Számelmélet ZH megoldások

2005 december 1.

1. Számoljuk ki a 11 413 és a 10 403 számok legnagyobb közös osztóját és adjuk meg a $11\,413x + 10\,403y = (11\,413, 10\,403)$ diofantikus egyenlet egy megoldását!

   Megoldás:
   Euklideszi algoritmussal számolva kapjuk, hogy

   $$\begin{array}{rcl|cc|} & & & 11\,413\cdot x & + \quad 10\,403\cdot y \\ 11\,413 & = & 10\,403\cdot 1 + 1010 & 1 & 0 \\ 10\,403 & = & 1\,010\cdot 10 + 303 & 0 & 1 \\ 1\,010 & = & 303\cdot 3 + 101 & 1 & -1 \\ 303 & = & 101\cdot 3 & -10 & 11 \\ 101 & & & 31 & -34 \\ \end{array}$$

   azaz a legnagyobb közös osztó 101 és $11\,413\cdot 31 + 10\,403\cdot(-34) = 101$.

2. Keressük meg az

   $$x^5 + x^2 + x + 1 \equiv 0 \quad (27)$$

   kongruencia összes megoldását!

   Megoldás:
   Miután $27 = 3^3$, ezért oldjuk meg először modulo 3. Az $x_1 \equiv 0\ (3)$ nem megoldás, ezért $(x_1, 3) = 1$ minden megoldásra, tehát az $x_1^2 \equiv 1\ (3)$ azonosságot kihasználva $0 \equiv x_1^5 + x_1^2 + x_1 + 1 \equiv x_1 + 1 + x_1 + 1 \equiv 2x_1 + 2\ (3)$, így $x_1 \equiv 2\ (3)$.

   Keressük $x^5 + x^2 + x + 1 \equiv 0\ (3^2)$ megoldását $x_2 = x_1 + 3y$ alakban. Legyen $f(x) = x^5 + x^2 + x + 1$, így az egyenlet

   $$\begin{aligned} 0 &\equiv f(2+3y) \equiv f(2) + 3yf'(2) \quad (3^2), \text{ azaz} \\ 0 &\equiv \frac{f(2)}{3} + yf'(2) \quad (3). \end{aligned}$$

   Miután $f(2) \equiv 3\ (3^2)$ és $f'(2) \equiv 1\ (3)$, azt kaptuk, hogy $0 \equiv 1 + y\ (3)$, amiből $y \equiv 2\ (3)$, tehát $x_2 \equiv 2 + 3\cdot 2 = 8\ (3^2)$.

   Végül $x^5 + x^2 + x + 1 \equiv 0\ (3^3)$ megoldásához legyen $x_3 = x_2 + 3^2y$, így $0 \equiv f(8) + 3^2yf'(8)\ (3^3)$. Nyilván $f'(8) \equiv f'(2) \equiv 1\ (3)$, továbbá $f(8) \equiv 9\ (3^3)$, tehát az egyenlet $0 \equiv 9 + 3^2y\ (3^3)$, azaz $0 \equiv 1 + y\ (3)$. Ezek szerint ismét $y \equiv 2\ (3)$, tehát $x_3 \equiv 8 + 3^2\cdot 2 = 26\ (3^3)$. A Hensel-felemelésről szóló tétel szerint más megoldása nem lehet a kongruenciának.

   Lehettünk volna ügyesebbek is, látható ugyanis, hogy -1 gyöke $f(x)$-nek. Miután kiszámoltuk, hogy modulo 3 egyetlen megoldás ($x_1 \equiv 2\ (3)$) van, továbbá hogy $f'(x_1) \not\equiv 0\ (3)$, már tudjuk az előbb említett tételből, hogy modulo 3^n is egyetlen megoldás van, ami csak -1 lehet.

3. Mennyi 13 rendje modulo 49?

   Megoldás:
   Tudjuk, hogy $o_{49}(13) \mid \varphi(49) = 42$, ezért $42 = 2\cdot 3\cdot 7$ osztóival kell csak próbálkoznunk. $13^2 \equiv 22\ (49)$, $13^3 \equiv -8\ (49)$, $13^6 \equiv 15\ (49)$, $13^7 \equiv -1\ (49)$. Utóbbiból $13^{14} \equiv 1\ (49)$, tehát $o_{49}(13) = 14$.

4. Keressünk primitív gyököt modulo 50. Határozzuk meg az

   $$x^{26} \equiv 31 \quad (50)$$

   összes megoldását.

   Megoldás:
   $\varphi(50) = 20$, tehát olyan elemet keresünk, aminek 20 a rendje modulo 50. A 3 jó is lesz: $3^2 \equiv 9\ (50)$, $3^4 \equiv 31\ (50)$, $3^5 \equiv -7\ (50)$ és $3^{10} \equiv -1\ (50)$.

   Ha $x = 3^y$, akkor az egyenlet $3^{26y} \equiv 3^4\ (50)$, tehát $26y \equiv 4\ (20)$, azaz $3y \equiv 2\ (10)$, $y \equiv 4\ (10)$. Tehát $y \equiv 4\ (20)$ vagy $y \equiv 14\ (20)$, ezért $x \equiv 3^4 \equiv 31\ (50)$ vagy $x \equiv 3^{14} = 3^4\cdot 3^{10} \equiv -31\ (50)$.

5. Adjuk meg azt a legkisebb z pozitív egész számot, amelyre

$$\sum_{a=1}^{17}(a^2-13)^{16} \equiv z \pmod{17}.$$

Megoldás:
A kis Fermat-tétel szerint $(a^2-13)^{16} \equiv 1 \pmod{17}$, ha $a^2-13 \not\equiv 0 \pmod{17}$. Miután

$$\left(\frac{13}{17}\right) = \left(\frac{-4}{17}\right) = \left(\frac{-1}{17}\right)\cdot\left(\frac{2}{17}\right)^2 = (-1)^{\frac{17-1}{2}} = 1,$$

ezért 13 négyzetelem, amiből következik, hogy pontosan két olyan $a \in \{1,2,\ldots,17\}$ szám van, amire $a^2 \equiv 13 \pmod{17}$. Erre a két a-ra $(a^2-13)^{16} \equiv 0 \pmod{17}$. Ezek szerint két nullát és 15 egyest adunk össze, azaz $z \equiv 15 \pmod{17}$.

6. Határozzuk meg az összes olyan $m \geq 2$ egész számot, amely rendelkezik a következő tulajdonsággal:

$$\text{ha } a \in \mathbb{Z},\ a \not\equiv 0 \pmod{m} \text{ akkor minden } n \in \mathbb{N} \text{ esetén } a^n \not\equiv 0 \pmod{m}.$$

Megoldás:
A négyzetmentes számokra igaz a fenti tulajdonság. Ha ugyanis m négyzetmentes, akkor $a \not\equiv 0$ (m)-ből következik, hogy m valamelyik p prímosztója nem osztja a-t. Ekkor viszont a semelyik hatványát nem osztja p, tehát m sem.

Ha pedig m nem négyzetmentes, mondjuk $p^2 \mid m$, akkor például $a = \frac{m}{p}$ egész, amelyet nem oszt m, de $a^2 = m\cdot\frac{m}{p^2} \equiv 0 \pmod{m}$, hiszen $\frac{m}{p^2}$ egész szám.

7. Mutassuk meg, hogy $(m_1,m_2)=d$ esetén az $x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$ kongruenciarendszer akkor és csak akkor oldható meg, ha $c_1 \equiv c_2 \pmod{d}$.
(Segítség: ha $c_1 \equiv c_2 \pmod{d}$, akkor mutassuk meg, hogy a $dy \equiv d \pmod{m_1}$, $dy \equiv 0 \pmod{m_2}$ rendszer megoldható és $x = y(c_1-c_2)+c_2$ megoldása az eredeti kongruenciáknak.)

Megoldás:
Tegyük fel, hogy a kongruenciarendszer megoldható, x egy megoldás. Ekkor $x \equiv c_i \pmod{m_i}$ és $d \mid m_i$ miatt $x \equiv c_i \pmod{d}$ is, tehát $c_1 \equiv x \equiv c_2 \pmod{d}$, azaz a feltétel szükséges.

Megfordítva, legyen $d \mid c_1-c_2$. Az útmutatás szerint eljárva tekintsük a $dy \equiv d \pmod{m_1}$, $dy \equiv 0 \pmod{m_2}$ kongruenciarendszert. Mindkettőt leosztva d-vel, azt kapjuk, hogy $y \equiv 1 \pmod{\frac{m_1}{d}}$, $y \equiv 0 \pmod{\frac{m_2}{d}}$, ami megoldható a kínai maradéktétel szerint, hiszen $(\frac{m_1}{d},\frac{m_2}{d})=1$. Legyen $x = y(c_1-c_2)+c_2 = yd\cdot\frac{c_1-c_2}{d}+c_2$. Miután $\frac{c_1-c_2}{d}$ egész szám a feltétel szerint, így $dy \equiv d \pmod{m_1}$ miatt $x \equiv d\cdot\frac{c_1-c_2}{d}+c_2 = c_1 \pmod{m_1}$ és $dy \equiv 0 \pmod{m_2}$ miatt $x \equiv 0\cdot\frac{c_1-c_2}{d}+c_2 = c_2 \pmod{m_2}$. Ezzel beláttuk, hogy x valóban megoldása a kongruenciarendszernek.

Az egyértelműségről a következő mondható:
Ha x_1 megoldás, akkor $x_2 \in \mathbb{Z}$ pontosan akkor megoldás, ha $x_1 \equiv x_2 \pmod{D}$, ahol $D=[m_1,m_2]$. Ha ugyanis x_1 és x_2 megoldások, akkor $x_1-x_2 \equiv c_i-c_i = 0 \pmod{m_i}$, amiből következik, hogy x_1-x_2 osztható m_1 és m_2 legkisebb közös többszörösével is. Ha pedig x_1 megoldás és $x_2 \equiv x_1 \pmod{D}$, akkor persze $x_2 \equiv x_1 \pmod{m_i}$ is, amiből látszik, hogy x_2 is megoldás.