Lukuteoria 1
Harjoitus 5, 14.2.2018
Ratkaisuehdotuksia

1. Todista Propositio 4.1.2: Olkoon $n \in \mathbb{N}\setminus\{0\}$ ja $a, b \in \mathbb{Z}$. Tällöin $a \equiv b \pmod{n}$ täsmälleen sillä ehdolla, että on luvut $k, l, r \in \mathbb{Z}$, $0 \leq r < n$, joille $a = kn + r$ ja $b = ln + r$.

Ratkaisu. Oletetaan ensin, että on on luvut $k, l, r \in \mathbb{Z}$, $0 \leq r < n$, joille $a = kn + r$ ja $b = ln + r$. Tällöin

$$a - b = (k - l)n,$$

eli $a \equiv b \pmod{n}$.

Oletetaan seuraavaksi, että $a \equiv b \pmod{n}$. Jakojäännöslauseen nojalla on jotkin luvut k, l, r_1, r_2 siten että

$$a = kn + r_1, \quad 0 \leq r_1 < n,$$

$$b = ln + r_2, \quad 0 \leq r_2 < n.$$

On osoitettava, että $r_1 = r_2$. Oletuksen nojalla n jakaa luvun $a - b = (k - l)n + (r_1 - r_2)$. Koska n jakaa myös luvun $(k - l)n$, Proposition 2.1.4 nojalla n jakaa luvun

$$(k - l)n + (r_1 - r_2) - (k - l)n = (r_1 - r_2).$$

Koska $0 \leq r_1 < n$ ja $0 \leq r_2 < n$, on oltava $r_1 - r_2 = 0n = 0$.

2. Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a, b \in \mathbb{Z}$. Osoita, että jos $a \equiv b \pmod{n}$ ja $d \in \mathbb{N} \setminus \{0\}$ on luvun n tekijä, niin $a \equiv b \pmod{d}$.

Ratkaisu. Oletusten nojalla $a - b = k_1 n$ jollakin $k_1 \in \mathbb{Z}$, ja $n = k_2 d$ jollakin $k_2 \in \mathbb{Z}$. Siis $a - b = (k_1 k_2)d$, joten $a \equiv b \pmod{d}$.

3. Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja $a_i, b_i \in \mathbb{Z}$ kaikilla $i \in \{1, ..., k\}$, missä $k \geq 2$ on luonnollinen luku. Oletetaan, että $a_i \equiv b_i \pmod{n}$ kaikilla $i \in \{1, ..., k\}$. Todista seuraavat väitteet:

(a)
$$\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{n}.$$

(b)
$$a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \pmod{n}.$$

Ratkaisu.

(a) Käytetään induktiota luvun k suhteen. Koska tiedetään että $k \geq 2$, alkuaskel on $k = 2$. Jos $a_1 \equiv b_1 \pmod{n}$ ja $a_2 \equiv b_2 \pmod{n}$, niin Lauseen nojalla (kun $x = 1 = y$) on $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, joten alkuaskel on ok.

Induktio-oletus: tehtävän väite pätee kun $k = m$: Oletamme siis, että kun $a_i \equiv b_i \pmod{n}$ kaikilla $i \in \{1, ..., m\}$, niin

$$\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} b_i \pmod{n}.$$

Induktio-väite $k = m + 1$: Oletetaan, että $a_i \equiv b_i \pmod{n}$ kaikilla $i \in \{1, ..., m + 1\}$. Tällöin

$$\sum_{i=1}^{m+1} a_i = \sum_{i=1}^{m} a_i + a_{m+1} \equiv \sum_{i=1}^{m} b_i + b_{m+1} = \sum_{i=1}^{m+1} b_i \pmod{n},$$

missä keskimmäinen päättely seurasi induktio-oletuksesta ja Lauseesta 4.1.5 (taas tapauksessa $x = 1 = y$).

(b) Päättely on käytännössä identtinen edelliseen verrattuna. Alkuaskel $k = 2$ seuraa taas suoraan Lauseesta 4.1.5. Induktio-oletus on, että tehtävän väite pätee kun $k = m$. Induktioväite $k = m + 1$ seuraa taas induktio-oletuksesta ja Lauseesta 4.1.5: Kun $a_i \equiv b_i \pmod{n}$ kaikilla $i \in \{1, ..., m+1\}$, on

$$a_1 a_2 \cdots a_{m+1} = (a_1 \cdots a_m)a_{m+1} \equiv (b_1 \cdots b_m)b_{m+1} = b_1 b_2 \cdots b_{m+1} \pmod{n}.$$

4. Todista Lauseen 4.1.8 yleinen versio: Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja olkoot $a, b, c \in \mathbb{Z}$ lukuja, joille $ac \equiv bc \pmod{n}$. Jos $d = \text{syt}(n, c)$, niin

$$a \equiv b \pmod{\frac{n}{d}}.$$

Ratkaisu. Oletuksen nojalla $c(a - b) = kn$ jollakin $k \in \mathbb{Z}$. Jakamalla puolittain luvulla d saadaan

$$\frac{c}{d}(a - b) = k\frac{n}{d}.$$

Huomaa, että luvut $\frac{c}{d}$ ja $\frac{n}{d}$ ovat kokonaislukuja, sillä d jakaa sekä luvun c että n. Lisäksi Lemman 2.5.2 nojalla lukujen $\frac{c}{d}$ ja $\frac{n}{d}$ suurin yhteinen tekijä on 1. Koska

$$\frac{n}{d} \mid \frac{c}{d}(a - b),$$

Lemman 2.5.1 nojalla $\frac{n}{d} \mid (a - b)$. Siis $a \equiv b \pmod{\frac{n}{d}}$.

5. Mitkä seuraavista väitteistä ovat oikein ja mitkä väärin?

(a) $3 \mid 18\,643\,560$.
(b) $4 \mid 18\,643\,560$.
(c) $9 \mid 18\,643\,560$.

Ratkaisu.

(a) Koska $1 + 8 + 6 + 4 + 3 + 5 + 6 + 0 = 33$ ja $3 \mid 33$, niin kappaleen 4.2 nojalla väite on tosi.
(b) Koska $4 \mid 60$, kappaleen 4.2 nojalla väite on tosi.
(c) Koska $9 \nmid 33$, kappaleen 4.2 nojalla väite on väärin.

6. (a) Onko sellaista lukua $a \in \{0, 1, 2, 3, 4, 5\}$, että $[3]_6[a]_6 = [1]_6$?
(b) Onko sellaista lukua $a \in \{0, 1, 2, 3, 4, 5, 6\}$, että $[3]_7[a]_7 = [1]_7$?

Ratkaisu.

(a) $[3]_6[0]_6 = [3 \cdot 0]_6 = [0]_6$, $[3]_6[1]_6 = [3 \cdot 1]_6 = [3]_6$, $[3]_6[2]_6 = [3 \cdot 2]_6 = [0]_6$, $[3]_6[3]_6 = [3 \cdot 3]_6 = [3]_6$, $[3]_6[4]_6 = [3 \cdot 4]_6 = [0]_6$, $[3]_6[5]_6 = [3 \cdot 5]_6 = [3]_6$. Vastaus: ei ole.
(b) Koska $[3]_7[5]_7 = [3 \cdot 5]_7 = [15]_7 = [1]_7$, vastaus on kyllä.

7. Osoita, että ei ole olemassa sellaista suorakulmaista kolmiota, jonka kaikkien sivujen pituudet ovat alkulukuja.

Ratkaisu. Tehdään vastaoletus, että on sellaiset alkuluvut p_1, p_2, p_3 että

$$p_1^2 + p_2^2 = p_3^2.$$

Jos kaikki kolme alkulukua olisivat parittomia, yhtälön vasemmalle puolelle tulisi parillinen ja oikealle puolelle pariton luku, mikä ei ole mahdollista. Oletetaan siis, että ainakin yksi alkuluvuista on parillinen (eli 2). Koska $p_1^2 + p_2^2 > 4$, luku p_3 ei voi olla 2. Oletetaan siis, että ainakin toinen luvuista p_1 ja p_2 on 2. Yleisyyttä menettämättä voidaan olettaa, että $p_2 = 2$. Nyt yhtälömme on siis

$$p_1^2 + 4 = p_3^2 \quad \iff \quad (p_3 + p_1)(p_3 - p_1) = 4.$$

Koska hypotenuusa on pidempi kuin kumpikaan kateeteista ja p_1 on alkuluku, pätee $p_3 > p_1 \geq 2$, siis $p_3 - p_1 \geq 1$ ja $p_3 + p_1 \geq 5$. Siis

$$(p_3 + p_1)(p_3 - p_1) \geq 5,$$

mikä on ristiriita. Todistus on valmis.