TÖL104G
Stærðfræðimynstur í tölvunarfræði
Verkefnablað 7 — Lausn

11. október 2015

1. (25%) Þáttið eftirfarandi tölur í prímþætti. Fyrir hverja tölu n skuluð þið skrifa jöfnu á sniðinu $n = p_1^{v_1} \cdot \ldots \cdot p_k^{v_k}$ þar sem $p_1, \ldots, p_k$ eru mismunandi prímtölur í vaxandi röð.

   Til dæmis, ef talan væri 54 þá ættuð þið að skrifa $54 = 2^1 \cdot 3^3$.

   a) $n = 6$ **Svar:** $6 = 2^1 \cdot 3^1$

   b) $n = 256$ **Svar:** $256 = 2^8$

   c) $n = 257$ **Svar:** $257 = 257^1$

   d) $n = 81$ **Svar:** $81 = 3^4$

   e) $n = 1000$ **Svar:** $1000 = 2^3 \cdot 5^3$

   f) $n = 1000000$ **Svar:** $1000000 = 2^6 \cdot 5^6$

   g) $n = 15360$ **Svar:** $15360 = 2^{10} \cdot 3^1 \cdot 5^1$

   h) $n = 697$ **Svar:** $697 = 17^1 \cdot 41^1$

   i) $n = 512$ **Svar:** $512 = 2^9$

   j) $n = 2310$ **Svar:** $2310 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1$

2. (25%) Reiknið $123^{33} \pmod{257}$ með algríminu fyrir mátaða veldishafningu sem finna má á einni glæru viku 6. Sýnið gildin á p, q og r fyrir hverja umferð lykkjunnar.

   Svar: Svarið er 134. Tafla 1 á næstu síðu sýnir gildin þegar búið er að fara n umferðir frá því fyrir fyrstu umferð ($n = 0$) þar til eftir síðustu umferð ($n = 7$, þegar $r = 0$).

n	p	q	r
0	1	123	33
1	123	123	32
2	123	223	16
3	123	128	8
4	123	193	4
5	123	241	2
6	123	256	1
7	134	256	0

Tafla 1: Útreikningur á $123^{33} (\text{mod } 257)$

3. (25%) Fyrir eftirfarandi köll á fallið „mátaðveldi“ fyrir mátaða veldishafningu, sem finna má á glærum viku 6, hve oft er framkvæmd margföldun? Með öðrum orðum hve oft samanlagt í hverju kalli eru gildisveitingarnar $p := p \cdot q \mod m$ og $q := q^2 \mod m$ framkvæmdar?
   a) mátaðveldi(11,111,1111); **Svar:** 12
   b) mátaðveldi(7,11,111); **Svar:** 6
   c) mátaðveldi(7,32,65537); **Svar:** 6
   d) mátaðveldi(7,33,65537); **Svar:** 7
   e) mátaðveldi(7,31,65537); **Svar:** 9
   f) mátaðveldi(7,1024,65537); **Svar:** 11
   g) mátaðveldi(7,1024·1024,65537); **Svar:** 21
   h) mátaðveldi(7,512,65537); **Svar:** 10
   i) mátaðveldi(7,513,65537); **Svar:** 11
   j) mátaðveldi(7,511,65537); **Svar:** 17

4. (25%) Sannið setningarnar tvær á glærunni um eiginleika deilanleika sem ekki eru sannaðar þar, þ.e. eftirfarandi setningar:
   a) Setning: Látum a, b og c vera heiltölur, $a \neq 0$. Ef $a \mid b$ þá $a \mid bc$.

      Sönnun: Þar eð $a \mid b$ er, samkvæmt skilgreiningu á deilanleika, til heiltala k þannig að $ka = b$. Þarmeð gildir $kac = bc$ (með því að margfalda með c báðu megin). Þess vegna er bc margfeldi af a, sem er skilgreiningin á að $a \mid bc$.
   b) Setning: Látum a, b og c vera heiltölur, $a \neq 0$. Ef $a \mid b$ og $b \mid c$ þá $a \mid c$.

      Sönnun: Þar eð $a \mid b$ er, samkvæmt skilgreiningu á deilanleika, til heiltala k_1 þannig að $k_1 a = b$. Þar eð $b \mid c$ er, samkvæmt skilgreiningu á deilanleika, til heiltala k_2 þannig að $k_2 b = c$. Setjum því $k_1 a$ í stað

b í seinni jöfnunni og fáum $k_2 k_1 a = c$. Þarmeð er c margfeldi af a og því gildir $a \mid c$.