MATA227 Lukuteoria

Kesä 2010

Tämä luentomoniste perustuu suurelta osalta Lassi Kuritun perusteelliseen luentomonisteeseen, jota kannattaa lukea mikäli kaipaa todistuksiin lisää yksityiskohtia.

Sisältö

1. Luonnolliset luvut 3
1.1. Lukujärjestelmät 4
1.2. Jaollisuus 6
1.3. Alkuluvuista 7
1.4. Alkulukujen tiheydestä 10
1.5. Fermat'n ja Mersennen luvut 14
1.6. Suurin yhteinen tekijä 15
1.7. Eukleideen algoritmi 16
1.8. Pienin yhteinen jaettava 17
1.9. Lineaarinen Diofantoksen yhtälö 19
2. Lukukongruenssit 20
2.1. Lineaarinen kongruenssiyhtälö 22
2.2. Lukukunnat ja alkuluvut 26
2.3. Eulerin φ-funktio 27
2.4. Eulerin, Fermat'n ja Wilsonin lauseet 32
Nopea potenssilasku 35
2.5. Kiinalainen jäännöslause 37
3. Neliönjäännökset 41
3.1. Resiprookkilause 44
3.2. Jacobin yleistetty symboli 46
4. Alkulukutestausta 47
4.1. Fermat 47
4.2. Legendre-Jacob 47
4.3. Miller-Rabin 48
4.4. Pépin 49
4.5. Lucas 50
4.6. Lucas-Lehmer 50
5. RSA 54
5.1. Viestin salaaminen 55
5.2. Viestin purkaminen 56
6. Luonnollisten lukujen esitykset summina 56
6.1. Neliöiden summista 56
6.2. Goldbachin konjektuuri 61
6.3. Muita ratkaisemattomia ongelmia 62
7. Korkeamman asteen kongruenssiyhtälöt 64

1. Luonnolliset luvut

Lukuteorialla tarkoitetaan yleensä oppia luonnollisista luvuista. Myös tällä kurssilla lukuteoria ymmärretään juuri luonnollisten lukujen (ja kokonaislukujen) teoriaksi. Palautetaan ensin mieleen mitä luonnollisilla luvuilla tarkoitetaan. Eräs standardi tapa määritellä luonnolliset luvut on seuraava joukko-opillinen konstruktio.

Määritelmä 1.1. Asetetaan $0 := \emptyset = \{\}$ ja määritellään jokaiselle joukolle A seuraaja $S(A) := A \cup \{A\}$. Luonnollisten lukujen joukko $\mathbb{N}$ voidaan antaa nyt leikkauksena

$$\mathbb{N} = \bigcap_{\mathcal{A}} \mathcal{A},$$

missä leikkaus otetaan kaikkien niiden joukkoperheiden $\mathcal{A}$ yli jotka sisältävät joukon 0 ja ovat suljettuja seuraajafunktion S suhteen, eli $A \in \mathcal{A} \Rightarrow S(A) \in \mathcal{A}$.

Tämän määritelmän mukaisesti luonnolliset luvut ovat siis

$$\begin{aligned}
0 &= \emptyset \\
1 &= \{\emptyset\} \\
2 &= \{\emptyset, \{\emptyset\}\} \\
3 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
&\vdots
\end{aligned}$$

ja luonnollisten lukujen järjestys voidaan määritellä inkluusion avulla $a \leq b :\Leftrightarrow a \subset b$. Tärkeä luonnollisten lukujen ominaisuus on induktio:

Lause 1.2. *Olkoon $A \subset \mathbb{N}$. Jos $0 \in A$ ja kaikilla $n \in A$ myös $n+1 \in A$, on $A = \mathbb{N}$.*

Todistus. Joukon A määritelmän perusteella $A \subset \mathbb{N}$. Toisaalta $0 \in A$ ja A on suljettu seuraajafunktion S suhteen, ja siten $\mathbb{N} \subset A$. Siispä $A = \mathbb{N}$. □

Luonnolliset luvut voidaan määritellä myös siten, että Lause 1.2 on suoraan tässä muodossa yksi aksioomista. Siksi sitä kutsutaankin *induktioaksioomaksi*. Induktioaksiooman kanssa yhtäpitävä oletus, joka tässä muotoillaan lauseena, on pienimmän alkion olemassaolo.

Esimerkki 1.3. Osoitetaan induktiolla, että $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} < 2\sqrt{n}$ kaikilla $n \in \mathbb{N}$, $n > 0$.

n=1: $\frac{1}{\sqrt{1}} = 1 < 2 = 2\sqrt{1}$.

induktioaskel: Oletetaan, että $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} < 2\sqrt{n}$ jollain $n \in \mathbb{N}$. Nyt

$$\begin{aligned}\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} &= \sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{n+1}} < 2\sqrt{n} + \frac{1}{\sqrt{n+1}} \\ &= \frac{2\sqrt{n(n+1)}+1}{\sqrt{n+1}} \leq \frac{\sqrt{4n^2+4n+1}+1}{\sqrt{n+1}} \\ &= \frac{2n+1+1}{\sqrt{n+1}} = 2\sqrt{n+1}.\end{aligned}$$

Lause 1.4. *Jokaisessa luonnollisten lukujen epätyhjässä osajoukossa on pienin luku.*

Todistus. (Harjoitustehtävä) □

Kokonaislukujen joukko $\mathbb{Z}$ voidaan määritellä luonnollisista luvuista esimerkiksi seuraavasti.

Määritelmä 1.5. Kokonaislukujen joukko on tekijäjoukko

$$\mathbb{Z} := \{(a,b) : a,b \in \mathbb{N}\}/\sim$$

ekvivalenssirelaatiolla $(a,b) \sim (c,d) :\Leftrightarrow a+d = b+c$.

Tässä määritelmässä siis järjestetyt lukuparit (a,b) sisältävät positiivisen osan a ja negatiivisen osan b ja ekvivalenssiluokka $[(a,b)] \in \mathbb{Z}$ ymmärretään kokonaislukuna $a-b$.

1.1. **Lukujärjestelmät.** Aloitetaan varsinainen lukuteoria ns. jakoyhtälöllä, jota tulemme jatkossa toistuvasti käyttämään.

Lause 1.6. *Jos $a,b \in \mathbb{Z}$ ja $b > 0$, on olemassa yksikäsitteiset luvut $q,r \in \mathbb{Z}$ siten, että $0 \leq r < b$ ja*

$$a = qb + r.$$

Todistus. Olkoon $A = \{a - qb : q \in \mathbb{Z}, a - qb \geq 0\} \subset \mathbb{N}$. Koska

$$0 \leq |a|(b-1) \leq a - (-|a|)b \in A$$

eli A on epätyhjä, on olemassa joukon A pienin luku. Olkoon se r ja olkoon $q \in \mathbb{Z}$ siten, että $r = a - qb$. Tällöin $r < b$, sillä muuten

$$0 \leq r' = a - (q+1)b = r - b \in A$$

eli r ei olisikaan pienin joukon A luku.

Jos $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $1 \leq r_1, r_2 < b$ ja $a = q_1 b + r_1 = q_2 b + r_2$, on

$$|q_1 - q_2||b| = |r_1 - r_1| < |b|,$$

mikä on mahdollista vain silloin kun $q_1 = q_2$, jolloin myös $r_1 = r_2$. □

Lauseen 1.6 luku q on luvun a osamäärä luvun b suhteen, ja luku r on luvun a jakojäännös luvun b suhteen.

Lauseen 1.6 avulla nähdään, että luonnolliset luvut voidaan esittää yksikäsitteisesti missä tahansa m-kantaisessa lukujärjestelmässä, kun $m \geq 2$.

Lause 1.7. *Olkoon $m, n \in \mathbb{N}$ siten, että $m \geq 2$ ja $n \geq 1$. Tällöin on olemassa $k \in \mathbb{N}$ ja luvut $a_0, a_1, \ldots, a_k \in \mathbb{N}$ siten, että*

$$0 \leq a_i < m \text{ kaikilla } i,$$

$$a_k \geq 1$$

ja

$$n = \sum_{i=0}^{k} a_i m^i.$$

Lisäksi summaesitys on yksikäsitteinen.

Todistus. Lauseen 1.6 mukaan on olemassa yksikäsitteiset luvut $a_0, n_0 \in \mathbb{Z}$ siten, että $0 \leq a_0 < m$ ja

$$n = n_0 m + a_0.$$

Lisäksi täytyy olla $n_0 \geq 0$, sillä jos näin ei olisi saataisiin

$$n \leq -m + a_0 < 0.$$

Jos $n_0 = 0$, on $k = 0$ ja luvut a_i on löydetty. Oletetaan nyt, että luvut $0 \leq a_0, \ldots, a_j < m$ ja $n_0, \ldots, n_{j-1} \geq 1$, $n_j \geq 0$, on määritelty siten, että

$$n_{i-1} = n_i m + a_i$$

kaikille $i = 1, \ldots, j$. Jos vieläkin $a_j \geq 1$, saadaan Lauseen 1.6 avulla $0 \leq a_{j+1} < m$ ja $n_{k+1} \geq 0$ siten, että

$$n_j = n_{j+1} m + a_{j+1}.$$

Koska $n \in \mathbb{N}$, on olemassa $k \in \mathbb{N}$, siten, että edellisellä induktiivisella määrittelyllä $n_k = 0$. Nyt

$$n = n_0 m + a_0 = n_0 m^1 + \sum_{i=0}^{0} a_i m^i.$$

Oletetaan, että

$$n = n_j m^{j+1} + \sum_{i=0}^{j} a_i m^i$$

jollain $j \in \{0, \ldots, k-1\}$. Tällöin

$$n = (n_{j+1} m + a_{j+1}) m^{j+1} + \sum_{i=0}^{j} a_i m^i = n_{j+1} m^{j+2} + \sum_{i=0}^{j+1} a_i m^i.$$

Siten erityisesti

$$n = n_k m^{k+1} + \sum_{i=0}^{k} a_i m^i = \sum_{i=0}^{k} a_i m^i.$$

Koska $a_j m^j$ on luvun

$$n - \sum_{i=0}^{j-1} a_i m^i$$

jakojäännös luvun m^{j+1} suhteen, on se Lauseen 1.6 mukaan yksikäsitteinen kun $j = 0$ ja siten myös kun $j = 1, 2, \ldots, k$. □

Esimerkki 1.8. Luvun 51 esitys 3-kantaisessa lukujärjestelmässä on

$$51 = 0 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + 1 \cdot 3^3.$$

Käytetty lukujärjestelmä kirjoitetaan usein alaindeksiin. Tällöin edellinen yhtälö saa muodon

$$51_{10} = 1220_3.$$

1.2. **Jaollisuus.**

Määritelmä 1.9. Olkoot $a, b \in \mathbb{Z}$, $b \neq 0$. Luku a on jaollinen luvulla b, $b \mid a$, jos on olemassa luku $q \in \mathbb{Z}$ siten, että $a = qb$.

Luku a on siis jaollinen luvulla $b \neq 0$ täsmälleen silloin kun luvun a jakojäännös luvun b suhteen on 0.

Merkinnällä $b \nmid a$ tarkoitetaan, että $b \mid a$ ei ole totta. Edellisen määritelmän mukaan on $1 \mid a$ totta kaikille $a \in \mathbb{Z}$ ja lisäksi $a \mid a$ kaikille $a \in \mathbb{Z} \setminus \{0\}$. Selvästi myös

(i) $b \mid a$ ja $c \mid b \Rightarrow c \mid a$,
(ii) $c \neq 0$ ja $b \mid a \Rightarrow bc \mid ac$ ja
(iii) $c \mid a$, $c \mid b$ ja $m, n \in \mathbb{Z} \Rightarrow c \mid ma + nb$.

Määritelmä 1.10. Luku $n \in \mathbb{N}$, $n > 1$, on alkuluku, jos se ei ole jaollinen millään luvulla $m \in \mathbb{N}$, jolle $1 < m < n$.

Lause 1.11. *Jokainen $n \in \mathbb{N}$, $n > 1$ on alkulukujen tulo.*

Todistus. Joko n on itse alkuluku (jolloin todistus on jo valmis) tai sillä on jokin jakaja $m \in \mathbb{N}$, $1 < m < n$. Olkoon p_1 pienin luvun n jakaja, jolle $1 < p_1 < m$. Tällöin p_1 on alkuluku, sillä muuten olisi olemassa $k \in \mathbb{N}$, $1 < k < p_1$ siten, että $k \mid p_1$ ja edelleen $k \mid n$. Siis $n = p_1 n_1$ jollain luonnollisella luvulla $1 < n_1 < n$.

Joko n_1 on alkuluku (jolloin todistus on valmis) tai sillä on edellisen päättelyn perusteella alkulukutekijä p_2 ja tällöin $n_1 = p_2 n_2$, missä $1 < n_2 < n_1$. Jatkamalla tätä saamme aidosti vähenevän jonon luonnollisia lukuja $n_1 > n_2 > n_3 \ldots$. Jonkin äärellisen määrän l askeleita jälkeen

törmäämme välttämättä alkulukuun $n_l = p_{l+1}$, jolloin alkuperäinen luku voidaan kirjoittaa muodossa

$$n = p_1 p_2 \cdots p_{l+1}.$$

□

Huomaa, että äskeinen todistus ei osoita, että esitys $p_1 p_2 \cdots p_{l+1}$ olisi (permutaatioita vaille) yksikäsitteinen. Tämä on kuitenkin totta.

Lause 1.12 (Aritmetiikan peruslause)**.** *Jokainen luku $n \in \mathbb{N}$, $n > 1$, voidaan kirjoittaa yksikäsitteisesti tulona*

$$n = p_l^{a_l} p_l^{a_l} \cdots p_l^{a_l},$$

missä $p_1 < p_2 < \cdots < p_l$ ovat alkulukuja ja $a_1, a_2, \ldots, a_l > 0$ luonnollisia lukuja.

Lause 1.12 seuraa seuraavasta lauseesta, joka todistetaan hieman myöhemmin.

Lause 1.13 (Eukleideen ensimmäinen lause)**.** *Jos p on alkuluku ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

Lauseen 1.12 todistus olettaen Lause 1.13. Lauseesta 1.13 seuraa selvästi, että jokaiselle alkuluvulle p pätee

$$p \mid a_1 a_2 \cdots a_n \Rightarrow p \mid a_i \text{ jollain } i \in \{1, 2, \ldots, n\}.$$

Olkoon nyt

$$n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l} = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k},$$

missä $(p_i)_{i=1}^l$ ja $(q_i)_{i=1}^k$ ovat aidosti kasvavia alkulukujonoja, ja $a_i, b_i > 0$ luonnollisia lukuja. Koska $p_i \mid q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$ kaikilla i ja vastaavasti $q_i \mid p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ kaikilla i, ovat luvut p_i ja q_i samat.

Vielä tulee osoittaa, että kertaluvuille pätee $a_i = b_i$ kaikilla i. Oletetaan, että on olemassa jokin j siten, että $a_j > b_j$. Jakamalla n luvulla b_j saadaan

$$p_1^{a_1} p_2^{a_2} \cdots p_j^{a_j - b_j} \cdots p_l^{a_l} = p_1^{b_1} p_2^{b_2} \cdots p_{j-1}^{b_{j-1}} p_{j+1}^{b_{j+1}} \cdots p_l^{b_l},$$

jossa siis vasen puoli on jaollinen luvulla p_j, mutta oikea puoli ei. Vastaavasti $b_j > a_j$ johtaa ristiriitaan. □

1.3. **Alkuluvuista.** Edellä esitetyn Aritmetiikan peruslauseen mukaan jokainen ykköstä suurempi luonnollinen luku voidaan esittää yksikäsitteisesti alkulukujen tulona. Kun annettu luonnollinen luku on hyvin suuri, voi tämän tuloesityksen löytäminen olla erittäin vaikeata - jopa lähes mahdotonta. "Aritmetiikan perusongelmana" voidaankin pitää luonnollisten lukujen tekijöihin jakoa. Ongelma liittyy hyvin läheisesti nykymaailmaan, sillä esimerkiksi useimmat käytössä olevat salausmenetelmät perustuvat juuri alkulukutekijöihin jakamisen vaikeuteen.

Alkulukujen listaa voi lähteä muodostamaan pienehköön rajaan asti käyttämällä niin sanottua **Eratostheneen seulaa**: Kaikki välin $[2, N]$

alkuluvut saadaan pyyhkimällä jonosta $2, 3, 4, \ldots, N$ ensin kaikki alkuluvun $p_1 = 2$ monikerrat $(4, 6, 8, 10, \ldots)$, tämän jälkeen kaikki jäljelle jääneet alkuluvun $p_2 = 3$ monikerrat $(9, 15, 21, \ldots)$ ja niin edelleen. Lopulta jäljelle jäävät vain alkuluvut. Seulomista ei itse asiassa tarvitse jatkaa kovin pitkälle, kuten näemme seuraavasta lauseesta.

Lause 1.14. *Olkoon $n \in \mathbb{N}$, $n > 1$. Mikäli n ei ole alkuluku, on sillä olemassa alkulukutekijä p, jolle $1 < p \leq \sqrt{n}$.*

Todistus. Jos $p > 1$ on luvun n pienin alkulukutekijä, on $a = pq$, missä välttämättä $p \leq q$. Siten $p^2 \leq pq = a$. □

Esimerkki 1.15. Etsitään Eratostheneen seulalla alkuluvut väliltä $[2, 100]$. Listataan siis ensin luvut kahdesta sataan.

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

Tämän jälkeen poistetaan kaikki luvun 2 monikerrat.

	2	3	5	7	9	11	13	15	17	19
21		23	25	27	29	31	33	35	37	39
41		43	45	47	49	51	53	55	57	59
61		63	65	67	69	71	73	75	77	79
81		83	85	87	89	91	93	95	97	99

Seuraavaksi poistetaan luvun 3 monikerrat.

	2	3	5	7		11	13		17	19
		23	25		29	31		35	37	
41		43		47	49		53	55		59
61			65	67		71	73		77	79
		83	85		89	91		95	97	

Tämän jälkeen luvun 5 monikerrat.

	2	3	5	7		11	13		17	19
		23			29	31			37	
41		43		47	49		53			59
61				67		71	73		77	79
		83			89	91			97	

Lopuksi vielä luvun 7 monikerrat.

	2	3	5	7		11	13		17	19
		23			29	31			37	
41		43		47			53			59
61				67		71	73			79
		83			89				97	

Koska 7 on suurin lukua $10 = \sqrt{100}$ pienempi alkuluku, on seulominen saatu päätökseen ja jäljelle ovat jääneet alkuluvut väliltä $[2, 100]$.

Vaikka Eratostheneen seula onkin tehoton tapa etsiä alkulukutekijöitä ei se kuitenkaan ole hyödytön. Jos esimerkiksi tietokoneohjelmassa tarvitsemme listan alkuluvuista vaikkapa väliltä kahdesta miljoonaan,

on järkevämpää laskea lista suoraan muistiin kuin lukea se kovalevyltä. Ongelma ei niinkään ole algoritmin nopeus vaan sen muistintarve.

Tällä hetkellä noin 200-numeroisten luonnollisten lukujen jako alkutekijöihin onnistuu järkevässä ajassa. Yleisen luvun (joka siis ei ole mitään erityistä muotoa, kuten $2^{2^m}+1$) tekijöihinjaossa käytetään tyypillisesti useita erilaisia algoritmejä. Ensin testataan onko luku alkuluku vai ei. Tämän testaaminen on yleensä nopeampaa kuin alkulukutekijöiden etsiminen. Mikäli luku ei ole alkuluku etsitään sille ensin hyvin pieniä tekijöitä kokeilemalla (tässä Eratostheneen seulasta voi olla hyötyä).

Mikäli tekijä löytyy, testataan onko jäljelle jäänyt osa alkuluku. Jos se ei ole, jatketaan pienten tekijöiden etsimistä. Kun tätä on jonkin aikaa järjestelmällisesti jatkettu, tiedetään ettei jäljelle jääneellä luvulla ole kovin pieniä tekijöitä ja on järkevämpää vaihtaa joihinkin toisiin etsintämenetelmiin, kuten Pollardin $p-1$ -menetelmään, Williamsin $p+1$ -menetelmään ja Lenstran elliptisten käyrien menetelmään. Näille menetelmille määritellään rajat, jotka määräävät etsittävän alkulukutekijän koon. Kyseiset menetelmät eivät välttämättä löydä tekijöitä, mutta riittävä määrä yrityksiä eri alkuarvoilla takaa että todennäköisyys löytää tekijä on sopivaa kokoluokkaa. Esimerkiksi etsittäessä elliptisten käyrien menetelmällä 50-numeroista tekijää sopivilla parametreillä, on noin 8 000 "epäonnistuneen" käyrän jälkeen todennäköisyys sille, että luvulla on alle 50-numeroinen tekijä enää 37%. (Yhden testin laskemiseen menee kotikoneella noin 5 min.)

Jos näilläkään menetelmillä ei löydetä kaikkia alkulukutekijöitä (järkevässä ajassa), vaihdetaan jälleen "järeämpään" algoritmiin, kuten GNFS (General Number Field Sieve). Tällä löydetään alkulukutekijät, mutta algoritmin vaativuus riippuu nyt enemmän sen luvun suuruudesta jonka tekijöitä etsitään (edellisten algoritmien vaativuus riippui lähinnä etsityn tekijän koosta). Siksi sitä ei ole järkevää käyttää heti ensimmäisenä menetelmänä, vaan vasta sen jälkeen kun tiedetään hyvin suurella todennäköisyydellä ettei luvulla ole pieniä tekijöitä.

Tällä kurssilla emme perehdy edellä mainittujen algoritmien toimintaan. On kuitenkin mielenkiintoista huomata, että edellä mainitut menetelmät (GNFS:n loppuosan lineaarialgebraa lukuun ottamatta) voidaan suorittaa pienissä toisistaan riippumattomissa palasissa. Siksi tekijöihinjako onkin viime aikoina hyötynyt erityisesti massatuotannossa olevista moniytimisistä laitteista kuten ohjelmoitavista näytönohjaimista ja pelikonsoleista.

Palataanpa tämän pienen sivuraiteen jälkeen takaisin varsinaiseen asiaan...

Lause 1.16 (Eukleideen toinen lause)**.** *Alkulukuja on äärettömän paljon.*

Todistus. Oletetaan, että alkulukuja on äärellinen määrä ja ne ovat $p_1 = 2 < p_2 = 3 < \cdots < p_k$. Olkoon $n = p_1 p_2 \cdots p_k + 1 > p_k$. Koska kaikilla i on luvun n jakojäännös luvun p_i suhteen 1, ei mikään alkuluvuista p_i jaa lukua n. Siten se on itse alkuluku. Tämä on ristiriidassa oletuksen kanssa. □

Huomaa, että edellä olleella lauseella ei voida tuottaa alkulukuja.

Lauseen 1.16 todistusta muuttelemalla saadaan monenlaisia tuloksia. Tässä eräs niistä.

Lause 1.17. *On olemassa äärettömän monta alkulukua jotka ovat muotoa $4m + 3$, missä $m \in \mathbb{N}$.*

Todistus. Olkoon k ensimmäistä alkulukua $2, 3, \ldots, p_k$ ja määritellään luku $n = 2^2 \cdot 3 \cdots p_k - 1$. Nyt n ei ole jaollinen millään luvuista $2, 3, \ldots, p_k$. Jos n on muotoa $4m + 1$ olevien alkulukujen tulo, on se myös itse muotoa $4m + 1$. Näin ei kuitenkaan ole, sillä luvun n jakojäännös luvun 4 suhteen on 3. Siispä on olemassa lukua p_k suurempi alkuluku, joka on muotoa $4m + 3$. □

Paljon yleisempikin lause on totta:

Lause 1.18 (Dirichlet'n lause)**.** *Olkoot $a, b \in \mathbb{Z}$, $a > 0$, siten, että luvuilla a ja b ei ole muita yhteisiä jakajia kuin 1. Tällöin on olemassa äärettömän monta alkulukua, jotka ovat muotoa $am + b$, missä $m \in \mathbb{N}$.*

Lauseen 1.18 todistus on tämän kurssin ulottumattomissa.

1.4. **Alkulukujen tiheydestä.** Alkulukujen lukumäärää välillä $[1, x]$, $1 < x \in \mathbb{R}$, merkitään

$$\pi(x) = \#\{p \in \mathbb{N} : 1 \leq p \leq x \text{ on alkuluku}\}.$$

Siis Esimerkin 1.15 mukaan on esimerkiksi $\pi(100) = 25$. Lauseen 1.16 mukaan taas $\pi(x) \to \infty$, kun $x \to \infty$. Funktion π asymptoottinen käyttäytyminen tiedetään paljon tarkemminkin. Vuonna 1848 Chebychev todisti seuraavan tuloksen.

Lause 1.19. *On olemassa vakiot $0 < A_1, A_2 < \infty$ siten, että*

$$A_1 \frac{x}{\log x} < \pi(x) < A_2 \frac{x}{\log x}$$

kaikille $x \geq 2$.

Todistetaan tämä joillakin vakioilla A_1 ja A_2 jotka eivät ole lähelläkään optimaalisia. Todistus perustuu binomikertoimien ominaisuuksiin, joten aloitetaan ensin määrittelemällä ne.

Määritelmä 1.20. Olkoot $n, k \in \mathbb{N}$ siten, että $k \leq n$. Tällöin binomikerroin $\binom{n}{k}$ määritellään

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Tässä (kuten yleensäkin) määritellään $0! = 1$. Luku $\binom{n}{k}$ kuvaa erilaisten n alkioisen joukon k alkioisten osajoukkojen lukumäärää.

Lemma 1.21. *Kaikille $1 \leq k \leq n$ on*

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Todistus. (Harjoitustehtävä) □

Lause 1.22 (binomikaava)**.** *Kaikille $x, y \in \mathbb{R}$ ja $n \in \mathbb{N}$ on*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Todistus. (Harjoitustehtävä) □

Sijoittamalla Lauseeseen 1.22 $x = y = 1$ saadaan $2^n = \sum_{k=0}^{n} \binom{n}{k}$. Erityisesti saadaan arvio

$$\binom{n}{k} \leq 2^n.$$

Lause 1.23 (Stirlingin approksimaatio)**.**

$$\lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}(n/e)^n} = 1.$$

käydään nyt varsinaisen todistuksen kimppuun osoittamalle ensin seuraava aputulos.

Lemma 1.24. *Kaikille $n \in \mathbb{N}$, $n \geq 1$ on voimassa*

(i) $n^{\pi(2n)-\pi(n)} < \binom{2n}{n} \leq (2n)^{\pi(2n)}$.

(ii) $2^n \leq \binom{2n}{n} \leq 2^{2n}$.

Todistus. Olkoon p alkuluku ja e_p suurin kokonaisluku, jolle $p^{e_p} \mid n!$. Merkitään luvulla t_p pienintä sellaista kokonaislukua, jolle $p^{t_p+1} > n$. Merkitään lisäksi $\lfloor a \rfloor$ suurinta kokonaislukua, jolle $\lfloor a \rfloor \leq a$. Nyt

$$e_p = \sum_{i=1}^{t_p} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

(Tämän todistus jätetään harjoitustehtäväksi.) Olkoon m_p suurin kokonaisluku, jolle $p^{m_p} \mid \binom{2n}{n}$. Koska

$$\binom{2n}{n} = \frac{(2n)!}{n!n!},$$

on

$$m_p = \sum_{i=1}^{k_p} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right),$$

missä k_p on pienin kokonaisluku, jolle $p^{k_p+1} > 2n$. Jos $1 \leq i \leq k_p$, on

$$\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor < \frac{2n}{p^i} - 2\left(\frac{n}{p^i} - 1\right) = 2.$$

Siten näille i on

$$\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \leq 1$$

eli $m_p \leq k_p$. Siispä

$$\binom{2n}{n} \Big| \prod_{p \leq 2n} p^{k_p},$$

missä tulo siis otetaan kaikkien lukua $2n+1$ pienempien alkulukujen yli. Tästä saadaan edelleen

$$\binom{2n}{n} \leq \prod_{p \leq 2n} p^{k_p} \leq \prod_{p \leq 2n} (2n) = (2n)^{\pi(2n)}.$$

Kohdan (i) toinen epäyhtälö on siis todistettu.

Jos alkuluvulle p on $n < p \leq 2n$, on $p \mid (2n)!$ mutta $p \nmid n!$. Siten

$$\prod_{n < p \leq 2n} p \Big| \binom{2n}{n}$$

ja edelleen

$$\binom{2n}{n} \geq \prod_{n < p \leq 2n} p > \prod_{n < p \leq 2n} n = n^{\pi(2n) - \pi(n)},$$

joten kohdan (i) ensimmäinenkin epäyhtälö on todistettu.

Kohdan (ii) epäyhtälöt saadaan laskemalla

$$\binom{2n}{n} \leq (1+1)^{2n} = 2^{2n}$$

ja

$$\binom{2n}{n} = \prod_{j=1}^{n} \frac{n+j}{j} \geq \prod_{j=1}^{n} 2 = 2^n.$$

□

Lauseen 1.19 todistus. Olkoon $x \geq 2$ ja $n \in \mathbb{N}$ siten, että

$$2n \leq x < 2n+2.$$

Yhdistämällä Lemman 1.24 kohdat (i) ja (ii) saadaan arviot

$$\pi(2n) - \pi(n) \leq \frac{2n \log 2}{\log n}$$

ja

$$\pi(2n) \geq \frac{n \log 2}{\log(2n)}.$$

Näistä jälkimmäisestä saadaan siis

$$\pi(x) \geq \pi(2n) \geq \frac{n \log 2}{\log(2n)} \geq \frac{n \log 2}{\log(x)} \geq \frac{(n2+2)\log 2}{4 \log(x)} > \frac{\log 2}{4} \frac{x}{\log x}.$$

Osoitetaan nyt arvio toiseen suuntaan. Tutkitaan ensin lukua $\pi(2^t)$, missä $t \in \mathbb{N}$, $t \geq 3$. Tälle on

$$\pi(2^t) - \pi(2^{t-1}) \leq \frac{2^t \log 2}{(t-1)\log 2} = \frac{2^t}{t-1}.$$

Koska $\pi(4) \leq 4 = \frac{2^2}{2-1}$, saadaan teleskooppisummaa käyttäen

$$\begin{aligned}
\pi(2^{2j}) &= \pi(4) + \sum_{t=3}^{2j} (\pi(2^t) - \pi(2^{t-1})) \leq \sum_{t=2}^{2j} \frac{2^t}{t-1} \\
&\leq \sum_{t=2}^{j} \frac{2^t}{t-1} + \sum_{t=j+1}^{2j} \frac{2^t}{t-1} \leq \sum_{t=2}^{j} 2^t + \sum_{t=j+1}^{2j} \frac{2^t}{j} \\
&= 2^{j+1} + \frac{1}{j} 2^{2j+1}.
\end{aligned}$$

Koska $j < 2^j$, on $2^{j+1} < \frac{2^{2j+1}}{j}$, ja siten kaikille $j \geq 2$ on

$$\pi(2^{2j}) < \frac{2^{2j+2}}{j}.$$

Olkoon $x > 4$ Valitaan nyt $j \in \mathbb{N}$, $j \geq 2$ siten, että $2^{2j-2} < x \leq 2^{2j}$. Tällöin

$$\log x \leq 2j \log 2$$

ja siten

$$\pi(x) \leq \frac{x}{2^{2j-2}} \pi(2^{2j}) < \frac{x}{2^{2j-2}} \frac{2^{2j+2}}{j} = 2^4 \frac{x}{j} \leq 2^5 \log 2 \frac{x}{\log x}.$$

□

Todistuksen vakiot $A_1 = \frac{\log 2}{4}$ ja $A_2 = 32 \log 2$ ovat hyvin karkeat. Chebychevin todistuksessakin nämä olivat jo paremmat $A_1 \approx 0,922$ ja $A_2 \approx 1,105$. Chebychevin tulosta asymptoottisesti tarkempi on ns. **alkulukulause**, jonka mukaan

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

Tätä emme kuitenkaan todista tällä kurssilla.

1.5. **Fermat'n ja Mersennen luvut.** Fermat'n luvuiksi sanotaan lukuja

$$F_m = 2^{2^m} + 1, \qquad m \in \mathbb{N}.$$

Luvut saivat nimensä Pierre de Fermat'n konjektuurista, jonka mukaan kaikki tätä muotoa olevat luvut olisivat alkulukuja. Luvut F_1, F_2, F_3 ja F_4 ovatkin alkulukuja. Euler kuitenkin osoitti jo vuonna 1732, että $F_5 = 641 \cdot 6700417$ eli F_5 ei ole alkuluku. Itse asiassa muita Fermat'n lukuja jotka olisivat alkulukuja ei tunneta.

Tällä hetkellä tiedetään 243 Fermat'n lukua jotka eivät ole alkulukuja. Fermat'n lukujen muodosta huomaa, että pienilläkin m luku F_m on erittäin suuri. Siksi Fermat'n lukujen todistaminen alkuluvuiksi on hyvin vaikeata. Ensimmäinen Fermat'n luku, josta ei tiedetä onko se alkuluku vai ei on F_{33}. Siinä on kymmenlukujärjestelmässä yli 2 miljardia numeroa. Pienin Fermat'n luku jonka kaikkia tekijöitä ei tunneta on F_{12} ja pienin jolle ei tunneta yhtään alkulukutekijää on F_{20}.

Näistä luvuista ei tietenkään voida päätellä onko olemassa muita Fermat'n lukuja jotka ovat alkulukuja. Tällaisia alkulukuja voisi olla vaikka äärettömän monta. Seuraava lause osoittaa, että Fermat'n luvut eivät ole niin erikoisia kuin miltä ne ensisilmäyksellä näyttävät.

Lause 1.25. *Jos $a \geq 2$ ja $a^n + 1$ on alkuluku, on tällöin välttämättä a parillinen ja $n = 2^m$ jollain $m \in \mathbb{N}$.*

Todistus. Jos a on pariton, on $a^n + 1$ parillinen. Jos taas luvulla n on pariton tekijä k ja $n = kl$, on

$$\frac{a^{kl} + 1}{a^l + 1} = a^{(k-1)l} - a^{(k-2)l} + \cdots + 1 > 1$$

luvun $a^n + 1$ jakaja. □

Lauseen 1.25 perusteella siis kaikki muotoa $2^n + 1$ olevat alkuluvut ovat välttämättä Fermat'n lukuja. Jos $a > 2$ on parillinen sanotaan muotoa $a^{2^m} + 1$ olevaa lukua yleistetyksi Fermat'n luvuksi. Entäpä muotoa $a^n - 1$ olevat luvut. Seuraava lause vähentää huomattavasti tätä muotoa olevia alkulukukandidaatteja.

Lause 1.26. *Jos $n > 1$ ja $a^n - 1$ on alkuluku, on tällöin välttämättä $a = 2$ ja n alkuluku.*

Todistus. Jos $a > 2$, niin $a - 1 \mid a^n - 1$. Jos taas $a = 2$ ja $n = kl$, niin $2^k - 1 \mid 2^n - 1$. □

Lukuja $M_p = 2^p - 1$, missä p on alkuluku, kutsutaan Mersennen luvuiksi Marin Mersennen mukaan, joka tutki kyseisiä lukuja 1600-luvulla. Mersennen luvuille on olemassa huomattavan nopea Lucasin-Lehmerin testi, jolla saadaan pääteltyä onko luku alkuluku vai ei. Tällä hetkellä tiedetään 47 Mersennen alkulukua, joista suurin on $M_{43112609}$, jossa on noin 13 miljoonaa numeroa kymmenjärjestelmässä. Mersennen

lukujen "helpon" testattavuuden takia tällä hetkellä yhdeksän suurinta alkulukua ovat Mersennen alkulukuja.

1.6. **Suurin yhteinen tekijä.** Palautetaan mieleen ryhmän määritelmä. Olkoon G epätyhjä joukko. Pari $(G, \circ)$ on ryhmä, jos se täyttää seuraavat ehdot

(G0) $\circ$ on joukossa G määritelty laskutoimitus eli $a \circ b \in G$ kaikilla $a, b, \in G$.
(G1) $(a \circ b) \circ c = a \circ (b \circ c)$ kaikilla $a, b, c \in G$.
(G2) On olemassa *neutraalialkio* $e \in G$ jolle $e \circ a = a \circ e = a$ kaikilla $a \in G$.
(G3) Jokaista $a \in G$ kohti on olemassa *käänteisalkio* $a^{-1} \in G$ jolle $a^{-1} \circ a = a \circ a^{-1} = e$.

Ryhmää $(G, \circ)$ sanotaan kommutatiiviseksi ryhmäksi eli Abelin ryhmäksi, jos se lisäksi toteuttaa ehdon

(G4) $a \circ b = b \circ a$ kaikilla $a, b, \in G$.

Esimerkiksi kokonaislukujen joukko yhteenlaskulla varustettuna $(\mathbb{Z}, +)$ on Abelin ryhmä.

Lause 1.27. *Jokaisella ryhmän $(\mathbb{Z}, +)$ aliryhmällä M on luku $0 \leq d \in M$ siten, että $M = \mathbb{Z}d = \{nd \in \mathbb{Z} : n \in \mathbb{Z}\}$.*

Todistus. Jos $M = \{0\}$, niin $d = 0 \in M$, sillä $M = \mathbb{Z}0$. Jos $M \neq \{0\}$, on $S = \{x \in M : x > 0\} \neq \emptyset$ ja siten on olemassa $d = \min S \in M$. Jokaisella $a \in M$ on Lauseen 1.6 nojalla $q, r \in \mathbb{Z}$ siten, että

$$a = qd + r, \qquad 0 \leq r < d.$$

Koska $r = a - qd \in M$ ja $0 \leq r < d$ on luvun d valinnan nojalla $r = 0$. Siis $a = qd \in \mathbb{Z}d$. Toisaalta koska M on ryhmä, on $\mathbb{Z}d \subset M$ ja siten $M = \mathbb{Z}d$. □

Lauseen 1.27 antamaa lukua d sanotaan aliryhmän M *virittäjäksi*. Joukon $S \in \mathbb{Z}$ virittämää aliryhmää merkitään

$$\langle S \rangle = \{k_1 a_1 + \cdots + k_n a_n : a_1, \ldots, a_n \in S, k_1, \ldots, k_n \in \mathbb{Z}, n \in \mathbb{N}\}.$$

Määritelmä 1.28. Olkoon $S \subset \mathbb{Z}$ lukujoukko joka sisältää jonkin nollasta eroavan luvun. Tällöin lukujen S suurin yhteinen tekijä, $\operatorname{syt} S$, on aliryhmän $\langle S \rangle$ virittäjä.

Usein kirjoitetaan $\operatorname{syt}(a_1, \ldots, a_n) = \operatorname{syt}\{a_1, \ldots, a_n\}$.

Lause 1.29. *Olkoon $S \subset \mathbb{Z}$ lukujoukko joka sisältää jonkin nollasta eroavan luvun. Tällöin*

$$\operatorname{syt} S = \max\{n \in \mathbb{Z} : n \mid m \text{ kaikilla } m \in S\}.$$

Todistus. Olkoon $k = \max\{n \in \mathbb{Z} : n \mid m \text{ kaikilla } m \in S\}$. Koska $k \mid m$ kaikilla $m \in S$, myös $k \mid m$ kaikilla $m \in \langle S \rangle$. Erityisesti $k \mid \operatorname{syt} S$ ja siten $k \leq \operatorname{syt} S$. Toisaalta, koska $\operatorname{syt} S$ virittää ryhmän $\langle S \rangle$, myös $\operatorname{syt} S \mid m$ kaikilla $m \in S$ eli $\operatorname{syt} S \leq k$. Siispä $k = \operatorname{syt} S$. □

Todistetaan nyt Eukleideen ensimmäinen lause.

Lauseen 1.13 todistus. Olkoon p alkuluku ja $p \mid ab$. Jos $p \nmid a$, on Lauseen 1.29 mukaan $\text{syt}(p, a) = 1$. Siten on olemassa $x, y \in \mathbb{Z}$ siten, että $xa + yp = 1$ eli

$$xab + ypb = b.$$

Koska $p \mid ab$ ja $p \mid pb$, täytyy $p \mid b$. □

1.7. **Eukleideen algoritmi.** Lukujen $a, b \in \mathbb{Z}$ suurin yhteinen tekijä voidaan helposti määrätä Eukleideen algoritmin avulla: Olkoon $0 < b < |a|$. Merkitään $r_0 = b$. Lauseen 1.6 nojalla on olemassa yksikäsitteiset $q_1, r_1 \in \mathbb{Z}$ siten, että

$$a = q_1 b + r_1, \qquad 0 \leq r_1 < b = r_0.$$

Oletetaan, että luvut $q_1, \ldots, q_m, r_1, \ldots, r_m \in \mathbb{Z}$ on määritetty siten, että

$$r_{j-1} = q_{j+1} r_j + r_{j+1}, \qquad 0 \leq r_{j+1} < r_j$$

kaikilla $1 \leq j < m$. Jos $r_m > 0$, on jälleen Lauseen 1.6 mukaan olemassa $q_{m+1}, r_{m+1} \in \mathbb{Z}$ siten, että

$$r_{m-1} = q_{m+1} r_m + r_{m+1}, \qquad 0 \leq r_{m+1} < r_m.$$

Koska jono $r_0 > r_1 > \cdots \geq 0$ on aidosti vähenevä, on olemassa $n \in \mathbb{N}$ siten, että $r_n > 0$ ja $r_{n+1} = 0$. Nyt

$$\text{syt}(a, b) = r_n.$$

Osoitetaan, että tämä on totta. Selvästi $r_n \mid r_{n-1}$, koska $r_{n+1} = 0$. Edelleen, koska $r_{n-2} = q_n r_{n-1} + r_n$, myös $r_n \mid r_{n-2}$. Näin jatkaen nähdään, että $r_n \mid r_0 = b$ ja $r_n \mid a$. Siten $1 \leq r_n \mid \text{syt}(a, b) =: d$.

Koska $d \mid a$ ja $d \mid b$, myös $d \mid r_1$. Vastaavasti $d \mid r_2, d \mid r_3, \ldots, d \mid r_n$.

Esimerkki 1.30. Määritetään Eukleideen algoritmilla $\text{syt}(6006, 1565)$.

$$\begin{aligned} 6006 &= 3 \cdot 1565 + 1311 \\ 1565 &= 1 \cdot 1311 + 254 \\ 1311 &= 5 \cdot 254 + 41 \\ 254 &= 6 \cdot 41 + 8 \\ 41 &= 5 \cdot 8 + 1 \\ 8 &= 8 \cdot 1 \end{aligned}$$

Siis $\text{syt}(6006, 1565) = 1$.

Eukleideen algoritmilla nähdään myös kuinka $\text{syt}(a, b)$ saadaan kirjoitettua muodossa $n_1 a + n_2 b$, missä $n_1, n_2 \in \mathbb{Z}$. Riittää huomata, että

$$\text{syt}(a, b) = r_n = r_{n-2} - q_n r_{n-1},$$

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$$

ja niin edelleen. Sovelletaan tätä havaintoa Esimerkin 1.30 tapaukseen.

$$\begin{aligned}1 &= 41 - 5 \cdot 8 = 41 - 5 \cdot (254 - 6 \cdot 41) = 31 \cdot 41 - 5 \cdot 254 \\ &= 31 \cdot (1311 - 5 \cdot 254) - 5 \cdot 254 = 31 \cdot 1311 - 160 \cdot 254 \\ &= 31 \cdot 1311 - 160 \cdot (1565 - 1311) = 191 \cdot 1311 - 160 \cdot 1565 \\ &= 191 \cdot (6006 - 3 \cdot 1565) - 160 \cdot 1565 = 191 \cdot 6006 - 733 \cdot 1565.\end{aligned}$$

Eukleideen algoritmiä voidaan soveltaa myös suuremman lukujoukon suurimman yhteisen tekijän etsimiseen, sillä

Lause 1.31. *Olkoot $a, b, c \in \mathbb{Z} \setminus \{0\}$. Tällöin*

$$\operatorname{syt}(a, b, c) = \operatorname{syt}(\operatorname{syt}(a, b), c).$$

Todistus. (Harjoitustehtävä) □

1.8. **Pienin yhteinen jaettava.**

Määritelmä 1.32. Olkoon $S \subset \mathbb{Z} \setminus \{0\}$ epätyhjä joukko. Joukon S pienin yhteinen jaettava, $\operatorname{pyj} S$, on

$$\operatorname{pyj} S = \min\{a \in \mathbb{N} : b \mid a \text{ kaikilla } b \in S\}.$$

Aritmetiikan peruslauseen avulla lukujen suurin yhteinen tekijä ja pienin yhteinen jaettava voidaan kirjoittaa helposti, mikäli niiden alkulukuesitys tunnetaan.

Lause 1.33. *Olkoot $p_1 < p_2 < \ldots$ kaikki alkuluvut ja*

$$a_k = \prod_{i=1}^{\infty} p_i^{\alpha_{k,i}},$$

missä $\alpha_{k,i} \in \mathbb{N}$, lukujen $a_1, \ldots, a_n$ alkulukuesitykset. Tällöin

$$\operatorname{syt}(a_1, \ldots, a_n) = \prod_{i=1}^{\infty} p_i^{\min_k \alpha_{k,i}}$$

ja

$$\operatorname{pyj}(a_1, \ldots, a_n) = \prod_{i=1}^{\infty} p_i^{\max_k \alpha_{k,i}}.$$

Todistus. Kaikilla $k \in \{1, \ldots, n\}$ on

$$a_k = \prod_{i=1}^{\infty} p_i^{\alpha_{k,i}} = \prod_{i=1}^{\infty} p_i^{\min_k \alpha_{k,i}} \cdot \prod_{i=1}^{\infty} p_i^{\alpha_{k,i} - \min_k \alpha_{k,i}}$$

eli

$$\prod_{i=1}^{\infty} p_i^{\min_k \alpha_{k,i}} \mid a_k.$$

Olkoon nyt

$$\operatorname{syt}(a_1, \ldots, a_n) = \prod_{i=1}^{\infty} p_i^{s_i}.$$

Oletetaan, että jokin $s_j > \min_k \alpha_{k,j}$. Tällöin on olemassa $m \in \{1, \ldots, n\}$ siten, että $\alpha_{m,j} = \min_k \alpha_{k,j}$. Koska

$$p_j^{s_j} \mid a_m,$$

on erityisesti voimassa

$$p_j \mid \prod_{i \neq j} p_i^{\alpha_{k,i}}.$$

Tämä taas on mahdotonta Lauseen 1.13 nojalla.

Todistus yhtälölle

$$\operatorname{pyj}(a_1, \ldots, a_n) = \prod_{i=1}^{\infty} p_i^{\max_k \alpha_{k,i}}$$

tulee vastaavasti. □

Esimerkki 1.34. Määritellään lukujen 980 ja 1092 suurin yhteinen tekijä ja pienin yhteinen jaettava niiden alkulukuesitysten kautta. Huomataan, että

$$980 = 2^2 \cdot 5 \cdot 7^2$$

ja

$$1092 = 2^2 \cdot 3 \cdot 7 \cdot 13.$$

Siten

$$\operatorname{syt}(980, 1091) = 2^2 \cdot 7 = 28$$

ja

$$\operatorname{pyj}(980, 1091) = 2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 13 = 38220.$$

Koska Esimerkissä 1.34 käytetyt luvut olivat hyvin pienet, saatiin niiden alkulukuesitykset helposti selville (esimerkiksi Eratostheneen seulalla ja kokeilemalla jakamista). Yleensä alkulukuesitysten etsiminen ei kuitenkaan ole helppoa. Siksi Eukleideen algoritmi on yleensä hyödyllinen. Esimerkin 1.34 luvuista huomataan, että $980 \cdot 1092 = 28 \cdot 38220$. Tämä ei ole sattumaa, kuten seuraava lause osoittaa.

Lause 1.35. *Olkoot $a, b \in \mathbb{N}$ siten, että ainakin toinen luvuista a, b eroo nollasta. Tällöin*

$$\operatorname{syt}(a, b) \operatorname{pyj}(a, b) = ab.$$

Todistus. Kirjoitetaan

$$a = \prod_{i=1}^{\infty} p_i^{\alpha_i} \qquad \text{ja} \qquad b = \prod_{i=1}^{\infty} p_i^{\beta_i}.$$

Lauseen 1.33 mukaan

$$\begin{aligned} \operatorname{syt}(a, b) \operatorname{pyj}(a, b) &= \prod_{i=1}^{\infty} p_i^{\min\{\alpha_i, \beta_i\}} \prod_{i=1}^{\infty} p_i^{\max\{\alpha_i, \beta_i\}} = \prod_{i=1}^{\infty} p_i^{\alpha_i + \beta_i} \\ &= \prod_{i=1}^{\infty} p_i^{\alpha_i} \prod_{i=1}^{\infty} p_i^{\beta_i} = ab. \end{aligned}$$

□

Siis vaikkapa Esimerkin 1.30 luvuille on $\operatorname{pyj}(6006, 1365) = 6006 \cdot 1565 / \operatorname{syt}(6006, 1565) = 6006 \cdot 1565 = 9399390$.

1.9. **Lineaarinen Diofantoksen yhtälö.**

Määritelmä 1.36. Olkoot $k \in \mathbb{N}$ ja $a_1, a_2, \ldots, a_k, b \in \mathbb{Z}$. Yhtälöä

$$\sum_{i=1}^{k} a_i x_i = b \tag{1}$$

sanotaan lineaariseksi Diofantoksen yhtälöksi. Vektoria $x = (x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k$ sanotaan tämän yhtälön ratkaisuksi, jos se toteuttaa yhtälön (1). Yhtälön täydelliseksi ratkaisuksi sanotaan joukkoa

$$\left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k : \sum_{i=1}^{k} a_i x_i = b \right\} \subset \mathbb{Z}^k.$$

Esimerkki 1.37. Yhtälö

$$2x_1 + 3x_2 = 5$$

on lineaarinen Diofantoksen yhtälö, jonka eräs ratkaisu on $x = (1, 1) \in \mathbb{Z}^2$ ja täydellinen ratkaisu on joukko

$$\{(x_1, x_2) \in \mathbb{Z}^2 : x_1 = 3q + 1 \text{ ja } x_2 = -2q + 1 \text{ jollekin } q \in \mathbb{Z}\} \subset \mathbb{Z}^2.$$

Esimerkki 1.38. Lineaarisella Diofantoksen yhtälöllä

$$15x_1 + 3x_2 = 10$$

ei ole ratkaisua.

Seuraavan lauseen avulla pystytään nopeasti sanomaan onko annetulla lineaarisella Diofantoksen yhtälöllä ratkaisuja.

Lause 1.39. *Olkoot $k \in \mathbb{N}$ ja $a_1, a_2, \ldots, a_k, b \in \mathbb{Z}$ siten, että ainakin yksi $a_i \neq 0$. Tällöin lineaarisella Diofantoksen yhtälöllä*

$$\sum_{i=1}^{k} a_i x_i = b \tag{2}$$

on ratkaisu, jos ja vain jos

$$\operatorname{syt}\{a_1, a_2, \ldots, a_k\} \mid b.$$

Todistus. Määritellään

$$H = \left\{ y \in \mathbb{Z} : y = \sum_{i=1}^{k} q_i a_i \text{ jollekin } q_i \in \mathbb{Z} \right\} \subset \mathbb{Z}.$$

Selvästi H on ryhmän $\mathbb{Z}$ aliryhmä ja lisäksi

$$H = d\mathbb{Z},$$

missä $d = \operatorname{syt}\{a_1, a_2, \ldots, a_k\}$.

Oletetaan, että yhtälöllä (2) on ratkaisu $x = (x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k$. Joukon H määritelmän mukaan tällöin $b \in H$ ja siten

$$d \mid b.$$

Osoitetaan seuraavaksi toinen suunta eli oletetaan, että $d \mid b$. Siis on olemassa jokin $m \in \mathbb{Z}$ siten, että $b = md$. Toisaalta $d \in d\mathbb{Z} = H$ eli on olemassa luvut $q_i \in \mathbb{Z}$ siten, että

$$d = \sum_{i=1}^{k} q_i a_i.$$

Tästä saadaan

$$b = md = \sum_{i=1}^{k} mq_i a_i.$$

eli $(mq_1, mq_2, \ldots, mq_k) \in \mathbb{Z}^k$ on yhtälön (2) ratkaisu. □

Lause 1.40. *Olkoon $m, n, q \in \mathbb{Z}$ siten, että ainakin toinen luvuista m, n ei ole nolla. Jos*

$$\text{syt}(m, n) = 1$$

ja

$$m \mid nq,$$

niin

$$m \mid q.$$

Todistus. Koska $m \mid nq$, on olemassa $r \in \mathbb{Z}$ siten, että

$$nq = mr.$$

Toisaalta Lauseen 1.39 mukaan on olemassa $x_1, x_2 \in \mathbb{Z}$ siten, että

$$mx_1 + nx_2 = 1.$$

Siispä

$$q = q(mx_1 + nx_2) = qmx_1 + qnx_2 = qmx_1 + mrx_2 = m(qx_1 + rx_2)$$

eli $m \mid q$. □

2. Lukukongruenssit

Määritelmä 2.1. Olkoon $n \in \mathbb{N}$. Luvut $a, b \in \mathbb{Z}$ ovat kongruentteja modulo n,

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

kun $a - b = kn$ jollakin $k \in \mathbb{Z}$.

Lause 2.2. *Kongruenssi $(\text{mod } n)$ on ekvivalenssirelaatio eli*

(i) $a \equiv a$,
(ii) $a \equiv b \Leftrightarrow b \equiv a$,
(iii) $a \equiv b$ *ja* $b \equiv c \Rightarrow a \equiv c$

kaikilla $a, b, c \in \mathbb{Z}$.

Todistus. (Harjoitustehtävä) □

Luvun $a \in \mathbb{Z}$ ekvivalenssiluokkaa kongruenssin (mod n) suhteen merkitään

$$[a]_n = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} \subset \mathbb{Z}$$

Jos $n > 1$, voidaan Lauseen 1.6 mukaan kokonaislukujen joukko $\mathbb{Z}$ jakaa kongruenssin avulla jäännösluokkiin (mod n),

$$\mathbb{Z}_n = \bigcup_{r=0}^{n-1} [r]_n.$$

Lause 2.3. *Jäännösluokat (mod n), $1 < n \in \mathbb{N}$, varustettuna yhteenlaskulla $[a+b]_n = [a]_n + [b]_n$ ja kertolaskulla $[ab]_n = [a]_n[b]_n$ muodostavat kommutatiivisen renkaan $\mathbb{Z}_n$, kokonaislukujen jäännösluokkarenkaan (mod n).*

Ennen Lauseen 2.3 todistamista palautetaan mieleen renkaan määritelmä.

Määritelmä 2.4. Kolmikko $(R, +, \cdot)$ on rengas, jos se täyttää ehdot

(R1) $(R, +)$ on Abelin ryhmä,
(R2) kertolasku $\cdot$ on joukossa R määritetty laskutoimitus,
(R3) $a(bc) = (ab)c$ kaikilla $a, b, c \in R$,
(R4) on olemasa $1 \in R$ jolle $a \cdot 1 = 1 \cdot a = a$ kaikilla $a \in R$,
(R5) $a(b+c) = ab + ac$ ja $(a+b)c = ac + bc$ kaikilla $a, b, c \in R$.

Jos lisäksi $ab = ba$ kaikilla $a, b, \in R$ on rengas kommutatiivinen.

Lauseen 2.3 todistus. Todistetaan ensin, että $(\mathbb{Z}_n, +)$ on Abelin ryhmä. Olkoot $[a]_n, [b]_n \in \mathbb{Z}_n$. Jos $a', b' \in Z$ siten, että $a' \in [a]_n$ ja $b' \in [b]_n$, on olemassa $k_1, k_2 \in \mathbb{Z}$ siten, että $a' = a + k_1 n$ ja $b' = b + k_2 n$. Siis

$$\begin{aligned}[a']_n + [b']_n &= [a' + b']_n = [a + k_1 n + b + k_2 n]_n \\ &= [a + b + (k_1 + k_2)n]_n = [a+b]_n = [a]_n + [b]_n\end{aligned}$$

eli yhteenlasku on hyvin määritelty. Ehdot (G1) – (G4) seuraavat nyt ryhmän $(\mathbb{Z}, +)$ rakenteesta. Alkio $[0]_n$ on siis nolla-alkio ja $[-a]_n$ alkion $[a]_n$ vasta-alkio.

Tarkistetaan seuraavaksi, että kertolasku on määritelty hyvin. Olkoot jälleen $[a]_n, [b]_n \in \mathbb{Z}_n$ ja $a', b' \in Z$ siten, että $a' \in [a]_n$ ja $b' \in [b]_n$. Taas on olemassa $k_1, k_2 \in \mathbb{Z}$ siten, että $a' = a + k_1 n$ ja $b' = b + k_2 n$. Nyt

$$\begin{aligned}[a']_n[b']_n = [a'b']_n &= [(a + k_1 n)(b + k_2 n)]_n = [ab + ak_2 n + bk_1 n + k_1 k_2 n^2]_n \\ &= [ab + (ak_2 + bk_1 + k_1 k_2 n)n]_n = [ab]_n = [a]_n[b]_n.\end{aligned}$$

Jälleen renkaan $(\mathbb{Z}_n, +, \cdot)$ loput ominaisuudet seuraavat renkaan $(\mathbb{Z}, +, \cdot)$ vastaavista ominaisuuksista. Ykkösalkiona renkaassa on siis $[1]_n$. □

Huomautus 2.5. Aina ei alkiolla $[a]_n \in \mathbb{Z}_n \setminus \{[0]_n\}$ ole käänteisalkiota kertolaskun suhteen, eli $\mathbb{Z}_n$ ei aina ole kunta. Esimerkiksi

$$[2]_4 \cdot [a]_4 \neq [1]_4$$

kaikilla $a \in \mathbb{Z}$.

2.1. **Lineaarinen kongruenssiyhtälö.**

Määritelmä 2.6. Olkoon $d \in \mathbb{N}$, $d \geq 1$ ja $a, b \in \mathbb{Z}$. Yhtälöä

$$[a]_d \cdot [x]_d = [b]_d$$

sanotaan lineaariseksi kongruenssiyhtälöksi. Luokkaa $[x]_d \in \mathbb{Z}_d$, joka toteuttaa yhtälön sanotaan kyseisen yhtälön ratkaisuksi. Yhtälön täydellinen ratkaisu on kaikkien ratkaisujen muodostama joukko.

Esimerkki 2.7. Yhtälön

$$[6]_8 \cdot [x]_8 = [4]_8$$

eräs ratkaisu on $[2]_8$. Toinen ratkaisu on $[6]_8$. Muita ratkaisuja ei ole eli täydellinen ratkaisu on $\{[2]_8, [6]_8\}$.

Lineaariset kongruenssiyhtälöt ja lineaariset Diofantoksen yhtälöt liittyvät kiinteästi toisiinsa, kuten seuraavassa lauseessa nähdään.

Lause 2.8. *Olkoon $d \in \mathbb{N}$, $d \geq 1$ ja $a, b, x \in \mathbb{Z}$ Tällöin luokka $[x]_d \in \mathbb{Z}_d$ on lineaarisen kongruenssiyhtälön*

$$[a]_d \cdot [x]_d = [b]_d$$

ratkaisu jos ja vain jos on olemassa $y \in \mathbb{Z}$ siten, että $(x, y) \in \mathbb{Z}^2$ on lineaarisen Diofantoksen yhtälön

$$ax + dy = b$$

ratkaisu.

Todistus. Oletetaan, että $[x]_d$ on yhtälön

$$[a]_d \cdot [x]_d = [b]_d$$

ratkaisu. Siis $[ax]_d = [b]_d$ eli $ax \equiv b \pmod{d}$. Siispä

$$ax - b = md \qquad \text{jollekin } m \in \mathbb{Z}.$$

Merkitään $y = -m \in \mathbb{Z}$. Tällöin

$$ax + dy = ax - md = ax - (ax - b) = b.$$

Oletetaan seuraavaksi, että on olemassa $y \in \mathbb{Z}$ siten, että

$$ax + dy = b.$$

Tällöin $ax - b = dy$ eli

$$[ax]_d = [b]_d$$

ja siten

$$[a]_d \cdot [x]_d = [b]_d.$$

□

Lause 2.9. *Olkoon $d \in \mathbb{N}$, $d \geq 1$ ja $a, b \in \mathbb{Z}$. Tällöin lineaarisella kongruenssiyhtälöllä*

$$[a]_d \cdot [x]_d = [b]_d$$

on ratkaisu jos ja vain jos

$$\text{syt}(a, d) \mid b.$$

Todistus. Lauseen 2.8 nojalla yhtälöllä on ratkaisu vain jos ja vain jos Diofantoksen yhtälöllä $ax + dy = b$ on ratkaisu. Tällä taas on ratkaisu Lauseen 1.39 nojalla jos ja vain jos $\text{syt}(a, d) \mid b$. □

Lause 2.10. *Olkoon $d \in \mathbb{N}$, $d \geq 1$ ja $a, b \in \mathbb{Z}$. Olkoon*

$$\text{syt}(a, d) = 1.$$

Tällöin lineaarisella kongruenssiyhtälöllä

$$[a]_d \cdot [x]_d = [b]_d$$

on täsmälleen yksi ratkaisu.

Todistus. Lauseen 2.9 mukaan on olemassa ainakin yksi $[x]_d$ siten, että

$$[a]_d \cdot [x]_d = [b]_d.$$

Oletetaan, että myös $[y]_d$ on kyseisen yhtälön ratkaisu. Tällöin

$$[ax - ay]_d = [a]_d[x]_d - [a]_d[y]_d = [b]_d - [b]_d = [b - b]_d = [0]_d.$$

Siispä

$$d \mid a(x - y).$$

Koska $\text{syt}(a, d) = 1$, on Lauseen 1.40 nojalla

$$d \mid (x - y).$$

Siten $[y]_d = [x]_d$. □

Lause 2.11. *Olkoon $d \in \mathbb{N}$, $d \geq 1$ ja $a, b \in \mathbb{Z}$. Olkoon*

$$s = \text{syt}(a, d)$$

ja oletetaan, että $s \mid b$. Tällöin lineaarisen kongruenssiyhtälön

$$[a]_d \cdot [x]_d = [b]_d$$

täydellisen ratkaisun alkioiden lukumäärä on s.

Todistus. Koska $s = \text{syt}(a, d)$, on $s \mid a$ ja $s \mid d$. On siis olemassa $a', d' \in \mathbb{Z}$ siten, että

$$a = sa' \qquad \text{ja} \qquad d = sd'$$

Nyt

$$\text{syt}(a', d') = 1,$$

sillä $\text{syt}(a', d')s \mid a$ ja $\text{syt}(a', d')s \mid d$.

Koska $s \mid b$, on olemassa $b' \in \mathbb{Z}$ siten, että

$$b = sb'.$$

Lauseen 2.10 mukaan yhtälöllä

$$[a']_{d'} \cdot [x]_{d'} = [b']_{d'}$$

on täsmälleen yksi ratkaisu. Merkitään sitä $[x']_{d'}$. Osoitetaan seuraavaksi, että

$$[a]_d \cdot [x]_d = [b]_d \iff \exists n \in \mathbb{Z} : x = x' + nd'. \tag{3}$$

Olkoon siis $x \in \mathbb{Z}$ siten, että $[a]_d \cdot [x]_d = [b]_d$. Siispä $[ax]_d = [b]_d$ eli $d \mid ax - b$, ja siten $ax - b = md$ jollakin $m \in \mathbb{Z}$. Tästä saadaan

$$sa'x - sb' = msd',$$

josta edelleen

$$a'x - b' = md'.$$

Lauseen 2.8 nojalla

$$[a']_{d'} \cdot [x]_{d'} = [b']_{d'}.$$

Siten $[x]_{d'} = [x']_{d'}$, ja $x = x' + nd'$ jollakin $n \in \mathbb{Z}$.

Osoitetaan seuraavaksi väite toiseen suuntaan eli olkoon $n \in \mathbb{Z}$ ja $x = x' + nd'$. Jälleen Lauseen 2.8 nojalla on

$$a'x' - b' = md'$$

jollakin $m \in \mathbb{Z}$. Siten

$$\begin{aligned} ax - b &= a(x' + nd') - b = sa'(x' + nd') - sb' = sa'x' + sa'nd' - sb' \\ &= s(a'x' - b') + a'nd = smd' + a'nd = md + a'nd = d(m + a'n). \end{aligned}$$

Lauseen 2.8 perusteella siis $[a]_d \cdot [x]_d = [b]_d$. Siten (3) on todistettu.

Vielä tulee osoittaa, että

$$\#\{[x]_d : x = x' + nd', n \in \mathbb{Z}\} = s. \tag{4}$$

Olkoon $0 \leq n_1 < n_2 < s$. Koska

$$0 < (x' + n_2d') - (x' + n_1d') = (n_2 - n_1)d' < sd' = d,$$

on

$$[x' + n_1d']_d \neq [x' + n_2d']_d.$$

Toisaalta Lauseen 1.6 mukaan kaikille $n \in \mathbb{Z}$ on olemassa $q, r \in \mathbb{Z}$, siten, että $0 \leq r < s$ ja $n = qs + r$. Tällöin

$$x' + nd' = x' + (qs + r)d' = x' + rd' + qsd' = x' + rd' + qd$$

eli $[x' + nd']_d = [x' + rd']_d$. Siten (4) on totta. □

Lauseet 2.8 – 2.11 antavat meille menetelmän yleisesti ratkaista kongruenssiyhtälö

$$[a]_d \cdot [x]_d = [b]_d.$$

Tämä tehdään siis vaiheittain

1) Määrätään $s = \text{syt}(a, d)$.
2) Mikäli $s \nmid b$, ei yhtälöllä ole lainkaan ratkaisuja. Jos taas $s \mid b$, jatketaan seuraavaan vaiheeseen.

3) Etsitään (jotenkin) yhtälön eräs ratkaisu $[x]_d$. Mikäli $s = 1$ on tämä ainoa ratkaisu. Jos taas $s > 1$, jatketaan edelleen.
4) Loput ratkaisut saadaan laskemalla

$$[x + nd/s]_d,$$

kun $0 < n < s$.

Esimerkki 2.12. Ratkaistaan yhtälöt

a) $[3]_9 \cdot [x]_9 = [8]_9$,
b) $[3]_8 \cdot [x]_8 = [9]_8$ ja
c) $[3]_{24} \cdot [x]_{24} = [9]_{24}$.

a) $\text{syt}(3, 9) = 3 \nmid 8$ eli yhtälöllä ei ole tarkaisuja.
b) $\text{syt}(3, 8) = 1$ eli yhtälöllä on täsmälleen yksi ratkaisu, $[3]_8$.
c) $\text{syt}(3, 24) = 3 \mid 9$ eli yhtälöllä on kolme ratkaisua. Selvästi eräs ratkaisuista on $[3]_{24}$. Loput kaksi saadaan laskemalla $[3 + 1 \cdot 24/3]_{24} = [3 + 8]_{24} = [11]_{24}$ ja $[3 + 2 \cdot 8]_{24} = [19]_{24}$.

Nyt kun tiedämme millainen lineaarisen kongruenssiyhtälön ratkaisujoukko on, saamme myös vastaavalle lineaariselle Diofantoksen yhtälölle täydellisen ratkaisujoukon.

Lause 2.13. *Olkoon $d \in \mathbb{N}$, $d \geq 1$ ja $a, b \in \mathbb{Z}$. Merkitään $s = \text{syt}(a, d)$. Jos $s \nmid b$, ei Diofantoksen yhtälöllä*

$$ax + dy = b$$

ole lainkaan ratkaisuja. Jos $s \mid b$, on yhtälöllä olemassa ratkaisu. Jos $(x_0, y_0) \in \mathbb{Z}^2$ on yhtälön ratkaisu, saadaan yhtälön täydellinen ratkaisu joukkona

$$\left\{(x, y) : x = x_0 + \frac{kd}{s} \text{ ja } y = y_0 - \frac{ka}{s} \text{ jollekin } k \in \mathbb{Z}\right\}.$$

Todistus. Lauseen 1.39 mukaan yhtälöllä on ratkaisu täsmälleen silloin kun $s \mid b$. Oletetaan siis, että $s \mid b$ ja $(x_0, y_0) \in \mathbb{Z}^2$ on yhtälön $ax+dy = b$ ratkaisu.

Olkoot $k \in \mathbb{Z}$, $x = x_0 + \frac{kd}{s}$ ja $y = y_0 - \frac{ka}{s}$. Nyt

$$ax + dy = ax_0 + a\frac{kd}{s} + dy_0 - d\frac{ka}{s} = ax_0 + dy_0 = b.$$

Olkoon seuraavaksi $(x, y) \in \mathbb{Z}^2$ yhtälön $ax + dy = b$ ratkaisu. Siten Lauseen 2.8 mukaan $[x]_d \cdot [a]_d = [b]_d$ ja siten Lauseen 2.11 ekvivalenssin (3) mukaan on olemassa $k \in \mathbb{Z}$ siten, että $x = x_0 + \frac{kd}{s}$. Nyt

$$y = \frac{b - ax}{d} = \frac{ax_0 + dy_0 - ax}{d} = y_0 + \frac{a}{d}(x_0 - x) = y_0 - \frac{a}{d}\frac{kd}{s}.$$

□

Esimerkki 2.14. Ratkaistaan Diofantoksen yhtälö

$$36x + 20y = 24.$$

Koska $\text{syt}(36, 20) = 4 \mid 24$, on ratkaisu olemassa. Eräs näistä on $(-1, 3) \in \mathbb{Z}^2$. Täydellinen ratkaisu saadaan siten joukkona

$$\{(x, y) : x = -1 + 5k, y = 3 - 9k, k \in \mathbb{Z}\}.$$

Edellisessä esimerkissä vain todettiin, että $(-1, 3) \in \mathbb{Z}^2$ on yhtälön ratkaisu. Jos ratkaisua ei heti näe, se voidaan etsiä käyttämällä Eukleideen algoritmia seuraavan esimerkin osoittamalla tavalla.

Esimerkki 2.15. Ratkaistaan Diofantoksen yhtälö

$$1935x - 3053y = 172.$$

Lasketaan ensin $\text{syt}(1935, 3053)$.

$$\begin{aligned}
3053 &= 1935 + 1118 \\
1935 &= 1118 + 817 \\
1118 &= 817 + 301 \\
817 &= 2 \cdot 301 + 215 \\
301 &= 215 + 86 \\
215 &= 2 \cdot 86 + 43 \\
86 &= 2 \cdot 43.
\end{aligned}$$

Siis $\text{syt}(1935, 3053) = 43$. Koska $172 = 4 \cdot 43$, on yhtälöllä ratkaisu. Eukleideen algoritmin vaiheista voidaan nyt kirjoittaa

$$\begin{aligned}
43 &= 215 - 2 \cdot 86 = 215 - 2(301 - 215) = 3 \cdot 215 - 2 \cdot 301 \\
&= 3(817 - 2 \cdot 301) - 2 \cdot 301 = 3 \cdot 817 - 8 \cdot 301 \\
&= 3 \cdot 817 - 8(1118 - 817) = 11 \cdot 817 - 8 \cdot 1118 \\
&= 11(1935 - 1118) - 8 \cdot 1118 = 11 \cdot 1935 - 19 \cdot 1118 \\
&= 11 \cdot 1935 - 19 \cdot (3053 - 1935) = 30 \cdot 1935 - 19 \cdot 3053.
\end{aligned}$$

Eräs ratkaisu on siis $(120, 76)$. Täydellinen ratkaisu saadaan joukkona

$$\{(x, y) : x = 120 - 71k, y = 76 - 45k, k \in \mathbb{Z}\}.$$

2.2. **Lukukunnat ja alkuluvut.** Kuten Lauseessa 2.3 nähtiin, ovat jäännösluokat $\mathbb{Z}_n$ kommutatiivisia renkaita. Avoimeksi jäi vielä kysymys siitä ovatko ne kuntia. Palautetaan taas ensin mieleen mitä kunnalla tarkoitetaan.

Määritelmä 2.16. Kolmikko $(K, +, \cdot)$ on kunta, jos

(K1) $(K, +, \cdot)$ on kommutatiivinen rengas ja
(K2) jokaisella joukon $K \setminus \{0\}$ alkiolla on olemassa käänteisalkio (kertolaskun $\cdot$ suhteen).

Siis $(K, +, \cdot)$ on kunta, jos ja vain jos sekä $(K, +)$, että $(K \setminus \{0\}, \cdot)$ ovat Abelin ryhmiä ja

$$a(b + c) = ab + ac \qquad \text{kaikilla } a, b, c \in K.$$

Esimerkki 2.17. a) $\mathbb{Z}_2$ on kunta: koska $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, riittää huomata, että alkiolla $[1]_2$ on kertolaskun suhteen käänteisalkiona $[1]_2$.
b) Myös $\mathbb{Z}_3$ on kunta. (Harjoitustehtävä)
c) $\mathbb{Z}_4$ ei ole kunta, sillä alkiolla $[2]_4$ ei ole käänteisalkiota. Tämä nähdään käymällä läpi kaikki mahdollisuudet:

$$[2]_4 \cdot [1]_4 = [2]_4 \neq [1]_4,$$
$$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4 \neq [1]_4 \text{ ja}$$
$$[2]_4 \cdot [3]_4 = [6]_4 = [2]_4 \neq [1]_4.$$

d) $\mathbb{Z}_5$ on kunta. (Harjoitustehtävä)

Yleisesti on voimassa seuraava sääntö.

Lause 2.18. *Olkoon $1 < n \in \mathbb{N}$. Tällöin jäännösluokkarengas $\mathbb{Z}_n$ on kunta jos ja vain jos n on alkuluku.*

Todistus. Oletetaan ensin, että $\mathbb{Z}_n$ on kunta. Tehdään lisäksi vastaoletus, että n on yhdistetty luku. Tällöin on siis olemassa $q, r \in \mathbb{N}$ siten, että $2 \leq q, r \leq n - 1$ ja $n = qr$. Tällöin $[q]_n \neq [0]_n \neq [r]_n$.

Koska $\mathbb{Z}_n$ on kunta, on alkiolla $[q]_n$ käänteisalkio $[y]_n$, jolle

$$[y]_n \cdot [q]_n = [1]_n.$$

Nyt saadaan

$$[r]_n = [1]_n \cdot [r]_n = [y]_n \cdot [q]_n \cdot [r]_n = [y]_n \cdot [n]_n = [y]_n \cdot [0]_n = [0]_n,$$

mikä on ristiriidassa havainnon $[r]_n \neq [0]_n$ kanssa.

Oletetaan nyt, että n on alkuluku. Olkoon $[a]_n \in \mathbb{Z}_n \setminus [0]_n$. On osoitettava, että alkiolla $[a]_n$ on käänteisalkio $[x]_n$. Nyt $\text{syt}(a, n) = 1$, joten Lauseen 2.10 mukaan kongruenssiyhtälöllä

$$[x]_n \cdot [a]_n = [1]_n$$

on olemassa ratkaisu $[x]_n \in \mathbb{Z}_n$, joka on siis haettu käänteisalkio. □

2.3. **Eulerin φ-funktio.** Käsitellään seuraavaksi hieman lukuteoriassa tärkeää Eulerin φ-funktiota.

Määritelmä 2.19. Määritellään kaikille $n \in \mathbb{N} \setminus \{0\}$ joukko

$$\Phi_n = \{k \in \mathbb{N} : \text{syt}(k, n) = 1, k < n\}$$

ja merkitään

$$\varphi(n) = \#\Phi_n.$$

Edelleen merkitään

$$[\Phi_n] = \{[k]_n : k \in \Phi_n\} \subset \mathbb{Z}_n.$$

Selvästi $1 \leq \varphi(n) \leq n$ kaikilla $n \in \mathbb{N} \setminus \{0\}$.

Lause 2.20. *Kaikille* $n \in \mathbb{N} \setminus \{0\}$ *on* $\varphi(n) = \#[\Phi_n]$.

Todistus. Selvästi $\#[\Phi_n] \leq \varphi(n)$. Olkoon $k, m \in \Phi_n$. Jos $[k]_n = [m]_n$, on $k \in [m]_n$ eli on olemassa $l \in \mathbb{Z}$ siten, että $k = ln + m$ eli $k - m = ln$. Koska $1 \leq k, m \leq n-1$, on välttämättä $l = 0$ eli $k = m$. □

Lause 2.21. *Olkoon* p *alkuluku. Tällöin* $\varphi(p) = p - 1$.

Todistus. Koska p on alkuluku, on $\text{syt}(0, p) = p$ ja $\text{syt}(k, p) = 1$ kaikilla $1 \leq k \leq p-1$. □

Lause 2.22. *Olkoon* $a, b \in \mathbb{N}$ *siten, että* $\text{syt}(a, b) = 1$. *Tällöin*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Todistus. Olkoon $x_1, x_2, \ldots, x_{\varphi(a)}$ luvun a kanssa jaottomien jäännösluokkien edustajat, ja vastaavasti $y_1, y_2, \ldots, y_{\varphi(b)}$ luvun b kanssa jaottomien jäännösluokkien edustajat. Väite on, että luvut

$$bx_i + ay_j, \qquad 1 \leq i \leq \varphi(a), 1 \leq j \leq \varphi(b),$$

muodostavat kaikkien tulon ab kanssa jaottomien jäännösluokkien edustajiston.

Jos $p \mid \text{syt}(bx_i + ay_j, a)$ jollain alkuluvulla p, on myös $p \mid bx_i$ ja $p \mid a$ ja edelleen $p \mid x_i$, sillä $\text{syt}(a, b) = 1$. Tämä on kuitenkin mahdotonta, joten $\text{syt}(bx_i + ay_j, a) = 1$. Vastaavasti myös $\text{syt}(bx_i + ay_j, b) = 1$. Siispä Lauseen 1.12 nojalla

$$\text{syt}(bx_i + ay_j, ab) = 1,$$

kaikilla $1 \leq i \leq \varphi(a)$ ja $1 \leq j \leq \varphi(b)$.

Jos nyt jollain i, j, k, l on

$$[bx_i + ay_j]_{ab} = [bx_k + ay_l]_{ab},$$

on myös

$$a \mid b(x_i - x_k) \qquad \text{ja} \qquad b \mid a(y_j - y_l)$$

ja, koska $\text{syt}(a, b) = 1$,

$$a \mid x_i - x_k \qquad \text{ja} \qquad b \mid y_j - y_l.$$

Tällöin on välttämättä $i = k$ ja $j = l$. Siten $\varphi(ab) \geq \varphi(a)\varphi(b)$.

Koska $\text{syt}(a, b) = 1$ on Lauseen 1.39 mukaan yhtälöllä

$$bx + ay = c$$

ratkaisu $x, y \in \mathbb{Z}$. Jos $\text{syt}(ab, c) = 1$, on myös $\text{syt}(c, a) = \text{syt}(c, b) = 1$. Koska myös $\text{syt}(x, a) \mid c$, $\text{syt}(x, a) \mid a$, $\text{syt}(y, b) \mid c$ ja $\text{syt}(y, b) \mid b$, välttämättä myös $\text{syt}(x, a) = 1$ ja $\text{syt}(y, b) = 1$. Siten on olemassa $1 \leq i \leq \varphi(a)$ ja $1 \leq j \leq \varphi(b)$ siten, että

$$[x]_a = [x_i]_a \qquad \text{ja} \qquad [y]_b = [y_j]_b.$$

Siispä

$$[c]_{ab} = [bx + ay]_{ab} = [bx_i + ay_j]_{ab}.$$

Jokaiselle tulon ab kanssa jaottomalle jäännösluokalle löytyy siis edustaja $bx_i + ay_j$ ja siten $\varphi(ab) = \varphi(a)\varphi(b)$ □

Lause 2.23. *Olkoon p alkuluku ja $m \in \mathbb{N} \setminus \{0\}$. Tällöin*

$$\varphi(p^m) = p^m - p^{m-1}.$$

Todistus. Merkitään $n = p^m$. Määritellään

$$B = \{k \in \mathbb{N} : k = pj \text{ jollekin } j \in \{0, 1, \ldots, p^{m-1} - 1\}\}.$$

Selvästi $\#B = p^{m-1}$. Lisäksi kaikilla $j \in \{0, 1, \ldots, p^{m-1} - 1\}$ on

$$0 \leq pj \leq p(p^{m-1} - 1) = p^m - p \leq p^m - 1.$$

Siten joukolle

$$A = \{0, 1, \ldots, p^m - 1\} \setminus B$$

on $\#A = p^m - p^{m-1}$. Osoitetaan, että

$$A = \Phi_n. \tag{5}$$

Olkoon $k \in A$. Halutaan näyttää, että $\text{syt}(k, n) = 1$. Merkitään

$$d = \text{syt}(k, n).$$

Nyt $d \mid k$ ja $d \mid p^m$. Jos $d > 1$ on sillä olemassa alkulukutekijä q, jolle siis myös

$$q \mid k \qquad \text{ja} \qquad q \mid p^m.$$

Tällöin Eukleideen ensimmäisen lauseen (Lause 1.13) mukaan $q \mid p$. Koska p on alkuluku, on

$$q = p.$$

Siten $p \mid k$, joten on olemassa $r \in \mathbb{Z}$ siten, että $k = rp$. Koska

$$0 \leq rp \leq n - 1 < p^m,$$

on

$$0 \leq r < p^{m-1}.$$

Siispä $k \in B$. Tämä on ristiriidassa oletuksen $k \in A$ kanssa, ja siten $d = 1$. Siten on osoitettu, että

$$A \subset \Phi_n.$$

Osoitetaan seuraavaksi inkluusio toiseen suuntaan. Olkoon siis $k \in \Phi_n$. Riittää osoittaa, että $k \notin B$. Tehdään jälleen vastaoletus $k \in B$. Tällöin on olemassa $j \in \{0, 1, \ldots, p^{m-1} - 1\}$ siten, että

$$k = pj.$$

Siis $p \mid k$ ja myös $p \mid n = p^m$. Siispä

$$p \mid \text{syt}(k, n).$$

Koska $p > 1$, on $\text{syt}(k, n) > 1$ mikä on ristiriidassa oletuksen $k \in \Phi_n$ kanssa. Siten $k \notin B$, $\Phi_n \subset A$, ja lause on todistettu. □

Yhdistämällä edelliset lauseet saadaan Eulerin φ-funktion arvo määrättyä kätevästi alkulukuesityksen kautta.

Lause 2.24. *Olkoon luvun $n \in \mathbb{N}$, $n \geq 2$ alkulukuesitys*

$$n = \prod_{i=1}^{\infty} p_i^{\alpha_i}.$$

Tällöin

$$\varphi(n) = \prod_{\substack{i \in \mathbb{N} \\ \alpha_i \neq 0}} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}).$$

Todistus. Koska $\text{syt}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ kaikille $i \neq j$, on Lauseen 2.22 nojalla

$$\varphi(n) = \prod_{\substack{i \in \mathbb{N} \\ \alpha_i \neq 0}} \varphi(p_i^{\alpha_i}).$$

Toisaalta Lauseen 2.23 mukaan on kaikille i

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1},$$

joten lause on todistettu. □

Esimerkki 2.25. Lasketaan esimerkiksi $\varphi(17325)$ eli joukon Φ_{17325} alkioiden lukumäärä käyttämällä Lausetta 2.24. Tässä tapauksessa alkulukuesitys löytyy helposti:

$$17325 = 3^2 \cdot 5^2 \cdot 7 \cdot 11.$$

Siten

$$\begin{aligned} \varphi(17325) &= (3^2 - 3^1)(5^2 - 5^1)(7^1 - 7^0)(11^1 - 11^0) \\ &= 6 \cdot 20 \cdot 6 \cdot 10 = 7200. \end{aligned}$$

Lause 2.26. *Kaikilla $n \geq 2$ on joukko $[\Phi_n]$ varustettuna jäännösluokkien kertolaskulla Abelin ryhmä.*

Todistus. Osoitetaan ensin, että jäännösluokkien kertolasku määrittelee laskutoimituksen joukkoon $[\Phi_n]$. Olkoon $[a]_n, [b]_n \in [\Phi_n]$. Siis $\text{syt}(a, n) = \text{syt}(b, n) = 1$. Tällöin myös $\text{syt}(ab, n) = 1$. (Jos näin ei olisi, olisi olemassa alkuluku $p \mid \text{syt}(ab, n)$. Edelleen, lauseen 1.13 mukaan $p \mid a$ tai $p \mid b$. Oletetaan että ensimmäinen on totta. Tällöin myös $p \mid \text{syt}(a, n)$, mikä on mahdotonta.)

Olkoon $q, r \in \mathbb{Z}$ siten, että $0 \leq r < n$ ja $ab = qn + r$. Nyt $\text{syt}(r, n) \mid n$, $\text{syt}(r, n) \mid qn + r = ab$ ja siten $\text{syt}(r, n) \mid \text{syt}(ab, n) = 1$ eli $\text{syt}(r, n) = 1$. Siispä $[a]_n \cdot [b]_n = [ab]_n \in [\Phi_n]$.

Selväsi kertolasku on assosiatiivinen ja kommutatiivinen. Joukon neutraalialkiona on $[1]_n \in [\Phi_n]$: ensinnäkin $\text{syt}(1, n) = 1$ ja $0 < 1 \leq n$ kaikille $n \geq 2$, joten $[1]_n \in [\Phi_n]$. Toisaalta se on ryhmän $(\mathbb{Z}_n, \cdot)$ neutraalialkio, joten se toimii kuten neutraalialkion tuleekin.

Vielä tulee osoittaa, että jokaisella alkiolla $[a]_n \in [\Phi_n]$ on olemassa käänteisalkio $[b]_n \in [\Phi_n]$. Koska $\text{syt}(a, n) = 1$, on Lauseen 2.10 mukaan yhtälöllä

$$[a]_n \cdot [x]_n = [1]_n$$

täsmälleen yksi ratkaisu $[x]_n \in \mathbb{Z}_n$. Toisaalta jälleen Lauseen 2.10 nojalla samaisella lauseella on ratkaisu $[a]_n$ vain, jos $\text{syt}(x, n) = 1$. Siten $[x]_n \in [\Phi_n]$. □

Määritelmä 2.27. Olkoon $n \geq 2$ ja $a \in \mathbb{Z}$ siten, että $\text{syt}(a, n) = 1$. Määritellään luvun a kertaluku modulin n suhteen

$$\text{ord}_n(a) = \min\{k \in \mathbb{N} \setminus \{0\} : [a^k]_n = [1]_n\}.$$

Esimerkki 2.28. Lasketaan $\text{ord}_{15}(2)$. Tämä on hyvin määritelty, sillä $\text{syt}(2, 15) = 1$. Edetään nyt yksinkertaisesti laskemalla

$$[2^1]_{15} = [2]_{15} \neq [1]_{15}$$
$$[2^2]_{15} = [4]_{15} \neq [1]_{15}$$
$$[2^3]_{15} = [8]_{15} \neq [1]_{15}$$
$$[2^4]_{15} = [16]_{15} = [1]_{15}.$$

Siis $\text{ord}_{15}(2) = 4$.

Lemma 2.29. *Olkoon $n \geq 2$ ja $a \in \mathbb{Z}$ siten, että* $\text{syt}(a, n) = 1$. *Olkoot lisäksi $j, k \in \mathbb{N}$. Tällöin*

$$[a^j]_n = [a^k]_n \qquad \Longleftrightarrow \qquad [j]_{\text{ord}_n(a)} = [k]_{\text{ord}_n(a)}.$$

Todistus. Merkitään $d = \text{ord}_n(a)$. Oletetaan ensin, että

$$[j]_d = [k]_d.$$

On siis olemassa $q \in \mathbb{Z}$ siten, että

$$j = k + qd.$$

Luvun d määritelmän mukaan on

$$[a]_n^d = [a^d]_n = [1]_n.$$

Siten

$$[a^j]_n = [a^{k+qd}]_n = [a^k]_n \cdot [a^d]_n^q = [a^k]_n \cdot [1]_n^q = [a^k]_n$$

ja lauseen toinen suunta on osoitettu.

Oletetaan nyt, että

$$[a^j]_n = [a^k]_n.$$

Olkoon $q, r \in \mathbb{Z}$ siten, että $0 \leq r < d$ ja

$$j - k = qd + r.$$

Tällöin

$$\begin{aligned}[a^k]_n = [a^j]_n = [a^{k+qd+r}]_m &= [a^k]_n \cdot [a^d]_n^q \cdot [a^r]_n \\ &= [a^d]_n \cdot [1]_n \cdot [a^r]_n = [a^k]_n \cdot [a^r]_n.\end{aligned}$$

Koska $\text{syt}(a, n) = 1$, on $[a]_n \in [\Phi_n]$. Lauseen 2.26 nojalla myös

$$[a^k]_n = [a]_n^k \in [\Phi_n]$$

ja alkiolla $[a^k]_n$ on olemassa kertolaskun suhteen käänteisalkio $[b]_n \in [\Phi_n]$. Nyt

$$[1]_n = [b]_n \cdot [a^k]_n = [b]_n \cdot [a^k]_n \cdot [a^r]_n = [a^r]_n.$$

Koska $0 \leq r < d = \mathrm{ord}_n(a)$, on $r = 0$. Siten $j - k = dq$ ja siis

$$[j]_d = [k]_d.$$

□

Lemma 2.30. *Olkoon $n \geq 2$ ja $a \in \mathbb{Z}$ siten, että* $\mathrm{syt}(a, n) = 1$. *Olkoon lisäksi $k \in \mathbb{N}$. Tällöin*

$$[a^k]_n = [1]_n \qquad \Longleftrightarrow \qquad \mathrm{ord}_n(a) \mid k.$$

Todistus. Koska $[1]_n = [a^0]_n$, väite seuraa Lemmasta 2.29. □

Lause 2.31. *Jos $n \in \mathbb{N}$, $n \geq 2$ ja $[a]_n \in \mathbb{Z}_n$ siten, että*

$$\mathrm{ord}_n(a) = n - 1,$$

on n alkuluku.

Todistus. Lemman 2.29 mukaan kaikilla $1 \leq j < k \leq \mathrm{ord}_n(a)$ on $[a^k]_n \neq [a^j]_n$. Toisaalta koska $\#\mathbb{Z}_n = n$, on jokaiselle $[b]_n \in \mathbb{Z}_n \setminus \{[0]_n\}$ olemassa $1 \leq m \leq n - 1$ siten, että

$$[a^m]_n = [b]_n$$

Siten alkion $[b]_n$ käänteisalkio kertolaskun suhteen on $[a^{n-1-m}]_n$. $\mathbb{Z}_n$ on siis kunta, joten lauseen 2.18 mukaan n on alkuluku. □

2.4. **Eulerin, Fermat'n ja Wilsonin lauseet.**

Lause 2.32 (Eulerin lause)**.** *Olkoon $n \geq 2$ ja $a \in \mathbb{Z}$ siten, että*

$$\mathrm{syt}(a, n) = 1.$$

Tällöin

$$[a^{\varphi(n)}]_n = [1]_n.$$

Ennen Eulerin lauseen todistamista palautetaan mieleen algebran kurssilla todistettu

Lause 2.33 (Lagrangen lause)**.** *Olkoon G äärellinen Abelin ryhmä ja H ryhmän G aliryhmä. Tällöin*

$$\#H \mid \#G.$$

Todistuksen idea. Määritellään kaikille $x \in G$ joukko

$$xH = \{xh : h \in H\}$$

ja merkitään kaikkien niiden kokoelmaa

$$\mathcal{H} = \{xH : x \in G\}.$$

Seuraavaksi osoitetaan, että

$$xH \cap yH \neq \emptyset \Longrightarrow xH = yH.$$

Tämän jälkeen valitaan jokaiselle $F \in \mathcal{H}$ edustaja $x_F \in G$, jolle $x_F H = F$. Määretellään kuvaus

$$\alpha\colon \mathcal{H} \times H \to G\colon (F, y) \mapsto x_F y$$

ja osoitetaan, että se on bijektio. Siten $\#G = \#\mathcal{H}\#H$. □

Lauseen 2.32 todistus. Merkitään $m = \mathrm{ord}_n(a)$. Koska Lauseen 2.26 nojalla $[\Phi_n]$ on Abelin ryhmä, Lauseen 2.20 mukaan $\#[\Phi_n] = \varphi(n)$ ja $\mathrm{ord}_n(a) = \#\{[a^k]_n : k \in \mathbb{Z}\}$, antaa Lause 2.33

$$m \mid \varphi(n)$$

eli

$$\varphi(n) = mk \qquad \text{jollekin } k \in \mathbb{Z}.$$

Toisaalta

$$[a]_n^m = [a^m]_n = [1]_n.$$

Siis

$$[a^{\varphi(n)}]_n = [a]_n^{\varphi(n)} = [a]_n^{mk} = ([a]_n^m)^k = [1]_n^k = [1^k]_n = [1]_n.$$

□

Eulerin lausetta voidaan hyödyntää laskettaessa suuria potensseja jonkin modulin suhteen.

Esimerkki 2.34. Lasketaan mitkä ovat luvun 77^{482} kaksi viimeistä numeroa kymmenjärjestelmässä. Tehtävänä on siis selvittää mitä on

$$[77^{482}]_{100}.$$

Koska $\mathrm{syt}(77, 100) = 1$, voidaan käyttää Eulerin lausetta. Lasketaan siis ensin

$$\varphi(100) = (5^2 - 5)(2^2 - 2) = 40.$$

Siten

$$\begin{aligned}[77^{482}]_{100} &= [77^{40}]_{100}^{12} \cdot [(-23)^2]_{100} = [77^{\varphi(100)}]_{100}^{12} \cdot [529]_{100} \\ &= [1]_{100}^{12} \cdot [29]_{100} = [29]_{100}.\end{aligned}$$

Lause 2.35. *Olkoon $n \in \mathbb{N}$, $n \geq 2$ ja $a \in \mathbb{Z}$ siten, että* $\mathrm{syt}(a, n) = 1$. *Tällöin*

$$\mathrm{ord}_n(a) \mid \varphi(n).$$

Todistus. Lauseen 2.32 nojalla

$$[a^{\varphi(n)}]_n = [1]_n,$$

joten väite seuraa Lemmasta 2.30. □

Esimerkki 2.36. Lasketaan $\mathrm{ord}_{19}(5)$. Koska $\mathrm{syt}(5, 19) = 1$, on kertaluku määritelty. Tiedetään Lauseen 2.35 perusteella, että $\mathrm{ord}_{19}(5) \mid \varphi(19) = 19 - 1 = 18$ eli $\mathrm{ord}_{19}(5) \in \{1, 2, 3, 6, 9, 18\}$. Lasketaan siis

$$\begin{aligned}
[5^1]_{19} &= [5]_{19} \neq [1]_{19}, \\
[5^2]_{19} &= [25]_{19} = [6]_{19} \neq [1]_{19}, \\
[5^3]_{19} &= [5 \cdot 6]_{19} = [11]_{19} \neq [1]_{19}, \\
[5^6]_{19} &= [11^2]_{19} = [121]_{19} = [7]_{19} \neq [1]_{19}, \\
[5^9]_{19} &= [11 \cdot 7]_{19} = [1]_{19}.
\end{aligned}$$

Siten $\mathrm{ord}_{19}(5) = 9$.

Määritelmä 2.37. Olkoon $n \in \mathbb{N}$, $n \geq 2$, ja $a \in \mathbb{Z}$ siten, että $\mathrm{syt}(a, n) = 1$. Tällöin a on primitiivinen juuri modulo n, jos

$$\mathrm{ord}_n(a) = \varphi(n).$$

Lause 2.38. *Olkoon p alkuluku. Tällöin primitiivisiä juuria modulo p on täsmälleen $\varphi(p-1)$ kappaletta.*

Todistus. (Ohitetaan todistus.) □

Esimerkki 2.39. Etsitään kaikki primitiiviset juuret modulo 5. Lauseen 2.38 mukaan niitä on $\varphi(5-1) = \varphi(4) = 2^2 - 2^1 = 2$ kappaletta. Koska $\varphi(5) = 4$, on $\mathrm{ord}_5(a) \in \{1, 2, 4\}$ kaikille $a \in \{1, 2, 3, 4\}$. Lasketaan

$$\begin{aligned}
[2^1]_5 &\neq [1]_5, \\
[2^2]_5 = [4]_5 &\neq [1]_5.
\end{aligned}$$

Siis $\mathrm{ord}_5(2) = 4$.

$$\begin{aligned}
[3^1]_5 &\neq [1]_5, \\
[3^2]_5 = [4]_5 &\neq [1]_5.
\end{aligned}$$

Siis $\mathrm{ord}_5(3) = 4$. Siten etsityt primitiiviset juuret ovat 2 ja 3.

Otetaan vielä esimerkki primitiivisten juurten käytöstä käytännössä.

Esimerkki 2.40 (Diffie-Hellmannin avainmenvaihtoprotokolla). Tavoitteena on konstruoida salausavain joka on vain osapuolten A ja B tiedossa. Tehdään se vaiheittain

(1) Valitaan suuri alkuluku p ja primitiivinen juuri g (modulo p). Nämä voidaan julkaista.
(2) A valitsee satunnainen kokonaisluvun $a \in \{1, 2, \ldots, p-1\}$ ja B luvun $b \in \{1, 2, \ldots, p-1\}$.
(3) A lähettää B:lle luvun g^a jakojäännöksen luvun p suhteen, ja B lähettää A:lle luvun g^b jakojäännöksen luvun p suhteen.
(4) Sekä A että B laskevat salausavaimen $[g^{ab}]_p = [g^a]_p^b = [g^b]_p^a$.

Protokolla toimii, koska luvun g^a jakojäännöksestä luvun p suhteen on hyvin vaikeata laskea lukua a. Toisaalta potenssin $[g^a]_p$ laskeminen ei ole kovin vaikeata.

Nopea potenssilasku. Tarkastellaan potenssilaskua

$$[g^a]_p.$$

Käyttämällä luvun a binääriesitystä

$$a = \sum_{i=1}^{k} a_i 2^i,$$

missä $a_i \in \{0, 1\}$, $k \in \mathbb{N}$ ja $a_k = 1$, voidaan $[g^a]_p$ laskea toistuvasti neliöimällä

$$[g^{2^i}]_p = [g^{2^{i-1}}]_p^2$$

ja lopuksi laskemalla

$$[g^a]_p = \prod_{i=1}^{k} [g^{2^i}]_p^{a_i}.$$

Esimerkki 2.41. Lasketaan $[5^{22}]_{47}$. Kirjoitetaan ensin $22 = 16+4+2 = 10110_2$ ja lasketaan (mod 47)

$$5^2 = 25,$$
$$5^4 = 625 \equiv 14,$$
$$5^8 = 196 \equiv 8,$$
$$5^{16} = 64 \equiv 17.$$

Siten $5^{22} \equiv 17^1 \cdot 8^0 \cdot 14^1 \cdot 25^1 \cdot 5^0 = 350 \cdot 17 \equiv 21 \cdot 17 = 357 \equiv 28$ (mod 47).

Käytännössä neliöinti tehdään tietokoneella laskiessa lähtien korkeimmasta bitistä. Lasketaan esimerkiksi uudestaan $[5^{22}]_{47}$. Siis $22 = 10110_2$. Ensin siis lasketaan potenssi $1_2 = 1$ eli

$$[5^1]_{47} = [5]_{47}$$

Tämän jälkeen potenssi $10_2 = 1_2^2$ eli

$$[5^2]_{47} = [25]_{47}.$$

Sitten potenssi $101_2 = 10_2 \cdot 10_2 + 1_2$ eli

$$[5^4 \cdot 5]_{47} = [25]_{47}^2 \cdot [5]_{47} = [23]_{47}$$

ja sitten potenssi $1011_2 = 10_2 \cdot 101_2 + 1_2$ eli

$$[5^{10} \cdot 5]_{47} = [23]_{47}^2 \cdot [5]_{47} = [13]_{47}.$$

Lopuksi vielä potenssi $10110_2 = 10_2 \cdot 1011_2$ eli

$$[5^{22}]_{47} = [13]_{47}^2 = [28]_{47}.$$

Otetaan vielä toinen esimerkki edellä esitellystä potenssiin korottamisesta. Testataan onko luku 167 Mersennen luvun $M_{83} = 2^{83} - 1$ tekijä. Kirjoitetaan ensin $83 = 64 + 16 + 2 + 1 = 1010011_2$ ja edetään

sitten bitti kerrallaan (mod 167)

$$\begin{aligned} 2 &= 2, \\ 2^2 &= 4, \\ 2 \cdot 4^2 &= 32, \\ 32^2 &= 1024 \equiv 22, \\ 22^2 &= 484 \equiv -17, \\ 2 \cdot 17^2 &= 578 \equiv 77, \\ 2 \cdot 77^2 &= 2 \cdot 5929 \equiv 2 \cdot 84 = 168 \equiv 1. \end{aligned}$$

Siis $[2^{83}]_{167} = [1]_{167}$ eli $167 \mid 2^{83} - 1$.

Palataan nyt potenssilaskuista takaisin lukuteorian klassisiin tuloksiin. Erikoistapauksena Eulerin lauseesta saadaan Fermat'n pieni lause.

Lause 2.42 (Fermat'n pieni lause)**.** *Olkoon p alkuluku ja $a \in \mathbb{Z}$. Tällöin*

$$[a^p]_p = [a]_p.$$

Jos lisäksi $p \nmid a$, niin

$$[a^{p-1}]_p = [1]_p.$$

Todistus. Osoitetaan ensin jälkimmäinen väite. Oletetaan, että $p \nmid a$. Koska p on alkuluku, on $\operatorname{syt}(a, p) = 1$. Toisaalta Lauseen 2.21 perusteella $\varphi(p) = p - 1$. Siten Lauseen 2.32 mukaan

$$[a^{p-1}]_p = [1]_p.$$

Tällöin myös

$$[a^p]_p = [a]_p[a^{p-1}]_p = [a]_p[1]_p = [a]_p.$$

Todistetaan tämä myös tapauksessa $p \mid a$. Tällöin $p \mid a^p$ eli

$$[a^p]_p = [0]_p = [a]_p.$$

□

Lause 2.43 (Wilsonin lause)**.** *Olkoon p alkuluku. Tällöin*

$$[(p-1)!]_p = [-1]_p.$$

Todistus. Koska p on alkuluku, on $\mathbb{Z}_p$ kunta Lauseen 2.18 nojalla. Siten jokaisella $[a]_p \in \mathbb{Z}_p \setminus \{[0]_p\}$ on olemassa käänteisalkio $[b]_p \in \mathbb{Z}_p$ eli $[b]_p[a]_p = [1]_p$. Jos $[a]_p = [b]_p$, on $[a]_p^2 = [1]_p$ eli $[a-1]_p[a+1]_p = [0]_p$. Yhä koska $\mathbb{Z}_p$ on kunta, on tällöin joko $[a]_p = [1]_p$ tai $[a]_p = [-1]_p$.

Siis kaikille alkioille $[a]_p \in \mathbb{Z}_p \setminus \{[0]_p, [1]_p, [p-1]_p\}$ on olemassa yksikäsitteinen käänteisalkio $[b]_p \neq [a]_p$. Siten kaikki muut tulon $[(p-1)!]_p$ tekijät paitsi $[1]_p$ ja $[p-1]_p$ voidaan järjestää pareiksi joiden tulo on $[1]_p$. Siispä

$$[(p-1)!]_p = [p-1]_p = [-1]_p.$$

□

2.5. **Kiinalainen jäännöslause.** Kiinalainen munkki Sun Zi esitti aikoinaan seuraavan arvoituksen

> *Meillä on jokin määrä esineitä, mutta emme tarkkaan tiedä montako. Jos esineet jaetaan kolmen ryhmiin, jää kaksi yli. Jos ne jaetaan viiden ryhmiin, jää kolme yli. Jos ne taas jaetaan seitsemän ryhmiin, jää kaksi yli. Montako esinettä meillä on?*

Tämän kurssin merkinnöillä arvoitus voidaan voidaan muotoilla yhtälöryhmäksi

$$\begin{cases} [x]_3 = [2]_3 \\ [x]_5 = [3]_5 \\ [x]_7 = [2]_7, \end{cases}$$

jonka ratkaisua x siis etsitään.

Määritelmä 2.44. Olkoon $k \geq 2$, $a_1, \ldots, a_k \in \mathbb{Z}$ ja $m_1, \ldots, m_k \geq 2$. Lukua $x \in \mathbb{Z}$ sanotaan lineaarisen kongruenssiyhtälöryhmän

$$\begin{cases} [x]_{m_1} = [a_1]_{m_1} \\ [x]_{m_2} = [a_2]_{m_2} \\ \vdots \\ [x]_{m_k} = [a_k]_{m_k} \end{cases}$$

ratkaisuksi, jos $[x]_{m_i} = [a_i]_{m_i}$ kaikilla $i = 1, \ldots, k$.

Todistetaan seuraavaksi riittävä ehto kongruenssiyhtälöryhmän ratkaisun olemassaololle.

Lause 2.45 (Kiinalainen jäännöslause)**.** *Olkoon $k \geq 2$, $a_1, \ldots, a_k \in \mathbb{Z}$ ja $m_1, \ldots, m_k \geq 2$. Jos*

$$\operatorname{syt}(m_i, m_j) = 1$$

kaikilla $i \neq j$, on kongruenssiyhtälöryhmällä

$$\begin{cases} [x]_{m_1} = [a_1]_{m_1} \\ [x]_{m_2} = [a_2]_{m_2} \\ \vdots \\ [x]_{m_k} = [a_k]_{m_k} \end{cases}$$

ratkaisu.

Jos yhtälöryhmällä on ratkaisu $x \in \mathbb{Z}$, on $y \in \mathbb{Z}$ myös ratkaisu jos ja vain jos

$$[y]_t = [x]_t, \qquad \text{missä } t = \prod_{i=1}^{k} m_i.$$

Todistus. Todistetaan ensin induktiolla että yhtälöryhmällä on eräs ratkaisu. Yhtälöllä

$$[x]_{m_1} = [a_1]_{m_1}$$

on triviaali ratkaisu $x = a_1$. Oletetaan seuraavaksi, että jollain $1 \leq n < k$ on yhtälöryhmällä

$$\begin{cases} [x]_{m_1} = [a_1]_{m_1} \\ [x]_{m_2} = [a_2]_{m_2} \\ \vdots \\ [x]_{m_n} = [a_n]_{m_n} \end{cases}$$

ratkaisu z. Merkitään

$$m = \prod_{i=1}^{n} m_i.$$

Jos alkuluvulle p on $p \mid m$, on silloin Lauseen 1.13 nojalla olemassa i siten, että $p \mid m_i$. Koska $\text{syt}(m_i, m_{n+1}) = 1$ on välttämättä $p \nmid m_{n+1}$. Siispä $\text{syt}(m, m_{n+1}) = 1$. Tarkastellaan nyt yhtälöparia

$$\begin{cases} [x]_m = [z]_m \\ [x]_{m_{n+1}} = [a_{n+1}]_{m_{n+1}}. \end{cases} \tag{6}$$

Lauseen 1.39 mukaan on lineaarisella Diofantoksen yhtälöllä

$$mx_0 + m_{n+1}x_1 = z - a_{n+1}$$

ratkaisu $(x_0, x_1) \in \mathbb{Z}^2$. Merkitään

$$x = z - mx_0.$$

Tällöin

$$[x]_m = [z - mx_0] = [a]_m.$$

Toisaalta

$$x = z - mx_0 = a_{n+1} + m_{n+1}x_1,$$

joten

$$[x]_{m_{n+1}} = [a_{n+1} + m_{n+1}x_1]_{m_{n+1}} = [a_{n+1}]_{m_{n+1}}.$$

Siis x on yhtälöparin (6) ratkaisu.

Osoitetaan seuraavaksi, että x on myös yhtälöiden $[x]_{m_i} = [a_i]_{m_i}$ ratkaisu kaikilla $i = 1, \ldots, n$. Koska $[x]_m = [z]_m$, on

$$m \mid x - z.$$

Koska $m_i \mid m$, on edelleen

$$m_i \mid x - z$$

eli $x - z = rm_i$ jollain $r \in \mathbb{Z}$. Toisaalta $[z]_{m_i} = [a_i]_{m_i}$, joten $z - a_i = sm_i$ jollain $s \in \mathbb{Z}$. Siten

$$x - a_i = x - z + z - a_i = rm_i + sm_i = (r + s)m_i$$

ja siis

$$[x]_{m_i} = [a_i]_{m_i}.$$

Löysimme siis yhtälöryhmälle

$$\begin{cases} [x]_{m_1} = [a_1]_{m_1} \\ [x]_{m_2} = [a_2]_{m_2} \\ \vdots \\ [x]_{m_{n+1}} = [a_{n+1}]_{m_{n+1}} \end{cases}$$

ratkaisun, joten lauseen ensimmäinen osa on todistettu.

Osoitetaan seuraavaksi, että mikäli x ja y ovat lauseen kongruenssyhtälöryhmän ratkaisuja, on

$$[y]_t = [x]_t.$$

Halutaan siis osoittaa, että $t \mid x - y$. Nyt kaikilla $i = 1, \ldots, m$ on

$$[y]_{m_i} = [a_i]_{m_i} = [x]_{m_i}$$

eli

$$m_i | x - y.$$

Olkoon p alkuluku ja $n \in \mathbb{N}$ siten, että $p^n \mid t$ ja $p^{n+1} \nmid t$. Koska $\text{syt}(m_i, m_j) = 1$ kaikilla $i \neq j$, täytyy olla olemassa $i \in \{1, \ldots, m\}$ siten, että $p^n \mid m_i$. Siispä

$$p^n \mid x - y$$

ja siten

$$t \mid x - y.$$

Lopuksi tulee vielä osoittaa, että mikäli x on kongruenssiyhtälöryhmän ratkaisu ja $y \in \mathbb{Z}$ on siten, että

$$[y]_t = [x]_t,$$

on myös y kongruenssiyhtälön ratkaisu. Koska $t \mid x - y$ ja $m_i \mid t$ kaikilla i, on myös $m_i \mid x - y$ kaikilla i eli

$$[y]_{m_i} = [x]_{m_i} = [a_i]_{m_i}$$

kaikilla i. □

Esimerkki 2.46. Ratkaistaan nyt alussa esitetty arvoitus, joka kongruenssiyhtälöryhmänä oli

$$\begin{cases} [x]_3 = [2]_3 \\ [x]_5 = [3]_5 \\ [x]_7 = [2]_7. \end{cases}$$

Koska

$$\text{syt}(3, 5) = \text{syt}(3, 7) = \text{syt}(5, 7) = 1,$$

on yhtälöryhmällä kiinalaisen jäännöslauseen nojalla olemassa ratkaisu. Etsitään sille ratkaisu kiinalaisen jäännöslauseen todistuksen osoittamalla tavalla. Siis etsitään ensin yhtälöparin

$$\begin{cases} [x]_3 = [2]_3 \\ [x]_5 = [3]_5 \end{cases} \tag{7}$$

ratkaisu. Tällainen löydetään siis vastaavan Diofantoksen yhtälön

$$3x_0 + 5x_1 = 2 - 3 = -1$$

ratkaisuna. Kyseinen Diofantoksen yhtälö taas voidaan muuttaa kongruenssiyhtälöksi

$$[3]_5 \cdot [x_0]_5 = [-1]_5,$$

jonka ratkaisu on

$$[x_0]_5 = [3]_5.$$

Siten eräs yhtälöparin (7) ratkaisu on

$$z = 2 - 3x_0 = -7.$$

Alkuperäisen yhtälöryhmän ratkaisu saadaan siis nyt ratkaisemalla yhtälöpari

$$\begin{cases} [x]_{15} = [-7]_{15} \\ [x]_7 = [2]_7. \end{cases} \tag{8}$$

Tästä saadaan Diofantoksen yhtälö

$$15y_0 + 7y_1 = -7 - 2 = -9,$$

joka muuntuu kongruenssiyhtälöksi

$$[15]_7 \cdot [y_0]_7 = [-9]_7.$$

Tämän ratkaisu taas on

$$[y_0]_7 = [5]_7.$$

Yhtälöparin (8) ja alkuperäisen yhtälöryhmän ratkaisu on siis

$$x = -7 - 15y_0 = -82.$$

Kaikki ratkaisut ovat nyt muotoa

$$y = x + k(3 \cdot 5 \cdot 7) = -82 + 105k, \qquad k \in \mathbb{Z}.$$

Pienin positiivinen ratkaisu on siis

$$y = 23.$$

Otetaan vielä toinen esimerkki kiinalaisen jäännöslauseen käytöstä.

Esimerkki 2.47. Ratkaistaan yhtälöryhmä

$$\begin{cases} [x]_2 = [1]_2 \\ [x]_9 = [7]_9 \\ [x]_{11} = [6]_{11}. \end{cases}$$

Tarkistetaan ensin, että ratkaisu on olemassa. Näin on, sillä $\text{syt}(2, 9) = \text{syt}(2, 11) = \text{syt}(9, 11) = 1$. Edetään nyt kuten edellisessä esimerkissä. Ratkaistaan siis ensin yhtälöpari

$$\begin{cases} [x]_2 = [1]_2 \\ [x]_9 = [7]_9. \end{cases}$$

Muunnetaan tämä Diofantoksen yhtälöksi

$$2x_1 + 9x_2 = 2 - 9 = -7,$$

jonka eräs ratkaisu on $x_1 = -3$ ja $x_2 = 0$. Siten yhtälöparin eräs ratkaisu on $z = 1 - 2 \cdot (-3) = 7$. Alkuperäisen yhtälöryhmän ratkaisu löydetään siis yhtälöparin

$$\begin{cases} [x]_{18} = [7]_{18} \\ [x]_{11} = [6]_{11} \end{cases}$$

ratkaisuna. Jälleen Diofantoksen yhtälönä kirjoitettuna

$$18x_1 + 11x_2 = 7 - 6 = 1,$$

jonka ratkaisu löydetään vaikkapa Eukleideen algoritmillä

$$\begin{aligned} 18 &= 11 + 7 \\ 11 &= 7 + 4 \\ 7 &= 4 + 3 \\ 4 &= 3 + 1 \end{aligned}$$

eli

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2(11 - 7) - 7 \\ &= 2 \cdot 11 - 3 \cdot 7 = 2 \cdot 11 - 3(18 - 11) = 5 \cdot 11 - 3 \cdot 18. \end{aligned}$$

Yhtälöparin ratkaisu on siis $x = 7 - 18 \cdot (-3) = 61$ ja kaikki alkuperäisen yhtälöryhmän ratkaisut saadaan

$$x = 61 + 2 \cdot 9 \cdot 11 \cdot k = 61 + 198k \qquad , k \in \mathbb{Z}.$$

3. Neliönjäännökset

Tutkitaan hieman korkeamman asteen kongruenssiyhtälöitä.

Lause 3.1. *Olkoon p alkuluku, $n \geq 1$ ja $a_0, \ldots, a_n \in \mathbb{Z}$ siten, että $[a_n]_p \neq [0]_p$. Tällöin n. asteen kongruenssiyhtälöllä*

$$P_n(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p} \tag{9}$$

on korkeintaan n ratkaisua.

Todistus. Olkoon $x_1, \ldots, x_m$, $m \leq n$, kongruenssiyhtälön (9) eri ratkaisuja (mod p). Koska $\mathbb{Z}_p$ on kunta, on alkiolla $[x - x_i]_p$ käänteisalkio, kun $[x]_p \neq [x_i]_p$. Siten voidaan kirjoittaa

$$P_n(x) \equiv (x - x_1) \cdots (x - x_m) P_{n-m}(x) \pmod{p},$$

missä $P_{n-m}(x)$ on asteen $n - m$ polynomi. Jos $n = m$, on

$$P_n(x) \equiv (x - x_1) \cdots (x - x_n) P_0(x) \pmod{p},$$

missä siis $[P_0(x)]_p = [a_n]_p \neq [0]_p$ on vakio. Siten yhtälöllä (9) ei voi olla muita ratkaisuja. □

Määritelmä 3.2. Olkoon p pariton alkuluku ja $a \in \mathbb{Z}$ siten, että $p \nmid a$. Sanotaan, että a on neliönjäännös (mod p), jos yhtälöllä

$$[x^2]_p = [a]_p$$

on olemassa ratkaisu $x \in \mathbb{Z}$. Jos yhtälöllä ei ole ratkaisua, on luku a epäjäännös (mod p).

Lause 3.3. *Olkoon p pariton alkuluku ja $a \in \mathbb{Z}$ siten, että $p \nmid a$. Tällöin a on neliönjäännös (mod p) jos ja vain jos*

$$[a^{(p-1)/2}]_p = [1]_p.$$

Vastaavasti a on epäjäännös (mod p) jos ja vain jos

$$[a^{(p-1)/2}]_p = [-1]_p.$$

Todistus. Olkoon nyt p pariton alkuluku ja $a \in \mathbb{Z}$ siten, että $p \nmid a$. Tällöin Fermat'n lauseen (Lause 2.42) nojalla

$$[a^{p-1}]_p = [1]_p.$$

Koska $p-1$ on parillinen ja

$$a^{p-1} - 1 = (a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1),$$

on Lauseen 1.13 mukaan joko

$$[a^{(p-1)/2}]_p = [1]_p$$

tai

$$[a^{(p-1)/2}]_p = [-1]_p.$$

Jos a on neliönjäännös eli $[a]_p = [b^2]_p$ jollain $b \in \mathbb{Z}$, on $p \nmid b$. Siten myös $p \nmid 2b$ eli

$$[b]_p \neq [-b]_p.$$

Toisaalta myös $[(-b)^2]_p = [a]_p$. Muita ratkaisuja ei yhtälöllä

$$[x^2]_p = [a]_p$$

Lauseen 3.1 mukaan olekaan. Siten neliönjäännöksiä on olemassa täsmälleen $(p-1)/2$ kappaletta (mod p).

Toisaalta neliönjäännökselle a on Fermat'n lauseen nojalla

$$[a^{(p-1)/2}]_p = [b^{p-1}]_p = [1]_p$$

ja Lauseen 3.1 mukaan yhtälöllä

$$[x^{(p-1)/2}]_p = [1]_p$$

on korkeintaan $(p-1)/2$ ratkaisua (mod p). Siten kaikille epäjäännöksille a täytyy olla

$$[a^{(p-1)/2}]_p = [-1]_p.$$

□

Esimerkki 3.4. Määräämällä lukujen $1, \ldots, \frac{p-1}{2}$ neliöiden jäännösluokat saadaan neliönjäännökset (mod p), kun esimerkiksi $p = 7, 11, 13$.

a) $[1^2]_7 = [1]_7$, $[2^2]_7 = [4]_7$ ja $[3^2]_7 = [2]_7$.

b) $[1^2]_{11} = [1]_{11}$, $[2^2]_{11} = [4]_{11}$, $[3^2]_{11} = [9]_{11}$, $[4^2]_{11} = [5]_{11}$ ja $[5^2]_{11} = [3]_{11}$.
c) $[1^2]_{13} = [1]_{13}$, $[2^2]_{13} = [4]_{13}$, $[3^2]_{13} = [9]_{13}$, $[4^2]_{13} = [3]_{13}$, $[5^2]_{13} = [12]_{13}$ ja $[6^2]_{13} = [10]_{13}$.

Määritelmä 3.5. Olkoon p pariton alkuluku ja $a \in \mathbb{Z}$ siten, että $p \nmid a$. Määritellään lukujen a ja p Legendren symboli $\left(\frac{a}{p}\right)$ asettamalla

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{kun } a \text{ on neliönjäännös} \pmod p, \\ -1, & \text{kun } a \text{ on epäjäännös} \pmod p. \end{cases}$$

Edellinen lause voidaan siis kirjoittaa muodossa

Lause 3.6. *Olkoon p pariton alkuluku ja $a \in \mathbb{Z}$ siten, että $p \nmid a$. Tällöin*

$$[a^{(p-1)/2}]_p = [\left(\frac{a}{p}\right)]_p$$

Lause 3.7. *Olkoon p pariton alkuluku ja $a, b \in \mathbb{Z}$ siten, että $p \nmid a, b$. Tällöin*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Todistus. Lauseen 3.6 nojalla

$$[\left(\frac{ab}{p}\right)]_p = [(ab)^{(p-1)/2}]_p = [a^{(p-1)/2}]_p [b^{(p-1)/2}]_p = [\left(\frac{a}{p}\right)]_p [\left(\frac{b}{p}\right)]_p.$$

□

Lause 3.8 (Gaussin lemma)**.** *Olkoon p pariton alkuluku ja $a \in \mathbb{Z}$ siten, että $p \nmid a$. Olkoon s negatiivisten jäännösten lukumäärä jonon*

$$a, 2a, \ldots, \frac{p-1}{2}a$$

itseisarvoltaan pienimpien jäännösten (mod p) joukossa. Tällöin

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Todistus. Olkoon $c_k \in \mathbb{Z}$, $k = 1, \ldots, (p-1)/2$, siten, että

$$[ka]_p = [c_k]_p$$

ja

$$1 \leq |c_k| \leq \frac{p-1}{2}.$$

Nyt

$$[|c_k| - |c_j|]_p = [\pm(k \pm j)a]_p$$

ja $1 \leq k \pm j < p-1$ kaikilla $1 \leq j < k \leq (p-1)/2$. Lisäksi $p \nmid a$, joten

$$[|c_k|]_p \neq [|c_j|]_p$$

kaikilla $k \neq j$. Siten (mod p)

$$((p-1)/2)!a^{\frac{p-1}{2}} = \prod_{k=1}^{\frac{p-1}{2}} ka \equiv \prod_{k=1}^{\frac{p-1}{2}} c_k = (-1)^s \prod_{k=1}^{\frac{p-1}{2}} |c_k| = ((p-1)/2)!(-1)^s.$$

Koska

$$[((p-1)/2)!]_p \neq [0]_p,$$

on

$$[a^{\frac{p-1}{2}}]_p = [(-1)^s]_p$$

ja väite siten seuraa Lauseesta 3.6. □

Lause 3.9. *Kun p on pariton alkuluku, on*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Todistus. Käytetään Lausetta 3.8 tapauksessa $a = 2$. Tällöin jonon

$$2, 4, \ldots, p-3, p-1$$

itseisarvoiltaan pienimmistä jäännöksistä negatiivisia ovat

$$-1, -2, \ldots, -(2s-1) > -\frac{p}{2},$$

missä $2s-1$ on suurin pariton luku, joka on pienempi kuin $p/2$. Siten

$$2s-1 = \frac{p-1}{2} \qquad \text{tai} \qquad 2s-1 = \frac{p-3}{2}.$$

Tällöin $s = \frac{p\pm1}{4}$, joka parillinen silloin, kun $p = 8n \pm 1$, ja pariton, kun $p = 8n \pm 3$. Väite seuraa nyt yhtälöstä

$$[((8n \pm k)^2 - 1)/8]_2 = [(k^2-1)/8]_2, \qquad k = 1, 3.$$

□

3.1. **Resiprookkilause.**

Lause 3.10. *Kun p ja q ovat parittomia alkulukuja, niin*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Todistus. Gaussin lemman (Lause 3.8) nojalla

$$\left(\frac{q}{p}\right) = (-1)^s,$$

kun jonon

$$q, 2q, \ldots, \frac{p-1}{2}q$$

itseisarvoltaan pienimmistä jäännöksistä (mod p) negatiivisia on s kappaletta. Jotta luvun hq, $1 \leq h \leq (p-1)/2$, itseisarvoltaan pienin jäännös (mod p) olisi negatiivinen, täytyy epäyhtälön

$$-\frac{p}{2} < hq - kp < 0$$

toteutua jollain $1 \leq k \in \mathbb{N}$, jolloin

$$(2k-1)p < 2hq \leq (p-1)q = pq - q,$$

ja siten täytyy olla

$$1 \leq k \leq \frac{q-1}{2}.$$

Vastaavasti

$$\left(\frac{p}{q}\right) = (-1)^t,$$

kun jonon

$$p, 2p, \ldots, \frac{q-1}{2}p$$

itseisarvoltaan pienimmistä jäännöksistä (mod q) negatiivisia on t kappaletta. Kuten edellä, on luvun kp, $1 \leq p \leq (q-1)/2$ itseisarvoltaan pienin jäännös (mod q) negatiivinen, jos ja vain jos on olemassa kerroin $1 \leq h \leq (p-1)/2$ siten, että

$$-\frac{q}{2} < kp - hq < 0,$$

eli

$$0 < hq - kp < \frac{q}{2}.$$

Siten on $s+t$ lukuparia (h,k), $1 \leq h \leq (p-1)/2$, $1 \leq k \leq (q-1)/2$, jolle on voimassa epäyhtälö

$$-\frac{p}{2} < hq - kp < \frac{q}{2}.$$

Siten on

$$\frac{(p-1)(q-1)}{4} - (s+t)$$

sellaista lukuparia, jolle

$$hq - kp \notin]-\frac{p}{2}, \frac{q}{2}[.$$

Jos nyt lukupari (h,k) toteuttaa ehdot $1 \leq h \leq (p-1)/2$ ja $1 \leq k \leq (q-1)/2$, ovat nämä ehdot myös tosia luvuille

$$h' = \frac{p+1}{2} - h \qquad \text{ja} \qquad k- = \frac{q+1}{2} - k,$$

eli siis $1 \leq h' \leq (p-1)/2$ ja $1 \leq k' \leq (q-1)/2$. Lisäksi

$$(hq - kp) + (h'q - k'p) = \frac{p+1}{2}q - \frac{q+1}{2}p = -\frac{p}{2} + \frac{q}{2},$$

joten (h,k) toteuttaa epäyhtälön

$$hq - kp < -\frac{p}{2}$$

jos ja vain jos sitä vastaava pari (h',k') toteuttaa epäyhtälön

$$\frac{q}{2} < h'q - k'p.$$

Jos epäyhtälö $hq - kp < -\frac{p}{2}$ toteutuu r määrällä pareja (h,k), niin kaikkiaan $2r$ parilla (h,k) on $hq - kp \notin]-\frac{p}{2}, \frac{q}{2}[$. Siten

$$s + t = \frac{(p-1)(q-1)}{4} - 2r,$$

josta saadaan

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^t(-1)^s = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}-2r} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

□

Esimerkkejä 3.11.

a)

$$\left(\frac{97}{101}\right) = \left(\frac{101}{97}\right) = \left(\frac{4}{97}\right) = \left(\frac{2}{97}\right)^2 = 1.$$

b)

$$\begin{aligned}\left(\frac{71}{83}\right) &= -\left(\frac{83}{71}\right) = -\left(\frac{12}{71}\right) = -\left(\frac{3}{71}\right)\left(\frac{4}{71}\right) \\ &= -\left(\frac{3}{71}\right)\left(\frac{2}{71}\right)^2 = \left(\frac{71}{3}\right) = \left(\frac{-1}{3}\right) = -1.\end{aligned}$$

3.2. **Jacobin yleistetty symboli.** Yleistetään Legendren symbolin määritelmä seuraavasti.

Määritelmä 3.12. Olkoon $a, b \in \mathbb{Z}$ siten, että $2 \nmid b$ ja $\text{syt}(a,b) = 1$. Tällöin määritellään lukujen a ja b Jacobin symboli asettamalla

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{k_1}\left(\frac{a}{p_2}\right)^{k_2}\cdots\left(\frac{a}{p_r}\right)^{k_r},$$

missä $b = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ on luvun b esitys alkulukupotenssien tulona.

Lause 3.13. *Olkoot $a, b, c \in \mathbb{Z}$ siten, että $\text{syt}(a,c) = \text{syt}(b,c) = 1$. Jos $c > 1$ on pariton, on*

$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right).$$

Jos taas $a, b > 1$ ovat parittomia, on

$$\left(\frac{c}{ab}\right) = \left(\frac{c}{a}\right)\left(\frac{c}{b}\right).$$

Todistus. Seuraa Lauseesta 3.7 ja alkutekijöihin jaon yksikäsitteisyydestä. □

Lause 3.14. *Kaikilla parittomilla $1 < a \in \mathbb{N}$ on*

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}$$

ja

$$\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}.$$

Jos $1 < a, b \in \mathbb{N}$ *ovat parittomia ja* $\text{syt}(a,b) = 1$, *on*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

Todistus. (Sivuutetaan) □

4. Alkulukutestausta

4.1. **Fermat.**

Lause 4.1. *Jos* p *on alkuluku ja* $\text{syt}(a,p) = 1$, *niin*

$$[a^{p-1}]_p = [1]_p.$$

Todistus. Seuraa suoraan Lauseesta 2.42. □

Esimerkkejä 4.2. a) Testataan lukua 2209.

$$[2^{2208}]_{2209} = [2069]_{2209} \neq [1]_{2209}$$

eli 2209 ei ole alkuluku.

b) Testataan seuraaksi lukua 2047. Nyt

$$[2^{2046}]_{2047} = [2^{11\cdot 186}]_{2047} = [2048^{186}]_{2047} = [1]_{2047},$$

joten vielä ei saatu ainakaan osoitettua että 2047 ei ole alkuluku.

$$[3^{2046}]_{2047} = \cdots = [1013]_{2047} \neq [1]_{2047}$$

eli 2047 ei ole alkuluku.

c) Testataan lukua 561.

$$[2^{560}]_{561} = [1]_{561}$$
$$[3^{560}]_{561} = [1]_{561}$$
$$[5^{560}]_{561} = [1]_{561}$$
$$\vdots$$

Osoittautuu, että luku 561 läpäisee Fermat'n testin. Se ei kuitenkaan ole alkuluku, vaan $561 = 3 \cdot 11 \cdot 17$.

4.2. **Legendre-Jacob.**

Fermat'n testiä voi hieman parantaa seuraavasti.

Lause 4.3. *Jos* p *on pariton alkuluku, niin*

$$[a^{(p-1)/2}]_p = [\left(\frac{a}{p}\right)]_p.$$

Todistus. Seuraa Lauseesta 3.6. □

4.3. **Miller-Rabin.**

Lause 4.4. *Jos p on pariton alkuluku ja $p-1=2^s d$, missä $1 \leq s$ ja d on pariton, niin kaikilla a joille* $\mathrm{syt}(a,p)=1$ *joko*

$$[a^d]_p = [1]_p$$

tai on $0 \leq r \leq s-1$ siten, että

$$[a^{2^r d}]_p = [-1]_p.$$

Todistus. Kun p on alkuluku on $\varphi(p) = p-1 = 2^s d$ jaollinen jokaisen alkion $[a] \in \mathbb{Z}_p \setminus \{0\}$ kertaluvulla. Jos siis ehto

$$[a^d]_p = [1]_p$$

ei toteudu, täytyy olla olemassa pienin $1 \leq t \leq s$ siten, että

$$[a^{2^t d}]_p = [1]_p.$$

Tällöin siis

$$[a^{2^{t-1} d}]_p \neq [1]_p.$$

Merkitään $b = a^{2^{t-1}d}$. Koska $[b^2]_p = [1]_p$ ja Lauseen 3.1 mukaan yhtälöllä $[x^2]_p = [1]_p$ on korkeintaan kaksi ratkaisua, on $[b]_p \in \{[1]_p, [-1]_p\}$. Siten $[b]_p = [-1]_p$ ja

$$[a^{2^r d}]_p = [-1]_p,$$

missä $0 \leq r = t-1 \leq s-1$. □

Esimerkki 4.5. Edellisessä esimerkissä olleelle luvulle 561 on

$$p - 1 = 560 = 2^4 \cdot 35.$$

Nyt

$$[2^{35}]_{561} = [263]_{561} \neq [1]_{561}$$

ja tästä edelleen

$$[2^{2 \cdot 35}]_{561} = [263^2]_{561} = [166]_{561} \neq [-1]_{561},$$

$$[2^{2^2 \cdot 35}]_{561} = [166^2]_{561} = [67]_{561} \neq [-1]_{561}$$

ja

$$[2^{2^3 \cdot 35}]_{561} = [67^2]_{561} = [1]_{561} \neq [-1]_{561}.$$

Siis 561 ei ole alkuluku.

4.4. **Pépin.** Pépinin testillä voidaan testata onko annettu Fermat'n luku $F_m = 2^{2^m} + 1$ alkuluku vai ei.

Lause 4.6. *Fermat'n luku F_m, $m > 0$, on alkuluku jos ja vain jos*

$$[3^{(F_m-1)/2}]_{F_m} = [-1]_{F_m}.$$

Todistus. Oletetaan ensin, että $[3^{(F_m-1)/2}]_{F_m} = [-1]_{F_m}$. Tällöin

$$[3^{F_m-1}]_{F_m} = [1]_{F_m}$$

ja siten Lemman 2.30 nojalla

$$\mathrm{ord}_{F_m}(3) \mid F_m - 1 = 2^{2^m}.$$

Toisaalta

$$\mathrm{ord}_{F_m}(3) \nmid \frac{F_m - 1}{2},$$

joten $\mathrm{ord}_{F_m}(3) = F_m - 1$. Siten Lauseen 2.31 mukaan F_m on alkuluku.

Todistetaan toinen suunta. Olkoon siis F_m alkuluku. Tällöin Lauseen 3.6 mukaan

$$[3^{(F_m-1)/2}]_{F_m} = [\left(\frac{3}{F_m}\right)]_{F_m}$$

Koska $[2^2]_3 = [1]_3$, on edelleen $[F_m]_3 = [2^{2^m}]_3 + [1]_3 = [-1]_3$. Siis jälleen Lauseen 3.6 mukaan

$$[\left(\frac{F_m}{3}\right)]_3 = [F_m^{(3-1)/2}]_3 = [-1]_3.$$

Resiprookkilauseen (Lause 3.10) mukaan

$$\left(\frac{F_m}{3}\right)\left(\frac{3}{F_m}\right) = (-1)^{\frac{F_m-1}{2}\frac{3-1}{2}} = (-1)^{2^{2^m-1}} = 1,$$

joten

$$\left(\frac{3}{F_m}\right) = -1.$$

□

Esimerkki 4.7. Testataan onko $F_3 = 2^{2^3} + 1 = 257$ alkuluku:

$$\begin{aligned}[3^{(F_3-1)/2}]_{257} &= [3^{2^7}]_{257} = [9^{2^6}]_{257} = [81^{2^5}]_{257} = [6561^{2^4}]_{257} \\ &= [(-121)^{2^4}]_{257} = [14641^{2^3}]_{257} = [(-8)^{2^3}]_{257} = [64^{2^2}]_{257} \\ &= [4096^2]_{257} = [(-16)^2]_{257} = [256]_{257} = [-1]_{257}.\end{aligned}$$

Lauseen 4.6 mukaan F_3 on siis alkuluku.

Edellisen esimerkin tapauksessa alkulukutestaus näytti turhankin pitkälliseltä. Hieman isommilla luvuilla Pépinin testin voima tulee kuitenkin esiin, sillä korotus potenssiin $(F_m - 1)/2$ voidaan tehdä neliöimällä $2^m - 1$ kertaa, kuten esimerkissä. Lisäksi laskeminen (mod F_m) pitää muistin tarpeen pienenä - tosin luvut F_m kasvavat hyvin nopeasti m:n kasvaessa, joten testi on käytännössä mahdollista tehdä vain noin parille kymmenelle ensimmäiselle Fermat'n luvulle.

Hyvin suuristakin Fermat'n luvuista tiedetään, että ne eivät ole alkulukuja, mutta vain koska niille on löydetty tekijä. Esimerkiksi

$$3 \cdot 2^{2478785} + 1 \mid F_{2478782}.$$

Kuten jo aikaisemmin todettiinkin ainoat tunnetut Fermat'n alkuluvut ovat F_0, F_1, F_2, F_3, F_4. Kaikki tunnetut Fermat'n lukujen tekijät löytyvät osoitteesta

`http://www.prothsearch.net/fermat.html`

4.5. **Lucas.**

Lause 4.8. *Olkoon $m > 1$. Jos on olemassa $x \in \mathbb{Z}$ siten, että*

$$[x^{m-1}]_m = [1]_m$$

ja

$$[x^{\frac{m-1}{q}}]_m \neq [1]_m$$

kaikille luvun $m-1$ alkulukutekijöille q, niin m on alkuluku.

Todistus. Koska $[x^{m-1}]_m = [1]_m$, niin $\mathrm{ord}_m(x) \mid m-1$. Jos $\mathrm{ord}_m(x) < m-1$, on olemassa $k \geq 2$ siten, että $m-1 = \mathrm{ord}_m(x) \cdot k$. Olkoon q luvun k alkulukutekijä. Tällöin

$$[x^{\frac{m-1}{q}}]_m = [x^{\frac{\mathrm{ord}_m(x)\cdot k}{q}}]_m = [x^{\mathrm{ord}_m(x)}]_m^{\frac{k}{q}} = [1]_m,$$

mikä on ristiriidassa oletuksen kanssa. Siten $\mathrm{ord}_m(x) = m-1$ ja Lauseen 2.31 mukaan m on alkuluku. □

4.6. **Lucas-Lehmer.** Lucas-Lehmerin testillä voidaan testata onko annettu Mersennen luku $M_p = 2^p - 1$ alkuluku vai ei.

Lause 4.9. *Olkoon $\{s_i\}_{i\in\mathbb{N}} \subset \mathbb{N}$ jono siten, että $s_0 = 4$ ja $s_i = s_{i-1}^2 - 2$, kun $i > 0$. Tällöin M_p on alkuluku jos ja vain jos*

$$[s_{p-2}]_{M_p} = [0]_{M_p}.$$

Aloitetaan lauseen todistus osoittamalla ensin seuraava aputulos.

Lemma 4.10. *Lauseessa 4.9 määritelty s_i saadaan kaikilla $i \in \mathbb{N}$ kaavastaa*

$$s_i = \omega^{2^i} + \overline{\omega}^{2^i},$$

missä $\omega = 2 + \sqrt{3}$ ja $\overline{\omega} = 2 - \sqrt{3}$.

Todistus. Osoitetaan väite induktiolla.

$$s_0 = 4 = 2 + \sqrt{3} + 2 - \sqrt{3} = \omega^{2^0} + \overline{\omega}^{2^0}.$$

Oletetaan nyt, että

$$s_i = \omega^{2^i} + \overline{\omega}^{2^i}$$

jollakin $i \in \mathbb{N}$. Tällöin

$$\begin{aligned} s_{i+1} &= s_i^2 - 2 = (\omega^{2^i} + \overline{\omega}^{2^i})^2 - 2 = \omega^{2^{i+1}} + \overline{\omega}^{2^{i+1}} + 2(\omega\overline{\omega})^{2^i} - 2 \\ &= \omega^{2^{i+1}} + \overline{\omega}^{2^{i+1}} + 2(\underbrace{(2+\sqrt{3})(2-\sqrt{3})}_{=1})^{2^i} - 2 = \omega^{2^{i+1}} + \overline{\omega}^{2^{i+1}}. \end{aligned}$$

□

Lauseen 4.9 todistus. Oletetaan, että $[s_{p-2}]_{M_p} = 0$. Tällöin on siis olemassa jokin $k \in \mathbb{Z}$ siten, että

$$kM_p = s_{p-2} = \omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}}. \tag{10}$$

Oletetaan, että M_p ei ole alkuluku. Koska M_p on pariton, on olemassa alkuluku $2 < q \leq \sqrt{M_p}$ siten, että $q \mid M_p$. Määritellään joukko

$$X = \{([a]_q, [b]_q) : [a]_q, [b]_q \in \mathbb{Z}_q\}$$

ja sinne sekä yhteenlasku

$$([a]_q, [b]_q) + ([c]_q, [d]_q) = ([a+c]_q, [b+d]_q)$$

että kertolasku

$$([a]_q, [b]_q) \cdot ([c]_q, [d]_q) = ([ac + 3bd]_q, [bc + ad]_q).$$

Alkion $([a]_q, [b]_q) \in X$ eräänä edustajana voi siis ymmärtää luvun $a + b\sqrt{3}$. Nyt $(X, +, \cdot)$ on rengas, muttei välttämättä kunta. Kuitenkin osajoukko

$$\begin{aligned} Y = \{([a]_q, [b]_q) \in X : &\text{ on olemassa } ([c]_q, [d]_q) \in X \text{ siten, että} \\ &([a]_q, [b]_q) \cdot ([c]_q, [d]_q) = ([1]_q, [0]_q)\} \end{aligned}$$

muodostaa kunnan $(Y \cup \{([0]_q, [0]_q)\}, +, \cdot)$.

Koska $\#\mathbb{Z}_q = q$ ja $([0]_q, [0]_q) \notin Y$, on $\#Y \leq q^2 - 1$. Yhtälöstä (10) saadaan nyt muoto

$$([0]_q, [0]_q) = ([kM_p]_q, [0]_q) = ([2]_q, [1]_q)^{2^{p-2}} + ([2]_q, [-1]_q)^{2^{p-2}}.$$

Koska $([2]_q, [1]_q) \cdot ([2]_q, [-1]_q) = ([1]_q, [0]_q)$, on

$$([2]_q, [1]_q), ([2]_q, [-1]_q) \in Y$$

ja siten

$$([2]_q, [1]_q)^{2^{p-1}} = ([-1]_q, [0]_q).$$

Edelleen

$$([2]_q, [1]_q)^{2^p} = ([-1]_q, [0]_q)^2 = ([1]_q, [0]_q).$$

Siispä nähdään, että

$$\operatorname{ord}(([2]_q, [1]_q)) \mid 2^p$$

Samoin kuin Lemmassa 2.30. Toisaalta saman lemman päättelyllä

$$\operatorname{ord}(([2]_q, [1]_q)) \nmid 2^{p-1}.$$

Siten täytyy välttämättä olla

$$\operatorname{ord}(([2]_q, [1]_q)) = 2^p.$$

Toisaalta kertaluku on korkeintaan ryhmän alkioiden lukumäärä eli

$$2^p \leq q^2 - 1 < q^2 \leq M_p = 2^p - 1.$$

Tämä on ristiriita, joten M_p on alkuluku.

Osoitetaan seuraavaksi väite toiseen suuntaa, eli oletetaan, että M_p on alkuluku. Koska

$$[M_p]_3 = [2^p]_3 - [1]_3 = [(-1)^p]_3 - [1]_3 = [-1]_3 - [1]_3 = [1]_3,$$

on

$$\left(\frac{M_p}{3}\right) = 1.$$

Siten Lauseen 3.10 nojalla

$$\left(\frac{3}{M_p}\right) = \left(\frac{M_p}{3}\right)(-1)^{\frac{M_p-1}{2}\frac{3-1}{2}} = (-1)^{2^{p-1}-1} = -1.$$

Siten Lause 3.6 antaa

$$[3^{(M_p-1)/2}]_{M_p} = [-1]_{M_p}. \tag{11}$$

Koska $[2^p]_{M_p} = [1]_{M_p}$, on

$$[2]_{M_p} = [2^{p+1}]_{M_p} = [2^{(p+1)/2}]^2_{M_p}$$

eli 2 on neliönjäännös ja siten

$$\left(\frac{2}{M_p}\right) = 1.$$

Jälleen Lause 3.6 antaa

$$[2^{(M_p-1)/2}]_{M_p} = [1]_{M_p}.$$

Olkoon X ja Y kuten yllä valinnalla $q = M_p$. Nyt binomikaavalla, Lauseella 2.42 ja yhtälöllä (11) nähdään, että

$$([6]_{M_p}, [2]_{M_p})^{M_p} = ([6^{M_p}]_{M_p}, [2^{M_p}3^{(M_p-1)/2}]_{M_p}) = ([6]_{M_p}, [-2]_{M_p}).$$

Koska

$$[24^{(M_p-1)/2}]_{M_p} = [2^{(M_p-1)/2}]^3_{M_p}[3^{(M_p-1)/2}]_{M_p} = [-1]_{M_p}$$

ja

$$([6]_{M_p}, [2]_{M_p})^2 = ([48]_{M_p}, [24]_{M_p}),$$

on

$$\begin{aligned}
&([24]_{M_p},[0]_{M_p})([2]_{M_p},[1]_{M_p})^{(M_p+1)/2}\\
&\quad=([-1]_{M_p},[0]_{M_p})([24]_{M_p}^{(M_p+1)/2},[0]_{M_p})([2]_{M_p},[1]_{M_p})^{(M_p+1)/2}\\
&\quad=([-1]_{M_p},[0]_{M_p})([24\cdot 2]_{M_p},[24]_{M_p})^{(M_p+1)/2}\\
&\quad=([-1]_{M_p},[0]_{M_p})([6]_{M_p},[2]_{M_p})^{M_p+1}\\
&\quad=([-1]_{M_p},[0]_{M_p})([6]_{M_p},[2]_{M_p})([6]_{M_p},[-2]_{M_p})\\
&\quad=([-1]_{M_p},[0]_{M_p})([24]_{M_p},[0]_{M_p}).
\end{aligned}$$

Lisäksi koska M_p on alkuluku, on $([24]_{M_p},[0]_{M_p})\in Y$ eli

$$([2]_{M_p},[1]_{M_p})^{(M_p+1)/2}=([-1]_{M_p},[0]_{M_p}).$$

Nyt

$$\begin{aligned}
&([2]_{M_p},[1]_{M_p})^{2^{p-2}}+([2]_{M_p},[-1]_{M_p})^{2^{p-2}}\\
&\quad=([2]_{M_p},[1]_{M_p})^{(M_p+1)/4}+([2]_{M_p},[-1]_{M_p})^{(M_p+1)/4}\\
&\quad=([2]_{M_p},[1]_{M_p})^{(M_p+1)/2}([2]_{M_p},[-1]_{M_p})^{(M_p+1)/4}+([2]_{M_p},[-1]_{M_p})^{(M_p+1)/4}\\
&\quad=([-1]_{M_p},[0]_{M_p})([2]_{M_p},[-1]_{M_p})^{(M_p+1)/4}+([2]_{M_p},[-1]_{M_p})^{(M_p+1)/4}\\
&\quad=0,
\end{aligned}$$

ja siten

$$[s_{p-2}]_{M_p}=[0]_{M_p}.$$

□

Esimerkki 4.11. Testataan onko $M_7=2^7-1=127$ alkuluku.

$$\begin{aligned}
[s_0]_{127}&=[4]_{127},\\
[s_1]_{127}&=[14]_{127},\\
[s_2]_{127}&=[194]_{127}=[-60]_{127},\\
[s_3]_{127}&=[3598]_{127}=[42]_{127},\\
[s_4]_{127}&=[1762]_{127}=[-16]_{127},\\
[s_5]_{127}&=[254]_{127}=[0]_{127}.
\end{aligned}$$

Siten Lauseen 4.9 mukaan M_7 on alkuluku.

Jälleen esimerkin lasku näyttää turhan monimutkaiselta verrattuna testattavan luvun suuruuteen. Kuitenkin samaan tapaan kuin Pépinin testissä, myös Lucas-Lehmerin testin tehokkuus ilmenee hieman suuremmilla luvuilla. Jälleen testistä selvitään laskemalla $p-2$ neliötä ja nekin (mod M_p), eli muistin tarve pysyy pienenä. Mersennen luvut M_p kasvavat huomattavasti hitaammin p:n kasvaessa ja niinpä testattavissa olevia lukuja riittää. Mersennen lukujen etsintää koordinoidaan internetin GIMPS-projektissa (Great Internet Mersenne Prime Search, `http://www.mersenne.org/`).

5. RSA

RSA on Ronald **R**ivestin, Adi **S**hamirin ja Len **A**delmanin vuonna 1977 kehittämä julkisen avaimen salausmenetelmä. (Tosin myöhemmin on paljastettu, että kyseinen salausmenetelmä, kuten myös Diffie-Hellmanin avaimenvaihtoprotokolla, olivat jo esimerkiksi GCHQ:n (Government Communications Headquarters, brittien tiedustelupalvelu) tiedossa joitain vuosia aikaisemmin.) Julkinen avain tarkoittaa sitä, että viestien koodaamiseen käytetty avain voi olla kaikkien saatavilla. Viestin purkaminen onnistuu vain vastaanottajan tuntemalla salaisella avaimella.

Avaimet konstruoidaan seuraavalla tavalla

- Valitaan kaksi suurta alkulukua p ja q, $p \neq q$.
- Lasketaan $m = pq$.
- Lasketaan $\varphi(m) = (p-1)(q-1)$.
- Valitaan luku e siten, että $\text{syt}(e, \varphi(m)) = 1$.
- Valitaan luku d siten, että $[ed]_{\varphi(m)} = [1]_{\varphi(m)}$.

Julkinen avain on ny pari (e, m) ja salainen avain pari (d, m).

Lasketaan esimerkiksi avainpari käyttäen pieniä alkulukuja. Olkoon

$$p = 53 \qquad \text{ja} \qquad q = 47.$$

Nyt

$$m = pq = 53 \cdot 47 = 2491$$

ja

$$\varphi(m) = (p-1)(q-1) = (53-1)(47-1) = 2392 = 2^4 \cdot 13 \cdot 23.$$

Luvuksi e voidaan valita esimerkiksi $e = 73$. Nyt luku d saadaan Eukleideen algoritmin avulla. Siis Eukleideen algoritmi antaa

$$\begin{aligned} 2392 &= 32 \cdot 73 + 56 \\ 73 &= 56 + 17 \\ 56 &= 3 \cdot 17 + 5 \\ 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

ja siitä saamme laskettua

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2(17 - 3 \cdot 5) = 7 \cdot 5 - 2 \cdot 17 = 7(56 - 3 \cdot 17) - 2 \cdot 17 \\ &= 7 \cdot 56 - 23 \cdot 17 = 7 \cdot 56 - 23(73 - 56) = 30 \cdot 56 - 23 \cdot 73 \\ &= 30(2392 - 32 \cdot 73) - 23 \cdot 73 = 30 \cdot 2392 - 983 \cdot 73. \end{aligned}$$

Voidaan siis valita $d = 2392 - 983 = 1409$. Julkinen avain on siten $(73, 2491)$ ja salainen avain $(1409, 2491)$

5.1. **Viestin salaaminen.** Jotta viesti voidaan salata käyttäen RSA-algoritmia, tulee se ensin muuttaa jonoksi luonnollisia lukuja väliltä $[0, m-1]$. Käytetään esimerkiksi seuraavaa merkistömuunnosta.

kirjain	**luku**	**kirjain**	**luku**	**kirjain**	**luku**
A	00	K	10	U	20
B	01	L	11	V	21
C	02	M	12	W	22
D	03	N	13	X	23
E	04	O	14	Y	24
F	05	P	15	Z	25
G	06	Q	16	Å	26
H	07	R	17	Ä	27
I	08	S	18	Ö	28
J	09	T	19	_	29

Kun merkit on muunnettu numerokoodiksi, pilkotaan koodi sopivan mittaisiin paloihin. Näin viesti on saatu kirjoitettua muodossa

$$a_1 a_2 a_3 a_4 \dots a_k,$$

missä luvut $a_i \in \{0, 1, \dots, m-1\}$, ja varsinainen koodaus voi alkaa. Kullekin $i \in \{1, 2, \dots, k\}$ lasketaan

$$[b_i]_m = [a_i^e]_m.$$

Näin saatu jono $b_1 b_2 \dots b_k$ on koodattu viesti.

Koodataan esimerkkinä edellä konstruoidulla julkisella avaimella viesti "OMENAA". Ensin muutetaan siis kirjaimet numerosarjaksi

$$141204130000.$$

Tämän jälkeen pätkitään viesti sopivan mittaisiksi eli tässä tapauksessa kolmen numeron paloiksi

$$141\ 204\ 130\ 000.$$

Seuraavaksi lasketaan tarvittavat potenssit (mod 2491). Huomataan, että $73 = 64 + 8 + 1 = 1001001_2$ ja lasketaan

$$\begin{aligned}
[141^2]_{2491} &= [-47]_{2491} \\
[141^4]_{2491} &= [47^2]_{2491} = [-282]_{2491} \\
[141^9]_{2491} &= [141 \cdot 282^2]_{2491} = [893]_{2491} \\
[141^{18}]_{2491} &= [893^2]_{2491} = [329]_{2491} \\
[141^{36}]_{2491} &= [329^2]_{2491} = [1128]_{2491} \\
[141^{73}]_{2491} &= [141 \cdot 1128^2]_{2491} = [1833]_{2491}
\end{aligned}$$

ja niin edelleen..

$$[141^{73}]_{2491} = [1833]_{2491},$$
$$[204^{73}]_{2491} = [2086]_{2491},$$
$$[130^{73}]_{2491} = [917]_{2491},$$
$$[0^{73}]_{2491} = [0]_{2491}.$$

Siten salattu viesti on

$$1833\ 2086\ 917\ 0.$$

5.2. **Viestin purkaminen.** Purkaminen tehdään jonosta $b_1 b_2 \dots b_k$ laskemalla

$$[b_i^d]_m = [a_i^{ed}]_m = [a_i^{\varphi(m)n+1}]_m = [a_i]_m$$

ja tämän jälkeen muuttamalla purettu numerokoodi takaisin aakkosiksi. Esimerkimme tapauksessa siis salatusta viestistä

$$1833\ 2086\ 917\ 0$$

lasketaan

$$[1833^{1409}]_{2491} = [141]_{2491},$$
$$[2086^{1409}]_{2491} = [204]_{2491},$$
$$[917^{1409}]_{2491} = [130]_{2491},$$
$$[0^{1409}]_{2491} = [0]_{2491}$$

ja saadaan viesti

$$141\ 204\ 130\ 0$$

eli

$$141204130000$$

jossa siis lukee "OMENAA".

RSA:n toimiminen perustuu siihen, että luvun m alkulukuesitelmän löytäminen on vaikeata. Ilman lukuja p ja q ei voida laskea lukua $\varphi(m)$, joka taas tarvitaan jotta luvun d löytämiseen.

6. Luonnollisten lukujen esitykset summina

Tutkitaan seuraavaksi millaisia summaesityksiä luonnollisille luvuille on mahdollista löytää. Aloitetaan neliöiden summilla ja siirrytään sen jälkeen alkulukujen summiin.

6.1. Neliöiden summista.

Määritelmä 6.1. Luonnollisten lukujen kolmikko (a, b, c) on Pythagoraan lukukolmikko mikäli $a^2 + b^2 = c^2$. Pythagoraan lukukolmikkoa sanotaan primitiiviseksi, jos $\text{syt}(a, b, c) = 1$.

Jos $(da)^2 + (db)^2 = (dc)^2$, on myös $a^2 + b^2 = c^2$. Siten Pythagoraan lukukolmikkojen tarkastelu voidaan aina palauttaa primitiivisten Pythagoraan lukukolmikkojen tarkasteluun.

Lause 6.2. *Lukukolmikko (a, b, c) on primitiivinen Pythagoraan lukukolmikko jos ja vain jos on olemassa $n, m \in \mathbb{N}$ siten, että $n > m$,* $\text{syt}(n, m) = 1$, *$n - m$ on pariton, $\{a, b\} = \{2mn, n^2 - m^2\}$ ja $c = n^2 + m^2$.*

Todistus. Jätetään ehtojen riittävyys harjoitustehtäväksi ja osoitetaan, että jokainen primitiivinen Pythagoraan lukukolmikko voidaan kirjoittaa lauseen osoittamassa muodossa.

Oletetaan siis, että (a, b, c) on primitiivinen Pythagoraan lukukolmikko. Koska $\text{syt}(a, b, c) = 1$ ja $a^2 + b^2 = c^2$, on korkeintaan yksi luvuista a, b, c parillinen. Oletetaan nyt, että sekä a että b ovat parittomia eli on olemassa $n_a, n_b \in \mathbb{N}$ siten, että

$$\begin{aligned} c^2 = a^2 + b^2 &= (2n_a + 1)^2 + (2n_b + 1)^2 \\ &= 2(2n_a^2 + 2n_b^2 + 2n_a + 2n_b + 1). \end{aligned}$$

Tällöin c^2 on parillinen muttei jaollinen neljällä. Tämä on mahdotonta eli toisen luvuista a, b täytyy olla parillinen.

Voidaan siis olettaa, että a on parillinen ja b ja c parittomia. Merkitään

$$u = \frac{c + b}{2} \qquad \text{ja} \qquad v = \frac{c - b}{2}.$$

Nyt $\text{syt}(u, v) = 1$. Nyt

$$a^2 = c^2 - b^2 = (c + b)(c - b) = 4uv.$$

Koska a on parillinen, on $w \in \mathbb{N}$ siten, että $a = 2w$ ja siten $w^2 = uv$. Koska $\text{syt}(u, v) = 1$, täytyy $u = n^2$ ja $v = m^2$ joillakin $n, m \in \mathbb{N}$. Siispä

$$a = 2mn, \qquad b = n^2 - m^2, \qquad c = n^2 + m^2.$$

Koska $\text{syt}(u, v) = 1$, on myös $\text{syt}(n, m) = 1$. Koska $b > 0$, on $n > m$. Luvut n ja m eivät voi olla molemmat parittomia eivätkä molemmat parillisia edellä tehtyjen päätelmien perusteella. Siten $n - m$ on pariton. □

Lause 6.3. *Yhtälöllä $x^4 + y^4 = z^2$ ei ole ratkaisua positiivisten kokonaislukujen joukossa.*

Todistus. Oletetaan, että joukko

$$\{z \in \mathbb{N} : z^2 = x^4 + y^4 \text{ joillakin } x, y \in \mathbb{N} \setminus \{0\}\}$$

on epätyhjä. Siinä on tällöin olemassa pienin alkio $z_0 > 0$ ja lisäksi $x_0, y_0 \in \mathbb{N} \setminus \{0\}$ siten, että $x_0^4 + y_0^4 = z_0^2$. Voidaan olettaa, että $\text{syt}(x_0, y_0, z_0) = 1$. Tällöin (x_0^2, y_0^2, z_0) on primitiivinen Pythagoraan lukukolmikko. Voidaan lisäksi olettaa, että y_0 on ainut parillinen luvuista x_0, y_0, z_0. Tällöin Lauseen 6.2 mukaan on olemassa $a, b \in \mathbb{N}$ siten, että $\text{syt}(a, b) = 1$ ja

$$x_0^2 = a^2 - b^2, \qquad y_0^2 = 2ab, \qquad z_0 = a^2 + b^2.$$

Nyt a ei voi olla parillinen, koska tällöin b olisi pariton ja siten $[x_0^2]_4 = [3]_4$. Siispä a on pariton ja b parillinen. Lukukolmikko (x_0, b, a) on primitiivinen Pythagoraan lukukolmikko ja Lauseen 6.2 mukaan on olemassa $c, d \in \mathbb{N}$ siten, että $\text{syt}(c, d) = 1$ ja

$$x_0 = c^2 - d^2, \qquad b = 2cd, \qquad a = c^2 + d^2.$$

Koska $\text{syt}(a, b) = 1$, on

$$\text{syt}(c, d) = \text{syt}(c, c^2 + d^2) = \text{syt}(d, c^2 + d^2) = 1.$$

Nyt

$$\left(\frac{1}{2}y_0\right)^2 = cd(c^2 + d^2).$$

Koska y_0 on parillinen, on oikean puolen tulon tekijät kaikki kokonaislukujen neliöitä. Siten on olemassa $x_1, y_1, z_1 \in \mathbb{N}$ siten, että $\text{syt}(x_1, y_1) = \text{syt}(x_1, z_1) = \text{syt}(y_1, z_1) = 1$ ja

$$x_1^2 = c, \qquad y_1^2 = d, \qquad z_1^2 = c^2 + d^2.$$

Näille luvuille on

$$c^2 + d^2 = x_1^4 + y_1^4 = z_1^2$$

eli ne toteuttavat lauseen väitteen yhtälön. Lisäksi

$$z_1 \leq z_1^2 = c^2 + d^2 = a < a^2 + b^2 = z_0,$$

mikä on ristiriidassa luvun z_0 valinnan kanssa. □

Nyt kun olemme vastanneet kysymykseen millaisilla luvuilla $a^2+b^2 = c^2$, voidaan miettiä vastaavaa yhtälöä, kun sen oikea puoli ei olekaan neliö. Tarkemmin ottaen, mille luvuille $n \in \mathbb{N}$ löytyy luvut $a, b \in \mathbb{N}$ siten, että

$$n = a^2 + b^2?$$

Tähän vastauksen antaa seuraava Fermat'n todistama tulos.

Lause 6.4. *Olkoon $n \in \mathbb{N} \setminus \{0\}$. Tällöin on olemassa $a, b \in \mathbb{N}$ siten, että $n = a^2 + b^2$ ja $\text{syt}(a, b) = 1$ jos ja vain jos -1 on neliönjäännös (mod n).*

Todistus. (Todistus ei ole vaikea, mutta ohitetaan se silti.) □

Siis kaikkia lukuja ei voida esittää kahden neliön summana. Seuraavaksi voidaan kysyä onnistuuko tämä kolmella neliöllä. Näin ei kuitenkaan ole. Esimerkiksi jos $n \in \mathbb{N}$, ei lukua $8n + 7$ voida esittää kolmen luonnollisen luvun neliön summana. (Jätetään tämän todistaminen harjoitustehtäväksi.) Luonnollisten lukujen summaesitykseen neljä on riittävä määrä neliöitä, kuten seuraava lause osoittaa.

Lause 6.5 (Lagrange)**.** *Olkoon $n \in \mathbb{N}$. Tällöin on olemassa $a, b, c, d \in \mathbb{Z}$ siten, että*

$$n = a^2 + b^2 + c^2 + d^2.$$

Todistetaan ensin aputulos.

Lemma 6.6. *Olkoon p alkuluku. Tällöin on olemassa $x, y \in \mathbb{Z}$ siten, että*

$$[x^2 + y^2]_p = [-1]_p.$$

Todistus. Väite on selvästi totta, kun $p = 2$. Oletetaan siis, että $p \geq 3$. Olkoon

$$S = \{[1^2]_p, [2^2]_p, \ldots, [(p-1)^2]_p\}.$$

Jos $[a^2]_p = [b^2]_p$, on $[a]_p = [\pm b]_p$. Siten $\#S = \frac{p-1}{2}$. Lisäksi $[0]_p \notin S$. Siispä

$$\{[0^2]_p, \ldots, [(p-1)^2]_p\} \cap \{[-0^2 - 1]_p, \ldots, [-(p-1)^2 - 1]_p\} \neq \emptyset.$$

Siten on olemassa $x, y \in \{0, 1, \ldots, p-1\}$ siten, että

$$[x^2]_p = [-y^2 - 1]_p.$$

□

Lauseen 6.5 todistus. Koska $0 = 0^2 + 0^2 + 0^2 + 0^2$, $1 = 1^2 + 0^2 + 0^2 + 0^2$ ja $2 = 1^2 + 1^2 + 0^2 + 0^2$, voidaan olettaa, että $n \geq 3$. Lisäksi koska

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) = A^2 + B^2 + C^2 + D^2,$$

missä

$$\begin{aligned} A &= ax + by + cz + dw, \\ B &= ay - bx - cw + dz, \\ C &= az + bw - cx - dy, \\ D &= aw - bz + cy - dx, \end{aligned}$$

voidaan olettaa että n on alkuluku.

Lemman 6.6 nojalla on olemassa $m, x, y \in \mathbb{Z}$ siten, että $|x|, |y| \leq \frac{n}{2}$ ja

$$mn = x^2 + y^2 + 1.$$

Nyt $0 < m \leq \frac{n}{2}$. Jos $m = 1$, on lause todistettu. Oletetaan siis, että meillä on ratkaisu

$$mn = x^2 + y^2 + z^2 + w^2,$$

missä $m > 1$ on pienin positiivinen kokonaisluku, jolle mn voidaan kirjoittaa neljän neliön summana. Olkoon $a \in [x]_m$, $b \in [y]_m$, $c \in [z]_m$ ja $d \in [w]_m$ siten, että $|a|, |b|, |c|, |d| \leq \frac{m}{2}$. Tällöin

$$[a^2 + b^2 + c^2 + d^2]_m = [0]_m$$

eli on olemassa $m' \in \mathbb{Z}$ siten, että

$$a^2 + b^2 + c^2 + d^2 = m'm.$$

Nyt

$$\begin{aligned} nm^2m' &= (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) \\ &= A^2 + B^2 + C^2 + D^2 \end{aligned}$$

samoilla A, B, C ja D kuten yllä. Helposti voidaan tarkistaa, että

$$[A]_m = [B]_m = [C]_m = [D]_m = [0]_m.$$

Siten nm' voidaan kirjoittaa neljän neliön summana. Huomataan, että

$$m' = \frac{a^2 + b^2 + c^2 + d^2}{m} \leq \frac{\frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4}}{m} = m.$$

Luvun m valinnan perusteella täytyy olla $m' = m$. Siten

$$|a| = |b| = |c| = |d| = \frac{m}{2}$$

ja edelleen

$$[2a]_m = [2b]_m = [2c]_m = [2d]_m = [2x]_m = [2y]_m = [2z]_m = [2w]_m = [0]_m.$$

Siten

$$4nm = 4x^2 + 4y^2 + 4z^2 = 4w^2 = vm^2$$

jollain $v \in \mathbb{Z} \setminus \{0\}$. Siispä $m \mid 4n$. Koska n on alkuluku ja $0 < m \leq \frac{n}{2}$, on $\text{syt}(m, n) = 1$ ja siten $m \mid 4$.

Jos $m = 4$, ovat x, y, z, w parillisia ja siten

$$n = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 + \left(\frac{w}{2}\right)^2.$$

Jos taas $m = 2$, on

$$\begin{aligned} 4n &= (1 + 1 + 0 + 0)2n \\ &= (1 + 1 + 0 + 0)(x^2 + y^2 + z^2 + w^2) = A^2 + B^2 + C^2 + D^2, \end{aligned}$$

missä $A = x + y$, $B = y - x$, $C = z + w$ ja $D = w - z$ ovat kaikki parillisia. Siten

$$n = \left(\frac{A}{2}\right)^2 + \left(\frac{B}{2}\right)^2 + \left(\frac{C}{2}\right)^2 + \left(\frac{D}{2}\right)^2.$$

□

Olemme tutkineet yhtälöitä $x^2 + y^2 = z^2$ ja $x^2 + y^2 = n$. Näistä ensimmäistä katsoessa herää kysymys: Mitä tapahtuu, jos luku 2 vaihdetaan joksikin suuremmaksi luonnolliseksi luvuksi? Vastauksen tähän antaa Fermat'n suuri lause.

Lause 6.7. *Kun $n \in \mathbb{N}$, $n > 2$, ei lauseella $x^n + y^n = z^n$ ole olemassa ratkaisua $x, y, z \in \mathbb{N} \setminus \{0\}$.*

Fermat esitti tämän väittämän vuonna 1637 ja se saatiin todistettua vasta yli 350 vuotta myöhemmin vuonna 1995.

Monia Fermat'n suuren lauseen suuntaisia kysymyksiä on vielä avoinna. Eräs näistä on miljardööri Andrew Bealin mukaan nimetty Bealin konjektuuri:

> Jos $a^x + b^y = c^z$, missä $x, y, z, a, b, c \in \mathbb{N}$, $a, b, c \geq 1$ ja $x, y, z \geq 3$, on välttämättä $\text{syt}(a, b, c) > 1$.

Beal on luvannut 100 000 Yhdysvaltain dollarin palkkion konjektuurin ratkaisijalle.

6.2. **Goldbachin konjektuuri.** Yksi matematiikan vanhimmista avoimista ongelmista on saanut nimensä Goldbachin vuonna 1742 Eulerille esittämästä konjektuurista

> Jokainen kakkosta suurempi kokonaisluku voidaan esittää kolmen alkuluvun summana.

Huomaa, että tuolloin myös lukua 1 pidettiin alkulukuna. Nykyisin Goldbachin konjektuurina ymmärretään seuraava väittämä:

> Jokainen parillinen kakkosta suurempi kokonaisluku voidaan kirjoittaa kahden alkuluvun summana.

Käydään läpi seuraavaksi hieman konjektuuriin liittyviä tuloksia.

Pipping laskemalla osoitti vuonna 1938, että väite on totta kaikille lukua 10^5 pienemmille luvuille. Tällä hetkellä konjektuuri on varmannettu noin lukuun $2 \cdot 10^{18}$ asti.

Vuonna 1930 Schnirelmann osoitti, että jokainen parillinen luku voidaan kirjoittaa korkeintaan 300 000 alkuluvun summana. Vuonna 1995 Ramare osoitti saman kuudella alkuluvulla.

Vinogradov osoitti vuonna 1937, että jokainen riittävän suuri pariton kokonaisluku voidaan kirjoittaa kolmen alkuluvun summana. Chen Jingrun puolestaan todisti vuonna 1973, että jokainen riittävän suuri luonnollinen luku voidaan kirjoittaa joko kahden alkuluvun summana tai alkuvun ja kahden alkuvuun tulon summana.

Miksi Goldbachin konjektuurin pitäisi olla totta? Alkulukulauseen mukaan

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\log(n)} = 1.$$

Siten todennäköisyys sille, että satunnaisesti valittu luku n on alkuluku on noin $\frac{1}{\log(n)}$. Luku n voidaan ilmaista muodossa $n = (n-k)+k$. Todennäköisyys sille, että $n-k$ on alkuluku on $\frac{1}{\log(n-k)}$ ja vastaavasti todennäköisyys sille, että k on alkuluku on $\frac{1}{\log(k)}$. Jos nämä olisivat alkulukuja riippumatta toisistaan, olisi todennäköisyys sille että molemmat ovat alkulukuja $\frac{1}{\log(n-k)} \cdot \frac{1}{\log(k)}$. Edelleen, olettaen kasan riippumattomuuttomuuksia, voidaan arvioida

$$\begin{aligned}
&P(\text{Lukua } n \text{ ei voida esittää kahden alkuluvun summana}) \\
&\leq \prod_{k=1}^{n/2} \left(1 - \frac{1}{\log(n-k)} \cdot \frac{1}{\log(k)}\right) \leq \exp\left(-\sum_{k=1}^{n/2} \frac{1}{\log(n-k)} \cdot \frac{1}{\log(k)}\right) \\
&\leq \exp\left(-\sum_{k=1}^{n/2} \frac{1}{\log(n)} \cdot \frac{1}{\log(n)}\right) = \exp\left(-\frac{n}{2(\log(n))^2}\right) \leq e^{-\sqrt{n}}
\end{aligned}$$

Koska $\sum_{n=1}^{\infty} e^{-\sqrt{n}} < \infty$, saadaan edellisestä arviosta

$$\begin{aligned} &P(\text{On olemassa lukua } n \text{ isompi luku jota ei} \\ &\quad \text{voida esittää kahden alkuluvun summana}) \\ &\leq \sum_{m=n}^{\infty} e^{-\sqrt{m}} \longrightarrow 0, \text{ kun } n \to \infty. \end{aligned}$$

Edellä esitetty arvionti ei tietenkään ole todenmukainen tehtyjen riippumattomuusoletusten takia. Silti tällaiset heuristiset laskut osoittavat, että ainakaan alkulukujen tiheyden ei pitäisi olla esteenä konjektuurin toteutumiselle.

6.3. **Muita ratkaisemattomia ongelmia.** Esitetään seuraavaksi muutama avoin lukuteorian ongelma lisää. Lukuparia $(p, p+2)$ sanotaan alkulukupariksi (tai alkulukukaksosiksi), jos molemmat luvuista p ja $p+2$ ovat alkulukuja. Esimerkiksi $(3,5)$, $(11,13)$, $(71,73)$ ja

$$(65516468355 \cdot 2^{333333} - 1, 65516468355 \cdot 2^{333333} + 1)$$

ovat alkulukupareja. Alkulukupareja tunnetaan paljon. Silti ei ole vielä pystytty todistamaan, onko niitä äärettömän monta.

Olettaen taas, että todennäköisyys sille, että n on alkuluku ja sille, että $n+2$ on alkuluku ovat riippumattomia toisistaan, on todennäköisyys sille, että $(n, n+2)$ on alkulukupari on $\frac{1}{\log(n)} \cdot \frac{1}{\log(n+2)}$. Toisaalta

$$\sum_{n=2}^{\infty} \frac{1}{\log(n)} \cdot \frac{1}{\log(n+2)} = \infty,$$

joten alkulukulause ei vastusta alkulukuparien määrän äärettömyyttäkään.

Alkulukuparien ongelmaa yleisempi kysymys on Polignacin konjektuurina tunnettu väittämä

> Kaikilla parillisilla $n \in \mathbb{N}$ on olemassa äärettömän monta lukuparia $(p, p+n)$ siten, että p ja $p+n$ ovat alkulukuja.

Väitettä ei ole pystytty todistamaan oikeaksi (eikä vääräksi) yhdelläkään $n > 0$.

Määritelmä 6.8. Lukua $n \in \mathbb{N}$ sanotaan täydelliseksi luvuksi, jos se on itseään pienempien positiivisten tekijöidensä summa.

Esimerkiksi luku 6 on täydellinen, sillä $6 = 1 + 2 + 3$. Parilliset täydelliset luvut voidaan karakterisoida Mersennen lukujen avulla.

Lause 6.9. *Luku $n \in \mathbb{N}$ on parillinen täydellinen luku, jos ja vain jos $n = 2^{p-1}M_p$ ja $M_p = 2^k - 1$ on alkuluku.*

Todistus. Oletetaan ensin, että M_p on alkuluku ja $n = 2^{p-1}M_p$. Tällöin luvun n tekijöiden summa on

$$\begin{aligned}&1 + 2 + \cdots + 2^{p-1} + M_p + 2M_p + \cdots + 2^{p-1}M_p \\ &\quad =(M_p + 1)(1 + 2 + \cdots + 2^{p-1}) = 2^p(2^p - 1) = 2n.\end{aligned}$$

Siten n on täydellinen luku.

Oletetaan seuraavaksi, että n on parillinen täydellinen luku. Kirjoitetaan $n = 2^t u$, missä $t, u \in \mathbb{N}$ ja u on pariton. Kaikki luvun n tekijät ovat muotoa $2^s m$, missä $0 \leq s \leq t$ ja $m \mid u$. Olkoon luvun u tekijöiden summa k. Tällöin luvun n tekijöiden summaksi saadaan

$$(1 + 2 + \cdots + 2^t)k = (2^{t+1} - 1)k.$$

Koska n on täydellinen luku, on

$$(2^{t+1} - 1)k = 2n = 2^{t+1}u.$$

Koska u on pariton, on $k = 2^{t+1}a$ jollakin $a \in \mathbb{N}$. Siten $u = (2^{t+1} - 1)a$. Tarkastellaan nyt uudestaan lukua k. Oletetaan, että $a > 1$. Tällöin ainakin 1, u ja a ovat luvun u tekijöitä ja siten

$$k \geq 1 + u + a = 1 + (2^{t+1} - 1)a + a = 1 + 2^{t+1}a = k + 1,$$

mikä on mahdotonta. Siispä täytyy olla $a = 1$. Tällöin

$$k = 2^{t+1} = (2^{t+1} - 1) + 1$$

eli $u = 2^{t+1} - 1$ on välttämättä alkuluku. Siten $n = 2^t M_{t+1}$ eli haluamaamme muotoa. □

Parillisten täydellisten lukujen etsiminen kulkee siis käsi kädessä Mersennen alkulukujen etsimisen kanssa. Ei tiedetä onko Mersennen alkulukuja (ja siten parillisia täydellisiä lukuja) olemassa äärettömän monta.

Parittomista täydellisistä luvuista edellinen lause ei sano mitään. Itse asiassa ei edes tiedetä onko parittomia täydellisiä lukuja olemassa lainkaan.

Monilla muillakin erityistä muotoa olevilla luvuilla on oma nimensä. Cullenin luvuiksi sanotaan lukuja jotka ovat muotoa

$$C_n = n \cdot 2^n + 1.$$

Woodallin luvut taas ovat muotoa

$$W_n = n \cdot 2^n - 1.$$

Kummastakaan ei tiedetä onko kyseistä muotoa olevia alkulukuja olemassa äärettömän paljon.

Sophie Germainin luvuiksi sanotaan alkulukuja p joille myös $2p + 1$ on alkuluku. Yllättäen ei tiedetä onko Sophie Germainin lukuja äärettömän monta vai ei.. Hieman tutummillekaan luvuille ei tiedetä vastaavaan kysymykseen vastausta. Onko esimerkiksi Fibonaccin lukujen joukossa äärettömän monta alkulukua?

Eräs kuuluisa alkulukujen tiheyteen liittyvä avoin ongelma on nimeltään Legendren konjektuuri:

> Kaikilla positiivisilla $n \in \mathbb{N}$ on välillä $[n^2, (n+1)^2]$ olemassa alkuluku.

Edellä esitetyt avoimet ongelmat liittyivät lähinnä alkulukuihin. On olemassa myös kuuluisia lukuteorian ongelmia joiden muotoilussa ei näy alkulukuja.

Esimerkkinä Brocardin ongelmana tunnettu kysymys:

> Onko yhtälöllä $n! + 1 = m^2$ ratkaisua $n, m \in \mathbb{N}$?

Esitetään vielä viimeisenä avoimena ongelmana Collatzin konjektuuri. Määritellään sitä varten kuvaus $f\colon \mathbb{N} \to \mathbb{N}$ asettamalla

$$f(n) = \begin{cases} \frac{n}{2} & , \text{ jos } n \text{ on parillinen,} \\ 3n+1 & , \text{ jos } n \text{ on pariton.} \end{cases}$$

Konjektuurina on, että kaikilla $n \in \mathbb{N}$, $n > 0$, on olemassa $m \in \mathbb{N}$ siten, että

$$\underbrace{f \circ f \circ \cdots \circ f}_{m \text{ kappaletta}}(n) = 1.$$

7. Korkeamman asteen kongruenssiyhtälöt

Aikaisemmin osoitettiin jo Lauseessa 3.1, että kokonaislukukertoimisella n. asteen yhtälöllä

$$P_n(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

on korkeintaan n ratkaisua, kun p on alkuluku. Tällöin ei vielä käsitelty tapausta, jossa p ei ole alkuluku. Osoittautuu, että tällöin yhtälön ratkaiseminen voidaan palauttaa pienempimodulisiin yhtälöihin alkulukuhajotelman kautta.

Ensimmäisenä tuloksena tähän suuntaan osoitetaan Henselin lemmana tunnettu tulos, jolla ratkaisuista (mod p) saadaan ratkaisut (mod p^k), $k > 1$.

Lause 7.1. *Olkoon p pariton alkuluku ja f kokonaislukukertoiminen polynomi. Olkoon lisäksi $m, r \in \mathbb{Z}$ siten, että $m > 0$ ja $f(r) \equiv 0$ (mod p^m). Tällöin yhtälön*

$$f(r + tp^m) \equiv 0 \pmod{p^{m+1}} \tag{12}$$

ratkaisuista t voidaan sanoa seuraavaa.

(i) *Jos $f'(r) \not\equiv 0$ (mod p) ja $f(r) \not\equiv 0$ (mod p^{m+1}), on olemassa täsmälleen yksi $t \in \mathbb{Z}$, $1 \leq t \leq p-1$ siten, että t toteuttaa yhtälön (12). Lisäksi t toteuttaa yhtälön*

$$tf'(r) \equiv -\frac{f(r)}{p^m} \pmod{p}$$

(ii) *Jos* $f'(r) \equiv 0 \pmod{p}$ *ja* $f(r) \equiv 0 \pmod{p^{m+1}}$*, niin jokainen* $t \in \mathbb{Z}$*,* $1 \leq t \leq p-1$*, toteuttaa yhtälön* (12)*.*

(iii) *Jos* $f'(r) \equiv 0 \pmod{p}$ *ja* $f(r) \not\equiv 0 \pmod{p^{m+1}}$*, niin kaikilla yhtälöllä* (12) *ei ole kokonaislukuratkaisuja* t*.*

Otetaan ennen lauseen todistamista yksi esimerkki sen käyttämisestä ratkaisujen etsimiseen.

Esimerkki 7.2. Etsitään yhtälön

$$x^2 + 4x + 9 \equiv 0 \pmod{343}$$

ratkaisut.

Huomataan ensin, että $343 = 7^3$. Merkitään $f(x) = x^2 + 4x + 9$. Tutkitaan siis ensin yhtälöä $f(x) \equiv 0 \pmod{7}$. Toisin kuin alkuperäiselle yhtälölle, tämän mahdolliset ratkaisut voidaan nopeasti etsiä kokeilemalla.

$$f(0) = 0^2 + 4 \cdot 0 + 9 = 9 \not\equiv 0$$
$$f(1) = 1^2 + 4 \cdot 1 + 9 = 14 \equiv 0$$
$$f(2) = 2^2 + 4 \cdot 2 + 9 = 21 \equiv 0.$$

Enempää ratkaisuja ei Lauseen 3.1 mukaan olekaan.

Käytetään nyt Lausetta 7.1 yhtälön $f(x) \equiv 0 \pmod{7^2}$ ratkaisujen löytämiseen. Lasketaan siis ensin $f'(x) = 2x + 4$. Koska $f'(1) = 6 \not\equiv 0 \pmod{7}$ ja $f(1) = 14 \not\equiv 0 \pmod{7^2}$, voidaan käyttää kohtaa (i). Ratkaistaan siis yhtälö

$$tf'(1) \equiv -\frac{f(1)}{7} \pmod{7}$$

eli yhtälö $6t \equiv -2 \pmod{7}$. Tämän ratkaisu on $t = 2$. Siis

$$f(1 + 2 \cdot 7) = f(15) \equiv 0 \pmod{7^2}.$$

Vastaavasti lasketaan $f'(2) = 8 \not\equiv 0 \pmod{7}$ ja $f(2) = 21 \not\equiv 0 \pmod{7^2}$. Ratkaistavaksi tulee siis yhtälö

$$tf'(2) \equiv -\frac{f(2)}{7} \pmod{7}$$

eli $8t \equiv t \equiv -3 \pmod{7}$. Tämän ratkaisu on tietenkin $t = 4$. Siten

$$f(2 + 4 \cdot 7) = f(30) \equiv 0 \pmod{7^2}.$$

Siirrytään seuraavaksi yhtälön $f(x) \equiv 0 \pmod{7^3}$ ratkaisujen kimppuun. Koska $f(15) = 294 \not\equiv 0 \pmod{7^3}$ ja $f'(15) = 34 \equiv 6 \not\equiv 0 \pmod{7}$, saadaan yksi ratkaisu ratkaisemalla ensin yhtälö

$$tf'(15) \equiv -\frac{f(15)}{7^2} \pmod{7}$$

eli yhtälö $6t \equiv -6 \pmod{7}$. Ratkaisu on siis $t = 6$. Siis

$$f(15 + 6 \cdot 7^2) = f(309) \equiv 0 \pmod{7^3}.$$

Vastaavasti tutkitaan toista edellisen tason ratkaisua. $f(30) = 1029 \equiv 0 \pmod{7^3}$, joten ratkaisu on jo löydetty.

Siten alkuperäisen yhtälön ratkaisut ovat $x = 30$ ja $x = 309$.

Todistetaan nyt Henselin lemma. Aloitetaan aputuloksella.

Lemma 7.3. *Olkoon p alkuluku, $m > 0$, f kokonaislukukertoiminen polynomi. Tällöin*

$$f(x + tp^m) \equiv f(x) + tp^m f'(x) \pmod{p^{m+1}}$$

kaikilla $x, t \in \mathbb{Z}$.

Todistus. Kirjoitetaan $f(x) = a_n x^x + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$. Tällöin

$$f(x+tp^m) = a_0 + \sum_{i=1}^{n} a_i (x+tp^m)^i = a_0 + \sum_{i=1}^{n} a_i \left(\sum_{j=0}^{i} \binom{i}{j} x^{i-j} (tp^m)^j \right).$$

Koska $p^{m+1} \mid (tp^m)^j$, kun $j > 1$, saadaan $\pmod{p^{m+1}}$

$$\begin{aligned} f(x + tp^m) &\equiv a_0 + \sum_{i=1}^{n} a_i \left(x^i + ix^{i-1} tp^m \right) \\ &= \sum_{i=0}^{n} a_i x^i + tp^m \sum_{i=1}^{n} i x^{i-1} = f(x) + tp^m f'(x). \end{aligned}$$

□

Henselin lemma seuraa nyt helposti.

Lauseen 7.1 todistus. (i) Olkoon $r \in \mathbb{Z}$ siten, että $f(r) \equiv 0 \pmod{p^m}$ ja $f'(r) \not\equiv 0 \pmod{p}$. Tällöin $\frac{f(r)}{p^m} \not\equiv 0 \pmod{p}$ ja siten yhtälöllä

$$tf'(r) \equiv -\frac{f(r)}{p^m} \pmod{p}$$

on olemassa yksikäsitteinen nollasta poikkeava ratkaisu (mod p). Tällöin Lemman 7.3 mukaan on $\pmod{p^{m+1}}$

$$\begin{aligned} f(r + tp^m) &\equiv f(r) + tp^m f'(r) = f(r) + p^m \left(kp - \frac{f(r)}{p^m} \right) \\ &\equiv f(r) - f(r) = 0, \end{aligned}$$

missä $k \in \mathbb{Z}$.

(ii) Oletetaan, että $f'(r) \equiv 0 \pmod{p}$ ja $f(r) \equiv 0 \pmod{p^{m+1}}$. Nyt $f'(r) = kp$ jollain $k \in \mathbb{Z}$ ja kaikilla t on $\pmod{p^{m+1}}$

$$f(r + tp^m) \equiv f(r) + tp^m f'(r) = f(r)tkp^{m+1} \equiv f(r) \equiv 0.$$

(iii) Oletetaan nyt, että $f'(r) \equiv 0 \pmod{p}$ ja $f(r) \not\equiv 0 \pmod{p^{m+1}}$. Nyt $f'(r) = kp$ jollain $k \in \mathbb{Z}$ ja samalla laskulla kuin edellä saadaan kaikilla t on $\pmod{p^{m+1}}$

$$f(r + tp^m) \equiv f(r) + tp^m f'(r) = f(r)tkp^{m+1} \equiv f(r) \not\equiv 0.$$

□

Esimerkki 7.4. a) Ratkaistaan yhtälö

$$f(x) = 3x^3 + 5x^2 + 2 \equiv 0 \pmod{243}.$$

Koska $243 = 3^5$, voidaan käyttää Lausetta 7.1. Tarkastellaan siis ensin mod 3

$$f(0) = 3 \cdot 0^3 + 5 \cdot 0^2 + 2 = 2 \not\equiv 0,$$
$$f(1) = 3 \cdot 1^3 + 5 \cdot 1^2 + 2 = 10 \equiv 1 \not\equiv 0,$$
$$f(2) = 3 \cdot 2^3 + 5 \cdot 2^2 + 2 = 46 \equiv 1 \not\equiv 0.$$

Siis kaikilla $a \in \mathbb{Z}$ on $[f(a)]_3 \in \{[1]_3, [2]_3\}$ eikä yhtälöllä ole siten yhtään ratkaisua.

b) Ratkaistaan yhtälö

$$f(x) = 3x^3 + 5x^2 + 1 \equiv 0 \pmod{243}.$$

Tarkastellaan taas ensin mod 3

$$f(0) = 3 \cdot 0^3 + 5 \cdot 0^2 + 1 = 1 \not\equiv 0,$$
$$f(1) = 3 \cdot 1^3 + 5 \cdot 1^2 + 1 = 9 \equiv 0,$$
$$f(2) = 3 \cdot 2^3 + 5 \cdot 2^2 + 1 = 45 \equiv 0.$$

Seuraavaksi lasketaan $f'(x) = 9x^2 + 10x$ ja edelleen mod 3

$$f'(1) = 9 \cdot 1^2 + 10 \cdot 1 = 19 \equiv 1,$$
$$f'(2) = 9 \cdot 2^2 + 10 \cdot 2 = 56 \equiv 2.$$

Siirrytään seuraavaksi laskemaan ratkaisut mod 9

$$f(1) = 3 \cdot 1^3 + 5 \cdot 1^2 + 1 = 9 \equiv 0,$$
$$f(2) = 3 \cdot 2^3 + 5 \cdot 2^2 + 1 = 45 \equiv 0.$$

Tämän jälkeen etsitään ratkaisut mod 27

$$f(1) = 3 \cdot 1^3 + 5 \cdot 1^2 + 1 = 9 \not\equiv 0,$$

joten ratkaistavaksi jää yhtälö

$$tf'(1) \equiv -\frac{f(1)}{9} \pmod{3}$$

jonka ratkaisu on $t \equiv 2 \pmod{3}$. Siten yksi ratkaisu mod 27 on

$$f(1 + 2 \cdot 9) = f(19) \equiv 0.$$

Etsitään toinen ratkaisu. Huomataan ensin, että

$$f(2) = 3 \cdot 2^3 + 5 \cdot 2^2 + 1 = 45 \equiv 0,$$

joten ratkaistavaksi jää yhtälö

$$tf'(2) \equiv -\frac{f(2)}{9} \pmod{3}$$

jonka ratkaisu on myös $t \equiv 2 \pmod 3$. Siten toinen ratkaisu alkuperäiselle yhtälölle mod 27 on

$$f(2 + 2 \cdot 9) = f(20) \equiv 0.$$

Siirrytään laskemaan mod 81.

$$f(19) \equiv 27 \not\equiv 0,$$

joten toinen ratkaisu saadaan yhtälön

$$tf'(19) \equiv -\frac{f(19)}{27} \pmod 3$$

avulla, jonka ratkaisu on $t \equiv 2 \bmod 3$. Siten ensimmäinen ratkaisu on

$$f(19 + 2 \cdot 27) = f(73) \equiv 0 \pmod{81}.$$

Toisaalta

$$f(20) \equiv 0 \pmod{81}$$

on toinen ratkaisu ja muita ei ole, sillä

$$f'(20) \not\equiv 0 \pmod{81}.$$

Etsitään lopuksi ratkaisut mod 243.

$$f'(73) \equiv 1 \pmod 3$$

ja

$$f(73) \equiv 81 \pmod{243},$$

joten näistä saadaan yksi ratkaisu laskemalla ensin yhtälöstä

$$tf'(73) \equiv -\frac{f(73)}{81} \pmod 3$$

ratkaisu $t \equiv 2$. Siis

$$f(73 + 2 \cdot 81) = f(235) \equiv 0 \pmod{243}.$$

Koska

$$f'(20) \equiv 2 \not\equiv 0 \pmod 3$$

ja

$$f(20) \equiv 0 \pmod{243},$$

on kaikki ratkaisut löydetty. Siis alkuperäisen yhtälön

$$f(x) \equiv 0 \pmod{243}$$

ratkaisut ovat

$$x = 20 \qquad \text{ja} \qquad x = 235.$$

Myös yhtälöt modulo n, missä luvulla n on useampi alkulukutekijä voidaan palauttaa pienempimodulisten yhtälöiden ratkaisemiseen kiinalaisen jäännöslauseen tyyliin.

Lause 7.5. *Olkoon luvun $m \in \mathbb{N}$ alkulukuesitys*

$$m = \prod_{i=1}^{n} p_i^{m_i}.$$

Olkoon lisäksi a_i, $i = 0, 1 \ldots, k$, kokonaislukuja. Tällöin yhtälön

$$a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{m}$$

ratkaisut ovat täsmälleen yhtälöryhmien

$$\begin{cases} x \equiv x_1 \pmod{p_1^{m_1}} \\ x \equiv x_2 \pmod{p_2^{m_2}} \\ \vdots \\ x \equiv x_n \pmod{p_n^{m_n}} \end{cases}$$

ratkaisut, missä kukin x_i on yhtälön

$$a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p_i^{m_i}}$$

eräs ratkaisu.

Todistus. Toinen suunta on triviaali ja toinen seuraa kiinalaisesta jäännöslauseesta. □

Esimerkki 7.6. Ratkaistaan yhtälö

$$f(x) = 3x^3 + 5x^2 + 1 \equiv 0 \pmod{1215}.$$

Koska $1215 = 3^5 \cdot 5$, on Lauseen 7.5 mukaan ratkaisut samat kuin yhtälöryhmien

$$\begin{cases} x_1 \equiv x \pmod{3^5} \\ x_2 \equiv x \pmod{5} \end{cases}$$

ratkaisut, missä

$$f(x_1) \equiv 0 \pmod{3^5}$$

ja

$$f(x_2) \equiv 0 \pmod{5}.$$

Yhtälöistä ensimmäisen ratkaisut jo tiedetäänkin Esimerkin 7.4 kohdan b) perusteella. Ne ovat $x_1 = 20$ ja $x_1 = 235$. Ratkaistaan siis yhtälö

$$f(x_2) \equiv 0 \pmod{5}$$

käymällä läpi kaikki vaihtoehdot mod 5

$$\begin{aligned} f(0) &= 3 \cdot 0^3 + 5 \cdot 0^2 + 1 = 1 \not\equiv 0, \\ f(1) &= 3 \cdot 1^3 + 5 \cdot 1^2 + 1 = 9 \not\equiv 0, \\ f(2) &= 3 \cdot 2^3 + 5 \cdot 2^2 + 1 = 45 \equiv 0, \\ f(3) &= 3 \cdot 3^3 + 5 \cdot 3^2 + 1 = 127 \not\equiv 0, \\ f(4) &= 3 \cdot 4^3 + 5 \cdot 4^2 + 1 = 273 \not\equiv 0. \end{aligned}$$

Ratkaisut saadaan siis yhtälöryhmistä

$$\begin{cases} x \equiv 20 \pmod{3^5} \\ x \equiv 2 \pmod{5} \end{cases}$$

ja

$$\begin{cases} x \equiv 235 \pmod{3^5} \\ x \equiv 2 \pmod{5} \end{cases}$$

Ratkaistaan näistä ensin ensimmäinen. Ratkaistaan siis yhtälö

$$243y + 5z = 20 - 2 = 18$$

ensin käyttämällä Eukleideen algoritmia

$$243 = 48 \cdot 5 + 3, 5 = 3 + 2, 3 = 2 + 1$$

ja sen jälkeen kirjoittamalla

$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(243 - 48 \cdot 5) - 5 = 2 \cdot 243 - 97 \cdot 5.$

Nyt siis ensimmäisen yhtälöparin ratkaisut ovat mod 1215

$$x \equiv 20 - 2 \cdot 18 \cdot 243 \equiv 992.$$

Vastaavasti jälkimmäisen yhtälöparin ratkaisut ovat mod 1215

$$x \equiv 235 - 2 \cdot 233 \cdot 243 \equiv -8 \equiv 1207.$$