Helsingin Yliopisto
Matemaattis-luonnontieteellinen tiedekunta
Matematiikan ja tilastotieteen osasto

Pro gradu -tutkielma

Lukiokurssi primitiivisistä juurista

Panu Turtio

Ohjaaja: Anne-Maria Ernvall-Hytönen 1.6.2021

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author
Panu Turtio

Työn nimi — Arbetets titel — Title

Lukiokurssi primitiivisistä juurista

Oppiaine — Läroämne — Subject		
Matematiikka		
Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Kesäkuu 2021	54 s.

Tiivistelmä — Referat — Abstract

Työn tavoitteena on tutkia, miten voidaan tuottaa lukiokurssi primitiivistä juurista. Primitiivistä juurista ei ole ennalta materiaalia lukiotasolle, joten työssä joudutaan kehittämään metodi yliopistotason materiaalin muuntamiselle lukiotasolle.

Työssä esitetään ja todistetaan lukuteorian lauseita. Nämä lauseet on valikoitu sellaisiksi, että ne ovat vähin mitä tarvitaan primitiivisten juurten käsittelyyn. Tämän lisäksi työssä esitellään Diffie-Hellman-avaintenvaihtoprotokolla ja murtamiseen käytettävä Square and multiply - algoritmi. Työssä tuotetaan lukuteorian lukiokurssi primitiivisistä juurista pohjautuen työssä läpikäytyyn materiaaliin. Lukiokurssi tuotetaan vertailemalla analyysin yliopiston ja lukion oppimateriaalien eroavaisuuksia. Näistä eroavaisuuksista pyritään analysoimaan säännönmukaisuuksia, millä yliopistontason materiaali voidaan muuntaa lukio-opetukseen sopivaksi.

Yliopisto- ja lukiotasoisten oppimateriaalien eroavaisuuksiksi havaittiin sisällön rajaus, matemaattisten merkkien muuntaminen kirjalliseksi kieleksi, opetettavan sisällön järjestys ja painotus todistuksiin yliopistossa sekä painotus esimerkkeihin lukiossa. Nämä havainnot huomioon ottaen, työn matematiikkaosion lauseista muunnettiin lukioympäristöön sopiva kokonaisuus. Tämä kokonaisuus on riittävä pohja lukiokurssin pitämiseen näistä aiheista ja sisältää myös opetuksen aikataulutuksen.

Avainsanat — Nyckelord — Keywords
Primitiiviset juuret, Lukuteoria, Lukio, Kurssi, Diffie-Hellman avaintenvaihtoprotokolla

Säilytyspaikka — Förvaringsställe — Where deposited
E-thesis

Muita tietoja — Övriga uppgifter — Additional information

Sisältö

Luku 1

Johdanto

Tämä tutkielma käsittelee lukuteorian osa-aluetta nimeltä primitiiviset juuret ja pyrkii analysoimaan niiden esittämistä lukion matematiikan oppimäärän viitekehyksessä. Tutkielmassa esitellään primitiiviset juuret ja Diffie-Hellman-avaintenvaihtoprotokolla. Tämän jälkeen tutkielmassa analysoidaan, miten lukion oppimäärän osaavalle henkilölle voidaan opettaa nämä kyseiset asiat hypoteettisellä lukion valinnaisella kurssilla, missä keskeisinä sisältöinä ovat primitiiviset juuret ja Diffie-Hellman-avaintenvaihtoprotokolla.

Tutkielman lukeminen ei edellytä lukijalta taustaa lukuteoriasta ja lähtee liikkeelle luvussa kaksi esittelemällä kaikki primitiivisten juurien esittämiseen vaadittavat lukuteorian käsitteet. Lähdemateriaalina käytetään Eero Saksmanin syksyn 2019 Introduction to number theory -kurssin kurssimateriaalia. Primitiivisten juurien esittäminen luvussa kolme mukailee sitä, miten ne esitetään kyseisessä kurssimateriaalissa. Luvussa neljä esitellään Diffie-Hellman-avaintenvaihtoprotokolla. Se on hypoteettisen lukiokurssin primitiivisiin juuriin liittyvä käytännön sovellus. Näiden sisältöjen lukiossa opettamisen analysointi perustuu lukion opetussuunnitelmissa oleviin lukuteorian sisältöihin, mitkä ovat oletettuna lukio-opiskelijoiden lähtötasona. Lisäksi vertailen analyysin oppikirjojen eroavaisuuksia lukio- ja yliopistotasolla. Tutkielmassa esitetään luvussa kuusi alustava ehdotus kurssisuunnitelmasta tuotettavalle hypoteettiselle lukion kurssille.

Luku 2

Lukuteorian peruskäsitteistö

Tässä luvussa esitellään peruskäsitteistö, minkä avulla tutkielmassa johdetaan primitiivisiin juuriin liittyvät lauseet. Kun tutkielmassa myöhemmin käytetään lauseita peruskäsitteistöstä, niin niihin viitataan kyseisen lauseen luvulla matemaattisissa teksteissä tyypilliseen tapaan. Myöhemmin käytettäviin määritelmiin, jotka löytyvät tästä osioista, viitataan samalla tavalla.

Lukuteorialla on pitkä historia. Alun perin se pohjautui luonnollisten lukujen ominaisuuksien tutkimiseen. Lukuteorian tutkiminen painottui historiallisesti luonnollisten lukujen jaollisuuteen. Vaikka lukuteoria on tyypillisesti ollut luonnollisten lukujen tutkimista, niin siinä tutkitaan myös Gaussin kokonaislukuja, mitkä ovat kompleksilukuja.

Kaikki tässä tutkielmassa esitetyt luvut, joita merkitään jollain kirjaimella ovat kokonaislukuja jos niiden yhteydessä ei erikseen mainita, mitä ne ovat. Tämä luku käyttää lähdemateriaalina Eero Saksmanin syksyn 2019 kurssin Introduction to number theory kurssikalvoja. Lähdetään liikkeelle jaollisuuden käsitteestä.

2.0.1 Jaollisuus ja suurin yhteinen tekijä

Määritelmä 2.1. Olkoot luvut a ja b luonnollisia lukuja. Nyt a jakaa luvun b jos

$$b = a \cdot k, \ jossa \ k \in \mathbb{Z}.$$

Tällöin a on myös luvun b tekijä. Käytetään jatkossa merkintää $|$ tarkoittamaan jaollisuutta. Nyt siis merkintä $a \mid b$ tarkoittaa, että a jakaa luvun b.Vastaavasti, jos halutaan ilmaista, että jokin luku ei jaa jotain lukua, niin käytetään merkintää $\nmid$ samalla tavalla.

Otetaan mukaan muutama tärkeä ominaisuus jaollisuudesta.

Lause 2.2. *i) Jos* $c \mid b$ *ja* $b \mid a$ *niin,* $c \mid a$.

ii) Jos $a \mid b$ *niin* $a \mid b \cdot c$ *kun* $c \in \mathbb{Z}$.

iii) Jos $a \mid b_1,\ a \mid b_2,\ ...,\ a \mid b_n,$ *niin* $a \mid (b_1 + b_2 ... + b_n)$.

Todistus. Aloitetaan kohdasta *i*). **Määritelmän 2.1.** mukaan ehto $c \mid b$ tarkoittaa, että $b = c \cdot k_1$. Vastaavasti saadaan, että

$$a = b \cdot k_2 = c \cdot k_1 \cdot k_2.$$

Nyt, koska luvut $k_1, k_2 \in \mathbb{Z}$ niin **määritelmän 2.1.** mukaan $c \mid a$. Vastaavasti kohdassa *ii*) ehdosta $a \mid b$ saadaan $b = a \cdot k$. Nyt pätee siis, että $b \cdot c = a \cdot k \cdot c$. Nyt, koska $k, c \in \mathbb{Z}$ niin $a \mid b \cdot c$. Kohdasta *iii*) taas saadaan, että

$$b_1 = a \cdot k_1, b_2 = a \cdot k_2, ..., b_n = a \cdot k_n.$$

Nyt pätee että

$$b_1 + b_2 + ... + b_n = a \cdot k_1 + a \cdot k_2 + ... + a \cdot k_n = a \cdot (k_1 + k_2 + ... + k_n).$$

Nyt siitä että $k_1, k_2, ..., k_n \in \mathbb{Z}$ seuraa $a \mid (b_1 + b_2 + ... + b_n)$.

□

Esimerkki 2.3. $2 \mid 4$, $4 \mid 32$ ja $2 \mid 32$.

Lause 2.4. *Olkoon* $b \geq 1$ *kokonaisluku. Tällöin mille tahansa kokonaisluvulle* a *löytyy yksiselitteiset luvut* k *ja* r *siten, että*

$$a = k \cdot b + r,\ r \in \{0, 1, 2, ..., b - 1\}.$$

Todistus. Näytetään aluksi, että tällaiset luvut k ja r on olemassa ja sitten, että ne ovat yksiselitteisiä. Määritellään aluksi joukko $U = \{a - u \cdot b \mid a - u \cdot b \geq 0,\ u \in \mathbb{Z}\}$. Nyt koska U on selkeästi epätyhjä, niin oletetaan, että r on sen pienin alkio. Nyt siis voidaan kirjoittaa $r = a - u_1 \cdot b$. Nyt jos $r > b$, niin

$$r > r - b = a - u_1 \cdot b - b = a - (u_1 + 1) \cdot b \geq 0.$$

Nyt $r - b \in U$, mutta luvun r piti olla pienin alkio joukossa U, joten ehto $r > b$ ei voi päteä. Siispä epäyhtälö $0 < r < b$ pätee. Valitaan luku $k = u_1$. Täten on olemassa luvut k ja r siten, että lauseen yhtälö pätee. Näytetään nyt, että ne ovat yksiselitteisiä. Olkoot meillä luvut $0 \leq r_1$ ja $r_2 < b$. Nyt,

$$r_1 = a - u_1 \cdot b \; ja \; r_2 = a - u_2 \cdot b.$$

Tällöin pätee, että

$$r_1 - r_2 = a - u_1 \cdot b - a + u_2 \cdot b = b \cdot (u_1 + u_2).$$

Nyt **Määritelmän 2.1.** mukaan $b \mid (r_1 - r_2)$. Nyt ehdosta $0 \leq r_1, r_2 < b$ seuraa, että $|r_1 - r_2| < b$ eli jotta b voisi jakaa erotuksen $r_1 - r_2$ niin tulee päteä että $r_1 - r_2 = 0$ jolloin $b \cdot 0 = r_1 - r_2$. Tästä seuraa että $r_1 = r_2$, jolloin myös $u_1 = u_2$.

□

Lause 2.5. *Olkoot $a \neq 0$ ja $b \neq 0$. Nyt on olemassa yksiselitteinen kokonaisluku d jolla on seuraavat ominaisuudet.*

i) $d \mid a \; ja \; d \mid b$.

ii) $jos \; d' \mid a \; ja \; d' \mid b \Rightarrow d' \mid d$.

iii) $d \geq 1$.

Todistus. Olkoot

$$d = min\{a \cdot x + b \cdot y \; jossa \; a \cdot x + b \cdot y \geq 1, \; x, y \in \mathbb{Z}\}.$$

Selkeästi määrittelemässämme joukko on epätyhjä joten d on olemassa. Lisäksi joukkomme määritelmän mukaan $d \geq 1$ eli ehto *iii*) täyttyy. Olkoot

$$d = a \cdot x_0 + b \cdot y_0.$$

Nyt jos $d' \mid a$ ja $d' \mid b$, niin

$$d = d' \cdot k_1 \cdot x_0 + d' \cdot k_2 \cdot y_0 = d' \cdot (k_1 \cdot x_0 + k_2 \cdot y_0).$$

Tästä seuraa **määritelmän 2.1.** mukaan, että $d^{'} \mid d$ eli ehto $ii)$ täyttyy. Ehdon $i)$ näyttämiseksi tehdään vastaoletus. Oletetaan että $d \nmid b$. Nyt **lauseen 2.4.** mukaan on olemassa luvut k ja r siten, että

$$a = d \cdot k + r, \quad 0 < r < d.$$

Kun tästä yhtälöstä ratkaistaan r niin saadaan

$$r = a - d \cdot k = a - a \cdot x_0 \cdot k + b \cdot y_0 \cdot k = a \cdot (1 - x_0 \cdot k) + b \cdot (y_0 \cdot k).$$

Luku r on määritetty pienemmäksi kuin d, mutta d on määritelmällisesti pienin luku joka on muotoa $ax + by$. Tästä seuraa ristiriita, eli $d \mid b$. Päättely sille, että $d \mid a$, on symmetrinen joten sitä ei erikseen esitetä. Näytetään vielä, että tämä luku d on yksiselitteinen. Oletetaan, että meillä on luvut d_1 ja d_2, jotka täyttävät nämä ehdot. Nyt kohtien $i)$ ja $ii)$ mukaan pätee, että $d_1 \mid d_2$ ja $d_2 \mid d_1$. Lisäksi ehdon $iii)$ mukaan luvut d_1 ja d_2 ovat positiivisia ja tästä seuraa, että $d_1 = d_2$.

□

Tämä luku d on nimeltään suurin yhteinen tekijä. Käytetään jatkossa suurimmasta yhteisestä tekijästä merkintää $syt(a, b)$. Nyt siis $syt(a, b)$ tarkoittaa sitä lukua, mikä täyttää luvuille a ja b luvun d ehdot **lauseessa 2.5.** Yleistetään suurin yhteinen tekijä kun lukuja, joista se otetaan, on n kappaletta.

Esimerkki 2.6. $syt(5, 15) = 5$, $syt(63, 165) = 3$ ja $syt(7, 31) = 1$.

Korollaari 2.7. *Olkoot $a \neq 0$ ja $b \neq 0$. Olkoot lisäksi $d = syt(a, b)$. Tällöin seuraavat ehdot ovat voimassa.*

$i)$ $d = a \cdot x_0 + b \cdot y_0$ *joillakin* $x_0, y_0 \in \mathbb{Z}$.

$ii)$ $\{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\} = \{k \cdot d \mid k \in \mathbb{Z}\}$.

Todistus. **Lauseessa 2.5.** on jo osoitettu kohdan $i)$ olemassaolo, joten riittää näyttää kohta $ii)$. Osoitetaan siis, että kohdan $ii)$ joukot ovat toistensa osajoukkoja. Olkoon meillä siis alkio joukosta $\{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\}$. Nyt koska $d = syt(a, b)$ niin **lauseen 2.5.** mukaan $d \mid a$ ja $d \mid b$. Siispä

$$x \cdot a + y \cdot b = x \cdot d \cdot k_1 + y \cdot d \cdot k_2 = d \cdot (x \cdot k_1 + y \cdot k_2).$$

Siis selkeästi mielivaltainen alkio $x \cdot a + y \cdot b \in \{k \cdot d \mid k \in \mathbb{Z}\}$, jolloin

$$\{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\} \subset \{k \cdot d \mid k \in \mathbb{Z}\}.$$

Todistetaan seuraavaksi toinen suunta. Nyt mielivaltaiselle alkiolle mikä kuuluu joukkoon $\{k \cdot d \mid k \in \mathbb{Z}\}$ pätee kohdan i) mukaisesti, että

$$k \cdot d = k \cdot (x \cdot a + y \cdot b) = k \cdot x \cdot a + k \cdot y \cdot b \in \{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\}.$$

Siispä myöskin

$$\{k \cdot d \mid k \in \mathbb{Z}\} \subset \{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\}.$$

Koska molemmat joukot ovat toistensa osajoukkoja, niin saadaan että

$$\{x \cdot a + y \cdot b \mid x, y \in \mathbb{Z}\} = \{k \cdot d \mid k \in \mathbb{Z}\}.$$

□

Esimerkki 2.8. $syt(6, 22) = 2$ jolloin luku 2 voidaan esittää muodossa $2 = 6 \cdot 4 + 22 \cdot (-1)$.

Lause 2.9. *Jos* $a \mid b \cdot c$ *ja* $syt(a, b) = 1$, *niin* $a \mid c$.

Todistus. **Korollaarin 2.7.** mukaan $syt(a, b)$ voidaan esittää muodossa

$$syt(a, b) = x_0 \cdot a + y_0 \cdot b = 1.$$

Kertomalla molemmin puolin luvulla c saadaan, että $c \cdot x_0 \cdot a + c \cdot y_0 \cdot b = c$. Selkeästi $a \mid c \cdot a \cdot x_0$ ja ehdosta $a \mid b \cdot c$ seuraa, että $a \mid c \cdot b \cdot y_0$. Siispä **lauseen 2.2.** kohdan iii) mukaan $a \mid c$.

□

Esimerkki 2.10. $7 \mid 10 \cdot 14$ ja $syt(7, 10) = 1$ jolloin $7 \mid 14$.

2.0.2 Alkuluvut

Tuodaan tässä vaiheessa mukaan alkuluvut. Alkuluvut ovat herättäneet kiinnostusta matemaatikoiden keskuudessa jo muutaman vuosituhannen ajan. Niillä on myös olennainen rooli primitiivissä juurissa, minkä englanninkieliset nimitykset "prime number" ja "primitive root" tuovatkin paremmin esiin. Kun fysiikassa kuvaillaan maailmaa, niin on pyritty

selvittämään aineen pienin rakennusosa. Jo muinaisessa kreikassa oltiin vakuuttuneita siitä, että sellainen on ja siitä käytettiin nimitystä atomi. Nykyään tiedetään, että atomit koostuvat elektroneista, protoneista ja neutroneista jotka taas koostuvat erilaisista kvarkeista. Ehkäpä vielä löydetään jotkin hiukkaset, mistä kvarkit koostuvat. Kun käsitellään luonnollisia lukuja, niin voidaan sanoa, että alkuluvut ovat luonnollisille luvuille kuin kreikkalaiset olettivat atomien olevan aineelle. Alkuluvut ovat hyvin perusteellinen osa lukuteoriaa ja niihin liittyy erittäin paljon mielenkiintoista matematiikkaa, mutta tässä tutkielmassa käydään läpi vain välttämättömät asiat, mitä tarvitaan primitiivisten juurten esittämiseen.

Määritelmä 2.11. Olkoot $p \in \mathbb{N}$, $p \geq 2$ ja $k \in \mathbb{N}$. Nyt, jos $k \mid p \Rightarrow k \in \{1, p\}$, niin p on alkuluku. Käytetään alkulukujen joukosta jatkossa merkintää $\mathbb{P}$.

Määritelmä 2.12. Olkoot $n \in \mathbb{N}$ ja $n \geq 2$. Nyt jos $n \notin \mathbb{P}$ niin silloin n on yhdistetty luku.

Lause 2.13. *Jokainen luonnollinen luku jolle pätee $n \geq 2$ on alkulukujen tulo.*

Todistus. Tehdään vastaoletus. Oletetaan siis, että on olemassa ainakin yksi vähintään luvun 2 suuruinen luonnollinen luku mikä ei ole alkulukujen tulo. Olkoon luku n pienin sellainen luku. Nyt luku n on joko alkuluku tai yhdistetty luku. Alkuluvut ovat triviaalisti alkulukujen tuloja koska jokainen luku on oma tekijänsä. Siispä n on yhdistetty luku mikä voidaan esittää muodossa $n_1 \cdot n_2 = n$, missä $n_1, n_2 > 1$. Kokonaislukujen ominaisuuksista tiedetään, että $n \geq n_1, n_2$. Nyt, koska n on pienin luku mikä ei ole alkulukujen tulo, niin n_1 ja n_2 ovat alkulukujen tuloja. Siispä luku n, mikä on niiden tulo on myös alkulukujen tulo. Tämä on ristiriita, joten alkuperäinen väittämä on tosi.

□

Lause 2.14. *Alkulukuja on ääretön määrä.*

Todistus. Tehdään vastaoletus. Oletetaan, että $\mathbb{P}$ on äärellinen, eli $\mathbb{P} = \{p_1, p_2, ..., p_k\}$. Olkoot nyt $n = p_1 \cdot p_2 \cdot p_3 ... \cdot p_k + 1$. Nyt, kaikilla luvun $j \in \mathbb{N}$ arvoilla pätee, että $p_j \nmid n$. Täten lukua n ei voida esittää alkulukujen tulona. Tämä on ristiriidassa **Lauseen 2.13.** kanssa eli alkuperäinen väittämä pätee.

□

Määritelmä 2.15. Jos $syt(a, b) = 1$, niin silloin luvut a ja b ovat keskenään jaottomia eli niiden tekijöissä ei ole yhtään samaa alkulukua. Käytetään niistä tästä eteenpäin termiä "suhteelliset alkuluvut".

Esimerkki 2.16. Luvut 2, 3 ja 11 ovat alkulukuja. Luku $6 = 2 \cdot 3$ on yhdistetty luku. Luvut $35 = 5 \cdot 7$ ja $44 = 2^2 \cdot 11$ ovat suhteellisia alkulukuja.

Korollaari 2.17. *Jos $p \in \mathbb{P}$ ja $p \mid a \cdot b$, niin $p \mid a$ tai $p \mid b$.*

Todistus. Nyt p joko jakaa tai ei jaa lukua a. Siis joko $syt(p, a) > 1$ tai $syt(p, a) = 1$. **Määritelmän 2.11.** mukaan jos $syt(p, a) > 1$ niin $syt(p, a) = p$ jolloin $p \mid a$ eli väite on tosi. Jos taas $syt(p, a) = 1$ niin **lauseen 2.9.** mukaan ehdosta $p \mid a \cdot b$ seuraa, että $p \mid b$ jolloin myös väite on tosi. Vastaavalla logiikalla voidaan käydä läpi tilanteet symmetrisesti b suhteen. Tämä tulos voidaan yleistää mielivaltaiselle määrälle tulontekijöitä.

□

Korollaari 2.18. *Jos $p \in \mathbb{P}$ ja $p \mid (a_1 \cdot a_2 \cdot ... \cdot a_n)$, niin $p \mid a_j$ jollakin $j \in \{1, 2, 3, ..., n\}$.*

Todistus. **Korollaarin 2.17.** mukaan tapaus jossa alkuluvun p jakamassa tulossa on kaksi tulontekijää on selvä. Oletetaan siis, että väite pätee kun tulontekijöitä on $k \in \mathbb{Z}$ kappaletta eli tehdään induktio-oletus: jos $p \mid (a_1 \cdot a_2 \cdot ... \cdot a_k)$ niin $p \mid a_j$ jollain $j \in \{1, 2, 3..., k\}$. Oletetaan myös, että $p \mid (a_1 \cdot a_2 \cdot ... \cdot a_k \cdot a_{k+1})$. Merkitään nyt, että $a_1 \cdot a_2 \cdot ... \cdot a_k = b$. Nyt, $p \mid b \cdot a_{k+1}$, jolloin **korollaarin 2.17.** mukaan $p \mid b$ tai $p \mid a_{k+1}$. Induktio-oletuksesta seuraa, että jos $p \mid (a_1 \cdot a_2 \cdot ... \cdot a_k)$, niin $p \mid a_j$ jossa $j \in \{1, 2, 3, ..., k\}$. Siis $p \mid a_j$ missä $j \in \{1, 2, 3, ..., k\}$ tai $p \mid a_{k+1}$ eli $p \mid a_j$ kun $j \in \{1, 2, 3, ..., k, k + 1\}$. Koska oletuksesta seuraa, että se pätee arvolla $k + 1$ niin induktion mukaan se pätee mielivaltaisella luvulla $n \in \mathbb{N}$.

□

Korollaari 2.19. *Jos $p \mid q_1 \cdot q_2, \cdot ... \cdot q_n$ ja $p, q_1, q_2, ..., q_n \in \mathbb{P}$ niin $p = q_j$ jollain $j \in \{1, 2, 3, ..., n\}$.*

Todistus. **Korollaarin 2.13.** mukaan $p \mid q_j$ jollain $j \in \{1, 2, 3, ..., n\}$. Tällöin **määritelmän 2.7.** mukaan $p = 1$ tai $p = q_j$, mutta koska $p \in \mathbb{P}$ niin on pakko olla, että $p = q_j$.

□

Lause 2.20. *(Aritmetiikan peruslause) Kaikki positiiviset kokonaisluvut $n \geq 2$ voidaan kirjoittaa muodossa*

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k,$$

missä luvut $p_1, p_2, ..., p_k \in \mathbb{P}$. Tämä esitystapa on yksiselitteinen kun ei oteta huomioon missä järjestyksessä tulontekijät esitetään (millä ei ole tietenkään merkitystä tuloksen kannalta kokonaislukujen kertolaskulla).

Todistus. **Lauseen 2.13.** mukaan kaikille $n \geq 2$ pätee, että ne ovat alkulukujen tuloja. Tehdään nyt vastaoletus. Oletetaan, että on olemassa kaksi esitystapaa alkulukujen tuloina luvulle n eli

$$n = p_1 \cdot p_2 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_t, \ kun \quad p_1, p_2, ...p_k, q_1, q_2, ..., q_t \in \mathbb{P}.$$

Oletetaan myös, että näitä esitystapoja ei voi muokata samoiksi uudelleenjärjestämällä tulontekijät ja että n on pienin sellainen luku, jolle tämä pätee. **Lauseen 2.1.** mukaan $p_1 \mid q_1 \cdot q_2 \cdot ... \cdot q_t$ jolloin **korollaarin 2.19.** mukaan $p_1 = q_j$ jollain $j \in \{1, 2, 3..., t\}$. Tällöin molemmat puolet voidaan jakaa luvulla p_1. Nyt kummastakin esityksestä on poistettu sama tulontekijä eli ne ovat edelleenkin erilaisia siten, että tulontekijöiden uudelleen järjestäminen ei tuota niistä samaa esitystä. Lisäksi on selvää, että $\frac{n}{p_1} < n$ vaikka luvun n piti olla pienin sellainen luku jolla on edellä vaadittu ominaisuus. Tämä on ristiriita joten alkuperäinen väite on tosi.

□

Esimerkki 2.21. Koska $3 \mid 138$ niin **korollaarin 2.19.** mukaan luku 3 sisältyy **lauseen 2.20.** mukaiseen luvun 138 alkulukuhajotelmaan. Kyseinen alkulukuhajotelma on muotoa $138 = 2 \cdot 3 \cdot 23$.

Määritelmä 2.22. Lauseen 2.20. nojalla mikä tahansa kokonaisluku $n \geq 1$ voidaan kirjoittaa yksikäsitteisessä muodossa

$$n = \prod_{k=1}^{\infty} p_k^{\alpha_k}$$

jossa $\alpha_k \geq 0$ ja luvuista $\alpha_t, \ \ t \in \{1, 2, ...\}$ vain äärellinen osa on aidosti nollaa suurempia (jotta rajataan luku n äärelliseksi). Lisäksi luvut $p_1, p_2, ..., p_k$ ovat alkulukuja suuruusjärjestyksessä eli $p_1 < p_2 < p_3...$

Esimerkki 2.23. Luku 120 voidaan esittää muodossa $120 = 2^3 \cdot 3 \cdot 5$ ja luku 1815 voidaan esittää muodossa $3 \cdot 5 \cdot 11^2$.

Lause 2.24. ***Määritelmään 2.22.*** *nojaten jos meillä on luvut* $a, b \in \mathbb{P}$*, niin*

$$a = \prod_{k=1}^{\infty} p_k^{\alpha_k} \quad ja \quad b = \prod_{k=1}^{\infty} p_k^{\beta_k}.$$

Tällöin

$$syt(a,b) = \prod_{k=1}^{\infty} p_k^{\gamma_k} \quad jossa \;\; \gamma_k = min\{\alpha_k, \beta_k\}.$$

Tässä vaiheessa ollaan käsitelty jaollisuus, alkuluvut ja suurin yhteinen tekijä. Voidaksemme siirtyä primitiivisiin juuriin, tarvitaan vielä kongruenssi, kongruenssiyhtälöt, jäännösluokat renkaille $\mathbb{Z}_m$ sekä Eulerin totienttifunktio. Renkaat ja jäännösluokat kuuluvat algebraan ja tässä tutkielmassa emme käy niitä perin pohjin läpi. Renkaiden osalta vain viitataan kirjallisuuteen, missä ne esitellään, mutta jäännösluokat ja jäännösluokkasysteemit käydään läpi riittävällä tarkkuudella sillä ne ovat keskeisessä roolissa primitiivisistä juurista puhuttaessa. Lähdetään liikkeelle määrittelemällä kongruenssi.

2.0.3 Kongruenssi

Määritelmä 2.25. Olkoon $m \neq 0$. Jos $m \mid (a - b)$, niin silloin sanotaan, että a on kongruentti luvun b kanssa modulo m. Käytetään kongruenttisuudesta merkintää

$$a \equiv b \pmod{m}.$$

Lisäksi, jos luvuilla a ja b on kongruensseja muilla moduloilla, ne voidaan listata merkinnällä $(mod\ a,\ b, ...)$. Tällöin siis merkintä

$$a \equiv b \pmod{m,\ n,\ t}$$

tarkoittaa, että a on kongruentti luvun b kanssa moduloilla m, n ja t. Jos taas luvut eivät ole kongruenttisia niin käytetään merkintää $a \not\equiv b \pmod{m}$.

[3]

Esimerkki 2.26. Koska $72 - 2 = 70$ on jaollinen luvulla 5 niin $72 \equiv 2 \pmod{5}$ ja vastaavasti luku 3 jakaa luvun 30, niin $30 \equiv 0 \pmod{3}$.

Lemma 2.27. *Kongruenssi on ekvivalenssirelaatio eli sillä on seuraavat ominaisuudet.*

i) $a \equiv a \pmod{m}$.

ii) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$.

iii) $a \equiv b \pmod{m}$ *ja* $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Todistus. Nyt luvulle a pätee, että

$$a - a = 0 = 0 \cdot m,\ m \in \mathbb{Z}\ ja\ m \neq 0,$$

niin selvästi kohta *i*) pätee. Nyt jos $m \mid (a-b)$ niin $(a-b) = k \cdot m$. Nyt

$$-k \cdot m = -(a-b) = (b-a)$$

eli **määritelmän 2.25.** mukaan $b \equiv a \pmod{m}$ eli kohta *ii*) pätee. Oletetaan että $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$. Tällöin $m \mid (a-b)$ ja $m \mid (b-c)$. Tällöin

$$b - c = k_1 \cdot m\ eli\ b = k_1 \cdot m + c.$$

Tästä seuraa, että

$$a - b = a - k_1 \cdot m - c = k_2 \cdot m\ eli\ a - c = m \cdot (k_1 + k_2),$$

jolloin $m \mid (a-c)$. Nyt siis $a \equiv c \pmod{m}$. Näin ollen kongruenssirelaatio on ekvivalenssirelaatio.

□

Lause 2.28. *i*) *Jos* $a \equiv b \pmod{m}$ *ja* $k \in \mathbb{Z}$, *niin*

$a + k \equiv b + k \pmod{m}$ *ja* $k \cdot a \equiv k \cdot b \pmod{m}$.

ii) *Jos* $a \equiv b \pmod{m}$ *ja* $c \equiv d \pmod{m}$, *niin*

$a + c \equiv b + d \pmod{m}$ *ja* $a \cdot c \equiv b \cdot d \pmod{m}$.

Todistus. Olkoot $a \equiv b \pmod{m}$ ja $k \in \mathbb{Z}$. Tällöin $m \mid (a-b)$. Nyt

$$(a + k) - (b + k) = a - b,$$

eli $m \mid ((a+k) - (b+k))$. Lisäksi

$$(k \cdot a) - (k \cdot b) = k \cdot (a - b)$$

jolloin **lauseen 2.2.** mukaan $d \mid ((k \cdot a) - (k \cdot b))$. Siispä väite $i)$ on tosi. Oletetaan lisäksi, että $c \equiv d \pmod{m}$. Tällöin $m \mid (c - d)$ eli nyt $c - d = k_1 \cdot m$ ja $a - b = k_2 \cdot m$. Nyt siis

$$(a + c) - (b + d) = a - b + c - d = k_2 \cdot m + k_1 \cdot m = m \cdot (k_1 + k_2).$$

Tällöin kongruenssin määritelmän mukaan $a + c \equiv b + d \pmod{m}$. Ratkaistaan nyt a ja d. Saadaan $a = k_2 \cdot m + b$ ja $d = c - k_1 \cdot m$. Tällöin siis

$$a \cdot c - b \cdot d = c \cdot (k_2 \cdot m + b) - b \cdot (c - k_1 \cdot m) = c \cdot k_2 \cdot m + c \cdot b - c \cdot b + b \cdot k_1 \cdot m = m \cdot (c \cdot k_2 + b \cdot k_1).$$

Tällöin $m \mid (a \cdot c - b \cdot d)$ eli $a \cdot c \equiv b \cdot d \pmod{m}$ ja väite $ii)$ on tosi.

□

Esimerkki 2.29. Koska $7 \equiv 20 \pmod{13}$, niin pätee, että $7 + 4 \equiv 20 + 4 \pmod{13}$ ja $7 \cdot 6 \equiv 20 \cdot 6$. Nyt $24 - 11 = 13$ ja $120 - 42 = 78 = 13 \cdot 6$. Tällöin ilmiselvästi $7 + 4 \equiv 20 + 4 \pmod{13}$ ja $7 \cdot 6 \equiv 20 \cdot 6 \pmod{13}$.

Lause 2.30. *Jos $P(x)$ on polynomi, jossa on kokonaislukukertoimet niin*

$$a \equiv b \pmod{m} \implies P(a) \equiv P(b) \pmod{m}.$$

Todistus. Jos $a \equiv b \pmod{m}$ niin silloin **lauseen 2.28.** kohdan $ii)$ mukaan $a \cdot a \equiv b \cdot b$. Tätä toistamalla saadaan $a^n \equiv b^n \pmod{m}$ mille tahansa epänegatiiviselle luvulle n. Olkoot nyt

$$P(x) = \sum_{n=0}^{t} c_n \cdot x^t.$$

Tällöin **lauseen 2.28.** kohdan $i)$ mukaan erityisesti $c_n \cdot a^n \equiv c_n \cdot b^n \pmod{m}$. Tällöin mille tahansa luvulle $n \in \{0, 1, 2..., t\}$ pätee, että $P(a) \equiv P(b) \pmod{m}$ toistamalla summan osille **lauseen 2.28.** kohtaa $i)$.

[3] □

Esimerkki 2.31. Olkoot $P(X) = 2x^2 + 5$ ja $8 \equiv 14 \pmod{3}$. Nyt $P(8) = 2 \cdot 8^2 + 5 = 133$ ja $P(14) = 2 \cdot 14^2 + 5 = 397$. Koska $397 - 133 = 264$ jossa $3 \mid 264$ niin $P(8) \equiv P(14) \pmod{3}$.

Kuten edellä mainittiin, niin tässä tutkielmassa ei esitellä algebraa mitä käytetään vaan viitataan kirjallisuuteen, missä ne on esitetty tarkasti. Algebralliset rakenteet jotka

olisi syytä tuntea ovat ryhmä, rengas, kunta ja ekvivalenssiluokat. Lukijan olisi myös hyvä tuntea vaihdannaisuus. Suosittelen lähdemateriaaliksi Jokke Häsän ja Johanna Rämön kirjaa "Johdatus abstraktiin algebraan". Kyseisessä kirjassa kolmannessa painoksessa esitellään ryhmät alkaen sivulta 43, ekvivalenssiluokat alkaen sivulta 140, renkaat alkaen sivulta 169 ja kunnat alkaen sivulta 184. Niiden alkioiden joukkoa jotka ovat ekvivalenssirelaatiossa tietyn alkion kanssa kutsutaan sen alkion ekvivalenssiluokaksi. Kongruenssin tapauksessa näitä ekvivalenssiluokkia kutsutaan jäännösluokiksi. [1]

2.0.4 Jäännösluokat

Lemma 2.32. *Kongruenssirelaatiolla, joka on modulo m, on m kappaletta erilaisia jäännösluokkia.*

Todistus. Olkoon $n \in \mathbb{Z}$. Tällöin **lauseen 2.4.** nojalla voidaan kirjoittaa

$$n = k \cdot m + r, \quad 0 \leq r \leq m - 1.$$

Tällöin $n - r = k \cdot m$ eli $n \equiv r \pmod{m}$. Siis mielivaltainen luku n on kongruentti jonkin luvun $0, 1, 2, ..., m-1$ kanssa. Selvästi mitkään näistä luvuista eivät ole keskenään kongruentteja modulo m. Tällöin siis ekvivalenssiluokkien määrä on sama kuinka monta erilaista vaihtoehtoa luvulle r on eli m kappaletta.

[3] □

Määritelmä 2.33. Luvun a jäännösluokka modulo m on joukko

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\} = \{a + k \cdot m \mid k \in \mathbb{Z}\}.$$

Käytetään siitä merkintää $\lfloor a \rfloor_m$.

[3]

Esimerkki 2.34.

$$\lfloor 3 \rfloor_5 = \{..., -7, -2, 3, 8, 13, ...\},$$

$$\lfloor 6 \rfloor_{11} = \{..., -16, -5, 6, 17, 28, ...\}.$$

Määritelmä 2.35. $\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$.

[3]

Esimerkki 2.36.

$$\mathbb{Z}_{17} = \{\lfloor 0 \rfloor_{17}, \lfloor 1 \rfloor_{17}, \lfloor 2 \rfloor_{17}, ..., \lfloor 16 \rfloor_{17}\}.$$

Määritelmä 2.37. $(\mathbb{Z}_m, +, \cdot)$ on vaihdannainen rengas jossa on m kappaletta alkioita, $+$ ja $\cdot$ on määritelty joukossa $\mathbb{Z}_m$ seuraavanlaisesti.

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}, \quad a, b \in \mathbb{Z}.$$

[3]

Määritelmä 2.38. Lemman 2.32. todistuksen mukaan, mikä tahansa $n \in \mathbb{Z}$ on kongruenttia täsmälleen yhden luvun $r \in \{0, 1, 2, ..., m-1\}$ kanssa. Tällöin r on luvun n pienin positiivinen jakojäännös modulo m.

[3]

Lause 2.39. *Olkoon $m \geq 2$. Rengas $\mathbb{Z}_m$ on kunta, jos ja vain jos $m \in \mathbb{P}$.*

[1]

Määritelmä 2.40. $\{a_1, a_2, ..., a_m\}$ on täydellinen jäännösluokkasysteemi modulo m jos

$$\{\overline{a_1}, \overline{a_2}, ..., \overline{a_m}\} = \mathbb{Z}_m.$$

Tällöin $\{a_1, a_2, ..., a_m\}$ sisältää täsmälleen yhden alkion jokaisesta jäännösluokasta.

[3]

Esimerkki 2.41. $\{0, 1, ..., 5\}$ on täydellinen jäännösluokkasysteemi, mutta $\{0, 2, ..., 5\}$ ei ole.

Lause 2.42. *Olkoot $m \geq 1$ ja $U \subset \mathbb{Z}$. Tällöin U on täydellinen jäännösluokkasysteemi modulo m, jos ja vain jos vähintään kaksi seuraavista ehdoista on totta:*

i) Joukossa U on m kappaletta alkioita.

ii) Mielivaltaiset kaksi alkiota joukosta U ovat toistensa kanssa ei−kongruentteja modulo m.

iii) Jokaista lukua a kohti on olemassa $u \in U$ s.e. $a \equiv u \pmod{m}$.

Todistus. Olkoon U täydellinen jäännösluokkasysteemi modulo m eli $U = \{u_1, u_2, ..., u_m\}$, missä $\{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\} = \mathbb{Z}_m$. Nyt **määritelmän 2.40.** mukaan U sisältää m kappaletta alkioita. Tämä todistaa kohdan i). Tehdään kohtaa ii) varten vastaoletus eli oletetaan että $u_a, u_b \in U$ ja että $u_a \equiv u_b \pmod{m}$. Tällöin a ja b kuuluvat samaan jäännösluokkaan. Tällöin U sisältää korkeintaan $m-1$ eri jäännösluokan edustajia joukossa $\{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\} = \mathbb{Z}_m$, mikä on ristiriidassa sen kanssa että kyseessä on täydellinen jäännösluokkasysteemi. Siispä kohta ii) on tosi. Sinänsä riittää näyttää tähän suuntaan, että vähintään kaksi ehdoista on tosia, mutta todistetaan, että myös ehto iii) on tosi jos U on täydellinen jäännösluokkasysteemi. Olkoon $a \in \mathbb{Z}$. **Lemman 2.32.** todistuksessa ilmeni että tällöin $\overline{a} \in \mathbb{Z}_m$. Mutta koska $\{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\} = \mathbb{Z}_m$ niin välttämättä on olemassa $u \in U$ siten että $\overline{a} = \overline{u}$ eli $u \equiv a \pmod{m}$ jolloin myös iii) on tosi.

Todistetaan ekvivalenssi vielä toiseen suuntaan. Nyt pitää olettaa että ainakin kaksi ehdoista ovat tosia eli on kolme eri tapausta. Tapaus 1: Oletetaan että i) ja ii) ovat tosia. Tällöin U sisältää m alkiota jotka ovat toistensa kanssa ei kongruentteja. Tästä seuraa, että U sisältää $m : n$ eri jäännösluokan edustajia ja koska $\mathbb{Z}_m$ sisältää m jäännösluokkaa niin välttämättä $\{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\} = \mathbb{Z}_m$ eli U on täydellinen jäännösluokkasysteemi.

Tapaus kaksi: Oletetaan että i) ja iii) ovat tosia. Tällöin U sisältää m alkiota ja mielivaltaisella $a \in \mathbb{Z}$ pätee että $u \equiv a \pmod{m}$ jollakin $u \in U$. Selkeästi $\{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\} \subset \mathbb{Z}_m$ koska U sisältää enintään m jäännösluokkaa. Olkoot $\overline{a} \in \mathbb{Z}_m$. Tällöin on olemassa $u \in U$ jolla $a \equiv u \pmod{m}$ eli $\overline{a} = \overline{u}$ jolloin $\overline{a} \in \{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\}$. Tällöin $\mathbb{Z}_m \subset \{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\}$. Nyt, koska molemmat joukot ovat toistensa osajoukkoja niin kyseessä on sama joukko eli $\{\overline{u_1}, \overline{u_2}, ..., \overline{u_m}\} = Z_m$ jolloin U on täydellinen jäännösluokkasysteemi.

Tapaus kolme: Oletetaan että ii) ja iii) ovat tosia. Koska U alkiot eivät ole kongruentteja ja jokaiselle kokonaisluvulle löytyy jäännösluokka niin riittää näyttää että U sisältää m alkiota. Ehdon ii) mukaan U sisältää enintään m jäännösluokkaa. Koska mielivaltaisella luvulla $1 \leq a \leq m$ on olemassa $u \in U$ jolla $a \equiv u \pmod{m}$ ja jokainen eri a on keskenään ei kongruentteja niin U sisältää vähintään m kappaletta alkioita. Tästä voimme päätellä että U sisältää tasan m kappaletta alkioita eli U on täydellinen jäännösluokkasysteemi. Nyt on osoitettu että kaksi ehdoista riittää siihen että U on täydellinen jäännösluokkasysteemi.

□

Korollaari 2.43. *Olkoot $\{a_1, a_2, ..., a_m\}$ täydellinen jäännösluokkasysteemi modulo m,*

$syt(k, m) = 1$ ja $b \in \mathbb{Z}$. Tällöin

$$A = \{k \cdot a_1 + b, k \cdot a_2 + b, ..., k \cdot a_m + b\}$$

on täydellinen jäännösluokkasysteemi modulo m.

Todistus. Selkeästi A sisältää tasan m alkiota, joten **lauseen 2.42.** mukaan riittää tarkistaa, että sen alkiot ovat keskenään ei kongruentteja. Oletetaan siis, että

$$k \cdot a_p + b \equiv k \cdot a_t + b \pmod{m}.$$

Tällöin kongruenssin määritelmän mukaan $m \mid k \cdot a_p + b - k \cdot a_t - b = k \cdot (a_p - a_t)$. Kuitenkin $syt(m, k) = 1$ jolloin $m \mid (a_p - a_t)$. Tällöin kongruenssin määritelmän mukaan $a_p \equiv a_t \pmod{m}$. Tällöin kyseessä on sama jäännösluokka eli $p = t$. Koska mielivaltaiset A alkiot jotka ovat keskenään kongruentteja ovat sama alkio niin A alkiot ovat keskenään ei-kongruentteja jolloin väite on tosi.

[3] □

Palataan tässä välissä hetkeksi alkulukuihin. Näitä kohtia ei ollut mielekästä käsitellä aiemmin alkulukujen yhteydessä sillä ne vaativat jäännösluokkasysteemejä jotta ne voitaisiin esitellä järkevästi.

Lause 2.44. *(Fermat'n pieni lause)*

Jos $p \in \mathbb{P}$ ja $p \nmid a$ niin $a^{p-1} \equiv 1 \pmod{p}$.

Todistus. $\{0, 1, 2, ..., p-1\}$ on täydellinen jäännösluokkasysteemi modulo p. Lisäksi koska $p \nmid a$ niin $syt(a, p) = 1$. Tällöin **korollaarin 2.43.** mukaan $\{0, a, 2 \cdot a, ..., a \cdot (p-1)\}$ on myös täydellinen jäännösluokkasysteemi. Tällöin luvut $\{0, 1, 2, ..., p-1\}$ ovat kongruentteja lukujen $\{0, a, 2 \cdot a, ..., a \cdot (p-1)\}$ kanssa jossain järjestyksessä. Siis **määritelmän 2.25.** laskusääntöjen mukaan,

$$a \cdot 2 \cdot a \cdot ... \cdot a \cdot (p-1) \equiv 1 \cdot 2 \cdot ... \cdot (p-1) \pmod{p} \iff (p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Siispä $p \mid (p-1)! \cdot (a^{p-1} - 1)$, mutta koska $p \nmid (p-1)!$ niin välttämättä pätee, että $p \mid (a^{p-1} - 1)$. Tällöin $a^{p-1} \equiv 1 \pmod{p}$.

[3] □

Esimerkki 2.45. Olkoot meillä luvut 7 ja 3. Nyt pätee, että $7 \in \mathbb{P}$ ja että $7 \nmid 3$. Tarkastellaan lukua 3^{7-1}. Tälle luvulle pätee että $3^{7-1} = 729 = 7 \cdot 104 + 1$. Tästä nähdään että $3^{7-1} \equiv 1 \pmod 7$ mikä vastaa **lauseen 2.44.** tulosta.

Korollaari 2.46. *Edellistä hieman muokkaamalla saadaan yhtäpitävä korollaari: Jos* $p \in \mathbb{P}$, *niin* $a^p \equiv a \pmod p$ *kaikilla* $a \in \mathbb{Z}$.

[3]

Vielä täytyy käsitellä Eulerin totienttifunktio ja vähennetty jäännösluokkasysteemi ennen kuin voimme siirtyä kongruenssiyhtälöihin ja primitiivisiin juuriin. Käydään Eulerin totienttifunktio läpi ensin koska se on olennainen osa vähennetyn jäännösluokkasysteemin määritelmää.

2.0.5 Eulerin Totienttifunktio ja vähennetty jäännösluokkasysteemi

Määritelmä 2.47. Eulerin totienttifunktio $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ määritellään asettamalla $\phi(1) = 1$. Lisäksi luvuille $n \geq 2$ totienttifunktion on niiden alkioiden $a \in \{1, 2, ..., m\}$ joille pätee, että $syt(a, m) = 1$ lukumäärä. Eulerin totienttifunktio laskee siis suhteellisten alkulukujen määrän funktion syötteeseen n asti.

[3]

Esimerkki 2.48. $\phi(4) = 2$, $\phi(9) = 6$, $\phi(15) = 8$.

Määritelmä 2.49. Lukuteoreettinen funktio on funktio jonka lähtöjoukko on luonnollisten lukujen joukko ja maalijoukko reaalilukujen joukko.

[3]

Määritelmä 2.50. Lukuteoreettinen funktio f on multiplikatiivinen jos

$$f(m \cdot n) = f(m) \cdot f(n)$$

silloin kun $syt(m, n) = 1$.

[3]

Lause 2.51. ϕ *on multiplikatiivinen lukuteoreettinen funktio.*

Todistus. Tarkastellaan taulukkoa

$$\begin{array}{cccccc} 0 & 1 & 2 & ... & m-1 \\ m & m+1 & m+2 & ... & 2\cdot m-1 \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)\cdot m & (n-1)\cdot(m+1) & (n-1)\cdot(m+2) & ... & n\cdot m-1. \end{array}$$

Jokaisen sarakkeen luvut ovat keskenään kongruenttisia modulo m sillä sarakkeen seuraavan rivin luku saadaan lisäämällä edellisen rivin lukuun m. Lisäksi ensimmäisestä rivistä voidaan päätellä että on vain $\phi(m)$ saraketta, jonka luvut ovat luvun m kanssa suhteellisia alkulukuja sillä ϕ laskee niiden lukumäärän ja ensimmäinen rivi sisältää $m-1$ alkiota. Lisäksi koska **korollaarin 2.43.** mukaan joka sarake on täydellinen jäännösluokkasysteemi niin jokaisella sarakkeella on $\phi(n)$ kappaletta lukuja jotka ovat luvun n kanssa suhteellisia alkulukuja. Tällöin $\phi(m\cdot n)=\phi(m)\cdot\phi(n)$.

[3]

□

Esimerkki 2.52. $\phi(3)=2$ ja $\phi(7)=6$. Eulerin totienttifunktio on multiplikatiivinen joten $\phi(3)\cdot\phi(7)=2\cdot 6=12$. Lukua $3\cdot 7=21$ pienemmät luonnolliset luvut joiden suurin yhteinen tekijä luvun 21 kanssa on 1 ovat 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19 ja 20. Näitä on 12 kappaletta kuten pitikin olla.

Lause 2.53.

$$\phi(n)=n\prod_{p|n}(1-\frac{1}{p}),$$

missä $\prod_{p|n}(1-\frac{1}{p})$ *käy läpi kaikki eri alkuluvut jotka jakavat luvun* n*.*

Todistus. Oletetaan että $n=p^k$, missä $p\in\mathbb{P}$ ja $k\geq 1$. Tällöin meillä on luku u, $1\leq u\leq p^k$. Luvulle u pätee $syt(p^k,u)>1$ jos ja vain jos $u=l\cdot p$ kun $1\leq l\leq p^{k-1}$ jolloin

$$\phi(p^k)=p^k-p^{k-1}=(1-\frac{1}{p})\cdot p^k.$$

Yleisessä tapauksessa **määritelmän 2.22** mukaan $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot ...\cdot p_l^{\alpha_l}$ joten ylemmän havainnon ja **lauseen 2.51** mukaan

$$\phi(n)=\phi(p_1^{\alpha_1})\cdot\phi(p_2^{\alpha_2})\cdot ...\cdot\phi(p_l^{\alpha_l})$$

$$= (1 - \frac{1}{p_1}) \cdot p_1^{\alpha_1} \cdot (1 - \frac{1}{p_2}) \cdot p_2^{\alpha_2} \cdot ... \cdot (1 - \frac{1}{p_l}) \cdot p_l^{\alpha_l}$$
$$= n \prod_{p|n} (1 - \frac{1}{p}).$$

[3] □

Lause 2.54. *Alkiota $\overline{u} \in \mathbb{Z}_m$ kutsutaan kääntyväksi jos on olemassa alkio $\overline{u}^{-1} \in \mathbb{Z}_m$ siten että $\overline{u} \cdot \overline{u}^{-1} = 1$. Lisäksi $\overline{u}$ on kääntyvä jos ja vain jos $syt(u, m) = 1$. Määritellään*

$$\mathbb{Z}_m^* = \{\overline{u} \in \mathbb{Z}_m \mid \overline{u} \text{ on kääntyvä}\}.$$

Todistus. Nyt $\overline{x} = \overline{u}^{-1}$ jos ja vain jos $x \cdot u \equiv 1 \pmod{m}$ mikä on yhtä pitävää sen kanssa, että $x \cdot u - m \cdot y = 1$ jollain y. Tällä yhtälöllä on ratkaisuja jos ja vain jos $syt(u, m) = 1$.

[3] □

Määritelmä 2.55. Olkoot $m \geq 2$. Joukkoa $U \subset \mathbb{Z}$ kutsutaan vähennetyksi jäännösluokkasysteemiksi modulo m jos U sisältää täsmälleen yhden alkion jokaisesta $\mathbb{Z}_m^*$ jäännösluokasta.

[3]

Esimerkki 2.56. Jos valitsemme luvuksi $m = 8$ olisi luonnollista valita joukoksi $U = \{1, 3, 5, 7\}$ Kuitenkin koska mikä tahansa jäännösluokan edustaja kelpaa niin vaihtoehtoisesti voitaisiin valita $U = \{-7, 3, 13, 31\}$.

Lause 2.57. *Olkoon $\{a_1, a_2..., a_{\phi(m)}\}$ vähennetty jäännösluokkasysteemi modulo m. Jos $syt(k, m) = 1$ niin silloin myös*

$$\{k \cdot a_1, k \cdot a_2, ..., k \cdot a_{\phi(n)}\}$$

on vähennetty jäännösluokkasysteemi modulo m.

Todistus. Väitteen todistamiseksi riittää osoittaa että funktio $f : \overline{u} \longrightarrow \overline{k} \cdot \overline{u}$ on bijektio joukosta Z_m^* itseensä. Bijektio tarkoittaa funktiota jossa jokaisella maalijoukon alkiolla on täsmälleen yksi lähtöjoukon alkio joka kuvautuu sille. Nyt, koska $syt(k, m) = 1$ niin pätee, että $k \in \mathbb{Z}_m^*$. Kyseinen funktio on hyvin määritelty koska jos pätee, että $\overline{u} \in \mathbb{Z}_m^*$ niin silloin $syt(k \cdot u, m) = 1$. Tällöin $\overline{k} \cdot \overline{u} \in \mathbb{Z}_m^*$. Nyt koska funktiolla f on ilmiselvä käänteisfunktio $f^{-1} : \overline{u} \longrightarrow \overline{k^{-1}} \cdot \overline{u}$ niin se on bijektio (funktio on bijektio jos ja vain jos sillä on käänteisfunktio). [3] □

Lause 2.58. *Olkoon $m \geq 2$ ja $syt(a, m) = 1$. Tällöin*

$$a^{\phi(m)} \equiv 1 \ \ (mod\ m).$$

Todistus. **Lauseen 2.40.** todistuksessa näytettiin että funktio $f : \overline{u} \longrightarrow \overline{u} \cdot \overline{a}$ on bijektio $\mathbb{Z}_m^* \longrightarrow \mathbb{Z}_m^*$. Tällöin

$$\{\overline{u_1}, \overline{u_2}, ..., \overline{u_{\phi(m)}}\} = \{\overline{a} \cdot \overline{u_1}, \overline{a} \cdot \overline{u_2}, ..., \overline{a} \cdot \overline{u_{\phi(m)}}\}.$$

Koska kerrointa a on $\phi(m)$ kappaletta niin

$$\overline{u_1} \cdot \overline{u_2} \cdot ... \cdot \overline{u_{\phi(m)}} = a^{\phi(m)} \cdot (\overline{u_1} \cdot \overline{u_2} \cdot ... \cdot \overline{u_{\phi(m)}}).$$

Nyt koska kyseessä on bijektio niin termi $\overline{u_1} \cdot \overline{u_2} \cdot ... \cdot \overline{u_{\phi(m)}}$ on kääntyvä jolloin se voidaan "jakaa" pois molemmilta puolilta ja saadaan

$$\overline{a^{\phi(m)}} = \overline{1} \Longleftrightarrow a^{\phi(m)} \equiv 1 \ \ (mod\ m).$$

[3] □

Luku 3

Primitiiviset juuret ja yleiset kongruenssipolynomit

Tässä luvussa esitellään primitiiviset juuret. Yleiset kongruenssipolynomit ovat viimeinen esitietona käytävä asia. Kongruenssipolynomit on sisällytetty lukuun 3 erikseen koska se on aiheena paljon läheisempi primitiivisten juurten kanssa. Tutkielmassa on aiemmin esiintynyt kongruenssiyhtälöitä muun muassa **lauseessa 2.44.** Kongruenssipolynomeissa mielenkiintoista on se kuinka monta ratkaisua niillä on ja mitkä ne ratkaisut ovat. Kun puhumme yleisestä kongruenssipolynomista tarkoitamme kongruenssia joka on muotoa:

$$p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_0 \equiv 0 \pmod{m}.$$

Polynomikongruensseissa tulee löytää ne muuttujan x arvot joilla kongruenssirelaatio pätee. Esimerkiksi, jos meillä on kongruenssi $x^2 + 3 \equiv 0 \pmod{7}$ niin kokeilemalla huomaamme että ratkaisut ovat $x = 2$ ja $x = 5$. Lisäksi huomaamme että myös $x = 9$ ratkaisee yhtälön. Tämä johtuu siitä että jo löydetty ratkaisu $x = 2 \equiv 9 \pmod{7}$. Eli ratkaisu ilmoitetaan aina kyseisen kongruenssin modulon suhteen. Tällöin ratkaisu edelliseen yhtälöön kirjoitettaisiin $x \equiv 2$ ja $x \equiv 5 \pmod{7}$. Kongruenssiyhtälöt ovat analogisia ekvivalenssiluokkien kuntaominaisuuden kautta perinteisten polynomien kanssa. Esittely käyttää lähdemateriaalina Eero Saksmanin kurssin Introduction to number theory kurssikalvoja paitsi **lauseen 3.11.** todistuksen kohdalla jossa käytetään Kenneth Irelandin ja Michael Rosenin kirjaa "A Classical Introduction to Modern Number Theory". Tässäkin luvussa kuhunkin lähteeseen viitataan aina todistuksen yhteydessä jos lähdettä on käytetty.

3.0.1 Kongruenssien polynomit

Lause 3.1. *Tarkastellaan asteluvun n kongruenssia*

$$p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_0 \equiv 0 \pmod{m}$$

ja oletetaan, että $m \in \mathbb{P}$ *sekä että* $m \nmid a_n$*. Tällöin kyseisellä kongruenssilla on enintään n kappaletta keskenään ei kongruenttisia ratkaisuja modulo m.*

Todistus. Todistetaan väite induktiolla. Merkitään $t(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x$. Näytetään aluksi tapaus n ja näytetään että se seuraa tapauksesta $n-1$. Olkoon x_1 ratkaisu lauseen kongruenssiin. Kyseisestä kongruenssista saadaan pyöriteltyä muotoon

$$p(x) = (x - x_1) \cdot q(x) + p(x_1)$$

jossa $q(x)$ on $\frac{t(x)-t(x_1)}{x-x_1}$. Jotta $q(x)$ olisi hyvin määritelty niin termin $x - x_1$ tulee jakaa polynomi $t(x) - t(x_1)$. Osoitetaan tämä yleisesti. Ottamalla termit a_j yhteisiksi tekijöiksi edellinen voidaan esittää muodossa

$$\frac{a_n \cdot (x^n - x_1^n) + a_{n-1} \cdot (x^{n-1} - x_1^{n-1}) + ... + a_1 \cdot (x - x_1)}{x - x_1}.$$

Jokaista termiä kertoo muoto $(x^k - x_1^k)$. Meidän siis tulee näyttää että $x - y \mid x^n - y^n$ millä tahansa luonnollisella luvulla n jotta esitysmuotomme olisi pätevä. Johdetaan tulos suoraan.

$$\begin{aligned} x^n - y^n &= x \cdot y^{n-1} + x^2 \cdot y^{n-2} + ... + x^n \cdot y^{n-n} - y^n \cdot x^{n-n} - y^{n-1} \cdot x - ... - y \cdot x^{n-1} \\ &= (x \cdot y^{n-1} - y^n) + (x^2 \cdot y^{n-2} - x \cdot y^{n-1}) + ... + (x^n - x^{n-1} \cdot y^{n-1}) \\ &= (x - y)(y^{n-1}) + (x - y)(x \cdot y^{n-2}) + ... + (x - y)(x^{n-1}) \\ &= (x - y) \sum_{k=0}^{n-1} x^k \cdot y^{n-k-1}. \end{aligned}$$

Jatketaan nyt itse lauseen todistamista. Koska $m \mid p(x_1)$ niin kongruenssimme on ekvivalenttia kongruenssin

$$(x - x_1) \cdot q(x) \equiv 0 \pmod{m}$$

kanssa. Nyt jos meillä on x_2 siten että $x_2 \not\equiv x_1 \pmod{m}$, eli ne ovat eri ratkaisuja, niin silloin

$$m \mid (x_2 - x_1) \cdot q(x_2).$$

Mutta koska $x_2 \not\equiv x_1 \pmod{m}$ ja $m \in \mathbb{P}$ niin välttämättä pätee, että $m \mid q(x_2)$. Tällöin muut juuret kuin x_1 ratkaisevat polynomikongruenssin

$$q(x) \equiv 0 \pmod{m}.$$

Nyt koska $m \nmid a_n$ mikä on funktion $q(x)$ korkeimman asteen termin kerroin niin tämä vastaa induktiossa kohtaa $n-1$. Edellä näytettiin että tässä tapauksessa $n-1 \Longrightarrow n$. Nyt siis pitää vielä näyttää että tapaus $n = 0$ pätee. Kun $n = 0$ niin saadaan $a_0 \equiv 0 \pmod{m}$. Koska oletuksesta seuraa, että $m \nmid a_0$ niin kongruenssilla ei tällöin ole ratkaisuja eli väite pätee kun kun $n = 0$. Siispä induktion mukaan väite on tosi kaikilla $n \in \mathbb{N}$.

[3]

□

Esimerkki 3.2. Tämän luvun alussa olevassa kongruenssiyhtälössä $x^2 + 1 \equiv 0 \pmod{5}$ löydettiin 2 juurta. Kyseisessä kongruenssissa $m = 5$ on alkuluku joten sillä tulisi olla enintään korkeimman x:n potenssin verran ratkaisuja eli 2 kappaletta. Toinen esitetty yhtälö $x^2 \equiv 1 \pmod{8}$ ei kuitenkaan omaa vain kahta ratkaisua vaan neljä. Tässä kuitenkaan modulo ei ollut alkuluku joten **lause 3.1.** ei päde tähän kongruenssiin.

Korollaari 3.3. *Olkoot $m \in \mathbb{P}$ ja $n < m$. Jos kongruenssilla*

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_0 \equiv 0 \pmod{m}$$

on enemmän kuin n ratkaisua $(mod\ m)$ niin $m \mid a_j$ kaikilla $j \in \{0, 1, ..., n\}$ ja kongruenssi on totta millä tahansa luvulla x.

Todistus. Oletetaan että kongruenssilla

$$a_{j_0} \cdot x^{j_0} + a_{j_0-1} \cdot x^{j_0-1} + ... + a_0 \equiv 0 \pmod{m}$$

on enemmän kuin n juurta, $m \nmid a_j$ jollain $j_0 \in \{0, 1, ..., n\}$. Nyt kongruenssi on ekvivalentti korollaarin kongruenssin kanssa ja $m \nmid a_{j_0}$. Nyt **lauseen 3.1.** mukaan kyseisellä kongruenssilla on enintään j_0 kappaletta juuria mikä on ristiriita. Siispä $m \mid a_j$ kaikilla $j \in \{0, 1, ..., n\}$ jolloin kongruenssi on tosi millä tahansa arvolla x.

[3] □

Korollaari 3.4. *Jos $p \in \mathbb{P}$ ja $d \mid (p-1)$ niin kongruenssilla*

$$x^d \equiv 1 \pmod{p}$$

on täsmälleen d ratkaisua modulo p.

Todistus. Koska $d \mid (p-1)$ niin voidaan kirjoittaa $p-1 = d \cdot d'$. Nyt

$$x^{p-1} - 1 = x^d \cdot x^{d \cdot d' - d} + x^d \cdot x^{d \cdot d' - 2d} + ... + x^{d \cdot d' - d \cdot d'} - x^{d \cdot d' - d} - x^{d \cdot d' - 2d} - ... - x^{d \cdot d' - d \cdot d'}$$

$$= (x^d - 1) \cdot (x^{(d'-1) \cdot d} + x^{(d'-2) \cdot d} + ... + x^{(d'-d') \cdot d}) = (x^d - 1) \cdot g(x).$$

Missä $g(x) = x^{(d'-1) \cdot d} + x^{(d'-2) \cdot d} + ... + x^{(d'-d') \cdot d}$ jolloin sen asteluku on $(d'-1) \cdot d = p-1-d$. Sen korkeimman asteen termin kerroin on 1 jolloin $p \nmid a_n = 1$. Tällöin **lauseen 3.1.** mukaan kongruenssilla

$$g(x) \equiv 0 \pmod{p}$$

on enintään $p-1-d$ ratkaisua modulo p. Toisaalta nyt **lauseen 2.44.** mukaan kongruenssilla $x^{p-1} - 1 \equiv 0 \pmod{p}$ on vähintään $p-1$ ratkaisua moduloa p. Erityisesti luvut $1, 2, ..., p-1$ ovat sen ratkaisuja. Nyt koska termien tulolla on ratkaisuja $p-1$ kappaletta ja toisella termillä $p-1-d$ kappaletta niin kongruenssilla $x^d - 1 \equiv 0 \pmod{p}$ tulee olla ainakin $p-1-(p-1-d) = d$ eri ratkaisua modulo p. **Lause 3.1.** taas takaa että ratkaisuja ei ole enempää kuin d joten ratkaisuja on tasan d kappaletta. [3] □

Lause 3.5. *Kokonaisluku $p \geq 2$ on alkuluku jos ja vain jos $(p-1)!+1$ on jaollinen luvulla p.*

Todistus. Tapauksessa $p = 2$ väitteestä saadaan $(2-1)! + 1 = 2, \quad 2 \mid 2$ joten sitä ei tarvitse erikseen tarkastella. Todistetaan aluksi " $\Rightarrow$ " suunta eli oletetaan, että $p \geq 3$ on alkuluku. **Lauseen 2.44.** mukaan kongruenssilla

$$x^{p-1} - 1 - (x-1) \cdot (x-2) \cdot ... \cdot (x-(p-1)) \equiv 0 \pmod{p}$$

on ainakin $p-1$ juurta jotka ovat $x = 1, 2, ..., p-1$. Toisaalta tämän kongruenssin asteluku on pienempi kuin $p-1$ kun sulut avataan niin polynomista vähennetään termi x^{p-1} jolloin sen asteluku on $p-2$. Tällöin **korollaarin 3.3.** mukaan kyseinen kongruenssi on tosi millä tahansa kokonaisluvulla x. Asetetaan nyt $x = 0$. Tällöin kongruenssi saa muodon

$$0 - 1 + (-1) \cdot (-1) \cdot (-2) \cdot ... \cdot (p-1) \equiv 0 \pmod{p}.$$

Alkuluku p on pariton joten $p-1$ on parillinen. Tällöin kun -1 kertoimet sievennetään pois niin kongruenssista saadaan $-1-(1\cdot 2\cdot ...\cdot (p-1))\equiv 0 \pmod{p}$. Tästä voidaan vielä johtaa

$$-((p-1)!+1)\equiv 0 \pmod{p}.$$

Tämä todistaa kongruenssin määritelmän mukaan väitteen. Todistetaan seuraavaksi vielä väitteen $\Leftarrow$ suunta eli oletetaan $p \mid (p-1)!+1$. Tällöin kongruenssi $(p-1)!\equiv 1 \pmod{p}$ pätee. Oletetaan lisäksi että p ei ole alkuluku. Tällöin sen jakajat löytyvät lukujen $1,2,...,p-1$ joukosta. Tällöin luvuilla p ja $(p-1)!$ on jokin lukua 1 suurempi yhteinen tekijä eli $syt((p-1)!,p)>1$. Tämä tarkoittaa että $(p-1)!\equiv 0 \pmod{p}$ mikä on ristiriidassa oletuksen kanssa joten p on alkuluku.

[3] □

Esimerkki 3.6. Luku 4 ei ole alkuluku. Myöskään ei päde että $(4-1)!+1=7$ olisi jaollinen luvulla 4. Alkuluvulle 5 taas pätee, että $(5-1)!+1=24+1=25$ on jaollinen luvulla 5.

3.0.2 Primitiiviset juuret

Nyt voimmekin siirtyä primitiivisiin juuriin. Mutta mistä primitiivisissä juurissa on kyse? Luku a on primitiivinen juuri modulolla m kun kaikki luvut b jotka ovat suhteellisia alkulukuja luvun m suhteen ovat kongruenttisia jonkin luvun a potenssin kanssa modulolla m. Käytännössä tämä näkyy siten että kun kyseessä on primitiivinen juuri ja jos lasketaan lukuja a^k sekä niiden jakojäännöksiä luvulla m niin tulokset muodostavat ketjun joka käy läpi kaikki luvut b toistaen tätä samaa järjestystä. Koska $x^0=1$ niin jokainen ketju alkaa luvulla 1. Ketjun pituus siis löydetään kun havaitaan pienin nollasta poikkeava potenssi k jolla pätee $a^k\equiv 1 \pmod{m}$. Primitiiviset juuret ovat siis tämänlaisia rakenteita jollain modulolla m. Tarkastellaan muutamaa esimerkkiä. Valitaan nyt luvuksi $a=5$. Tarkastellaan luvun 5 potenssien kongruenssia moduloilla 9 ja 7.

$$Tapaus\ p=9$$

$$5^0\equiv 1 \pmod{9}$$
$$5^1\equiv 5 \pmod{9}$$
$$5^2\equiv 7 \pmod{9}$$
$$5^3\equiv 8 \pmod{9}$$

$$5^4 \equiv 4 \pmod 9$$
$$5^5 \equiv 2 \pmod 9$$
$$5^6 \equiv 1 \pmod 9$$
$$5^7 \equiv 5 \pmod 9$$
$$\vdots$$

$$Tapaus\ p = 7$$
$$5^0 \equiv 1 \pmod 7$$
$$5^1 \equiv 5 \pmod 7$$
$$5^2 \equiv 4 \pmod 7$$
$$5^3 \equiv 6 \pmod 7$$
$$5^4 \equiv 2 \pmod 7$$
$$5^5 \equiv 3 \pmod 7$$
$$5^6 \equiv 1 \pmod 7$$
$$5^7 \equiv 5 \pmod 7$$
$$\vdots$$

Luvun 5 korkeampien potenssien jakojäännösten tarkastelu voi olla työlästä jos ei ole käytössä laskinohjelmaa joka laskee erikseen jakojäännöksiä. Jos sellaista ei ole käytettävissä niin suositeltava strategia on laske potenssin tulos ja redusoida se edellisten tulosten kanssa. Esimerkiksi tapauksessa $p = 7$ kun ollaan jo selvitetty että $5^2 \equiv 4 \pmod 7$ niin tapauksessa 5^3 voidaan hyödyntää tietoa $5^3 = 5^2 \cdot 5$ on kongruenttia $4 \cdot 5 = 20 \equiv 6 \pmod 7$. Edeltävää logiikkaa toistamalla isojenkin potenssien jakojäännöksen laskeminen on helppoa.

Selkeästi molemmissa tapauksissa jäännösluokat käyvät läpi jotakin kuviota kun luvun a potensseja kasvatetaan aina yhdellä. Lisäksi jäännösluokkien lukumäärä on enintään $p-1$. Nyt mielekäs tutkittava asia on se, että voimmeko johtaa jotain säännönmukaisuuksia yleisesti luvuilla a ja p. Määritellään apufunktio tämänlaista tarkastelua varten.

Määritelmä 3.7. Olkoot $m \geq 2$ ja $syt(a, m) = 1$. Tällöin $ord_m(a)$ on pienin positiivinen eksponentti $t \geq 1$ siten että $a^t \equiv 1 \pmod m$. Tällöin sanomme että t on luvun a kertaluku moduloa m.

[3]

Tämä funktio on hyvin määritelty sillä ainakin **lauseen 2.58.** mukaan $a^{\phi(m)} \equiv 1 \pmod{m}$. Nyt jos tarkastellaan edellä käsiteltyjä potenssien sarjoja niin tällöin $ord_7(5) = 6$ ja $ord_9(5) = 6$.

Lause 3.8. *Olkoot* $syt(a, m) = 1$ *ja* $m \geq 2$. *Olkoot* $t = ord_m(a)$.

i) Mille tahansa eksponentille $n \geq 0$ *on voimassa :* $a^n \equiv 1 \pmod{m} \iff t \mid n$.

ii) $t \mid \phi(m)$. *Jolloin erityisesti* $1 \leq t \leq \phi(m)$.

iii) Olkoot $n_1, n_2 \geq 0$. *Silloin* $a^{n_1} \equiv a^{n_2} \pmod{m} \iff t \mid (n_1 - n_2)$.

iv) Jos $n \geq 1$, *niin* $ord_m(a^n) = \frac{t}{syt(n,t)}$.

Todistus. i) Kirjoitetaan n muodossa $n = k \cdot t + r$ jossa $0 \leq r \leq t - 1$. Oletetaan lisäksi että $a^n \equiv 1 \pmod{m}$. Nyt saadaan että

$$1 \equiv a^n \equiv a^{t \cdot k} \cdot a^n \equiv 1^k \cdot a^r \equiv a^r \pmod{m}.$$

Nyt **määritelmän 3.7.** ja oletuksen $0 \leq r \leq t - 1$ mukaan $r = 0$.Tämä seuraa siitä, jos $r \neq 0$ niin silloin $r = t$ mikä olisi ristiriita. Siispä $n = k \cdot t$ jolloin $t \mid n$.

ii) **Lauseen 2.58.** mukaan $a^{\phi(m)} \equiv 1 \pmod{m}$ jolloin kohta *ii)* seuraa suoraan kohdasta *i)*.

iii) Olkoot $n_1, n_2 \geq 0$ ja $a^{n_1} \equiv a^{n_2} \pmod{m}$. Nyt koska $syt(a^{n_2}, m) = 1$ niin yhtälö voidaan jakaa puolittain luvulla a^{n_2} ja saadaan tämän kanssa ekvivalentti kongruenssiyhtälö $a^{n_1 - n_2} \equiv 1 \pmod{m}$. Nyt kohdan *i)* mukaan tämä on ekvivalenttia sen kanssa että $t \mid (n_1 - n_2)$.

iv) Olkoot $s = ord_m(a^n)$, $d = syt(n, t)$, $n = d \cdot n'$ ja $t = d \cdot t'$. Nyt

$$(a^n)^t \equiv a^{d \cdot n' \cdot t'} \equiv (a^t)^{n'} \equiv 1^{n'} \equiv 1 \pmod{m}.$$

Tällöin **määritelmästä 3.7.** seuraa että $s \leq t'$. Nyt koska $a^n \cdot s \equiv (a^n)^s \equiv 1 \pmod{m}$ niin kohdan *i)* mukaan $t \mid n \cdot s$. Olkoot $n \cdot s = t \cdot k$ jollakin positiivisella kokonaisluvulla k. Tällöin

$$n \cdot s = t \cdot k \iff n' \cdot d \cdot s = t' \cdot d \cdot k \iff n' \cdot s = t' \cdot k.$$

Nyt, koska $d = syt(n,t)$ niin välttämättä pätee, että $syt(n^{'}, t^{'}) = 1$. Nyt, koska $t^{'} \mid n^{'} \cdot s$ niin pätee että $t^{'} \mid s$. Tästä seuraa, että $s \geq t^{'}$. Nyt, koska $s \geq t^{'}$ ja $s \leq t^{'}$ niin $s = t^{'}$ jolloin $t = d \cdot t^{'}$ saadaan että $t = syt(n,t) \cdot s \Longleftrightarrow s = ord_m(a^n) = \frac{t}{syt(n,t)}$.

[3] □

Nyt voimmekin antaa määritelmän primitiivisille juurille. Tämän lisäksi voimme antaa määritelmän kanssa ekvivalentteja väitteitä jotka myös riittävät näyttämään että jokin luku a on primitiivinen juuri modulo m.

Määritelmä 3.9. Kokonaisluku a on primitiivinen juuri modulo m jos $syt(a,m) = 1$ ja $ord_m(a) = \phi(m)$ missä ord on **määritelmän 3.9.** funktio ja ϕ on Eulerin totienttifunktio.

[3]

Lause 3.10. *Luku a on primitiivinen juuri modulo m jos ja vain jos $\{1, a, a^2, ..., a^{p-2}\}$ on vähennetty jäännösluokkasysteemi modulo m jos ja vain jos*

$$\mathbb{Z}_p^* = \{\overline{a}^k \mid \quad k = 0, 1, 2, ..., p-2\}.$$

Todistus. Ekvivalenssit seuraavat suoraan **määritelmästä 3.9.** ja **määritelmästä 2.55.** eikä niitä käydä tässä läpi sen tarkemmin.

[3] □

Lemma 3.11. *Olkoot $p \in \mathbb{P}$ ja $t \geq 1$. Tällöin:*

i) jos $t \nmid (p-1)$ niin $ord_p(a) \neq t$ kaikilla $a \in \mathbb{Z}$,

ii) jos $t \mid (p-1)$ niin silloin on olemassa 0 tai $\phi(t)$ kappaletta eri lukuja a $(mod\ p)$ joilla $ord_p(a) = t$ on totta.

Todistus. Kohta i): tehdään vastaoletus ja oletetaan että $ord_m(a) = t$. Nyt Eulerin totienttifunktion määritelmän mukaisesti $\phi(p) = p - 1$. Tällöin **lauseen 3.8.** kohdan *ii)* mukaan $t \mid (p-1)$. Tämä on kuitenkin ristiriidassa oletuksen kanssa joten $ord_m(a) \neq t$.

Kohta ii): jos $t = ord_p(a) = 1$ niin ord funktion määritelmän mukaan $a \equiv 1 \pmod p$ jolloin a kuuluu uniikkiin jäännösluokkaan modulo p. Voimme siis olettaa että $t \geq 2$ ja $t \mid (p-1)$. Oletetaan lisäksi että on olemassa a jolla $syt(a,p) = 1$ ja $ord_p(a) = t$. Tällöin **lauseen 3.10.** ja **lauseen 3.8.** kohdan *iii)* mukaan luvut $1, a, a^2, ..., a^{t-1}$ ovat keskenään ei kongruentteja modulo p. Lisäksi jokainen niistä ratkaisee kongruenssin $x^t \equiv 1 \pmod p$

koska $a^{j \cdot t} \equiv (a^t)^j \equiv i^j \equiv 1 \pmod{p}$ kun $j = 0, 1, 2, ...$ Tällöin **lause 3.1.** implikoi että kyseiset luvut sisältävät kaikki ratkaisut edelliseen yhtälöon moduloa p. Siispä kaikki sellaiset x jotka ratkaisevat yhtälön $ord_p(x) = t$ ovat lukujen $1, a, a^2, ..., a^{t-1}$ joukossa. Nyt **lauseen 3.8.** kohdan *iv)* mukaan $ord_p(a^s) = \frac{t}{syt(t,j)}$. Siispä $ord_p(a^j) = t$ pätee vain jos $syt(t, j) = 1$. Nyt, koska eksponenttien $0, 1, 2, ..., t-1$ joukossa on täsmälleen $\phi(t)$ kappaletta sellaisia eksponentteja joilla $syt(t, j) = 1$ niin tämä todistaa väitteen.

[3] □

Lause 3.12. *Olkoot $p \in \mathbb{P}$ ja olkoot luku $t \geq 1$ sellainen että $t \mid (p-1)$. Silloin*

$$\#\{n \in \{1, 2, ..., p-1\} : ord_p(n) = t\} = \phi(t).$$

Merkintä # tarkoittaa merkin jälkeen tulevan joukon alkioiden lukumäärää. Erityisesti tämä lause tarkoittaa että kaikilla alkuluvuilla on primitiivisiä juuria $\phi(p-1)$ kappaletta.

Todistus. Olkoot nyt $p \in \mathbb{P}$, $t \geq 1$, $t \mid (p-1)$ ja

$$\Phi(t) = \#\{n \in \{1, 2, ..., p-1\} : ord_p(n) = t\}.$$

Nyt selkeästi $1 \mid (p-1)$ ja $1^1 \equiv 1 \pmod{p}$. Siispä selkeästi kaikilla $p \in \mathbb{P}$ pätee, että $\Phi(t) \neq 0$. Nyt **lemman 3.11.** kohdan *ii)* mukaan siis $\Phi(t) = \phi(t)$.

□

Korollaari 3.13. *Jos $p \in \mathbb{P}$ niin $\mathbb{Z}_p^*$ on syklinen eli se on yhden alkion virittämä.*

Todistus. Olkoot a primitiivinen juuri modulo p. Edellisen lauseen mukaan tällainen on aina olemassa. Nyt **lauseen 3.10.** mukaan $\mathbb{Z}_p^* = \{\overline{1}, \overline{a}, \overline{a^2}, ..., \overline{a^{p-2}}\}$.

[3] □

Lause 3.14. *Z_m^* on jaksollinen täsmälleen silloin kun $m = 2$, $m = 4$, $m = p^e$ tai $m = 2 \cdot p^e$, missä $p \in \mathbb{P}$ ja $e \geq 1$.*

Todistus. **Korollaarista 3.13.** nähdään että kun puhutaan Z_m^* jaksollisuudesta niin puhutaan että millä luvuilla m on primitiivisiä juuria. Tarvitsemme muutaman identiteetin tämän näyttämiseksi. Olkoot $t \geq 1$ ja $a \equiv b \pmod{p_1^t}$ jossa $p_1 \in \mathbb{P}$. Tällöin siis $a = b + c \cdot p_1^t$. Nyt binomilauseen mukaan $a^p = b^p + \frac{p!}{(p-1)!} \cdot b^{p-1} \cdot c \cdot p^t + A$ missä on kokonaisluku mikä on jaollinen luvulla p^{t+2}. Lisäksi

$$\frac{p!}{(p-1)!} \cdot b^{p-1} \cdot c \cdot p^t = \frac{(p-1)!}{(p-1)!} \cdot b^{p-1} \cdot c \cdot p^t \cdot p = \frac{(p-1)!}{(p-1)!} \cdot b^{p-1} \cdot c \cdot p^{t+1}$$

eli lausekkeen toinen termi on jaollinen luvulla p^{t+1}. Lisäksi $A = k \cdot p^{t+2} = k \cdot p \cdot p^{p+1}$. Siispä kongruenssin määritelmän mukaan $a^p \equiv b^p \pmod{p^{p+1}}$. Olkoon tämä ominaisuus i).

Tarkastellaan nyt primitiivisiä juuria kun $m = 2^s$. Väitämme että kun $s = 1$ tai $s = 2$ niin primitiivisiä juuria on ja kun $s \geq 3$ niin niitä ei ole. Lisäksi jos $s \geq 3$ niin silloin joukko $\{(-1)^a \cdot 5^b \mid a = 0 \; tai \; a = 1 \; ja \; 0 \leq b < 2^{s-2}\}$ on vähennetty jäännösluokka systeemi modulo 2^s. Tällöin kun $s \geq 3$ niin kyseessä on kahden jaksollisen ryhmän tulo joiden kertaluvut ovat 2 ja 2^{s-2}. Koska niiden kertaluvuilla on yhteinen tekijä 2 niin niiden tulo ei ole jaksollinen ryhmä eli tapauksissa $s \geq 3$ ei ole primitiivisiä juuria.

Nyt 1 on primitiivinen juuri modulo 2 ja 3 on primitiivinen juuri modulo 2^2 eli tapauksissa $s = 1$ ja $s = 2$ on primitiivisiä juuria. Olkoot nyt $s \geq 3$. Nyt väitämme että $5^{2^{s-3}} \equiv 1 + 2^{s-1} \pmod{2^s}$. Tämä on tosi kun $s = 3$ sillä silloin se saa muodon $5^1 \equiv 5 \pmod{8}$ mikä on tosi. Näytetään nyt että kongruenssi pätee kun $s \geq 3$. Ensimmäiseksi huomaamme että $(1 + 2^{s-1})^2 = 1 + 2^s + 2^{2 \cdot s-2}$ ja että $2 \cdot s - 2 \geq s + 1$ kaikilla $s \geq 3$. Käyttämällä nyt ominaisuutta i) edelliseen kongruenssiimme saamme että $5^{2^{s-2}} \equiv 1 + 2^s \pmod{2^{s+1}}$. Nyt väite seuraa induktiosta eli luvuilla $m = 2^s$ ei ole primitiivisiä juuria kun $s \geq 3$.

Lauseen 3.12. modulolla $p \in \mathbb{P}$ on primitiivisiä juuria. Tarkastellaan nyt kuitenkin alkulukua $p \neq 2$. Jos $g \in \mathbb{Z}$ on primitiivinen juuri moduloa p niin silloin myös $g + p$ on primitiivinen juuri. Jos $g^{p-1} \equiv 1 \pmod{p^2}$ niin $(g+p)^{p-1} \equiv g^{p-1} + (p-1) \cdot g^{p-2} \cdot p \equiv 1 + (p-1) \cdot g^{p-2} \cdot p \pmod{p^2}$. Koska $p^2 \mid ((p-1) \cdot (g^{p-2} \cdot p))$ niin voimme olettaa että g on primitiivinen juuri modulo p ja että $g^{p-1} \not\equiv 1 \pmod{p^2}$. Väitämme nyt että tällainen g on primitiivinen juuri modulo p^e. Tämän osoittamiseksi riittää osoittaa että jos $g^n \equiv 1 \pmod{p^e}$ niin $\phi(p^e) = p^{e-1} \cdot (p-1) \mid n$. Nyt $g^{p-1} = 1 + a \cdot p$ jossa $p \nmid a$. Nyt ominaisuuden i) ja lähdemateriaalin **korollaarin 2** mukaan $ord_{p^e}(1 + a \cdot p) = p^{e-1}$. Nyt koska $(1 + a \cdot p)^n \equiv 1 \pmod{p^e}$ niin $p^{e-1} \mid n$. Kirjoitetaan nyt $n = p^{e-1} \cdot n'$. Tällöin $g^n = (g^{p^{e-1}})^{n'} \equiv g^{n'} \pmod{p}$ jolloin $g^{n'} \equiv 1 \pmod{p}$. Nyt koska g on primitiivinen juuri modulo p niin $(p-1) \mid n'$ eli $p^{e-1} \cdot (p-1) \mid n$ mikä oli todistettava. Siispä primitiivisiä juuria on kun $m = p^e$.

Kaikki luvut muotoa $m = 2^s$ ja $m = p^e$ on jo käsitelty eli oletetaan että $m \neq 2^s$ ja $m \neq p^e$, $s \geq 3$. Kirjoitetaan nyt $m = m_1 \cdot m_2$ joilla $syt(m_1, m_2) = 1$ ja $m_1, m_2 > 2$. Tällöin $\phi(m_1)$ ja $\phi(m_2)$ ovat parillisia ja $\mathbb{Z}'_m$ on isomorfinen ryhmien $\mathbb{Z}^*_{m_1}$ ja $\mathbb{Z}^*_{m_2}$ tulon kanssa. Nyt

molemmilla tekijäjoukoista on alkioita joiden potenssin kasvattaminen kahdella tuottaa neutraalialkion. Tästä seuraa että $\mathbb{Z}_m^*$ ei ole syklinen sillä syklisessä ryhmässä voi olla vain yksi alkio jolle tämä pätee.

Nyt ollaan näytetty että luvut mitkä ovat muotoa 2, 4 ja p^e omaavat primitiivisiä juuria ja että luvuilla 2^s kun $s \geq 3$ ja keskenään eri alkuluvuista muodostetuilla tuloilla ei ole primitiivisiä juuria. Nyt $\mathbb{Z}_{2 \cdot p^e}$ on isomorfinen $\mathbb{Z}_2^*$ ja $\mathbb{Z}_{p^e}^*$ tulon kanssa joka on isomorfinen $\mathbb{Z}_{p^e}^*$ kanssa. Tästä seuraa, että $\mathbb{Z}_{2 \cdot p^e}$ on syklinen eli $m = 2 \cdot p^e$ omaa primitiivisiä juuria.

[2] □

Esimerkki 3.15. Esimerkiksi modulolla $m = 2 \cdot 5 = 10$ on primitiivisiä juuria. Nyt joukossa $\{\mathbb{Z}_{10}^*\}$ on alkioita $\phi(10) = 4$ kappaletta. Kyseiset alkiot ovat jäännösluokat $\{1, 3, 7, 9\}$. Kun käydään lävitse näitten lukujen potensseja a, a^2, a^3 jne. niin kun kyseisen luvun järjestys on 4 niin kyseessä on primitiivinen juuri moduloa 10. Luvun 1 kaikkien potenssien jäännösluokka on 1. Luvulla 3 ne ovat 3, 9, 7, 1 eli luvun 3 järjestys on 4 eli se on primitiivinen juuri moduloa 10. Vastaavasti luvulle 7 jakojäännökset ovat 7, 9, 3, 1 jne. Ja lopuksi luvulle 9 ne ovat 9, 1, 9 jne. Siispä myös 7 on primitiivinen juuri moduloa 10 mutta luku 9 ei. Moduloilla voi olla useita primitiivisiä juuria ja **lause 3.14.** lähinnä kertoo millä moduloilla on ainakin yksi primitiivinen juuri.

Luku 4

Diffie-Hellman avaintenvaihtoprotokolla

Nyt tutkielmassa on käyty läpi primitiiviset juuret, mutta entä mitä niillä voi tehdä? Koska tutkielman tavoite on myös esittää primitiivisten juurten lukiossa opettamisen suunnitelma niin kyseiselle hypoteettiselle kurssille tulisi tuoda mukaan käytännön sovelluksena Diffie-Hellman avaintenvaihtoprotokolla. Tässä luvussa esitellään miten Diffie-Hellman toimii käyttämällä primitiivisiä juuria. Lisäksi koska Diffie-Hellman on helppo murtaa niin se, miten se murretaan, esitellään myös. Diffie-Hellman oli ensimmäinen julkisen avaimen salaus. Diffie-Hellman-avaintenvaihtoprotokollassa kaksi henkilöä voivat kommunikoida julkisessa viestinvälitysverkostossa. Henkilöillä on julkinen salausavain, mikä on kaikkien tiedossa ja he luovat yhteisen salaisen avaimen lähettämällä toisilleen tiedot joilla se ratkeaa heille. Salauksen heikkous on se, että siinä ei varmisteta viestin lähettäjän henkilöllisyyttä joten jos joku on henkilöiden viestinnän välissä, niin hän pystyy selvittämään itselleen yhteisen sovitun avaimen ja sitä kautta tarkastelemaan viestiliikennettä. Siitä huolimatta useat HTTPS sivustot sallivat Diffie-Hellmanin käytön salauksena.

Käydään nyt tarkasti läpi vaihe vaiheelta miten Diffie-Hellman toimii. Tiivistettynä Diffie-Hellman käyttää syklisiä ryhmiä moduloa p jossa $p \in \mathbb{P}$ ja ryhmän alkio g on primitiivinen juuri modulo p. Henkilöt valitsevat siis modulon p ja jonkin sen primitiivistä juurista g. Tällöin salainen luku voi olla mikä tahansa positiivinen kokonaisluku joka on pienempi kuin p. On siis erittäin tärkeää valita todella suuri p. Meillä on nyt kaksi henkilöä: Pirita ja Lili.

1. Pirita ja Lili valitsevat modulokseen alkuluvun $p = 31$ ja primitiiviseksi juurekseen luvun $t = 3$. Näitä lukuja ei tarvitse pitää salassa.

2. Pirita valitsee salaisen kokonaisluvun $a = 12$ ja lähettää Lilille luvun x jolle pätee $t^a \equiv x \pmod{31}$ eli jaetaan luku t^a luvulla p ja lähetetään jakojäännös vastapuolelle. Valituilla luvuilla siis $3^{12} \equiv x \pmod{31} \iff x = 8$.

3. Vastaavasti Lili valitsee salaisena pidettävän kokonaisluvun $b = 7$ ja lähettää Piritalle luvun y jolla $t^b \equiv y \pmod{p}$ eli nyt $3^7 \equiv y \pmod{31} \iff y = 17$.

4. Nyt Pirita voi laskea itselleen luvun z jolle pätee $y^a \equiv z \pmod{p}$ eli tässä tapauksessa $17^{12} \equiv z \pmod{31} \iff z = 2$.

5. Vastaavasti Lili laskee luvun v jolle pätee että $x^b \equiv v \pmod{p}$ eli tässä tapauksessa $8^7 \equiv v \pmod{31} \iff v = 2$.

Pirita ja Lili ovat nyt onnistuneesti luoneet salaisen avaimen 2 jota he voivat käyttää salauksen purkukoodina johonkin muuhun viestinsalausmetodiin joka ratkeaa jollakin avaimella. Olennaista on pitää luonnollisesti salausavain 2 salaisena, mutta Piritan ja Lilin on myös pidettävä salassa valitsemansa luvut a ja b koska lähetettyjen viestien perusteella salausavain voidaan selvittää jos tiedetään luvut a ja b. Todellisessa tilanteessa tulisi tietysti valita riittävän suuret luvut a, b ja p. Tämä johtuu siitä että tunnetuista luvuista p, a, b, x ja z voidaan ratkaista avain $z = v$. Se kuinka kauan algoritmilla kestää ratkaista riippuu siitä kuinka isot luvut valitaan. Lukujen a ja b suurudella ei ole merkitystä ratkaisunopeuden kannalta. Salauksen käyttäjän siis olisi hyvä tuntea tehokkain lukujen selvitysalgoritmi ja valita sopivat luvut jotta sillä kyseisellä algoritmilla kestää suojauksen murtamisessa mahdollisimman kauan aikaa. Myöskään luvun t suuruudella ei ole olennaista merkitystä avaimen ratkaisemisen nopeuden kannalta.

Kuten edellä mainittiin niin esitellään myös se kuinka salaus voidaan päihittää. Esitämme yhden algoritmin jolla salaus voidaan purkaa. Jos ajatellaan salauksen purkua hyökkääjän näkökulmasta, niin hänen täytyy ratkaista yhtälö joka on muotoa: $x^b \equiv v \pmod{p}$. Tämä yhtälö on diskreettinen logaritmi ongelma ja valitsemalla riittävän ison luvut salaajat voivat tehdä viestin purkamisesta työlästä koska diskreettien logaritmien ratkaisemiseksi ei ole keksitty kovin tehokkaita algoritmeja. Salauksen suurin heikkous on kuitenkin se että viestin lähettäjää ei varmenneta. Tämä mahdollistaa niin sanotun mies välissä hyökkäyksen tehokkaan toimivuuden. Mies välissä hyökkäyksessä salattu viesti siepataan viestittelijöiden välissä. Siis tilanteessa jossa Pirita ja Lili lähettävät toisilleen ensimmäiset viestinsä, joku voi saada Piritan ja Lilin viestit. Vastaamalla Piritalle ja Lilille protokollan mukaisesti hyökkääjä voi muodostaa salaisen yhteyden kumpaankin Liliin ja Piritaan heidän tietämättään. Tässä tapauksessa hyökkääjä kykenee esiintymään viestitteleville osapuolille vastakkaisena osapuolena. Esitellään tämä vielä tarkasti. Olkoon meillä nyt Petteri joka haluaa selvittää Piritan ja Lilin viestittelyn. Tällöin Petterin pitää kaapata Piritan ja Lilin viestit ja toimia seuraavanlaisesti.

1. Petteri valitsee omat 2 salassa pidettävää lukua $d_1 = 4$ ja $d_2 = 7$. Petteri generoi Diffie-Hellman avaintenvaihtoprotokollan mukaisesti luvut x_p ja y_p.

2. Petterin pitää kaapata Piritan ja Lilin toisilleen lähettämät luvut y ja x. Tässä yhteydessä Petteri voi Diffie-Hellmanin kohdan 4 ja 5 mukaisesti generoida avaimet jolla kommunikoida Piritan ja Lilin kanssa.

3. Petterin pitää vielä lähettää Piritalle ja Lilille omat generoimansa luvut x_p ja y_p joista Pirita ja Lili generoivat omat avaimensa jotka Diffie-Hellmanin mukaisesti ovat samat mitkä Petteri generoi kohdassa 2. [4]

Nyt Piritan ja Lilin näkökulmasta he loivat toisilleen avaimet salaiseen keskusteluun jota ei voi murtaa kovin helposti, mutta todellisuudessa kummatkin heistä loivat erillisen avaimen Petterin kanssa keskustelemiseen. Nyt Petteri voi seurata kaikkea salaista keskustelua mitä Pirita ja Lili lähettelevät toisilleen. Kaikki tämä tietysti edellyttää että Petteri saa Piritan ja Lilin viestit haltuunsa ennen kuin ne saavuttavat määränpäätänsä.

Diffie-Hellman avaintenvaihtoprotokollaa käytettäessä on tarpeellista pystyä laskemaan melko suurien potenssien jakojäännöksiä tietyllä modulolla. Kun tietokoneet laskevat näitä lukuja niin yksi olennainen seikka on se kuinka monta laskutoimitusta tietokone tekee. Square and multiply algoritmi toimii siten että aluksi muutetaan potenssi binääriseksi eli kaksikantaiseen lukukantaan. Ensimmäisen binääriluvussa esiintyvän 1 kohdalla listataan kantalukumme. Jokaisesta 0 joka tulee tämän jälkeen korotetaan kantaluku potenssiin 2. Jokaisesta 1 joka ensimmäisen 1 jälkeen luku korotetaan potenssiin 2 ja kerrotaan kantaluvulla.

Jos noudattaa potenssien laskukaavaa suoraan niin esimerkiksi laskettaessa lukua 2^7 toteutetaan laskutoimitukset $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$. Tässä on yhteensä 9 laskutoimitusta. Kokeillaan nyt square and multiply algoritmilla. Luku 9 on binäärisenä 1001. Joten ensimmäisen 1 kohdalla listataan kantaluku 2. Tämän jälkeen tulee nolla eli korotetaan potenssiin 2 eli $(2)^2$. Tämän jälkeen tulee 0 eli taas korotetaan potenssiin 2 eli $((2)^2)^2$. Viimeinen luku on 1 eli korotetaan potenssiin 2 ja kerrotaan kantaluvulla eli aluksi $(((2)^2)^2)^2$ ja sitten $((((2)^2)^2)^2) \cdot 2$. Tällöin laskuvaiheita oli 4. Eli tällä algoritmilla laskeminen oli tässä tapauksessa hieman yli 50 prosenttia tehokkaampaa. Tehokkuus korostuu todella suurissa potensseissa vielä enemmän. Esimerkiksi potenssiin miljoona tilanteessa säästyy 999975 laskuvaihetta eli on jo lähes 100 prosenttia tehokkaampaa vaikkakin potensiin miljoona on jo tarpeettoman iso luku. Tietysti teoriassa tähän pitää lisätä ne vaiheet jotka tarvitaan luvun muuttamiseen binääriseksi mutta tämän algoritmin käyttäminen suurilla luvuilla on tehokkaampaa.

Binäärisestä luvusta voidaan laskea laskuvaiheiden määrä laskemalla ensimmäisen ykkösen jälkeisten nollien ja ykkösten määrät. Jokaista nollaa vastaa yksi laskutoimitus ja jokaista ykköstä vastaa 2 laskutoimitusta. Jos binääriluku on pitkähkö niin voi olla hyödyllistä pyrkiä etsimään sellainen jossa on vain muutama ykkönen. Tämä nopeuttaa luvun

merkintää jos square and multiply algoritmia käyttää manuaalisesti. Olisi todella suotavaa jos kurssin materiaalissa näkyisi square and multiply algoritmin koodi vaikka opettaja tai opiskelija voi hyvinkin hakea sitä myös esimerkiksi googlesta. En usko että kurssilla riittää aikaa square and multiply algoritmin koodaamiseen.

Nyt ollaan esitelty primitiiviset ja juuret ja Diffie-Hellman avaintenvaihtoprotokolla. Seuraavaksi tutkielmassa pyritään analysoimaan näiden asiasisältöjen opettamista lukion viitekehyksessä ja tuottamaan tarpeeksi tarkan kurssisuunnitelman jotta tämän tutkielman lukeva voi sen toteuttaa. Vaikkakin primitiiviset juuret ovat kyseisen hypoteettisen kurssin pääaihe niin Diffie-Hellman-avaintenvaihtoprotokolla luo siihen hyvin mielekkyyttä opiskelijoille primitiivisten juurten sovelluksena. Primitiiviset juuret itsessään voivat olla yliopistoon matematiikka pääaineenaan tähtäävälle jo tarpeeksi mielekästä puuhaa, mutta erityisesti tietojenkäsittelytieteistä ja erityisesti kryptografiasta kiinnostuneelle Diffie-Hellman on kiinnostavinta.

Luku 5

Primitiivisten juurten opettaminen lukiossa

Tässä luvussa tutkitaan miten primitiivisten juurten opetus sopisi lukioympäristöön. Tavoitteena on myös tuottaa kurssisuunnitelma sellaiselle kurssille jonka keskeinen aihe on primitiiviset juuret, mutta se tehdään vasta kappaleessa 6. Materiaalia missä primitiiviset juuret on esitetty lukiotasolle tarkoitettuna on erittäin niukasti jos ollenkaan. Tästä syystä joudumme kehittämään toisen keinon analysoidaksemme sen lukioon soveltumista.

Koska kyseessä on yliopistomatematiikan aihe mikä muunnellaan sopivaksi lukion opetukseen niin otamme mallia toisesta aiheesta joka on tyypillinen yliopiston opetuksessa. Analyysistä on paljon lukio-opetukseen suunnattua materiaalia koska nykyisin MAA 13 kurssi eli differentiaali- ja integraalilaskennan jatkokurssi käsittelee yliopiston analyysin kursseilla käytäviä aiheita. Tarkoituksemme on analysoida lukiopuolen ja yliopistopuolen analyysin opetuksen eroja ja näiden eroavaisuuksien pohjalta johtaa se, miten itse lähestyisimme primitiivisten juurten opettamista. Tämän lisäksi tuottamamme kurssin tulisi mukailla lukion opetussuunnitelman matematiikan oppiaineen yleisiä tavoitteita.

Matematiikkalehti Solmussa on Jukka Pihkon kirjoittama artikkeli jossa hän esittelee toteuttamansa kurssin "Lukuteorian helmiä lukiolaisille". Tämä artikkeli sisältää Pihkon käyttämän kurssimateriaalin. Pihko noudattaa paljon yliopistokurssille tyypillisempää lähestymistapaa eli hän rakentaa matemaattisen tekstin jossa edetään määritelmillä, lauseilla, niiden todistuksilla ja seuraamuksilla. Tekstistä löytyy myös esimerkkejä. Vaikka pyrimmekin analysoimaan analyysin kohdalta nimen omaan lukio-opetuksen ja yliopisto-opetuksen eroavaisuuksia niin joudumme myös pohtimaan, että onko enemmän lukio-opetuksen näköinen kokonaisuus mielestämme parempi kuin Pihkon enemmän yliopistomatematiikalta näyttävä tyyli. Tämä tietysti riippuu vahvasti myös opetettavasta

asiasta ja siitä kuinka suuret valmiudet lukion pakolliset kurssit käyneeltä on ymmärtää kurssin sisällöt.

5.0.1 Lukiokurssin ja yliopistokurssin eroavaisuudet

Tarkastellaan aluksi eroavaisuuksia. Lukion opetusta edustavana materiaalina käytetään Sanoma pro MAA13 kirjaa joka noudattaa lukion vuoden 2003 opetussuunnitelmaa. Kyseistä opetussuunnitelmaa käytettiin vuoteen 2015 asti ja sen jälkeisissä opetussuunnitelmissa kysein kurssin keskeiset sisällöt ovat vain hieman kasvaneet mutta kokonaissisältö analyysiin liittyvistä aiheista ei ole juurikaan muuttunut joten tämä vuoden 2013 painos antaa mielestäni ihan hyvän kuvan kyseisen aiheen opetuksesta lukiossa. Helsingin yliopistossa analyysin kursseilla eli kursseilla: Raja-arvot, Differentiaalilaskenta, Integraalilaskenta ja Sarjat käytetään oppikirjana teosta "Analyysia reaaliluvuilla". Vertaillaan siis Sanoma pron MAA13 kurssin kirjan sisältöjä siihen, miten samat asiat esitellään kirjassa "Analyysia reaaliluvuilla" ja pyritään johtamaan samalla tavalla tässä tutkielmassa esitetystä materiaalista sopiva kokonaisuus josta saadaan aikaiseksi lukiokurssi primitiivisistä juurista.

Tarkastellaan aluksi yleistä tyylieroa lukion oppimateriaalissa ja yliopiston oppimateriaalissa. Yliopistossa matematiikan kursseissa oppimateriaali on tyypillisesti hyvin saman näköinen kuin matemaattinen osuus tässä tutkielmassa. Yliopiston oppimateriaalissa on toki enemmän esimerkkejä mikä on nähtävissä esimerkiksi lukuteorian luentomuistiinpanoissa mitä käytimme lähdemateriaalina matematiikkaosiossa. MAA13 kirjassa sanotaan lukujen lähtevän liikkeelle aihepiiriin johdattelevalla ongelmalla tai esimerkillä. Opetettavaan aiheeseen liittyvä uusi tieto kootaan ja perustellaan ja lisäesimerkit opastavat tiedon hyödyntämiseen ja syventämiseen. Olennaisina eroavaisuuksina ovat esimerkkien sijainti ja niiden määrä. Lukioon suunnatussa tekstissä esimerkit ovat ensisijaisesti se mistä lähdetään liikkeelle. Toki näin tehdään esimerkiksi luentokalvoissa primitiivisten juurten kappaleen alussa mutta suurimmilta osin yliopiston puolella useammin aloitetaan määritelmästä ja lähdetään rakentamaan siitä lauseita ja niiden todistuksia. Lisäksi opetettavaan asiaan littyvissä määritelmissä, lauseissa, korollaareissa, lemmoissa ja esimerkeissä kokonaisuutena on tyypillisesti lukion oppikirjassamme reilusti yli puolet opetusmateriaalista esimerkkejä ja niiden ratkaisuja kun taas yliopistokirjassamme toisin päin eli yli puolet numeroiduista kohdista jotain muuta kuin esimerkkejä. Kun muodostamme omaa kurssisuunnitelmaamme primitiivisten juurien opetukseen meidän pitäisi huolehtia tämän perusteella esimerkkien paljoudesta ja siitä että ne tukevat opetettavan aiheen ymmärtämistä mahdollisimman hyvin.

Vertaillaan nyt itse aihesisältöjen opettamisen eroavaisuuksia lukion ja yliopiston op-

pikirjoissamme. Opetettavat asiat mitä vertailemme ovat Funktion raja-arvo, funktion jatkuvuus, derivaatta, epäoleellinen integraali ja lukujonon raja-arvo. Tarkastelemme kunkin aiheen kohdalta miten niiden esitys eroaa lukion ja yliopiston oppikirjoissa ja pohdimme mahdollisia syitä niihin eroihin. Tämän jälkeen koostamme olennaiset eroavaisuudet ja perustelemme niillä oman kurssikokonaisuutemme luomisessa tekemiämme valintoja.

Kun lukion oppikirjassa puhutaan raja-arvosta on vain kolme teoriaobjektia. Teoriaobjektilla tarkoitamme nyt lauseita, määritelmiä, itse asiassa kaikkea muuta kuin esimerkkejä. Lukion oppikirjassa on nyt määritelmä raja-arvolle, määritelmä toispuoleisille raja-arvoille ja lause joka kertoo niiden yhteyden. Ei pureuduta tarkemmin siihen vaan mitä eroavaisuuksia näiden esittämisellä on. Vastaavat teoriaobjektit löytyvät yliopiston oppikirjasta mutta ulkonäöllisesti niillä on suuria eroavaisuuksia. Yliopiston oppikirjassa näkyy epsilon-delta määritelmä kun taas lukion oppikirjassa epsilon-delta osuus on ikään kuin selitetty sanoin. Toispuoleisissa raja-arvoissa on sama ilmiö. Määritelmää on ikään kuin pelkistetty lukion oppikirjoissa, eli kaikki merkinnät joiden tulkinta on lukion oppimäärän yli tai oletetaan olevan ylimääräistä ovat sensuroitu pois. Kun toteutamme itse primitiivisille juurille kurssisuunnitelmaa luvussa 6 niin meidän tulee valita lauseistamme ne asiat jotka ovat mielekkäämpiä piilottaa kuin näyttää jotta kurssi ei olisi liian työläs tai sekava opiskelijalle.

Funktion jatkuvuudesta puhuttaessa on lukionkin oppikirjassa määritelmän lisäksi monia lauseita kuten Bolzanon lause, jatkuvan funktion väliarvolause ja suurimman ja pienimmän arvon olemassaololause. Määritelmissä ja lauseissakin pätee raja-arvoissakin havaittu pelkistys eli matemaattisen tekstin korvaaminen selkokielisellä selityksellä. Näistä lauseista kuitenkin vain väliarvolauseen todistamista pidetään lukion oppikirjassa toteutettavana ja se onkin harjoitustehtävänä. Kahdesta muusta lauseesta tosin todetaan, että niiden todistus menee kaikin muodoin yli lukiossa pidettävän kurssin vaatimusten. Näkökulma on kuitenkin sama kuin yliopistossa eli esitetyt lauseet pitää todistaa, mutta jos se ei ole mielekestä lukiokurssilla niin sitä tulee vähintäänkin kommentoida. Useat lukuteorian lauseet todistetaan vastaoletuksella joten niiden kanssa pitää pohtia, että voisiko lukiolainen keksiä miten ne tehdään jos esimerkiksi antaa vihjeitä maaliin pääsemiseksi. Suunnitelmamme kurssin tulisi myös identifioitua sen suhteen, että haluammeko sen olevan lukiomaisempi vai kuten matematiikkalehti solmussa ollut lukuteorian helmiä lukiolaisille kurssi missä oli yliopistomatematiikkaan valmentava sävy.

Derivaatan kohdalla kiinnitämme erityistä huomiota esittämisjärjestykseen. Lukion oppikirjassa annetaan aluksi "derivaatan kuvaileva määritelmä" käyrään asetettavien tangenttien kulmakertoimien avulla ja sen jälkeen tarkka määritelmä erotusosamäärän raja-arvona. Tangenttitulkinta annetaan yliopiston oppikirjassa vasta tarkan määritelmän jälkeen. Kummassakin kirjassa todetaan tangenttitulkinnan olevan kätevä asian ymmärtämisen kannalta mutta tässä näkyy painotusero. Kummankin kirjan kirjoittajilla on ollut

hieman eri näkemys siitä missä järjestyksessä nämä esitetään ja tässä kyseisessä tilanteessa vaikuttaisi olevan kyse teorian painottamisessa yliopistopuolella. Lukion oppikirjan alussa selitettiin että kirjassa edetään rakentamalla teoria esimerkkien ympärille joten sille on luonnollisempaa käydä tangenttianalogia ensin. Toisaalta kyseessä voi olla myöskin vain makuero kirjojen kirjoittajien välillä, mutta tämänlaisten valintojen hyödyllisyys opiskelijalle pitää ottaa huomioon kurssia suunnitellessa.

Epäoleellisessa integraalissa ja muissakin aiheissa mitä olemme vertailleet näkyy laajuusero. Lukiokurssi on tietysti asiasisällöltään suppeampi kuin yliopistokurssi, mutta useimmissa aiheissa näkyy se, että kun lukiokirjassa tuodaan määritelmä ja ehkä muutama tärkeä tulos aiheeseen liittyen, niin yliopistokirjassa jatketaan eteenpäin kaikenlaisilla seuraamuksilla ja tuloksilla. Lukiokurssi on tyypillisesti kuusi viikkoa ja joka viikolla kolme 75 minuutin oppituntia. Tämä luo aikarajan mikä tarkoittaa että tässä tutkielmassakin esiintyvästä materiasta osa täytyy "karsia" pois lopullisesta kurssisuunnitelmasta. Karsittavan materiaalin tulisi olla seuraamuksia jotka eivät ole olennaisia kurssin ydinsisällön kannalta. Muilta osin lukion oppikirjan epäoleellinen integraali muistuttaa muitten asioiden esitystä sievennetyllä muodollaan verrattuna yliopisto-oppikirjan asioihin.

Lukujonon raja-arvo esitellään lukion oppikirjassa vasta viimeisenä asiana ennen sarjoja, kaiken muun jälkeen. Yliopiston oppikirjassa lukujonojen raja-arvo on ensimmäinen asia mitä käsitellään kun puhutaan ollenkaan raja-arvosta. Derivaatan kohdalla kirjojen asioiden järjestysero oli spekuloitavissa enemmän makuasiaksi mutta näin iso eroavaisuus palvelee tarkkaan harkittua tarkoitusperää. Syy vaikuttaisi olevan juurikin siinä että määritelmiä on lukion oppikirjassa yksinkertaistettu. Sarja on konseptuaalisesti lähempänä lukujonoa kuin funktiota joten on järkevää esittää lukujonot ja sarjat peräkkäin lukion oppikirjassa. Syy miksi lukujonot esitetään heti aluksi yliopistopuolella vaikuttaa olevan se, että lukujonon raja-arvosta puhuttaessa käytetään epsilon määritelmää. Lukujonoista siirryttäessä funktioihin epsilonista siirrytään epsilon-deltaan. Epsilon-delta määritelmä on helpompi ymmärtää jos asia on jo järkeilty lukujonojen kanssa epsilonin avulla. Looginen asioiden esitysjärjestys voi siis riippua siitä, että onko kokonaisuus esitettävissä lukiotasolla vai yliopistotasolla.

5.0.2 Havaintojen kokoaminen

Kootaan nyt havainnot. Ensinnäkin kun suunnitellaan kurssia yliopistomatematiikan aiheesta lukiolaiselle, niin tulee tehdä valinta että pyrkiikö kurssista tekemään varsinaisen lukiokurssin vai enemmän yliopisto-opiskeluun johdattelevan. Tämä valinta vaikuttaa suuresti kurssin ulkonäköön. Lukiomatematiikan ominaisia piirteitä jotka havaitsimme edellisessä analyysissä ovat sisällön rajaus tärkeimpiin määritelmiin ja lauseisiin, liian haastavan matematiikan selkeytys paremmin ymmärrettävään muotoon, painotus esimerkkeihin jot-

ka auttavat asian ytimen ymmärtämisessä ja perustelu opetettavan sisällön järjestykselle. Jos kurssista päätetään tehdä enemmän yliopistomatemaattisempi niin silloin teoriasisältöä laajennetaan esimerkkien lievällä kustannuksella.

Primitiivisten juurien läpi käyminen edellyttää esitietoja joista iso osa on jo lukiossa olevassa lukuteorian kurssissa. Lisäksi osa vaadituista esitiedoista ei löydy lukion oppimäärästä. Käsitellään tässä kappaleessa kuitenkin vain itse primitiiviset juuret sisältävän kokonaisuuden. Kurssi joka suunnitellaan kappaleessa 6 pohjautuu tässä tutkielmassa olevaan matemaattiseen sisältöön luvuissa 2 - 4. Analysoimme siis tässä luvussa vain **määritelmästä 3.7.** alkaen **lauseeseen 3.14.** asti sisältyvät aiheet. Nämä aiheet ovat *ord* funktio ja sen ominaisuudet, mikä on primitiivinen juuri ja ehdot millä jokin luku a on primitiivinen juuri jollakin modulo m. Analysoimme edellä esitettyjen yliopisto- ja lukiokurssien opetuksen erojen avulla sitä miten nämä aiheet voisi opettaa lukiokurssilla kun meillä on käytössämme yliopistokurssilla käytettävä materiaali.

5.0.3 Primitiivisten juurten opetus lukiossa

Ensiksi meidän on tehtävä rajaus tärkeimpiin määritelmiin ja lauseisiin. Kun lukiokurssin aihetta muunnetaan lukioon sopivaksi niin yleensä aiheeseen liittyvistä lauseista poistetaan ne mitkä ovat esitettävän asian opettamisen kannalta ylimääräisiä ja vähintäänkin liian työläät tai haastavat todistukset poistetaan näkyvistä. **Määritelmä 3.7.** on olennainen koska *ord* funktio on yksi opetettavista aiheista. Perustelu sen määrittelylle on lukioon nähden hieman turha ja opiskelijat voivat hyvin "uskoa" opettajaa siinä. Toki sen perusteleminen on helppo toteuttaa pyydettäessä. Runsaat esimerkit ovat tarpeen ja voivat hyödyntää potenssien sarjoja esimerkkien tuottamiseksi. Aiheeseen liittyviä harjoitustehtäviä voisi olla nimenomaan helpoista luvuista *ord* funktion arvon selvittäminen. **Lauseessa 3.8.** kerrotaan muutamia *ord* funktion määritelmän seuraamuksia ja ominaisuuksia. Kohtien i, ii ja iii todistukset ovat yksinkertaisia mutta kohdan iv todistus vaatii suurta luovuutta. Tämän tyyppiset todistukset joissa ikään kuin hatusta vedetään identiteettejä ovat melko hämääviä ja todennäköisesti eivät palvele tavoitteita koska opiskelijan näkökulmasta todistus lähtee liikkeelle täysin selittämättömästi. Siitä syystä kohdan iv todistaminen olisi syytä jättää pois opetusmateriaalista. Lukiotasolla on tärkeämpää osata käyttää näitä ominaisuuksia kuin osata todistaa ne, joten muissakin kohdissa niitä ei tarvitse näyttää osana opetusta vaikkakin asiasta kiinnostuneille niiden löytyminen oppimateriaalista on hyödyllistä. **Määritelmää 3.7.** edeltävät potenssisarjat ovat erinomainen havainnollistus siitä että millaisia rakenteita käsitellään kun puhutaan primitiivisistä juurista.

Jälkimmäiset lauseet käsittelevät ehtoja joilla jokin luku a on primitiivinen juuri moduloa m. **Määritelmä 3.9.** on suoraviivainen opiskelijalle joka on jo käynyt läpi totient-

tifunktion ja *ord* funktion. Tuotettavalla kurssilla on tarkoitus jonkin asteisesti käydä läpi jäännösluokkasysteemit, erityisesti vähennetty jäännösluokkasysteemi. Tästä syystä **lause 3.10.** on myös melko suoraviivainen kunhan jäännösluokkasysteemi on käyty kurssilla riittävän tarkasti läpi. **Lemma 3.11.** on enemmän ylimääräistä tietoa. Sitä käytetään **lauseen 3.12.** todistamiseen ja se on muuten irrallinen ja melko hankala. **Lausetta 3.12.** voi "yksinkertaistaa" esittämällä sanallisesti sen mitä **lauseen 3.12.** matemaattinen sisältö tarkoittaa eli sen että kaikilla alkuluvuilla on primitiivisiä juuria $\phi(p-1)$ kappaletta. Tällöin **lauseen 3.12.** todistus voidaan jättää pois materiaalista koska se on lähinnä **lemman 3.11.** todistaminen mikä taas vaatii sen tasoista kongruenssin laskusääntöjen hallintaa ja ymmärrystä mikä ylittää lukiotason. Loput, eli **korollaari 3.13.** ja **lause 3.14.** käyttävät **lauseen 3.10.** tiedosta muotoa "jaksollinen ryhmä". Terminä jaksollinen ryhmä on selkeästi lukion oppimäärän ulkopuolella eikä **lauseessa 3.8.** esitettyä asiaa ole olennaista kutsua jaksolliseksi ryhmäksi tässä kontekstissa vaan riittää matemaattinen muoto joukolle $\mathbb{Z}_p^*$. Sen sijaan että sanotaan milloin $\mathbb{Z}_p^*$ on jaksollinen voidaan sanoa että milloin sillä on primitiivisiä juuria. **Lauseen 3.14.** todistus sisältää paljon sellaista tietoa mitä ei lukiossa käydä ja ei voida sisällyttää primitiivisten juurten kurssille joten se pitää myös jättää pois materiaaleista.

Näin ollaan saatu rajattua itse primitiivisistä juurista ne lauseet ja todistukset mitkä voidaan sisällyttää lukiossa pidettävässä kurssissa. Katsastelimme myös jo sellaisia asioita mitä pitää muuttaa helpommin ymmärrettävään muotoon mutta käydään kaikki edellisessä kohdassa valittu materiaali läpi vielä siten, että pohditaan sitä että onko niitä tarpeellista muokata johonkin toiseen muotoon. Tyypillisin syy esitystavan muodon muuttamiseen mikä havaittiin analyysin oppikirjoissa oli se että jos tarkka määritelmä tai todistus sisältää merkintöjä jotka ovat ennaltaan tuntemattomia ja jotka siten vievät turhaan opiskelijan huomiota koska olennaista on asiasisältö. Kongruenssi tuttuna konseptina ei aiheuta ongelmia. Ord funktio ja totienttifunktio taas funktioina ovat hyvin luontevia. Nähdäkseni ongelmina ovat vähennetty jäännösluokkasysteemi ja **lauseen 3.12.** joukkomerkinnät. Joukkoja ei juurikaan käsitellä lukiotasolla ja vaikka esimerkiksi luonnollisten lukujen joukon esittäminen aaltosuluilla on melko helppolukuista niin edellä mainittujen kohtien joukkomerkinnät ovat melko monimutkaisia eivätkä sen takia mielestäni edistä asian oppimista. Opiskelijan vaivannäköä kuluu joukkomerkinnän kääntämiseen selkokielelle. Niissä siis tulisi muuttaa matemaattinen merkintä selkokieleksi kuvailemalla millainen objekti on kyseessä.

Jäljellä on vielä opetettavien asioiden järjestyksen perustelu ja esimerkkien painotus. Emme tässä luvussa tuota esimerkkejä vaan ne tehdään luvussa 6 jossa tuotetaan kurssisuunnitelma primitiivisten juurten kurssille. Siispä enää pitää analysoida voimmeko esittää primitiivisten juurten lukiokurssilla nämä lauseet samassa järjestyksessä kuin yliopiston kurssilla. Yliopistokurssilla aluksi kerrotaan mitä primitiiviset juuret ovat, sitten

määritellään ord funktio avuksi. Tämän jälkeen määritellään ehtoja millä jokin on primitiivinen juuri. Kokonaisuutena tämä järjestys on hyvin looginen eikä niiden järjestystä ole tarpeellista muuttaa tai erottaa toisistaan. Opetettavien asioiden järjestys vaikuttaa enemmän muuhun kurssiin jossa on syytä pohtia että kuuluuko jotkin aiheet lähemmäs primitiivisiä juuria kuin toiset. Syy lukujonojen esittämiseen sarjojen yhteydessä oli lukiokurssilla perusteltu lähestymistavalla mutta vastaavaa ei ole mahdollista perustella primitiivisten juurten paketin sisällä.

Luku 6

Primitiivisten juurten kurssi lukiossa

Tässä tutkielmassa tehdään kurssisuunnitelma lukiossa opetettavalle kurssille jonka pääaiheina ovat primitiiviset juuret ja Diffie-Hellman avaintenvaihtoprotokolla. Teimme edellisessä luvussa jaottelun akselilla "lukiokurssimainen" ja "yliopistokurssimainen". Koska useat keskeiset sisällöt jotka käsitellään primitiivisten juurten esitietoina ovat jo olemassa olevan lukuteoriaa käsittelevän lukiokurssin keskeisissä sisällöissä niin pyrimme toteuttamaan jonkinasteista välimuotoa edellä mainitusta jaottelusta. Kurssi rakennetaan sen pohjalta että opiskelija olisi jo käynyt lukuteoriaa sisältävän kurssin, mutta se ei kuitenkaan ole välttämätöntä. Tämä näyttäytyy siten että lukuteorian kurssilla jo käsitellyt asiat esitellään "tarkemmin" sen kaltaisena miltä ne näyttävät yliopiston materiaaleissa ja tässä tutkielmassa. Entuudestaan tuntemattomat asiat pyritään esittämään pelkistetyssä muodossa jossa lukiolaisen on helpompi ymmärtää mistä on kyse. Kurssi suunnitellaan käyttämään kuusi viikkoa ja joka viikossa kolme 75 minuutin oppituntia. Vuonna 2021 voimaan tulevissa lukion opetussuunnitelmissa tämä tulee vastaamaan kahta opintopistettä. Käydään tässä luvussa läpi tarkkaan mitä asioita kurssi sisältää ja mikä on kyseisten asioiden läpikäymiseen suositeltu ajastus. Perustelemme mitä tämän tutkielman lauseita ja teorioita sisällytämme ja miten niitä pelkistetään jos se on tarpeellista. Tämän jälkeisessä luvussa annamme tarkan kurssisuunnitelman mikä sisältää esimerkkejä joilla halukas opettaja saa kehyksen jonka ympärille toteuttaa tämä kurssi. Aloitetaan peruskäsitteillä jotka ovat jo entuudestaan opiskelijoille tuttuja. Käydään nämä läpi samaan tyyliin kuin matematiikkalehti Solmun artikkelissa "lukuteorian helmiä opiskelijoille."

6.0.1 Opetettavat aiheet ja niihin käytettävä aika

Lukion 2021 opetussuunnitelman perusteiden mukaan keskeisiä sisältöjä mitä kurssi MAA 11: Lukuteoria ja algoritmit sisältää ovat muunmuassa jaollisuus, kongruenssi, jakoyhtä-

lö, aritmetiikan peruslause ja alkulukujen ominaisuuksia. Nämä ovat myös tässä tutkielmassa määriteltyjä perustietoja jotka tarvitaan primitiivisiin juuriin etenemiseen. Vaikka nämä asiat ovat oletuksellisesti entuudestaan tuttuja, ne käsitellään yliopistomaisemmin. Ensimmäinen kokonaisuus on jaollisuus ja jakoyhtälö. Tämä kattaa tutkielmassa kohdat 2.1., 2.2. ja 2.4. Määritelmä 2.1. voidaan esittää sellaisenaan koska siinä ei ole mitään uusia merkintöjä. Sama pätee lauseille 2.2. ja 2.4. Lausen 2.4. todistus on sopivaa olla osa opetusta koska pyritään yliopistomaisempaan käsittelyyn. Lauseesta 2.2. ainakin kaksi kohtaa voisi olla opiskelijoiden harjoitustehtävinä. Yhden opettaja voisi näyttää koska muut ovat hyvin samankaltaisia. Lauseen 2.4. todistus on todennäköisimmin liian haastavaa keskiverto lukion tason opiskelijalle itse keksittäväksi vielä tässä vaiheessa kun todistustekniikkaa ei ole vielä hiottu tarpeeksi. Kokonaisuus on jo entuudestaan tuttu joten tähän voisi mielestäni käyttää yhden 75 minuutin oppitunnin. Joka aiheeseen liittyvät esimerkit esitellään tämän luvun lopussa.

Seuraava kokonaisuus on suurin yhteinen tekijä. Tämä sisältää tutkielman kohdat 2.5., 2.7. ja 2.9. Suurin yhteinen tekijä on konseptuaalisesti helppo joten tällä kurssilla voidaan hyvin perehtyä sen formaalimpaan määrittämiseen. Lauseen 2.5. todistaminen on liian työläs tarkkaan läpi käymiseen tässä kontekstissa, mutta jos on ylimääräistä aikaa niin opettaja voi sen myös näyttää. Korollaarin 2.7. todistus sisältää logiikan miten kaksi joukkoa todistetaan toisikseen. Se ei kuulu lukion oppimäärään joten senkin esittäminen on enemmän ajankäyttöön liittyvä valinta. Lausen 2.9. todistaminen vaatii hieman mielikuvitusta mutta se soveltuu hyvin harjoitustehtäväksi. Suurimmasta yhteisestä tekijästä on kuitenkin tämän kurssin viitekehyksessä tärkeämpää ymmärtää miten sitä käytetään eikä matematiikkaa taustalla.

Seuraava aihekokonaisuus on alkuluvut. Alkulukujen kokonaisuus tällä kurssilla kattaa tutkielmasta objektit 2.11. - 2.15., 2.17. - 2.20. Objektit 2.11. - 2.13. ovat jo entuudestaan tutut koska ne käsitellään osana lukion lukuteorian kurssia. Kuten muissakin jo entuudestaan tutuissa asioissa, pyrimme suuntaamaan kurssin sisällön yliopistomaisemman näköisenä. Erityisesti lauseen 2.13. todistus tulisi esittää opettajan toimesta. Lauseiden 2.13. ja 2.14. todistukset kumpikin käyttävät vastaoletusta. Lauseen 2.13. todistuksen esittäminen on hyvä valmistelu sille että opiskelija itse keksii lauseen 2.14. todistuksen. Jos se on haastaavaa niin vihjeenä voi juurikin antaa sen että se ratkeaa vastaoletuksella. Määritelmä 2.15. antaa uuden termin käyttöön eikä sisällä haastavaa matematiikkaa joten se voidaan esittää sellaisenaan. Korollaarit 2.17. ja 2.18. muodostavat parin eli toinen yleistää edeltävän, kun tulontekijöitä on n kappaletta. Tämän tyyppiset parilliset lauseet ovat yleensä hyvä käsitellä niin että opettaja todistaa tilanteen jossa termejä on kaksi kappaletta ja opiskelijan tulee yleistää tämä n kappaletta tilanteelle. Korollaarin 2.19. todistus on sen verran yksinkertainen että sekin soveltuu harjoitustehtäväksi. Lause 2.20. eli aritmetiikan peruslause on jo osana lukion lukuteorian kurssia mutta sen todistaminen tarkasti voi-

si olla alkulukuosion huipentuma tällä kurssilla. Alkulukujen kokonaisuus on sen verran laajahko että ehdotan siihen käytettäväm kaksi 75 minuutin oppituntia.

Seuraava aihekokonaisuus on kongruenssi. Kongruenssin aihekokonaisuus käsittää kohdat 2.25., 2.27., 2.28. ja 2.30. tästä tutkielmasta. Kongruenssi on jo lukion lukuteorian kurssilta melko tuttu joten tässäkin vaiheessa keskitytään enemmän asioiden tarkempaan ilmaisuun eli esitellään kongruenssi siten kuin se näyttäytyy yliopiston puolella. Esimerkiksi lauseen 2.28. laskusäännöt ovat erinomaisia harjoitustehtäviä koska lukiomatematiikanpuolella tämän tyyppiset asiat yleensä otetaan sääntöinä mutta yliopistomatematiikan puolella ne ovat ominaisuuksia mitkä pitää todistaa. Myös lemman 2.27. kohtien todistaminen määritelmän 2.25. avulla ovat erinomaisia harjoitustehtäviä eivätkä haasteellisuudeltaan ylimalkaisia. Lause 2.30. lieneekin ainoa uusi asia kongruenssiin liittyen joten sen todistuksen esittäminen lankeaa opettajan rooliksi. Kokonaisuutena kongruenssi aihe on jo melko selkeä opiskelijoille joten tähänkin suositellaan käytettävän yksi 75 minuutin oppitunti.

Seuraava aihe on jäännösluokat ja jäännösluokkasysteemit. Nämä ovat tällä kurssilla tuleva ensimmäinen uusi aihe. Lähdemateriaalissa oli tässä välissä hieman algebraa. Meidänkin olisi hyvä alustaa jäännösluokkia esittelemällä niin kutsuttu kellotauluaritmetiikka eli modulaarinen aritmetiikka. Kellon ajannäyttö käyttää modulaarista aritmetiikkaa modulo 12 joten se on hyvä esimerkki jäännösluokilla laskemisen esittelemiseen. Tähän aihepiiriin ei suoraan löydy materiaalia tästä tutkielmasta, mutta tämän tavoitteena on purkaa auki jäännösluokkia olioina ennen kuin niihin paneudutaan matemaattisesti. Tähän tulisi käyttää yksi 75 minuutin oppitunti.

Varsinainen jäännösluokat ja jäännösluokka systeemit kokonaisuus vastaa tämän tutkielman objekteja 2.32. - 2.46. Nämä kaiken kaikkiaan ovat liian laaja kokonaisuus lukiokurssin ajankäytön kannalta. Ehdotan että tämä kokonaisuus jaetaan kolmeen palaseen. Ensimmäisen palasen materiaali ovat objektit 2.32, 2.35, 2.37 ja 2.38. Objekti 2.33. karsitaan pois opetuksellisesti turhana ja merkintöjen tulkinnan haasteellisuutena lukiotasolla. Sen sijaan esitetään että $\overline{a}$ tarkoittaa luvun a jäännösluokkaa ilman formaalia määritelmää koska jäännösluokat on jo pyritty lisäämään käsitteistöön edellisellä oppitunnilla. Määritelmästä 2.37. voidaan jättää sana rengas pois ja puhua ennemmin määritelmän 2.35. objektista jolle kerrotaan laskusäännöt. Toinen palanen sisältää objektit 2.40., 2.42. ja 2.43. Ensimmäisen palasen aihe on jäännösluokat ja toisen palasen aihe on täydelliset jäännösluokkasysteemit. Määritelmä 2.39. jätetään pois koska termin kunta määrittäminen ei palvele tämän kurssin tarkoitusta. Lauseen 2.42. todistus on liian työläs esitettäväksi mutta korollaarin 2.43. todistus olisi hyvä olla edes materiaalissa esillä. Viimeinen palanen sisältää objektit 2.44. ja 2.46. Eli siis käytännössä Fermat'n pienen lauseen. Tässä yhteydessä opettaja voi esittää lauseen 2.44. todistuksen ja kertoa sen historiasta. Näihin kolmeen palaseen tulisi yhteensä käyttää kolme 75 minuutin oppituntia.

Seuraava aihekokonaisuus on Eulerin totienttifunktio. Eulerin totienttifunktio kokonaisuus kattaa objektit 2.47., 2.49. - 2.51. ja 2.53. Määritelmät 2.34. ja 2.50. olisi suotavaa jättää pois opetuksesta sillä tämän aihekokonaisuuden tavoite on harjoitella totienttifunktion käyttöä ja oppia mitä se tarkoittaa. Se mitä lukuteoreettinen funktio tarkoittaa olisi suotavaa lisätä lauseeseen 2.51. opetustilanteessa. Kumpikin tähän kokonaisuuteen liittyvä lause näyttää hyvin paljon laskusäännöltä. Pyrittäessä selkeyteen lauseen 2.53. todistus olisi hyvä jättää pois näkyvistä. Lauseen 2.51. intuitiivisuus ja todistuksessa käytettävä kuva soveltuvat hyvin opetukseen ja harjaannuttaa opiskelijoiden matemaattista ajattelua. Muuten tässä kokonaisuudessa lähinnä määritellään Eulerin totienttifunktio ja annetaan muutama laskusääntö sille. Tähän olisi hyvä käyttää yksi 75 minuutin oppitunti.

Seuraava aihe on vähennetyt jäännösluokkasysteemit. Tämä kokonaisuus sisältää objektit 2.54., 2.55. ja 2.57. 2.38 - 2.40. mutta koska tällä pyritään tuottamaan hyvin keskeinen tulos eli lause 2.58. niin se olisi myös hyvä olla osana tätä kokonaisuutta. Termit surjektio, bijektio ja injektio eivät esiinny 2021 voimaan tulevassa lukion opetussuunnitelmassa eikä niiden käsittely ole olennaista tämän kurssin kannalta. Ne olisi siis hyvä "sensuroida" pois. Tästä syystä lauseiden 2.57. ja 2.58. todistuksien ei tulisi olla osana itse opetusta mutta niiden olisi hyvä olla materiaalissa esillä jotta opiskelija voi itse sitä katsella. Tässäkin termin bijektio tilalla esimerkiksi tulisi olla selitys siitä mitä se tarkoittaa jotta opiskelija voisi itsenäisesti lukea todistuksen läpi. Tämäkin kokonaisuus on melko lyhyt ja siitä syystä tähän olisi hyvä käyttää yksi 75 minuutin oppitunti.

Seuraava aihekokonaisuus on polynomien kongruenssi. Tutkielmasta tämä aihe kattaa objektit 3.1. ja 3.3.-3.5. jossa 3.5. on tärkeä tulos mikä saadaan korollaarin 3.3. avulla vaikka ei suoraan itse sisällöltään vaikuta liittyvän polynomien kongruensseihin. Tämä laajentaa opiskelijan mahdollisuutta käsitellä kongruenssirelaation sisältäviä objekteja paljon joten tässä olisi hyvä edetä rauhalliseen tahtiin vaikka kongruenssi itsessään on jo tässä vaiheessa hyvin tuttu opiskelijoille. Ehdotan että tämä jaetaan kahteen 75 minuutin oppituntiin siten, että ensimmäisellä esitellään objektit 3.1., 3.3. ja 3.4. joista 3.4. todistus esitetään opettajajohtoisesti. Objektien 3.3. ja 3.4. todistukset ovat lyhyitä ja melko suoraviivaisia joskin objektin 3.4. todistus voi vaatia lievää opettajan johdattelua. Kumpikin kuitenkin nähdäkseni sopivat hyvin harjoitustehtäviksi vaikkakin itse lauseet annetaan oppimateriaalissa sellaisinaan ominaisuuksina. Jälkimmäisellä oppitunnilla taas käydään läpi lause 3.5. Koska lauseessa 3.5. pitää todistaa ekvivalenssi niin kätevä strategia sen opetuksessa on opettajajohtoisesti todistaa ekvivalenssin yksi suunta ja jättää toinen suunta harjoitustehtäväksi.

Seuraava aihekokonaisuus on primitiiviset juuret. Niiden opetus on jo analysoitu tarkemmin luvussa viisi joten tässä kohtaa esitämme vain aika-arvion siitä mitä olisi suotava käyttää niihin. Koska primitiiviset juuret ovat täysin uutta asiaa ja melko työlästä materiaalia niin olisi suotavaa käyttää kolme 75 minuutin oppituntia niihin.

Viimeiseksi aiheeksi tällä kurssilla jää Diffie-Hellman avaintenvaihtoprotokolla. Mielestäni Diffie-Hellman on oiva motivaattori tämänlaiselle kurssille koska se on yksi suora esimerkki siitä miten primitiivisiä juuria voidaan soveltaa oikeassa elämässä. Diffie-Hellman on sinänsä yksinkertainen joten tämän aiheen opetus tulisi koostua protokollan toiminnan esittämisestä ja siitä mitä ongelmia siinä voi olla. Opiskelijat voivat harjoitella protokollan käyttöä ja samalla harjoittelevat primitiivisten juurten laskemista. Opetuksessa tulisi esittää luvussa neljä käsitelty square and multiply algoritmi. Tähän olisi suotavaa käyttää yksi tai kaksi 75 minuutin oppituntia.

6.0.2 Yhteenveto

Yhteenvetona kurssin sisältö:

- Jaollisuus ja jakoyhtälö 1 x 75 min
- Suurin yhteinen tekijä 1 x 75 min
- Alkuluvut 2 x 75 min
- Kongruenssi 1 x 75 min
- (Algebraa) Jäännösluokat kellotauluaritmetiikalla 1 x 75 min
- Jäännösluokat ja jäännösluokkasysteemit 3 x 75 min
- Totienttifunktio 1 x 75 min
- Täydelliset jäännösluokkasysteemit 1 x 75 min
- Polynomien kongruenssit 2 x 75 min
- Primitiiviset juuret 3 x 75 min
- Diffie-Hellman avaintenvaihtoprotokolla 1 x 75 min
- Kertaus tai ylimääräinen aika mille tahansa kurssin aiheelle 1 x 75 min

Yhteensä siis 18 x 75 minuuttia oppitunteja. Muuten kurssi noudattaa kaavaa siten, että aiheeseen liittyy matemaattisia objekteja kuten lauseita, korollaareja, määritelmiä jne. Joka aihepiirin aiheisiin on esimerkkejä materiaalissa ja sitten opiskelijat voivat itsenäisesti harjoitella aiheen sisältöjä harjoitustehtävillä jotka liittyät aiheisiin. Tässä tutkielmassa ei tuoteta tämänlaiseen kurssiin kokonaista oppikirjaa mutta joka aihepiiriin annetaan muutama esimerkki mitä voi käyttää opetuksessa. Kaikista aihepiireistä on käsitelty että mitä lauseita niissä esitellään ja millä aikataululla joten kurssisuunnitelman muodostaminen tutkielman pohjalta on helppoa.

6.0.3 Esimerkit

Kuten edellä kuvailtiin, niin tässä kurssissa ne alueet mitkä ovat jo tuttuja käsitellään yliopistomaisemmin eli vähemmällä määrällä esimerkkejä. Tarkoitus on niihin kappaleisiin tuottaa yksi esimerkki kun taas ne kappaleet jotka sisältävät uutta asiaa niin niihin tuotetaan kolme esimerkkiä. Esimerkkejä voi käyttää osana opetusta tai ne voivat olla vain materiaalissa mukana ja opiskelijat voivat itse käyttää niitä opiskelun tukena. Tässä kohtaa esitellään vain esimerkkejä eikä esimerkkien ulkopuolella olevaa teoriaopetusta.

Jaollisuus ja jakoyhtälöt

Esimerkki 1. Lauseen 2.4. todistuksen esittäminen.

Suurin yhteinen tekijä

Esimerkki 1. Lauseen 2.9. todistus.

Alkuluvut

Esimerkki 1. Lauseen 2.17. todistus.

Esimerkki 2. Korollaarin 2.18. todistus.

Kongruenssi

Esimerkki 1. Lauseen 2.28. todistus.

Jäännösluokat kellotauluaritmetiikalla

Esimerkki 1. Kellotaulussa on luvun 12 kohdalla luku nolla. Kello on yhdeksän. Mitä kellotaulun lukua tuntiviisari näyttää kun kuluu kaksi tuntia? Tällöin viisari näyttää lukua $9 + 2 = 11$.

Esimerkki 2. Entäs jos aikaa kului 3 tuntia? Tällöin viisari on kellotaulussa siinä kohtaa missä perinteisesti on 12 mutta tässä kellotaulussa on luku nolla.

Esimerkki 3. Entäs jos kuluikin viisi tuntia? Tällöin kellotaulu siirtyy aluksi kolme kohtaa eli kohtaan nolla jonka jälkeen on vielä kaksi viisarin siirtymää eli loppullinen tuntiviisarin paikka on kaksi.

Jäännösluokat ja jäännösluokkasysteemit

Esimerkki 1. Edellisen kappaleen kellotauluesimerkeissä kellotaulun tuntiviisarin osoittamat ajat ovat jakojäännöksiä. Jokainen jakojäännös edustaa jäännösluokkaa. Tällöin jäännösluokat olivat moduloa 12.

Esimerkki 2. Tarkastellaan jäännösluokkia modulo viisi. Tällöin mahdollisia jakojäännöksiä on viisi kappaletta ja ne sisältyvät joukkoon $\{0, 1, 2, 3, 4\}$. Tällöin jäännösluokat ovat $[0]_5 = \{5 \cdot k \mid \quad k \in \mathbb{Z}\}$, $[1]_5 = \{5 \cdot k + 1 \mid \quad k \in \mathbb{Z}\}$, $[2]_5 = \{5 \cdot k + 2 \mid \quad k \in \mathbb{Z}\}$, $[3]_5 = \{5 \cdot k + 3 \mid \quad k \in \mathbb{Z}\}$ ja $[4]_5 = \{5 \cdot k + 4 \mid \quad k \in \mathbb{Z}\}$.

Esimerkki 3. Jäännösluokkasysteemi on kokoelma kokonaislukuja. Jäännösluokkasysteemi on täydellinen, kun (siitä löytyy jokaista jäännösluokkaa ja) jokaisesta jäännösluokasta on systeemissä täsmälleen yksi edustaja. Jäännösluokkasysteemi $\{1, 2, 3, 5\}$ ei ole täydellinen jäännösluokkasysteemi modulo 4 koska jäännösluokalla $\overline{4}$ ei ole edustajia systeemissä.

Esimerkki 4. $\{1, 2\}$ on täydellinen jäännösluokkasysteemi modulo 2.

Esimerkki 5. Korollaarin 2.43. todistus.

Esimerkki 6. Lauseen 2.44. todistus.

Eulerin Totienttifunktio

Esimerkki 1. Lauseen 2.51. todistus.

Esimerkki 2. Lasketaan luvun 10 totienttifunktion arvo. Lukujen 2 ja 5 suurin yhteinen tekijä on 1. Tällöin $\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5)$. On helppo nähdä että $\phi(2) = 1$ ja että $\phi(5) = 4$. Tällöin $\phi(10) = 1 \cdot 4 = 4$.

Esimerkki 3. Lasketaan luvun 17 totienttifunktion arvo. Koska 17 on alkuluku niin kaikki sitä pienemmät luvut ovat sen kanssa suhteellisia alkulukuja. Tällöin totienttifunktion määritelmän mukaan $\phi(17) = 17 - 1 = 16$.

Vähennetty jäännösluokkasysteemi

Täydellisestä jäännösluokkasysteemistä saadaan vähennetty jäännösluokkasysteemi poistamalla siitä ne alkiot jotka eivät ole suhteellisia alkulukuja kyseisen jäännösluokkasysteemin modulolle.

Esimerkki 1. $\{1, 2, 3...8\}$ on täydellinen jäännösluokkasysteemi moduloa 8. Nyt luvut 1, 3, 5 ja 7 ovat ainoat lukua 8 pienemmät luonnolliset luvut joilla ei ole yhteisiä tekijöitä luvun 8 kanssa. Siispä tätä vastaava vähennetty jäännösluokkasysteemi on $\{1, 3, 5, 7\}$.

Esimerkki 2. Miten voi varmistaa että on löydetty esimerkin 1 kaltaisessa tilanteessa kaikki vähennetyn jäännösluokkasysteemin alkiot? Ottamalla Eulerin totienttifunktion arvo täydellisen jäännösluokkasysteemin modulosta saadaan sitä vastaavan vähennetyn jäännösluokkasysteemin alkioiden lukumäärä. Tällöin moduloa 8 vastaavassa vähennetyssä systeemissä on $\phi(8) = 4$ alkiota. Vastaavasti moduloa 21 vastaavassa systeemissä on $\phi(21) = 20$ alkiota jne.

Polynomien kongruenssit

Esimerkki 1. Korollaarin 3.4. todistus.

Esimerkki 2. Lauseen 3.5. todistuksen $\Rightarrow$ suunta.

Primitiiviset juuret

Esimerkki 1. ja 2. Kohdan 3.0.2. Primitiiviset juuret tapaukset $p = 9$ ja $p = 7$.

Esimerkki 3. Lauseen 3.8. kohtien i, ii ja iii todistukset

Esimerkki 4. Katsotaan lauseen 3.14. avulla onko luvuilla primitiivisiä juuria tapauksissa $m = 14$ ja $m = 81$. Ensimmäisessä kohdassa $m = 14 = 2 \cdot 7$ jossa 7 on alkuluku eli kyseessä on tapaus $m = 2 \cdot p^e$ jossa $e = 1$. Kun kyseessä on $m = 81 = 3 \cdot 3 \cdot 3 = 3^3$ eli kyseessä on tapaus $m = p^e$ kun $p = 3$ ja $e = 3$.

Diffie-Hellman avaintenvaihtoprotokolla

Esimerkki 1.Luvussa 4 esitelty salauksen lähetys.

Esimerkki 2. Luvulla m on primitiivisiä juuria kun $m = 2 \cdot p^e$ jossa p on alkuluku ja e positiivinen kokonaisluku. Käytetään square and multiply algoritmia luvun $2 \cdot 11^{200}$ laskemiseen. Kyseessä on lauseen 3.12. mukaan primitiivisen juuren antava modulo. Nyt luku 200 on binäärisenä 11001000. Tämän selvittämiseen voi käyttää algoritmia tai laskemalla itse että $200 = 128 + 64 + 8 = 2^7 + 2^6 + 2^3$. Nyt square and multiply algoritmilla saamme laskutoimitukseksi $(((((((((11)^2) \cdot 11)^2)^2)^2) \cdot 11)^2)^2)^2$.

Luku 7

Loppusanat

Tutkielman tavoitteena on luoda tarpeeksi laaja viitekehys jonka avulla tutkielman lukenut lukion opettaja pystyy suunnittelemaan ja toteuttamaan mahdollisen valinnaisen lukion kurssin jonka keskeisenä teemana on primitiiviset juuret. Mielestäni jokaiseen opetettavaan aiheeseen on kelvollisia ja halutessaan muokattavia esimerkkejä mitä voisi käyttää opetuksessa. Diffie-Hellmanin avaintenvaihtoprotokollassa käytettävää square and multiply algoritmia lukuunottamatta tutkielmassa ei esiinny juurikaan digitaalisia sovelluksia ynnä muuta vastaavaa, mitä kurssin aikana voisi toteuttaa. Geogebralla voi kyllä demonstroida lukuteoriaankin liittyviä ominaisuuksia mutta visuaaliset havainnollistukset eivät ole lukuteoriassa yhtä helppoja kuin useissa muissa matematiikan haaroissa. Ehdotankin siis että jos kokee tarpeelliseksi digitaalisen sisällön lisäämisen niin kurssin alkupäästä voidaan karsia tämän kurssin ja jo olemassa olevan lukion lukuteorian kurssin yhteisiä sisältöjä. Siten saadaan loppupäähän lisää ja sen voi käyttää esimerkiksi square and multiply algoritmin koodaamiseen.

Oma henkilökohtainen toivomukseni on että tämänlainen kurssi päästäisiin jossakin lukiossa joskus toteuttamaan mikäli sille löytyy innostunut opettaja ja tarpeeksi paljon aiheesta kiinnostuneita opiskelijoita.

Kirjallisuutta

[1] Jokke Häsä ja Johanna Rämö: Johdatus abstraktiin algebraan, 3. painos, Gaudeamus Oy, 2012 & 2015

[2] Kenneth Ireland ja Michael Rosen: A Classical Introduction to Modern Number Theory, 2. painos, Springer, 1972 & 1982 & 1990 & 1998

[3] Eero Saksman: Introduction to number theory, kurssi kalvot, Helsingin yliopisto, 2019 syksy

[4] Manoj Mishra ja Jayaprakash Kar: A study on diffie-hellman key exchange protocols, volume 114 ,International Journal of Pure and Applied Mathemathics, Numero 2 2017

[5] Jukka Kangasaho, Jukka Mäkinen, Juha Oikkonen, Johannes Paasonen, Maija Salmela ja Jorma Tahvanainen: Pitkä matematiikka 13 Differentiaali ja integraalilaskennan jatkokurssi, 3. painos, Sanoma Pro Oy, 2013

[6] Jukka Pihko: Lukuteorian helmiä lukiolaisille, Matematiikkalehti Solmu, 1 osa, 2008

[7] Opetushallitus, Lukion opetussuunnitelman perusteet 2019