Számítástudomány alapjai

11. gyakorlat – *Számelmélet* – 2008. 11. 13.

http://www.cs.bme.hu/~peresz/sza/

1. (12.1.1) Számítsuk ki az euklideszi algoritmus segítségével 504 és 372 legnagyobb közös osztóját!

2. (12.1.2) Ha b osztója a-nak, mik a lehetséges értékei a $d(a, a+b)$, és a $d(2a, a-b)$ legnagyobb közös osztóknak? ($d(a,b)$ a és b legnagyobb közös osztóját jelenti.)

3. (12.1.3) Az $a_1, a_2, \ldots$ számok relatív prímek, ha nincs olyan egynél nagyobb szám, mely mindegyiknek osztója lenne. Mutasson három olyan relatív prímszámot, melyek közül semelyik kettő nem relatív prím!

4. (12.1.4) Bizonyítsa be, hogy ha $d(a,4) = d(b,4) = 2$ akkor $a+b$ osztható 4-gyel!

5. (12.1.5) Legyen a és b páratlan. Mennyi $d(a^2+b^2, 4)$?

6. (12.1.9) Bizonyítsuk be, hogy minden a, b egészre $d(ab) \le d(a)d(b)$ és egyenlőség pontosan akkor teljesül, ha a és b relatív prímek! ($d(a)$: a osztóinak a száma)

7. (ZH, 2005) Bizonyítsuk be, hogy ha az $n > 1$ számnak 2005 osztója van, akkor n nem lehet egy egész szám 5-dik hatványa!

8. (ZH, 1999) Relatív prím-e a következő két szám: $2^{100} - 1$ és $3^{100} - 1$?

Megoldások

Ezek csak vázlatos megoldások. Ennyi indoklás a ZHn nem elég!

1. $504 = 1 \cdot 372 + 132$
   $372 = 2 \cdot 132 + 108$
   $132 = 1 \cdot 108 + 24$
   $108 = 4 \cdot 24 + 12$
   $24 = 2 \cdot 12$
   Azaz $d(504,372) = 12$.
2. $a = qb$
   $d(a, a+b) = d(qb, (q+1)b) = b \cdot d(q, q+1) = b$, mert $d(q, q+1) = 1$.
   $d(2a, a-b) = d(2qb, qb-b) = b \cdot d(2q, q-1) = bx$
   $x \mid 2q$ és $x \mid q-1 \Rightarrow x \mid 2q-(q-1) \Rightarrow x \mid q+1 \Rightarrow x \mid q+1-(q-1) \Rightarrow x \mid 2$, tehát $x = 1$ vagy $x = 2$. Itt azt használtuk, hogy ha *x* osztója két számnak, akkor osztója a különbségüknek is.
   Ha *q* páratlan, akkor $x = 2$, ha páros, akkor $x = 1$.
3. $a_1 = 2 \cdot 3$, $a_2 = 5 \cdot 3$, $a_3 = 5 \cdot 2$
4. $d(a,4) = 2 \Rightarrow$ *a* páros, de nem osztható 4-gyel, azaz 4-gyel osztva 2-t ad maradékul. Ugyanígy *b* is, amiből már következik az állítás.
5. Mivel *a* páratlan, 4-gyel osztva 1 vagy 3 maradékot ad. Azaz a^2 $1^2 = 1$-et vagy $3^2 = 9$-et, ami 4-gyel osztva szintén 1. Tehát a^2 1-et ad maradékul és ugyanez igaz b^2-re is. Ekkor $d(a^2 + b^2, 4) = 2$.
6. $x = d(a)d(b)$
   $y = d(ab)$
   a és *b* kanonikus alakja legyen: $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$. Ebből $x = \prod_{i=1}^{n} (\alpha_i + 1) \prod_{j=1}^{m} (\beta_j + 1)$. Ha *a* és *b*-nek nincs közös prímosztója, akkor *ab* kanonikus alakja $ab = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$, és így $x = y$.
   Egyébként ha pl. $p_i = q_j$, akkor *ab* kanonikus alakjában $p_i^{\alpha_i + \beta_j}$ van, azaz *y*-ban $\alpha_i + \beta_j + 1$ szerepel szorzótényezőként $(\alpha_i + 1)(\beta_j + 1) = \alpha_i \beta_j + \alpha_i + \beta_j + 1$ helyett.
   Mivel $\alpha_i + \beta_j + 1 < \alpha_i \beta_j + \alpha_i + \beta_j + 1$, ebből már következik az állítás.
7. Indirekt tegyük fel, hogy $d(n) = 2005$ és $n = m^5$. *m* kanonikus alakja: $m = \prod_{i=1}^{k} p_i^{\alpha_i}$.
   Ekkor *n* kanonikus alakja: $n = \prod_{i=1}^{k} p_i^{5\alpha_i}$. Ebből $d(n) = 2005 = \prod_{i=1}^{k} (5\alpha_i + 1)$. A jobb oldalon 5-tel nem osztható számok szorzata áll, 2005 pedig osztható 5-tel, ami ellentmondás.
8. Nem, mert 5 közös osztó. Ehhez az kell, hogy 10-es számrendszerben az utolsó számjegy 0 vagy 5, tehát a kérdés az hogy: $2^{100} - 1 \equiv ? \pmod{10}$
   Ehhez írjuk fel 2 hatványait egy ideig:
   $2^1 \equiv 2 \pmod{10}$

$2^2 \equiv 4 \pmod{10}$

$2^3 \equiv 8 \pmod{10}$

$2^4 \equiv 6 \pmod{10}$

$2^5 \equiv 2 \pmod{10}$

$2^6 \equiv 4 \pmod{10}$

…

Azaz 4-től a maradékok 4-esével ismétlődnek. Ebből:

$2^{100} \equiv 2^4\left(2^4\right)^{24} \equiv 2^4 \equiv 6 \pmod{10}$. Azaz $2^{100}-1$ utolsó jegye 5.

Hasonlóan végigcsinálva 3-ra látható, hogy $3^{100}-1$ utolsó jegye 0.