9. Kokonaislukujen jaollisuus

Tarkastelemme tässä luvussa jaollisuutta kokonaislukujen renkaassa $\mathbb{Z}$ ja todistamme tuloksia, joita käytetään kongruenssiluokkien renkaan $\mathbb{Z}/q\mathbb{Z}$ ominaisuuksien tarkastelussa. Luvussa 10 tarkastelemme polynomien jaollisuutta. Seuraavat jaollisuuden perusominaisuudet on helppo tarkastaa yleisessä tapauksessa.

Propositio 9.1. *Olkoon K kokonaisalue. Tällöin*
(1) $a \mid a$ kaikille $a \in K$.
(2) Jos $a \mid b$ ja $b \mid a$, niin $a = ub$ jollain $u \in K^\times$.
(3) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.
(4) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

Todistus. Harjoitustehtävä 100. □

Alkiot, joilla on vain vähän tekijöitä ovat tärkeässä osassa jaollisuutta tarkasteltaessa.

Määritelmä 9.2. Luonnollinen luku $p \neq 1$ on *alkuluku*, jos kaikilla $m, n \in \mathbb{N}$, joille $mn = p$ pätee $m = 1$ tai $n = 1$.

Esimerkki 9.3. Luvut $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$ ovat alkulukuja.

Kokonaislukuja käsiteltäessä merkintää p käytetään yleensä vain alkuluvuille.

Propositio 9.4. *Jokainen nollasta poikkeava kokonaisluku $q \in \mathbb{Z} \setminus \{0\}$ voidaan esittää alkulukujen tulona muodossa*

$$q = (-1)^{m(q)} \prod_p p^{a_p(q)},$$

missä $m(q) \in \{0, 1\}$ ja $a_p(q) \in \mathbb{N}$ kaikille alkuluvuille p ja $a_p(q) \neq 0$ vai äärelliselle joukolle alkulukuja p.

Todistus. Riittää tarkastella positiivisia lukuja. Selvästi väite pätee pienille luvuille $1, 2, 3, \ldots$ ja kaikille alkuluvuille. Oletetaan, että $N \in \mathbb{N}$ on pienin luku, jota ei voi esittää väitetyssä muodossa. Koska N ei erityisesti ole alkuluku, on $m, n \in \mathbb{N} \setminus \{1, p\}$, joille $N = mn$. Mutta nyt $2 \leq m, n < N$, joten luvuilla m ja n on haluttu esitys. Kertomalla nämä esitykset keskenään saadaan luku N esitettyä halutussa muodossa. □

Määritelmä 9.5. Jos luku $d \in \mathbb{Z}$ jakaa kokonaisluvut a ja b, niin d on lukujen a ja b *yhteinen tekijä*. Jos $m, n \in \mathbb{Z} \setminus \{0\}$ $d \in \mathbb{Z}$ on lukujen m ja n yhteinen tekijä, jonka jokainen lukujen m ja n yhteinen tekijä jakaa, niin d on lukujen m ja n *suurin yhteinen tekijä*, merkitään $d = \mathrm{syt}(m, n)$.

Jos $\mathrm{syt}(m, n) = 1$, sanotaan, että luvut m ja n ovat *suhteellisia alkulukuja*, ja että m ja n ovat *keskenään jaottomia*.

Jos $d = \mathrm{syt}(m, n)$, niin myös $-d = \mathrm{syt}(m, n)$, joten $\mathrm{syt}(m, n)$ on merkintä, ei funktio. Proposition 9.1 nojalla kahden kokonaisluvun suurin yhteinen tekijä on määritelty merkkiä vaille, jos voidaan osoittaa, että kaikilla kokonaislukupareilla on suurin yhteinen tekijä. Tämä seuraa alla todistettavasta Propositiosta 9.6.

Propositio 9.6. *Olkoot $m, n \in \mathbb{Z} \setminus \{0\}$. Jos $\langle m, n \rangle = \langle d \rangle$, niin $d = \mathrm{syt}(m, n)$.*

Todistus. Olkoon $e \neq 0$ lukujen m ja n yhteinen tekijä. Koska $d \in \langle m, n \rangle$, on luvut $r, s \in \mathbb{Z}$ siten, että

$$rm + sn = d.$$

Siispä Proposition 9.1(4) nojalla $e \mid d$. □

Seuraus 9.7. *Nollasta poikkeavilla kokonaisuvuilla on suurin yhteinen tekijä, joka on merkkiä vaille yksikäsitteinen.*

Todistus. Proposition 5.16 mukaan kaikki kokonaislukujen additiivisen ryhmän aliryhmät ovat syklisiä, joten on $d \in \mathbb{N}$ siten, että $\langle d \rangle = \langle m, n \rangle$. Väite seuraa siis Propositiosta 9.6 ja siitä, että $\mathbb{Z}^\times = \{-1, 1\}$. □

Seuraus 9.8. *(1)* $\mathbb{Z}/q\mathbb{Z} = \langle a + q\mathbb{Z} \rangle$*, jos ja vain jos* $1 = \text{syt}(a, q)$.
(2) $a + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$ *on yksikkö, jos ja vain jos* $1 = \text{syt}(a, q)$.

Todistus. (1) Harjoitustehtävä 101.
(2) Kongruenssin määritelmän nojalla $ab \equiv 1 \mod q$, jos ja vain jos on $c \in \mathbb{Z}$, jolle $ab = 1 + cq$. Tämä taas on Proposition 9.6 ja Seurauksen 9.7 nojalla yhtäpitävää sen kanssa, että $1 = \text{syt}(a, q)$. □

Edellisten tulosten nojalla siis kokonaislukujen $m, n \in \mathbb{Z}$ suurin yhteinen tekijä d voidaan esittää sopivien kokonaislukujen $r, s \in \mathbb{Z}$ avulla muodossa

$$d = rm + sn. \tag{9}$$

Yhtälöä (9) kutsutaan *Bezout'n yhtälöksi.*

Suurin yhteinen tekijä voidaan määritellä vastaavasti myös useammalle kokonaisluvulle: Aliryhmän $\langle a_1, a_2, \ldots, a_n \rangle$ virittäjä on lukujen $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ suurin yhteinen tekijä.

Esimerkki 9.9. (a) $\text{syt}(12, 30) = 6$: Luvun 12 positiiviset tekijät ovat $1, 2, 3, 4, 6$ ja luvun positiiviset tekijät ovat 30 $1, 2, 3, 5, 6, 10, 15, 30$.
(b) $\text{syt}(6, 10, 15) = 1$.
(c) $\text{syt}(n, n+1) = 1$ kaikilla $n \in \mathbb{N}$: Olkoon $d \in \mathbb{N}$ lukujen n ja $(n+1)$ jakaja. Koska d jakaa luvun $n + (-1)(n+1) = -1$, niin on oltava $d = 1$. Luvuilla n ja $n+1$ ei siis ole muita positiivisia yhteisiä tekijöitä kuin 1.

Propositio 9.10. *Alkulukuja on äärettömän monta.*

Todistus. Harjoitustehtävä 104 □

Seuraavat jaollisuustulokset pätevät keskenään jaottomille luvuille.

Propositio 9.11. *Olkoot* $a, b \in \mathbb{Z}$ *keskenään jaottomia ja* $c \in \mathbb{Z}$*. Tällöin*
(1) Jos $a \mid c$ *ja* $b \mid c$*, niin* $ab \mid c$.
(2) Jos $a \mid bc$*, niin* $a \mid c$.

Todistus. (1) Koska $\text{syt}(a, b) = 1$, niin $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$. Oletuksen nojalla on $k, l \in \mathbb{Z}$ siten, että $ka = c = lb$. Nyt on

$$c = c(xa + yb) = cxa + cyb = (lb)xa + (ka)yb = ab(lx + ky)$$

ja $lx + ky \in \mathbb{Z}$, joten $ab \mid c$.
(2) Kuten kohdassa (1) saadaan $c = cxa + cyb$ jollain $x, y \in \mathbb{Z}$. Koska $a \mid bc$ ja $a \mid a$, niin a jakaa summan $cxa + ybc = c$. □

Proposition 9.11 väitteet eivät päde ilman oletusta keskinäisestä jaottomuudesta. Tämä on helppo todeta esimerkiksi kohdan (1) tapauksessa huomaamalla, että 2 jakaa luvun 2 mutta $2 \cdot 2 = 4$ ei jaa lukua 2.

Lemma 9.12 (Eukleideen lemma)**.** *Olkoot* p *alkuluku ja* $a, b \in \mathbb{Z}$*. Jos* $p \mid (ab)$*, niin* $p \mid a$ *tai* $p \mid b$*. Yleisemmin, jos* $p \mid (a_1 \cdots a_n)$*, missä* $a_i \in \mathbb{Z}$ *kaikilla* $i = 1, \ldots, n$*, niin* $p \mid a_i$ *jollain* i.

Todistus. Jos $p \nmid a$, niin $\text{syt}(a,p) = 1$. Proposition 9.11(2) perusteella $p \mid b$. Yleinen tapaus todistetaan induktiolla. □

Nyt voimme täydentää Proposition 9.4 tuloksen kokonaislukujen aritmetiikan keskeiseksi tulokseksi.

Lause 9.13 (Aritmetiikan peruslause)**.** *Jokainen nollasta poikkeava kokonaisluku $q \in \mathbb{Z} \setminus \{0\}$ voidaan voidaan esittää alkulukujen äärellisenä tulona muodossa*

$$q = (-1)^{m(q)} \prod_p p^{a_p(q)},$$

missä $m(q) \in \{0,1\}$ ja $a_p(q) \in \mathbb{N}$ kaikille alkuluvuille p. Tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.

Todistus. Propositiossa 9.4 osoitettiin, että q voidaan esittää väitteen mukaisen tulona. Osoitetaan yksikäsitteisyys. Riittää käsitellä positiivisia lukuja. Oletetaan, että

$$q = p_1 \cdots p_k = q_1 \cdots q_s, \tag{10}$$

missä p_i ja $q_j$ovat alkulukuja kaikilla $1 \leq i \leq k$ ja $1 \leq j \leq s$.

Koska $p_1 \mid n$, niin Lemman 9.12 perusteella se jakaa luvun q_j jollain $j = 1, \ldots, s$. Numeroimalla tekijät $q_1, \ldots, q_s$ tarvittaessa uudelleen voidaan olettaa, että $p_1 \mid q_1$. Koska p_1 ja q_1 ovat alkulukuja, niin on $p_1 = q_1$. Supistamalla tekijä p_1 saadaan yhtälöstä (10)

$$p_2 \cdots p_k = q_2 \cdots q_s.$$

Kuten edellä päättelemme, että $p_2 = q_2$. Toistamalla prosessia, joka loppuu $\min(k,s)$ askeleen jälkeen, saamme $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k$, erityisesti, $k = s$. □

Määritelmä 9.14. Aritmetiikan peruslauseen antamaa luvun $n \in \mathbb{N}$, $n \geq 2$, esitystä

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

missä $p_1 < \cdots < p_k$ ovat alkulukuja ja $e_1, \ldots e_k \in \mathbb{N}$, sanotaan luvun n *alkutekijäesitykseksi*. Luvut p_i ovat luvun n *alku(luku)tekijöitä.*

Sovellamme jaollisuustuloksia renkaiden $\mathbb{Z}/q\mathbb{Z}$ teoriaan:

Lause 9.15. *Seuraavat väitteet ovat yhtäpitäviä:*

(1) $\mathbb{Z}/q\mathbb{Z}$ *on kokonaisalue.*
(2) $\mathbb{Z}/q\mathbb{Z}$ *on kunta.*
(3) q *on alkuluku.*

Todistus. Kohtien (1) ja (2) yhtäpitävyys seuraa Lauseesta 8.13. Osoitetaan, että kohdat (1) ja (3) ovat yhtäpitäviä: Olkoot $x, y \in \mathbb{Z} \setminus q\mathbb{Z}$. Jos $(x+q\mathbb{Z})(y+q\mathbb{Z}) = q\mathbb{Z}$, niin $q \mid xy$. Jos q on alkuluku, niin Eukleideen lemman nojalla $q \mid x$ tai $q \mid y$, jolloin $(x+q\mathbb{Z}) = 0$ tai $(y+q\mathbb{Z}) = 0$. Jos $q = ab$, $a, b \notin \{\pm 1\}$, ei ole alkuluku, niin q ei jaa tekijöitä a ja b, joten $a+q\mathbb{Z}$ ja $b+q\mathbb{Z}$ ovat nollan jakajia. □

Lauseen 9.15 todistusta tarkastelemalla saadaan kaikkia kongruenssiluokkien muodostamia renkaita koskeva tulos

Propositio 9.16. *Alkio $a+q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z}$, $a \notin q\mathbb{Z}$, on nollan jakaja, jos ja vain jos* $\text{syt}(a,q) > 1$.

Todistus. Harjoitustehtävä 103. □

Seuraus 9.17. *Renkaan $\mathbb{Z}/q\mathbb{Z}$ nollasta poikkeava alkio on joko nollan jakaja tai yksikkö.*

Esimerkki 9.18. Renkaan $\mathbb{Z}/8\mathbb{Z}$ yksiköiden ryhmä on isomorfinen Kleinin neliryhmän $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ kanssa: Yksiköt toteuttavat $1 = 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \mod 8$ ja $3 \cdot 5 \equiv 7 \mod 8$. Kuvaus $1 \mapsto (0,0)$, $3 \mapsto (0,1)$, $5 \mapsto (1,0)$, $7 \mapsto (1,1)$ on isomorfismi.

Rengasteoriassa käytetään usein hieman alkuluvun määritelmää kuin tässä luvussa käytetty Määritelmä 9.2: Sanotaan, että renkaan R alkio p, joka ei ole yksikkö, on *renkaan R alkuluku*, jos kaikille $a, b \in R$ pätee $p \mid a$ tai $p \mid b$, jos $p \mid ab$, toisin sanoen, jos Eukleideen lemman väite pätee alkiolle p. Alkiota $p \in R$, jonka kaikki tekijät ovat yksiköitä tai muotoa up, missä u on renkaan R yksikkö, sanotaan *renkaan R jaottomiksi alkioiksi*. Kokonaislukujen renkaassa jaottomat alkiot ja (rengasteorian määritelmän mukaiset) alkuluvut ovat samoja. Näillä määritelmillä luvut $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29, \ldots$ ovat alkulukuja ja jaottomia lukuja. Aritmetiikan peruslause (Lause 9.14) pätee tälläkin määritelmällä kunhan alkutekijäesityksessä rajoitutaan positiivisiin alkulukuihin.

Alkulukuesityksen yksikäsitteisyys ei ole itsestään selvä asia: Olkoon

$$\mathbb{P} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} = \{n \in \mathbb{Z} : n \text{ on parillinen}\}.$$

Joukko $\mathbb{P}$ on yhteenlaskun ja kertolaskun suhteen vakaa joukko mutta se ei ole rengas koska kertolaskulla ei ole neutraalialkiota. Yhteen- ja kertolaskulla varustetussa joukossa $\mathbb{P}$ voidaan määritellään käsitteet tekijä, jaollisuus ja alkuluku samaan tapaan kuin kokonaislukujen joukossa, esim. luku $m \in \mathbb{P}$ jakaa luvun $n \in \mathbb{P}$, jos on $k \in \mathbb{P}$ siten, että $n = km$. Joukon $\mathbb{P}$ alkulukuja ovat esimerkiksi $2, 6, 10, 14, 18, 26$ ja 30. Nyt

$$180 = 6 \cdot 30 = 10 \cdot 18,$$

missä kaikki tekijät ovat joukon $\mathbb{P}$ alkulukuja.

Kahden kokonaisluvun suurimman yhteisen tekijän etsiminen listaamalla ensin molempien lukujen kaikki tekijät ja etsimällä suurin yhteinen tekijä näiden joukosta on isoilla luvuilla työläs menetelmä. Seuraavaan lemmaan perustuva *Eukleideen algoritmi* antaa tehokkaamman keinon suurimman yhteisen tekijän löytämiseksi.

Lemma 9.19. *Jos $a, b, q, r \in \mathbb{Z}$ ja $a = qb + r$, niin* $\operatorname{syt}(a, b) = \operatorname{syt}(b, r)$.

Todistus. Proposition 9.1 nojalla jokainen lukujen b ja r yhteinen tekijä jakaa summan $qb + r = a$. Vastaavasti jokainen lukujen a ja b yhteinen tekijä jakaa luvun $a - qb = r$. Pareilla a, b ja b, r on siis samat yhteiset tekijät. Siten on myös $\operatorname{syt}(a, b) = \operatorname{syt}(b, r)$. □

Eukleideen algoritmi: Olkoot $a, b \in \mathbb{Z} \setminus \{0\}$. Merkitään $d = \operatorname{syt}(a, b)$. Koska

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

niin voidaan olettaa, että $a, b \in \mathbb{N}$ ja että $a > b$.

Jakamalla a luvulla b saadaan luvut $q_1, r_1 \in \mathbb{Z}$, joille

$$a = q_1 b + r_1 \quad \text{ja } 0 \leq r_1 < b. \tag{11}$$

Jos $r_1 = 0$, niin $b \mid a$. Tällöin $d = b$; lopetetaan.
Jos $r_1 > 0$, jaetaan b luvulla r_1. Jakoyhtälö antaa luvut $q_2, r_2 \in \mathbb{Z}$, joille

$$b = q_2 r_1 + r_2 \quad \text{ja } 0 \leq r_2 < r_1. \tag{12}$$

Lemman 9.19 nojalla $\operatorname{syt}(a, b) = \operatorname{syt}(b, r_1)$. Siten, jos $r_2 = 0$, niin $d = r_1$; lopetetaan.
Jos $r_2 > 0$, jaetaan r_1 luvulla r_2. Jakoyhtälö antaa luvut $q_3, r_3 \in \mathbb{Z}$, joille

$$r_1 = q_3 r_2 + r_3 \quad \text{ja } 0 \leq r_3 < r_2. \tag{13}$$

Jatketaan kuten edellä. Koska jakoyhtälön antamat jakojäännökset r_i eivät ole negatiivisia ja ne muodostavat aidosti vähenevän jonon,

$$b > r_1 > r_2 > \cdots \geq 0,$$

niin jollain n on oltava $r_n = 0$ Viimeiset kaksi vaihetta ovat

$$r_{n-3} = q_{n-1}r_{n-2} + r_{n-1}, \qquad 0 < r_{n-1} < r_{n-2}, \tag{14}$$

$$r_{n-2} = q_n r_{n-1} + r_n, \qquad r_n = 0. \tag{15}$$

Propositio 9.20 (Eukleideen algoritmi)**.** *Olkoot a, b ja jakojäännökset r_i kuten yllä. Tällöin r_{n-1}, viimeinen positiivinen jakojäännös, on* $\operatorname{syt}(a, b)$.

Todistus. Lemma 9.19 sovellettuna lausekkeisiin (11)–(14) kertoo, että

$$d = \operatorname{syt}(a, b) = \operatorname{syt}(b, r_1) = \operatorname{syt}(r_1, r_2) = \cdots = \operatorname{syt}(r_{n-2}, r_{n-1}).$$

Yhtälön (15) perusteella $r_{n-1} \mid r_{n-2}$, joten $\operatorname{syt}(r_{n-2}, r_{n-1}) = r_{n-1}$. Siten $d = r_{n-1}$. □

Esimerkki 9.21. Lasketaan $\operatorname{syt}(22, 60)$ ja etsitään sellaiset luvut $x, y \in \mathbb{Z}$, että $\operatorname{syt}(a, b) = xa + yb$. Eukleideen algoritmilla saadaan

$$\begin{aligned} 60 &= 2 \cdot \underline{22} + \boxed{16} & 16 &= 60 - 2 \cdot 22 \\ \underline{22} &= 1 \cdot \boxed{16} + \underline{\underline{6}} & 6 &= 22 - 16 \\ \boxed{16} &= 2 \cdot \underline{\underline{6}} + \boxed{4} & 4 &= 16 - 2 \cdot 6 \\ \underline{\underline{6}} &= 1 \cdot \boxed{4} + \underline{2} & 2 &= 6 - 4 \\ \boxed{4} &= 2 \cdot \underline{2}. \end{aligned}$$

Siten $\operatorname{syt}(22, 60) = 2$. "Peruuttamalla" algoritmissa saadaan

$$\begin{aligned} 2 &= 6 - 4 = 6 - (16 - 2 \cdot 6) = 3 \cdot 6 - 16 = 3(22 - 16) - 16 \\ &= 3 \cdot 22 - 4 \cdot 16 = 3 \cdot 22 - 4(60 - 2 \cdot 22) \\ &= 11 \cdot 22 - 4 \cdot 60. \end{aligned}$$

Harjoitustehtäviä.

Tehtävä 99. Olkoon K kokonaisalue ja olkoot $a \in K \setminus \{0\}$ ja $u, v \in K$. Osoita, että $u = v$, jos $au = av$.

Tehtävä 100. Olkoon K kokonaisalue. Osoita, että

(1) $a \mid a$ kaikille $a \in \mathbb{Z}$

(2) Jos $a \mid b$ ja $b \mid a$, niin $a = ub$ jollain $u \in K^\times$.

(3) Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.

(4) Jos $a \mid b$ ja $a \mid c$, niin $a \mid b + c$.

Tehtävä 101. Osoita, että $\mathbb{Z}/q\mathbb{Z} = \langle a + q\mathbb{Z} \rangle$, jos ja vain jos $1 = \operatorname{syt}(a, q)$.

Tehtävä 102. Määritä $\langle 30, 42, 70, 105 \rangle \leq (\mathbb{Z}, +)$.

Tehtävä 103. Olkoot $a \in \mathbb{Z}$, $q \in \mathbb{N}$. Osoita, että $[a] \in \mathbb{Z}/q\mathbb{Z}$ on nollan jakaja, jos ja vain jos $\operatorname{syt}(a, q) > 1$.

Tehtävä 104. Osoita, että alkulukuja on äärettömän monta.

Tehtävä 105. Määritä renkaiden $\mathbb{Z}/6\mathbb{Z}$ ja $\mathbb{Z}/10\mathbb{Z}$ ja $\mathbb{Z}/101\mathbb{Z}$ yksiköt.

[104] Vihje: Olkoot $p_1, p_2, \ldots, p_n$ alkulukuja. Mitä voit päätellä luvusta $p_1 p_2 \cdot \cdots \cdot p_n + 1$?

Tehtävä 106. Määritä renkaan $\mathbb{Z}/9\mathbb{Z}$? yksiköt ja nollan jakajat. Onko renkaan $\mathbb{Z}/9\mathbb{Z}$ yksiköiden ryhmä syklinen?

Tehtävä 107. Määritä Eukleideen algoritmilla lukujen 1059 ja 675 suurin yhteinen tekijä.