Aalto-yliopisto

MS-A0402 Diskreetin matematiikan perusteet — Gripenberg, Ketola
Harjoitus 4
17–21.3.2014, viikko 12

Palauta P-tehtävät viimeistään 24.3.2014 kl. 16
Muista kirjoittaa nimesi, opiskelijanumerosi ja harjoitusryhmäsi!

P1. Kun A kirjoitti henkilötunnuksensa niin tulos oli $1211x9 - 510J$ missä luku x oli jäänyt niin suttuisaksi, ettei siitä voinut saada selvää. Mikä x on? Tarkistusmerkki J tarkoittaa, että kun tarkistusmerkkiä edeltävien numeroiden muodostama luku jaetaan luvulla 31 niin jakojäänös on 17.

Tähän kysymyksen löytyy tietenkin ratkaisu kokeilemalla, mutta tässä sinun pitää muodostaa yhtälö, josta voit ratkaista x:n ja voit käyttää hyväksi tietoa, että mod $(121109510, 31) = 12$, mod $(10000, 31) = 18$ ja $[18]_{31}^{-1} = [19]_{31}$ ja kannattaa kirjoittaa luvun $1211x9510$ muodossa $121109510 + x \cdot 10000$.

Vastaus: 2

P2. Osoita, että $[10^j]_{11} = [(-1)^j]_{11}$, $j \geq 0$ käyttämällä kaavaa $[m^j]_n = [m]_n^j$ kaksi kertaa. Osoita, että jos luku m kymmenjärjestelmässä kirjoitettuna on $x_k x_{k-1} \dots x_0$ niin $[m]_{11} = [x_0 - x_1 + x_2 - \dots + (-1)^k x_k]_{11}$.

Selvitä tämän tuloksen avulla onko luku $1\,213\,144\,615\,171\,819$ jaollinen 11:lla?

P3. Salaa viesti ”6” RSA-algoritmin ja julkisen avaimen $(22, 3)$ avulla. Koska 22 on hyvin pieni luku verrattuna siihen mitä sen pitäisi olla ei ole kovinkaan vaikeata määrittää yksityistä avainta. Mikä se on?

P4. Osoita Eukleideen algoritmin avulla, että lukujen $11n + 3$ ja $7n + 2$ suurin yhteinen tekijä on 1 kaikilla $n \geq 1$.

P5. Jos lasketaan mod $(11^{19}, 7)$ `matlab/octave`:lla niin tulos on 0. 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.

Vastaa Stack-tehtäviin (`stack3.aalto.fi/course/view.php?id=17`)
viimeistään 24.3.2014 kl. 16.00
