Kodutöö nr. 6 esimene tärnülesanne

Joosep Näks

Väidan, et antud jadas leidub iga mooduli n jaoks mingi liige a_k, millest alates on kõik järgnevad liikmed mooduli n järgi samad, ehk periood on 1. Võtan suvalise liikme a_t, $t \geq k$ mooduli n järgi.

Kui n on paarisarv, saab seda avaldada kujul $n = 2^p \cdot b$, kus b on paaritu ehk $(2^p, b) = 1$, seega $\mathbb{Z}_n$ ja $\mathbb{Z}_{2^p} \times \mathbb{Z}_b$ on isomorfsed, ehk saab vaadata eraldi liikme jääki 2^p ja b järgi. Liige a_k on valitud sobivalt, et $t \geq k > p$ ehk $a_t = 2^{(2^{2^{\cdot^{\cdot}}})} = (2^p)^q \equiv 0 \pmod{2^p}$. Mooduli b jaoks saab kasutada Euleri teoreemi, kuna $(2, b) = 1$ ehk $2^{\varphi(b)} \equiv 1 \pmod{b}$. Tähistan a_t astendaja: $a_t = 2^x$ ning jagan seda arvuga $\varphi(b)$ jäägiga: $x = q\varphi(b) + r$. Nüüd saab vaadeldava liikme avaldada: $a_t = 2^x = (2^{\varphi(b)})^q \cdot 2^r \equiv 2^r \pmod{b}$. Ehk kokkuvõttes a_t vastab $\mathbb{Z}_{2^p} \times \mathbb{Z}_b$ liikmele $(0, 2^r)$, $r < \varphi(b)$, $r \equiv x \pmod{\varphi(b)}$.

Kui n on paaritu, saab kohe kasutada Euleri teoreemi ning analoogselt saab, et $a_t \equiv 2^r \pmod{n}$, kus $r < \varphi(n)$ ja $r \equiv x \pmod{\varphi(n)}$, kus $a_t = 2^x$.

Nüüd saab seda korrata, võttes a_t asemele x ning n asemele vastavalt $\varphi(b)$ või $\varphi(n)$, olenevalt kas n oli paaris või paaritu. Seda saab nii kaua korrata, kuni moodul, mille järgi jääki võetakse (ehk algselt n, hiljem $\varphi(n)$ või $\varphi(b)$ ning järgmisel tasemel $\varphi(\varphi(n))$ või midagi sarnast jne) on mõni 2 aste 2^w. Sel juhul nagu varem näidatud, kui on a_k sobivalt valitud, on alles jäänud astendajate jääk 2^w järgi 0.

Moodul jõuab kindlasti lõpliku koguse sammude jooksul mõne 2 astmeni, kuna alati kehtib $\varphi(n) < n$. Seda seetõttu, et $\varphi(n)$ on arvust n väiksemate ja võrdsete arvude kogus, mille suurim ühistegur arvuga n on 1, kuid arvust n väiksemaid arve on $n - 1$ tükki ning $(n, n) = 1$ kehtib vaid juhul kui $n = 1$ ehk kui $n > 1$ siis $\varphi(n) < n$. Seega kui vahepeal mõne muu 2 astmeni ei jõua, tuleb lõpuks 2 ise vastu. Arvust 2 ei saa mööda minna kuna $\varphi(n)$ ei saa kunagi olla väiksem kui 1, kuna 1 on alati arvu n jagaja ehk $\varphi(n)$ on vähemalt 1, ja $\varphi(n)$ väärtus saab olla 1 vaid juhul, kui $n = 2$, kuna kui n on mõni suurem arv, on $(1, n) = 1$ ja $(n, n-1) = 1$, sest kui kehtiks $d|n$ ja $d|n-1$, kehtiks ka $d|n-(n-1) = 1$, kuid ükski algarv ei jaga arvu 1.

Seega kokkuvõttes kui a_p on valitud piisavalt kaugele, on kõik järgnevad liikmed sellega võrdsed mooduli n järgi.