Aalto-yliopisto

MS-A0401 Diskreetin matematiikan perusteet GG, EH, TH, PK, JT, LT, VÄ
Harjoitus 4
3–7.10.2016, viikko 40

Palauta P-tehtävät ja vastaa S-tehtäviin viimeistään 10.10.2016 klo. 16.
Muista kirjoittaa nimesi, opiskelijanumerosi ja harjoitusryhmäsi!

P1. Osoita induktiolla, että lukujen $2^{(2^n)}+2$, $n \geq 2$ desimaaliesitys päättyy aina numeroon 8.

Vihje: Formuloi ensin väite muodossa $[2^{(2^n)}]_{10} = [\text{"jotain"}]_{10}$ *ja käytä laskusääntöjä* $2^{k+1} = 2^k + 2^k$ *ja* $[x \cdot y]_{10} = [x]_{10} \cdot [y]_{10}$ *induktioaskeleen todistuksessa.*

P2. Ratkaise yhtälösysteemi

$$[2]_5 \cdot [x]_5 + [4]_5 \cdot [y]_5 = [2]_5$$
$$[3]_5 \cdot [x]_5 + [2]_5 \cdot [y]_5 = [0]_5.$$

Vihje: Jos kyseessä olisi normaali yhtälösysteemi voisit Gaussin algoritmin mukaisesti kertoa ensimmäinen yhtälö $\frac{3}{2}$*:lla ja vähentää tulos jälkimmäisestä, jonka jälkeen voisit ratkaista* y*:n, tai voisit ratkaista* x*:n ensimmäisestä yhtälöstä ja sitten sijoittaa tuloksen jälkimmäiseen yhtälöön jne. Menettele samalla tavalla mutta nyt esimerkiksi* $\frac{3}{2}$*:n paikalla on* $[3]_5 \cdot [2]_5^{-1}$ *ja* $\frac{1}{2}$*:n paikalla on* $[2]_5^{-1}$ *jne.*

Vastaus: $[x]_5 = [y]_5 = [2]_5$.

P3. Kun A kirjoitti henkilötunnuksensa niin tulos oli $1211x9 - 510J$ missä numero 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 jakojäännös on 17.

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

Vastaus: 2

P4. A haluaa lähettää viestin B:lle ja pyytää B:ltä, että hän lähettää 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?

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: 3 *ja* 5

P5. Olkoon $k \in \mathbb{Z}$. Osoita Eukleideen algoritmin avulla, ettei murtolukua

$$\frac{8 \cdot k + 3}{5 \cdot k + 2},$$

voi supistaa eli että osoittajan ja nimittäjän ainoa yhteinen (positiivinen) tekijä on 1.

Vihje: Tarkastele erikseen tapaukset $k \geq 1$, $k = 0$, $k = -1$ *ja* $k \leq -2$ *ja muista, että* $\text{syt}\,(m, n) = \text{syt}\,(|m|, |n|)$.