Bevezetés a Számításelméletbe II.

12. gyakorlat

1. A 8. feladatsor 4. és 10. feladatát oldjuk meg most az euklideszi algoritmus segítségével.

2. Az (angol) ábécé huszonhat betűjét a $0, 1, \ldots 25$ számokkal helyettesítem ($A = 0$, $B = 1$, $C = 2$, stb., $Z = 25$). Nyilvános kódolófüggvényem:

$$x \mapsto x^{43} \qquad (\mathrm{mod}\, 85).$$

(Ezzel a $0, 1, \ldots, 84$ számokat lehet kódolni, de csak az első huszonhat számnak van valódi jelentése.) Ezzel a függvénnyel kódoltam titkos üzenetemet is:

$$59 \quad 2 \quad 59 \quad 20 \quad 44 \quad 52$$

Törd fel a kódomat, vagyis készíts a fenti kódolófüggvényhez dekódolófüggvényt, majd fejtsd meg vele titkos üzenetemet!

3. A nyilvános kulcsú titkosírás dekódoló kulcsának működése a következő állításon alapszik: ha x és n adottak, akkor

$$x^{k\cdot\varphi(n)+1} \equiv x \qquad (\mathrm{mod}\, n)$$

teljesül tetszőleges k pozitív egészre. Ez az állítás könnyen bizonyítható, ha az Euler-Fermat tételből nyert $x^{\varphi(n)} \equiv 1 \pmod{n}$ összefüggést k-adik hatványra emeljük, majd x-szel szorozzuk. Azonban az Euler-Fermat tétel alkalmazásához szükség van arra is, hogy $(x, n) = 1$ teljesüljön.

Bizonyítsd be, hogy ha n két különböző prím szorzata (és a nyilvános kulcsú titkosírásnál ez a helyzet), akkor a fenti állítás teljesüléséhez nincs szükség arra, hogy $(x, n) = 1$ igaz legyen!

4. Bizonyítsd be, hogy 561 ($= 3 \cdot 11 \cdot 17$) Carmichael-szám!

5. Legyen A egy egyszerű irányítatlan gráf szomszédossági mátrixa. Mutassuk meg, hogy A^2 főátlóbeli elemeit összeadva páros számot kapunk!

6. Legyen A az n csúcsú G egyszerű irányítatlan gráf szomszédossági mátrixa. Mutassuk meg, hogy ha $A^2 + A$ minden eleme pozitív, akkor G összefüggő!

7. Mennyi az irányított 3 hosszú kör illeszkedési mátrixának rangja?

8. Legyen G egy legalább 3 pontú csillag. Mennyi a determinánsa a G gráf szomszédossági mátrixának?

9. Hogyan tudjuk eldönteni egy gráf szomszédossági mátrixának hatványai alapján, hogy páros-e?

http://amanita-design.net/samorost-1/
http://amanita-design.net/samorost-2/