \sum_{(i,j)} \deg(A_i)\deg(B_j) = \sum_i \deg(A_i) \cdot \sum_j \deg(B_j) = \deg(A)\deg(B)$$

Täten $\deg(D) \leq \deg(A)\deg(B)$, joten yleisesti $\deg(D) \leq \deg(P_1)\deg(P_2)\dots\deg(P_n)$.

Rajan tiukkuus osoitetaan lauseen 2 todistuksen lopussa.

3 Lauseen 2 todistus

Olkoon D lauseen 1 mukaisesti sellainen, jolla $S_d(D) = S_d(P_1) \cap S_d(P_2) \cap \ldots \cap S_d(P_n)$. Tämä D voidaan valita niin, että $\deg(D) \leq \deg(P_1)\deg(P_2)\dots\deg(P_n)$. Osoitetaan, että $\delta(S(D))$ on olemassa ja vähintään $\deg(D)^{-1}$. Tämä todistaa väitteen, koska lemman 2 nojalla pätee $\delta(S_v(D)) = \delta(S(D))$.

Lemma 11. *$\delta(S(D))$ on olemassa, ja $\delta(S(D)) \geq \deg(D)^{-1}$ kaikilla $D \in \mathbb{Z}_*[x]$.*

Todistus. Väite on todistettu viitteessä [25] (lemma 3) jaottomille pääpolynomeille D. Todistus toimii myös jaollisille polynomeille D. Lemman 8 nojalla väite pätee myös muilla kuin pääpolynomeilla. □

Seuraavaksi esitetään Frobeniuksen lause, koska sitä käytetään viitteen [25] todistuksessa lemmalle 11 sekä lauseen 3 todistuksessa. Lauseita varten määritellään polynomin Galois'n ryhmä ja jakautuminen alkuluvuissa.

Määritelmä 2. *Olkoon polynomin $D \in \mathbb{Q}[x]$ juuret $\alpha_1, \dots, \alpha_n$, ja olkoon $K = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$. Polynomin D Galois'n ryhmä $G = G(D)$ on niiden kuvausten $\sigma : K \to K$ joukko, jotka ovat isomorfismeja [26].*

Huomautus. *Nimitys Galois'n ryhmä tulee siitä, että G on ryhmä operaation $\circ$ suhteen: jos $\sigma_1, \sigma_2 \in G$, niin kuvaus $\sigma(x) := \sigma_1(\sigma_2(x))$ kuuluu joukkoon G. Lisäksi jokaisella alkiolla on käänteisalkio, ja neutraalialkiona toimii identiteettikuvaus.*

Jokainen $\sigma \in G$ voidaan määrittää yksikäsitteisesti, kun on annettu $\sigma(\alpha_i) \forall i$, koska jokainen K:n alkio voidaan esittää rationaalilukukertoimisena polynomina muuttujista $\alpha_1, \dots, \alpha_n$. Lisäksi $\sigma(\alpha_i)$ kuvautuu aina joksikin

polynomin D juurista, koska $0 = \sigma(0) = \sigma(D(\alpha_i)) = \sigma(a_0 + a_1\alpha_i + \ldots + a_d\alpha_i^d) = a_0 + a_1\sigma(\alpha_i) + \ldots + a_d\sigma(\alpha_i)^d = D(\sigma(\alpha_i))$, missä $a_i \in \mathbb{Q}$ ovat D:n kertoimet.

Siispä jokainen $\sigma \in G$ permutoi D:n juurien joukkoa $S = \{\alpha_1, \ldots, \alpha_d\}$. σ voi jakaa joukon S pienempiin joukkoihin $T_1, T_2, \ldots, T_k$, joilla $\sigma(t_i) \in T_i, \forall t_i \in T_i, \forall i$. Valitaan mahdollisista kokoelmista $\{T_1, \ldots, T_k\}$ se, joka maksimoi joukkojen määrän k. Olkoon $T(\sigma) := \{|T_1|, |T_2|, \ldots, |T_k|\}$ joukko, missä sama luku voi esiintyä monta kertaa.

Polynomien jakautumisesta modulo alkuluku esitetään lausetta varten seuraavat määritelmät.

Määritelmä 3. *Olkoon p alkuluku, ja olkoot $P, Q \in \mathbb{Z}[x]$. Sanotaan, että $P \equiv Q \pmod{p}$, jos $\deg(P) = \deg(Q)$, ja $P - Q$ on polynomi, jonka kaikki kertoimet ovat jaollisia p:llä.*

Määritelmä 4. *Olkoon p alkuluku, ja olkoon $P \in \mathbb{Z}[x]$. Sanotaan, että P on jaoton modulo p, jos ei ole olemassa $Q, R \in \mathbb{Z}_*[X]$, joilla $P \equiv QR \pmod{p}$.*

Määritelmä 5. *Olkoon p alkuluku, ja olkoon $P \in \mathbb{Z}[x]$ pääpolynomi. Sanotaan, että P jakautuu polynomeiksi, joiden asteet ovat $a_1, a_2, \ldots, a_k$ modulo p, jos on olemassa pääpolynomit $P_1, P_2, \ldots, P_k$, jotka toteuttavat seuraavat ehdot:*

- *P_i on jaoton modulo p kaikilla i.*
- *$P \equiv P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k} \pmod{p}$*
- *$P_i \not\equiv P_j \pmod{p}$ kaikilla $i \neq j$.*

Frobeniuksen lause yhdistää polynomin D jakautumisen modulo p sen Galois'n ryhmän kuvausten σ joukkoihin $T(\sigma)$, kun $D \in \mathbb{Z}_*[x]$ on pääpolynomi.

Frobeniuksen lause. *Olkoon $D \in \mathbb{Z}_*[x]$ pääpolynomi. Olkoon k positiivinen kokonaisluku, ja olkoot $a_1, \ldots, a_k \in \mathbb{Z}_+$ sellaisia, joilla $a_1 + \ldots + a_k = \deg(D)$. Olkoon S niiden p joukko, joilla D jakautuu täsmälleen k polynomiksi modulo p, joiden asteet ovat $a_1, \ldots, a_k$. Olkoon $N(\{a_1, \ldots, a_k\})$ niiden $\sigma \in G(D)$ joukko, joilla $T(\sigma) = \{a_1, \ldots, a_k\}$. Tällöin*

$$\delta(S) = \frac{|N(\{a_1, \ldots, a_k\})|}{|G(D)|}$$

Todistus Frobeniuksen lauseelle on esitetty viitteessä [27] (s. 165-166). Lähteessä on kuitenkin todistettu väite heikompana versiona, missä luonnollinen tiheys δ on korvattu Dirichlet'n tiheydellä. Frobeniuksen lause on erikoistapaus vahvemmasta ja vaikeammasta Chebotarevin tiheyslauseesta, jonka todistus luonnolliselle tiheydelle löytyy viitteestä [28] (luku 6).

Osoitetaan sitten, että lauseen 2 alaraja tiheydelle on tiukka. Olkoon $P_1 = \Phi_k$, missä Φ_k kuvaa k:tta syklotomista polynomia. Tällöin $\deg(P_1) = \phi(n)$, missä ϕ on Eulerin fii-funktio, ja äärellisen montaa p lukuun ottamatta pätee $p \in S(\Phi_n) \implies p \equiv 1 \pmod{n}$ [29] (lause 5.4.). Niiden p tiheys, joilla $p \equiv 1 \pmod{n}$, on $\frac{1}{\phi(n)}$ [30]. Täten $\delta(S_v(P_1)) = \delta(S(P_1)) \leq \frac{1}{\phi(n)}$. Esimerkkinä rajan tiukkuudesta monelle polynomille toimii valinta $P_i = \Phi_{p_i}$, missä p_i ovat eri alkulukuja. Tämän toimivuus voidaan osoittaa kuten edellä käyttäen apuna kiinalaista jäännöslausetta. Lauseen 1 yläraja polynomin D asteelle on myös tiukka: valitsemalla polynomit P_i niin, että $\delta(S_v(P_1) \cap \ldots \cap S_v(P_n)) = \Big(\deg(P_1) \ldots \deg(P_n)\Big)^{-1}$, tulee lemman 11 nojalla päteä $\deg(D) \geq \deg(P_1) \ldots \deg(P_n)$.

4 Lauseen 3 todistus

Osoitetaan seuraava väite vahvalla induktiolla muuttujan n suhteen.

Olkoot $P_1, \ldots, P_n, F_1, \ldots, F_n, F$ kuten lauseessa 3, ja oletetaan, että $[F : \mathbb{Q}] = [F_1 : \mathbb{Q}] \ldots [F_n : \mathbb{Q}]$. Tällöin

$$\delta(S(P_1) \cap \ldots \cap S(P_n)) = \delta(S(P_1)) \ldots \delta(S(P_n))$$

ja

$$\delta(S(P_1) \cup \ldots \cup S(P_n)) = 1 - \Big(1 - \delta(S(P_1))\Big)\Big(1 - \delta(S(P_2))\Big) \ldots \Big(1 - \delta(S(P_n))\Big)$$

Huomaa, että tiheydet ovat olemassa lauseen 1 ja lemmojen 10 ja 11 nojalla.

Tapauksessa $n = 1$ väite on selvä. Osoitetaan väite tapauksessa $n = 2$, minkä jälkeen suoritetaan induktioaskel.

Todistetaan ensin, että $\delta(S(P_1) \cup S(P_2)) = \delta(S(P_1)) + \delta(S(P_2)) - \delta(S(P_1))\delta(S(P_2))$. Toinen osa seuraa tästä inkluusio-ekskluusio -periaatteella, koska $\delta(S(P_1) \cup S(P_2)) + \delta(S(P_1) \cap S(P_2)) = \delta(S(P_1)) + \delta(S(P_2))$.

Olkoot G_1, G_2, G_{12} polynomien P_1, P_2, P_1P_2 Galois'n ryhmät. Lähteen [31] lauseen 5.1. nojalla ehdosta $[F : \mathbb{Q}] = [F_1 : \mathbb{Q}][F_2 : \mathbb{Q}]$ seuraa, että on olemassa luonnollinen bijektio ryhmän G_{12} alkioiden σ_{12} ja parien $(\sigma_1, \sigma_2) \in G_1 \times G_2$ välillä. Tämä bijektio voidaan määritellä kuvaamalla alkiolle σ_{12} pari (σ_1, σ_2), missä $\sigma_i(x) = \sigma_{12}(x)$ kaikilla $x \in F_i$, kun $i = 1, 2$. Koska kuvaus on bijektio, voidaan parista $(\sigma_1, \sigma_2) \in G_1 \times G_2$ määritellä kuvaus $\sigma_{12} \in G_{12}$ vastaavasti.

Tämän vuoksi $|G_{12}| = |G_1||G_2|$. Olkoon N_1 niiden $\sigma_1 \in G_1$ joukko, joilla on olemassa polynomin P_1 juuri α, jolla $\sigma_1(\alpha) = \alpha$. Määritellään vastaavasti N_2 ja N_{12}. Määritetään joukon N_{12} koko, minkä jälkeen sovelletaan Frobeniuksen lausetta väitteen osoittamiseksi.

Valitaan mielivaltainen $\sigma_{12} \in G_{12}$, ja olkoon (σ_1, σ_2) sitä vastaava joukon $G_1 \times G_2$ alkio. On neljä mahdollista tapausta:

1. $\sigma_1 \in N_1$ ja $\sigma_2 \in N_2$. On siis olemassa sellainen polynomin P_1 juuri α_1, jolla $\sigma_1(\alpha_1) = \alpha_1$. Bijektion määrittelyn nojalla $\sigma_{12}(\alpha_1) = \sigma_1(\alpha_1) = \alpha_1$, eli σ_{12} kuvaa polynomin P_1P_2 juuren α_1 itselleen. Täten $\sigma_{12} \in N_{12}$.

2. $\sigma_1 \in N_1$ ja $\sigma_2 \notin N_2$. Voidaan menetellä kuten tapauksessa 1., joten $\sigma_{12} \in N_{12}$.

3. $\sigma_1 \notin N_1$ ja $\sigma_2 \in N_2$. Voidaan menetellä kuten tapauksessa 1. käyttäen polynomin P_1 juuren sijasta jotain polynomin P_2 juurta. Siispä $\sigma_{12} \in N_{12}$.

4. $\sigma_1 \notin N_1$ ja $\sigma_2 \notin N_2$. Osoitetaan, että $\sigma_{12} \notin N_{12}$ vastaoletuksella: oletetaan, että on jokin polynomin P_1P_2 juuri α, jolla $\sigma_{12}(\alpha) = \alpha$. Koska $P_1(\alpha)P_2(\alpha) = 0$, pätee $P_i(\alpha) = 0$ jollain $i \in \{1, 2\}$. Täten $\alpha \in F_i$, joten bijektion määrittelyn nojalla $\sigma_i(\alpha) = \sigma_{12}(\alpha) = \alpha$. Täten $\sigma_i \in N_i$ vastoin oletusta.

Tapauksen 1, 2, 3, 4, mukaisia σ_{12} on $|N_1||N_2|, |N_1|(|G_2| - |N_2|), (|G_1| - |N_1|)|N_2|, (|G_1| - |N_1|)(|G_2| - |N_2|)$, vastaavasti. Siispä

$$|N_{12}| = |N_1||N_2| + |N_1|(|G_2| - |N_2|) + |N_2|(|G_1| - |N_1|) = |N_1||G_2| + |G_1||N_2| - |N_1||N_2|$$

Frobeniuksen lauseen nojalla

$$\delta(S(P_1P_2)) = \frac{|N_{12}|}{|G_{12}|} = \frac{|N_1|}{|G_1|} + \frac{|N_2|}{|G_2|} - \frac{|N_1||N_2|}{|G_1||G_2|} = \delta(S(P_1)) + \delta(S(P_2)) - \delta(S(P_1))\delta(S(P_2))$$

Tämä osoittaa väitteen tapauksessa $n = 2$.

Oletetaan sitten, että väite pätee kaikilla $n \leq k$, ja osoitetaan väite arvolla $n = k + 1$. Olkoon $P = P_1P_2 \ldots P_k$, ja olkoon F_P P:n juurikunta.

Lemma 12.

$$[F : \mathbb{Q}] = [F_P : \mathbb{Q}][F_{k+1} : \mathbb{Q}]$$

Todistus. Olkoot $\gamma_1, \gamma_2, \ldots, \gamma_{k+1}$ sellaisia, joilla $F_i = \mathbb{Q}(\gamma_i)$. Selvästi $F_P = \mathbb{Q}(\gamma_1, \ldots, \gamma_k)$, joten kuntalaajennusten asteiden multiplikatiivisuuden nojalla

$$[F_P : \mathbb{Q}] = [\mathbb{Q}(\gamma_1, \ldots, \gamma_k) : \mathbb{Q}(\gamma_1, \ldots, \gamma_{k-1})] \cdots [\mathbb{Q}(\gamma_1, \gamma_2) : \mathbb{Q}(\gamma_1)][\mathbb{Q}(\gamma_1) : \mathbb{Q}]$$

Tutkitaan yksittäistä laajennusta $\mathbb{Q}(\gamma_1,\ldots,\gamma_i)/\mathbb{Q}(\gamma_1,\ldots,\gamma_{i-1})$. Tämän laajennuksen aste on luvun γ_i minimaalisen polynomin aste kunnassa $\mathbb{Q}(\gamma_1,\ldots,\gamma_{i-1})$, mikä on enintään luvun γ_i minimaalisen polynomin aste kunnassa $\mathbb{Q}$. Täten $[\mathbb{Q}(\gamma_1,\ldots,\gamma_i):\mathbb{Q}(\gamma_1,\ldots,\gamma_{i-1})] \leq [F_i:\mathbb{Q}]$. Täten

$$[F_P:\mathbb{Q}] \leq [F_1:\mathbb{Q}]\ldots[F_k:\mathbb{Q}]$$

Vastaavasti saadaan

$$[F:\mathbb{Q}] = [F_P(\gamma_{k+1}):F_P][F_P:\mathbb{Q}] \leq [F_{k+1}:\mathbb{Q}][F_P:\mathbb{Q}]$$

Yhdistämällä nämä kaksi epäyhtälöä saadaan

$$[F:\mathbb{Q}] \leq [F_1:\mathbb{Q}]\ldots[F_{k+1}:\mathbb{Q}]$$

Tässä epäyhtälössä pätee yhtäsuuruus, joten myös aiemmissa epäyhtälöissä pätee yhtäsuuruus. Erityisesti,

$$[F:\mathbb{Q}] = [F_P:\mathbb{Q}][F_{k+1}:\mathbb{Q}]$$

□

Lemman 12 nojalla voidaan soveltaa induktio-oletusta polynomeille P ja P_{k+1}. Käyttäen induktio-oletusta arvoilla $n=2$ ja $n=k$ saadaan laskettua $\delta(S(P)) = \delta(S(P_1)\cup\ldots\cup S(P_k))$:

$$\delta(S(P)\cup S(P_{k+1})) = 1-\Big(1-\delta(S(P))\Big)\Big(1-\delta(S(P_{k+1}))\Big) = 1-\Big(1-\delta(S(P_1))\Big)\Big(1-\delta(S(P_2))\Big)\ldots\Big(1-\delta(S(P_{k+1}))\Big)$$

Yhtälön vasemman puolen tiheys on $\delta(S(P_1)\cup S(P_2)\cup\ldots\cup S(P_{k+1}))$, joten tämä osoittaa alkutekijäjoukkojen unionia koskevan väitteen.

Vastaavasti kuin lemmassa 12 voidaan osoittaa, että induktio-oletusta voidaan soveltaa mille tahansa polynomien $P_1,P_2,\ldots,P_{k+1}$ aidolle osajoukolle. Siispä inkluusio-ekskluusion ja induktio-oletuksen nojalla

$$\delta(S(P_1)\cup\ldots\cup S(P_{k+1})) =$$
$$\sum_{\emptyset\neq I\subset\{1,2,\ldots,k+1\}} (-1)^{|I|+1}\delta\Big(\bigcap_{i\in I} S(P_i)\Big) =$$
$$\sum_{\substack{\emptyset\neq I\subset\{1,2,\ldots,k+1\}\\ I\neq\{1,2,\ldots,k+1\}}} (-1)^{|I|+1}\prod_{i\in I}\delta(S(P_i)) + (-1)^{k+2}\delta\Big(\bigcap_{1\leq i\leq k+1} S(P_i)\Big)\Big) =$$
$$1-\Big(1-\delta(S(P_1))\Big)\Big(1-\delta(S(P_2))\Big)\ldots\Big(1-\delta(S(P_{k+1}))\Big) + (-1)^{k+1}\prod_{1\leq i\leq k+1}\delta(S(P_i)) + (-1)^{k+2}\delta\Big(\bigcap_{1\leq i\leq k+1} S(P_i)\Big)\Big) =$$
$$\delta(S(P_1)\cup\ldots\cup S(P_{k+1})) + (-1)^{k+1}\prod_{1\leq i\leq k+1}\delta(S(P_i)) + (-1)^{k+2}\delta\Big(\bigcap_{1\leq i\leq k+1} S(P_i)\Big)\Big)$$

Täten $\delta(S(P_1)\cap\ldots\cap S(P_{k+1})) = \delta(S(P_1))\ldots\delta(S(P_{k+1}))$. Induktioaskel on otettu ja väite on täten tosi.

5 Lauseen 4 todistus

Lause 4 osoitetaan ensin konstruoimalla tietyn juurikunnan omaavia polynomeja, joilla on haluttu alkutekijöiden tiheys. Lopullinen väite osoitetaan näiden lemmojen ja lauseen 3 avulla.

Lemma 13. *Olkoon $k \in \mathbb{Z}_+$. Olkoon S niiden n joukko, joilla $1 \leq n \leq k$, ja luvut n, k ovat yhteistekijättömiä. Olkoon H jokin S:n osajoukko, joka on kertolaskun suhteen suljettu, kun kertolasku tehdään modulo k. On olemassa polynomi $P \in \mathbb{Z}$, jolla on seuraavat ominaisuudet:*

1. *$p \in S(P)$ jos ja vain jos $p \equiv h \pmod{k}$ jollain $h \in H$.*
2. *P:n juurikunta F_P on kunnan $\mathbb{Q}(\zeta_k)$ osakunta, missä ζ_k on primitiivinen k:nnes yksikköjuuri, eli sellainen kompleksiluku, jolla $\zeta_k^k = 1$ ja $\zeta_k^m \neq 1$ kaikilla $0 < m < k$.*

Todistus. Väitteen ovat osoittaneet Ram Murty ja Nithum Thain [6]. Ensimmäisen ehdon todistavat viitteen lauseet 4 ja 5, ja toinen ehto seuraa konstruktiosta. □

Osoitetaan lemman 13 avulla lauseen väite arvolla $r = \frac{1}{n}$ tietyin lisävaatimuksin, mitä käytetään yleisen tapauksen osoittamiseen.

Lemma 14. *Olkoon $n \geq 2$ kokonaisluku. On olemassa äärettömän monta alkulukua p, joita kohden on olemassa $P \in \mathbb{Z}[x]$, joka toteuttaa seuraavat ehdot:*

1. *$\delta(S(P)) = \frac{1}{n}$.*
2. *P:n juurikunta F_P on kunnan $\mathbb{Q}(\zeta_p)$ osakunta.*

Todistus. Dirichlet'n lauseen nojalla on olemassa äärettömän monta p, joilla $p \equiv 1 \pmod{n}$. Valitaan jokin tällainen p, ja kirjoitetaan $p = mn + 1$, $m \in \mathbb{Z}$. Olkoon g primitiivijuuri modulo p [3] (luku 4). Valitaan lemman 13 notaatioita käyttäen $k = p$, ja joukoksi H luvut muotoa g^{ni}, $i = 0, 1, \ldots, m-1$. Tämä on kertolaskun suhteen suljettu ryhmä, koska $g^{mn} \equiv 1 \pmod{p}$ Fermat'n pienen lauseen nojalla. Lisäksi alkiot ovat erisuuria, koska g on primitiivijuuri.

Olkoon nyt P kuten lemmassa 13. Tällöin on olemassa täsmälleen m kokonaislukua sisältävä joukko H, joilla $p \in S(P) \Leftrightarrow p \equiv h \pmod{p}$ jollain $h \in H$. Dirichlet'n lauseen tiheyttä käsittelevän muodon nojalla pätee $\delta(S(P)) = \frac{m}{p-1} = \frac{1}{n}$. Tämä todistaa ehdon 1, ja ehto 2 seuraa P:n valinnasta ja lemmasta 13. □

Osoitetaan induktiolla muuttujan k suhteen, että kaikilla $\frac{m}{k}$ on olemassa halutunlainen P, kun $0 \leq m \leq k$, $m, k \in \mathbb{Z}$, $k \neq 0$. Tapaus $k = 1$ on selvä, koska tällöin mahdolliset tiheydet ovat 0 ja 1, joita varten voidaan valita polynomit 1 ja x. Oletetaan, että väite pätee arvolla $k = n - 1$ kaikille m, ja osoitetaan se arvolla $k = n \geq 2$.

Osoitetaan siis, että kaikilla $0 \leq m \leq n$ on olemassa polynomi, jonka alkutekijöiden tiheys on $\frac{m}{n}$. Väite on selvä arvolla $m = 0$, joten oletetaan $m > 0$. Induktio-oletuksen nojalla on olemassa polynomi P, jonka alkutekijöiden tiheys on $\frac{m-1}{n-1}$.

Lemma 15. *On olemassa polynomi $Q \in \mathbb{Z}[x]$, jolla on seuraavat ominaisuudet:*

1. *$\delta(S(Q)) = \frac{1}{n}$*
2. *$F_P \cap F_Q = \mathbb{Q}$.*

Todistus. Lemman 14 nojalla on olemassa mielivaltaisen suuria alkulukuja p ja polynomeja Q_p, joilla $\delta(S(Q_p)) = \frac{1}{n}$ ja $F_{Q_p} \subset \mathbb{Q}(\zeta_p)$. Riittää osoittaa, että vähintään yksi näistä Q_p on sellainen, jonka juurikunta ei leikkaa P:n juurikuntaa. Osoitetaan tämä vastaoletuksella, eli oletetaan, että mikään näistä Q_p ei ole halutunlainen. Tämä tarkoittaa, että äärettömän monella p pätee $F_P \cap \mathbb{Q}(\zeta_p) \neq \mathbb{Q}$. Galois'n teorian peruslauseen nojalla kunnalla F_P on yhtä monta osakuntaa kuin P:n Galois'n ryhmässä on alkioita [32], joten F_P:llä on vain äärellisen monta osakuntaa. Täten on olemassa kaksi erisuurta alkulukua p_1, p_2, joilla $F_P \cap \mathbb{Q}(\zeta_{p_1}) = F_P \cap \mathbb{Q}(\zeta_{p_2}) = K \neq \mathbb{Q}$. Siis kunnilla $\mathbb{Q}(\zeta_{p_1})$, $\mathbb{Q}(\zeta_{p_2})$ on yhteinen epätriviaali osakunta K. Tämä on ristiriita, koska syklotomisilla laajennuksilla muotoa $\mathbb{Q}(\zeta_p)$ ei ole yhteisiä osakuntia p:n ollessa alkuluku [33] (lause 3.4.). □

Olkoon Q kuten lemmassa 15. Tällöin $F_P \cap F_Q = \mathbb{Q}$, mikä on ekvivalenttia lauseen 3 ehdon kanssa viitteen [31] lauseen 5.1. nojalla, joten lauseen 3 nojalla $\delta(S(P) \cap S(Q)) = \delta(S(P))\delta(S(Q)) = \frac{m-1}{n(n-1)}$. Täten

$$\delta(S(P) \cup S(Q)) = \delta(S(P)) + \delta(S(Q)) - \delta(S(P) \cap S(Q)) = \frac{m-1}{n-1} + \frac{1}{n} - \frac{m-1}{n(n-1)} = \frac{m}{n}$$

Täten $\delta(S(PQ)) = \frac{m}{n}$, mikä todistaa väitteen.

Induktioaskel on suoritettu, joten väite on tosi kaikilla m, n, ja siis tosi kaikilla rationaaliluvuilla $r \in [0, 1]$.

6 Algoritmiikka

Todistus lauseelle 1 on konstruktiivinen. Voidaan siis kirjoittaa algoritmi, joka määrittää polynomin D, kun on annettu polynomit $P_1, \ldots, P_n$. Algoritmi jaetaan kahteen osioon samalla tavalla kuin lauseen 1 todistus. Algoritmin yksinkertaistamista varten polynomeista P_i oletetaan, että ne ovat jaottomia. Lisäksi heikkoa versiota varten tehdään lisäoletus, joka koskee polynomien P_i juurien luomia kuntalaajennuksia. Lisäoletus toteutuu todennäköisesti satunnaisilla jaottomilla polynomeilla, mutta on mahdollista luoda syötteitä, joilla oletus ei toteudu. Tällöin algoritmi voi tuottaa virheellisen polynomin.

Toteutus heikosta versiosta C++-ohjelmointikielellä löytyy osoitteesta [LINKKIÄ GITTIIN TÄHÄN]. Vahvaa versiota vastaavaa algoritmia ei ole toteutettu, koska se on hyvin hidas. Algoritmi kuitenkin osoittaa, että vahvan version muunnokset voidaan tehdä äärellisen monella laskutoimituksella.

6.1 Heikko versio

Syöte: $P_1, P_2, \ldots P_n \in \mathbb{Z}_*[x]$, missä P_i ovat jaottomia polynomeja. Oletetaan, että on olemassa polynomien P_i juuret α_i, joilla $[\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}] = \deg(P_1) \ldots \deg(P_n)$.

Tulos: $D \in \mathbb{Z}_*[x]$, jolla $S_v(P_1) \cap S_v(P_2) \cap \ldots \cap S_v(P_n) \in S_v(D)$ ja $S_v(P_1) \cap \ldots \cap S_v(P_n) \approx S_v(D)$.

Olkoon Q_i se pääpolynomi, joka saadaan polynomista P_i lemman 8 transformaatiolla. Tällöin $S_v(P_i) \subset S_v(Q_i)$ ja $S_v(Q_i) \approx S_v(Q_i')$. Jos D_* on sellainen, joka toteuttaa vaaditut ehdot polynomeille Q_i, se toteuttaa ehdot myös polynomeilla P_i. Tämän vuoksi oletetaan, että algoritmissa käsiteltävät P_i ovat pääpolynomeja.

Olkoot α_i määritelty kuten edellä, ja olkoon $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Olkoon $\mathbb{Q}$-vektoriavaruuden K kanta B, missä B sisältää alkiot muotoa $\alpha_1^{i_1}\alpha_2^{i_2} \ldots \alpha_n^{i_n}$, $i_j < \deg(P_j)$ kaikilla j. Indeksoidaan B:n alkiot mielivaltaisesti indekseillä $1, 2, \ldots, T$, ja merkitään B:n alkioita $B_1, B_2, \ldots, B_T$.

Algoritmin toiminta

1. Lasketaan rekursiolla luvun s^i esitys kannan B alkioiden avulla ilmaistuna, kun $0 \leq i \leq T$. Olkoon $s_{i,j}$ luvun s^i esityksessä lukua B_j vastaava kerroin.
2. Ratkaistaan lineaarinen yhtälöryhmä

$$\begin{cases} x_0 s_{0,1} + x_1 s_{1,1} + \ldots + x_T s_{T,1} = 0 \\ x_0 s_{0,2} + x_1 s_{1,2} + \ldots + x_T s_{T,2} = 0 \\ \vdots \\ x_0 s_{0,T} + x_1 s_{1,T} + \ldots + x_T s_{T,T} = 0 \end{cases}$$

   missä $x_i \in \mathbb{Q}$. Valitaan sellainen ratkaisu, jossa $x_T = 1$
3. Muodostetaan polynomi $D(t) := t^T + x_{T-1}t^{T-1} + \ldots + x_1 t + x_0$

Todistus toimivuudesta

Ensin todistetaan kaksi väitettä liittyen kuntalaajennuksiin, minkä jälkeen osoitetaan kohdan 2 yhtälöryhmän ratkeavuus. Olkoon $K_i := \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ kaikilla i.

Lemma 16. $[K_i : \mathbb{Q}] = \deg(P_1)\deg(P_2)\ldots\deg(P_i)$ *kaikilla* $1 \leq i \leq n$.

Todistus. Todistus on analoginen lemman 12 todistuksen kanssa. □

Olkoon $s_i := \alpha_1 + \alpha_2 + \ldots + \alpha_i$ kaikilla i.

Lemma 17. *$\mathbb{Q}(s_i) = K_i$ kaikilla $1 \leq i \leq n$.*

Todistus. Väite pätee arvolla $i = 1$. Oletetaan, että väite pätee arvolla $i = k$, ja osoitetaan se arvolla $i = k + 1$. Induktio-oletuksen ja lemman 16 nojalla $[\mathbb{Q}(\alpha_{k+1}, s_i) : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \ldots, \alpha_{k+1}) : \mathbb{Q}] = \deg(P_1) \ldots \deg(P_{k+1}) = [\mathbb{Q}(\alpha_{k+1}) : \mathbb{Q}][\mathbb{Q}(s_k) : \mathbb{Q}]$. Lähteen [31] lauseen 6.6. nojalla ehdosta $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]$ seuraa $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$. Soveltamalla tätä ja induktio-oletusta saadaan $\mathbb{Q}(s_{k+1}) = \mathbb{Q}(\alpha_{k+1}, s_k) = K_{i+1}$. Induktioaskel on otettu, ja väite on tosi kaikilla i. □

Lemma 18. *Matriisin*

$$\begin{bmatrix} s_{0,1} & s_{1,1} & \ldots & s_{T-1,1} \\ s_{0,2} & s_{1,2} & \ldots & s_{T-1,2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{0,T} & s_{1,T} & \ldots & s_{T-1,T} \end{bmatrix}$$

pystyrivit ovat keskenään lineaarisesti riippumattomia rationaalilukujen yli.

Todistus. Todistetaan väite vastaoletuksella. Olkoon matriisin i:nnes pystyrivi v_i. Olkoot $q_0, q_1, \ldots, q_{T-1}$ sellaisia rationaalilukuja, jotka eivät kaikki ole nollia, ja joilla vektori $v = q_0 v_0 + q_1 v_1 + \ldots + q_{T-1} v_{T-1}$ on nollavektori. Tällöin $q_0 s_{0,i} + q_1 s_{1,i} + \ldots + q_{T-1} s_{T-1,i} = 0$ kaikilla i. Kertomalla tämän yhtälön luvulla B_i ja summaamalla kaikkien i yli saadaan yhtälö $q_0 s^0 + q_1 s^1 + \ldots + q_{T-1} s^{T-1} = 0$. Lemman 17 nojalla $K = \mathbb{Q}(s)$, eli $[K : \mathbb{Q}] = T$, joten luvun s minimaalisen polynomin aste on T. Tämä on ristiriidassa edellisen yhtälön kanssa. Vastaoletus johti ristiriitaan, joten väite on tosi. □

Lemman 18 nojalla matriisin

$$\begin{bmatrix} s_{0,1} & s_{1,1} & \ldots & s_{T,1} \\ s_{0,2} & s_{1,2} & \ldots & s_{T,2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{0,T} & s_{1,T} & \ldots & s_{T,T} \end{bmatrix}$$

pystyriveistä voidaan valita T ensimmäistä pystyriviä, jotka ovat keskenään lineaarisesti riippumattomia. Koska matriisin lineaarisesti riippumattomien pysty- ja vaakarivien määrä on sama [34], on kyseisellä matriisilla T toisistaan lineaarisesti riippumatonta vaakariviä. Täten algoritmin kohdan 2 yhtälöryhmällä on äärettömän monta ratkaisua, koska yhtälöryhmässä on $T + 1$ muuttujaa ja T toisistaan riippumatonta yhtälöä. Valitaan jokin ratkaisu $X = (x_0, x_1, \ldots, x_T)$, ja oletetaan, että kaikki x_i eivät ole 0. Jos $x_T = 0$, palautuu kohdan 2 yhtälöryhmä sellaiseksi, jossa on T muuttujaa ja T riippumatonta yhtälöä, jolloin sillä on vain triviaaliratkaisu $X = 0$. Oletetaan siis, että $x_T \neq 0$. Nyt ratkaisun X alkiot x_i voidaan kertoa luvulla x_T^{-1}, jolloin saadaan halutunlainen ratkaisu, jossa $x_T = 1$.

Samalla tavalla kuin lemman 18 todistuksessa osoitettiin polynomiyhtälö muuttujalle s kertomalla yhtälöitä sopivasti kannan B alkioilla B_j voidaan osoittaa $D(s) = s^T + x_{T-1} s^{T-1} + \ldots + s_0 = 0$. Koska $\deg(D) = T = [K : \mathbb{Q}(s)]$, on D luvun s minimaalinen polynomi.

Kuten lauseen 1 heikon version todistuksessa todettiin $D \in \mathbb{Z}_*[x]$ nojaten siihen, että algebralliset kokonaisluvut muodostavat renkaan, on s algebrallinen kokonaisluku, ja algoritmin tuottama D on kokonaislukukertoiminen.

Lopuksi osoitetaan, että $S_v(P_1) \cap \ldots \cap S_v(P_n) \approx S_v(D)$ ja $S_v(P_1) \cap \ldots \cap S_v(P_n) \subset S_v(D)$. Olkoon D_i luvun s_i minimaalinen polynomi, ja olkoon $S_i := S_v(P_1) \cap \ldots \cap S_v(P_i)$ kaikilla i.

Lemma 19. *$S_i \approx S_v(D_i)$ ja $S_i \subset S_v(D_i)$ kaikilla $1 \leq i \leq n$.*

Todistus. Osoitetaan väite induktiolla muuttujan i suhteen. Väite pätee arvolla $i = 1$. Oletetaan, että se pätee arvolla $i = k$, ja osoitetaan se arvolla $i = k + 1 \leq n$. Koska s_k on algebrallinen kokonaisluku, $D_k \in \mathbb{Z}_*[x]$. Täten heikon version nojalla on olemassa sellainen D_*, jolla $S_v(D_k) \cap S_v(P_{k+1}) \approx S_v(D_*)$ ja $S_v(D_k) \cap S_v(P_{k+1}) \subset S_v(D_*)$.

Heikon version todistuksesta voidaan lukea, että D_* voidaan valita polynomiksi D_{k+1}. Nimittäin, todistuksessa valitaan D_* olemaan muotoa $s_k + n_i\alpha_{k+1,j}$ olevien lukujen minimaalisten polynomien tulo, missä $\alpha_{k+1,j}$ käy läpi polynomin D_{k+1} eri juuria läpi, ja n_i ovat sellaisia kokonaislukuja, joilla $\mathbb{Q}(s_k, \alpha_{k+1,j}) = \mathbb{Q}(s_k + n_i\alpha_{k+1,j})$. Lemmojen 16 ja 17 nojalla P_{k+1} ei jakaudu kunnassa $\mathbb{Q}(s_k) = K_k$, joten tarvitsee valita vain yksi polynomin P_{k+1} juuri α_{k+1}, jolloin siis D_* on luvun $s_k + n\alpha_{k+1}$ minimaalinen polynomi. Lemman 17 nojalla $K_{k+1} = \mathbb{Q}(s_{k+1})$, joten voidaan valita $n = 1$. Täten $D_* = D_{k+1}$, mikä todistaa väitteen. □

Lemman 19 nojalla $D_n = D$ on haluttu polynomi.

Tehokkuus

Algoritmin kokonaisaikavaativuus on $O(T^3)$, missä O kuvaa iso-O -notaatiota [35]. Osoitetaan tämä analysoimalla kunkin algoritmin kohdan aikavaativuutta.

Kohta 1 voidaan suorittaa $O(T^3)$ laskutoimituksella. Tutkitaan, miten luvun s^{i+1} esitys kannan B avulla voidaan laskea tehokkaasti luvun s^i esityksen $(s_{i,1}, s_{i,2}, \ldots, s_{i,T})$ avulla. Tämä voidaan tehdä seuraavan yhtälön avulla

$$s^{i+1} = ss^i = (\alpha_1 + \alpha_2 + \ldots + \alpha_n)s^i = \alpha_1 s^i + \alpha_2 s^i + \ldots + \alpha_n s^i$$

Lemma 20. *Olkoon $S \in K$ luku, jonka esitys kannan B avulla on annettu. Luvun $\alpha_i S$ kantaesitys voidaan laskea $O(T)$ ajassa.*

Todistus. Valitaan jokin $1 \leq j \leq T$. Tutkitaan, mitä tapahtuu, kun B_j kerrotaan luvulla α_i. Jos luvun α_i eksponentti luvussa B_j ei ole $\deg(P_i) - 1$, pätee $B_j\alpha_i \in B$. Muussa tapauksessa luvun $B_j\alpha_i$ esitys kannan B avulla sisältää enintään $\deg(P_i)$ nollasta eroavaa kerrointa, jotka voidaan määrittää käyttäen yhtälöä $P_i(\alpha_i) = 0$. Ensimmäisen tapauksen mukaisia j on $T - \frac{T}{\deg(P_i)}$ ja toisen tapauksen mukaisia $\frac{T}{\deg(P_i)}$.

Luvun $\alpha_i S$ kantaesityksen määrittäminen voidaan tehdä soveltamalla edellä tehtyjä havaintoja. Luku $\alpha_i S$ voidaan muodostaa kertomalla α_i yksitellen jokaisen S:n kanta-alkiota vastaava kerroin, ja päivittämällä muistiin uutta tulosta. Jos kanta-alkio B_j on ensimmäisen tapauksen mukainen, tämä voidaan tehdä vakioajassa. Toisen tapauksen mukainen B_j vie $\deg(P_i)$ laskutoimitusta. Laskutoimitusten määrä on täten $T - \frac{T}{\deg(P_i)} + \frac{T}{\deg(P_i)} \deg(P_i) = O(T)$. □

Lemman 20 nojalla luvun $\alpha_j s^i$ kantaesitys voidaan määrittää $O(T)$ ajassa. Kahden kantaesityksen avulla ilmaistun luvun summa voidaan myös laskea $O(T)$ ajassa. Täten s^{i+1} saadaan laskettua $O(T^2)$ laskutoimituksella, kun on valmiiksi laskettu s^i. Suorittamalla tämän kaikille $0 \leq i < n$ saadaan kokonaisaikavaativuudeksi $O(T^3)$.

Kohdan 2 yhtälöryhmän ratkaiseminen voidaan toteuttaa Gaussin-Jordanin eliminointimenetelmällä [36] $O(T^3)$ ajassa [37] (luku 2).

Kohta 3 voidaan suorittaa $O(T)$ ajassa.

Täten algoritmin kokonaisaikavaativuus on $O(T^3)$.

Lopuksi huomautetaan, että on olemassa huomattavasti tehokkaampi algoritmi heikon version mukaisen D löytämiseksi. Algoritmi on esitetty viitteessä [38]. Olkoot $f, g \in \mathbb{Z}_*[x]$ mielivaltaisia pääpolynomeja (jotka eivät välttämättä ole jaottomia), joiden juuret ovat $\alpha_1, \ldots, \alpha_n$ ja $\beta_1, \ldots, \beta_m$. Tulo $D(x) = \prod_{i,j}(x - (\alpha_i + \beta_j))$ voidaan laskea $O(mn)$ ajassa, kun O-notaatiossa jätetään logaritmikertoimet huomioimatta [38] (lause 1). Voidaan osoittaa, että yleisessä tapauksessa n polynomilla $P_1, \ldots, P_n \in \mathbb{Z}_*[x]$ halutunlainen D on yllä esitetyn tulomuodon mukainen, tarvittaessa sopivien polynomeille P_i tehtyjen transformaatioiden jälkeen. Yksityiskohdat sivuutetaan tässä. Tämä osoittaa yhdessä lauseen 1 polynomin asteen ylärajan tiukkuuden kanssa, että on olemassa logaritmikertoimia huomioimatta tehokkuudeltaan optimaalinen algoritmi heikon version polynomin D määrittämiseen.

6.2 Yleinen tapaus

Syöte: Jaottomat [*3] $P_1, P_2, \ldots, P_n, D \in \mathbb{Z}_*[x]$, missä $S_v(P_1) \cap \ldots \cap S_v(P_n) \approx S_v(D)$ ja $S_v(P_1) \cap \ldots \cap S_v(P_n) \subset S_v(D)$.

Tulos: Sellainen D_*, jolla $S_d(P_1) \cap \ldots \cap S_d(P_n) = S_d(D)$.

Voidaan olettaa, että $D(0) \neq 0$, koska muuten D voidaan korvata polynomilla $D_*(x) := D(x+c)$ kuten lemmassa 7.

Olkoot $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ sellaisia nollasta eroavia kokonaislukuja, joilla kaikilla i on olemassa sellaiset X_i, Y_i, joilla Bezout'n lemman mukaisesti $P_i X + P_i' Y = m_i$. Määritellään m_0 vastaavasti jaottomalle polynomille D. Tällaiset m_i voidaan määrittää Bezout'n lemman todistuksen [4] tapaisesti Eukleideen algoritmilla äärellisellä määrällä operaatioita. Merkitään $M = m_0 m_1 \ldots m_n$. Ennen itse algoritmia esitetään lemma, johon algoritmi perustuu. Lemman väite ja todistus perustuu viitteen [39] materiaaliin.

Lemma 21. *Olkoon $P \in \mathbb{Z}_*[x]$, ja olkoon $0 \neq m \in \mathbb{Z}[x]$ sellainen, jolla on olemassa $X, Y \in \mathbb{Z}[x]$ niin, että $PX + P'Y = m$. Olkoon p mielivaltainen alkuluku, ja olkoon v suurin kokonaisluku, jolla $p^v | m$. Jos $p^{2v+1} \in S_d(P)$, niin $p \in S_v(P)$.*

Todistus. Olkoon a sellainen, jolla $P(a) \equiv 0 \pmod{p^j}$, $j \geq 2v+1$. Osoitetaan, että $p^{j+1} \in S_d(P)$. Olkoon s suurin kokonaisluku, jolla $p^s | P'(a)$. Sijoittamalla polynomiyhtälöön $PX + P'Y = m$ arvon a saadaan tutkimalla yhtälön puolien jaollisuutta p:n potensseilla epäyhtälö $\min(s, j) \leq v$. Siis $s \leq v$.

Sijoitetaan Henselin lemman todistuksen identiteettiin $P(a + bp^k) \equiv P(a) + bp^k P'(a) \pmod{p^{2k}}$ arvo $k = j - s$. Koska $2k = 2j - 2s \geq 2j - 2v \geq j + 1$, pätee täten yhtälö $P(a + bp^{j-s}) \equiv P(a) + bp^{j-s} P'(a) \pmod{p^{j+1}}$. Yhtälön oikea puoli on jaollinen luvulla p^j, koska $P(a) \equiv 0 \pmod{p^j}$ ja $p^s | P'(a)$. Täten $P(a + bp^{j-s}) \equiv 0 \pmod{p^j}$. Jaetaan yhtälö puolittain luvulla p^j, jolloin saadaan yhtälö $\frac{P(a+bp^{j-s})}{p^j} \equiv \frac{P(a)}{p^j} + b\frac{P'(a)}{p^s} \pmod{p}$. Yhtälön oikea puoli on ensimmäisen asteen polynomi muuttujan b suhteen, missä b:n kerroin ei ole $0 \pmod{p}$ luvun s määritelmän nojalla. Täten on olemassa sellainen b, jolla yhtälön oikea puoli on jaollinen p:llä. Tällä b pätee $\frac{P(a+bp^{j-s})}{p^j} \equiv 0 \pmod{p}$, joten $P(a + bp^{j-s}) \equiv 0 \pmod{p^{j+1}}$. Siis $p^{j+1} \in S_d(P)$. Täten $S_d(P)$ sisältää mielivaltaisen suuria p:n potensseja, mikä todistaa väitteen. □

Algoritmin toiminta

Käydään läpi kaikki $p|M$. Kullekin p suoritetaan seuraavat operaatiot:

1. Olkoon v_i suurin kokonaisluku, jolla $p^{v_i} \mid m_i$. Jos yhtälöllä $D(x) \equiv 0 \pmod{p^{2v_0+1}}$ ja yhtälöillä $P_i(x) \equiv 0 \pmod{p^{2v_i+1}}$ on ratkaisut kaikilla i, jatketaan seuraavaan alkulukuun p.
2. Etsitään suurin $k \in \mathbb{Z}$, jolla yhtälöllä $P_i(x) \equiv 0 \pmod{p^k}$ on ratkaisu kaikilla i.
3. Muutetaan D polynomiksi $D_p(x) := p^k \frac{D(p^{t+1}x)}{p^t}$, missä t on suurin kokonaisluku, jolla $p^t | D(0)$.

Todistus toimivuudesta

Olkoon algoritmin tuottama polynomi D_*. Osoitetaan, että D_* on halutunlainen. Lemman 1 nojalla riittää osoittaa, että joukot $S := S_d(P_1) \cap \ldots \cap S_d(P_n)$ ja $S_d(D_*)$ sisältävät samat alkulukujen potenssit. Lemman 7 todistuksen nojalla algoritmin kohdan 3 esitetty muunnos $D \to D_p$ muuttaa polynomin D tekijöistä ainoastaan niitä alkuluvun potensseja, jotka ovat p:n potensseja. Lisäksi tällä p pätee $p^x \in S_d(D_p) \Leftrightarrow p^x \in S$. Siis kaikilla niillä p, jotka käsitellään algoritmin kohdassa 3 pätee $p^x \in S \Leftrightarrow p^x \in S(D_*)$.

Jokainen alkuluku voidaan jakaa johonkin seuraavista kategorioista, jotka käsitellään erikseen.

1. $p \in S_v(D)$, $p \in S_v(P_1) \cap \ldots \cap S_v(P_n)$.
2. $p \in S_v(D)$, $p \notin S_v(P_1) \cap \ldots \cap S_v(P_n)$.
3. $p \notin S_v(D)$, $p \notin S_v(P_1) \cap \ldots \cap S_v(P_n)$.

[3] Heikon version algoritmin tuottama D on jaoton. Algoritmi toimii myös jaollisilla polynomeilla, kunhan niillä ei ole kaksoisjuuria.

Kategorian 1 alkulukuja p joko ei käsitellä algoritmin aikana (jos $p \nmid M$) tai ne poissuljetaan algoritmin kohdassa 1 (jos $p|M$) lemman 21 nojalla. Täten nämä p käsitellään kuten kuuluukin.

Kategorian 2 alkuluvut p käsitellään algoritmin aikana, koska lemman 2 todistuksen nojalla $p \notin S_v(P_i) \implies p|m_i$. Täten $p \notin S_v(P_1) \cap \ldots \cap S_v(P_n) \implies p|M$. Tätä p ei poissuljeta algoritmin kohdassa 1 lemman 21 nojalla, joten se käsitellään kohdassa 3. Täten nämä p käsitellään kuten kuuluukin.

Kategorian 3 alkuluvut p käsitellään algoritmin aikana aivan kuten kategorian 2 alkuluvut. Täten nämä p käsitellään kuten kuuluukin.

Tapauskäsittely osoittaa lemman 1 avulla, että $S = S_d(D_*)$. Täten D_* on halutunlainen polynomi.

7 Viitteet

Nettilinkit haettu 14.1.2019.

[1] *I. Schur, Uber die Existenz unendlich vieler Primzahlen in einiger speziellen arithmetischen Progressionen, S-B Berlin. Math. Ges., 11 (1912), 40–50.*

[2] *Samuel Moy, An Introduction to the Theory of Field Extensions, The University of Chicago, VIGRE program 2009* http://www.math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Moy.pdf

[3] *Esa V. Vesalainen, Lyhyt johdatus alkeelliseen lukuteoriaan* https://matematiikkakilpailut.fi/kirjallisuus/laajalukuteoriamoniste.pdf

[4] *Keith Conrad, Analogies with Polynomials* http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/analogypoly.pdf

[5] *Alireza Salehi Golsefidy, Modern Algebra II Lecture 17, 2012* http://www.math.ucsd.edu/~asalehig/Lecture17-math103b-w-12.pdf

[6] *Murty, Ram; Thain, Nithum. Primes in Certain Arithmetic Progressions. Funct. Approx. Comment. Math. 35 (2006), 249–259* https://projecteuclid.org/euclid.facm/1229442627

[7] *MacDuffee, C. C. "The p-Adic Numbers of Hensel." The American Mathematical Monthly, vol. 45, no. 8, 1938, pp. 500–508* www.jstor.org/stable/2303739

[8] *Thurston, H. S. "The Solution of p-Adic Equations." The American Mathematical Monthly, vol. 50, no. 3, 1943, pp. 142–148* www.jstor.org/stable/2302393

[9] *Gerst, Irving, and John Brillhart. "On the Prime Divisors of Polynomials." The American Mathematical Monthly, vol. 78, no. 3, 1971, pp. 250–266* www.jstor.org/stable/2317521

[10] *Suresh, Arvind, "On the Characterization of Prime Sets of Polynomials by Congruence Conditions"(2015). CMC Senior Theses. 993* https://scholarship.claremont.edu/cmc_theses/993

[11] *Domingo Gómez, Jaime Gutierrez, Math. Comp. 83 (2014), 2953-2965* https://pdfs.semanticscholar.org/2983/ddf026a1c65813f91505a55849babe0c8e6f.pdf

[12] *Richard Gottesman, Kwokfung Tang, Quadratic Recurrences with a Positive Density of Prime Divisors, International Journal of Number TheoryVol. 06, No. 05, pp. 1027-1045 (2010)* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.367.909&rep=rep1&type=pdf

[13] *Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc. (2), 78(2):523–544, 2008* https://people.carleton.edu/~rfjones/Preprints/Jonesqd2preprint.pdf

[14] *Roskam, Hans. Prime divisors of linear recurrences and Artin's primitive root conjecture for number fields. Journal de théorie des nombres de Bordeaux, Volume 13 (2001) no. 1, pp. 303-314* http://www.numdam.org/item/JTNB_2001__13_1_303_0/

[15] *P.J. Stephens, Prime divisors of second-order linear recurrences. I, Journal of Number Theory, Volume 8, Issue 3, 1976, Pages 313-332* https://www.sciencedirect.com/science/article/pii/0022314X7690010X

[16] *Shorey, T. N.; Tijdeman, R. On the greatest prime factors of polynomials at integer points. Compositio Mathematica, Volume 33 (1976) no. 2, pp. 187-195* http://www.numdam.org/item/CM_1976__33_2_187_0/

[17] *Cecile Dartyge, Greg Martin, Gerald Tenenbaum, Polynomial values free of large prime factors, Periodica Mathematica Hungarica 43, 1-2 (2001), 111-119* http://www.iecl.univ-lorraine.fr/~Gerald.Tenenbaum/PUBLIC/PPP/Psi_F(x,y).pdf

[18] *Michael Filaseta (Columbia, S.C.), Squarefree values of polynomials, ACTA ARITHMETICA LX.3 (1992)* http://matwbn.icm.edu.pl/ksiazki/aa/aa60/aa6032.pdf

[19] *Booker, Andrew R., Square-free Values of Reducible Polynomials, (2017)* https://www.semanticscholar.org/paper/Square-free-Values-of-Reducible-Polynomials-Booker/9c3c1062a8cf6a403cc558ef573268a6e6bd5965

[20] *Kaisa Matomäki, A note on primes of the form $p = aq^2 + 1$. Acta Arith. 137, 133-137 (2009)* http://users.utu.fi/ksmato/papers/Primesaq2p1.pdf

[21] *Yitang Zhang, Bounded gaps between primes, Annals of Mathematics, Pages 1121-1174 from Volume 179 (2014), Issue 3* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.308.998&rep=rep1&type=pdf

[22] *Sachi Hashimoto, Introduction to Ring Theory, 2015* http://math.bu.edu/people/svh/RingTheoryMathcamp.pdf

[23] *Ken Brown, Cornell University, The Primitive Element Theorem, October 2010, Mathematics 6310* http://pi.math.cornell.edu/~kbrown/6310/primitive.pdf

[24] *Nate Sauder, Notes on introductory algebraic number theory, 2013* http://math.uchicago.edu/~may/REU2013/REUPapers/Sauder.pdf

[25] *Christian Ballot, Florian Luca, Prime factors of $a^{f(n)} - 1$ with an irreducible polynomial $f(x)$, New York J. Math. 12 (2006) 39–45* https://www.researchgate.net/publication/268860079_Prime_factors_of_a_fn_-1_with_an_irreducible_polynomial_fx

[26] *Keith Conrad, Galois groups as permutation groups* http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/galoisaspermgp.pdf

[27] *Franz Lemmermeyer, Class Field Theory, 2007* http://www.fen.bilkent.edu.tr/~franz/cft/cfb.pdf

[28] *Nicholas George Triantafillou, The Chebotarev density theorem, 2015* https://math.mit.edu/~ngtriant/notes/chebotarev.pdf

[29] *Brett Porter, Cyclotomic Polynomials, 2015* https://www.whitman.edu/Documents/Academics/Mathematics/2015/Final%20Project%20-%20Porter,%20Brett.pdf

[30] *Soprunov, Ivan. (2010). A short proof of the prime number theorem for arithmetic progressions* https://www.researchgate.net/publication/251779481_A_SHORT_PROOF_OF_THE_PRIME_NUMBER_THEOREM_FOR_ARITHMETIC_PROGRESSIONS

[31] *Keith Conrad, Galois theory at work* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.211.2314&rep=rep1&type=pdf

[32] *Andry N. Rabenantoandro, Fundamental theorems of Galois theory, 2012* http://math.sun.ac.za/wp-content/uploads/2012/09/Galois.pdf

[33] *Keith Conrad, Cyclotomic extensions* http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cyclotomic.pdf

[34] *Wardlaw, William P. "Row Rank Equals Column Rank." Mathematics Magazine, vol. 78, no. 4, 2005, pp. 316–318.* www.jstor.org/stable/30044181

[35] *P. Danziger, Big O Notation* http://www.scs.ryerson.ca/~mth110/Handouts/PD/bigO.pdf

[36] *P. Danziger, Gaussian Elimination, 2005* http://www.math.ryerson.ca/~danziger/professor/MTH108/Handouts/gauss.pdf

[37] *P. Danziger, Complexity, 2005* http://www.math.ryerson.ca/~danziger/professor/MTH108/Handouts/gauss-complexity.pdf

[38] *Bostan, A., Flajolet, P., Salvy, B., and Schost, É. (2002). Fast Computation With Two Algebraic Numbers.* https://www.semanticscholar.org/paper/Fast-Computation-With-Two-Algebraic-Numbers-Bostan-Flajolet/459c92ec313bb1613b90036352b24bd74132c3e0

[39] *Arturo Magidin (https://math.stackexchange.com/users/742/arturo-magidin), Hensel's Lemma:* $f'(x) \equiv 0 \pmod{p}$ *case., URL (version: 2011-12-14):* https://math.stackexchange.com/q/90856