TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Timo D. Talvitie

Kokonaisluvun kertaluvun sovelluksia

Matematiikan ja tilastotieteen laitos
Matematiikka
Huhtikuu 2008

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

TALVITIE, TIMO D. : Kokonaisluvun kertaluvun sovelluksia

Pro gradu -tutkielma, 23 s.

Matematiikka

Huhtikuu 2008

Tiivistelmä

Tässä tutkielmassa perehdymme lukuteorian alaan kuuluvien kokonaisluvun kertaluvun ja primiitiivisten juurten sovelluksiin.

Ensimmäisessä luvussa käymme läpi muutamia valmistavia tarkasteluja ja taustateoriaan, joita tarvitsemme varsinaisessa aiheessa eli sovelluksissa. Määrittelemme muun muassa *kokonaisluvun kertaluvun, primitiivisten juurten ja diskreetin logaritmin* käsitteet.

Toisessa luvussa pääsemme jo käsiksi sovelluksiin ja esittelemme erilaisia alkulukutestejä. Havainnollistamme yksinkertaisten esimerkkien avulla eri testien toimivuutta.

Kolmannessa luvussa heittäydymme tietotekniseksi ja luomme katsauksen pseudosatunnaislukujen generoimiseen. Esittelemme erilaisia menetelmiä ja havainnollistamme jälleen niiden käyttöä esimerkkien avulla.

Viimeisessä luvussa esittelemme erään lukuteorian kryptologisen sovelluksen eli ElGamalin salausjärjestelmän. Näytämme, kuinka sen avulla voidaan salata ja purkaa viestejä sekä sähköisesti allekirjoittaa niitä.

Tämän tutkielman rakenne noudattelee pääosin Kenneth H. Rosenin teosta *Elementary Number Theory and Its Applications, fifth edition*.

Sisältö

Johdanto **3**

1 Valmistavia tarkasteluja **4**
1.1 Eulerin funktio 4
1.2 Kokonaisluvun kertaluku 4
1.3 Primitiiviset juuret 5
1.4 Diskreetti logaritmi 6
1.5 Universaali eksponentti 6

2 Alkulukutestit **7**
2.1 Lucasin lause ja sen seuraukset 7
2.2 Pocklingtonin alkulukutesti 10
2.3 Prothin alkulukutesti 11

3 Pseudosatunnaislukugeneraattorit **12**
3.1 Lineaarinen kongruenssimenetelmä 13
3.2 Puhtaasti multiplikatiivinen kongruenssimenetelmä 14
3.3 Neliöpseudosatunnaislukugeneraattori 16

4 ElGamalin salausjärjestelmä **18**
4.1 Viestien salaus ja salauksen purku 18
4.2 Viestien sähköinen allekirjoittaminen 20

Viitteet **23**

Johdanto

Tässä tutkielmassa perehdymme lukuteorian alaan kuuluvien kokonaisluvun kertaluvun ja primiitiivisten juurten sovelluksiin. Lukuteorian tutkimuksen historiaan kuuluvat oleellisesti matemaatikot Leonhard Euler ja Carl Friedrich Gauss, joita pidetään eräinä kaikkien aikojen suurimmista matemaatikoista. Euler muun muassa havaitsi vuonna 1773, että jokaisella alkuluvulla on primitiivinen juuri. Tässä tutkielmassa käyttämämme Eulerin funktio on luonnollisesti myös Eulerin käsialaa. Gauss puolestaan esitteli ensimmäisenä käsitteen *luvun a kertaluku modulo m*. Gauss kehitti myös merkittävästi lukuteoriaa vuonna 1801 julkaistussa kirjassaan *Disquisitiones Arithmeticae*, jossa hän esitteli muun muassa *diskreetin logaritmin* käsitteen.

Ensimmäisessä luvussa käymme läpi muutamia valmistavia tarkasteluja ja taustateoriaan, joita tarvitsemme varsinaisessa aiheessa eli sovelluksissa. Määrittelemme muun muassa *kokonaisluvun kertaluvun, primitiivisten juurten ja diskreetin logaritmin* käsitteet. Lauseiden todistukset on sivuutettu, etteivät ne veisi päähuomiota tutkielman varsinaiselta aiheelta eli sovelluksilta.

Toisessa luvussa pääsemme jo käsiksi sovelluksiin ja esittelemme erilaisia alkulukutestejä. Havainnollistamme yksinkertaisten esimerkkien avulla eri testien toimivuutta.

Kolmannessa luvussa heittäydymme tietotekniseksi ja luomme katsauksen pseudosatunnaislukujen generoimiseen. Esittelemme erilaisia menetelmiä ja havainnollistamme jälleen niiden käyttöä esimerkkien avulla.

Viimeisessä luvussa esittelemme erään lukuteorian kryptologisen sovelluksen eli ElGamalin salausjärjestelmän. Näytämme, kuinka sen avulla voidaan salata ja purkaa viestejä sekä sähköisesti allekirjoittaa niitä.

Tutkielmassa emme käsittele likimainkaan kaikkea pohjateoriaa, mitä sovellukset vaativat. Tämän seurauksena edellytämme lukijalta joidenkin lukuteorian, joukko-opin, logiikan ja algebran perusasioiden tuntemusta. Esimerkiksi kongruenssin sievennykset ja käsitteet joukon hyvinjärjestys ja supistettu jäännössysteemi oletamme tunnetuiksi.

Tämän tutkielman rakenne noudattelee pääosin Kenneth H. Rosenin teosta *Elementary Number Theory and Its Applications, fifth edition*. Tutkielmassa esiintyvät todistukset ovat pääosin lähdeteoksista. Tekijä on tosin tehnyt joitain parannuksia yksittäisissä todistuksissa. Kaikki esimerkit ovat tekijän itse ratkaisemia, vaikkakin moniin niistä on otettu mallia lähdeteosten vastaavanlaisista esimerkeistä.

Esimerkkien ratkaisuissa on käytetty ahkerasti apuna Mathematica-ohjelmistoa. Isojen kongruenssilaskujen ratkaisuissa on käytetty funktiota Mod$[a, m]$, joka palauttaa laskun a/m jakojäänöksen ja käänteislukujen ratkaisemisen yhteydessä on käytetty PowerMod$[a, -1, m]$, joka antaa luvun a käänteisluvun modulo m.

1 Valmistavia tarkasteluja

Tässä kappaleessa tarkastelemme varsinaisissa sovelluksissa tarvittavia määritelmiä ja lauseita.

1.1 Eulerin funktio

Määritelmä. Olkoon m positiivinen kokonaisluku. *Eulerin funktio* $\phi(m)$ on niiden lukua m pienempien positiivisten kokonaislukujen määrä, jotka ovat suhteellisia alkulukuja luvun m kanssa.

Lause 1.1. *Jos p on alkuluku, niin $\phi(p) = p-1$. Käänteisesti, jos p on positiivinen kokonaisluku ja $\phi(p) = p-1$, niin p on alkuluku.*

Todistus. Ks. [1, s. 240]. □

1.2 Kokonaisluvun kertaluku

Olkoot a ja $m(>0)$ keskenään jaottomia kokonaislukuja. Tällöin Eulerin-Fermat'n lauseen mukaan $a^{\phi(n)} \equiv 1 \pmod{m}$. Näin ollen on olemassa ainakin yksi sellainen positiivinen kokonaisluku x, joka toteuttaa kongruenssin $a^x \equiv 1 \pmod{m}$. Koska positiivisten kokonaislukujen joukko on hyvinjärjestetty ([3, s. 35], on olemassa pienin tällainen positiivinen kokonaisluku x, joka toteuttaa kongruenssin.

Määritelmä. Olkoot a ja m keskenään jaottomia positiivisia kokonaislukuja. Silloin luvun *a kertaluku modulo m* on pienin sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$. Merkitään $x = ord_m a$.

Lause 1.2. *Olkoot a ja $m(>0)$ keskenään jaottomia kokonaislukuja. Silloin positiivinen kokonaisluku x on kongruenssin $a^x \equiv 1 \pmod{m}$ ratkaisu, jos ja vain jos $ord_m a \mid x$.*

Todistus. Ks. [1, s. 334]. □

Seuraus 1.2.1. *Jos a ja $m(>0)$ ovat keskenään jaottomia kokonaislukuja, niin $ord_m a \mid \phi(m)$.*

Todistus. Ks. [1, s. 335]. □

Lause 1.3. *Olkoot a ja $m(>0)$ keskenään jaottomia kokonaislukuja ja i sekä j ei-negatiivisia kokonaislukuja. Tällöin*

$$a^i \equiv a^j \pmod{m} \iff i \equiv j \pmod{ord_m a}.$$

Todistus. Ks. [1, s. 336]. □

Propositio 1. *Olkoon $ord_m a = k$ ja $ord_m b = l$. Tällöin on olemassa alkio g kertalukua $[k, l]$.*

Todistus. Ks. [2, s. 177]. □

1.3 Primitiiviset juuret

Jos a on sellainen positiivinen kokonaisluku, että $(a, m) = 1$, niin seurauksen 1.2.1 mukaan $ord_m a \mid \phi(m)$, joten luvun $ord_m a$ suurin arvo on $\phi(m)$. Tästä seuraa primitiivisen juuren määritelmä.

Määritelmä. Olkoot a ja $m(> 0)$ keskenään jaottomia kokonaislukuja. Jos $ord_m a = \phi(m)$, niin a on *primitiivinen juuri* modulo m.

Lause 1.4. *Olkoot r ja $m(> 0)$ keskenään jaottomia kokonaislukuja. Jos r on primitiivinen juuri modulo m, niin kokonaisluvut*

$$r^1, r^2, \ldots, r^{\phi(m)}$$

muodostavat supistetetun jäännössysteemin modulo m.

Todistus. Ks. [1, s. 337]. □

Kun kokonaisluvulla on primitiivinen juuri, sillä on yleensä useampia primitiivisiä juuria.

Lause 1.5. *Jos $ord_m a = t$ ja u on positiivinen kokonaisluku, niin*

$$ord_m(a^u) = \frac{t}{(t, u)} .$$

Todistus. Ks. [1, s. 338]. □

Seuraus 1.3.1. *Olkoon r primitiivinen juuri modulo $m(> 1)$. Tällöin r^u on primitiivinen juuri modulo m, jos ja vain jos $(u, \phi(m)) = 1$.*

Todistus. Ks. [1, s. 338]. □

Lause 1.6. *Jos positiivisella kokonaisluvulla m on primitiivinen juuri, niin epäkongruenttien pritiivisten juurten kokonaismäärä on $\phi(\phi(m))$.*

Todistus. Ks. [1, s. 338]. □

Lause 1.7. *Jos p on alkuluku ja $d \mid p - 1$, niin kongruenssilla $x^d - 1 \equiv 0 \pmod{p}$ on täsmälleen d epäkongruenttia ratkaisua modulo p.*

Todistus. Ks. [1, s. 343]. □

Seuraus 1.3.2. *Jokaisella alkuluvulla on pritiivinen juuri.*

Todistus. Ks. [1, s. 343]. □

1.4 Diskreetti logaritmi

Lauseen 1.4 perusteella tiedämme, että kokonaisluvut

$$r^1, r^2, \ldots, r^{\phi(m)}$$

muodostavat supistetetun jäännössysteemin modulo m. Nyt, jos kokonaisluku a on suhteellinen alkuluku luvun m kanssa, on olemassa sellainen kokonaisluku x, että $1 \leq x \leq \phi(m)$ ja

$$r^x \equiv a \pmod{m}.$$

Tästä seuraa *diskreetin logaritmin* määritelmä.

Määritelmä. Olkoon r primitiivinen juuri modulo m ja a suhteellinen alkuluku luvun m suhteen. Tällöin lukua x, joka täyttää ehdot $1 \leq x \leq \phi(m)$ ja $r^x \equiv a \pmod{m}$, sanotaan luvun *a r-kantaiseksi diskreetiksi logaritmiksi (ts. indeksiksi) modulo m*. Merkitään $x = ind_r a$.

1.5 Universaali eksponentti

Olkoon $m = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}$ positiivinen kokonaisluku, missä luvut $p_1, p_2, \ldots, p_n$ ovat erisuuria alkulukuja. Jos $(a, m) = 1$, niin Eulerin-Fermat'n lauseen mukaan

$$a^{\phi(p^t)} \equiv 1 \pmod{p^t},$$

missä p^t on yksi luvun m alkulukutekijöistä.
Merkitään $U = [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_n^{t_n})]$ eli U on kokonaislukujen $\phi(p_i^{t_i})$ $(i = 1, 2, \ldots, n)$ pienin yhteinen monikerta. Koska $\phi(p_i^{t_i}) \mid U$, niin lauseen 1.2 mukaan $a^U \equiv 1 \pmod{p_i^{t_i}}$, kun $i = 1, 2, \ldots, n$. Tiedetään, että jos

$$a \equiv b \pmod{n_1}, a \equiv b \pmod{n_2}, \ldots, a \equiv b \pmod{n_k},$$

missä a ja b ovat kokonaislukuja ja luvut $n_1, n_2, \ldots, n_k$ ovat pareittain suhteellisia alkulukuja, niin

$$a \equiv b \pmod{n_1 n_2 \cdots n_k}.$$

Näin ollen kongrunssista

$$a^U \equiv 1 \pmod{p_i^{t_i}}, \quad \text{kun } i = 1, 2, \ldots, n,$$

seuraa, että

$$a^U \equiv 1 \pmod{m}.$$

Tästä seuraa *universaalin eksponentin* määritelmä.

Määritelmä. Positiivisen kokonaisluvun *m universaali eksponentti* on sellainen positiivinen kokonaisluku U, että

$$a^U \equiv 1 \pmod{m},$$

aina, kun a on suhteellinen alkuluku luvun m suhteen.

Määritelmä. *Pienin universaali ekponentti* λ on pienin sellainen positiivinen kokonaisluku, että

$$a^\lambda \equiv 1 \pmod{m}$$

aina, kun a on suhteellinen alkuluku luvun m suhteen.

2 Alkulukutestit

Jos p on alkuluku ja a on sellainen kokonaisluku, että $(a, p) = 1$, niin Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$. Käänteislause ei kuitenkaan ole tosi, sillä vaikka $a^{m-1} \equiv 1 \pmod{m}$, missä a on positiivinen kokonaisluku, m voi edelleen olla yhdistetty luku. Voimmeko sitten muodostaa osittaisia käänteislauseita eli oletuksia lisäämällä saada käänteislauseen todeksi?

Tässä kappaleessa todistamme muutamia Fermat'n pienen lauseen osittaisia käänteislauseita. Aloitamme tuloksella, jonka todisti matemaatikko Edouard Lucas vuonna 1876. Tuloksen kuitenkin julkaisi ensimmäisenä D.H. Lehmer vuonna 1927.

2.1 Lucasin lause ja sen seuraukset

Lause 2.1 (Lucasin lause)**.** *Olkoon m positiivinen kokonaisluku. Jos on olemassa sellainen kokonaisluku x, että*

$$x^{m-1} \equiv 1 \pmod{m}$$

ja

$$x^{(m-1)/q} \not\equiv 1 \pmod{m}$$

kaikilla luvun $m-1$ alkulukutekijöillä q, niin m on alkuluku.

Todistus. (Vrt. [1, s. 366]) Koska $x^{m-1} \equiv 1 \pmod{m}$, niin on oltava $(x, m) = 1$. Nyt lauseen 1.2 nojalla $ord_m x \mid m-1$. Osoitamme, että $ord_m x = m-1$. Tehdään vastaoletus ts. oletetaan, että $ord_m x \neq m-1$. Koska $ord_m x \mid m-1$, on olemassa sellainen kokonaisluku k, että $m-1 = k \cdot ord_m x$. Nyt $k > 1$, koska vastaoletuksen mukaan $ord_m x \neq m-1$. Olkoon q luvun k alkulukutekijä. Nyt

$$x^{(m-1)/q} = x^{(k \cdot ord_m x)/q} = (x^{ord_m x})^{k/q} \equiv 1^{k/q} \equiv 1 \pmod{m},$$

mikä on ristiriidassa lauseen oletusten kanssa. Täten on oltava $ord_m x = m - 1$. Koska $ord_m x \leq \phi(m)$ ja $\phi(m) \leq m - 1$, niin $\phi(m) = m - 1$. Lauseen 1.1 perusteella m on alkuluku. □

Huomautus. Lauseen todistuksessa on lähdeteoksessa virhe. Lähdeteoksessa yhtälö on saatu muotoon $x^{(n-1)/q} = x^{k/(ord_n x \cdot q)}$, kun sen pitäisi olla $x^{(n-1)/q} = x^{(k \cdot ord_n x)/q}$.

Lauseesta 2.1 seuraa, että jos on olemassa kokonaisluku kertalukua $m - 1$ modulo m, niin m on alkuluku.

Esimerkki 1. Osoitamme, että luku $m = 127$ on alkuluku käyttämällä Lucasin lausetta 2.1). Valitaan $x = 3$. Nyt

$$3^{126} \equiv 1 \pmod{127}.$$

Koska $126 = 2 \cdot 3^2 \cdot 7$, niin luvun $m - 1 = 126$ alkulukutekijät ovat 2, 3 ja 7. Laskemalla saamme

$$\begin{aligned} 3^{126/2} &\equiv 3^{63} \equiv 126 \pmod{127}, \\ 3^{126/3} &\equiv 3^{42} \equiv 107 \pmod{127}, \\ 3^{126/7} &\equiv 3^{18} \equiv 4 \pmod{127}. \end{aligned}$$

Lauseen 2.1 nojalla 127 on alkuluku.

Seuraava lause on hieman Lucasin lausetta tehokkaampi alkulukutesti.

Lause 2.2. *Olkoon m pariton positiivinen kokonaisluku. Jos on olemassa sellainen kokonaisluku x, että*

$$x^{(m-1)/2} \equiv -1 \pmod{m}$$

ja

$$x^{(m-1)/q} \not\equiv 1 \pmod{m}$$

kaikilla parittomilla luvun $m - 1$ alkulukutekijöillä q, niin m on alkuluku.

Todistus. (Vrt. [1, s. 366]) Koska $x^{(m-1)/2} \equiv -1 \pmod{m}$, niin

$$x^{m-1} \equiv (x^{(m-1)/2})^2 \equiv (-1)^2 \equiv 1 \pmod{m}.$$

Nyt Lucasin lauseen ehdot toteutuvat, joten m on alkuluku. □

Esimerkki 2. Osoitamme, että 271 on alkuluku käyttämällä lausetta 2.2. Valitaan $x = 6$. Nyt

$$6^{270/2} \equiv 6^{135} \equiv -1 \pmod{271}.$$

Koska $270 = 2 \cdot 3^3 \cdot 5$, niin luvun $m - 1 = 270$ parittomat alkulukutekijät ovat 3 ja 5. Laskemalla saamme

$$\begin{aligned} 6^{270/3} &\equiv 6^{90} \equiv 242 \pmod{271}, \\ 6^{270/5} &\equiv 6^{54} \equiv 10 \pmod{271}. \end{aligned}$$

Lauseen 2.2 nojalla 271 on alkuluku.

On tärkeätä tarkastaa ensin, että $x^{m-1} \equiv 1 \pmod{m}$ (tai vaihtoehtoisesti, että $x^{(m-1)/2} \equiv -1 \pmod{m}$), sillä todistuksen loppuosa ei ole pätevä ilman tämän ehdon voimassaoloa. Ehdon täyttävä kokonaisluku x on primitiivinen juuri modulo m. Useimmiten kyseinen primitiivinen juuri on nopea löytää kokeilemalla peräkkäisiä kokonaislukuja $2, 3, 4 \ldots$.
Joskus pienin primitiivinen juuri on kuitenkin todella suuri ja siten ehdon täyttävän luvun x etsiminen vaatii paljon aikaa. Teemme seuraavaksi sellaisen parannuksen lauseen ehtoihin, että ei ole enää välttämätöntä löytää primitiivistä juurta väitteen $\phi(m) = m - 1$ todistamiseen.
Jos luku x ei toteuta Lucasin lauseen (lause 2.1) kongruenssin ehtoa, niin on olemassa sellainen q, että

$$x^{(m-1)/q} \equiv 1 \pmod{m}.$$

Monille muille alkuluvuille q' on kuitenkin mahdollista, että

$$x^{(m-1)/q'} \not\equiv 1 \pmod{m}.$$

Sen sijaan, että jatkaisimme sopivan kantaluvun x etsimistä, voimme käyttää havaitsemaamme tietoa hyväksemme. Seuraavassa lauseessa näytämme kuinka voimme käyttää tietoa väitteen $\phi(m) = m - 1$ todistamiseen. Parannus on mahdollinen, sillä ei ole välttämätöntä löytää alkiota kertalukua $m - 1$ modulo m, vaan osoittaa, että sellainen on olemassa(propositio 1).

Lause 2.3. *Olkoon $q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$ luvun $m - 1$ alkulukukehitelmä. Olkoon jokaista lukua i, $1 \leq i \leq k$, kohti olemassa sellainen kokonaisluku a_i, että*

$$a_i{}^{m-1} \equiv 1 \pmod{m}$$

ja

$$a_i{}^{(m-1)/q_i} \not\equiv 1 \pmod{m}.$$

Tällöin m on alkuluku.

Todistus. (Vrt. [2, s. 188]) Osoitamme, että jokainen luvun $m - 1$ alkulukukehitelmän termeistä $q_i^{e_i}$ jakaa luvun $\phi(m)$ ja siten myös niiden tulokin jakaa luvun $\phi(m)$. Kiinnitetään indeksi i; jos a_i toteuttaa kongruenssin

$$a_i{}^{m-1} \equiv 1 \pmod{m},$$

niin $(a_i, m) = 1$ ja edelleen lauseen 1.2 perusteella $ord_m a_i \mid m - 1$. Olkoon $m - 1 = k \cdot ord_m a_i$. Väitetään, että $q_i \nmid k$. Jos $q_i \mid k$, niin

$$a_i^{(m-1)/q_i} = a_i^{ord_m a_i \cdot k/q_i} \equiv 1^{k/q_i} \equiv 1 \pmod{m},$$

mikä on ristiriidassa oletuksen kanssa. Koska $(q_i, k) = 1$ ja $q_i^{e_i}$ esiintyy luvun $m - 1 = k \cdot ord_m a$ alkulukukehitelmässä, niin $q_i^{e_i} \mid ord_m a_i$. Täten $m - 1 \mid \phi(m)$ eli m on alkuluku. □

Esimerkki 3. Käytämme lausetta 2.3 todistaaksemme, että $m = 311$ on alkuluku. Luvun $m - 1$ alkulukukehitelmä $311 = 2 \cdot 5 \cdot 31$. Laskemalla saamme

$$\begin{aligned} 11^{310} &\equiv 1 \pmod{m} \quad \text{ja} \quad 11^{(310)/2} \equiv 11^{155} \equiv -1 \not\equiv 1 \pmod{m}, \\ 2^{310} &\equiv 1 \pmod{m} \quad \text{ja} \quad 2^{(310)/7} \equiv 2^{62} \equiv 52 \not\equiv 1 \pmod{m}, \\ 2^{310} &\equiv 1 \pmod{m} \quad \text{ja} \quad 2^{(310)/13} \equiv 2^{10} \equiv 91 \not\equiv 1 \pmod{m}. \end{aligned}$$

Lauseen 2.3 nojalla 311 on alkuluku. Pienin primiitivinen juuri modulo 311 on 17. Täten kehittyneemmän tavan käyttö on tehokkaampaa kuin primitiivisen juuren etsiminen.

2.2 Pocklingtonin alkulukutesti

Toisen Fermat'n pienen lauseen osittaisen käänteislauseen kehitti Henry Pocklington vuonna 1914. Hän osoitti, että luku m voidaan todistaa alkuluvuksi käyttämällä luvun $m - 1$ osittaista alkulukukehitelmää. Käytämme seuraavassa todistuksessa yleistä merkintää $m - 1 = FR$, missä F on se osa luvusta $m - 1$, joka on jaettu alkulukutekijöihinsä ja R on jäljelle jäävä jakamaton osa.

Lause 2.4 (Pocklingtonin alkulukutesti)**.** *Olkoon m sellainen kokonaisluku, että $m - 1 = FR$, missä $(F, R) = 1$ ja $F > R$. Luku m on alkuluku, jos on olemassa sellainen kokonaisluku a, että*

$$a^{m-1} \equiv 1 \pmod{m}$$

ja

$$(a^{(m-1)/q} - 1, m) = 1$$

aina, kun q on sellainen alkuluku, että $q \mid F$.

Todistus. (Vrt. [1, s. 368]) Oletetaan luvun a täyttävän oletusten ehdot. Olkoon p sellainen luvun m alkulukujakaja, että $p \leq \sqrt{m}$. Koska $a^{m-1} \equiv 1 \pmod{m}$ ja $p \mid m$, niin $a^{m-1} \equiv 1 \pmod{p}$. Näin ollen lauseen 1.2 mukaan $ord_p a \mid m-1$. On siis olemassa sellainen kokonaisluku t, että $m-1 = t \cdot ord_p a$. Oletetaan sitten, että q on sellainen alkuluku, että $q \mid F$. Osoitetaan, että $q \nmid t$. Tehdään vastaoletus, että $q \mid t$. Nyt

$$a^{(m-1)/q} = a^{ord_p a(t/q)} \equiv 1^{t/q} \equiv 1 \pmod{p}.$$

Nyt siis $p \mid a^{(m-1)/q} - 1$ ja $p \mid m$ eli $p \mid (a^{(m-1)/q} - 1, m)$. Tämä on ristiriidassa oletusten kanssa. Siis on oltava $q \nmid t$. Täten $q^e \mid ord_p a$, missä q^e on alkuluvun q ilmentymä alkulukukehitelmässä. Koska tämä pätee jokaiselle luvun F alkulukutekijälle, niin $F \mid ord_p a$. Koska $ord_p a \mid p - 1$, $F \mid p - 1$, joten $F < p$. Oletusten mukaan $F > R$ ja $m - 1 = FR$. Täten $m - 1 < F^2$. Koska sekä $m - 1$ että F^2 ovat kokonaislukuja, niin $m \leq F^2$ ja siten $p > F \geq \sqrt{m}$. Täten m on alkuluku. □

Esimerkki 4. Osoitamme, käyttämällä Pocklingtonin alkulukutestiä, että $m = 701$ on alkuluku. Jaamme luvun $m - 1 = 700 = FR$ vain osittain alkulukutekijöihin. Olkoot $F = 35 = 7 \cdot 5$ ja $R = 20$. Siis $F > R$. Valitsemalla $a = 2$ saamme

$$\begin{aligned} 2^{700} \equiv (2^{100})^7 \equiv ((2^{25})^4)^7 \equiv (336^4)^7 \equiv 19^7 \equiv 1 \pmod{700}, \\ 2^{700/7} \equiv 2^{100} \equiv (2^{25})^4 \equiv 336^4 \equiv 19 \pmod{700}, \\ 2^{700/5} \equiv 2^{140} \equiv 2^{100} \cdot 2^{40} \equiv 19 \cdot 380 \equiv 210 \pmod{700}. \end{aligned}$$

Nyt, käyttämällä Eukleideen algoritmia, saamme

$$(2^{700/7} - 1, 701) = (18, 701) = 1$$

ja

$$(2^{700/5} - 1, 701) = (209, 701) = 1.$$

Pocklingtonin alkulukutestin nojalla $m = 701$ on alkuluku. Huomaamme, että Pocklingtonin alkulukutestiä käytettäessä meidän ei tarvitse jakaa testattavaa lukua kokonaan alkulukutekijöihinsä. Tämä nopeuttaa luvun todistamista alkuluvuksi.

2.3 Prothin alkulukutesti

Pocklingtonin alkulukutestin avulla voimme kehittää toisen alkulukutestin, jolla voimme testata, ovatko tiettyä muotoa olevat luvut alkulukuja. Tämän testin todisti Francois Proth vuonna 1878. Se on siis todistettu jo Pocklingtonin alkulukutestiä aikaisemmin. Tässä käytämme kuitenkin Pocklingtonin alkulukutestiä seuraavan todistuksen pohjana.

Lause 2.5 (Prothin alkulukutesti)**.** *Olkoon m sellainen positiivinen kokonaisluku, että $m = k2^n + 1$, missä k on pariton kokonaisluku ja n on kokonaisluku. Lisäksi $k < 2^n$. Jos on olemassa sellainen kokonaisluku a, että*

$$a^{(m-1)/2} \equiv -1 \pmod{m},$$

niin m on alkuluku.

Todistus. (Vrt. [1, s. 369] ja[2, s. 190]) Käytämme hyväksi Pocklingtonin alkulukutestiä. Luvun $m-1$ alkulukutekijöihin jaettu osa F on 2^n ja jakamaton osa R on k. Oletetaan, että

$$a^{(m-1)/2} \equiv -1 \pmod{m}. \tag{1}$$

Nyt, jos $d \mid (a^{(m-1)/2} - 1)$ ja $d \mid m$, niin kongruenssin (1) perusteella $d \mid (a^{(m-1)/2} + 1)$. Näin ollen d jakaa luvun $(a^{(m-1)/2} - 1) + (a^{(m-1)/2} + 1) = 2$. Koska m on pariton, niin $d = 1$. Täten$(a^{(m-1)/2} - 1, m) = 1$. Koska lauseen oletuksen mukaan $2^n > k$, niin kaikki Pocklingtonin alkulukutestin ehdot täyttyvät. Näin ollen m on alkuluku. □

Esimerkki 5. Osoitamme, käyttämällä Prothin alkulukutestiä, että $m = 7 \cdot 2^4 + 1 = 113$ on alkuluku. Huomaamme, että $7 < 2^4 = 16$. Valitaan $a = 3$. Mathematicaa hyväksikäyttäen saamme

$$3^{(m-1)/2} = 3^{112/2} = 3^{56} \equiv 112 \equiv -1 \pmod{113}.$$

Prothin alkulukutestin nojalla 113 on alkuluku.

Prothin alkulukutestiä on käytetty laajasti suurten muotoa $k2^n + 1$ olevien lukujen alkuluvuksi todistamisessa. Tällä hetkellä[4] kymmenestä suurimmasta alkuluvusta neljä on löydetty Prothin alkulukutestillä. Kuusi suurinta ovat kuitenkin Mersennen alkulukuja.

3 Pseudosatunnaislukugeneraattorit

Satunnaisesti valitut luvut ovat hyödyllisiä monissa sovelluksissa. Niitä tarvitaan esimerkiksi tietokonesimulaatioihin eri tieteen aloilla kuten atomifysiikassa, operaatiotutkimuksessa ja tietoverkoissa. Niitä voidaan käyttää satunnaisnäytteiden luomiseen, jolloin voidaan tarkkailla systeemin käyttäytymistä eri tapauksissa kattavasti, vaikka kaikkia mahdollisia tapauksia ei olisikaan mahdollista testata. Satunnaislukuja käytetään testaamaan tietokonealgoritmien suorituskyky ja ajamaan satunnaisia algoritmeja, jotka tekevät satunnaisia ajonaikaisia valintoja. Satunnaisluvuilla on myös paljon sovelluksia matematiikassa, erityisesti numeerisessa analyysissä. Satunnaislukuja voidaan käyttää esimerkiksi Riemannin summaa käyttävien integraalien arvioimisessa. Myös lukuteoriassa ja kryptauksessa satunnaisluvuilla on monia sovelluksia, kuten salausavainten generointi.

Satunnaisluvuista puhuttaessa tarkoitamme lukujonon termejä, joista jokainen on valittu sattumalta, riippumatta toisista lukujonon termeistä. (Ei ole mielekästä väittää, että yksittäinen numero, vaikkapa 69, on satunnainen, mutta se voi toki olla yksi satunnaisen lukujonon termeistä.) Ennen 1940-lukua satunnaislukuja tarvitsevat tiedemiehet tuottivat niitä esimerkiksi heittämällä noppaa, pyörittämällä rulettia tai heittämällä kolikkoa. 1940-luvulla keksittiin koneita satunnaislukujen tuottamiseksi ja 1950-luvulla tietokoneita käytettiin satunnaislukujen tuottamiseen satunnaisäänigeneraatoreita hyväksikäyttäen. Ne eivät kuitenkaan toimineet luotettavasti, eikä tietokoneohjelman tuottamia tuloksia voitu toistaa fyysisin ilmiöin tuloksen tarkastamiseksi.

Satunnaislukujen generoimista mekaanisen menetelmä sijasta tietokoneohjelman avulla ehdotti ensimmäisenä John Von Neumann vuonna 1946. Hänen ehdottamansa keskineliömenetelmä oli seuraavanlainen: nelinumeroisten satunnaislukujen generoimiseksi valitaan aluksi mielivaltainen nelinumeroinen luku, esimerkiksi 6139. Otetaan tämän luvun neliö

37687321 ja tästä otetaan neljä keskimmäistä numeroa seuraavaksi luvuksi, siis 6873. Toistamalla tätä menettelyä saadaan lukujono satunnaislukuja. Näin tuotetut lukujonot eivät kuitenkaan todellisuudessa ole satunnaisesti valittuja. Kun ensimmäinen luku tiedetään, koko jono on määritelty. Tällä tavoin muodostettu lukujono vaikuttaa kuitenkin satunnaiselta ja saadut luvut voivat olla käyttökelpoisia tietokonesimulaatioissa. Jonoissa olevia kokonaislukuja, jotka on valittu tietyn menetelmän avulla, mutta vaikuttavat satunnaisilta, kutsutaan *pseudosatunnaisluvuiksi*.

Keskineliömenetelmällä on valitettavasti joitain ilmeisiä heikkouksia. Sen ikävin ominaisuus on, että tietyillä aloitusluvun valinnoilla menetelmä tuottaa saman pienen joukon lukuja uudelleen ja uudelleen. Valitessamme aloitusluvuksi 4100 ja käytäessämme keskineliömenetelmää saamme lukujonon $8100, 6100, 2100, 4100, 8100, 6100, 2100, 4100, \ldots$, joten lukujonossa on vain neljä eri lukua ennen toistumista.

3.1 Lineaarinen kongruenssimenetelmä

Lineaarinen kongruenssimenetelmä on suosituin menetelmä pseudosatunnaislukujen generoimiseksi. Sen kehitti D.H. Lehmer vuonna 1949. Menetelmällä on lukuisia sovelluksia, mutta sen ennakoitavuus rajoittaa sen käyttöä salausmenetelmissä.

Menetelmä toimii seuraavalla tavalla: Valitaan sellaiset kokonaisluvut m, a, c ja x_0, että $2 \leq a < m$, $0 \leq c < m$ ja $0 \leq x_0 < m$. Pseudosatunnaislukujono määritellään rekursiivisesti kongruenssilla

$$x_{n+1} \equiv ax_n + c \pmod{m} \quad , 0 \leq x_{n+1} < m,$$

missä $n = 0, 1, 2, 3, \ldots$. Muuttujat ovat nimeltään moduli (m), alkuarvo (x_0), kertoja (a) ja lisäys (c). Seuraavissa esimerkeissä havainnollistamme lineaarisen kongruenssimenetelmän käyttöä.

Esimerkki 6. Valitsemme muuttujiksi $m = 12$, $a = 3$, $c = 5$ ja $x_0 = 4$. Rekursiokongruenssista saamme $x_1 = 3 \cdot 4 + 5 = 17 \equiv 5 \pmod{12}$ eli $x_1 = 5$. Samalla tavoin $x_2 = 8$, koska $x_2 = 3 \cdot 5 + 5 = 20 \equiv 8 \pmod{12}$ ja $x_3 = 5$, koska $x_3 = 3 \cdot 8 + 5 = 29 \equiv 5 \pmod{12}$ ja niin edelleen. Täten kaava tuottaa näillä muuttujan valinnoilla vain kolme eri kokonaislukua ennen toistumista. Saatu pseudosatunnaislukujono on $4, 5, 8, 5, 8, 5, 8, \ldots$.

Esimerkki 7. Valitsemme muuttujiksi $m = 9$, $a = 7$, $c = 4$ ja $x_0 = 3$. Rekursiokongruenssista saamme $x_1 = 7 \cdot 3 + 4 = 25 \equiv 7 \pmod{9}$ eli $x_1 = 7$. Samalla tavoin $x_2 = 8$, koska $x_2 = 7 \cdot 7 + 4 = 53 \equiv 8 \pmod{9}$ ja $x_3 = 6$, koska $x_3 = 7 \cdot 8 + 4 = 60 \equiv 6 \pmod{9}$ ja niin edelleen. Saamme lukujonon $3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots$. Lukujonossa on siis yhdeksän lukua ennen toistumista.

Huomautus. Tietokonesimulaatioiden tarpeisiin on joskus hyödyllistä generoida pseudosatunnaislukuja väliltä $[0, 1]$. Tällöin jaamme jokaisen generoidun lukujonon termin x_i modulilla m. Näin saamme uuden lukujonon $x_i/m,\ i = 1, 2, 3, \ldots$. Pseudosatunnaisbittijonon saamme käyttämällä ensin menetelmää ja sitten laskien kaavasta $z_n \equiv x_n \pmod 2$.

Seuraava lauseen avulla voimme löytää lineaarisen kongruenssimenetelmän generoimat pseudosatunnaislukujonon termit suoraan kertojan, lisäyksen ja alkuarvon avulla.

Lause 3.1. *Lineaarisen kongruenssimenetelmän generoimat lukujonon termit saadaan kongruenssista*

$$x_k \equiv a^k x_0 + c(a^k - 1)/(a - 1) \pmod m, \quad 0 \leq x_k < m.$$

Todistus. Todistamme lauseen matemaattisella induktiolla. Kun $k = 1$, väite on selvästi tosi, koska $x_1 \equiv ax_0 + c \pmod m$, $0 \leq x_1 \leq m$. Oletamme, että väite pätee, kun $k = n$ eli

$$x_n \equiv a^n x_0 + c(a^n - 1)/(a - 1) \pmod m, \quad 0 \leq x_n < m.$$

Todistetaan, että väite pätee, kun $k = n + 1$.Koska

$$x_{n+1} \equiv ax_n + c \pmod m, \quad 0 \leq x_n < m,$$

saadaan

$$\begin{aligned} x_{n+1} &\equiv a(a^n x_0 + c(a^n - 1)/(a - 1)) + c \\ &\equiv a^{n+1} x_0 + c(a(a^n - 1)/(a - 1) + 1) \\ &\equiv a^{n+1} x_0 + c(a^{n+1} - 1)/(a - 1) \pmod m, \end{aligned}$$

mikä on oikea asteen $n + 1$ termi. Lause on induktioperiaatteen nojalla todistettu. □

Lineaarisen pseudosatunnaislukugeneraattorin *jakson pituus* on jonon maksimipituus ilman lukujen toistumista. Kun mikä tahansa luku toistuu lukujonossa, täytyy myös lukujonon alkaa toistamaan tiettyä jaksoa. Oletamme, että $x_i = x_j,\ j > i$. Tällöin $x_{i+1} = x_{j+1}, \ldots, x_{i+k} = x_{j+k}$, kun $k > 0$. Koska jokaisella termillä x_i on vain m mahdollista arvoa, täytyy jonon toistua viimeistään m:n termin jälkeen. Lukujonon jakso on pienin sellainen positiivinen kokonaisluku T, että $x_{i+T} = x_i$, kaikille $i > i_0$, jollakin $i_0 > 0$.

3.2 Puhtaasti multiplikatiivinen kongruenssimenetelmä

Lineaarisen kongruenssimenetelmän tapaus, jossa lisäys $c = 0$ on yksinkertaisuutensa takia erityisen mielenkiintoinen. Tällöin menetelmää kutsutaan *puhtaasti multiplikatiiviseksi kongruenssimenetelmäksi*. Lisäyksen ollessa

nolla määrittelemme, kuten aiemminkin, modulin, kertoimen ja alkuarvon. Pseudosatunnaislukujono määritellään rekursiivisesti kongruenssilla

$$x_{n-1} \equiv ax_n \pmod{m}, \quad 0 < x_{n-1} < m.$$

Voimme myös ilmaista pseudosatunnaisluvut kertoimen ja alkuarvon avulla:

$$x_n \equiv a^n x_0 \pmod{m}, \quad 0 < x_{n-1} < m.$$

Olkoon l puhtaasti multiplikatiivista generaattoria käyttämällä saadun pseudosatunnaislukujonon jakson pituus. Tällöin l on pienin sellainen positiivinen kokonaisluku, että

$$x_0 \equiv a^l x_0 \pmod{m}.$$

Jos $(x_0, m) = 1$, niin $a^l \equiv 1 \pmod{m}$. Kongruenssin perusteella suurin mahdollinen jakson pituus on $\lambda(m)$, missä $\lambda(m)$ on pienin universaali eksponentti modulo m.

Puhtaasti multiplikatiivista generaattoria käyttävissä sovelluksissa käytetään yleensä Mersennen alkulukua $M_{31} = 2^{31} - 1$. Kun valitsemme moduliksi m alkuluvun, saamme suurimmaksi mahdolliseksi jonon pituudeksi $m - 1$ ja sen saavutamme, kun a on luvun m primitiivinen juuri. Luvun M_{31} sovelluksissa hyödyllisen primitiivisen juuren löytämiseksi todistetaan ensin, että 7 on yksi luvun M_{31} primitiivisistä juurista.

Lause 3.2. *Kokonaisluku 7 on luvun $M_{31} = 2^{31} - 1$ primitiivinen juuri.*

Todistus. (Vrt. [1, s. 383]) Lucasin lauseen (lause 2.1) perusteella voimme päätellä, että väitteen todistamiseksi riittää osoittaa, että

$$7^{(M_{31}-1)/q} \not\equiv 1 \pmod{M_{31}},$$

kaikilla luvun $M_{31} - 1$ alkulukutekijöillä q. Luvun M_{31} alkulukutekijöiden löytämiseksi huomaamme, että

$$\begin{aligned} M_{31} - 1 = 2^{31} - 2 &= 2(2^{30} - 1) = 2(2^{15} - 1)(2^{15} + 1) \\ &= 2(2^5 - 1)(2^{10} + 2^5 + 1)(2^5 + 1)(2^{10} - 2^5 + 1) \\ &= 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331. \end{aligned}$$

Luvun $M_{31} - 1$ alkulukutekijät ovat siis $2, 3, 7, 11, 31, 151$ ja 331. Nyt

$$\begin{aligned} 7^{(M_{31}-1)/2} &\equiv 2\,147\,483\,646 \not\equiv 1 \pmod{M_{31}}, \\ 7^{(M_{31}-1)/3} &\equiv 1\,513\,477\,735 \not\equiv 1 \pmod{M_{31}}, \\ 7^{(M_{31}-1)/7} &\equiv \quad 120\,536\,285 \not\equiv 1 \pmod{M_{31}}, \\ 7^{(M_{31}-1)/11} &\equiv 1\,969\,212\,174 \not\equiv 1 \pmod{M_{31}}, \\ 7^{(M_{31}-1)/31} &\equiv \qquad\qquad 512 \not\equiv 1 \pmod{M_{31}}, \\ 7^{(M_{31}-1)/151} &\equiv \quad 535\,044\,134 \not\equiv 1 \pmod{M_{31}} \\ \text{ja} \quad 7^{(M_{31}-1)/331} &\equiv 1\,761\,885\,083 \not\equiv 1 \pmod{M_{31}}. \end{aligned}$$

Täten kokonaisluku 7 on luvun M_{31} primitiivinen juuri. □

Käytännössä emme kuitenkaan halua käyttää primitiivistä juurta 7 pseudosatunnailukujen generoimiseen, koska tällöin ensimmäiset generoidut luvut ovat pieniä. Seurauslauseen 1.3.1 perusteella löydämme kuitenkin suurempia luvun M_{31} primitiivisiä juuria luvun 7 avulla. Siis käytämme primitiivistä juurta 7^k, missä $(k,\ M_{31}-1) = 1$. Esimerkiksi, kun $k = 5$, niin $(5,\ M_{31}-1) = 1$ ja siten $7^5 = 16\,807$ on primitiivinen juuri modulo M_{31}. Toinen mahdollisuus olisi samasta syystä $7^{13} = 252\,246\,292$

3.3 Neliöpseudosatunnaislukugeneraattori

Annetaan aluksi positiivinen kokonaisluku m (moduli) ja ensimmäinen termi x_0 (alkuarvo). *Neliöpseudosatunnaislukugeneraattori* tuottaa pseudosatunnaislukujonon käyttäen kongruenssia

$$x_{i+1} \equiv x_i^2 \pmod{m}, \quad \text{missä } 0 \leq x_{i+1} < m.$$

Jonon yksittäinen termi saadaan siis kongruenssista

$$x_i \equiv x_0^{2^i} \pmod{m}, \quad \text{missä } 0 \leq x_i < m.$$

Esimerkki 8. Olkoon $m = 257$ moduli ja $x_0 = 6$ alkuarvo. Neliöpseudosatunnaislukugeneraattori tuottaa nyt lukujonon

$$6, 36, 11, 121, 249, 64, 241, 256, 1, 1, \ldots .$$

Yhdeksännen termin jälkeen generaattori antaa siis pelkkiä ykkösiä. Esimerkki osoittaa, että lähtölukujen valintaan on kiinnitettävä erityistä tarkkaavaisuutta.

Esimerkki 9. (Vrt. [1, s. 384] Olkoon $m = 209$ moduli ja $x_0 = 6$ alkuarvo. Neliöpseudosatunnaislukugeneraattori tuottaa nyt lukujonon

$$6, 36, 42, 92, 104, 157, 196, 169, 137, 168, 9, 81, 82, 36, 42, \ldots .$$

Tämän lukujonon jakson pituus on 12. Ensimmäinen termi ei ole osa jaksoa.

Seuraavassa lauseessa määrittelemme neliöpseudosatunnaislukugeneraattorin jakson pituuden kokonaisluvun kertaluvun avulla.

Lause 3.3. *Olkoon $(x_0, m) = 1$. Neliöpseudosatunnaislukugeneraattorin jakson pituus alkuarvolla x_0 ja modulilla m on $ord_s 2$, missä s on sellainen pariton positiivinen kokonaisluku, että $ord_m x_o = 2^t s$, missä $t \geq 0$.*

Todistus. (Vrt. [1, s. 384]) Osoitetaan ensin, että $ord_s 2$ jakaa neliöpseudosatunnaislukugeneraatorin jakson pituuden l. Oletetaan, että $x_j = x_{j+l}$ jollakin kokonaisluvulla j. Tällöin

$$x_0^{2^j} \equiv x_0^{2^{j+l}} \pmod{m},$$

mistä seuraa, että

$$x_0^{2^{j+l}-2^j} \equiv 1 \pmod{m}.$$

Kokonaisluvun kertaluvun määritelmän (määritelmä 1.2) perusteella nyt

$$ord_m x_0 \mid (2^{j+l} - 2^j)$$

ja koska $ord_m x_o = 2^t s$, niin

$$2^{j+l} \equiv 2^j \pmod{2^t s}. \tag{2}$$

Koska $2^t \mid (2^{j+l} - 2^j)$ ja $2^{j+l} - 2^j = 2^j(2^l + 1)$, niin $j \geq t$. Nyt kongruenssi (2) voidaan kirjoittaa muotoon

$$2^{j+l-t} \equiv 2^{j-t} \pmod{s}.$$

Lauseen 1.3 nojalla saadaan $j + l - t \equiv j - t \pmod{ord_s 2}$. Täten $l \equiv 0 \pmod{ord_s 2}$ eli $ord_s 2$ jakaa jakson pituuden l.
Osoitetaan sitten, että jakson pituus l jakaa $ord_s 2$ eli $ord_s 2$ on luvun l monikerta. Riittää osoittaa, että on olemassa kaksi sellaista termiä x_j ja $x_k = x_j$, että $j \equiv k \pmod{ord_s 2}$. Oletetaan, että $j \equiv k \pmod{ord_s 2}$ ja $k \geq j \geq t$. Lauseen 1.3 perusteella saadaan

$$2^j \equiv 2^k \pmod{s}.$$

Lisäksi

$$2^k \equiv 2^j \pmod{2^t},$$

koska $2^k - 2^j = 2^j(2^{k-j} - 1)$ ja $j \geq t$. Seurauslauseen 1.3.2 ja tiedon $(2^t, s) = 1$ perusteella voimme päätellä, että

$$2^j \equiv 2^k \pmod{2^t s}.$$

Koska $ord_m x_0 = 2^t s$, niin

$$ord_m x_o \mid (2^k - 2^j).$$

Tämä tarkoittaa, että

$$x_0^{2^k-2^j} \equiv 1 \pmod{m}.$$

Siis

$$x_0^{2^k} \equiv x_0^{2^j} \pmod{m}.$$

Tästä seuraa, että $x_k = x_j$. Tästä voimme päätellä, että luvun $ord_s 2$ täytyy olla luvun l monikerta. Väite on täten todistettu. □

Huomautus. Lauseen todistuksessa on lähdeteoksessa virheitä. Ensiksi sivun 384 viimeisessä kappaleessa moduliksi on vahingossa lipsahtanut $ord_2 s$, kun sen pitäisi olla $ord_s 2$. Toiseksi sivulla 385 puuttuu 0 luvun x alaindeksistä. Lisäksi lähdeteoksessa lauseen oletuksista puuttuu, että $(x_0, m) = 1$.

Esimerkki 10. Esimerkissä 9 käytimme neliöpseudosatunnaislukugeneraattoria modulilla $m = 209$ ja alkuarvolla $x_0 = 6$. Mathematican avulla näemme, että $ord_{209}6 = 90$. Koska $90 = 2 \cdot 45$, lauseen 3.3 perusteella generaattorin jakson pituus on $ord_{45}2 = 12$. Tämä vastaa termejä listaamalla saatua jakson pituutta.

4 ElGamalin salausjärjestelmä

Tässä kappaleessa esittelemme ElGamalin salausjärjestelmän, joka on yksi julkisen avaimen salausjärjestelmistä. Sen on esittänyt Taher ElGamal vuonna 1985. ElGamalin salausjärjestelmä, kuten monet muutkin salausjärjestelmät, perustuu diskreetin logaritmin ratkaisemisen vaikeuteen, kun modulina on suuri alkuluku. Diskreetin logaritmin määritelmän (määritelmä 1.4) mukaan, jos $r^x \equiv a \pmod{p}$, niin x on luvun a r-kantainen diskreetti logaritmi modulo p.

4.1 Viestien salaus ja salauksen purku

ElGamalin salausjärjestelmässä jokainen henkilö valitsee alkuluvun p ja alkuluvun p primitiivisen juuren r. Lisäksi jokainen heistä valitsee salaiseksi avaimekseen sellaisen satunnaisen kokonaisluvun a, että $0 < a < p - 1$ ja laskee tämän jälkeen $b \equiv r^a \pmod{p}$. Julkinen avain on $K = (p, r, b)$. Seuraavassa esimerkissä havainnollistamme, miten ElGamalin salausjärjestelmän avaimet valitaan.

Esimerkki 11. Julkisen ja salaisen avaimen luomiseksi ElGamalin salausjärjestelmällä valitsemme aluksi alkuluvun p. Valitsemme vaikkapa $p = 2539$. (Tämän alkuluvun valitsimme vain osoittaaksemme, kuinka salausjärjestelmä toimii. Todellisuudessa nelinumeroinen alkuluku ei riittäisi, vaan alkuluvun tulisi olla useita satoja numeroita pitkä.) Seuraavaksi valitsemme luvun $p = 2539$ primitiivisen juuren r. Pienin luvun 2539 primitiivinen juuri on 2. Sitten valitsemme salaiseksi avaimeksi satunnaisesti sellaisen kokonaisluvun a, että $0 \leq a \leq 2538$. Valitsemme $a = 15$. Nyt laskemme luvun $b \equiv 2^{15} \equiv 2300 \pmod{2539}$. Julkinen avain on täten $K = (2539, 2, 2300)$.

Viestin m, missä $0 < m < p$, salaus ElGamalin salausjärjestelmällä tehdään seuraavalla algoritmilla:

1. Valitse satunnaisesti sellainen kokonaisluku k, että $1 < k < p - 1$.
2. Laske $\gamma \equiv r^k \pmod{p}$ ja $\delta \equiv m \cdot b^k \pmod{p}$.
3. Salakirjoitusteksti on järjestetty pari $E(m) = (\gamma, \delta)$.

Varsinainen viesti m on kätketty kertomalla se luvulla b^k, mistä saadaan näin luku δ. Tämä kätketty viesti lähetetään yhdessä luvun γ kanssa. Ainoastaan henkilö, jolla on salainen avain a voi laskea luvut b^k ja γ ja siten saada selville alkuperäisen viestin. On huomioitava, että salakirjoitettu viesti on tuplasti niin pitkä kuin alkuperäinen teksti. Jos alkuperäinen viesti on pitempi kuin p, niin se täytyy jakaa pienempiin lohkoihin, jotka ovat alkulukua p pienempiä. Tämän jälkeen jokainen lohko salataan erikseen. Satunnaisen kokonaisluvun k käyttäminen salauksen yhteydessä on välttämätöntä turvallisuuden saavuttamiseksi.

ElGamalin salausjärjestelmällä salatun viestin purkaminen ei onnistu ilman salaista avainta a. Ensimmäinen askel salakirjoituksen järjestetyn parin (γ, δ) purkamisessa on laskea luku $\overline{\gamma^a}$, joka on luvun γ^a käänteisluku modulo p. Tämä tehdään laskemalla γ^{p-1-a} modulo p. Sitten pari $C = (\gamma, \delta)$ puretaan laskemalla

$$D(C) = \overline{\gamma^a}\delta.$$

Voidaan tarkistaa purkamisen onnistuminen laskemalla

$$\begin{aligned} D(C) &\equiv \overline{\gamma^a}\delta \pmod{p} \quad , \gamma \equiv r^k \\ &\equiv \overline{r^{ka}} \cdot mb^k \pmod{p} \\ &\equiv \overline{r^a}^k mb^k \pmod{p} \quad , r^a \equiv b \\ &\equiv \overline{b^k} b^k m \pmod{p} \\ &\equiv m \pmod{p}. \end{aligned}$$

Seuraavasssa esimerkissä havainnolistamme salausta ja sen purkua ElGamalin salausjärjestelmällä.

Esimerkki 12. Salaamme viestin

LUKUTEORIA ON KIVAA

käyttämällä ElGamalin salausjärjestelmää. Käytämme esimerkissä 11 luomaamme julkista avainta. Siinä julkinen avain oli $K = (2539, 2, 2300)$ ja salainen avain oli $a = 15$. Ennen kuin voimme salata viestin ElGamalin salausjärjestelmää käyttäen meidän täytyy muuttaa kirjaimet vastaamaan numeerisia vastineitaan. Aloitamme numeroinnin kirjaimesta A ja numeroinnin luvusta 0. Ääkkösiä emme ota tässä huomioon, vaan viimeinen kirjain on Z ja sitä vastaa luku 25. Järjestämme luvut neljänumeroisiksi lohkoiksi(luvut alle kymmenen kirjoitetaan siten, että ne ovat kaksinumeroisia, esim. 8 = 08). Nyt suurin mahdollinen lohkon arvo on 2525, joka on pienempi kuin käyttämämme alkuluku $p = 2539$. Saamme alkuperäinen tekstin muotoon

1120 1020 1904 1417
0800 1413 1008 2100
0023,

missä viimeinen lohko on täytetty lisäämällä loppuun kirjain X eli luku 23. Valitaan sitten sellainen satunnainen kokonaisluku k, että $1 < k \leq 2537$(käytämme jokaiseen lohkoon samaa lukua k, vaikka käytännön sovelluksissa käyttäisimme joka lohkossa turvallisuuden parantamiseksi eri lukua k). Valitsemme $k = 10$ ja salaamme jokaisen lohkon käyttämällä suhdetta $E(C) = (\gamma, \delta)$, missä

$$\gamma \equiv 2^{10} \equiv 1024 \pmod{2539}$$

ja

$$\delta \equiv m \cdot 2300^{10} \pmod{2539}, \quad 0 \leq \delta \leq 2538.$$

Otetaan esimerkkinä ensimmäisen lohkon salaus:

$$\gamma \equiv 2^{10} \equiv 1024 \pmod{2539}$$

ja

$$\delta \equiv 1120 \cdot 2300^{10} \equiv 1886 \pmod{2539}.$$

Siis ensimmäinen lohko salattuna on järjestetty pari $(1024, 2159)$. Kun jokainen lohko on salattu, saadaan seuraava salattu viesti:

$$\begin{aligned}&(1024, 1886)\ (1024, 2171)\ (1024, 1175)\ (1024, 2436)\\ &(1024, 0259)\ (1024, 0924)\ (1024, 0174)\ (1024, 1632)\\ &(1024, 1077)\ .\end{aligned}$$

Voimme purkaa salatun viestin laskemalla

$$D(C) = \overline{\gamma^a}\delta \equiv \overline{\gamma^{15}}\delta \pmod{2539}.$$

Esimerkiksi toisen lohkon purkamiseksi lasketaan

$$\begin{aligned}D((1024, 0198)) &\equiv \overline{1024^{15}} \cdot 2171\\ &\equiv \overline{378} \cdot 2171\\ &\equiv 356 \cdot 2171\\ &\equiv 1020 \pmod{2539}.\end{aligned}$$

Huomaamme, että se vastaa alkuperäistä toisen lohkon lukua.

4.2 Viestien sähköinen allekirjoittaminen

Seuraavassa esittelemme, kuinka ElGamalin salausjärjestelmää voidaan käyttää viestien sähköisessä allekirjoituksessa. Olkoon p alkuluku ja r primitiivinen juuri modulo p. Nyt henkilön julkinen avain on (p, r, b) ja hänen salainen avaimensa on sellainen kokonaisluku a, että $b \equiv r^a \pmod{p}$. Henkilö, jonka salainen avain on a, allekirjoittaa viestin m seuraavasti: Aluksi

hän valitsee sellaisen kokonaisluvun k, että $(k, p-1) = 1$. Sitten hän laskee muuttujat

$$\gamma \equiv r^k \pmod{p}, \quad 0 \leq \gamma \leq p-1$$

ja

$$s \equiv (m - a\gamma)\overline{k} \pmod{p-1}, \quad 0 \leq s \leq p-2.$$

Viestin m sähköinen allekirjoitus on pari (γ, s). On huomioitava, että allekirjoitus riippuu aina satunnaisesta kokonaisluvusta k. Jokainen, jolla on tiedossa julkinen avain ja viesti m, voi tarkistaa allekirjoituksen oikeellisuuden laskemalla

$$V_1 \equiv \gamma^s b^\gamma \pmod{p}, \quad 0 \leq V_1 \leq p-1$$

ja

$$V_2 \equiv r^m \pmod{p}, \quad 0 \leq V_2 \leq p-1.$$

Allekirjoitus on aito, jos saadaan $V_1 = V_2$. Jos allekirjoitus on aito,

$$\begin{aligned}
V_1 &\equiv \gamma^s b^\gamma \pmod{p} \\
&\equiv \gamma^{(m-a\gamma)\overline{k}} b^\gamma \pmod{p} \\
&\equiv (\gamma^{\overline{k}})^{m-a\gamma} b^\gamma \pmod{p} \\
&\equiv r^{m-a\gamma} b^\gamma \pmod{p} \\
&\equiv r^m r^{-a\gamma} b^\gamma \pmod{p} \\
&\equiv r^m \overline{r^{a\gamma}} b^\gamma \pmod{p} \\
&\equiv r^m \overline{b^\gamma} b^\gamma \pmod{p} \\
&\equiv r^m \pmod{p} \\
&\equiv V_2.
\end{aligned}$$

Esimerkki 13. Oletetaan, että Hannulla on julkinen ElGamal avain $(p, r, b) = (2539, 2, 2300)$ ja vastaavasti salainen ElGamal avain $a = 15$. Hannu allekirjoittaa viestin $m = 112$ valitsemalla aluksi sellaisen satunnaisen kokonaisluvun $k = 457$, että $1 \leq k \leq 2538$ ja $(k, 2538) = 1$. Viestin $m = 112$ sähköinen allekirjoitus saadaan laskemalla

$$\gamma \equiv r^k \equiv 2^{457} \equiv 1079 \pmod{2539}$$

ja

$$\begin{aligned}
s &\equiv (112 - 15 \cdot 1079) \cdot \overline{457} \pmod{2538} \\
&\equiv (-16073) \cdot 2227 \pmod{2538} \\
&\equiv 1693 \cdot 2227 \pmod{2538} \\
&\equiv 1381 \pmod{2538}.
\end{aligned}$$

Jokainen, jolla on tiedossa allekirjoitus $(1079, 1381)$ ja viesti $m = 112$, voi tarkistaa allekirjoituksen oikeellisuuden laskemalla

$$2300^{1079}1079^{1381} \equiv 2316 \pmod{2359}$$

ja

$$2^{1}12 \equiv 2316 \pmod{2359}.$$

Viitteet

[1] Rosen, K.H. *Elementary Number Theory and Its Applications*, AT&T Laboratories and Kenneth H. Rosen, 2005.

[2] Kumanduri, R. & Romero, C. *Number Theory with Computer Applications*, Prentice-Hall, 1998.

[3] Merikoski, J. & Virtanen, A. & Koivisto, P. *Johdatus diskreettiin matematiikkaan*, WSOY, 2003.

[4] Caldwell, C.K. *The Largest Known Primes - A Summary [Verkkodokumentti],* 2008 [21.4.2008] http://primes.utm.edu/largest.html