Alkuluvut

LUKUTEORIA JA TODISTAMINEN, MAA11

Jokainen luku $(\neq 0)$ on jaollinen ainakin itsellään, vastaluvullaan ja luvuilla ± 1. Kun muita eri ole, niin kyseinen luku on alkuluku.

Määritelmä, alkuluku/yhdistetty luku:
Luku $a \geq 2$ on *alkuluku*, jos se ei ole jaollinen muilla positiiviluvuilla kuin itsellään ja yhdellä. Muussa tapauksessa a on *yhdistetty luku*.

Esimerkki **a)** Ensimmäiset alkuluvut ovat $2, 3, 5, 7, 11, 13, 17, 19$.
b) Ensimmäiset yhdistetyt luvut ovat $4 = 2 \cdot 2, 6 = 3 \cdot 2, 8 = 2 \cdot 2 \cdot 2$.
c) Luku 1 ei ole alkuluku eikä yhdistetty luku.

Huomautus **a)** Alkulukujen joukkoa voidaan merkitä vahvennetulla P kirjaimella, siis $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$
b) Luku 2 on ainoa parillinen alkuluku!

Määritelmä, alkutekijä:
Luvun a *alkutekijä* on tämän luvun sellainen tekijä, joka on alkuluku.

Esimerkki Jaa alkutekijöihin luku 252 eli esitä se alkulukujen tulona.

Tapa 1: $\underbrace{252}_{\substack{\text{jaol.}\\ \text{2:lla}}} = 2 \cdot \underbrace{126}_{\substack{\text{jaol.}\\ \text{2:lla}}} = 2 \cdot 2 \cdot \underbrace{63}_{\substack{\text{jaol.}\\ \text{3:lla}}} = 2 \cdot 2 \cdot 3 \cdot \underbrace{21}_{\substack{\text{jaol.}\\ \text{3:lla}}} = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$

Tapa 2: $\underbrace{252}_{\substack{\text{jaol.}\\ \text{9:lla}}} = 9 \cdot \underbrace{28}_{\substack{\text{jaol.}\\ \text{4:lla}}} = \underbrace{9}_{\substack{\text{jaol.}\\ \text{3:lla}}} \cdot 4 \cdot 7 = 3 \cdot 3 \cdot \underbrace{4}_{\substack{\text{jaol.}\\ \text{2:lla}}} \cdot 7 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$

Molemmissa tapauksissa saatiin samat alkutekijät, mutta eri järjestys.

Lause, aritmetiikan peruslause:
Jokainen luku $a \geq 2$, voidaan tekijöiden järjestystä vaille *yksikäsitteisesti* esittää alkulukujen tulona, eli jakaa alkulukuihin.

Todistus Pitää osoittaa kaksi asiaa: yksikäsitteisyys ja tulo alkuluvuista, yksikäsitteisyys jätetään myöhemmäksi, osoitetaan tulo.

Olkoon $a \geq 2$. Jos luku a on alkuluku, niin asia selvä. Jos taas luku a on yhdistetty luku, niin $a = bc$, missä $b, c \geq 2$. Jos b ja c ovat alkulukuja, niin alkutekijöihin jako on valmis. Muutoin ainakin toinen luvuista b tai c on yhdistetty luku, joten löytyy d ja e siten että $b = de$ (tai $c = de$). Näin jatkaen saadaan lopulta $a = bcde$ ..., missä b, c, d, e jne. ovat alkulukuja.
(Tarkasti ottaen yllä oleva pitäisi tehdä induktiolla. Jaon olemassaolon voisi osoittaa myös antiteesin kautta!)

Alkulukujen ominaisuuksia

Mistä tiedetään onko annettu luku alkuluku? Tähän kysymykseen liittyen tarkastellaan kahta menetelmää.

1. Eratostheneen seula: Kun annettu luku on pieni (tietokoneille pieni luku on ihmiselle suuri), voidaan hyödyntää Eratostheneen seulaa, jolla saadaan kaikki annettua lukua pienemmät alkuluvut.

Esimerkki Määrää kaikki lukua 14 pienemmät alkuluvut.
Kirjoitetaan aluksi kaikki luvut.
a) $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14$

Toisessa vaiheessa poistetaan kaikki 2:lla jaolliset luvut.
b) $2, 3, \quad 5, \quad 7, \quad 9, \quad 11, \quad 13$

Kolmannessa vaiheessa poistetaan kaikki 3:lla jaolliset luvut.
c) $2, 3, \quad 5, \quad 7, \quad 11, \quad 13$
Enempää ei tarvitse testata (Syy: alkulukutesti, johon palataan). Näin on saatu määrättyä kaikki lukua 14 pienemmän alkuluvut. Entäpä lukua 200 pienemmät alkuluvut?

Aivan vastaavalla tavalla, ensin 2:lla jaolliset pois, sitten 3:lla, 5:llä, 7:llä jne. aina siihen alkulukuun p asti, jolle $p < \sqrt{200} \approx 14{,}1421$. Eli viimeisessä vaiheessa poistetaan 13:sta jaolliset luvut pois.

Aluksi kaikki luvut 1— 200.

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	101	102	103	104	105	106
107	108	109	110	111	112	113	114	115	116	117	118	119	120	121
122	123	124	125	126	127	128	129	130	131	132	133	134	135	136
137	138	139	140	141	142	143	144	145	146	147	148	149	150	151
152	153	154	155	156	157	158	159	160	161	162	163	164	165	166
167	168	169	170	171	172	173	174	175	176	177	178	179	180	181
182	183	184	185	186	187	188	189	190	191	192	193	194	195	196
197	198	199	200											

Poistetaan 2:lla jaolliset. Nyt huomaat, että 2 on ainoa parillinen alkuluku.

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		101		103		105	
107		109		111		113		115		117		119		121
	123		125		127		129		131		133		135	
137		139		141		143		145		147		149		151
	153		155		157		159		161		163		165	
167		169		171		173		175		177		179		181
	183		185		187		189		191		193		195	
197		199												

Poistetaan 3:lla jaolliset.

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			101	103		
107		109			113	115			119	121
			125	127			131	133		
137		139			143	145			149	151
			155	157			161	163		
167		169			173	175			179	181
			185	187			191	193		
197		199								

Poistetaan 5:llä jaolliset.

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			101	103		
107		109			113				119	121
				127			131	133		
137		139			143				149	151
				157			161	163		
167		169			173				179	181
				187			191	193		
197		199								

Poistetaan 7:llä jaolliset.

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			101	103	
107		109				113				121
				127			131		
137		139				143			149	151
				157				163	
167		169				173			179	181
				187			191	193	
197		199							

Poistetaan 11:sta jaolliset.

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			101	103	
107		109				113				
				127			131		
137		139							149	151
				157				163	
167		169				173			179	181
							191	193	
197		199							

Ja viimeisessä vaiheessa poistetaan 13:sta jaolliset.

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		101	103		
107		109			113				
				127		131			
137		139						149	151
				157			163		
167					173			179	181
						191	193		
197		199							

Tässä ovat kaikki lukua 200 pienemmät alkuluvut. Eratostheneen seulan avulla voidaan periaatteessa aina selvittää onko annettu luku alkuluku vai ei. Menetelmä on kuitenkin liian hidas.

Palataan Eratostheneen seulassa esille tulleeseen alkulukutestiin. Alkulukutesti on alkeellinen menetelmä sen tutkimiseksi, onko tietty luku alkuluku.

2. Alkulukutesti: Aluksi tarvitaan pieni lemma (aputulos).

Lemma, tekijöiden epäyhtälö:
Olkoon $a \geq 1$. Jos $a = bc$, missä $1 \leq b \leq c$, niin $b \leq \sqrt{a}$ ja $c \geq \sqrt{a}$.

Todistus Vastaoletus: $b > \sqrt{a}$ tai $c < \sqrt{a}$.

Tällöin, kun $b > \sqrt{a}$, niin saadaan

$$a \overset{\text{ol.}}{=} bc \overset{\text{ol.}}{\geq} b^2 \overset{\text{vastaol.}}{>} a \implies a > a, \quad \text{ristiriita.}$$

Toisaalta, kun $c < \sqrt{a}$, niin saadaan

$$a \overset{\text{ol.}}{=} bc \overset{\text{ol.}}{\leq} c^2 \overset{\text{vastaol.}}{<} a \implies a < a, \quad \text{jälleen ristiriita.}$$

Näin ollen vastaoletus johtaa aina ristiriitaan ja väite on siten tosi.

Olkoon sitten $n \geq 2$. Jos n on yhdistetty luku, niin edellisen lemman nojalla sillä on tekijä p, jolle $2 \leq p \leq \sqrt{n}$. Riittää siis käydä läpi tämän ehdon toteuttavat luvut.
Aritmetiikan peruslauseesta saadaan tarkemmin. Nimittäin sen nojalla riittää käydä läpi vain ehdon $2 \leq p \leq \sqrt{n}$ toteuttavat alkuluvut.

Lause, alkulukutesti:
Luku $n\ (\geq 2)$ on alkuluku, jos ja vain jos se ei ole jaollinen millään sellaisella alkuluvulla, joka on enintään $\sqrt{n}$.

Esimerkki: Onko 163 alkuluku?
Voitaisiin käyttää Eratostheneen seulaa ja tutkia miten käy. Tarkastellaan kuitenkin niitä alkulukuja p, joille $p \leq \sqrt{163}$. Koska $11^2 = 121 < 163$ ja $13^2 = 169 > 163$, niin riittää tutkia jakolaskut $163 : p$, missä $p = 2,3,5,7$ tai 11. Jos jako menee tasan, niin 163 ei ole alkuluku!
Osoittautuu, että 163 ei ole jaollinen millään edellä mainituista luvuista, joten 163 on alkuluku.

Esimerkki: Onko $20154003698204 \cdot 10^{15900} \pm 1$ alkuluku?

Esimerkki: Onko $20154003698204 \cdot 10^{15900} \pm 1$ alkuluku?
Tällä hetkellä parhaimmat alkulukutestit toimivat sellaisella nopeudella, että testissä tarvitaan s^6 laskutoimitusta, missä s on testattavan luvun numeroiden määrä kymmenjärjestelmässä. → Jätetään asia hautumaan → hyvä koetehtävä ☺.

https://en.wikipedia.org/wiki/Largest_known_prime_number

Lause, alkulukujen määrä:
Alkulukuja on äärettömän paljon.
Todistus On jo tehty.

http://www.isthe.com/chongo/tech/math/digit/m57885161/prime-c-e.html#middle

Määritelmä, Mersennen alkuluvut ja Mersennen luvut:
Olkoon p alkuluku. Tällöin muotoa $2^p - 1$ olevia lukuja sanotaan *Mersennen luvuiksi* ja merkitään M_p. Jos lisäksi $M_p = 2^p - 1 \in \mathbb{P}$, eli on alkuluku, niin sitä sanotaan *Mersennen alkuluvuksi*.

Huomautus **a)** Määritelmässä ei sanota, että kaikki Mersennen luvut olisivat alkulukuja!
b) Tällä hetkellä suurin löydetty (tammikuu 2016!) Mersennen alkuluku on $2^{74\,207\,281} - 1$ (yli 22 milj. numeroa), joka 49. Mersennen alkuluku.

Esimerkki: Totea, että kun $p = 2,3,5$ ja 7, niin $M_p = 2^p - 1$ on alkuluku (eli Mersennen alkuluku).
Suorat laskut antavat:

$$M_2 = 2^2 - 1 = 4 - 1 = 3, \qquad 3 \in \mathbb{P}, \qquad \text{OK}$$

$$M_3 = 2^3 - 1 = 8 - 1 = 7, \qquad 7 \in \mathbb{P}, \qquad \text{OK}$$

$$M_5 = 2^5 - 1 = 32 - 1 = 31, \qquad 31 \in \mathbb{P}, \qquad \text{OK}$$

$$M_7 = 2^7 - 1 = 128 - 1 = 127, \qquad 127 \in \mathbb{P}, \qquad \text{OK}$$

Esimerkki: Totea, että kun $p = 11$, niin $M_p = 2^p - 1$ ei ole alkuluku (mutta on silloin Mersennen luku).
Suora lasku antaa:

$$M_{11} = 2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89, \qquad \text{OK}$$

Esimerkki: Osoita, ettei alkuluku ole välttämättä Mersennen luku.
Tarkastellaan lukua 5. Nyt $5 \in \mathbb{P}$, mutta $\nexists\, p \in \mathbb{P}$, jolle $2^p - 1 = 5$.

Kaksi edellistä esimerkkiä osoittavat etteivät Mersennen lukujen joukko eikä alkulukujen joukko ole toistensa osajoukkoja.

Mielenkiintoinen alkulukuesimerkki/-tehtävä.
Esimerkki: Olkoon $n \geq 2$. Osoita, että luvut $n! + 2, n! + 3, \dots, n! + n$ ovat kaikki yhdistettyjä lukuja. Hyödynnä tulosta ja osoita, että kahden peräkkäisen alkuluvun välissä voi olla mielivaltaisen monta yhdistettyä lukua.
Annetuille luvuille saadaan

$$n! + 2 = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n + 2 = 2(1 \cdot 3 \cdot \dots \cdot n + 1)$$

$$n! + 3 = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n + 3 = 3(1 \cdot 2 \cdot \dots \cdot n + 1)$$

$$\vdots$$

$$n! + n = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n + n = n(1 \cdot 2 \cdot \dots \cdot (n-1) + 1)$$

Näin ollen ne kaikki ovat yhdistettyjä lukuja. Mutta koska luku n oli mielivaltainen niin löytyy sellaiset alkuluvut p_1 ja p_2, joille $p_1 < n$ ja $p_2 > n! + n$. Nyt alkulukujen p_1 ja p_2 välissä on mielivaltaisen monta yhdistettyä lukua.