Matematiikka tutuksi -kurssi

Alkuluvut ja jaollisuus

Avoin yliopisto & Matematiikan ja tilastotieteen laitos
Helsingin yliopisto
Kesä 2015

Juulia Lahdenperä

Lukuteoria

Lukuteoria on eräs vanhimmista matematiikan aloista. On sanottu, että siinä missä matematiikka on tieteiden kuningatar, on lukuteoria matematiikan kuningatar. Perehdymme seuraavassa luonnollisten lukujen jaollisuuteen ja alkulukuihin.

Eukleides Aleksandrialainen
(n. 300 eaa)

Jaollisuus

Määritelmä

Luku $m \in \mathbb{Z}$ jakaa luvun $n \in \mathbb{Z}$, merkitään $m|n$, mikäli on olemassa sellainen $k \in \mathbb{Z}$, että $n = m \cdot k$.

Sanomme tällöin myös, että n on jaollinen m:llä.
Tämä tarkoittaa sitä, että jako n/m menee tasan, eikä jakojäännöstä jää.

- Esimerkiksi $6 = 2 \cdot 3$, joten $2|6$ ja $3|6$
- Määritelmästä seuraa, että jokainen luonnollinen luku on jaollinen itsellään ja ykkösellä!

Määritelmä

Ykköstä suurempaa luonnollista lukua p, joka ei ole jaollinen muilla luonnollisilla luvuilla kuin itsellään ja ykkösellä, sanotaan **alkuluvuksi**.

Ts. luonnollinen luku $p \geq 2$ on alkuluku jos $\{n \in \mathbb{N} \mid n|p\} = \{1, p\}$.
Alkulukuja ovat luvut $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Jakoyhtälö

Kun luonnollinen luku n jaetaan nollasta poikkeavalla luonnollisella luvulla m, saadaan osamäärä k, joka kertoo kuinka monta kokonaista kertaa luku m mahtuu lukuun n, sekä jakojäännös r, joka kertoo, kuinka paljon jää yli. Jakojäännös on aina vähintään 0 mutta alle m. Näin saadaan **jakoyhtälö**.

Lause (Jakoyhtälö)

Olkoot n ja m luonnollisia lukuja, ja $m > 0$. Tällöin on olemassa luonnolliset luvut k ja r, joilla pätee:

$$n = m \cdot k + r,$$

ja $0 \leq r < m$.

Esimerkkejä jakoyhtälöstä

Muodostetaan jakoyhtälö, kun luku 18 jaetaan luvulla 7. 7 menee lukuun 18 kaksi kokonaista kertaa, ja jakojäännös on 4. Siispä jakoyhtälö on

$$18 = 7 \cdot 2 + 4.$$

Kun taas luku 251 jaetaan luvulla 20, saadaan osamääräksi 12 ja jakojäännökseksi 11. Tällöin jakoyhtälö on

$$251 = 20 \cdot 12 + 11.$$

Parillisuus

Kahdella jaollista luonnollista lukua sanotaan **parilliseksi**. Parilliset luvut ovat siis muotoa $2k$ jollakin $k \in \mathbb{N}$. Muotoa $2k+1$ olevat luvut ovat **parittomia**. Soveltamalla jakoyhtälöä tapauksessa $m = 2$ tiedetään, että jokainen luonnollinen luku on joko parillinen tai pariton.

Jos jakoyhtälöä sovelletaan esimerkiksi valinnalla $m = 3$, voidaan jokainen luonnollinen luku n kirjoittaa jossain seuraavista muodoista:

- $n = 3k$ jollakin $k \in \mathbb{N}$ (kun n on jaollinen kolmella)
- $n = 3k + 1$ jollakin $k \in \mathbb{N}$ (kun laskettaessa $n/3$ jakojäännös on 1)
- $n = 3k + 2$ jollakin $k \in \mathbb{N}$ (kun laskettaessa $n/3$ jakojäännös on 2)

Esimerkkitehtävä

Olkoon n luonnollinen luku. Osoitetaan, että tällöin $n^2 - n$ on parillinen.

Jakoyhtälön nojalla joko $n = 2k$ jollakin $k \in \mathbb{N}$ tai $n = 2k + 1$ jollakin $k \in \mathbb{N}$. Tarkastellaan nämä tapaukset erikseen:
Jos $n = 2k$ jollakin $k \in \mathbb{N}$, niin
$n^2 - n = (2k)^2 - 2k = 4k^2 - 2k = 2(2k^2 - k)$. Tämä on jaollinen luvulla 2.
Jos taas $n = 2k + 1$ jollakin $k \in \mathbb{N}$, niin
$n^2 - n = (2k + 1)^2 - (2k + 1) = 4k^2 + 4k + 1 - 2k - 1 =$
$4k^2 + 2k = 2(2k^2 + k)$. Tämä on jaollinen luvulla 2.
Siispä kummassakin tapauksessa $n^2 - n$ on parillinen.

Esimerkkitehtävä

Olkoon n luonnollinen luku. Osoitetaan, että $n(n^2+2)$ on jaollinen luvulla 3.

Tarkastellaan eri tapaukset:
Jos $n = 3k$ jollakin $k \in \mathbb{N}$, niin

$$n(n^2+2) = 3k((3k)^2+2),$$

mikä on kolmella jaollinen.
Jos taas $n = 3k+1$ jollakin $k \in \mathbb{N}$, niin

$$n(n^2+2) = (3k+1)((3k+1)^2+2) = (3k+1)(9k^2+6k+2+1),$$

mikä myös on kolmella jaollinen.
Lopuksi, jos $n = 3k+2$ jollakin $k \in \mathbb{N}$, niin

$$n(n^2+2) = (3k+2)((3k+2)^2+2) = (3k+2)(9k^2+12k+4+2),$$

mikä jälleen on kolmella jaollinen.
Siis kaikissa tapuksissa luku $n(n^2+2)$ on kolmella jaollinen.

Suurin yhteinen tekijä syt

Esimerkki. Mikä on lukujen 5 ja 10 suurin yhteinen tekijä eli $syt(5, 10)$?

Tutkitaan molempien lukujen jakajia. Luku 5 on jaollinen luvuilla 1 ja 5. Luku 10 on jaollinen luvuilla $1, 2, 5$ ja 10. Lukujen 5 ja 10 suurin yhteinen jakaja on luku 5. Näin ollen $syt(5, 10) = 5$.

Esimerkki. $syt(75, 25) = 25$, sillä luku 25 on suurin mahdollinen luku, joka jakaa molemmat luvut 75 ja 25.

Euklideen algoritmi I

Euklideen algoritmin avulla etsitään lukujen suurinta yhteistä tekijää.

Esimerkki. Etsi lukujen $2\ 100$ ja 510 suurin yhteinen tekijä.

$$2\ 100 = 510 \cdot 4 + 60$$
$$510 = 60 \cdot 8 + 30$$
$$60 = 30 \cdot 2 + 0$$

Näin ollen $syt(2\ 100, 510) = 30$.

Euklideen algoritmi II

Esimerkki. Etsi lukujen $1\ 210$ ja 522 suurin yhteinen tekijä.

$$
\begin{aligned}
1\ 210 &= 522 \cdot 2 + 1660 \\
522 &= 166 \cdot 3 + 24 \\
166 &= 24 \cdot 6 + 22 \\
24 &= 22 \cdot 1 + 2 \\
22 &= 2 \cdot 11 + 0
\end{aligned}
$$

Näin ollen $syt(1\ 210, 522) = 11$.

Eratostheneen seula

Eratostheneen seula on algoritmi, jolla löydetään kaikki alkuluvut annettuun lukuun $n \in \mathbb{N}$ asti. Kokeillaan algoritmia arvolla $n = 100$:

1. listaa järjestyksessä luonnolliset luvut $2, 3, \ldots, n$
2. merkitse punaisella listan ensimmäinen merkitsemätön alkuluku p
3. pyyhi listasta kaikki alkuluvun p:n monikerrat
4. toista vaiheet 2 ja 3 kunnes $p^2 > n$
5. loput listan luvut ovat alkulukuja!

	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

Aritmetiikan peruslause

Alkuluvut ovat luonnollisten lukujen "rakennuspalikoita", kuten **Aritmetiikan peruslause** kertoo:

Lause

Jokainen luonnollinen luku (poislukien 0 ja 1) voidaan esittää yksikäsitteisesti alkulukujen äärellisenä tulona.

Yksikäsitteisyys on voimassa tekijöiden järjestystä lukuunottamatta. Huomaa, että kukin tekijä voi esiintyä tulossa useamman kerran.

Esim.
$308 = 2 \cdot 154 = 2^2 \cdot 77 = 2^2 \cdot 7 \cdot 11$
$975 = 3 \cdot 325 = 3 \cdot 5 \cdot 65 = 3 \cdot 5^2 \cdot 13$

Luonnollisen luvun esitystä alkulukujen tulona sanotaan luvun **alkutekijähajotelmaksi**.

Alkulukujen äärettömyys

Lause

Alkulukuja on äärettömän monta.

Todistus.

Tehdään vastaoletus: Alkulukuja on vain äärellisen monta, merkitään niitä $p_1, p_2, \ldots, p_n$. Tarkastellaan sitten lukua

$$N = p_1 \cdot p_2 \cdots p_n + 1.$$

Aritmeriikan peruslauseesta seuraa, että N on jaollinen jollakin alkuluvuista $p_1, p_2, \ldots, p_n$. Siis jokin luvuista p_i, $i = 1, \ldots, n$ jakaa N:n ja tulon $p_1 \cdot p_2 \ldots p_n$, joten se jakaa myös erotuksen

$$N - p_1 \cdot p_2 \cdots p_k = 1.$$

Tämä on ristiriita, sillä ykkönen ei ole jaollinen millään (alku)luvulla, joten alkuperäinen väite on todistettu. □

$\mathbb{Q}$ on numeroituva

Eräs tapa osoittaa positiivisten rationaalilukujen joukko (ja siten koko $\mathbb{Q}$) numeroituvaksi on tarkastella positiivisten kokonaislukujen pareilla määriteltyä funktiota

$$f(n,m) = 2^n 3^m, \quad n,m \in \mathbb{Z}_+.$$

Koska 2 ja 3 ovat alkulukuja, niin Aritmetiikan peruslauseen nojalla

$$2^{n_1}3^{m_1} = 2^{n_2}3^{m_2} \quad \Longleftrightarrow \quad n_1 = n_2 \quad \text{ja} \quad m_1 = m_2.$$

Jos siis $f(n_1,m_1) = f(n_2,m_2)$, niin $(n_1,m_1) = (n_2,m_2)$, eli f on injektio. Tämä tarkoittaa sitä, että positiivisten kokonaislukujen parien muodostama joukko on "korkeintaan" yhtä mahtava kuin $\mathbb{N}$. Takuulla noita pareja on kuitenkin äärettömän monta ja siten niiden joukko on yhtä mahtava kuin $\mathbb{N}$. Positiiviset rationaaliluvut voidaan puolestaan ajatella positiivisten kokonaislukujen parien joukon osajoukkona.

Mersennen alkuluvut

Tarkastellaan muotoa $2^n - 1$ olevia lukuja arvoilla $n \geq 2$:
$2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^4 - 1 = 15$, $2^5 - 1 = 31$, $2^6 - 1 = 63$, ...
Huomataan, että tapauksissa $n = 2, 3, 5$ luku $2^n - 1$ on alkuluku, kun taas tapauksissa $n = 4, 6$ näin ei ole.
Onko $2^n - 1$ alkuluku aina, kun n on alkuluku?
Ei: $2^{11} - 1 = 2047 = 23 \cdot 89$.
Käänteinen väite on kuitenkin voimassa:
Jos $2^n - 1$ on alkuluku, niin myös n on alkuluku.

Määritelmä

Muotoa $2^p - 1$ olevia alkulukuja sanotaan *Mersennen alkuluvuiksi*.

Käytämme eksponentissa kirjainta p, koska tiedämme sen olevan alkuluku edellisen nojalla.

The Great Internet Mersenne Prime Search (GIMPS)

Tällä hetkellä tunnetaan 48 Mersennen alkulukua. Suurin tunnettu alkuluku on Mersennen alkuluku

$$2^{57\ 885\ 161} - 1,$$

joka löydettiin 25.1.2013. Tammikuusta 1996 lähtien on Mersennen alkulukuja etsitty yhteisvoimin internetissä The Great Internet Mersenne Prime Search -projektissa. Käy tutustumassa ja osallistu etsintään!

Avoimia ongelmia

Alkulukuihin liittyy vielä tällä hetkellä avoimia ongelmia.
Esimerkiksi

- Onko Mersennen alkulukuja äärettömän monta?
- *Alkulukuparit:* Onko olemassa äärettömän monta alkulukua p, jolle myös $p+2$ on alkuluku?
  Esim. 3 ja 5, 5 ja 7, 11 ja 13, 17 ja 19, 29 ja 31, $\ldots$?
- *Goldbachin konjektuuri:* Jokainen kakkosta suurempi parillinen luku voidaan lausua kahden alkuluvun summana.
  Esim. $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$,
  $12 = 5+7$, $14 = 7+7$, $\ldots$?