Diszkrét matematika előadás H.F. feb. 18-ra; megoldás

34. Tétel. Tetszőleges a, b, c, d, m, n egész számokra érvényesek az alábbiak:

(1) $a \equiv a \pmod{m}$;

(2) ha $a \equiv b \pmod{m}$, akkor $b \equiv a \pmod{m}$;

(3) ha $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}$, akkor $a \equiv c \pmod{m}$;

(4) ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a \pm c \equiv b \pm d \pmod{m}$;

(5) ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a \cdot c \equiv b \cdot d \pmod{m}$;

(6) $ca \equiv cb \pmod{m}$ akkor és csak akkor, ha $a \equiv b \pmod{\frac{m}{\text{lnko}(c,m)}}$, feltéve hogy $c, m \neq 0$;

(7) ha $a \equiv b \pmod{m}$ és $a \equiv b \pmod{n}$ akkor és csak akkor, ha $a \equiv b \pmod{\text{lkkt}(m,n)}$;

(8) ha $a \equiv b \pmod{m}$, akkor $\text{lnko}(a,m) = \text{lnko}(b,m)$.

Bizonyítás.

(1) Bármely a és m egészek esetén $m \mid a - a$ a 2. Tétel (5) pontja alapján, így valóban $a \equiv a \pmod{m}$.

(2) Ha $m \mid a - b$, akkor $m \mid b - a$ a 2. Tétel (8) pontja miatt, így $b \equiv a \pmod{m}$.

(3) Ha $m \mid a - b$ és $m \mid b - c$, akkor $m \mid (a - b) + (b - c) = a - c$ a 2. Tétel (7) pontja alapján, így $a \equiv c \pmod{m}$.

(4) Ha $m \mid a - b$ és $m \mid c - d$, akkor $m \mid -c + d$ a 2. Tétel (8) pontja szerint, így $m \mid (a - b) + (c - d) = a + c - (b + d)$ és $m \mid (a - b) + (-c + d) = a - c - (b - d)$ a 2. Tétel (7) pontja alapján, így valóban $a \pm c \equiv b \pm d \pmod{m}$.

(5) Ha $m \mid a - b$ és $m \mid c - d$, akkor, mivel $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$, így $m \mid ac - bd$ és $a \cdot c \equiv b \cdot d \pmod{m}$ a 2. Tétel (8) és (7) pontjai szerint.

(6) Az állítás abból következik, hogy a 16. Tétel szerint $m \mid ca - cb$ pontosan akkor teljesül, ha $\frac{m}{\text{lnko}(c,m)} \mid a - b$.

(7) Az állítás abból következik, hogy az $m \mid a - b$ és $n \mid a - b$ oszthatóságok pontosan akkor teljesülnek, ha $\text{lkkt}(m,n) \mid a - b$, a legkisebb közös többszörös definíciója szerint.

(8) Ha $a \equiv b \pmod{m}$, akkor $a - b = mq$ valamely q egész számra, így $a = mq + b$, tehát $\text{lnko}(a,m) = \text{lnko}(mq + b, m) = \text{lnko}(b,m)$ teljesül a 11. Következmény (vagy 6. Lemma (3)) alapján.

□