Università degli studi di Roma Tre
Corso di Laurea in Matematica, a.a. 2002/2003
TN01 - Tutorato - Andrea Cova
Mercoledì 26 febbraio 2003

1. Sia $n \geq 2$ un intero fissato. Mostrare che:

(1) $a \equiv b \pmod{n}$, $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$;
(2) $a \equiv b \pmod{n}$, $c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$;
(3) $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$, per ogni $k \geq 1$;
(4) $a \equiv b \pmod{n}$ $m \mid n \Rightarrow a \equiv b \pmod{m}$;
(5) $a \equiv b \pmod{n}$, $m \neq 0$, $\Rightarrow am \equiv bm \pmod{nm}$;
(6) $a \equiv b \pmod{n}$, $d \neq 0$, $d \mid a$, $d \mid b$, $d \mid n \Rightarrow a/d \equiv b/d \pmod{n/d}$;
(7) $ac \equiv bc \pmod{n}$, $d = \mathrm{MCD}(c, n) \Rightarrow a \equiv b \pmod{n/d}$;
(8) $ac \equiv bc \pmod{n}$, $\mathrm{MCD}(c, n) = 1 \Rightarrow a \equiv b \pmod{n}$;
(9) $ac \equiv bc \pmod{p}$, p primo, $p \nmid c \Rightarrow a \equiv b \pmod{p}$;
(10) $a \equiv b \pmod{n}$, $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{\mathrm{mcm}(n, m)}$.

Si noti che, in (h), la condizione sul MCD essenziale per effettuare la cancellazione (dare un esempio in cui non si pu effettuare la cancellazione).

2. Sia $S := \{x_1, \cdots, x_n\}$ un sistema completo di residui (modulo n) e siano $a, b \in \mathbb{Z}$ tali che $\mathrm{MCD}(a, b) = 1$. Verificare che l'insieme $S' = \{ax_1 + b, \cdots, ax_n + b\}$ è ancora un sistema completo di residui (modulo n).

3. Siano m ed n interi positivi relativamente primi e siano $S^* := \{x_1, \cdots, x_{\varphi(n)}\}$ e $T^* := \{y_1, \cdots, y_{\varphi(m)}\}$ rispettivamente un sistema ridotto di residui (modulo n) ed un sistema ridotto di residui (modulo m). Verificare che:

$$V^* := \{mx_i + ny_j,\ 1 \leq i \leq \varphi(n), 1 \leq j \leq \varphi(m)\}$$

è un sistema ridotto di residui (modulo mn).

4. Stabilire se la seguente proposizione vera o falsa.
"Se $a \in \mathbb{Z}$, allora $a^2 \equiv 0 \pmod{4}$ oppure $a^2 \equiv 1 \pmod{4}$."

5. Sia $a := 24365789098765434562754326 39$. Determinare la classe di congruenza (mod 4) di a e di a^2 (determinarne cioè un rappresentante x con $0 \leq x \leq 3$).

6. Trovare n tale che $1060 \leq n \leq 1071$ e tale che

$$\{861; 280; 908; n; 144; 555; 1079; 186; 658; 302; 401; 445\}$$

sia un sistema completo di residui (mod 12).

7. Determinare tutte le soluzioni delle seguenti congruenze:

(1) $25X \equiv 15 \pmod{29}$;
(2) $6X \equiv 15 \pmod{21}$;
(3) $17X \equiv 9 \pmod{4}$;
(4) $34X \equiv 60 \pmod{98}$;
(5) $18X \equiv 30 \pmod{42}$;
(6) $243X \equiv 713 \pmod{7007}$.

8. Siano $a, b, n, \in \mathbb{Z}$ con $a, b \geq 1$, $n \geq 2$. Mostrare che:

$$a \equiv b \pmod{n} \Rightarrow \mathrm{MCD}(n, a) = \mathrm{MCD}(n, b).$$

È vero il viceversa? In caso di risposta negativa dare un controesempio.