Lukuteoria 1
Harjoitus 7, 28.2.2018
Ratkaisuehdotuksia

1. Ratkaise kongruenssiyhtälö $17x \equiv 100 \pmod{67}$.
Opastus: Seuraukset 4.4.9 ja 4.4.10.

Ratkaisu. Huomataan, että 67 on alkuluku. Seurauksen 4.4.9 nojalla kongruenssiluokalla $[17]_{67}$ on oltava käänteisalkio, ja kokeilemalla huomataan, että

$$[17]_{67} \cdot [4]_{67} = [68]_{67} = [1]_{67}.$$

Seurauksen 4.4.10 nojalla tehtävän kongruenssiyhtälöllä on yksikäsitteinen ratkaisu (kongruenssiluokkana)

$$x \equiv 400 \equiv 65 \pmod{67}.$$

Siis yhtälön ratkaisu on kongruenssiluokka $[65]_{67}$.

2. Osoita Fermat'n pienen lauseen avulla, että $3^{31} \equiv 3 \pmod{7}$.

Ratkaisu. Huomataan, että 7 on alkuluku. Koska $7 \nmid 3$, on $7 \nmid 3^j$ kaikilla $j \in \mathbb{N}$, joten molemmat Fermat'n pienen lauseen versiot ovat käytössä. Käyttämällä seurauksen versiota saadaan

$$3^{31} \equiv 3^{5 \cdot 6+1} \equiv (3^5)^{7-1} \cdot 3 \equiv 3 \pmod{7}.$$

3. Osoita Fermat'n pienen lauseen avulla, että $12^{772} \equiv 2 \pmod{71}$.

Ratkaisu. Huomataan, että 71 on alkuluku ja $71 \nmid 772$, joten molemmat Fermat'n pienen lauseen versiot ovat käytössä. Saadaan

$$12^{772} \equiv (12^{10})^{71} \cdot 12^{62} \equiv 12^{10} \cdot 12^{62} = 12^{71} \cdot 12 \equiv 12 \cdot 12 \equiv 2 \cdot 71 + 2 \equiv 2 \pmod{71}.$$

4. Vastaa kiinalaisen munkin Sun Zin kysymykseen: Onko lukua $x \in \mathbb{Z}$, jolle lineaariset kongruenssiyhtälöt

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

ovat totta?

Ratkaisu. Koska $\text{syt}(3,5) = 1 = \text{syt}(3,7) = \text{syt}(5,7)$, Kiinalaisen jäännöslauseen oletus on voimassa. Siis kongruenssiyhtälöryhmällä on yksikäsitteinen ratkaisu (kongruenssiluokkana modulo 105). Kokeilemalla voidaan huomata, että luku 23 toteuttaa kaikki kolme kongruenssiyhtälöä. Siis kongruenssiyhtälöryhmän ratkaisu on $[23]_{105}$.

5. Selvitä englanninkielisestä Wikipediasta, mikä on *twin prime* (alkulukukaksonen). Mainitse jokin tähän käsitteeseen liittyvä avoin ongelma.

Ratkaisu. Twin prime eli alkulukukaksonen on sellainen alkuluku p, että joko $p-2$ tai $p+2$ on alkuluku. Yksi lukuteorian kuuluisimmista avoimista ongelmista on, onko alkulukukaksosia ääretön määrä. Vahva veikkaus on, että konjektuuri on totta. Pienimmät alkulukukaksoset ovat 3, 5, 7, 11, 13, 17, 19, 29, 31, 37, 39.

6. Selvitä englanninkielisestä Wikipediasta, mikä on *Goldbach's conjecture* (Goldbachin (vahva) konjektuuri). Tarkista, että konjektuuri on totta parillisille luvuille neljästä kahteenkymmeneen.

Ratkaisu. Goldbachin (vahva) konjektuuri sanoo, että jokainen parillinen luku $a \geq 4$ voidaan esittää kahden alkuluvun summana. Konjektuuri muotoutui Goldbachin ja Eulerin välisessä kirjeenvaihdossa vuonna 1742. Kysymys on edelleen avoin ja sen ratkaisusta on vuosisatojen mittaan tarjottu isoja palkintoja. Pienimmille luvuille saadaan

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 5 + 3, \quad 10 = 7 + 3, \quad 12 = 7 + 5$$
$$14 = 7 + 7, \quad 16 = 11 + 5, \quad 18 = 11 + 7, \quad 20 = 13 + 7.$$

7. Olkoot $p, q \in \mathbb{N} \setminus \{0\}$ sellaiset luvut, että

$$\frac{p}{q} < \sqrt{7}.$$

Osoita, että

$$\frac{p}{q} + \frac{1}{pq} < \sqrt{7}.$$

Ratkaisu. Jos $p = 1$, väite on totta, sillä $\frac{p}{q} + \frac{1}{pq} \leq 2 < \sqrt{7}$.

Oletetaan seuraavaksi, että $p > 1$. Oletuksen nojalla $p^2 < 7q^2$. Koska pätee

$$[0]_7^2 = [0]_7 \quad [1]_7^2 = [1]_7, \quad , [2]_7^2 = [4]_7, \quad [3]_7^2 = [2]_7, \quad [4]_7^2 = [2]_7,$$
$$[5]_7^2 = [4]_7, \quad [6]_7^2 = [1]_7,$$

yhtälöt $p^2 + 1 = 7q^2$ ja $p^2 + 2 = 7q^2$ eivät ole mahdollisia. On siis oltava $p^2 + 2 < 7q^2$. Koska $p > 1$, tästä seuraa, että

$$p^2 + 2 + \frac{1}{p} < 7q^2 \quad \iff (p + \frac{1}{p})^2 < 7q^2 \quad \iff p + \frac{1}{p} < \sqrt{7}q,$$

josta väite seuraa.