Aalto-yliopisto

MS-A0402 Diskreetin matematiikan perusteet — Gripenberg, Karvonen
Harjoitus 4
16–20.3.2015, viikko 12

Palauta P-tehtävät (ja vastaa S-tehtäviin) viimeistään 23.3.2015 klo. 16.
Muista kirjoittaa nimesi, opiskelijanumerosi ja harjoitusryhmäsi!

P1. Eräässä yliopistossa opiskelijanumerot sisältävät kuusi numeroa ja tarkistuskirjaimen. Opiskelija kirjoitti numeronsa muodossa $53x576J$ missä numero x jäi niin suttuisaksi, ettei siitä saanut selvää. Määritä x käyttämällä hyväksi tietoa, että tarkistuskirjain J tarkoittaa, että kun J:tä edeltävien numeroiden muodostama luku jaetaan 23:lla niin jakojäännös on 9 ja käytä myös hyväksi tulokset $[530576]_{23} = [12]_{23}$, $[1000]_{23} = [11]_{23}$ ja $[11]_{23}^{-1} = [21]_{23}$. (Älä siis kokeile kaikilla luvuilla $0, 1, \ldots, 9$ kunnes löydät oikean.)

Vastaus: 6

P2. Ratkaise yhtälösysteemi

$$[2]_7 \cdot [x]_7 + [3]_7 \cdot [y]_7 = [4]_7$$
$$[3]_7 \cdot [x]_7 + [5]_7 \cdot [y]_7 = [1]_7,$$

tai yhtäpitävästi, systeemi

$$2x + 3y \equiv_7 4,$$
$$3x + 5y \equiv_7 1.$$

Vihje: Jos kyseessä olisi normaali yhtälösysteemi voisit Gaussin algoritmin mukaisesti kertoa ensimmäinen yhtälö $\frac{3}{2}$:lla ja vähentää tulos jälkimmäisestä. Menettele samalla tavalla mutta nyt $\frac{3}{2}$:n paikalla on $[3]_7 \cdot [2]_7^{-1}$ jne.

Vastaus: $[x]_7 = [3]_7$ and $[y]_7 = [4]_7$.

P3. A haluaa lähettää viestin B:lle ja pyytää, että B lähettää oman julkisen RSA-algoritmi-avaimensa A:lle. C kuitenkin sieppaa tämän avaimen joka on $(14, 5)$ ja lähettää sen sijaan oman julkisen avaimensa, joka on $(22, 7)$ A:lle. Seuraavaksi A lähettää viestin, joka salattuna on 9, C:lle 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?

Vastaus: 3 ja 5

P4. Osoita Eukleideen algoritmin avulla, että lukujen $24n+7$ ja $17n+5$ suurin yhteinen tekijä on 1 kaikilla $n \geq 1$.

P5. Jos lasketaan mod $(11^{19}, 7)$ ja mod $(11^{20}, 7)$ Matlabilla (versio R2014b) niin tulokset ovat 1 ja 3. 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.

Vihje: Jos mod $(11^{19}, 7) = 1$ *niin mitä silloin* mod $(11^{20}, 7)$ *tulee olemaan?*