Eulerin lause

LuK-tutkielma
Riku Laiti
2497080
Matemaattisten tieteiden tutkimusyksikkö
Oulun yliopisto
Kevät 2019

Sisältö

Johdanto

Ilmiömäisestä laskupäästään ja tuotteliaisuudestaan tunnettu matemaatikko Leonhard Euler sai inspiraatiota lukuteorian kehittämiseen tutkiessaan Pierre de Fermat'n sata vuotta aikaisemmin tekemää työtä. Hän todisti Fermat'n pienen lauseen vuonna 1736, yleisti sen myöhemmin vuonna 1760 nimeään kantavaksi lauseeksi ja todisti sen joukko-opin käsitteiden avulla. Tämä lause onkin kyseisen matematiikan alan ensimmäisiä lauseita. Fermat'n pieni lause liittyy alkulukumoduloisiin kongruensseihin ja Eulerin lause laajentaa moduloluvun mielivaltaiseksi. Tämän mahdollistaa Eulerin kehittämä ϕ-funktio, joka on tärkeä osa lausetta. [Childs 2009]

Tutkielmani käsittelee Eulerin lausetta. Tutkielmassa määritellään aluksi kongruenssi, jäännösluokat ja Eulerin ϕ-funktio. Niistä käydään läpi ominaisuuksia ja muita aputuloksia, joita tarvitaan Eulerin lauseen todistamiseksi. Käsitellään myös esimerkkejä lauseen käytöstä ja viimeisessä kappaleessa sen sovelluksia.

Eulerin lause on hyödyllinen, sillä se auttaa laskemaan eksponentteja sisältäviä kongruenssilaskuja ja tulosta käytetään mm. kryptografiassa RSA:n perustana. Sen avulla on myös mahdollista testata, onko luku yhdistetty luku. Eulerin lauseesta käytetään myös nimityksiä Euler-Fermat'n lause ja Euler-Fermat'n teoreema.

0.1 Merkintöjä

Käytetään tutkielmassa seuraavia merkintöjä:

- Luonnollisten lukujen joukko: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- Kokonaislukujen joukko: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- Alkulukujen joukko: $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$
- Lukua m suuremmat kokonaisluvut $\mathbb{Z}_{\geq m} = \{a \in \mathbb{Z} \mid a \geq m\}$
- Lukujen a ja b suurin yhteinen tekijä eli $syt(a, b)$

1 Kongruenssi

Määritellään kongruenssi ja sen avulla jäännösluokat ja alkuluokat.

Määritelmä 1.1. Olkoon $m \in \mathbb{N}$. Kahden kokonaisluvun a ja b sanotaan olevan kongruentteja modulo m, merkitään

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

jos m jakaa erotuksen $a - b$ eli $a - b = km$ jollekin kokonaisluvulle k.

Määritelmä 1.2. Kokonaislukujen joukossa $\mathbb{Z}$ määritellyn kongruenssin

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

perusteella määritellään jäännösluokat modulo m. Kokonaisluvun b määräämästä jäännösluokasta modulo m käytetään merkintää

$$[b] = [b]_m = \{a \in \mathbb{Z} \mid a \equiv b \pmod{m}\}$$

Määritellään myös jäännösluokkien modulo m kertolasku seuraavasti:

$$[a][b] = [ab]$$

Huomautus 1.3. Kertolasku modulo m ei riipu jäännösluokkien edustajista a ja b .

Todistus. Todistus esitetään teoksessa [Erickson, Vazzana 2008, s.58]. □

Määritelmä 1.4. Jäännnösluokkaa $[a] \pmod{m}$ sanotaan alkuluokaksi modulo m, mikäli $syt(a, m) = 1$. Alkuluokkien joukkoa merkitään $\mathbb{Z}_m^*$. Siis

$$\mathbb{Z}_m^* = \{[a] \in \mathbb{Z}_m \mid syt(a, m) = 1\}.$$

Huomautus 1.5. Jos p on alkuluku, niin

$$\mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\}.$$

Todistus. Olkoon $a \in \mathbb{Z}$ ja $0 < a < p$. Koska p on alkuluku, niin $syt(a, p) = 1$. Siten Määritelmän 1.4 nojalla

$$[a] \in \mathbb{Z}_p^*.$$

□

2 Eulerin ϕ-funktio

Nyt voidaan määritellä Eulerin lauseen oleellisin osa eli Eulerin ϕ-funktio. ϕ-funktio kuvastaa argumenttinsa osittuvuutta eli kuinka kuinka monen alkuluvun tulo luku on. Mitä suurempi ϕ-funktion arvo on, sitä vähemmän luvulla on alkutekijöitä. Selvitetään myös, miten funktion arvo lasketaan.

Määritelmä 2.1. Funktio $\phi : \mathbb{Z}_+ \to \mathbb{Z}_+,\ \phi(m) = |\mathbb{Z}_m^*|$ on Eulerin ϕ-funktio. Funktio $\phi(m)$ kertoo lukumäärän niille alkioille, jotka ovat pienempää kuin m ja keskenään jaottomia sen kanssa. Toisin sanoen

$$\phi(m) = |\{x \mid x \in \mathbb{N},\ x < m \ ja\ syt(x, m) = 1\}|.$$

Esimerkki 2.2.

m	3	4	5	6	7	8	9	10	13	15
$\phi(m)$	2	2	4	2	6	4	6	4	12	8

Huomautus 2.3. Kun m on alkuluku, $\phi(m) = m - 1$.

Todistus. Kaikki alkulukua m pienemmät positiiviset luvut ovat keskenään jaottomia sen kanssa, joten ϕ-funktion määritelmän perusteella voidaan todeta, että funktion arvoksi saadaan $m - 1$. □

Lause 2.4. *Olkoot m ja n keskenään jaottomat positiiviset kokonaisluvut. Tällöin pätee*

$$\phi(mn) = \phi(m)\phi(n).$$

Kutsutaan tätä ominaisuutta multiplikatiivisuudeksi.

Todistus. Esitetään tuloa mn pienemmät positiiviset kokonaisluvut seuraavasti:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\
\vdots & \vdots & \vdots & & \vdots \\
\mathrm{r} & m+r & 2m+r & \dots & (n-1)m+r \\
\vdots & \vdots & \vdots & & \vdots \\
\mathrm{m} & 2m & 3m & \dots & mn.
\end{array}$$

Olkoon r positiivinen kokonaisluku ja pienempi kuin m. Oletetaan myös, että $syt(m, r) = d > 1$. Yksikään r:nnen rivin luku ei ole keskenään jaoton tulon mn kanssa, sillä kaikki rivin alkiot ovat muotoa $km + r$, missä $k \in \mathbb{Z},\ 1 \leq$

$k \leq n-1$ ja $d \mid (km+r)$, koska $d \mid m$ ja $d \mid r$. Jotta löydetään tulon mn kanssa jaottomat kokonaisluvut, tarkastellaan riviä r vain, jos $syt(m,r) = 1$.

Oletetaan nyt, että $syt(m,r) = 1$ ja $1 \leq r \leq m$. Täytyy päätellä, kuinka moni kokonaisluku on keskenään jaoton tulon mn kanssa. Alkiot rivillä r ovat $r, m+r, 2m+r, \ldots, (n-1)m+r$. Koska $syt(r,m) = 1$, jokainen näistä kokonaisluvuista on keskenään jaoton luvun m kanssa. Koska r:nnen rivin alkiot muodostavat jäännösluokkien joukon modulo n, tarkalleen $\phi(n)$ kokonaislukua ovat keskenään jaottomia luvun n kanssa. Nämä $\phi(n)$ kokonaislukua ovat myös keskenään jaottomia luvun m kanssa ja täten myös tulon mn kanssa.

Rivejä on $\phi(m)$ kappaletta ja jokainen niistä sisältää $\phi(n)$ kokonaislukua, jotka ovat keskenään jaottomia tulon mn kanssa. Siis $\phi(mn) = \phi(m)\phi(n)$.

□

Esimerkki 2.5. Huomautuksen 2.3 ja Lauseen 2.4 nojalla

$$\phi(77) = \phi(7)\phi(11) = (7-1)(11-1) = 6 \cdot 10 = 60$$

Lause 2.6. *Olkoon $p \in \mathbb{P}$. Nyt kaikilla $a \in \mathbb{Z}_{\geq 1}$ pätee*

$$\phi(p^a) = (p-1)p^{a-1}.$$

Todistus. Jos kokonaisluvulle $1 \leq t \leq p^a$ pätee $syt(t,p) \neq 1$, niin kokonaisluku t on alkuluvun p monikerta. Tällöin $t = kp$, missä $1 \leq k \leq p^{a-1}$. Tällasia kokonaislukuja k on tarkalleen p^{a-1} kappaletta. Siis on olemassa

$$p^a - p^{a-1} = (p-1)p^{a-1}$$

kappaletta pienempiä kokaislukuja kuin p^a, jotka ovat keskenään jaottomia luvun p^a kanssa. Täten $\phi(p^a) = (p-1)p^{a-1}$.

□

Seuraus 2.7. *Olkoon $m = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ alkulukuhajotelma. Tällöin*

$$\phi(m) = \prod_{i=1}^{k}(p_i - 1)p_i^{a_i-1}$$

Todistus. Lauseiden 2.4 ja 2.6 nojalla

$$\phi(m) = \phi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}) \overset{l.\,2.4}{=} \prod_{i=1}^{k}\phi(p_i^{a_i}) \overset{l.\,2.6}{=} \prod_{i=1}^{k}(p_i-1)p_i^{a_i-1}$$

□

Esimerkki 2.8. Lasketaan

(a) $\phi(12)$

(b) $\phi(100)$

(c) $\phi(720)$

käyttämällä Seurausta 2.7.

(a) $\phi(12) = \phi(2^2 3) = (2-1)2^{2-1} \cdot (3-1)3^{1-1} = 4$

(b) $\phi(100) = \phi(2^2 5^2) = (2-1)2^{2-1} \cdot (5-1)5^{2-1} = 40$

(c) $\phi(720) = \phi(2^4 3^2 5) = (2-1)2^{4-1} \cdot (3-1)3^{2-1} \cdot (5-1)5^{1-1} = 192$

3 Eulerin lause

Lause 3.1 (Eulerin lause)**.** *Olkoot $a \in \mathbb{Z}$ ja $m \in \mathbb{Z}_+$. Jos kokonaisluvut a ja m ovat keskenään jaottomat, niin $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Todistus. Olkoot $[r_i]$, missä $i = 1, \ldots, t = \phi(m)$, alkuluokat modulo m. Nyt $[ar_1], \ldots, [ar_t]$ ovat alkuluokat modulo m, koska $syt(a, m) = 1$. Oletetaan $[ar_i] = [ar_j]$, missä $i \neq j$. Siten $ar_i \equiv ar_j \pmod{m}$. Koska $syt(a, m) = 1$, niin $[a] \in \mathbb{Z}_m^*$ ja siis tulo $[a][r_i] \in \mathbb{Z}_m^*$. Voidaan supistaa a ja tällöin

$$r_i \equiv r_j \pmod{m},$$

jolloin saadaan ristiriita $[r_i] = [r_j]$.

Koska toisistaan poikkeavat jäännösluokat $[ar_1], \ldots, [ar_t]$ ovat alkuluokkia modulo m ja se sisältää t kappaletta erilaisia luokkia, täytyy päteä

$$\mathbb{Z}_m^* = \{[ar_1], \ldots, [ar_t]\}.$$

Tällöin

$$\prod_{i=1}^{t} [r_i] = \prod_{i=1}^{t} [ar_i] = [a]^{\phi(m)} \prod_{i=1}^{t} [r_i].$$

Koska jäännösluokat $[r_i]$ ovat keskenään jaottomia luvun m kanssa, niin on niiden tulokin. Koska $[a]^{\phi(m)} = [a^{\phi(m)}]$, supistamalla saadaan $[a]^{\phi(m)} = [1]$, jolloin

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

□

Lause 3.2. *Myös Eulerin lauseen käänteinen väite pätee. Olkoot $a \in \mathbb{Z}$ ja $B, m \in \mathbb{Z}_+$. Jos $a^B \equiv 1 \pmod{m}$, niin $syt(a, m) = 1$.*

Todistus. Koska $a^B \equiv 1 \pmod{m}$, kokonaisluku m jakaa luvun $a^B - 1$. Eli on olemassa jokin kokonaisluku k, että

$$a^B - 1 = km \iff a^B - km = 1$$

Tehdään vastaoletus: Jos $syt(a, m) = t > 1$, niin $\begin{cases} a = tc \\ m = td \end{cases}$ jollekin $c, d \in \mathbb{Z}$.

Nyt

$$aa^{B-1} - km = 1$$
$$tca^{B-1} - ktd = 1$$
$$t(ca^{B-1} - kd) = 1$$

Eli t jakaa luvun 1, joten $t = \pm 1$, mikä on ristiriita, koska $t > 1$.
Siispä jos $a^B \equiv 1 \pmod{m}$, niin $syt(a, m) = 1$.

□

Eulerin lause voidaan todistaa myös käyttämällä induktiota, binomilausetta ja joukko-opin käsitteitä. Todistukset käsitellään teoksissa [Burton 2011, s.139] ja [Childs 2009, s.179, s.190].

Eulerin lausetta voidaan käyttää esimerkiksi käänteisarvojen löytämiseen modulo m:

Seuraus 3.3. *Luku $a^{\phi(m)-1}$ on käänteisalkio luvulle $a \pmod{m}$.*

Todistus. Jos a ja m ovat keskenään jaottomia, niin

$$a \cdot a^{\phi(m)-1} = a^{\phi(m)} \equiv 1 \pmod{m}$$

joten Eulerin lauseen perusteella $a^{\phi(m)-1}$ on $a \pmod{m}$ käänteisalkio.

□

Seuraus 3.4. *Kun $m \in \mathbb{P}$, Eulerin lauseesta saadaan erikoistapaus: Fermat'n pieni lause*

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

Todistus. Huomautuksen 2.3 nojalla $\phi(m) = m - 1$. Eulerin lauseen perusteella

$$a^{m-1} = a^{\phi(m)} \equiv 1 \pmod{m}$$

□

Fermat'n pieni lause on hyödyllinen, kun halutaan sieventää kongruensseja modulo p, missä $p \in \mathbb{P}$.

Esimerkki 3.5. Osoitetaan, että

(a) $3^{145} \equiv 3 \pmod{252}$

(b) $10^{70n+8} \equiv 69 \pmod{71}$, missä $n \in \mathbb{N}$.

Nyt

(a) Koska $\phi(252) = 72$, Eulerin lauseen nojalla

$$3^{145} = 3^{2 \cdot 72+1} = (3^{72})^2 \cdot 3 \equiv 1^2 \cdot 3 = 3 \pmod{252}.$$

(b) Koska $\phi(71) = 70$ ja $syt(10, 71) = 1$, niin Eulerin lauseen nojalla

$$10^{70} \equiv 1 \pmod{71}.$$

Siis

$$\begin{aligned} (10^{70})^n \cdot 10^8 &\equiv 1^n \cdot 10^8 = 10^8 = (10^2)^3 && \pmod{71} \\ &= 100^3 \equiv 29^3 = 1276 && \pmod{71} \\ &\equiv 69 && \pmod{71}. \end{aligned}$$

4 Sovelluksia

4.1 RSA

Tämän alikappaleen tiedot ovat pääosin teoksesta [Childs 2009, s.201-205]. Eulerin lause on todettu hyödylliseksi kryptografiassa, sillä se toimii perustana kuuluisalle RSA-menetelmälle. RSA on julkisen avaimen salausalgoritmi, jota käytetään laajasti. RSA allekirjoitusta käytetään varmenteena sivuston turvallisuudesta ja aitoudesta yhteyden muodostamisessa. Sen kehittivät R.L. Rivest, A. Shamir ja L. Adleman vuonna 1977.

RSA:han kuuluu neljä vaihetta: avaimen muodostus, avaimen jakaminen, salaaminen ja salauksen purkaminen. Tarkastellaan esimerkin kautta: Henkilö A haluaa vastaanottaa suojattuja viestejä. Hän valitsee kaksi erittäin suurta alkulukua p ja q ja muodostaa niiden tulon $n = pq$. Henkilö A valitsee myös kokonaisluvun $E < n$ siten, että $syt(E, \phi(n)) = 1$, missä $\phi(n) = (p-1)(q-1)$ on Eulerin ϕ-funktio. Luvulla E voidaan muodostaa salaovifunktio, joka salaa viestin. Hän asettaa kokonaisluvut n ja E julkisiksi. Ne muodostavat avaimen, jolla muut voivat salata viestejä. Salattujen viestien purkamiseksi täytyy tietää alkutekijät p ja q, ja jos ne ovat tarpeeksi suuria, esimerkiksi 150 numeroisia kumpikin, niin tunnetut tekijöihinjakometodit eivät saa selvitettyä lukua n järkevässä ajassa. Prosessi voi viedä jopa 100 vuotta.

RSA:lla salattava viesti voi olla esimerkiksi ketju kirjaimia tai numeroita. Oletetaan, että viesti on ketju kokonaislukuja $T < n$. Henkilö B salaa jokaisen kokonaisluvun T luvuiksi $C \equiv T^E \pmod{n}$ ja lähettää ne henkilölle A. Henkilö A voi nyt purkaa salauksen seuraavasti: Koska hän tietää luvut p ja q, hän voi muodostaa tulon $m = (p-1)(q-1)$ ja ajaa Eukleideen algoritmin parille (E, m) löytääkseen kokonaisluvun D siten, että $DE \equiv 1 \pmod{m}$. Nyt hän ottaa viestin C ja laskee $C^D \pmod{n}$. Tulos on

$$C^D \equiv (T^E)^D = T^{DE} \pmod{n}$$

mutta, koska $DE \equiv 1 \pmod{m}$, Eulerin lauseen perusteella $C^D \equiv T \pmod{n}$. Henkilöllä A on siis alkuperäinen viesti, jonka henkilö B hänelle lähetti. RSA:n hyvä puoli on siinä, että salatun tekstin lähettäminen ei välttämättä vaadi turvallista yhteyttä. Vaikka se siepattaisiin, niin sitä ei voi purkaa ilman annettua avainta.

Turvallisen RSA:sta tekee salaovifunktion yksisuuntaisuus. On helppo laskea tulo $(p-1)(q-1) = \phi(n)$, mutta erittäin suuren luvun n jakaminen alkutekijöihinsä on jopa tietokoneille hyvin hidas prosessi. Koska suurten alkulukujen tietäminen on yksi merkittävä tekijä RSA-salausmenetelmän käyttämisessä, on tärkeä myös kehittää menetelmiä niiden löytämiseksi.

4.2 Jaollisuustesti

Alikappaleen tiedot ovat teoksesta [Childs 2009, s.205-208].

Alkulukujen löytämisestä lähtien matemaatikkoja on kiinnostanut kehittää tapoja löytää niitä lisää. Esimerkiksi suurille luvuille n on tehotonta kokeilla jakamista jokaisella lukua $\sqrt{n}$ pienemmällä luvulla. Fermat'n pieni lause liittyy yhteen yksinkertaisimmista testeistä, joka esitellään tässä.

Fermat'n pienen lauseen mukaan alkuluvun n ollessa keskenään jaoton minkä tahansa kokonaisluvun a kanssa, alkuluku n jakaa luvun $a^{n-1} - 1$. Lauseen käänteinen muoto on seuraavanlainen: Jos kokonaisluku a on keskenään jaoton luvun n kanssa siten, että $a^{n-1} - 1$ ei ole jaollinen luvulla n, niin n ei ole alkuluku. Tästä erikoistapauksena saadaan 2-jaollisuustesti: Jos $2^{n-1} \not\equiv 1 \pmod{n}$, niin n on yhdistetty luku. Esimerkiksi luku 10 on yhdistetty, sillä $2^9 \equiv 2 \neq 1 \pmod{10}$, mutta alkuluvu11a $n = 11$ pätee $2^{10} \equiv 1 \pmod{11}$.

Testi toimii pienillä luvuilla n, joten sitä voidaan käyttää alkulukutestinä lukuun 341 asti. Siitä eteenpäin testin avulla löytyy näennäisalkulukuja, eli yhdistettyjä lukuja n, joille pätee $2^{n-1} \not\equiv 1 \pmod{n}$. 2-jaollisuustestiä ei voi siis käyttää varmana alkulukutestinä, koska esimerkiksi $2^{2700} \equiv 1 \pmod{2701}$, mutta $2701 = 37 \cdot 73$. Voidaan kuitenkin huomata näennäisalkulukujen olevan harvinaisempia verrattuna alkulukuihin, joten testiä voi käyttää todennäköisyyspohjaisena alkulukutestinä. Tutkittaessa jotain satunnaisesti valittua jaollisuustestin toteuttavaa lukua voidaan sanoa sen olevan todennäköisesti alkuluku.

4.3 Minkä luvun viides potenssi?

Eulerin lausetta voi myös käyttää arkisemmassa tilanteessa. Lauseen avulla voi nopeasti selvittää, minkä kaksinumeroisen kokonaisluvun joku toinen on korottanut viidenteen potenssiin, kun hän lausuu sen ääneen laskijalle. Temppu perustuu Eulerin lauseeseen, josta seuraa, että luvun n^5 viimeinen numero on aina sama kuin luvulla n modulo 10. Mille tahansa kokonaisluvulle a pätee

$$a^5 = m \cdot 10 + a, m \in \mathbb{Z}.$$

Esimerkiksi $36^5 = 6046617 \cdot 10 + 6 = 60466176$ ja $12^5 = 24883 \cdot 10 + 2 = 248832$. Jotta laskija voi "laskea"tuloksen nopeasti, hänen täytyy suunnilleen muistaa kymmenten viidensien potenssien rajat, kuten alla olevassa taulukossa, ja kuunnella luku loppuun saadakseen viimeisen numeron.

$10^5 = 100000$	$40^5 = 102400000$	$70^5 = 1680700000$
$20^5 = 3200000$	$50^5 = 312500000$	$80^5 = 3176800000$
$30^5 = 24300000$	$60^5 = 777600000$	$90^5 = 5904900000$

Esimerkkinä tilanne: Päässälaskija A pyytää henkilöä B valitsemaan jonkin kaksinumeroisen luvun ja korottamaan sen viidenteen potenssiin laskimellaan. B valitsee luvun 28, suorittaa laskutoimituksen ja lausuu saamansa vastauksen ääneen A:lle. A on tarkkana tässä vaiheessa lausutun luvun alussa ja lopussa. Hän kuulee luvun 17210368 alun ja tietää heti, että haettu luku on jotain lukujen 20^5 ja 30^5 väliltä, eli B:n valitseman luvun ensimmäisen numeron on oltava 2. Kun A kuulee lausutun luvun 17210368 viimeisen numeron, joka on 8, A voi päätellä nopeasti alkuperäisen luvun olleen 28.

Lähdeluettelo

[Burton 2011] Burton, D. M.: *Elementary Number Theory.* The McGraw-Hill Companies, Inc., Singapore, 2011.

[Childs 2009] Childs, L. N.: *A Concrete Introduction to Higher Algebra.* Springler-Verlag New York, 2009.

[Debnath 2010] Debnath, L.: *Legacy Of Leonhard Euler, The: A Tricentennial Tribute.* London: Imperial College Press. 2010.

[Erickson, Vazzana 2008] Erickson, M.: Vazzana, A.: *Introduction to Number Theory.* Chapman & Hall/CRC, 2008.