

## Számelmélet 2005/2006 őszi

### 3. gyakorlat: Euklideszi algoritmus, kongruenciák bevezető

- 1. Határozzuk meg a  $(693, 147)$  és a  $(233, 377)$  legnagyobb közös osztókat és adjuk meg a  $693x + 147y = (693, 147)$  egyenlet egy  $x, y$  egész megoldását.
- 2. Igazoljuk, hogy adott  $a, b$  és  $c$  egészek mellett az  $ax + by = c$  diofantikus egyenlet pontosan akkor megoldható  $x, y$ -ra, ha  $(a, b) \mid c$ . Speciálisan tehát  $a$  és  $b$  pontosan akkor relatív prím, ha van olyan  $x$  és  $y$ , amire  $ax + by = 1$ .

$a, b, m \in \mathbb{Z}$ -re  $a$  kongruens  $b$ -vel modulo  $m$ , azaz  $a \equiv b \pmod{m}$ , ha  $m \mid a - b$ . Nyilván igaz, hogy

- (a)  $a \equiv a \pmod{m}$  (reflexív),
- (b) ha  $a \equiv b \pmod{m}$ , akkor  $b \equiv a \pmod{m}$  (szimmetrikus) és
- (c) ha  $a \equiv b \pmod{m}$ ,  $b \equiv c \pmod{m}$ , akkor  $a \equiv c \pmod{m}$  (tranzitív),

azaz  $\equiv$  ekvivalenciareláció.

- 3. Bizonyítsuk be, hogy amennyiben  $a \equiv a' \pmod{m}$ ,  $b \equiv b' \pmod{m}$ , akkor

- (a)  $a + b \equiv a' + b' \pmod{m}$ ,
- (b)  $a \cdot b \equiv a' \cdot b' \pmod{m}$ ,

azaz  $\equiv$  kompatibilis a szorzással és az összeadással. Mutassunk példát arra, hogy  $r \equiv s \pmod{m}$ , de  $a^r \not\equiv a^s \pmod{m}$ .

- 4. Lássuk be, hogy  $a \equiv b \pmod{m_i}$  minden  $i = 1, 2, \dots, r$  esetén, akkor és csak akkor, ha  $a \equiv b \pmod{[m_1, \dots, m_r]}$ .

- 5. Igazoljuk az alábbi, kongruenciákra vonatkozó összefüggéseket:

- (a) ha  $a \equiv b \pmod{cm}$ , akkor  $a \equiv b \pmod{m}$ ;
- (b)  $c \neq 0$  egészre  $a \equiv b \pmod{m}$  akkor és csak akkor, ha  $ac \equiv bc \pmod{mc}$ ;
- (c)  $c \neq 0$  egészre  $ac \equiv bc \pmod{m}$  akkor és csak akkor, ha  $a \equiv b \pmod{\frac{m}{(m,c)}}$ .

- 6. Bizonyítsuk be, hogy tetszőleges  $a, c, m$  egészek esetén az  $ax \equiv c \pmod{m}$  kongruencia pontosan akkor oldható meg  $x$ -re, ha  $(a, m) \mid c$ .

- 7. Bizonyítsuk, hogy az euklideszi algoritmus Fibonacci-számokra a leglassabb, azaz ha  $a \geq b$  legnagyobb közös osztóját keresve az algoritmus  $n$  maradékos osztást végez, akkor  $a \geq F_{n+1}$ . (Útmutatás: igazoljuk  $j$ -re vonatkozó indukcióval, hogy  $0 \leq j \leq n$  esetén  $a_{n-j} \geq F_{j+1}$ , ahol az algoritmusban az

$$a_0 := a$$

$$a_1 := b$$

$$a_0 = a_1 q_1 + a_2$$

$$a_1 = a_2 q_2 + a_3$$

$$a_2 = a_3 q_3 + a_4$$

...

$$a_{n-1} = a_n q_n$$

jelöléseket használjuk.)