Lukuteorian alkeet
Neljänsien harjoitusten ratkaisuita

1. Etsi modulo 30 jokin redusoitu jäännössysteemi.

Ratkaisu. Kuten luennoissa sanotaan, riittää valita jokin täydellinen jäännössysteemi modulo 30, vaikkapa 0, 1, 2, 3, ..., 29, ja poistaa siitä ne luvut, joilla on yhteinen tekijä luvun 30 kanssa. Koska $30 = 2 \cdot 3 \cdot 5$ pitää siis poistaa parilliset luvut, kolmella jaolliset luvut ja viidellä jaolliset luvut. Jäljelle jäävät

$$1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23 \text{ ja } 29.$$

2. Määritä primitiiviset juuret modulo 11 sekä redusoidun jäännössysteemin kaikkien alkioiden kertaluvut modulo 11.

Ratkaisu. Tarkastellaan ensin luvun 2 kertalukua modulo 11. Lemman 34 nojalla $\operatorname{ord}_{11} 2 \mid (11-1) = 10$, eli $\operatorname{ord}_{11} 2$ on jokin luvuista 1, 2, 5 ja 10. Selvästi $\operatorname{ord}_{11} 2 \neq 1$, ja koska lisäksi

$$2^2 \equiv 4 \not\equiv 1 \pmod{11} \quad \text{ja} \quad 2^5 \equiv 32 \equiv 10 \not\equiv 1 \pmod{11},$$

on oltava $\operatorname{ord}_{11} 2 = 10$. Erityisesti luku 2 on primitiivinen juuri modulo 11.

Tiedämme nyt, että luvun 2 potenssit $2, 2^2, 2^3, \ldots, 2^{10}$ muodostavat redusoidun jäännössysteemin modulo 11, ja toisaalta lemman 36 nojalla potenssin 2^α (missä $\alpha \in \mathbb{Z}_+$) kertaluku on $\frac{10}{(\alpha,10)}$. Nyt laskemalla luvun 2 potenssit saadaan redusoitu jäännössysteemi modulo 11, joka sisältää luvut

$$\begin{aligned} 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 5, \quad 2^5 \equiv 10, \\ 2^6 \equiv 9, \quad 2^7 \equiv 7, \quad 2^8 \equiv 3, \quad 2^9 \equiv 6, \quad 2^{10} \equiv 1, \end{aligned}$$

ja näiden asteet ovat

$$\begin{aligned} 10, \quad \tfrac{10}{2} = 5, \quad 10, \quad \tfrac{10}{2} = 5, \quad \tfrac{10}{5} = 2, \\ \tfrac{10}{2} = 5, \quad 10, \quad \tfrac{10}{2} = 5, \quad 10, \quad 1. \end{aligned}$$

Siistimpänä taulukkona:

n	1	2	3	4	5	6	7	8	9	10
$\operatorname{ord}_{11} n$	1	10	5	5	5	10	10	10	5	2

Todetaan lopuksi, että primitiiviset juuret modulo 11 ovat 2, 6, 7 ja 8.

3. Etsi polynomin $x^2 - x$ juuret modulossa 5. Etsi vielä tämän polynomin juuret modulossa 6, ja selitä, miksi tämä ei ole ristiriidassa Lagrangen lauseen kanssa.

Ratkaisu. Luku viisi on alkuluku, ja Lagrangen lauseen nojalla tällä polynomilla on enintään kaksi juurta modulo 5. Koska $0^0 - 0 \equiv 0$ ja $1^1 - 1 \equiv 0 \pmod 5$, ovat 0 ja 1 polynomin ainoat juuret modulo 5.

Modulo 6 polynomin juuret saadaan käymällä läpi sen arvot täydellisen jäännössysteemin luvuilla:

$$0^0 - 0 \equiv 0, \quad 1^1 - 1 \equiv 0, \quad 2^2 - 2 \equiv 2, \quad 3^2 - 3 \equiv 0, \quad 4^2 - 4 \equiv 0, \quad 5^2 - 5 \equiv 2.$$

Juuret modulo 6 ovat siis 0, 1, 3 ja 4. Se, että näitä juuria on neljä vaikka polynomin aste on vain kaksi, ei ole ristiriidassa Lagrangen lauseen kanssa koska luku 6 ei ole alkuluku.

4. Todista Wilsonin lause, eli mikäli p on alkuluku, niin

$$(p-1)! \equiv -1 \pmod{p}.$$

Ratkaisu. Tulos on helppo tarkistaa tapauksessa $p = 2$; onhan $(2-1)! = 1 \equiv -1 \pmod 2$. Oletetaan siis, että $p \neq 2$.

Olkoon g jokin primitiivinen juuri modulo p. Tällöin lauseen 28 nojalla kaikki kertoman $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ tulontekijät voi kirjoittaa jossakin järjestyksessä potensseina g, g^2, g^3, $\ldots$, g^{p-1} modulo p. Täten

$$(p-1)! \equiv 1 \cdot g \cdot g^2 \cdot g^3 \cdot \ldots \cdot g^{p-1} \equiv g^{p(p-1)/2} \equiv (g^p)^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p},$$

missä viimeisessä kongruenssissa käytettiin Fermat'n pientä lausetta.

Fermat'n pienen lauseen nojalla

$$\left(g^{(p-1)/2}\right)^2 \equiv g^{p-1} \equiv 1 \pmod{p},$$

eli $g^{(p-1)/2} \equiv \pm 1 \pmod p$, ja koska g on primitiivinen juuri, on $g^{(p-1)/2} \not\equiv 1 \pmod p$. Jäljelle jää siis vain vaihtoehto $g^{(p-1)/2} \equiv -1 \pmod p$.

5. Todista Wilsonin lauseen toinen suunta, eli mikäli

$$(n-1)! \equiv -1 \pmod{n},$$

on n alkuluku.

Ratkaisu. Teemme vastaoletuksen: olkoon n yhdistetty luku, jolle $(n-1)! \equiv -1 \pmod n$. Jos $n = 4$, niin $(4-1)! = 3! = 6 \equiv 2 \not\equiv -1 \pmod 4$. Jos n on parittoman alkuluvun p neliö, niin kertomassa $1 \cdot 2 \cdot \ldots \cdot (n-1)$ esiintyvät ainakin luvut p ja $2p$, ja siis $(n-1)! \equiv 0 \not\equiv -1 \pmod n$.

Lopuksi, jos n on yhdistetty luku, joka ei ole alkuluvun neliö, niin valitsemalla alkulukutekijä $p \mid n$, todetaan, että kertomassa $1 \cdot 2 \cdot \ldots \cdot (n-1)$ esiintyvät luvut p ja $\frac{n}{p}$, ja täten jälleen $(n-1)! \equiv 0 \not\equiv -1 \pmod n$.

6. Osoita, että muotoa $4k+3$ olevia alkulukuja on äärettömän paljon. (Vihje: Mieti, miten todistettiin, että alkulukuja on äärettöman paljon. Voisiko tätä todistusta jotenkin muokata?)

Ratkaisu. Tehdään se vastaoletus, että muotoa $4k+3$ olevia alkulukuja on vain äärellinen määrä. Olkoot kyseiset alkuluvut q_1, q_2, $\ldots$, q_n. (Tämä lista ei ole tyhjä, koska tunnetusti luku 3 kuuluu siihen.) Todetaan, että kaikki muut parittomat alkuluvut ovat kongruentteja luvun 1 kanssa modulo 4.

Tarkastellaan lukua

$$N = 4q_1q_2 \cdots q_n - 1.$$

Kirjoitetaan luku N alkulukujen tulona $p_1p_2 \cdots p_m$. Koska luku N on pariton, on sen jokainen alkulukutekijä p_ℓ pariton, eli $p_\ell \equiv 1$ tai $p_\ell \equiv -1 \pmod 4$. Koska luku N on yhteistekijätön kaikkien luvuista q_1, $\ldots$, q_n kanssa, on oltava $p_1 \equiv p_2 \equiv \ldots \equiv p_m \equiv 1 \pmod 4$. Mutta nyt

$$-1 \equiv N \equiv p_1p_2 \cdots p_m \equiv 1 \cdot 1 \cdot \ldots \cdot 1 \equiv 1 \pmod{4},$$

mikä on mahdotonta.