LUKUTEORIAN ALKEET

3. LASKUHARJOITUKSET

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

(2) Ratkaise kongruenssiyhtälö

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

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

(4) Ratkaise kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 3 \ (\mathrm{mod} 9) \\ x \equiv 7 \pmod 8. \end{cases}$$

(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.)

(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

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

toteuttaa yhtälöryhmän

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