Lukuteoria 1
Harjoitus 6, 21.2.2018
Ratkaisuehdotuksia

1. Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a, b \in \mathbb{Z}$. Oletetaan, että $x_0 \in [a]_n$ ja $y_0 \in [b]_n$. Osoita, että $x_0 y_0 \in [ab]_n$. (Tämä tulos perustelee, miksi kongruenssiluokkien välinen kertolasku on hyvin määritelty laskutoimitus.)

Ratkaisu. Oletusten nojalla $x_0 \equiv a \pmod{n}$ ja $y_0 \equiv b \pmod{n}$, joten Lauseen 4.1.5 kohdan (1) nojalla $x_0 y_0 \equiv ab \pmod{n}$ eli $x_0 y_0 \in [ab]_n$.

Tämä tulos siis perustelee kongruenssiluokille määrittelemämme kertolaskun järkevyyden: Jos nimittäin $[a_1]_n = [a_2]_n$ (eli a_1 ja a_2 ovat saman konruenssiluokan lukuja) ja $[b_1]_n = [b_2]_n$, niin määrittelemämme kertolaskun mukaan $[a_1]_n[b_1]_n = [a_1 b_1]_n$ ja $[a_2]_n[b_2]_n = [a_2 b_2]_n$. Jotta tässä olisi tolkkua, pitää olla $[a_1 b_1]_n = [a_2 b_2]_n$, eli $a_1 b_1 \in [a_2 b_2]_n$. Tämän tehtävän tulos takaa, että näin on.

2. Olkoon $a \in \mathbb{Z}$. Osoita kongruenssiluokkien avulla, että luku a^2 voidaan esittää muodossa $a^2 = 5k + r$, missä $k \in \mathbb{Z}$ ja $r \in \{0, 1, 4\}$.

Ratkaisu. Lauseen 4.3.3 nojalla $a \in [0]_5 \cup [1]_5 \cup [2]_5 \cup [3]_5 \cup [4]_5$. On

$$[0]_5^2 = [0]_5, \quad [1]_5^2 = [1]_5, \quad [2]_5^2 = [4]_5, \quad [3]_5^2 = [4]_5, \quad [4]_5^2 = [1]_5.$$

Siis $a^2 \in [0]_5 \cup [1]_5 \cup [4]_5$, eli $a^2 = 5k + r$ jollakin $k \in \mathbb{Z}$, $r \in \{0, 1, 4\}$.

3. Olkoon $a \in \mathbb{Z}$ pariton luku. Osoita kongruenssiluokkien avulla, että $a^2 \in [1]_8$.

Ratkaisu. Jakojäännöslauseen ja parittomuuden nojalla $a \in [i]_8$ jollakin $i \in \{1, 3, 5, 7\}$. On

$$[1]_8^2 = [1]_8, \quad [3]_8^2 = [1]_8, \quad [5]_8^2 = [1]_8, \quad [7]_8^2 = [1]_8.$$

Siis $a^2 \in [1]_8$.

4. Etsi kongruenssiyhtälön $4x \equiv 5 \pmod{6}$ kaikki ratkaisut.

Ratkaisu. Koska $\text{syt}(4, 6) \nmid 5$, Lauseen 4.4.4 nojalla kongruenssiyhtälöllä ei ole ratkaisuja.

Huomautus: Jos ei muista Lausetta 4.4.4, voi myös todeta, että $4x - 5$ on pariton kaikilla $x \in \mathbb{Z}$, joten se ei voi olla jaollinen kuudella.

5. Etsi kongruenssiyhtälön $4x \equiv 8 \pmod{6}$ kaikki ratkaisut.

Ratkaisu. Koska $\text{syt}(4, 6) = 2$ ja $2 \mid 8$, Lauseen 4.4.4 nojalla kongruenssiyhtälöllä on kaksi ratkaisua (kongruenssiluokkina). Nähdään, että $x_0 = 2$ on eräs ratkaisu, joten koko kongruenssiluokka $[2]_6$ on ratkaisu. Lauseen 4.4.4 nojalla toinen ratkaisu on kongruenssiluokka $[2 + 1 \cdot \frac{6}{2}]_6 = [5]_6$, ja muita ratkaisuja ei ole.

Huomautus: Jos ei muista Lausetta 4.4.4, voi myös todeta, että koska $\mathbb{Z}$ on yhdiste kongruenssiluokista $[i]_6$, $i \in \{0,1,2,3,4,5\}$, niin riittää katsoa yksitellen, mitkä luvut joukosta $\{0,1,2,3,4,5\}$ toteuttavat kongruenssiyhtälön, jolloin ratkaisuja ovat täsmälleen toteuttavien lukujen määräämät kongruenssiluokat. Lause 4.4.4 ei siis ole mitenkään välttämätön haluttaessa löytää kongruenssiyhtälön kaikki ratkaisut, mutta se keventää työmäärää varsinkin jos "mod n"on hyvin suuri.

Tehtävän voi tehdä vielä kolmannella tavalla, nimittäin tarkastelemalla kongruenssiyhtälöön liittyvää Diofantoksen yhtälöä $4x - 6y = 8$ ja etsimällä sen kaikki ratkaisut. Tällä menetelmällä päätyy siihen, että kongruenssiyhtälön kaikki ratkaisut muodostavat kongruenssiluokan $[2]_3$. Tämä on yhtälailla oikea ratkaisu kuin aiemmin löytämämme, sillä $[2]_6 \cup [5]_6 = [2]_3$.

Määritelmä. Olkoot $m, n \in \mathbb{N} \setminus \{0\}$ ja $a, b \in \mathbb{Z}$. Luku $x_0 \in \mathbb{Z}$ on *kongruenssiyhtälöparin*

$$\begin{cases} x \equiv a & (\mathrm{mod}\, m) \\ x \equiv b & (\mathrm{mod}\, n) \end{cases}$$

ratkaisu, jos $x_0 \equiv a\,(\mathrm{mod}\, m)$ ja $x_0 \equiv b\,(\mathrm{mod}\, n)$.

6. Osoita, että edellä määritellyllä kongruenssiyhtälöparilla on ainakin yksi kokonaislukuratkaisu täsmälleen sillä ehdolla, että

$$a \equiv b \pmod{d},$$

missä $d = \mathrm{syt}(m, n)$.

Ratkaisu. Oletetaan ensin, että on sellainen luku $x_0 \in \mathbb{Z}$ että $x_0 \equiv a\,(\mathrm{mod}\, m)$ ja $x_0 \equiv b\,(\mathrm{mod}\, n)$. Tällöin on sellaiset luvut $k_1, k_2 \in \mathbb{Z}$, että $x_0 - a = k_1 m$ ja $x_0 - b = k_2 n$. Vähentämällä puolittain jälkimmäinen yhtälö ensimmäisestä saadaan

$$b - a = k_1 m - k_2 n.$$

Koska d on lukujen m, n tekijä, on sellaiset luvut $l_1, l_2 \in \mathbb{Z}$ että $m = l_1 d$ ja $n = l_2 d$. Siis

$$b - a = (k_1 l_1 - k_2 l_2)d \quad \Longrightarrow \quad a \equiv b \pmod{d}.$$

Oletetaan seuraavaksi, että $a \equiv b \pmod{d}$. Koska siis $d \mid (a - b)$, Seurauksen 2.3.12 nojalla on sellaiset luvut r_0, s_0 että

$$r_0 m + s_0 n = a - b \quad \Longleftrightarrow \quad a - r_0 m = b + s_0 n.$$

Olkoon $x_0 = a - r_0 m = b + s_0 n$. Tämä x_0 on ratkaisu kongruenssiyhtälöparille. Väite on todistettu.

7. (a) Onko kongruenssiyhtälöparilla

$$\begin{cases} x \equiv 3 & (\mathrm{mod}\, 2) \\ x \equiv 2 & (\mathrm{mod}\, 3) \end{cases}$$

ratkaisuja? Jos on, keksi yksi ratkaisu.

(b) Onko kongruenssiyhtälöparilla

$$\begin{cases} x \equiv 4 & (\mathrm{mod}\, 2) \\ x \equiv 2 & (\mathrm{mod}\, 3) \end{cases}$$

ratkaisuja? Jos on, keksi yksi ratkaisu.

Ratkaisu. Koska $\text{syt}(2,3) = 1$, kummallakin kongruenssiyhtälöparilla on ratkaisuja. Kohdassa a ratkaisuja ovat kaikki ne parittomat luvut, joiden jakojäännös jaettaessa kolmella on 2. Eräs ratkaisu on 5. (Viimeisellä luentoviikolla mainitun Kiinalaisen jäännöslauseen nojalla kongruenssiluokka $[5]_6$ muodostaa kaikki ratkaisut, mutta tätä ei tehtävässä luonnollisesti vaadittu.)

Vastaavasti b-kohdassa ratkaisuja ovat kaikki ne parilliset luvut, joiden jakojäännös jaettaessa kolmella on 2. Eräs ratkaisu on 2. (Kiinalaisen jäännöslauseen nojalla kongruenssiluokka $[2]_6$ muodostaa kaikki ratkaisut.)