Lukuteoria ja ryhmät

Harjoitus 4 kevät 2014

1. Ratkaise seuraavat kongruenssiyhtälöt (et tarvitse Eukleideen algoritmia):
   a) $2x \equiv 8\ (7)$,
   b) $4x \equiv 10\ (12)$,
   c) $5x \equiv 35\ (40)$,
   d) $3x + 5 \equiv 6x + 6\ (8)$,
   e) $765x \equiv 63\ (11)$.

2. Ratkaise seuraavat kongruenssiyhtälöt:
   a) $17x \equiv 14\ (21)$,
   b) $66x \equiv 18\ (630)$.

3. Määrää kaikki sellaiset kokonaislukuparit x ja y, että
   a) $180x + 42y = 6$,
   b) $55x + 33y = 56341235$.

4. a) Määrää joukot $\mathbb{Z}_{27}$ ja $\mathbb{Z}_{27}^*$.
   b) Miten voit esittää paremmin joukon $\mathbb{Z}_{27}$ alkiot $[325]$ ja $[-87]$?

5. Laske $\varphi(n)$, kun n on
   a) 27, b) 252, c) 2000, d) 1776.

6. a) Luku 44^{49} jaetaan luvulla 105. Mikä on jakojäännös?
   b) Määrää luvun 41^{82} kaksi viimeistä numeroa.
   c) Määrää luvun 7^{11999} kolme viimeistä numeroa.

7. Olkoon p alkuluku.
   a) Osoita, että yhtälön $x^2 \equiv 1\ (p)$ ratkaisu on $x \equiv 1\ (p)$ tai $x \equiv -1\ (p)$.
   b) Oletetaan, että p on muotoa $4n + 3$, $n \in \mathbb{N}$. Osoita, että yhtälöllä

$$x^2 \equiv -1\ (p)$$

   ei ole ratkaisua. (Vihje: Osoita ristiriita Fermat'n pienen lauseen kanssa.)