Aalto-yliopisto

MS-A0401 Diskreetin matematiikan perusteet
Harjoitus 4
28.9–2.10.2015, viikko 40

Gripenberg, Potka, Pöllänen, Tuhkanen, Ääri

Palauta P-tehtävät ja vastaa S-tehtäviin viimeistään 5.10.2015 klo. 16.
Muista kirjoittaa nimesi, opiskelijanumerosi ja harjoitusryhmäsi!

P1. Kun eräs henkilö kirjoitti henkilötunnuksensa niin tulos oli $2x1189 - 321W$ missä luku x oli jäänyt niin suttuisaksi, ettei siitä saanut selvää. Mikä x on? Tarkistusmerkki W tarkoittaa, että kun tarkistusmerkkiä edeltävien numeroiden muodostama luku jaetaan luvulla 31 niin jakojäännös on 28.

Tähän kysymyksen löytyy tietenkin ratkaisu kokeilemalla, mutta tässä sinun pitää muodostaa yhtälö, josta voit ratkaista x:n ja voit käyttää hyväksi tietoa, että mod $(201\,189\,321, 31) = 3$, mod $(10\,000\,000, 31) = 20$ ja $[20]_{31}^{-1} = [14]_{31}$ ja luku $2x1\,189\,321$ kannattaa kirjoittaa muodossa $201\,189\,321 + x \cdot 10\,000\,000$.

P2. Osoita Eukleideen algoritmin avulla, että lukujen $11n + 3$ ja $7n + 2$ suurin yhteinen tekijä on 1 kaikilla $n \geq 1$.

Huom! *Kun $n = 1$ algoritmi toimii hieman eri tavalla kuin tapauksissa missä $n \geq 2$.*

P3. A haluaa lähettää viestin B:lle ja pyytää, että B lähettää oman julkisen RSA-algoritmi-avaimensa A:lle. C kuitenkin sieppaa viestin joka sisältää avaimen, joka on $(21, 5)$ ja lähettää sen sijaan A:lle oman julkisen avaimensa, joka on $(34, 11)$. Seuraavaksi A lähettää C:lle viestin, joka salattuna on 15, vaikka luulee lähettävänsä sen B:lle. C purkaa salauksen, lukee viestin, ja lähettää sen eteenpäin B:lle, nyt salattuna B:n julkisella avaimella.

Mikä on alkuperäinen viesti, ja minkä viestin C lähettää B:lle?

Huom! *Tässä on siis kyse C:n suorittamasta ns. "Man-in-the-middle"-hyökkäyksestä ja tässä tapauksessa C ainoastaan lukee viestin, ei muuta sitä.*

Vastaus: 9 ja 18

P4. Jos lasketaan mod $(13^{21}, 9)$ ja mod $(13^{22}, 9)$ Matlabilla (versio R2015a) niin tulokset ovat 7 ja 4. Mistä nähdään, että tämä tulos on väärä ja mistä virhe johtuu?

Sen sijaan lasku onnistuu seuraavalla funktiolla joka laskee mod (a^b, n):n (mutta ei esimerkiksi tarkista ovatko argumentit jotain muuta kuin positiivisia kokonaislukuja):

```
function y=pmod(a,b,n)
  y=1;
  z=mod(a,n);
  while b>0
   k=mod(b,2);
   if k==1
     y=mod(z*y,n);
   end
   z=mod(z*z,n);
   b=(b-k)/2;
  end
endfunction
```

Määritä funktio h siten, että jos $m = a^b$ missä a ja b ovat positiivisia kokonaislukuja ja lasketaan mod (m, n) komennolla `pmod(a,b,n)` niin ohjelma laskee $O(h(m))$ kertaa `mod`-funktion arvon (eikä h ole "turhan nopeasti" kasvava funktio).

Vihje: Jos mod $(13^{21}, 9) = 7$ *niin mitä silloin* mod $(13^{22}, 9)$ *tulee olemaan?*

P5. Jos sinun pitää ratkaista yhtälö $[a]_n \cdot [x]_n = [b]_n$ ja syt $(a, n) = 1$ niin käänteisalkio $[a]_n^{-1}$ on olemassa ja ratkaisu on $[x]_n = [a]_n^{-1}[b]_n$ (ja tämä ratkaisu on myös yksikäsitteinen kongruenssiluokkana). Määritä mahdolliset ratkaisut siinä tapauksessa, että syt $(a, n) = d > 1$ seuraavalla tavalla:

(a) Osoita, että jos on olemassa ratkaisu niin $d \mid b$ joten oletetaan tästä eteenpäin että näin on asian laita.

(b) Määrittele $c = a/d$ ja $m = n/d$ (jotka molemmat ovat kokonaislukuja) ja osoita, että syt $(c, m) = 1$.

(c) Määrittele $e = b/d$ (joka oletuksen mukaan on kokonaisluku). Koska syt $(c, m) = 1$ (b)-kohdan nojalla niin on olemassa luku y siten, että $[y]_m = [c]_m^{-1}$ eli $c \cdot y = 1 + k \cdot m$. Osoita, että $x = y \cdot e$ on alkuperäisen probleeman ratkaisu (osoittamalla, että $a \cdot x = b + r \cdot n$).

(d) Osoita, että myös $y \cdot e + j \cdot m$ on ratkaisu jokaisella $j \in \mathbb{Z}$, (mutta sinun ei tarvitse osoittaa, että tällä tavalla saadaan täsmälleen d eri kongruenssiluokkaa $[x]_n$).