5. Számelmélet gyakorlat (2009/2010)

Néhány megoldás

1. (a) $23x \equiv 11\ (5)$, $3x \equiv 6\ (5)$, $x \equiv 2\ (5)$.

(b) $36x \equiv 81\ (21)$, $15x \equiv -24\ (21)$, $5x \equiv -8 \equiv -15\ (7)$, $x \equiv -3\ (7)$, $x \equiv -3, 4, 11\ (21)$.

(c) $80x \equiv 32\ (108)$, $80x \equiv 140\ (108)$, $4x \equiv 7\ (27)$, $4x \equiv -20\ (27)$, $x \equiv -5\ (27)$, $x \equiv -5, 22, 49, 76\ (108)$.

(d) $40x \equiv 6\ (12)$ nem megoldható, mert $(40, 12) = 4 \nmid 6$.

(f) $15x + 13y = 19$ helyett a $15x \equiv 19\ (13)$ kongruenciát vizsgáljuk. $2x \equiv 6\ (13)$, $x \equiv 3\ (13)$, vagyis $x = 13n + 3$ alakú, ebből $y = \frac{19-15(13n+3)}{13} = -2 - 15n$. Például $x = 3$ és $y = -2$.

2. Kétféleképpen is okoskodhatunk:

1. A $0, 1, \ldots, m-1$ számok mindegyike pontosan egy b-re megoldása az $ax \equiv b\ (m)$ kongruenciának, vagyis minden maradékosztályt pontosan egyszer számolunk a szummában, ezért az összeg m.

2. Azon b-kre van megoldás, amikre $(a, m) \mid b$, vagyis $b = (a, m)$, $2(a, m)$, $\ldots$, $\frac{m}{(a,m)}(a, m)$ lehetséges és minden esetben (a, m) darab (páronként inkongruens) megoldás van, vagyis $\sum_{b=1}^{m} f(b) = \frac{m}{(a,m)}(a, m) = m$.

3. (a) $x \equiv 3\ (7)$, $x \equiv 2\ (13)$. Tehát $x = 7k + 3 \equiv 2\ (13)$, $7k \equiv -1 \equiv -14\ (13)$, $k \equiv -2\ (13)$, vagyis $k = 13\ell - 2$ alakú, amiből $x = 7(13\ell - 2) + 3 = 91\ell - 11$, vagyis $x \equiv -11\ (91)$.

(b) $x \equiv 3\ (8)$, $x \equiv 5\ (6)$. Tehát $x = 8k + 3 \equiv 5\ (6)$, $2k \equiv 2\ (6)$, $k \equiv 1\ (3)$, vagyis $k = 3\ell + 1$ alakú, amiből $x = 8(3\ell + 1) + 3 = 24\ell + 11$, vagyis $x \equiv 11\ (24)$.

(c) $4x \equiv 2\ (6)$, $12x \equiv 3\ (21)$. Először külön-külön kell megoldani őket, aztán a szimultán rendszer(eke)t.

(d) $2x^{20} + 3x + 4 \equiv 0\ (176)$. $176 = 2^4 \cdot 11$, vagyis a kongruencia ekvivalens a következő két egyenletből álló rendszerrel:

I. $2x^{20} + 3x + 4 \equiv 0\ (16)$

II. $2x^{20} + 3x + 4 \equiv 0\ (11)$

I. Ha $2 \mid x$, akkor $16 \mid x^{20}$, tehát $3x + 4 \equiv 0\ (16)$, amiből $3x \equiv -4 \equiv 12\ (16)$, $x \equiv 4\ (16)$.

Ha x pártalan, akkor $2x^{20}+3x+4$ is pártalan vagyis nem lehet osztható 16-tal.

II. $11 \nmid x$ különben ellentmondást kapunk. Az Euler-Fermat Tétel szerint ekkor $x^{10} \equiv 1 \ (11)$, amiből $2+3x+4 \equiv 0 \ (11)$, $3x \equiv -6 \ (11)$, $x \equiv -2 \ (11)$.

Tehát már csak az $x \equiv 4 \ (16)$, $x \equiv -2 \ (11)$ szimultán rendszert kell megoldanunk. $x = 16k+4 \equiv -2 \ (11)$, $5k \equiv -6 \equiv 5 \ (11)$, $k \equiv 1 \ (11)$, vagyis $k = 11\ell + 1$ alakú, amiből $x = 16(11\ell+1)+4 = 176\ell + 20$, tehát $x \equiv 20 \ (176)$.

4. Nincsen ilyen polinom. Az $f(x) \equiv 0 \ (30)$ kongruencia ekvivalens a következő kongruenciarendszerrel:

I. $f(x) \equiv 0 \ (2)$

II. $f(x) \equiv 0 \ (3)$

III. $f(x) \equiv 0 \ (5)$

I.-nek $0, 1, 2$ megoldása lehet, II.-nek $0, 1, 2, 3$, III.-nak $0, 1, 2, 3, 4, 5$. Az eredeti kongruancia megoldásszáma az I.,II.,III. kongruenciák megoldásszámának szorzata (Kínai Maradéktétel). Azonban a szorzat semmiképpen nem lehet 7-tel osztható.

5. A Wilson Tétel szerint $1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1) \equiv -1 \ (p)$, vagyis $1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdots (-1) \equiv -1 \ (p)$. Legyen $A = \left(\frac{p-1}{2}\right)!$, ekkor $A^2 \cdot (-1)^{\frac{p-1}{2}} \equiv -1 \ (p)$. Mivel $\frac{p-1}{2} = \frac{4k-1-1}{2} = 2k-1$ páratlan, ezért $-A^2 \equiv -1 \ (p)$, vagyis $A^2 \equiv 1 \ (p)$. Másképpen $p \mid A^2 - 1 = (A-1)(A+1)$. Ha $p \mid A-1$, akkor $A \equiv 1 \ (p)$, ha $p \mid A+1$, akkor $A \equiv -1 \ (p)$.

6. Az $m = p$ prím esettel nem foglalkozunk. Legyen m összetett, $m = m_0 m_1$, ahol $1 < m_0, m_1 < m$.

Ha $m_0 \neq m_1$, akkor mindketten szorzótényezők $(m-1)!$-ban, vagyis ekkor $(m-1)! \equiv 0 \ (m)$.

Ha m nem bontható fel két nála kisebb különböző (természetes) szám szorzatára, akkor $m = p^2$ prímnégyzet lehet csak. $p = 2$ esetén $3! \equiv 2 \ (4)$. Ha $p > 2$, akkor $(p^2-1)!$-ban szorzótényezőként megjelenik p és $2p$ is, vagyis ekkor $(p^2-1)! \equiv 0 \ (p^2)$.

Összefoglalva: 1) Ha m prím, akkor $(m-1)! \equiv -1 \ (m)$. 2) Ha $m = 4$, akkor $(m-1)! \equiv 2 \ (m)$. 3) Különben $(m-1)! \equiv 0 \ (m)$.