Wilson-tétel, lineáris kongruenciák, diofantikus egyenletek

12. gyakorlat

2011. november 29.

Tétel: Az $ax \equiv b \pmod{m}$ kongruenciának akkor és csak akkor létezik megoldása, ha $(a, m)|b$.
Tétel: Ha az $ax \equiv b \pmod{m}$ kongruencia megoldható, akkor a megoldásszáma (a, m).
Euler-Fermat-tétel: $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$.
A kis Fermat-tétel: Ha p prím és $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$.
A kis Fermat-tétel másik alakja: Ha p prím, akkor bármely a egész számra $a^p \equiv a \pmod{p}$.
Wilson-tétel: Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.
Tétel: Legyenek a, b és c rögzített egész számok, ahol a és b közül legalább az egyik nem nulla. Az $ax + b = c$ lineáris diofantikus egyenlet akkor és csak oldható meg, ha $(a, b)|c$.

1. Döntsük el, hogy megoldhatók-e az alábbi lineáris kongruenciák, és a megoldhatóakat oldjuk meg.
   (a) $3x \equiv 5 \pmod{7}$
   (b) $14x \equiv 8 \pmod{21}$
   (c) $11x \equiv 12 \pmod{18}$
2. Oldjuk meg az alábbi lineáris kongruenciákat:
   (a) $202x \equiv 157 \pmod{203}$
   (b) $91x \equiv 252 \pmod{35}$
   (c) $152x \equiv 88 \pmod{66}$
3. Bizonyítsuk be, hogy tetszőleges p prímre $(a + b)^p \equiv a^p + b^p \pmod{p}$.
4. Oldjuk meg az alábbi kongruenciákat!
   (a) $x \equiv 108^{182} \pmod{19}$
   (b) $x \equiv 5^{1997} \pmod{17}$
   (c) $x \equiv 1998! + 111^{1998} \pmod{1999}$
5. Legyen $p > 3$ prím. Milyen maradékot ad $3(p-3)!$, ha p-vel maradékosan elosztjuk?
6. Oldjuk meg az alábbi lineáris diofantikus egyenleteket:
   (a) $43x + 25y = 98$
   (b) $7x + 11y = 118$
   (c) $64x + 26y = 4$

7. Oldjuk meg az alábbi diofantikus egyenleteket:

   (a) $ab + 2a + 3b = 36$

   (b) $x^2 + y^2 = 2x + 2y - 3$

   (c) $a^2 + b^2 + c^2 = ab + bc + ca$