Bevezetés a számításelméletbe II.

2010. Április 19.

9. gyakorlat: Számelmélet

1. Egy perzsa sahnak 100 felesége van, a börtönében is épp 100 rab sínylődik, 1-től 100-ig számozott cellákban. A börtöncellák zárjai "kétállásúak": ha egyet fordítanak rajtuk, a bezárt ajtó kinyílik, a nyitott ajtó bezáródik. A sah születésnapján a 100 feleség végigvonul a börtönön és a zárakkal játszanak. Az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján egyet fordít, stb., a k-adik feleség minden k-adik ajtó zárján egyet fordít, egészen a 100. feleségig. Végül azok a rabok, akiknek az ajtaja nyitva van, kiszabadulnak. Milyen sorszámú cellákban laknak a szerencsések?

2. Melyek azok a pozitív p prímszámok, melyre
   (a) $p + 10$ és $p + 14$ is prím,
   (b) $p^2 + 2$ is prím,
   (c) $p^2 + 4$ és $p^2 + 6$ is prím?

3. Számítsd ki a 84 és 270 legnagyobb közös osztóját az Euklideszi algoritmus segítségével!

4. Bizonyítsd be, hogy a szomszédos *Fibonacci-számok* relatív prímek! De vajon mennyi a másodszomszédos Fibonacci-számok legnagyobb közös osztója?

5. Melyik az a legkisebb 3-mal nem osztható szám, melynek 15 osztója van?

6. Mennyi $\phi(9)$, $\phi(133)$, $\phi(540)$, $\phi(7!)$?

7. Az Euler-féle ϕ függvény tulajdonságait felhasználva,
   (a) bizonyítsuk be, hogy $11 \mid n^{11} + 10n$,
   (b) igazoljuk, hogy ha n nem osztható 17-tel, akkor $n^8 + 1$ vagy $n^8 - 1$ biztosan osztható 17-tel,
   (c) számítsuk ki 108^{182} maradékát 19-cel osztva,
   (d) bizonyítsuk be, hogy $42 \mid n^7 - n$.

8. Kiszámítandó $(((43)^{43})^{43})^{43}$ modulo 49.

9. Határozzuk meg az utolsó
   (a) három számjegyét 403^{402}-nek,
   (b) számjegyét $7^{6^{5^{4^{3^2}}}}$-nek!