Luku $n^{n^{n^n}} - n^{n^n}$, $n \geq 3$, on jaollinen luvulla 17

Johdanto

Tutkimme otsikossa mainitun potenssitornien erotuksen jaollisuutta.

Todistuksen kantava ajatus on potenssien jakojäännösten jakso. Esimerkki tästä on luvun kaksi potenssien viimeiset numerot: 2, 4, 8, 1**6**, 3**2**, 6**4**, 12**8**, 25**6**. Jakson pituus on neljä, eli lukujen 2^n ja 2^{n+4} viimeinen numero on sama.

Todistus koostuu kolmesta osasta. Ensin osoitamme, että $n^n - n$ on jaollinen neljällä. Sitten päättelemme tästä, että $n^{n^n} - n^n$ on jaollinen luvulla 16, josta lopuksi päättelemme alkuperäisen väitteen. Käymme vaiheet läpi käänteisessä järjestyksessä, kuin purkaen potenssitornia pala kerrallaan.

Merkinnät ja määritelmät

Merkintä $[a]_b$ tarkoittaa jakolaskun a/b jäännöstä. Esimerkiksi $[18]_5 = 3$, ja $[a]_{10}$ on luvun a viimeinen numero normaalissa kymmenjärjestelmässä. Selvästi $[a]_b = 0$ merkitsee, että b jakaa luvun a tasan.[1]

Luvut ovat *keskenään jaottomia*, ellei niillä ole yhtä suurempaa yhteistä jakajaa. Esimerkiksi 15 ja 21 eivät ole keskenään jaottomia, koska molemmat ovat kolmella jaollisia.

[1] Lähdeteoksissa jakojäännöksen sijaan käytetään kongruenssin käsitettä. Näiden yhteydestä ks. esim. [1, s. 18-22]

Ensimmäinen vaihe: Fermat'n pieni lause

Fermat'n pienen lauseen mukaan $[a^p]_p = [a]_p$ aina, kun p on alkuluku [2, s. 99]. Koska 17 on alkuluku, pätee $[a^{17}]_{17} = [a]_{17}$ eli $[a^{16+1}]_{17} = [a^1]_{17}$.

Tiedetään, että $[ab]_c = [[a]_c[b]_c]_c$. [1, s. 20 seuraus] Tämä tarkoittaa, että voimme laskea tulon jakojäännöksen kertomalla jäännökset: Esimerkiksi tulon $53 \cdot 76$ viimeinen numero on sama kuin tulon $3 \cdot 6$ viimeinen numero.

Näistä päättelemme $[a^{16+b}]_{17} = [[a^{17}]_{17}[a^{b-1}]_{17}]_{17} = [[a^1]_{17}[a^{b-1}]_{17}]_{17} = [a^b]_{17}$ ja laajemmin $[a^{16n+b}]_{17} = [a^b]_{17}$, kun $n \in \mathbb{N}$. Yleisemmin kun p on alkuluku, toistavat luvut $[a^1]_p$, $[a^2]_p$, $[a^3]_p$, $\ldots$ itseään jaksolla, jonka pituus on $p - 1$.

Osoitamme seuraavaksi, että haettu jakson pituus on 16 eli $[n^{n^n} - n^n]_{16} = 0$.

Toinen vaihe: Carmichaelin funktio

Carmichaelin funktio $\lambda(a)$ tarkoittaa pienintä lukua b, jolla pätee $[a^b]_b = 1$ aina, kun a ja b ovat keskenään jaottomia [4, s. 13-14].

Myös Carmichaelin funktio on helpoin ymmärtää jaksona. Kun esimerkiksi 100 ja 27 on keskenään jaottomia, toistavat lukujen 27^1, 27^2, $\ldots$ viimeiset kaksi numeroa itseään jaksolla, jonka pituus on enintään $\lambda(100)$. Sama ei välttämättä päde lukuihin 28^1, 28^2, $\ldots$, koska 100 ja 28 ovat molemmat jaollisia luvulla 4, eivätkä siis keskenään jaottomia.

Jos n on parillinen ja kahta suurempi, niin selvästi sekä n^{n^n} että n^n ovat jaollisia luvulla 16, jolloin niiden erotuskin on.

Koska $16 = 2^4$, ovat 16 ja n keskenään jaottomia, kun n on pariton. Tiedämme, että $\lambda(16) = 4$.[3]

Osoitamme lopuksi, että $n^n - n$ on jaollinen neljällä, kun n on pariton.

Kolmas vaihe: $n^n - n$ on jaollinen neljällä

Jos n on pariton, se on joko muotoa $4m+1$ tai $4m+3$, jossa $m \in \mathbb{N}$.

Selvästi $[4m+3]_4 = 3$. Edellä totesimme, että tulon jakojäännös lasketaan kertomalla tekijöiden jakojäänökset ja ottamalla tuloksesta vielä kerran jakojäännös. Siis $[(4m+3)(4m+3)]_4 = [3 \cdot 3]_4 = 1$. Havaitsemme, että luvut $[(4m+3)^1]_4$, $[(4m+3)^2]_4$, $[(4m+3)^3]_4$, $\ldots$ muodostavat itseään toistavan sarjan 3,1,3,1,... Tässä sarjassa siis $[(4m+3)^a]_4 = 3$ aina, kun a on pariton.

Siis edellisen perusteella $[(4m+3)^{4m+3}]_4 = 3$, ja kun tästä vähennetään $[4m+3]_4 = 3$, on tulos neljällä jaollinen.

Jos n on muotoa $4m+1$, pääsemme vielä helpommalla. Nyt $[(4m+1)^n]_4 = [1^n]_4 = 1$, ja tietysti tällöin $[(4m+1)^{(4m+1)} - (4m+1)]_4 = 0$.

Viitteet

[1] Haukkanen, Pentti. *Algebra I, kevät 2004* http://mtl.uta.fi/Opetus/Algebra/algI04.pdf, viitattu 29.1.2012.

[2] Judson, Thomas W. *Abstract Algebra: Theory and Applications.* http://abstract.ups.edu, viitattu 28.1.2012.

[3] OEIS-A002322. http://oeis.org/A002322, viitattu 28.1.2012.

[4] Ribenboim, Paolo. *My numbers, My friends: Popular Lectures on Number Theory.* Springer, 2000.