



Alkulukuja ja yhdistettyjä lukuja – ylioppilastehtävä yleistyksineen

Anne-Maria Ernvall-Hytönen

Helsingin yliopisto

Tämän syksyn ylioppilaskokeessa tehtävässä 9 piti osoittaa, että on olemassa 1000 000 peräkkäistä yhdistettyä lukua, ja ohjeistukseksi annettiin hyödyntää lukua $1000\,001! + 2$:

Osoita lukua $1000\,001! + 2$ käyttämällä, että on olemassa miljoona peräkkäistä kokonaislukua, joista yksikään ei ole alkuluku.

Ratkaisu. Huomataan, että koska kertomassa $1000\,001!$ on tekijöinä kaikki positiiviset luvut $2, 3, \dots, 1000\,001$, on se jaollinen millä tahansa luvuista $2 \leq k \leq 1000\,001$. Siispä

$$k \mid (1000\,001! + k)$$

kaikilla $2 \leq k \leq 1000\,001$, eli luvut $1000\,001! + 2, 1000\,001! + 3, \dots, 1000\,001! + 1000\,001$ ovat miljoona peräkkäistä yhdistettyä lukua.

Vastaavasti voidaan itse asiassa löytää n peräkkäistä positiivista kokonaislukua, joista mikään ei ole alkuluku millä tahansa positiivisella n . Jos $n = 1$, on tilanne kovin mielenkiinnoton. Yksittäisiä yhdistettyjä lukuja kyllä löytyy. Keskitytään siis tapaukseen, jossa $n \geq 2$. Tarkastellaan lukua $(n + 1)! + k$, kun $2 \leq k \leq n + 1$. Koska luvussa $(n + 1)!$ on luku k tekijänä, on summa $(n + 1)! + k$ kahden luvulla k jaollisen luvun summana jaollinen luvulla k .

Äärettömästi alkulukuja

Ehkäpä yllättävää, mutta melkein samasta lähtökohdasta voi myös todistaa, että alkulukuja on äärettömän paljon. Klassinen todistus alkulukujen määrän äärettömyydelle on seuraava: Tehdään vastaoletus, että alkulukuja onkin vain äärellinen määrä, ja alkuluvut ovat p_1, p_2, \dots, p_k . Nyt luku $p_1 p_2 \cdots p_k + 1$ on suurempi kuin yksikään listan alkuluvuista. Lisäksi se ei voi olla jaollinen millään listan alkuluvuista, sillä luku $p_1 p_2 \cdots p_k$ on jaollinen kaikilla listan alkuluvuista, ja jos myös luku $p_1 p_2 \cdots p_k + 1$ olisi jaollinen esimerkiksi alkuluvulla p_j , niin myös näiden lukujen erotus

$$(p_1 p_2 \cdots p_k + 1) - p_1 p_2 \cdots p_k = 1$$

olisi jaollinen sillä. Ykkönen ei tunnetusti ole jaollinen millään alkuluvulla, joten tästä tulee ristiriita. Luku $p_1 p_2 \cdots p_k + 1$ ei siis ole jaollinen millään listan alkuluvuista, ja on täten joko itse alkuluku tai jaollinen jollain alkuluvulla, joka ei ole listalla. On siis todistettu, että alkulukuja on ääretön määrä.

Jos nyt oletettaisiinkin, että kaikki alkuluvut ovat korkeintaan luvun n suuruisia, niin tarkastelemalla lukua $n! + 1$ saataisiin vastaava ristiriita: Jos jokin alkuluku $p \leq n$ jakaisi luvun $n! + 1$, niin koska se jakaa myös luvun $n!$, niin sen pitäisi jakaa myös näiden lukujen erotus $n! + 1 - n! = 1$. Tämä ei ole mahdollista. Siispä joko

luku $n! + 1$ on alkuluku tai jaollinen jollain alkuluvulla, joka on suurempi kuin n .

Kumpi tahansa skenaario on itse asiassa mahdollinen. Tämä nähdään hyvin pienillä erikoistapauksilla:

$$4! + 1 = 25 = 5 \cdot 5$$

ja

$$3! + 1 = 7,$$

joka on alkuluku.

Tulosten tehokkuus

Käytännössä olemme todistaneet, että jos n on alkuluku, niin viimeistään luvun $n! + 1$ on oltava alkuluku sekä että jos halutaan löytää n peräkkäistä yhdistettyä lukua, niin viimeistään nämä löytyvät lukujen $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$ joukosta.

Ensimmäinen näistä tuloksista on auttamatta tehoton. Tämän toteamiseksi riittää vedota Bertrandin postulaattiin, jonka mukaan luvun n ja $2n$ välillä on aina alkuluku, kun $n \geq 2$. Tulos ei välttämättä ole lukijalle tuttu, mutta sille on itse asiassa olemassa (ja helposti verkosta löydettävissä) varsin alkeellinen ja lyhyt todistus, joka ensisijaisesti nojautuu lähinnä binomikertoimien suuruusluokkatarkasteluihin. Melko vähällä vaivalla (tosin huomattavasti suuremmalla kuin tämän ylioppilaskoetehtävän ratkaisun vaatimalla) saadaan valtavasti parempi tulos.

Peräkkäisten yhdistettyjen lukujen kanssa ollaan ehkäpä hieman mielekkäämmässä suuruusluokassa. Alkukulauseeseen mukaan nimittäin tiedetään, että korkeintaan luvun n suuruisia alkulukuja on suurin piirtein

$\frac{n}{\ln(n)}$ kappaletta, kun n on suuri. Tämä siis tarkoittaa sitä, että lukuun n mennessä luvuista keskimäärin joka $\ln(n)$. luku on alkuluku, eli suomeksi sanottuna, keskimäärin $\ln(n)$ lukua peräkkäin on jotain muuta kuin alkulukuja, ja sitten tulee alkuluku. Tämä ei tietenkään ole koko totuus. Ensinnäkin alkuluvut keskimäärin harventuvat. Toisekseen, alkuluvut eivät ole säännöllisesti tasaisin välein. Kuitenkin kyyhkyslakkaperiaatteen nojalla tämä tarkoittaa sitä, että noin lukuun n mennessä on ollut peräkkäiset noin $\ln n$ lukua (intuitiivisesti kyse on siitä, että jos alkuluvut ovat jossain harvakseltaan, niin jossain niitä pitää olla tiheästi, jotta niitä voi olla riittävästi annetussa joukossa), joista yksikään ei ole ollut alkuluku, eli noin lukuun e^n mennessä on ollut peräkkäiset noin n lukua, joista yksikään ei ole ollut alkuluku.

Kertoman suuruusluokka ei välttämättä ole aivan ilmeinen. Tämän arvioinnissa auttaa kuitenkin ns. Stirlingin kaava. Sen perusteella

$$(n+1)! \approx \left(\frac{n+1}{e}\right)^{n+1} \sqrt{2\pi(n+1)},$$

joka voidaan kirjoittaa eksponenttifunktion avulla muotoon

$$= e^{(n+1)\ln(n+1) - n - 1 + \frac{1}{2}\ln(2\pi(n+1))}.$$

Tämä luku (joka on listan alkupiste) on toki huomattavasti suurempi kuin e^n . Silti heitto on tässä paljon järkevämpi. Aiemmassa mentiin lineaarisesta kertoman suuruusluokkaan, nyt *vain* eksponentiaalisesta kertoman suuruusluokkaan. Voitto tämäkin.