

ALGEBRA 1
Prof. M. Fontana
Tutorato 5- Andrea Cova (30 ottobre 2002)

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

- (a) $a \equiv b \pmod{n}$, $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$;
- (b) $a \equiv b \pmod{n}$, $c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$;
- (c) $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$, per ogni $k \geq 1$;
- (d) $a \equiv b \pmod{n}$, $m \mid n \Rightarrow a \equiv b \pmod{m}$;
- (e) $a \equiv b \pmod{n}$, $m \neq 0, \Rightarrow am \equiv bm \pmod{nm}$;
- (f) $a \equiv b \pmod{n}$, $d \neq 0$, $d \mid a$, $d \mid b$, $d \mid n \Rightarrow a/d \equiv b/d \pmod{n/d}$;
- (g) $ac \equiv bc \pmod{n}$, $d = \text{MCD}(c, n) \Rightarrow a \equiv b \pmod{n/d}$;
- (h) $ac \equiv bc \pmod{n}$, $\text{MCD}(c, n) = 1 \Rightarrow a \equiv b \pmod{n}$;
- (i) $ac \equiv bc \pmod{p}$, p primo, $p \mid c \Rightarrow a \equiv b \pmod{p}$;
- (j) $a \equiv b \pmod{n}$, $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{\text{mcm}(n, m)}$.

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

2. Alcuni criteri di divisibilità. Sia a un intero non nullo. Scriviamo $|a|$ in forma decimale:

$$|a| = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0$$

con $0 \leq a_i \leq 9$, $0 \leq i \leq m$, e $a_m \neq 0$. Poniamo:

$$S(a) := \sum a_i, \quad A(a) := \sum (-1)^i a_i.$$

Dimostrare i seguenti criteri di divisibilità:

- (a) $2 \mid a \Leftrightarrow 2 \mid a_0$;
- (b) $3 \mid a \Leftrightarrow 3 \mid S(a)$;
- (c) $4 \mid a \Leftrightarrow 4 \mid (a_1 10 + a_0)$;
- (d) $5 \mid a \Leftrightarrow 5 \mid a_0$;
- (e) $9 \mid a \Leftrightarrow 9 \mid S(a)$;
- (f) $11 \mid a \Leftrightarrow 11 \mid A(a)$.

Mostrare che:

- Sia a un intero fissato e sia a' l'intero ottenuto invertendo l'ordine delle cifre di a , nella sua scrittura decimale (ad es. $a = 1324$, allora $a' = 4231$). Mostrare che: $9 \mid (a - a')$.
- Si dice **palindrome** un numero $a \in \mathbb{N}$ tale che $a' = a$ (stessa notazione del punto precedente). Mostrare che, se a è una palindrome con un numero pari di cifre (ad es. 435534), allora: $11 \mid a$.
- Stabilire se: 1345 è divisibile per 9; 57417 è divisibile per 7; 59741 è divisibile per 11; 951214 è divisibile per 4.

3. Determinare un inverso aritmetico di 32 modulo 625.

4. Risolvere, quando è possibile, le seguenti congruenze lineari:

$$9X \equiv 27 \pmod{20}; \quad 9X \equiv 27 \pmod{18}; \quad 9X \equiv 12 \pmod{18}; \quad 9X \equiv 18 \pmod{12}; \\ 150X \equiv 1 \pmod{727}; \quad 150X \equiv 11 \pmod{727}; \quad 150X \equiv 11 \pmod{39275}; \quad 150X \equiv 39 \pmod{231}.$$

5. a) dimostrare il Teorema di Wilson: sia p un numero primo, allora $(p-1)! \equiv -1 \pmod{p}$;

b) dimostrare che il Teorema di Wilson si inverte, infatti: n è primo $\Leftrightarrow (n-1)! \equiv -1 \pmod{n}$.

6. Determinare per ognuna delle seguenti relazioni quali tra le proprietà riflessiva, simmetrica e transitiva sono soddisfatte ed in caso che la relazione sia di equivalenza determinare le classi di equivalenza.

• Sia $R^2 = \{(x, y) : x, y \in R\}$.

a) $(x_1, y_1) \rho (x_2, y_2) \Leftrightarrow \exists \lambda \in R, \lambda \neq 0$, tale che $\lambda x_1 = x_2$ e $\lambda y_1 = y_2$

b) $(x_1, y_1) \rho (x_2, y_2) \Leftrightarrow (x_1 - x_2)^2 + (y_1 - y_2)^2 \leq 1$

c) $(x_1, y_1) \rho (x_2, y_2) \Leftrightarrow x_1 y_1 = x_2 y_2$

• Sia $Z^x = \{q \in \mathbb{Q}; q \neq 0\}$.

d) $x \rho y \Leftrightarrow xy > 0$

e) $x \rho y \Leftrightarrow \sqrt{x^2 + y^2} \in \mathbb{Z}$

f) $x \rho y \Leftrightarrow x/y \geq 1$

• Sia C l'insieme composto dalle circonferenze del piano. Data $C \in C$ denotiamo con $r(C)$ il raggio di C e con $c(C)$ il suo centro.

g) $C_1 \rho C_2 \Leftrightarrow C_1 \cap C_2 \neq \emptyset$

h) $C_1 \rho C_2 \Leftrightarrow r(C_1) = r(C_2)$

i) $C_1 \rho C_2 \Leftrightarrow c(C_1) = c(C_2)$