Lagrangen lauseen sovellus lukuteoriaan

Palautetaan mieleen alkuluokkien modulo n joukko

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n \mid \text{syt}(a,n) = 1\}.$$

Esimerkkejä ryhmästä, 2 -sivulla todetaan, että tämä joukko muodostaa ryhmän jäännösluokkien kertolaskun $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ suhteen. Ryhmän neutraalialkio on $\overline{1}$.

Ryhmän $(\mathbb{Z}_n^*, \cdot)$ kertaluvulle on määritelty lukuteoriassa oma funktio.

Määritelmä. *Eulerin φ-funktio,* $\varphi(n)$, on niiden kokonaislukujen m lukumäärä, joille $\text{syt}(m,n) = 1$ ja $1 \leq m \leq n$.

Siis $\sharp\mathbb{Z}_n^* = \varphi(n)$. Jos $n = p$ on alkuluku, niin $\varphi(p) = p - 1$. Esimerkkinä todetaan, että $\varphi(10) = 4$, sillä luvut $1,3,7,9$ ovat suhteellisia alkulukuja luvun 10 kanssa ja nämä ovat ainoita, jotka ovat positiivisia ja enintään 10.

Lagrangen lauseen avulla voidaan todistaa seuraava lukuteoreettisesti tärkeä **Eulerin lause.**

Lause. [Eulerin lause] Jos $\text{syt}(a,n) = 1$, niin

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Todistus. Koska $\mathbb{Z}_n^*$ muodostaa ryhmän, jonka kertaluku on $\varphi(n)$ niin Lagrangen lauseen toisen seurauslauseen mukaan kaikilla $\overline{a} \in \mathbb{Z}_n^*$ on $\overline{a}^{\sharp\mathbb{Z}_n^*} = \overline{a}^{\varphi(n)} = \overline{1}$. Kirjoittamalla tämä kongruenssin muotoon saadaan väite. □

Eulerin lauseen erikoistapauksena saadaan **Fermat'n pikkulause.**

Lause. [Fermat'n pikkulause] Olkoon p alkuluku. Jos $p \nmid a$, niin

$$a^{p-1} \equiv 1 \pmod{p}.$$

Kaikille kokonaisluvuille on voimassa

$$a^p \equiv a \pmod{p}.$$

Todistus. Jos $p \nmid a$ eli $\text{syt}(a,p) = 1$, niin ensimmäinen väite seuraa Eulerin lauseesta, sillä $\varphi(p) = p - 1$. Toisen väitteen todistamiseksi huomataan ensin, että jos $p \nmid a$, niin $a \cdot a^{p-1} \equiv a \pmod{p}$ eli $a^p \equiv a \pmod{p}$. Jos $p \mid a$, niin $a \equiv 0 \pmod{p}$, joten myös $a^p \equiv 0 \pmod{p}$ eli $a^p \equiv a \pmod{p}$. □

Linkit:
Lagrangen lause
Esimerkkejä ryhmistä 2