Algebra 1B, Harjoitus 1, 21.1. 2015

1. Anna osamäärä q ja jakojäännös $0 \leq r < b$ kun luku a jaetaan luvulla b, missä (i) $a = 17$ ja $b = 4$, (ii) $a = -17$ ja $b = 4$, (iii) $a = -5$ ja $b = 12$.

2. Etsi kaikki kokonaislukuratkaisut x kongruenssiyhtälölle $a \equiv x \pmod{n}$, kun (i) $a = 12$ ja $n = 5$, (ii) $a = 24$ ja $n = 6$, (iii) $a = -25$ ja $b = 4$.

3. Esitä jäännösluokkarenkaiden $\mathbb{Z}_2$ ja $\mathbb{Z}_4$ laskutoimitukset $\oplus$ ja $\odot$ taulukoiden avulla.

4. Esitä jäännösluokkarenkaan $\mathbb{Z}_7$ laskutoimitukset $\oplus$ ja $\odot$ taulukoiden avulla.

5. Olkoon $a \in \mathbb{Z}$. Osoita, että $a^2 \equiv 0 \pmod{3}$ tai $a^2 \equiv 1 \pmod{3}$ (vihje: sovella jakoyhtälöä).

6. Merkitään $A = [0]_3$, $B = [1]_3 \cup \{5\} \setminus \{4\}$ ja $C = [2]_3 \cup \{4\} \setminus \{5\}$, missä $[a]_3$ ovat jäännösluokkia modulo 3. Onko laskutoimitus $\oplus$ hyvin määritelty joukossa $\{A, B, C\}$, kun asetetaan $X \oplus Y = Z$ jos $x + y \in Z$ jollain $x \in X$, $y \in Y$?

7. Onko väite tosi: Jos $[a] \odot [b] = [a] \odot [c]$ renkaassa $\mathbb{Z}_n$, ja $[a] \neq [0]$, niin $[b] = [c]$?

8. Etsi kaikki ratkaisut yhtälölle

(i) $x \oplus x \oplus x = [0]$ renkaassa $\mathbb{Z}_3$,

(ii) $[3] \odot x = [3]$ renkaassa $\mathbb{Z}_6$,

(iii) $x^2 \oplus [3] \odot x = [4]$ renkaassa $\mathbb{Z}_5$.

9.

(i) Etsi kaikki ratkaisut yhtälölle $x^2 \oplus x = [0]$ renkaassa $\mathbb{Z}_6$.

(ii) Osoita, että jos $p > 1$ on alkuluku, niin $x^2 \oplus x = [0]$ renkaassa $\mathbb{Z}_p$ täsmälleen silloin, kun $x = [0]$ tai $x = [p - 1]$.

10. Olkoon $p > 1$ alkuluku. Osoita, että jäännösluokkarenkaassa $\mathbb{Z}_p$ pätee

$$(a \oplus b)^p = a^p \oplus b^p \quad \text{kaikilla } a, b \in \mathbb{Z}_p.$$