Számelmélet 1. ZH megoldások

2006 november 7.

1. Adjuk meg a $66\,049x + 32\,639y = 7\,967$ diofantikus egyenlet egy egész megoldását.

   Megoldás:
   Euklideszi algoritmussal számolva kapjuk, hogy

$$\begin{array}{rcl|cc|} & & & 66\,049\cdot x & + \quad 32\,639\cdot y \\ 66\,049 & = & 32\,639\cdot 2+771 & 1 & 0 \\ 10\,403 & = & 771\cdot 42+257 & 0 & 1 \\ 771 & = & 257\cdot 3+0 & 1 & -2 \\ 257 & & & -42 & 85 \end{array}$$

   azaz a legnagyobb közös osztó 257 és $66\,049\cdot(-42)+32\,639\cdot 85 = 257$. Miután $\frac{7\,967}{257} = 31$, ezért az utóbbi egyenletet 31-gyel szorozva kapjuk a megoldást: $x = -42\cdot 31 = -1302$ és $y = 85\cdot 31 = 2635$.

2. Melyik az a legkisebb pozitív egész x szám, amelyre

$$x \equiv 13^{11^{17}} \quad (9)$$

   teljesül.

   Megoldás:
   Miután $\varphi(9) = 6$ és $11^{17} \equiv (-1)^{17} = -1$ (6), ezért $13^{11^{17}} \equiv 13^{-1} \equiv 4^{-1}$ (9), tehát 4 modulo 9 inverzét kell kiszámolni: $4\cdot 2 = 8 \equiv -1$ (9), azaz $4^{-1} \equiv -2 \equiv 7$ (9), $x = 7$.

3. Keressük meg a

$$39x^5 \equiv 8 \quad (7)$$

   és a

$$39x^5 \equiv 8 \quad (19)$$

   kongruenciák összes megoldásait (külön-külön a kettőt).

   Megoldás:
   Ha $39x^5 \equiv 8$ (7), akkor $4x^5 \equiv 1$ (7), így $x^5 \equiv 2$ (7). Mivel $3^2 \equiv 2$ (7), $3^3 \equiv -1$ (7), és $\varphi(7) = 6$, ezért a 3 primitív gyök modulo 7. Ha bevezetjük az $y = \mathrm{ind}_3\, x$ új változót, akkor az egyenletünk $3^{5y} \equiv 3^2$ (7), tehát $5y \equiv 2$ (6). Innen $y \equiv 4$ (6), $x \equiv 3^4 \equiv -3$ (7).

   Ha $39x^5 \equiv 8$ (19), akkor $x^5 \equiv 8$ (19). Mivel 2 primitiv gyök modulo 19 és $\mathrm{ind}_2\, 8 = 3$, tehát ha $x = 2^y$, akkor $5y \equiv 3$ (18). Ezt megoldva kapjuk, hogy $y \equiv 15$ (18), azaz $x \equiv 2^y = 2^{15} \equiv -2^6 \equiv -7$ (19).

4. Adjuk meg a

$$39x^5 \equiv 8 \quad (931)$$

   kongruencia összes megoldását! (Segítség: $931 = 7^2\cdot 19$)

   Megoldás:
   Tanultuk, hogy a megadott kongruencia megoldása ekvivalens a $39x^5 \equiv 8$ (7^2), $39x^5 \equiv 8$ (19) kongruenciarendszer megoldásával. Ehhez a $39x^5 \equiv 8$ (7) kongruencia előző feladatban kiszámolt megoldását fogjuk felemelni modulo 7^2 megoldássá.

   Legyen $f(x) = 39x^5 - 8$. Ekkor $f'(x) = 195x^4 \equiv -x^4$ (7), innen $f(-3) \equiv 21$ (49) és $f'(-3) \equiv 3$ (7). Tehát az $x = -3 + 7y$ alakú megoldásokra felírhatjuk a

$$0 \equiv f(-3) + 7y\cdot f'(-3) \quad (49)$$

   egyenletet. Héttel leosztva és $f(-3)$, $f'(-3)$-at behelyettesítve:

$$0 \equiv 3 + 3y \quad (7),$$

   tehát $y \equiv -1$ (7), azaz $x = -3 - 7 = -10$ a keresett megoldás modulo 49.

Az eredeti $39x^5 \equiv 8 \ (931)$ egyenlet megoldásait úgy kapjuk, hogy kínai maradéktétellel összerakjuk a modulo 49 és a modulo 19 megoldásokat. Tehát meg kell oldanunk az

$$\begin{aligned} x &\equiv -10 \quad (49) \\ x &\equiv -7 \quad (19) \end{aligned}$$

rendszert. A megoldáshoz az euklideszi algoritmus segítségével kapjuk, hogy $49 \cdot 7 + 19 \cdot (-18) = 1$, tehát $19^{-1} \equiv -18 \ (49)$ és $49^{-1} \equiv 7 \ (19)$. Innen $x \equiv 49 \cdot 7 \cdot (-7) + 19 \cdot (-18) \cdot (-10) \equiv 88 \ (931)$.

5. Egy k számot köbmentesnek nevezünk, ha $m^3 \mid k$-ból következik $m = \pm 1$. Mutassuk meg, hogy ha $n \in \mathbb{N}^+$, akkor n egyértelműen bontható fel egy pozitív köbmentes szám és egy pozitív harmadik hatvány szorzatára. (Tehát létezik $k \in \mathbb{N}^+$ köbmentes és m természetes szám, hogy $n = k \cdot m^3$, továbbá k és m egyértelmű.)

   Megoldás:
   Először is vegyük észre, hogy k pontosan akkor köbmentes, ha minden $p \mid k$ prímszám legfeljebb második hatványon szerepel kanonikus alakjában.

   Legyen $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, ahol p_i prímek különbözőek és legyen $\beta_i = \left\lfloor \frac{\alpha_i}{3} \right\rfloor$, $\gamma_i = \alpha_i - 3\beta_i$. Ekkor $m = \prod_{i=1}^{r} p_i^{\beta_i}$ és $k = \prod_{i=1}^{r} p_i^{\gamma_i}$ a kívánt felbontást adja:
   $k \cdot m^3 = n$, mert minden i-re $\gamma_i + 3\beta_i = \alpha_i$,
   k köbmentes, mert $\gamma_i < 3$.

   Egyértelműség:
   Tegyük fel, hogy $n = k \cdot m^3$. Megmutatjuk, hogy k és m csak a fent definiált lehet. Miután m és k is osztója n-nek, ezért m és k kanonikus alakjában ugyanazok a prímek fordulhatnak elő, mint n felbontásában. Legyen tehát n, k és m kanonikus alakja $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, $k = \prod_{i=1}^{r} p_i^{\gamma_i}$ és $m = \prod_{i=1}^{r} p_i^{\beta_i}$, ahol természetesen $\beta_i = 0$ és $\gamma_i = 0$ előfordulhat. Az $n = k \cdot m^3$ összefüggésből $\gamma_i + 3\beta_i = \alpha_i$ következik, abból pedig, hogy k köbmentes, azt látjuk, hogy $\gamma_i < 3$. Ezt a két egyenlőséget pontosan $\beta_i = \left\lfloor \frac{\alpha_i}{3} \right\rfloor$ és $\gamma_i = \alpha_i - 3\beta_i$ elégíti ki.

6. Legyen p prím és a egész, amelyre $o_p(a) = 6$.

   (a) Igazoljuk, hogy $a^2 - a + 1 \equiv 0 \ (p)$

   (b) Mutassuk meg, hogy $a - 1$ modulo p rendje 3.

   Megoldás:

   (a) Abból, hogy $1 \equiv a^6 \ (p)$, következik

   $$0 \equiv a^6 - 1 = \left(a^3 - 1\right)\left(a^3 + 1\right) = \left(a^3 - 1\right)(a + 1)\left(a^2 - a + 1\right) \quad (p).$$

   Miután $\mathbb{Z}_p$ nullosztómentes (prímtulajdonság), ezért az utóbbi szorzat valamelyik tényezője 0 modulo p. Az $a^3 - 1 \equiv 0 \ (p)$ kongruencia azt jelentené, hogy a rendje legfeljebb 3, $a + 1 \equiv 0 \ (p)$-ből pedig $o_p(a) = o_p(-1) \leq 2$ következne. Marad tehát, hogy $a^2 - a + 1 \equiv 0 \ (p)$.

   (b) Nézzük meg, hogy mi $a - 1$ harmadik hatványa. Alkalmazva az előbb igazolt összefüggést, a^2 lecserélhető $a - 1$-re.

   $$(a-1)^3 = a^3 - 3a^2 + 3a - 1 \equiv a(a-1) - 3(a-1) + 3a - 1 = a^2 - a + 2 \equiv 1 \quad (p)$$

   Ezek szerint $o_p(a - 1)$ osztója 3-nak. Annyit kell látni, hogy a rend nem egy, azaz $a - 1 \equiv 1 \ (p)$ lehetetlen. Ha mégis így lenne, akkor $a \equiv 2 \ (p)$-ből következik $o_p(2) = 6$ tehát $2^6 \equiv 1 \ (p)$, azaz $p \mid 2^6 - 1 = 63$, így $p = 3$, vagy $p = 7$. Viszont $o_3(2) = 2$ és $o_7(2) = 3$ miatt ezen prímekre sem 6 a 2 rendje.

7. Legyenek p és q különböző páratlan prímszámok.

(a) Mutassuk meg, hogy ha $(a, pq) = 1$, akkor az $x^2 \equiv a \ (pq)$ kongruenciának vagy 0, vagy 4 modulo pq különböző megoldása van.

(b) Bizonyítsuk be, hogy a pq-hoz relatív prím, modulo pq különböző négyzetelemek száma $\frac{\varphi(pq)}{4}$.

Megoldás:

(a) Tegyük fel, hogy $x^2 \equiv a \ (pq)$ kongruenciának van megoldása. Belátjuk, hogy ekkor pontosan 4 megoldás van.

Ha $x^2 \equiv a \ (pq)$ megoldható, akkor $x^2 \equiv a \ (p)$ is az, tehát a négyzetelem modulo p. Legyenek a négyzetgyökei $\pm b$. Hasonlóan $x^2 \equiv a \ (q)$ megoldásai legyenek $\pm c$. A kínai maradéktétel szerint az

(1) $y \equiv b \ (p)$, $y \equiv c \ (q)$
(2) $y \equiv b \ (p)$, $y \equiv -c \ (q)$
(3) $y \equiv -b \ (p)$, $y \equiv c \ (q)$
(4) $y \equiv -b \ (p)$, $y \equiv -c \ (q)$

kongruenciarendszereknek egy-egy megoldása van modulo pq, amelyek mind kielégítik az $x^2 \equiv a \ (pq)$ egyenletet, hiszen mind a négy esetben $y^2 \equiv b^2 \equiv a \ (p)$ és $y^2 \equiv c^2 \equiv a \ (q)$, tehát $y^2 \equiv a \ (pq)$. Négy különböző megoldást tudtunk mutatni.

Azt kell még látni, hogy több megoldás nincs. Ha egy d az eredeti egyenlet egy tetszőleges megoldása, akkor d megoldása az $x^2 \equiv a \ (p)$ és $x^2 \equiv a \ (q)$ kongruenciáknak is. Tanultuk, hogy modulo egy prímszám legfeljebb két négyzetgyöke van a-nak , tehát $d \equiv \pm b \ (p)$ és $d \equiv \pm c \ (q)$, ami azt jelenti, hogy d a fenti négy egyenletrendszer egyikének megoldása.

(b) Legyen $\{b_1, \ldots, b_{\varphi(pq)}\}$ redukált maradékrendszer modulo pq. Ekkor az összes négyzetelemek halmaza nyilván $\{b_1^2, \ldots, b_{\varphi(pq)}^2\}$. Utóbbiak között minden négyzetelem pontosan 4-szer szerepel, hiszen egy a feladat előző része szerint egy négyzetelemnek pontosan négy négyzetgyöke van modulo pq. Ez azt jelenti, hogy a négyzetelemek száma épp $\frac{\varphi(pq)}{4}$.