Lukuteoria ja ryhmät

Vihjeet 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) $765x \equiv 63\ (11)$.

   Vihje. Käytä Lausetta 2.30 ja Seurausta 2.31 muotoa $ax \equiv b\ (m)$, $0 \leq |a|, |b| < m$, oleviin yhtälöihin. Muulloin yhtälöä kannattaa sieventää kongruenssin laskusääntöjen avulla. Kun yhtälö on yksinkertaisimmassa muodossa, yksittäinen ratkaisu kannattaa etsiä kokeilemalla.

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

   Vihje. Suurin yhteinen tekijä kannattaa laskea ilman Eukleideen algoritmia ja tämän jälkeen sieventää yhtälöä, jos se on mahdollista. Eukleideen algoritmia kannattaa käytää lopullisen kongruenssiyhtälön ratkaisemisessa.

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

   Vihje. Yhtälöllä $ax + by = c$ on ratkaisuja vain silloin, jos $\text{syt}(a, b) \mid c$. Kun yhtälöllä on ratkaisuja, yhtälö kannattaa jakaa suurimmalla yhteisellä tekijällä $\text{syt}(a, b)$. Tämän jälkeen yhtälö kannattaa muuttaa yhden muuttujan kongruenssiyhtälöksi, jonka moduloluku on pienempi x:n ja y:n kertoimista. Jos moduloluku on y:n kerroin saat x:n ratkaistua (vastaavasti toisinpäin). Ilmoita x kongruenssin määritelmän avulla sellaisessa muodossa, jossa kongruenssia ei ole enää näkyvissä (ääretön määrä ratkaisuja) ja sijoita x ratkaistavaan yhtälöön, josta saat y:n ratkaistua.

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

   Vihje. Määritelmät 3.1 ja 3.2.

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

   Vihje. Esitä n alkulukujen potenssien tulona ja käytä Lausetta 3.6.

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.

   Vihje. Sama periaate kuin edellisen harjoituksen tehtävässä 4. Nyt vain kannattaa käyttää Lausetta 3.7 (Eulerin teoreema) apuna "potenssien pienentämisessä". Kun c)-kohdassa on edellä mainutun asian tehnyt, kannattaa miettiä, mitä hyötyä on yhtälön $7x \equiv 1\ (1000)$ ratkaisuista.

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.)

   Vihje. a) Kongruenssin määritelmää ja Apulause 2.15.
   b) Tarkastale kahta eri tapausta
      1° $\text{syt}(x, p) \neq 1$: Osoita, että $x^2 \not\equiv -1\ (p)$.
      2° $\text{syt}(x, p) = 1$: Oleta, että $x^2 \equiv -1\ (p)$. Näytä, että Fermat'n pieni lause ei ole pidä nyt paikkaansa.