Matematiikan ja tilastotieteen laitos
Algebra I (Kevät 2009)
Harjoitus 5
Ratkaisuja (Jussi Martin)

1. Todista alkulukuhajoitelman yksikäsitteisyyden avulla seuraavat väitteet:
a) Kuvaus $(m,n) \mapsto 3^m 5^n$ on injektio $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.
b) Jos p on alkuluku, niin yhtälöllä $x^2 = p$ ei ole ratkaisua $x \in \mathbb{Q}$.

Ratkaisu:

a)-kohta:
Koska 3 ja 5 ovat erisuuria alkulukuja, on alkulukuhajotelman yksikäsiteisyyden nojalla oltava:

$$3^m 5^n = 3^{m'} 5^{n'} \quad \Leftrightarrow \quad m = m' \quad \text{ja} \quad n = n'$$

ja näin ollen kuvaus $(m,n) \mapsto 3^m 5^n$ on injektio $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.
b)-kohta:
Jos yhtälö pätisi jollakin $x \in \mathbb{Q}$, olisi olemassa luvut $m \in \mathbb{Z} \setminus \{0\}$ ja $n \in \mathbb{N}_+$, joilla $x = m/n$ ja

$$(\frac{m}{n})^2 = p \quad \text{eli} \quad m^2 = pn^2.$$

Olkoon nyt lukujen alkutekijähajotelmat

$$m = p_1^{j_1} \dots p_s^{j_s}, \quad n = p_1^{k_1} \dots p_t^{k_t}.$$

Nyt siis

$$(p_1^{j_1} \dots p_s^{j_s})^2 = p(p_1^{k_1} \dots p_t^{k_t})^2 \quad \text{eli} \quad p_1^{2j_1} \dots p_s^{2j_s} = p^1 p_1^{2k_1} \dots p_t^{2k_t},$$

mutta tällöin yhtälön vasemmalla puolella esiintyy alkulukuja korotettuna vain parillisiin potensseihin, kun taas oikealla puolella on luku p korotettuna parittomaan potenssiin (joka on joko 1 tai $2k_r + 1$ riippuen siitä, onko $p = p_r$ jollakin $1 \leq r \leq t$ yhtälön oikealla puolella), mutta tämä on ristiriidassa alkulukuhajotelman yksikäsitteisyyden kanssa.

2. Etsi Eratosteneen seulaa käyttäen kaikki alkuluvut < 150. Etsi tämän jälkeen lukujen 7676, 7677 ja 19317 alkutekijähajoitelmat. (Kokeile laskimen avulla jaollisuutta löytämilläsi alkuluvuilla.)

Ratkaisu:
Erastoteneen seulaa kättämällä löydetään alkuluvut $p < 150$:
2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,
107,109,113,127,131,137,139,149.

Luvun $n \in \mathbb{N}_+$ alkutekijöitä etsittäessä kannattaa muistaa, että joko n on alkuluku tai jollekin alkutekijälle p_i pätee: $p_i \leq \sqrt{n}$. Nyt kaikki tarkasteltavat luvut ovat pienempiä kuin $149^2 = 22201$, joten meillä on riittävä määrä alkulukuja käytössä. Kokeilemalla laskimella jaollisuutta, saadaan seuraavat tekijöihin jaot:

$$7676 = 2^2 19^1 101^1,$$
$$7677 = 3^2 853^1$$
$$19317 = 3^1 47^1 137^1,$$

missä luku 853 havaittiin alkuluvuksi, koska se ei ole jaollinen millään alkuluvulla $p \leq 30$, sillä $\sqrt{853} \approx 29,2 < 30$.

3. Tutki jokaisella $\alpha \in \mathbb{Z}_5$, kuinka monta eri alkiota on joukossa $\{\alpha, \alpha^2, \alpha^3, \ldots\}$.

Ratkaisu:
Nyt

$$[0]_5^k = [0^k]_5 = [0]_5 \quad \text{ja} \quad [1]_5^k = [1^k]_5 = [1]_5, \quad \text{kaikilla} \quad k \in \{1, 2, 3, \ldots\},$$

lisäksi selvästi

$$[m]_5^1 = [m^1]_5 = [m]_5, \quad \text{kaikilla} \quad m \in \{0, \ldots, 4\}.$$

Tarkastellaan siis alkioiden $[2]_5, [3]_5$ ja $[4]_5$ potensseja $k \geq 2$.
$[2]_5$:n potenssit:

$$[2]_5^2 = [4]_5, \quad [2]_5^3 = [8]_5 = [3]_5, \quad [2]_5^4 = [16]_5 = [1]_5$$

eli

$$\{[2]_5, [2]_2^2, [2]_5^3, \ldots\} = \{[1]_5, [2]_5, [3]_5, [4]_5\},$$

sillä $[0]_5$ ei voi kuulua joukkoon, koska tällöin olisi $2^k = 5j$, joillakin $k, j \in \mathbb{N}_+$, mikä olisi ristiriidassa alkulukuhajotelman yksikäsitteisyyden kanssa.
$[3]_5$:n potenssit:

$$[3]_5^2 = [9]_5 = [4]_5, \quad [3]_5^3 = [27]_5 = [2]_5, \quad [3]_5^4 = [81]_5 = [1]_5,$$
$$[3]_5^5 = [243]_5 = [3]_5$$

eli

$$\{[3]_5, [3]_2^2, [3]_5^3, \ldots\} = \{[1]_5, [2]_5, [3]_5, [4]_5\},$$

sillä $[0]_5$ ei voi kuulua joukkoon, koska tällöin olisi $3^k = 5j$, joillakin $k, j \in \mathbb{N}_+$, mikä olisi ristiriidassa alkulukuhajotelman yksikäsitteisyyden kanssa.
$[4]_5$:n potenssit:

$$[4]_5^2 = [16]_5 = [1]_5, \quad [4]_5^3 = [64]_5 = [4]_5,$$

nyt saadaan, että

$$[4]_5^{2m} = ([4]_5^2)^m = [1]_5^m = [1]_5, \quad \text{kun} \quad k = 2m, \quad m \in \mathbb{N}_+$$

ja

$$[4]_5^{2m+1} = ([4]_5^2)^m \cdot [4]_5 = [4]_5, \quad \text{kun} \quad k = 2m + 1, \quad m \in \mathbb{N}_+$$

eli

$$\{[4]_5, [4]_2^2, [4]_5^3, \ldots\} = \{[1]_5, [4]_5\},$$

sillä taaskaan $[0]_5$ ei voi kuulua joukkoon, koska tällöin olisi $2^{2k} = 5j$, joillakin $k, j \in \mathbb{N}_+$ mikä olisi ristiriidassa alkulukuhajotelman yksikäsitteisyyden kanssa.

4. **a)** Ratkaise kongruenssi $16x \equiv 3 \pmod{23}$ etsimällä sellainen $c \in \mathbb{Z}$, että $c \cdot 16 \equiv 1 \pmod{23}$.
b) Ratkaise kongruenssi $4x \equiv 8 \pmod{12}$ esimerkiksi kokeilemalla.
c) Ratkaise samanaikaiset kongruenssit $x \equiv 5 \pmod{8}$ ja $x \equiv 4 \pmod{17}$ kiinalaisen jäännöslauseen avulla.

Ratkaisu:

a)-kohta:
Nyt nähdään, että $\text{syt}(16, 23) = 1$ ja etsimällä löydetään luku $c = 13$, jolla

$$13 \cdot 16 = 208 = 1 + 9 \cdot 23 \quad \text{eli} \quad 13 \equiv 1 \pmod{23}.$$

Luentojen perusteella tiedetään, että yhtälöllä on tällöin olemassa yksikäsiteinen ratkaisu:

$$x \equiv 13 \cdot 3 = 39 = 16 + 23 \equiv 16 \pmod{23}.$$

b)-kohta:
Tässä kohdassa puolestaan nähdään, että $\text{syt}(4, 12) = 4 > 1$. Nyt haluttiin siis, että $4x \equiv 8 \pmod{12}$, mikä on yhtäpitävää sen kanssa, että

$$4x = 8 + 12k, \quad \text{jollakin} \quad k \in \mathbb{Z} \quad \Leftrightarrow \quad x = 2 + 3k, \quad \text{jollakin} \quad k \in \mathbb{Z}$$

eli ratkaisuksi saadaan: $x \equiv 2 \pmod{3}$.

c)-kohta:
Sovelletaan kiinalaisen jäännöslauseen metodia. Koska 8 ja 17 ovat keskenään jaottomia, on $1 = 17 - 2 \cdot 8$, minkä esimerkiksi Euklideen algoritmi antaa. Siten

$$5 \cdot 17 - 4 \cdot 2 \cdot 8 = 85 - 64 = 21$$

on eräs ratkaisu. Tällöin, koska $8 \cdot 17 = 136$, niin kiinalaisen jäännöslauseen mukaan yleinen ratkaisu on $x \equiv 21 \pmod{136}$.

Esitetään vielä vaihtoehtoinen tapa yksittäisen ratkaisun etsimiseksi. Halutaan itse asiassa ratkaista yhtälö

$$m8 + 5 = n17 + 4 \quad \text{joillakin} \quad m, n \in \mathbb{N}_+,$$

missä siis $x = m8 + 5 = n17 + 4$. Tämä on yhtäpitävä yhtälön

$$5 - 4 = 1 = n17 - m8 \quad \text{joillakin} \quad m, n \in \mathbb{N}_+$$

kanssa, jonka yksi ratkaisu saadaan arvoilla $n = 1$ ja $m = 2$, jolloin siis $x = 21$.

Menetelmä yleistyy seuraavasti:
Olkoon $\text{syt}(m, n) = 1$ ja ratkaistavana yhtälöt $x \equiv k \pmod{m}$, $x \equiv l \pmod{n}$. Etsitään Euklideen algoritmilla a ja b, joilla $am + bn = 1$ ja asetetaan $r = (l - k)a$, $s = (k - l)b$. Tällöin $rm - sn = l - k$, joten $k + rm = l + sn$, ja siis $x = k + rm = l + sn$ on eräs ratkaisu. Nyt

$$x = k + (l - k)am = lam + k(1 - am) = lam + kbn$$

eli saadaan sama kaava kuin kiinalaisen jäännöslauseen todistuksessa.

5. Määritellään $x \top y = x + y + xy$, kun $x, y \in \mathbb{Z}$. Osoita, että joukon $\mathbb{Z}$ laskutoimitus $\top$ on liitännäinen ja vaihdannainen ja että sillä on neutraalialkio (mikä nimittäin?).

Ratkaisu:

Liitännäisyys:
Olkoon x, y ja z mielivaltaisia alkioita $\mathbb{Z}$:ssa; tällöin

$$(x \top y) \top z = (x + y + xy) \top z$$

$$= (x + y + xy) + z + (x + y + xy)z = x + y + xy + z + xz + yz + xyz$$

ja

$$x \top (y \top z) = x \top (y + z + yz)$$

$$= x + (y + z + yz) + x(y + z + yz) = x + y + z + yz + xy + xz + xyz,$$

mistä nähdään, että

$$(x \top y) \top z = x \top (y \top z),$$

sillä

$$x + y + xy + z + xz + yz + xyz = x + y + z + yz + xy + xz + xyz,$$

koska yhteenlasku on vaihdannainen $\mathbb{Z}$:ssa.

Vaihdannaisuus:
Olkoon x ja y mielivaltaisia alkioita $\mathbb{Z}$:ssa; tällöin

$$x \top y = x + y + xy \quad \text{ja} \quad y \top x = y + x + yx$$

mistä nähdään, että

$$x \top y = y \top x,$$

sillä

$$x + y + xy = y + x + yx,$$

koska yhteenlasku ja kertolasku ovat vaihdannaisia $\mathbb{Z}$:ssa.

Nyt 0 on neutraalialkio, sillä

$$0 \top y = 0 + y + 0y = y \quad \text{ja} \quad x \top 0 = x + 0 + x0 = x \quad \text{kaikilla} \quad x, y \in \mathbb{Z}.$$

6. Olkoon $\top$ joukon A laskutoimitus, jolla on neutraalialkio ja jolla

$$a \top (b \top c) = (a \top c) \top b \quad \text{kaikilla } a, b, c \in A.$$

Osoita, että $\top$ on liitännäinen ja vaihdannainen.

Ratkaisu:

Osoitetaan ensin vaihdannaisuus:
Olkoon b ja c mielivaltaisia A:n alkioita ja e laskutoimituksen neutraalialkio; tällöin

$$e \top (b \top c) = (e \top c) \top b,$$

ja koska e on neutraalialkio, on

$$e \top (b \top c) = b \top c \quad \text{ja} \quad e \top c = c,$$

minkä avulla nähdään, että

$$b \top c = c \top b$$

Nyt liitännäisyys saadaan käyttämällä vaihdannaisuutta:
olkoon a, b ja c mielivaltaisia A:n alkioita; tällöin

$$a \top (b \top c) = a \top (c \top b) = (a \top b) \top c,$$

missä ensimmäinen yhtälö seurasi vaihdannaisuudesta ja toinen tehtävänannossa mainitusta laskutoimituksen ominaisuudesta.

Huomautus:
Kääntäen pätee: Liitännäisyys ja vaihdannaisuus antavat tehtävän ehdon, sillä tällöin

$$a \top (b \top c) = a \top (c \top b) = (a \top c) \top b$$

eli tehtävänannossa onkin kyseessä vaihtoehtoinen juonikas tapa määritellä kommutatiivinen monoidi.