LOGICA MATEMATICA

Claudia Malvenuto
Canale E-O
Scheda esercizi n. 7

7 ottobre 2003

Rifugiamoci un po' nell'aritmetica:
dodici, ventiquattro, trentasei...
È un bell'aiuto quando si farnetica.
Ma ora non cosí come vorrei.
(Patrizia Valduga, 'Quartine, Seconda centuria')

1. Mostrare che se $n > 5$ ed n *non* è primo, allora
$$(n-1)! \equiv 0 (\mathrm{mod}\ n).$$

2. (*Teorema di Wilson*) Mostrare che se n è primo allora
$$(n-1)! \equiv -1 (\mathrm{mod}\ n).$$

3. Sia $a \in \mathbb{N}$ non nullo. Scriviamo a in forma decimale:
$$a = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0,$$
con $0 \leq a_i \leq 9$ per $0 \leq i \leq m$ e $a_m \neq 0$. Poniamo $S(a) = \sum_{i=0}^m a_i$ (somma delle cifre di a scritto in base 10). Dimostrare usando le congruenze (modulo 10) i ben noti criteri di divisibilità per 2, per 3 e per 9:

   (a) $2|a \Leftrightarrow 2|a_0$;

   (b) $3|a \Leftrightarrow 3|S(a)$;

(c) $9|a \Leftrightarrow 9|S(a)$.

4. (Criterio di divisibilità per 11). Un intero a è divisibile per 11 se e solo se 11 divide $A(a) = \sum_{i=0}^{m} (-1)^i a_i$ (la somma a segni alterni delle sue cifre, con le notazioni dell'esercizio precedente).

5. Si dice *palindrome* un numero $a \in \mathbb{N}$ tale che la successione delle sue cifre decimali sia la stessa se letta da sinistra verso destra o da destra verso sinistra (ad esempio 373 oppure 2002). Mostrare che se a è un palindrome con un numero pari di cifre, allora $11|a$.

6. Determinare gli elementi invertibili (e i loro inversi) di $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$.

7. Sia p un numero primo ed $a \in \mathbb{Z}$ tale che p non divide a. Mostrare, usando il piccolo Teorema di Fermat, che:
$$a^{p-1} \equiv 1 (\text{mod } p).$$

8. Quali e quanti sono gli elementi invertibili di $\mathbb{Z}/24\mathbb{Z}$? Trovare (anche empiricamente!) l'inverso di ognuno degli elementi invertibili.

9. Scrivere l'algoritmo di Euclide delle divisioni successive in pseudo–codice.

10. Trovare l'inverso di ogni elemento $\overline{a} \in \mathbb{Z}/29\mathbb{Z} \setminus \{\overline{0}\}$, tramite il piccolo teorema di Fermat (ovvero calcolando a^{27}...), oppure cercando i coefficienti s, t per l'identità di Bézout $1 = as + 29t$ relativa al massimo comune divisore $1 = (a, 29)$.

11. Per ognuna delle seguenti coppie di numeri $a, b \in \mathbb{N}$ trovare il massimo comune divisore (a, b) di a e b tramite l'*algoritmo di Euclide* ed esprimerlo nella forma $as + bt$ per opportuni $s, t \in \mathbb{Z}$ (identità di Bézout):

    (a) $a = 1705$ e $b = 625$

    (b) $a = 1625$ e $b = 858$

    (c) $a = 2094$ e $b = 12$

    (d) $a = 5307$ e $b = 9150$

Per gli interi a e b del punto d), trovare (a, b) anche con il metodo noto dalla scuola media della fattorizzazione in primi.

12. Dimostrare che $n(n+1)(2n+1) \equiv 0 (\mathrm{mod}\ 6)$

13. Dimostrare che $a^2 + b^2 \equiv 0 (\mathrm{mod}\ 3)$ implica che $a \equiv 0 (\mathrm{mod}\ 3)$ e $b \equiv 0 (\mathrm{mod}\ 3)$.