TÖL 104G

Stærðfræðimynstur í tölvunarfræði
Einstaklingverkefni viku: 7

Nemandi:
Rakel María Brynjólfsdóttir

Póstfang:
rmb3@hi.is

Dæmi 1: Þáttið eftirfarandi tölur í prímþætti.

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

b) n = 256 $256 = 2^8$

c) n = 257 $257 = 257^1$

d) n = 81 $81 = 3^4$

e) n = 1 000 $1000 = 2^3 \cdot 5^3$

f) n = 1 000 000 $1\,000\,000 = 2^6 \cdot 5^6$

g) n = 15 360 $15\,360 = 2^{10} \cdot 3^1 \cdot 5^1$

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

i) j = 2 310 $2\,310 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1$

Dæmi 2: Reiknið $123^{33} \pmod{257}$ með algríminu fyrir mátaða veldishafningu, sýnið gildin á *p*, *g* og *r* fyrir hverja umferð lykkjunar.

Upphafsgildi:
p: 1 q: 123 r: 33

Lykkja númer:

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

Svar: $123^{33} \pmod{257} = 134$

Dæmi 3: Fyrir eftirfarandi köll á fallið “mátaðveldi” fyrir mátaða veldishafningu, hve oft er framkvæmd margföldun?

a) mátaðveldi(11,111,1111) : 12
b) mátaðveldi(7,11,111) : 6
c) mátaðveldi(7,32,65537) : 6
d) mátaðveldi(7,33,65537) : 7
e) mátaðveldi(7,31,65537) : 9
f) mátaðveldi(7,1024,65537) : 11
g) mátaðveldi(7,1024·1024,65537) : 21
h) mátaðveldi(7,512,65537) : 10
i) mátaðveldi(7,513,65537) : 11
j) mátaðveldi(7,511,65537) : 17

Dæmi 4: Sannið setningarnar.

a) Þar sem $a \mid b$ er til heiltala n þannig að $b = na$. Þá fæst $bc = nac$ sem hægt er að skrifa $bc = (nc)a$ og því er bc margfeldi a.

b) Þar sem $a \mid b$ er til heiltala n þannig að $b = na$. Þar sem $b \mid c$ er til heiltala m þannig að $c = mb$. Þá fæst að $b = na$ og $b = c/m$, þá getum við skrifa $na = c/m$ og því er $c = mna$ sem hægt er að skrifa $c = (mn)a$ og því er c margfeldi a.