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 $m \in \mathbb{N}$ jakaa luvun $n \in \mathbb{N}$, merkitään $m|n$, mikäli on olemassa sellainen $k \in \mathbb{N}$, 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.

- esim. $6 = 2 \cdot 3$, joten $2|6$ ja $3|6$
- jokainen luonnollinen luku on jaollinen itsellään ja ykkösellä!

Määritelmä

Ykköstä suurempaa luonnollista lukua p, joka on jaollinen vain itsellään ja ykkösellä, sanotaan **alkuluvuksi**.

Ts. luonnollinen luku $p \geq 2$ on alkuluku jos ainoastaan $p|p$ ja $1|p$.
Alkulukuja: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Parillisuus

Kahdella jaollista luonnollista lukua sanotaan **parilliseksi**. Parilliset luvut ovat siis muotoa $2k$ jollakin $k \in \mathbb{N}$.
Muut luonnolliset luvut ovat **parittomia** ja ne ovat muotoa $2k + 1$ jollakin $k \in \mathbb{N}$.
Annettua muotoa olevien lukujen jaollisuutta tutkittaessa on usein kätevää hajoittaa tarkastelu osiin erilaisten esitysten suhteen.
Esim. Jokainen luonnollinen luku n on jotain 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 $n(n^2+2)$ 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.

Jaollisuussääntöjä

Lukujen jaollisuus annetulla luvulla voidaan usein päätellä nopeasti sen numeroista mm. seuraavien sääntöjen avulla:

- Luku on jaollinen kolmella, jos sen numeroiden summa on jaollinen kolmella.
  Esim. $3|51741$, sillä $5+1+7+4+1=18$ on jaollinen kolmella.
- Luku on jaollinen seitsemällä, jos vähentämällä sen "ensimmäisten" numeroiden muodostamasta luvusta kaksi kertaa viimeinen numero saadaan seitsemällä jaollinen luku.
  Esim. $7|791$, sillä $79-2\cdot 1=77$ on jaollinen seitsemällä.
  $7|1512$, sillä $151-2\cdot 2=147=21\cdot 7$
- Luku on jaollinen yhdellätoista, jos sen numerot kerrottuna vuorotelleen $+1$:llä ja -1:llä oikealta lähtien muodostavat yhteenlaskettuna yhdellätoista jaollisen luvun.
  Esim. $11|14729$, sillä $9-2+7-4+1=11$ on jaollinen yhdellätoista.

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 luku p
3. pyyhi listasta kaikki 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
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

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.

$308 = 2 \cdot 154 = 2^2 \cdot 77 = 2^2 \cdot 7 \cdot 11$

$975 = 3 \cdot 325 = 3 \cdot 5 \cdot 65 = 3 \cdot 5^2 \cdot 13$

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

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

Aritmeriikan peruslauseesta seuraa, että N on jaollinen jollakin alkuluvuista $p_1, p_2, \ldots, p_n$. Mutta jos jokin luvuista p_i, $i = 1, \ldots, n$, niin tällöin se jakaa myös luvun

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

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

$\sqrt{2}$ on irrationaalinen

Todistetaan nyt aikaisemmin esittämämme väite $\sqrt{2}$:n irrationaalisuudesta.
Tehdään vastaoletus: $\sqrt{2}$ on rationaalinen, eli muotoa $\frac{m}{n}$, joillakin luonnollisilla luvuilla m ja n. Siten

$$n\sqrt{2} = m,$$

josta korottamalla puolittain toiseen saadaan

$$2n^2 = m^2.$$

Yhtälön oikean puolen luvussa tekijä 2 esiintyy parillisen määrän kertoja (jos m on parillinen, sisältää m^2 parillisen määrän tekijää 2). Vasemman puolen luvussa tekijä 2 esiintyy sen sijaan parittoman määrän kertoja. Tämä on ristiriidassa Aritmetiikan peruslauseen kanssa, joten vastaoletuksen on oltava väärin ja väitteen siten totta.

$\log_2 3$ on irrationaalinen

Osoita, että $\log_2 3$ on irrationaalinen.
Tehdään vastaoletus: $\log_2 3$ on rationaalinen, eli muotoa $\frac{m}{n}$ joillakin luonnollisilla luvuilla m ja n. Logaritmin määritelmän mukaan tällöin

$$3 = 2^{\frac{m}{n}}.$$

Korottamalla puolittain potenssiin n saadaan

$$3^n = 2^m.$$

Tämä on ristiriidassa Aritmetiikan peruslauseen kanssa, joten vastaoletuksen on oltava väärin ja väitteen totta.

$\mathbb{Q}$ 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

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

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.

Alkulukujen lukumääristä

Tiedämme, että alkulukuja on kaikkiaan äärettömän monta. Entä kuinka monta alkulukua on kullakin rajoitetulla reaalilukuvälillä ja kuinka niiden lukumäärä riippuu tämän välin pituudesta?
Merkitään korkeintaan n:n suuruisten alkulukujen lukumäärää $\pi(n)$:llä (merkintä ei liity lukuun π). Saadaan siis funktio

$$\pi : \mathbb{Z}_+ \to \mathbb{N}, \quad \pi(n) = \sharp\{p \in \mathbb{Z}_+ : p \text{ alkuluku }, p \leq n\}.$$

Lasketaan muutamia pieniä arvoja:
$\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$, $\pi(5) = 3$, ...

Alkulukulause

Arvojen $\pi(n)$ suuruusluokkaa voidaan arvioida logaritmifunktion avulla:

$$\pi(n) \sim \frac{n}{\ln n}$$

Tämä tulos tunnetaan Alkulukulauseena ja sillä tarkoitetaan sitä, että

$$\frac{\pi(n)}{n/\ln n} \to 1, \quad \text{kun } n \to \infty,$$

eli osamäärä lähestyy ykköstä, kun n kasvaa rajatta.

Alkulukulausen taulukointia

n	$\pi(n)$	osuus %	$n/\ln n \approx$
10	4	40,0	4
10^2	25	25,0	22
10^3	168	16,8	145
10^4	1229	12,3	1086
10^5	9592	9,6	8686
10^6	78498	7,8	72382
10^7	664579	6,6	620421
10^8	5761455	5,8	5428681
10^9	50847534	5,1	48254942
10^{10}	455052511	4,6	434294482

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 47 Mersennen alkulukua. Suurin tunnettu alkuluku on Mersennen alkuluku

$$2^{43112609} - 1.$$

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

Avoimia ongelmia

Alkulukuihin liittyy vielä tällä hetkellä ratkaisemattomia (eli 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, ...?
- Goldbachin konjektuuri: Jokainen kakkosta suurempi parillinen luku voidaan lausua kahden alkuluvun summana.
  Esim. $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$, $12 = 5+7$, $14 = 7+7$, ...?
  Huom. konjektuuri on "otaksuma", eli väite jonka uskotaan pitävän paikkansa, mutta jota ei olla pystytty todistamaan!

Kryptografia

Kryptografiassa tutkitaan menetelmiä salata välitettävää tietoa. Menetelmät voi jakaa kahteen tyyppiin:

- **Salaisen avaimen menetelmissä** kutkin keskenään tietoa välittävät henkilöt joutuvat sopimaan salaisesti avaimesta keskenään. Siitä syystä menetelmä soveltuu vain pienen ryhmän käyttöön. Jo muinaiset roomalaiset käyttivät näitä menetelmiä.
- **Julkisen avaimen menetelmissä** kukin tiedonvälittäjä julkistaa oman avaimensa. Salaisia avaimenvaihtoja ei siis tarvita ja siten nämä menetelmät soveltuva suurille joukoille. Mutta kuinka tällainen menetelmä voi onnistua salaamaan tiedonkulun?

Kaksoislukko

Esitetään seuraavaksi klassinen esimerkki salausmenettelystä, jossa salaista avaimenvaihtoa ei tarvita.
Oletetaan, että henkilö A haluaa lähettää salaisen viestin henkilölle B. He toimivat näin:

1. A laittaa viestinsä laatikkoon, jonka lukitsee omalla lukollaan L_A (vain A:lla on avain lukkoon L_A) ja lähettää laatikon B:lle
2. B vastaanottaa laatikon, lukitsee sen lisäksi omalla lukollaan L_B (vain B:llä on avain lukkoon L_B) ja lähettää "kaksoislukitun" laatikon takaisin A:lle
3. A vastaanottaa kaksoislukitun laatikon, poistaa siitä oman lukkonsa L_A ja lähettää laatikon B:lle
4. vastaanotettuaan laatikon voi B avata oman lukkonsa L_B ja lukea viestin

Menetelmän turvallisuus perustuu siis siihen, että kullakin tiedonvälittäjällä on avain vain omaan lukkoonsa. Myöskään salaista avaimenvaihtoa ei tarvita.

Suurin yhteinen tekijä ja Eulerin funktio

Olkoot a ja b positiivisia kokonaislukuja. Suurinta positiivista kokonaislukua, joka jakaa sekä a:n että b:n sanotaan niiden **suurimmaksi yhteiseksi tekijäksi**, merk. $\text{syt}(a, b)$.
Esim. $\text{syt}(3, 6) = 3$, $\text{syt}(20, 8) = 4$, $\text{syt}(5, 4) = 1$
Eulerin funktio on kuvaus $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$, jolle

$$\varphi(n) = \text{niiden lukujen } k \in \mathbb{Z}_+ \text{ lukumäärä, joilla } k \leq n \text{ ja } \text{syt}(k, n) = 1$$

ts.

$$\varphi(n) = \sharp\{k \in \mathbb{Z}_+ : k \leq n, \text{syt}(k, n) = 1\}.$$

Pieniä arvoja: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, ...
Huom.

- $\varphi(p) = p - 1$, kun p on alkuluku.
- Jos $\text{syt}(m, n) = 1$, niin $\varphi(mn) = \varphi(m)\varphi(n)$. Erityisesti, jos p ja q ovat eri alkulukuja, niin $\varphi(pq) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$.

RSA

Ron Rivest, Adi Shamir ja Len Adleman esittivät vuonna 1978 seuraavanlaisen salausalgoritmin:
Oletetaan, että henkilö A haluaa lähettää salaisen viestin henkilölle B.

1. B valitsee satunnaisesti kaksi suurta alkulukua $p \neq q$ ja laskee luvut $N = pq$ ja $\varphi(N) = (p-1)(q-1)$
2. B valitsee vielä positiivisen kokonaisluvun e, jolle $1 < e < \varphi(N)$ ja $\text{syt}(e, \varphi(N)) = 1$ ja etsii positiivisen kokonaisluvun d, jolle $ed \equiv 1 \pmod{\varphi(N)}$, ts. kun luku ed jaetaan luvulla $\varphi(N)$, jää jakojäännökseksi 1
3. B julkistaa luvut N ja e
4. A koodaa viestinsä luvuksi (tai luvuiksi) M, jolle $M \leq N$
5. A laskee luvun M^e, jakaa sen luvulla N, ja lähetää jakojäännöksen B:lle
6. B korottaa saamansa luvun (salaiseen) potenssiin d ja laskee jakojäännöksen luvulla N jaettaessa.
7. B on siis laskenut luvun $(M^e)^d$ jakojäännöksen luvulla N jaettaessa. Koska $ed \equiv 1 \pmod{\varphi(N)}$, niin Fermat'n pienen lauseen nojalla $M^{ed} \equiv M \pmod{N}$, eli B:n laskema jakojäännös on täsmälleen alkuperäinen viesti!

RSA

Mihin menetelmän turvallisuus perustuu? Viestin purkamiseen riittää siis tietää luku d. Laskeakseen luvun d, tarvitsee tietää e (julkinen) ja $\varphi(N)$. Mutta vaikka N on julkinen, on luvun $\varphi(N)$ laskeminen suunnilleen yhtä työlästä kuin luvun $N = pq$ tekijöihinjako, joka puolestaan on erittäin työlästä, koska p ja q ovat suuria (salaisia) alkulukuja.