Lukuteorian alkeet
Kolmansien harjoitusten ratkaisuita

1. Määritä luvun 5 käänteisluku modulo 9, eli etsi sellainen x, että $5x \equiv 1 \pmod 9$.

Ratkaisu. Arvaamalla, käymällä läpi eri vaihtoehtoja tai soveltamalla Eukleideen algoritmia yhtälöön $5x - 9y = 1$ löydämme erikoisratkaisun $x = 2$. Kongruenssista $5x \equiv 1 \pmod 9$ seuraa, että

$$x \equiv 10x = 2 \cdot 5x \equiv 2 \cdot 1 \equiv 2 \pmod 9,$$

eli jokaiselle ratkaisulle x pätee $x \equiv 2 \pmod 9$. Toisaalta, jos kokonaisluvulle x pätee $x \equiv 2 \pmod 9$, niin varmasti $5x \equiv 5 \cdot 2 \equiv 1 \pmod 9$.

2. Ratkaise kongruenssiyhtälö

$$5x + 3 \equiv 4 \pmod 7$$

Ratkaisu. Kongruenssille $5x \equiv 1 \pmod 7$ saadaan arvaamalla, käymälle läpi eri vaihtoehtoja, tai soveltamalla Eukleideen algoritmia yhtälöön $5x - 7y = 1$, erityisratkaisu $x = 3$.

Jos kokonaisluku x on kongruenssin ratkaisu, niin

$$x \equiv 15x \equiv 3 \cdot 5x \equiv 3 \cdot 1 \equiv 3 \pmod 7,$$

eli jokaiselle ratkaisulle x pätee $x \equiv 3 \pmod 7$. Toisaalta, jos $x \equiv 3 \pmod 7$, niin varmasti $5x \equiv 5 \cdot 3 \equiv 15 \equiv 1 \pmod 7$.

3. Osoita, että $17 \mid 11^{1600} - 1$.

Ratkaisu. Luku 17 on alkuluku, joka ei jaa lukua 11, ja Fermat'n pienen lauseen nojalla siis

$$11^{1600} = \left(11^{16}\right)^{100} \equiv 1^{100} \equiv 1 \pmod{17}.$$

4. Ratkaise kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 3 \pmod 9 \\ x \equiv 7 \pmod 8. \end{cases}$$

Ratkaisu. Olkoon x ratkaisu. Ensimmäisen kongruenssin nojalla $x = 3 + 9k$, jollakin kokonaisluvulla k. Sijoittamalla tämä toiseen kongruenssiin se saa muodon

$$3 + 9k \equiv 7 \pmod 8, \quad \text{eli} \quad k \equiv 4 \pmod 8.$$

On siis oltava $k = 4 + 8\ell$ jollakin kokonaisluvulla ℓ, ja alkuperäisen ratkaisun x on siis oltava muotoa

$$x = 3 + 9k = 3 + 9\,(4 + 8\ell) = 3 + 9 \cdot 4 + 9 \cdot 8\ell = 39 + 72\ell \equiv 39 \pmod{72}.$$

Toisaalta, jos $x \equiv 39 \pmod{72}$, niin $x = 39 + 72\ell$ jollakin kokonaisluvulla ℓ ja

$$x \equiv 3 + 0 \equiv 3 \pmod 9, \quad \text{ja} \quad x \equiv 7 + 0 \equiv 7 \pmod 8.$$

5. Monisteessa määritellään Eulerin φ-funktio, ja väitetään, että jos $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (luvun n alkutekijähajotelma), niin

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1} (p_j - 1) .$$

Todista väite. (Vihje: Todista väite ensin alkulukupotensseille, ja tee sen jälkeen induktio erisuurten alkutekijöiden lukumäärän suhteen.)

Ratkaisu. Olkoon ensin p alkuluku ja $\alpha \in \mathbb{Z}_+$. Kokonaisluku n on yhteistekijätön alkulukupotenssin p^α kanssa täsmälleen silloin kun luku n ei ole jaollinen alkuluvulla p. Luvuista $1, 2, \ldots, p^\alpha$ alkuluvulla p jaollisia ovat $p, 2p, \ldots, p^{\alpha-1} \cdot p$, joita on $p^{\alpha-1}$ kappaletta. Loput ovat yhteistekijättömiä luvun p^α kanssa, ja täten

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1} (p - 1) .$$

Useamman alkuluvun potenssille todistettava kaava seuraa induktiolla alla todistetusta lemmasta: Jos kaava tiedetään todeksi jollakin $k \in \mathbb{Z}_+$, ja tarkastellaan lukua, jonka alkutekijähajotelma on $p_1^{\alpha_1} \cdots p_{k+1}^{\alpha_{k+1}}$ joillakin eri alkuluvuilla $p_1, \ldots, p_{k+1}$ ja joillakin positiivisilla kokonaisluvuilla $\alpha_1, \ldots, \alpha_{k+1}$, niin lemman ja induktio-oletuksen nojalla

$$\begin{aligned} \varphi\big(p_1^{\alpha_1} \cdots p_k^{\alpha_k} \cdot p_{k+1}^{\alpha_{k+1}}\big) &= \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k})\, \varphi\big(p_{k+1}^{\alpha_{k+1}}\big) \\ &= \prod_{j=1}^{k} p_j^{\alpha_j - 1} (p_j - 1) \cdot p_{k+1}^{\alpha_{k+1} - 1} (p_{k+1} - 1) = \prod_{j=1}^{k+1} p_j^{\alpha_j - 1} (p_j - 1) , \end{aligned}$$

kuten pitääkin.

Lemma. *Jos m ja n ovat keskenään yhteistekijättömiä positiivisia kokonaislukuja, niin*

$$\varphi(mn) = \varphi(m)\, \varphi(n) .$$

Todistamme tämän kirjoittamalla luvut $1, 2, \ldots, mn$ seuraavanlaisen taulukon muotoon:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \cdots & 3n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (m-1)\,n+1 & (m-1)\,n+2 & (m-1)\,n+3 & \cdots & mn \end{array}$$

Tässä taulukossa on funktion $\varphi(\cdot)$ määritelmän nojalla täsmälleen $\varphi(mn)$ lukua, jotka ovat yhteistekijättömiä luvun mn kanssa. Toisaalta, koska luku on yhteistekijätön luvun mn kanssa jos ja vain jos se on yhteistekijätön molempien luvuista m ja n kanssa erikseen, voimme laskea kyseiset $\varphi(mn)$ lukua toisellakin tavalla.

Koska taulukossa yhdessä sarakkeessa olevat luvut ovat keskenään kongruentteja modulo n, taulukossa olevat luvun n kanssa yhteistekijättömät luvut muodostavat täsmälleen $\varphi(n)$ kokonaista saraketta. Edellä mainitut $\varphi(mn)$ lukua sijaitsevat siis näissä sarakkeissa.

Tarkastellaan sitten yhtä näistä $\varphi(n)$ sarakkeesta. Koska $(m,n) = 1$, sen luvut ovat m keskenään epäkongruenttia lukua modulo m (vertaa esimerkiksi luentojen lauseen 22 todistukseen). Siis kyseisen sarakkeen luvuista täsmälleen $\varphi(m)$ ovat yhteistekijättömiä, paitsi luvun n kanssa, myös luvun m kanssa, ja olemme valmiit.

6. Viimeistele kiinalaisen jäännöslauseen todistus, eli olkoon $M = m_1 m_2 \cdots m_k$, missä luvut m_j ovat pareittain yhteistekijättömiä. Määritellään $M_j = \frac{M}{m_j}$ ja olkoon y_j luvun M_k käänteisluku modulo m_j, eli $M_j y_j \equiv 1 \pmod{m_j}$. Todista, että

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k \pmod{M}$$

toteuttaa yhtälöryhmän

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Ratkaisu. Olkoon $j \in \{1, 2, \ldots, k\}$. Luku m_j esiintyy tulontekijänä luvussa

$$a_\ell M_\ell y_\ell = a_\ell m_1 m_2 \cdots m_{\ell-1} m_{\ell+1} \cdots m_k y_\ell,$$

kun $\ell \in \{1, 2, \ldots, k\}$ ja $\ell \neq j$, ja siis $a_\ell M_\ell y_\ell \equiv 0 \pmod{m_j}$. Koska lisäksi $a_j M_j y_j \equiv a_j \cdot 1 \equiv a_j \pmod{m_j}$, on oltava

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + \ldots + a_{j-1} M_{j-1} y_{j-1} + a_j M_j y_j + a_{j+1} M_{j+1} y_{j+1} + \ldots + a_k M_k y_k \\ &\equiv 0 + \ldots + 0 + a_j + 0 + \ldots + 0 \equiv a_j \pmod{m_j}. \end{aligned}$$