Alkulukutestaus ja tekijöihinjako

LuK-tutkielma
Aada Illikainen
2550891
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2019

Sisältö

Johdanto

Tässä tutkielmassa tarkastellaan tekijöihinjakoon ja alkulukutestaukseen liittyviä menetelmiä. Alkulukutesteillä tarkoitetaan testejä, joilla voidaan määrittää onko positiivinen kokonaisluku alkuluku. Jotkut testit kykenevät sanomaan varmuudella vain luvun olevan yhdistetty. Tällaiset testit ovat probabilistisia alkulukutestejä ja tässä tutkielmassa näitä menetelmiä nimitetään jaollisuustesteiksi.

Pollardin Rho -menetelmä on tekijöihinjakomenetelmä. Tässä menetelmässä muodostetaan valitun polynomin avulla rekursiivisesti lukujono. Lukujonon termit ovat tekijöihinjaettavan luvun jäännösluokkia. Jonon termien erotuksien ja tutkittavan luvun suurinta yhteistä tekijää lasketaan, kunnes epätriviaali tekijä löytyy.

Pollardin $p-1$ -menetelmä on myös tekijöihinjakomenetelmä. Pollardin $p-1$ -menetelmässä valitaan suurehko kokonaisluku q ja kokonaisluku a. Epätriviaali tekijä löytyy jollain kokonaisluvun q arvolla ratkaisemalla m kongruenssiyhtälöstä $a^q \equiv m \pmod{n}$ ja laskemalla $\text{syt}(m-1, n)$, missä n on tutkittava luku ja a kokonaisluku.

Ketjumurtolukumenetelmä on tekijöihinjakomenetelmä. Ketjumurtolukumenetelmässä muodostetaan ketjumurtolukuesitys luvulle $\sqrt{n}$, missä n on tutkittava luku. Ketjumurtolukumenetelmä käyttää pohjana Kraitchikin tekijöihinjakomenetelmää. Tässä tutkielmassa on käyty läpi erilaisia tekniikoita löytää menetelmän avulla epätriviaaleja tekijöitä.

Neliöseulan menetelmä perustuu Kraitchikin tekijöihinjakomenetelmään. Neliöseulan menetelmässä tavoitteena on muodostaa Kraitchikin menetelmän tilanne, missä on sellaiset kokonaisluvut x ja y, jotka toteuttavat yhtälöt $x^2 \equiv y^2 \pmod{n}$ ja $x \not\equiv y \pmod{n}$. Luku n on tutkittava luku. Neliöseulan menetelmässä näitä lukuja seulotaan polynomin $f(x) = x^2 - n$ avulla niin, että keskenään kerrottuna jotkut funktion arvot muodostavat neliön.

Fermat'n jaollisuustesti on probabilistinen alkulukutesti. Kaikki alkuluvut, sekä harvassa olevat yhdistetyt luvut toteuttavat Fermat'n pienen lauseen. On siis mahdollista antaa arvio, millä todennäköisyydellä testin lä-

päissyt luku on alkuluku. Kun jokin kokonaisluku ei toteuta Fermat'n lausetta, se on varmuudella yhdistetty.

Lucasin testi on alkulukutesti. Tässä tutkielmassa on käyty läpi myös Lucasin testin parannelmia. Kun jokin kokonaisluku läpäisee Lucasin testin, se on varmuudella alkuluku. Lucasin testi perustuu Fermat'n pienelle lauseelle.

Miller-Rabinin jaollisuustesti on probabilistinen alkulukutesti. Miller-Rabinin testissä tarkastellaan kokonaislukua $n-1$, missä n on tutkittava luku. Oletuksena testissä on, että tutkittava luku on pariton. Luvun $n-1$ avulla muodostettujen kongruenssien avulla voidaan määrittää, onko luku jaollinen.

Tässä tutkielmassa on käytetty pääasiallisena lähteenä kirjaa *David M. Burton: Elementary number theory* (1997) [1].

1 Tekijöihinjako

1.1 Pollardin Rho -menetelmä

Pollard Rho -menetelmän avulla jaetaan suurehkoja kokonaislukuja tekijöihin eli menetelmä on tehokas 20 numeron mittaisiin lukuihin asti. Pollardin Rho -menetelmällä on onnistuttu jakamaan vuonna 1980 Fermat'n luku $F_8 = 2^{2^8} + 1$ tekijöihin.

Olkoon n jokin tutkittava, pariton yhdistetty positiivinen kokonaisluku. Aluksi valitaan jokin yksinkertainen vähintään toisen asteen kokonaislukukertoiminen polynomi. Esimerkiksi

$$f(x) = x^2 + a, a \neq -2, 0.$$

Tämän jälkeen valitaan jokin kokonaisluku x_0, jonka avulla lasketaan luvut $x_1, x_2, x_3, \ldots$ rekursiivisesti seuraavasti:

$$x_{k+1} \equiv f(x_k) \pmod{n}, k = 0, 1, 2, \ldots$$

Tällöin itseasiassa saadaan luvut

$$x_1 = f(x_0), x_2 = f(f(x_0)), x_3 = f(f(f(x_0))), \ldots$$

laskettua $\pmod{n}$.

Olkoon d jokin luvun n epätriviaali jakaja, kuitenkin niin että d on lukuun n verrattuna hyvin pieni. Koska d on nyt valittu suhteellisen pieneksi, sen määräämiä kongruenssiluokkia on myös vähän. Tästä johtuen on todennäköisesti olemassa jotkin luvut x_k ja x_j, jotka ovat samassa d määräämässä kongruenssiluokassa mutta eivät ole samassa n määräämässä kongruenssiluokassa. Tästä seuraa siis, että d jakaa luvun $x_k - x_j$ mutta n ei. Joten $\text{syt}(x_k - x_j, n)$ on luvun n epätriviaali jakaja. Luku d saadaan tietoon vasta kun lasketaan edellä mainittuja x arvoja ja niiden avulla saatuja suurimpia yhteisiä tekijöitä luvun n kanssa. Jos löytyy jokin suurin yhteinen tekijä, joka ei ole 1, on mahdollisuus että suurin yhteinen tekijä on n. Tällöin voidaan valita jokin muu lähtöarvo tai uusi funktio.

Esimerkki 1.1. Valitaan $n = 1001$, $x_0 = 1$ ja $f(x) = x^2 + 1$. Iteraatiosta saadaan

$$x_1 = 2, x_2 = 5, x_3 = 26, x_4 = 677, x_5 = 936$$

Huomataan, että $x_5 - x_4 = 286$ ja $\text{syt}(1001, 286) = 143$, joka on siis luvun 1001 jakaja.

Kuitenkaan ei ole kovin tehokasta laskea kaikkia $\text{syt}(x_k - x_j, n)$ kaikille $j < k$. Monessa tapauksessa on tehokkaampaa tarkastella vain tilanteet, missä $k = 2j$. Olkoot d taas jokin luvun n epätriviaali jakaja. Nyt jos $x_k \equiv x_j \pmod{d}$ kun $k > j$, niin aiemmin valitun funktion $f(x)$ mukaan

$$x_{j+1} = f(x_j) \equiv f(x_k) = x_{k+1} \pmod{d}$$

Tästä seuraa, että kun luvut $\{x_k\}$ lasketaan modulo d niin $k - j$ kappaletta kokonaislukuja toistuu äärettömän monta kertaa. Kun on olemassa $r \equiv s \pmod{k - j}$, missä $r, s \leq j$. Tästä seuraa, että $x_r \equiv x_s \pmod{d}$. Etenkin siis $x_t \equiv x_{2t} \pmod{d}$ aina kun t on luvun k moninkerta, ollen kuitenkin suurempi kuin j. Täten on mahdollista että on olemassa k siten, että $1 < \text{syt}(x_{2k} - x_k, n) < n$.

Esimerkki. Valitaan $n = 30623$, $x_0 = 3$ ja $f(x) = x^2 - 1$. Tästä saadaan

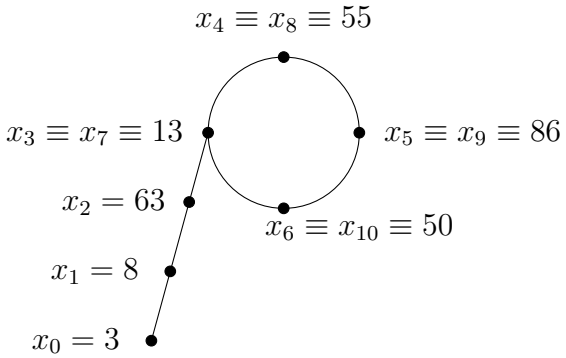
$$8, 63, 3968, 4801, 21104, 28526, 18319, 18926 \ldots$$

$$\begin{aligned} x_2 - x_1 = 63 - 8 = 55 \quad & \text{syt}(55, n) = 1 \\ x_4 - x_2 = 4801 - 63 = 4738 \quad & \text{syt}(4738, n) = 1 \\ x_6 - x_3 = 28526 - 3968 = 24558 \quad & \text{syt}(24558, n) = 1 \\ x_8 - x_4 = 18926 - 4801 = 14125 \quad & \text{syt}(14125, n) = 113 \end{aligned}$$

Eli siis 30623 on jaollinen luvulla 113. Kun funktion $f(x) = x^2 - 1$ avulla saatuja lukuja $\{x_k\}$ lasketaan (mod 113) saadaan jaksollinen jono

$$8, 63, 13, 55, 86, 50, 13, 55 \ldots,$$

jossa toistuu neljä lukua $13, 55, 86$ ja 50. Jaksollisen jonon toistuvien lukujen määrä tulee suoraan niiden x arvojen indeksistä, minkä avulla tekijä on löydetty. Tässä tapauksessa tekijä löydettiin, kun $x_8 \equiv x_4 \pmod{113}$. Toistuvien lukujen määrä on $8 - 4 = 4$. Tilanne voidaan esittää kuvan avulla:



Muoto muistuttaa kreikkalaista kirjainta rho (ρ), jonka johdosta menetelmä tunnetaan Pollardin rho -menetelmänä.

1.2 Pollardin $p - 1$ menetelmä

Pollard p-1 -menetelmän tarkoitus on jakaa lukuja tekijöihin. Olkoon n jokin pariton yhdistetty kokonaisluku, jolla on sellainen alkulukutekijä p, että $p-1$ on pienten alkulukujen tulo.

Olkoon q jokin kokonaisluku siten, että $(p-1)|q$. Esimerkiksi q voisi olla $k!$, kun k on valittu riittävän suureksi. Seuraavaksi valitaan kokonaisluku a siten, että $1 < a < p-1$. Lasketaan $a^q \equiv m \pmod{n}$. Nyt koska $q = (p-1)j$ jollakin luvulla j, niin saadaan

$$m \equiv a^q \equiv (a^{p-1})^j \equiv 1^j = 1 \pmod{p}$$

Josta saadaan, että $p|(m-1)$. Näin saadaan $n > \text{syt}(m-1, n) > 1$, joka on siis luvun epätriviaali jakaja kun $m \not\equiv 1 \pmod{n}$. Jos $m \equiv 1 (\text{mod } n)$, niin tällöin $m - 1 = nk$, missä k on kokonaisluku. Tästä seuraa, että $\text{syt}(m-1, n) = \text{syt}(nk, n) = n$. Josta seuraa, että ei saada epätriviaalia jakajaa, kun $m \equiv 1 \pmod{n}$. Tekijää luvulle n ei myöskään välttämättä löydy, jos luku q on

valittu liian pieneksi tai luvun $p-1$ tekijät ovat liian suuria taikka pieniä alkutekijöitä suureen potenssiin.

Esimerkki 1.2. Olkoon $n = 9943$. Valitaan nyt $q = 5!$ ja $a = 2$. Lasketaan

$$2^{5!} (\text{mod } 9943)$$

Josta saadaan

$$\begin{aligned} 2^2 &\equiv 4 \text{ mod } 9943 \\ 4^3 &\equiv 64 \text{ mod } 9943 \\ 64^4 &\equiv 3375 \text{ mod } 9943 \\ 3375^5 &\equiv 2685 \text{ mod } 9943 \end{aligned}$$

Koska $\text{syt}(2685 - 1, 9943) = 61$, niin $61|9943$

1.3 Ketjumurtolukumenetelmä

Ketjumurtolukumenetelmää voidaan käyttää yhdistettyjen lukujen tekijöihinjaossa. Kehittyneiden tietokoneiden ansiosta ketjumurtolukumenetelmä on varteenotettava menetelmä. Morrison ja Brillhart jakoivat 39-numeron mittaisen Fermat'n luvun $F_7 = 2^{2^7} + 1$ tekijöihin ketjumurtolukumenetelmällä.

Määritelmä 1.3. Olkoon n reaaliluku. Lattiafunktion $\lfloor n \rfloor$ arvo on suurin kokonaisluku, joka on pienempi tai yhtäsuuri kuin n. Eli

$$\lfloor n \rfloor = max\{m \in \mathbb{Z} | m \leq n\}.$$

Olkoon n positiivinen luku, joka ei ole neliö. Ketjumurtolukuesitys luvulle $\sqrt{n}$ on muotoa

$$\sqrt{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

Merkitään esitystä notaatiolla $\sqrt{n} = [a_0; a_1, a_2, a_3, \ldots]$. Kokonaisluvut a_k ovat määritelty rekursiivisesti

$$\begin{aligned} a_0 &= \lfloor x_0 \rfloor, & x_0 &= \sqrt{n} \\ a_{k+1} &= \lfloor x_{x+1} \rfloor, & x_{k+1} &= \tfrac{1}{x_k - a_k} \end{aligned}$$

kaikille $k \geq 0$. Koska luku $\sqrt{n}$ on irrationaalinen, kun n ei ole neliö, ketjumurtolukuesitys luvulle $\sqrt{n}$ on äärettömän pitkä. Lukua voidaan approksimoida katkaistulla ketjumurtoluvulla, joka on rationaaliluku. Ketjumurtoluvun $\sqrt{n}$ k.s konvergentti on

$$C_k = [a_0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k}.$$

Esimerkki 1.4. Kolmannes konvergentti luvulle $\sqrt{n}$ on $[a_0; a_1, a_2, a_3]$, eli

$$\frac{a_3(a_2(a_1a_0 + 1) + a_0) + (a_1a_0 + 1)}{a_3(a_2a_1 + 1) + a_1}.$$

Luvut p_k ja q_k saadaan laskettua palautuskaavoilla:

$$p_{-2} = q_{-1} = 0, \quad p_{-1} = q_{-2} = 1$$

ja

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2} \text{ kaikille } k \geq 0 \end{aligned}$$

Määritellään kokonaislukujen $a_0, a_1, a_2, \ldots$ avulla kokonaisluvut s_k ja t_k seuraavasti

$$\begin{aligned} &s_0 = 0,\ t_0 = 1 \\ &s_{k+1} = a_k t_k - s_k,\ t_{k+1} = (n - s_{k+1}^2)/t_k \text{ kaikille } k \geq 0. \end{aligned}$$

Lause 1.5. *Jos luvut p_k/q_k ovat ketjumurtoluvun $\sqrt{n}$ konvergentteja ja $k = 0, 1, 2, 3, \ldots$, niin*

$$p_k^2 - nq_k^2 = (-1)^{k+1} t_{k+1}, \text{ missä } t_{k+1} > 0.$$

Lauseen 1.3 nojalla saadaan

$$p_{k-1}^2 \equiv (-1)^k t_k \pmod{n}.$$

Jos kokonaisluku t_k on neliö, kun k on parillinen kokonaisluku, esimerkiksi $t_k = y^2$, saadaan edellä mainitun yhtälön avulla

$$p_{k-1}^2 \equiv y^2 \pmod{n}.$$

Jos $p_{k-1} \not\equiv \pm y \pmod{n}$, niin $\text{syt}(p_{k-1} + y, n)$ ja $\text{syt}(p_{k-1} - y, n)$ ovat epätriviaaleja tekijöitä luvulle n.

Esimerkki 1.6. Valitaan tekijöihin jaettava luku $n = 1241$. Ketjumurtoluku luvulle n on muotoa

$$\sqrt{1241} = [35; 4, 2, 1, 1 \ldots]$$

Kerätään taulukkoon s_k, $t_k$ja p_k arvot:

k	0	1	2	3	4
a_k	35	4	2	1	1
s_k	0	35	29	21	11
t_k	1	16	25	32	35
p_k	35	141	317	458	775

Ensimmäinen t_k arvo, joka on neliö ja k on parillinen, on $t_2 = 25$. Saadaan kongruenssi

$$p_1^2 \equiv (-1)^2 t_2 \pmod{n}.$$

Sijoittamalla luvut saadaan

$$141^2 \equiv 5^2 \pmod{1241}.$$

Epätriviaalit tekijät ovat

$$\text{syt}(141 + 5, 1241) = 73$$
$$\text{syt}(141 - 5, 1241) = 17$$

Näin ollen $1241 = 17 \cdot 73$.

Epätriviaalia tekijää luvulle n ei kuitenkaan välttämättä löydy, vaikka t_k olisi neliö ja k parillinen.

Esimerkki 1.7. Valitaan kokonaisluku $n = 1121$, jolle ketjumurtolukuesitys on muotoa

$$\sqrt{1121} = [33; 2, 12, 1, 8, 1, 1, \ldots].$$

Tällöin voidaan kerätä taulukkoon s_k, t_k ja p_k arvot:

k	0	1	2	3	4	5	6
a_k	33	2	12	1	8	1	1
s_k	0	33	31	29	27	29	11
t_k	1	32	5	56	7	40	25
p_k	33	67	873	904	8069	8973	17042

Huomataan, että t_6 on neliö ja $k = 6$ on parillinen. Kongruenssiksi saadaan $p_5^2 \equiv (-1)^6 t_6 \pmod{1121}$, eli

$$8973^2 \equiv 5^2 \pmod{1121}$$

Epätriviaalia tekijää ei kuitenkaan löydy, sillä

$$\text{syt}(8973 + 5, 1121) = 1 \text{ ja}$$
$$\text{syt}(8973 - 5, 1121) = 1121.$$

Tässä tapauksessa epätriviaalia tekijää ei siis löytynyt, koska $8973 \equiv 5 \pmod{1121}$.

Kun ei löydy t_k arvoja, missä t_k on neliö ja k parillinen, voidaan löytää epätriviaali tekijä etsimällä joukko lukuja t_k, joiden tulo on neliö.

Esimerkki 1.8. Valitaan kokonaisluku $n = 7811$. Ketjumurtolukuesitys luvulle $\sqrt{7811}$ on muotoa

$$\sqrt{7811} = [88; 2, 1, 1, 1, 2, 1, 1, 2, \ldots].$$

Tällöin voidaan kerätä taulukkoon s_k, t_k ja p_k arvot:

k	0	1	2	3	4	5	6	7
a_k	88	2	1	1	1	2	1	1
s_k	0	88	46	39	35	54	56	29
t_k	1	67	85	74	89	55	85	82
p_k	88	177	256	442	707	1856	2563	4419

Huomataan, että lukujen t_2 ja t_6 tulo on neliö. Saadaan kaksi kongruenssia,

$$p_1^2 \equiv (-1)^2 t_2 \pmod{7811} \text{ ja } \quad p_5^2 \equiv (-1)^6 t_6 \pmod{7811}.$$

Kun tehdään sijoitukset, saadaan

$$177^2 \equiv 85 \pmod{7811} \text{ ja } \quad 1856^2 \equiv 85 \pmod{7811}.$$

Kerrotaan molemmat puolet keskenään ja saadaan

$$\begin{aligned} &(177 \cdot 1856)^2 \equiv 85^2 \pmod{7811}, \text{ eli} \\ &450^2 \equiv 85^2 \pmod{7811}. \end{aligned}$$

Täten löydetään epätriviaalit tekijät

$$\begin{aligned} &\text{syt}(450 + 85, 7811) = 107 \text{ ja} \\ &\text{syt}(450 - 85, 7811) = 73. \end{aligned}$$

Molemmat tekijät löydettiin, $7811 = 107 \cdot 73$.

Epätriviaalin tekijän voi löytää myös tarkastelemalla luvun $\sqrt{nm}$ ketjumurtolukuesitystä, missä m on alkuluku tai muutaman pienimmän alkuluvun tulo. Epätriviaali tekijä saattaa löytyä, kun löydetään kokonaisluvut x ja y, joille pätee $x^2 \equiv y^2 \pmod{mn}$.

Esimerkki 1.9. Valitaan kokonaisluvut $n = 1189$ ja $m = 6$. Tarkastellaan lukua $7134 = 1189 \cdot 6$. Ketjumurtolukuesitys on

$$\sqrt{7134} = [84; 2, 6, 3, 1, \ldots]$$

k	0	1	2	3	4
a_k	84	2	6	3	1
s_k	0	84	72	78	48
t_k	1	78	25	42	115
p_k	84	169	1098	3463	4561

Huomataan, että $t_2 = 25$ on neliö ja $k = 2$ on parillinen. Saadaan

$$p_1^2 \equiv (-1)^2 t_2 \pmod{7134}, \text{ eli}$$
$$169^2 \equiv 5^2 \pmod{7134}.$$

Epätriviaaliksi tekijäksi saadaan

$$\text{syt}(169 + 5, 7134) = \text{syt}(29 \cdot 6, 1189 \cdot 6) = 6 \cdot 29.$$

Eli 29 on epätriviaali tekijä, $1189 = 29 \cdot 41$.

1.4 Neliöseulan menetelmä

Neliöseulan menetelmää voidaan käyttää suurien yhdistettyjen lukujen tekijöihinjaossa. Esimerkiksi 129 numeron mittainen RSA-kisaluku on onnistuttu jakamaan tekijöihin tällä menetelmällä. Neliöseulan menetelmä perustuu Kraitchikin tekijöihinjakomenetelmään. Kraitchikin menetelmä perustuu siihen, että yhdistetty luku n voidaan jakaa tekijöihin, jos on olemassa kokonaisluvut x ja y siten, että ne toteuttavat

$$x^2 \equiv y^2 \pmod{n}$$

ja

$$x \not\equiv \pm y \pmod{n}.$$

Epätriviaalit tekijät luvulle n ovat silloin $\text{syt}(x - y, n)$ sekä $\text{syt}(x + y, n)$. Kraitchik etsi näitä kongruensseja laittamalla

$$x_i^2 \equiv y_i \pmod{n}, i = 1, 2, \ldots, r.$$

Tästä kerätään y_i arvot, joiden tulosta muodostuu neliö. Saadaan

$$(x_1 x_2, \cdots, x_r)^2 \equiv y_1 y_2 \cdots y_r = c^2 \pmod{n},$$

jolloin päästään haluttuun tilanteeseen $x^2 \equiv y^2 \pmod{n}$. Jotta tekijä löydetään, pitää täyttää vielä ehto $x \not\equiv \pm y \pmod{n}$.

John Brillhart sekä Michael Morrison kehittivät 1970-luvulla menetelmän edellä edellä mainittujen kongruenssien löytämiseen, missä $x_i^2 \equiv y_i \pmod{n}$ tulosta saadaan neliö. Menetelmässä valitaan aluksi tekijäkanta $\{-1, p_1, p_2, \ldots, p_r\}$, jossa luku p_1 on 2 ja luvut p_i ovat pieniä parittomia alkulukuja siten, että luku n on jokaisen luvun p_i neliönjäännös.

Määritelmä 1.10. Kokonaisluku a on luvun n neliönjäännös, jos on olemassa kokonaisluku x siten, että

$$x^2 \equiv a \pmod{n}.$$

Määritelmä 1.11. Olkoon p pariton alkuluku ja a kokonaisluku, Legendre symbolin $(\frac{a}{p})$ arvoksi asetetaan

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ jos } a \text{ on luvun } p \text{ neliönjäännös,} \\ -1, \text{ jos } a \text{ ei ole luvun } p \text{ neliönjäännös,} \\ 0, \text{ jos } a \equiv 0 \pmod{p}. \end{cases}$$

Esimerkki 1.12. Luku 6 on luvun 10 neliönjäännös, koska

$$4^2 = 16 \equiv 6 \pmod{10}.$$

Tällöin Legendren symboli $(6/10) = 1$.

Kun tekijäkanta on tehty, muodostetaan toisen asteen polynomi

$$f(x) = x^2 - n,$$

missä polynomia tarkastellaan luvun $\lfloor \sqrt{n} \rfloor$ ympäristössä. Valitaan arvot $x = \lfloor \sqrt{n} \rfloor, \pm 1 + \lfloor \sqrt{n} \rfloor, \pm 2 + \lfloor \sqrt{n} \rfloor, \ldots$. Kun -1 on lisätty tekijäkantaan, jokainen tekijäkannan luku jakaa vähintään yhden polynomin $f(x)$ arvoista.

Etsitään sellaiset $f(x)$ arvot, jotka muodostuvat pelkästään tekijäkannassa olevilla arvoilla, eli

$$f(x) = (-1)^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},\ k_0 = 0 \text{ tai } 1,\ k_i \geq 0 \text{ kaikille } i = 1, 2, \ldots, r$$

jolloin komponentit saadaan tallennettua $(r+1)$ kokoiseen eksponenttivektoriin. Eksponenttivektori on

$$v(x) = (k_0, j_1, j_2, \ldots, j_r), \text{ missä } j_i \equiv k_i \pmod 2 \text{ kaikille } i = 1, 2, \ldots, r.$$

Näin saadaan komponentin j_i arvoksi 1, jos tekijäkannan alkukulu p_i on luvun $f(x)$ tekijänä parittoman määrän kertoja tai 0 parillisilla kerroilla. Kun löydetään eksponenttivektoreita suurempi määrä kuin tekijäkannassa on tekijöitä, muodostuu lineaarinen riippuvuus joidenkin eksponenttivektorien välille. Lineaarinen riippuvuus voi kuitenkin muodostua aiemminkin. Toisin sanoen tällöin on olemassa osajoukko $x_1, x_2, \ldots, x_s$, jolle pätee

$$v(x_1) + v(x_2) + \cdots + v(x_s) \equiv (0, 0, \ldots, 0) \pmod 2,$$

eli jos lisätään nämä eksponenttivektorit yhteen, saadaan luvun $f(x)$ kaikki tekijät tuloon parillisen määrän kertoja. Saadaan

$$x_1^2 x_2^2 \cdots x_s^2 \equiv (x_1^2 - n)(x_2^2 - n) \cdots (x_s^2 - n) \equiv f(x_1) f(x_2) \cdots f(x_s) \equiv y^2 \pmod n,$$

missä y on kokonaisluku. Jos tämän lisäksi $(x_1 x_2 \cdots x_s) \not\equiv \pm y \pmod n$, saadaan luvulle n epätriviaaliksi tekijäksi $\text{syt}(x_1 x_2 \cdots x_s \pm y, n)$. Jos epätriviaalia ei löydy, kokeillaan toista eksponenttivektorien lineaarista riippuvuutta.

Esimerkki 1.13. Valitaan tutkittavaksi luvuksi $n = 8131$. Nyt $\lfloor \sqrt{n} \rfloor = 90$. Tekijäkannaksi valitaan $\{-1, 2, 3, 5, 7\}$. Tarkastellaan funktiota $f(x) = x^2 - 8131$ luvuilla $x = i + 90 (i = 0, \pm 1, \ldots, \pm 20)$ Kerätään taulukkoon kaikki $f(x)$ arvot, jotka jakautuvat täydellisesti tekijäkannan osiin.

x	$f(x)$	-1	2	3	5	7
79	$-1890 = -2 \cdot 3^3 \cdot 5 \cdot 7$	1	1	1	1	1
86	$-735 = -3 \cdot 5 \cdot 7^2$	1	0	1	1	0
89	$-210 = -2 \cdot 3 \cdot 5 \cdot 7$	1	1	1	1	1
91	$150 = 2 \cdot 3 \cdot 5^2$	0	1	1	0	0
109	$3750 = 2 \cdot 3 \cdot 5^4$	0	1	1	0	0

Taulukosta huomataan, että esimerkiksi $v(91)$ ja $v(109)$ ovat lineaarisesti riippuvia. Eli

$$v(91) + v(109) \equiv (0, 0, \ldots, 0) (\text{mod } 2),$$

Ja edelleen saadaan

$$f(91) \equiv 91^2 \equiv 2 \cdot 3 \cdot 5^2 (\text{mod } 8131)$$
$$f(109) \equiv 109^2 \equiv 2 \cdot 3 \cdot 5^4 (\text{mod } 8131)$$

Kerrotaan funktioiden arvot yhteen ja saadaan $(91 \cdot 109)^2 \equiv (2 \cdot 3 \cdot 5^3)^2 \pmod{8131}$ eli $9919^2 \equiv 750^2 \pmod{8131}$. Tämän lisäksi $9919 \not\equiv 750 \pmod{8131}$, josta seuraa, että $\text{syt}(9919 - 750, 8131) = 173$ ja $\text{syt}(9919 + 750, 8131) = 47$ ovat luvun 8131 epätriviaaleja tekijöitä.

Kun löydetään luku x, jolla alkuluku p jakaa $f(x)$, huomataan että jokainen $x + kp$ arvo on myös jaollinen luvulla p, koska

$$f(x + kp) = (x + kp)^2 - n \equiv x^2 - n = f(x) \pmod{p}.$$

kaikille $k = 0, \pm 1, \pm 2, \ldots$. Esimerkiksi luku 7 jakaa $f(79), f(86), f(93), \ldots$. Kaikki $f(x)$ arvot, joilla on tekijäkannan tekijöitä voidaan seuloa näin. Eli voidaan karsia pois luvut, joilla ei ole tekijäkannan tekijöitä.

2 Alkulukutestaus

2.1 Fermat'n jaollisuustesti

Lause 2.1. *Fermat'n pieni lause. Olkoon p alkuluku ja a kokonaisluku. Tällöin*

$$a^p \equiv a \pmod{p}$$

Koska Fermat'n pienen lauseen toteuttaa alkulukujen lisäksi ääretön määrä yhdistettyjä lukuja, ei testiä voida käyttää alkuluvuksi toteamiseen. Mutta koska kaikki alkuluvut toteuttavat lauseen, voidaan Fermat'n pienen lauseen avulla tutkia, onko jokin kokonaisluku yhdistetty. Olkoon $n > 1$ tutkittava

pariton kokonaisluku. Jos on olemassa kokonaisluku a siten, että $1 < a < n$ ja $a^{n-1} \not\equiv 1 \pmod{n}$, niin n on yhdistetty luku.

Kaikki yhdistetyt luvut, jotka toteuttavat Fermat'n pienen lauseen, ovat pseudoalkulukuja kannan a suhteen. On myös olemassa pseudoalkulukuja kaikille kantojen a suhteen, eli absoluuttisia pseudoalkulukuja tai Carmichael lukuja.

2.2 Lucasin testi

Lisäämällä rajoituksia Fermat'n pieneen lauseeseen, on mahdollista saada varmuus, onko tutkittava luku alkuluku. Edouard Lucasin teoreema on tällainen (1876).

Määritelmä 2.2. Olkoon n ja a positiivisia kokonaislukuja. Tällöin $ord_n(a)$ on pienin positiivinen kokonaisluku, jolla

$$a^{ord_n(a)} \equiv 1 \pmod{n}$$

Lause 2.3. *Lucas. Luku n on alkuluku, jos on olemassa kokonaisluku a siten, että $a^{n-1} \equiv 1 \pmod{n}$ ja $a^{(n-1)/p} \not\equiv 1 \pmod{n}$ kaikille alkuluvuille p, jotka ovat luvun $n-1$ tekijöitä.*

Todistus. Olkoon $k = ord_n(a)$. Oletuksena on, että $a^{n-1} \equiv 1 \pmod{n}$. Jakoalgoritmin mukaan $n-1 = jk+r$, $0 \leq r < k$. Jolloin $a^h = a^{jk+r} = (a^k)^j a^r$. Nyt koska $a^k \equiv 1 \pmod{n}$ ja $a^h \equiv 1 \pmod{n}$, niin täytyy $a^r \equiv 1 \pmod{n}$. Tästä saadaan $r = 0$, koska muuten saadaan ristiriita oletuksen $k = ord_n(a)$ kanssa. Oletuksesta $a^{n-1} \equiv 1 \pmod{n}$ siis seuraa, että $k|n-1$. Eli $n-1 = kj$, jollekin kokonaisluvulle j. Jos $j > 1$, niin luvulla j on alkulukutekijä q. On siis olemassa kokonaisluku h, jolle $j = qh$. Tästä seuraa

$$a^{(n-1)/q} = (a^k)^h \equiv 1^h = 1 \pmod{n},$$

joka on ristiriidassa lauseen kanssa. Kaikesta seuraa, että $j = 1$. Koska $ord_n(a) \leq \phi(n)$, niin $n-1 = k \leq \phi(n) \leq n-1$, josta seuraa että $\phi(n) = n-1$, jolloin luvun n täytyy olla alkuluku. □

Esimerkki 2.4. Olkoon $n = 1301$. Olkoon kantana $a = 2$, jolloin saadaan $2^{1300} \equiv 1 \pmod{1301}$. Lisäksi $n - 1 = 1300 = 2^2 \cdot 5^2 \cdot 13$. Lasketaan

$$\begin{aligned} 2^{1300/2} = 2^{650} &\equiv 1300 \pmod{1301} \\ 2^{1300/5} = 2^{260} &\equiv 163 \pmod{1301} \\ 2^{1300/13} = 2^{100} &\equiv 78 \pmod{1301}. \end{aligned}$$

Lauseen 2.2 nojalla 1301 on alkuluku.

Lausetta 2.2 paranneltiin 1960-luvulla niin, että kaikkia ehtoja ei tarvitse toteuttaa samalla kannalla.

Lause 2.5. *Jos jokaiselle luvun n alkulukutekijälle p_i on olemassa kokonaisluku a_i siten, että $a_i^{n-1} \equiv 1 \pmod{n}$, mutta $a_i^{(n-1)/p_i} \not\equiv 1 \pmod{n}$, niin n on alkuluku.*

Todistus. Olkoon $n - 1 = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, jossa p_i ovat eri alkulukuja. Olkoon $h_i = ord_n(a_i)$. Tällöin $h_i | n - 1$ ja $h_i \not| (n-1)/p_i$, joista seuraa että $p_i^{k_i} | h_i$. Koska jokaiselle luvulle i pätee $h_i | \phi(n)$, pätee myös $p_i^{k_i} | \phi(n)$. Tästä seuraa, että $n - 1 | \phi(n)$, joten n on alkuluku. □

Esimerkki 2.6. Kuten edellisessä esimerkissä, olkoon $n = 1301$. Luvun $n-1$ alkulukutekijät ovat siis 2, 5 ja 13. Valitaan kannoiksi 2, 3 ja 5 ja lasketaan

$$\begin{aligned} 2^{1300/2} = 2^{650} &\equiv 1300 \pmod{1301} \\ 3^{1300/5} = 3^{260} &\equiv 1019 \pmod{1301} \\ 5^{1300/13} = 5^{100} &\equiv 988 \pmod{1301}. \end{aligned}$$

Lauseen 2.4 nojalla 1301 on alkuluku.

Vuonna 1914 Henry Pocklington näytti, ettei ole tarpeellista tietää kaikkia luvun $n - 1$ tekijöitä. Kun luvun $n - 1$ tekijöitä löydetään siihen asti, että tekijöihin jaettu osa on suurempi kuin jakamatta oleva osa, voidaan tutkia luvun n jaollisuutta.

Lause 2.7. *Olkoon* $n-1 = mj$, *missä* $m = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$, $m \geq \sqrt{n}$ *ja* $syt(m,j) = 1$. *Jos jokaista alkulukua* p_i $(1 \leq i \leq s)$ *kohti on olemassa kokonaisluku* a_i, *jolle pätee* $a_i^{n-1} \equiv 1 \pmod{n}$ *ja* $syt(a_i^{(n-1)/p_i} - 1, n) = 1$, *niin luku* n *on alkuluku.*

Todistus. Olkoon p luvun n alkulukutekijä ja $h_i = ord_p(a_i)$. Tällöin $h_i|p-1$. Koska $a_i^{n-1} \equiv 1 \pmod{p}$, saadaan $h_i|n-1$. Oletus $\text{syt}(a_i^{(n-1)/p_i} - 1, n) = 1$ näyttää, että $a_i^{(n-1)/p_i} \not\equiv 1 \pmod{p}$, jolloin $h_i \not| (n-1)/p_i$. Voidaan päätellä, että $p_i^k|h_i$, josta seuraa $p_i^{k_i}|p-1$. Koska tämä on totta jokaiselle i, niin $m|p-1$. Tästä seuraa, että mikä tahansa luvun n alkulukutekijä on suurempi kuin $m \geq \sqrt{n}$. Tämä on ristiriita, joten n on alkuluku. □

Esimerkki 2.8. Valitaan taas $n = 997$. Nyt $n - 1 = 996 = 12 \cdot 83$, missä $83 > \sqrt{997}$. Olkoon kanta $a = 2$. Nyt $2^{996} \equiv 1 (\text{mod } 997)$.

$$\text{syt}(2^{996/83} - 1, 997) = \text{syt}(4095, 997) = 1$$

Joten voidaan jälleen kerran todeta, että 997 on alkuluku.

2.3 Miller-Rabinin jaollisuustesti

Fermat'n jaollisuustestin tavoin Miller-Rabinin testillä voidaan määrittää, onko luku yhdistetty. On hyvä pitää mielessä, vaikka lukua ei testissä todettaisi yhdistetyksi, voi se silti olla yhdistetty.

Olkoon n tutkittava luku ja olkoon $n - 1 = 2^h m$, missä m on pariton kokonaisluku. Olkoon $1 < a < n - 1$ kokonaisluku. Muodostetaan jono

$$a^m, a^{2m}, a^{4m}, \ldots, a^{2^{h-1}m}, a^{2^h m} = a^{n-1} \pmod{n},$$

missä jokainen alkio on edeltäjän neliö. Luku n läpäisee Miller-rabinin testin kannalle a, jos luku 1 esiintyy ensimmäisen kerran ensimmäisessä termissä, tai kaikki seuraavat termit ovat -1.

Pariton kokonaisluku n voidaan todeta yhdistetyksi, jos se ei läpäise testiä.

Lause 2.9. *Olkoon p pariton alkuluku ja $p-1 = 2^h m$, missä m on pariton kokonaisluku ja $h \geq 1$. Tällöin mille tahansa kokonaisluvulle a $(1 < a < p-1)$ pätee $a^m \equiv 1 \pmod{p}$ tai $a^{2^j m} \equiv -1 \pmod{p}$ jollain kokonaisluvulla $j = 1, 2, \ldots, h-1$*

Todistus. Olkoon $k = ord_p(a)$. Tällöin $k|p-1 = 2^h m$. Kun k on pariton niin $k|m$, joten $m = kr$ ja r on kokonaisluku.

$$a^m = (a^k)^r \equiv 1^r = 1 \pmod{p}.$$

Kun k on parillinen, $k = 2^{j+1}d$ missä $j \geq 0$ ja d on pariton kokonaisluku. Koska $k|2^h m$, niin $2^{j+1}d|2^h m$. Tästä seuraa, että $j+1 \leq h$ ja $d|m$. Kongruenssista $a^{2^{j+1}d} \equiv 1 \pmod{p}$ saadaan $a^{2^j d} \equiv \pm 1 \pmod{p}$. Koska $k = ord_p(a)$, niin $a^{2^j d} \equiv 1 \pmod{p}$ ei ole mahdollista. Tästä seuraa, että $a^{2^j d} \equiv -1 \pmod{p}$. Saadaan $m = dt$ jollekin parittomalle kokonaisluvulle t. Tästä seuraa

$$a^{2^j m} = (a^{2^j d})^t \equiv (-1)^t = -1 \pmod{p}.$$

lause siis pätee, kun p on pariton alkuluku. □

Esimerkki 2.10. Olkoon $n = 2201$. Nyt $n - 1 = 2^3 \cdot 275$. Tarkastellaan seuraavia kongruensseja (mod 2201)

$$\begin{aligned} 2^{275} &\equiv 1582 \\ 2^{550} &\equiv 187 \\ 2^{1100} &\equiv 1954 \\ 2^{2200} &\equiv 1582 \end{aligned}$$

Joten 2201 ei läpäise Miller-Rabinin testiä kannalle $a = 2$. Näin ollen 2201 on siis yhdistetty luku.

Miller-Rabinin testin läpäisy ei siis kerro onko luku alkuluku, koska ääretön määrä yhdistettyjä lukuja läpäisee Miller-Rabinin testin. Parittomia yhdistettyjä lukuja jotka läpäisevät Miller-Rabinin testin kutsutaan vahvoiksi pseudoalkuluvuiksi.

Lause 2.11. *Kaikki Fermat'n yhdistetyt luvut* $F_n = 2^{2^n} + 1$ *ovat vahvoja pseudoalkulukuja kannalle 2.*

Todistus. Luku $F_n - 1 = 2^h \cdot m$, missä $h = 2^n$, $m = 1$ ja $a = 2$. Tarkastellaan kongruenssia

$$2^{2^j m} = 2^{2^j} \equiv -1 \pmod{F_n}.$$

Valitaan $j = n < 2^n = h$. Kongruenssiksi saadaan $2^{2^n} \equiv -1 \pmod{F_n}$, joka pätee, koska $F_n = 2^{2^n} + 1 | (2^{2^n} + 1)$. Näin ollen kaikki Fermat'n luvut läpäisevät Miller-Rabinin testin kannalle $a = 2$. □

Lähdeluettelo

[1] *David M. Burton(1997). Elementary number theory. University of New Hampshire: Elizabeth J. Haefele.*