SzA XI. gyakorlat

2008. november x/20.

Hasznos tudnivalók

- Ha $a \equiv b \pmod{m}$, akkor
  - $a \pm c \equiv b \pm c \pmod{m}$
  - $a \cdot c \equiv b \cdot c \pmod{m}$
  - $\frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{m}{c}}$, ha $c \mid a, b, m$
  - $\frac{a}{c} \equiv \frac{b}{c} \pmod{m}$, ha $(c, m) = 1$
  - $a \cdot c \equiv b \cdot d \pmod{m}$, ha $c \equiv d \pmod{m}$
- $a \cdot x \equiv b \pmod{m}$ lineáris kongruenciának
  - $\exists$ megoldása $\Leftrightarrow (a, m) \mid b$
  - $\exists$ megoldása $\Leftrightarrow (a, m) \pmod{m}$ megoldása létezik
- Euler-Fermat témakör
  - $\varphi(m)$: 1 és m közötti m-hez relatív prímek száma; $\varphi(p) = p - 1$, ha p prím
  - $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, ha p prím
  - $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, ha $(a, b) = 1$
  - Ha $(a, m) = 1$, akkor $1 \equiv a^{\varphi(m)} \pmod{m}$
  - Ha p prím és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$
  - Ha p prím, akkor $a \equiv a^p \pmod{p}$

Feladatok

1. A $\{0, 1, \ldots, 16\}$ mod 16 teljes maradékrendszer mely elemeihez tartoznak a következő számok: 221, 152, 193, 46, 66, 209, 11980, 46628?
2. Bizonyítsuk be, hogy minden n természetes számra $n^7 - n$ osztható 42-vel!
3. Ha 10839-et és 11863-at elosztjuk ugyanazzal a háromjegyű számmal, akkor ugyanazt a maradékot kapjuk. Mi ez a maradék?
4. Bizonyítsuk be, hogy minden n természetes számra $n^{11} + 10n$ osztható 11-gyel!
5. Bizonyítsuk be, hogy $39^{14} - 1$ osztható 5-tel!
6. Mi az alábbi lineáris kongruenciák megoldása?
   (a) $9x \equiv 24 \pmod{96}$
   (b) $8x \equiv 3 \pmod{21}$
   (c) $5^{1997} \equiv x \pmod{17}$
   (d) $108^{182} \equiv x \pmod{19}$
7. Határozzuk meg x-et!

(a) $49^{49} \equiv x \pmod{15}$

(b) $42^{600} \equiv x \pmod{13}$

(c) $205^{206^{207}} \equiv x \pmod{103}$

(d) $x^{11999} \equiv 5 \pmod{13}$

(e) $x^{1993} \equiv 5 \pmod{21}$

(f) $1998! + 111^{1998} \equiv x \pmod{1999}$

8. Bizonyítsuk be, hogy tetszőleges p prímszámra:

$$\binom{2p}{p} \equiv 2 \pmod{p}$$

9. Határozzuk meg az összes olyan n-et, amire $\varphi(n)$

(a) prím,

(b) páratlan!