Alkuluvut

- Ykköstä suurempi kokonaisluku on *alkuluku*, jos se ei ole jaollinen muilla positiivisilla kokonaisluvuilla kuin luvulla 1 ja itsellään.
- Muut ykköstä suuremmat kokonaisluvut ovat *yhdistettyjä lukuja*.
- Jos luvun tekijä on alkuluku, niin tätä tekijää kutsutaan *alkutekijäksi.*
  - Esimerkiksi luvun 15 alkutekijät ovat 3 ja 5.
- Alkulukuja on äärettömän monta
  - Todistus:

    Oletetaan, että alkulukuja on vain äärellinen määrä n.

    Muodostaan kaikkien alkulukujen $p_1, p_2, \dots, p_n$ avulla uusi luku

    $$P = p_1 \cdot p_2 \cdots \cdot p_n + 1$$

    Tämä luku on yhdistetty luku, koska se on kaikkia alkulukuja suurempi.

Käytetään ns. *epäsuoraa todistusta,* jossa oletetaan, että väite ei pidä paikkansa, ja osoitetaan, että tästä seuraa ristiriita.

Yhdistetyn luvun P täytyy olla jaollinen jollakin alkuluvuista p_i.
Toisaalta, jos lukua P jaetaan millä tahansa alkuluvuista p_i, jakojäännökseksi saadaan 1.
Tästä seuraa, että luku P ei ole jaollinen millään alkuluvulla, mikä on ristiriita.
Alkulukuja täytyy siis olla ääretön määrä.

- Eukleides todisti edellisen tuloksen jo. vuonna 300 eaa.
- Alkulukuihin liittyy myös useita todistamattomia olettamuksia (konjektuureja), kuuluisimpana näistä *Goldbachin konjektuuri*, jonka mukaan jokainen kahta suurempi parillinen luku voidaan esittää kahden alkuluvun summana.
- Alkulukuja voidaan etsiä esimerkiksi *Eratostheneen seulalla*:
  - Menetelmän (algoritmin) toimintaperiaate oppikirjassa s. 45.

Etsitään Eratostheneen seulan avulla kaikki sataa pienemmät alkuluvut.
Riittää testata alkuluvuilla, jotka ovat pienempiä kuin $\sqrt{100} = 10$. Nämä alkuluvut ovat $2, 3, 5$ ja 7.

1. Ensimmäinen alkuluku on 2. Poistetaan sen monikerrat.
2. Seuraavaksi poistetaan kolmen monikerrat (joita ei ole vielä poistettu).
3. Jatketaan menettelyä viiden monikerroille.
4. Vielä on löydettävä 7:n monikerrat, joita ei ole vielä poistettu:

$$7 \cdot 7 = 49$$
$$7 \cdot 11 = 77$$
$$7 \cdot 13 = 91$$

	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

Sataa pienemmät alkuluvut ovat
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89$ ja 97.

t. 256, s. 52

Oletus: p on alkuluku ja $p > 3$.

Väite: $p^2 - 1$ on jaollinen luvulla 12.

Todistus:

$p^2 - 1 = (p - 1)(p + 1)$

Koska $p > 3$ on alkuluku, niin se on pariton (eli muotoa $p = 2k + 1$).

Siis $p - 1$ ja $p + 1$ ovat parillisia (muotoa $2k$ ja $2k + 2$).

Tämän perusteella $p^2 - 1$ on kahden parillisen luvun tulo eli jaollinen neljällä.

($p^2 - 1 = 2k(2k + 2) = 4k(k + 1)$).

Osoitetaan vielä, että $p^2 - 1$ on jaollinen kolmella.

Mieti mihin oletusta $p > 3$ tarvitaan?!

Kolmesta peräkkäisestä luvusta $p - 1, p, p + 1$ yksi on jaollinen kolmella.

Tämä kolmella jaollinen luku ei voi olla p, koska p on alkuluku ja $p \neq 3$.

Siis toinen luvun $p^2 - 1 = (p + 1)(p - 1)$ tekijöistä on jaollinen kolmella.

Koska luku $p^2 - 1$ on jaollinen kolmella ja neljällä, on se jaollinen myös luvulla 12. □