Lukuteoria 1 (MATA151)
Kurssitentti, 7.3.2018
Malliratkaisut

1. (a) Olkoot $a, b, c, m, n \in \mathbb{Z}$. Oletetaan, että $a \mid b$ ja $a \mid c$. Osoita, että

$$a \mid (mb + nc).$$

(b) Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a, b, c \in \mathbb{Z}$. Oletetaan, että $a \equiv b \,(\mathrm{mod}\, n)$ ja $b \equiv c \,(\mathrm{mod}\, n)$. Osoita, että

$$a \equiv c \,(\mathrm{mod}\, n).$$

Ratkaisu.
(a) Oletusten nojalla $b = k_1 a$ ja $c = k_2 a$ joillakin $k_1, k_2 \in \mathbb{Z}$. Saadaan

$$mb + nc = m(k_1 a) + n(k_2 a) = (mk_1 + nk_2)a,$$

joten $a \mid (mb + nc)$.

(b) Oletusten nojalla $a - b = k_1 n$ ja $b - c = k_2 n$ joillakin $k_1, k_2 \in \mathbb{Z}$. Saadaan

$$a - c = (a - b) + (b - c) = k_1 n + k_2 n = (k_1 + k_2)n,$$

joten $a \equiv c \,(\mathrm{mod}\, n)$.

2. (a) Selvitä Eukleideen algoritmin avulla lukujen 154 ja 30 suurin yhteinen tekijä $\mathrm{syt}(154, 30)$.

(b) Etsi yksi kokonaislukuratkaisu Diofantoksen yhtälölle

$$154x + 30y = 6.$$

Ratkaisu.
(a) Eukleideen algoritmilla saadaan

$$\begin{aligned} 154 &= 5 \cdot 30 + 4 \\ 30 &= 7 \cdot 4 + 2 \\ 4 &= 2 \cdot 2. \end{aligned}$$

Siis $\mathrm{syt}(154, 30) = 2$.

(b) Edellisen kohdan päättely kääntämällä (”peruuttamalla”) saadaan

$$2 = 30 - 7 \cdot 4 = 30 - 7(154 - 5 \cdot 30) = -7 \cdot 154 + 36 \cdot 30.$$

Siis $6 = -21 \cdot 154 + 108 \cdot 30$, joten eräs kokonaislukuratkaisu tehtävän Diofantoksen yhtälölle on $x = -21$, $y = 108$.

3. (a) Olkoot p_1 ja p_2 jotkin keskenään erisuuret alkuluvut, ja olkoon

$$a = p_1 p_2 + 1.$$

Osoita, että on olemassa sellainen alkuluku p, että $p \mid a$, $p \neq p_1$ ja $p \neq p_2$.

(b) Olkoon $p > 3$ alkuluku. Osoita, että luku $p^2 + 2$ on yhdistetty luku.

Ratkaisu.

(a) Koska $p_1 \geq 2$ ja $p_2 \geq 2$, on $a \geq 2$. Siis aritmetiikan peruslauseen nojalla luku a on jaollinen jollakin alkuluvulla p. Jos olisi $p = p_1$ tai $p = p_2$, niin p jakaisi luvun $a - p_1 p_2 = 1$, mikä ei ole mahdollista, sillä $p \geq 2$. Siis tämä luku p toteuttaa tehtävässä vaaditut ehdot.

(b) Koska $p > 3$ on alkuluku, pätee $3 \nmid p$. Siis $p \in [1]_3$ tai $p \in [2]_3$. Koska $[1]_3^2 = [1]_3$ ja $[2]_3^2 = [1]_3$, on $p^2 \in [1]_3$. Siis $p^2 = 3k + 1$ jollakin $k \in \mathbb{Z}$, joten $p^2 + 2 = 3(k + 1)$ jollakin $k \in \mathbb{Z}$. Siis $3 \mid (p^2 + 2)$, ja koska lisäksi $p^2 + 2 > 3$, kyseessä on yhdistetty luku.

4. (a) Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a \in \mathbb{Z}$. Anna määritelmä luvun a määräämälle kongruenssiluokalle modulo n, $[a]_n$.

(b) Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a, b \in \mathbb{Z}$. Oletetaan, että $[a]_n \cap [b]_n \neq \emptyset$, missä symboli $\emptyset$ tarkoittaa tyhjää joukkoa. Osoita, että $[a]_n = [b]_n$.

Ratkaisu.

(a)
$$[a]_n = \{b \in \mathbb{Z} \ : \ a \equiv b \pmod{n}\}.$$

(b) Oletuksen nojalla on sellainen $c \in \mathbb{Z}$, että $c \in [a]_n \cap [b]_n$, eli $a \equiv c \pmod{n}$ ja $b \equiv c \pmod{n}$. Jälkimmäisestä seuraa, että $c \equiv b \pmod{n}$, joten (katso 1.(b)) $a \equiv b \pmod{n}$.
Osoitetaan ensin, että $[a]_n \subset [b]_n$. Olkoon $d \in [a]_n$. Koska $d \equiv a \pmod{n}$ ja $a \equiv b \pmod{n}$, on $d \equiv b \pmod{n}$, eli $d \in [b]_n$. Siis $[a]_n \subset [b]_n$.
Aivan vastaavasti todistetaan, että $[b_n] \subset [a]_n$. Olkoon $e \in [b]_n$. Koska $e \equiv b \pmod{n}$ ja $b \equiv a \pmod{n}$, on $e \equiv a \pmod{n}$, joten $e \in [a]_n$. Siis $[b]_n \subset [a]_n$.

5. Olkoot $a, b, c \in \mathbb{N} \setminus \{0\}$ lukuja, jotka toteuttavat yhtälön
$$a^2 + b^2 = c^2.$$
Osoita, että $abc \equiv 0 \pmod{30}$.

Ratkaisu. Koska $30 = 2 \cdot 3 \cdot 5$, riittää osoittaa, että luvun abc alkutekijäesiteyksessä esiintyy luvut $2, 3$ ja 5, eli riittää todistaa, että $2 \mid abc$, $3 \mid abc$ ja $5 \mid abc$.

Osoitetaan ensin, että $2 \mid abc$. Jos kaikki luvut a, b, c olisivat parittomia, niin myös luvut a^2, b^2, c^2 olisivat parittomia ($[1]_2^2 = [1]_2$), jolloin $a^2 + b^2$ olisi parillinen. Tämä on ristiriita. Siis ainakin yksi luvuista a, b, c on parillinen, joten $2 \mid abc$.

Osoitetaan seuraavaksi, että $3 \mid abc$. Jos mikään luvuista a, b, c ei olisi jaollinen kolmella, olisi $a^2, b^2, c^2 \in [1]_3$ (katso tehtävän 3.(b) ratkaisu). Tällöin olisi $a^2 + b^2 \in [2]_3$. Tämä on ristiriita. Siis ainakin yksi luvuista a, b, c on jaollinen kolmella, joten $3 \mid abc$.

Osoitetaan vielä, että $5 \mid abc$. Oletetaan, että mikään luvuista a, b, c ei ole jaollinen viidellä, ja pyritään taas ristiriitaan. Koska
$$[1]_5^2 = [1]_5, \quad [2]_5^2 = [4]_5, \quad [3]_5^2 = [4]_5, \quad [4]_5^2 = [1]_5,$$
olisi $a^2 + b^2 \in [0]_5 \cup [2]_5 \cup [3]$. Tämä ei ole mahdollista, sillä $c^2 \in [1]_5 \cup [4]_5$. Siis ainakin yksi luvuista a, b, c on jaollinen viidellä, joten $5 \mid abc$. Todistus on valmis.