Liite 3: Indeksien käyttöä

Huomautus 0.1. Selvästi 5 on primitiivinen juuri (mod 14). Voidaan todistaa, että *primitiivinen juuri (mod n) on olemassa silloin ja vain silloin kun n = 1, 2, 4, p^t, tai $2p^t$*, missä p on pariton alkuluku ja t luonnollinen luku. Tapaukset $n = 1,\ 2$ tai 4 ovat triviaaleja, ja näiden lisäksi tulemme osoittamaan seuraavassa pykälässä, että jokaista paritonta alkulukua kohti on olemassa primitiivinen juuri. Yleinen tapaus käsitellään jatkokurssissa.

Esimerkki 0.2. Seuraavissa taulukoissa on alkuluokkien kertaluvut (mod 11) ja (mod 21). Siitä näkyy, että $2, 6, 7$ ja 8 ovat primitiivisiä juuria (mod 11), kun taas primitiivisiä juuria (mod 21) ei ole olemassa.

a	1	2	3	4	5	6	7	8	9	10
ord_{11}(a)	1	10	5	5	5	10	10	10	5	2

a	1	2	4	5	8	10	11	13	16	17	19	20
ord_{21}(a)	1	6	3	6	2	6	6	2	3	6	6	2

Liitteenä jaetussa taulukossa on lueteltu lukua 1000 pienempiä alkulukuja vastaavat pienimmät positiiviset primitiiviset juuret. (Demojen 6 yhteydessä on hieman toiselainen taulukko primitiivisiä juuria ja indeksejä - Gaussin alkuperäinen!)

Valitaan jokin primitiivinen juuri r (mod p), joka on seuraavassa tarkastelussa kiinteä. Silloin r:n potenssit $r^0 = 1,\ r, \ldots, r^{p-2}$ muodostavat s.j.s:n (mod p) eli käyvät luvut 1, 2, ..., p-1 (mod p) jossakin järjestyksessä. Jokaista lukua kohti määräytyy siis tietty eksponentti, jolla on lukuteoriassa sama rooli kuin analyysissa on luvun logaritmilla.

Määritelmä 0.3. Olkoon p alkuluku, r primitiivinen juuri (mod p) ja a p:llä jaoton luku. Lukua i, joka täyttää ehdot

$$r^i \equiv a \pmod{p}, \qquad 0 \le i \le p-2, \tag{0.1}$$

sanotaan *a:n indeksiksi* (mod p) *kantaluvun* r suhteen. Merkitään $i = \mathrm{ind}_r a$.

Käytettäessä indeksejä esimerkiksi kongruenssien ratkaisemiseen tarvitaan *indeksitauluja*, joissa on taulukoitu eri moduleille indeksien arvoja mahdollisimman pienen primitiivisen juuren suhteen. Monisteen lopussa liitteessä 2 on indeksitaulut moduleille < 50.

Lause 0.4. *Olkoon r primitiivinen juuri* (mod p) *ja $p \nmid a$, $p \nmid b$. Silloin*

$$ind_r(ab) \equiv ind_r a + ind_r b \pmod{p-1}, \tag{0.2}$$

ja

$$ind_r a^n \equiv n \cdot ind_r a \pmod{p-1} \qquad (n = 1, 2, \ldots). \tag{0.3}$$

Todistus. Indeksin määritelmän mukaan on

$$r^{\mathrm{ind}_r(ab)} \equiv ab \pmod{p}$$

ja samoin

$$r^{\mathrm{ind}_r a} \equiv a \pmod{p},$$

$$r^{\mathrm{ind}_r b} \equiv b \pmod{p}.$$

Kertomalla jälkimmäiset kongruenssit keskenään ja vertaamalla tulosta ensimmäiseen nähdään, että

$$r^{\mathrm{ind}_r(ab)} \equiv r^{\mathrm{ind}_r a + \mathrm{ind}_r b} \pmod{p}.$$

Tästä seuraa väite (1.2) lauseen **??** (2) nojalla. □

Induktiolla voidaan (1.2) yleistää tapaukseen, jossa tulon tekijöitä on useampia kuin kaksi. Silloin (1.3) on tämän yleisemmän kaavan erikoistapaus.
Esimerkkejä indeksitaulujen käytöstä.
1) Ratkaistaan lineaarinen kongruenssi $15x \equiv 7 \pmod{11}$. Tässä 15 voidaan korvata sen kanssa kongruentilla luvulla 4. Primitiiviseksi juureksi (mod 11) voidaan valita $r = 2$. Jätetään seuraavassa indeksin alaindeksi yksinkertaisuuden vuoksi merkitsemättä. Siirtymällä ratkaistavassa kongruenssissa indekseihin saadaan $\mathrm{ind}\, 4 + \mathrm{ind}\, x \equiv \mathrm{ind}\, 7 \pmod{10}$. Indeksitaulujen mukaan on $\mathrm{ind}\, 4 = 2$ ja $\mathrm{ind}\, 7 = 7$. Täten $\mathrm{ind}\, x = 5$ ja $x \equiv 10 \pmod{11}$.

2) Tutkitaan vastaavasti toisen asteen kongruenssia $x^2 \equiv 5 \pmod{11}$. Indeksimuodossa tämä on $2\,\mathrm{ind}\, x \equiv 4 \pmod{10}$ eli $\mathrm{ind}\, x \equiv 2 \pmod{5}$. Modulo 10 on siis kaksi ratkaisua: $\mathrm{ind}\, x = 2$ tai 7. Tauluista nähdään, että $x_1 \equiv 4 \pmod{11}$ ja $x_2 \equiv 7 \pmod{11}$ ovat ratkaistavan kongruenssin juuret.

3) Indeksit soveltuvat myös ”eksponentiaalisiin” kongruensseihin, joissa tuntematon esiintyy eksponentissa. Tällainen on esimerkiksi $8^x \equiv 9 \pmod{11}$. Otetaan indeksit puolittain: $x\,\mathrm{ind}\, 8 \equiv \mathrm{ind}\, 9 \pmod{10}$ eli $3x \equiv 6 \pmod{10}$. Tämän lineaarisen kongruenssin ratkaisu on $x \equiv 2 \pmod{10}$. Huomattakoon, että ratkaisussa on *eri* moduli kuin alkuperäisessä kongruenssissa. Tämä johtuu siitä, että kyseessä ei ollut algebrallinen kongruenssi.