Harjoitukset 8 **Lukuteoria**
tiistai 8.11.2011 16.00-17.30 MaD-302

1. *Käy läpi seuraava leikkiesimerkki RSA-algoritmista: Salaiset luvut:* $p = 11$, $q = 13$*; julkiset luvut* $m = pq = 143$ *ja avainluku* $e = 77$.
   a) *Laske tulkinta-avainluku* d.
   b) *Kryptaa sanoma 50*
   c) *Totea, että saat alkuperäisen, kun tulkitset kryptatun sanoman.*
   d) *Jos olisit alunperin tiennyt vain salausavaimen* $e = 77$*, olisitko voinut kryptata sanoman?*
      Entä olisitko (näillä luvulla e, m*) osannut murtaa koodin tuntematta salaisia lukuja* p, q*? Miten tositilanne eroaa esimerkistä?*

2. *Ratkaise liitteen 4 tehtävä 4.1.*

3. *Muuta muotoon* $D^2 \equiv a \pmod{m}$, $\quad D = ax + b$.
   a) $x^2 + 4x + 5 \equiv 0 \pmod{10}$
   b) $x^2 + 3x + 5 \equiv 0 \pmod{10}$
   c) $x^2 + 3x + 5 \equiv 0 \pmod{9}$
   d) $3x^2 + x + 5 \equiv 0 \pmod{9}$

4. *Olkoon* p *pariton alkuluku ja* $(a, p) = (b, p) = 1$*. Osoita, että jos kummallakaan kongruensseista* $x^2 \equiv a \pmod{p}$ *ja* $x^2 \equiv b \pmod{p}$ *ei ole ratkaisua, niin silloin kongruenssilla* $x^2 \equiv ab \pmod{p}$ *on ratkaisu.*

5. *Mitkä seuraavista kongruensseista ovat ratkeavia?*
   a) $x^2 \equiv 7 \pmod{101}$
   b) $x^2 \equiv -7 \pmod{101}$
   c) $x^2 \equiv 7 \pmod{303}$

6. *Mille alkuluvuille* p *on kongruenssi* $x^2 \equiv -3 \pmod{3p}$ *ratkeava?*

7. *Ratkaise lineaariset (kokonaisluku-) Diofantoksen yhtälöt:*
   a) $3x + 2y = 1$
   b) $3x - 2y = 1$
   c) $6x + 4y = 2$
   d) $17x - 43y = 100$
   e) $110x - 174y = 18$

8. *Olkoot* a, b *ja* c *positiivisia kokonaislukuja ja* $(a, b) = 1$*. Osoita, että Diofantoksen yhtälöllä* $ax + by = c$
   a) *on positiivilukuratkaisu, jos* $ab < c$,
   b) *ei ole positiivilukuratkaisua, jos* $a + b > c$.

9. *Määrää kaikki primitiiviset Pythagoraan kolmikot* (x, y, z)*, joilla* $y = 40$*. Määrää myös ei-primitiiviset.*

10. *Osoita, että Pythagoraan kolmikossa* (x, y, z) *aina*
    a) *vähintään yksi luvuista* x, y, z *on jaollinen 3:lla*
    b) *vähintään yksi luvuista* x, y, z *on jaollinen 4:lla*
    c) *vähintään yksi luvuista* x, y, z *on jaollinen 5:llä.*