Esercizio 8.13

Osservazioni preliminari: Sia n un intero positivo. Ricordiamo le seguenti proprietà della congruenza modulo n.

a) Per ogni $a \in \mathbb{Z},\ a \equiv 0 \pmod{n} \Leftrightarrow n|a$.
b) Per ogni $a, b \in \mathbb{Z}$ tali che $a \equiv b\ (mod\ n)$, si ha che $n|a \Leftrightarrow n|b$.
c) Siano $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ tali che $a \equiv a' \pmod{n}, b \equiv b' \pmod{n},\ c \equiv c' \pmod{n},\ d \equiv d' \pmod{n}$. Allora

$$ab \equiv a'b' \pmod{n},$$
$$cd \equiv c'd' \pmod{n},$$

e dunque

$$ab + cd \equiv a'b' + c'd' \pmod{n}.$$

Ciò è conseguenza della compatibilità della congruenza modulo n rispetto alla somma e al prodotto di numeri interi.
Per induzione si deduce che, dati un intero $r \geq 2$ ed interi $x_1, \dots x_r, x_1', \dots, x_r',\ y_1, \dots y_r, y_1', \dots, y_r'$, tali che, per ogni $i = 1, \dots, r$ si abbia

$$x_i \equiv x_i' \pmod{n},$$
$$y_i \equiv y_i' \pmod{n},$$

si ha

$$\sum_{i=1}^{r} x_i y_i \equiv \sum_{i=1}^{r} x_i' y_i' \pmod{n}.$$

In altri termini, in una somma di prodotti di numeri interi, se si sostituisce ad un qualunque fattore un numero intero ad esso congruo modulo n, si ottiene una somma che è congrua alla precedente modulo n.

Si consideri un numero intero positivo la cui rappresentazione in base 10 sia

$$n = \sum_{i=0}^{N} a_i 10^i.$$

Tenuto conto che

$$10 \equiv 1 \pmod{3},$$
$$10 \equiv 1 \pmod{9},$$
$$10 \equiv -1 \pmod{11},$$

si avrà, dunque,

$$n \equiv \sum_{i=0}^{N} a_i 1^i = \sum_{i=0}^{N} a_i \pmod{3},$$

$$n \equiv \sum_{i=0}^{N} a_i 1^i = \sum_{i=0}^{N} a_i \pmod 9,$$
$$n \equiv \sum_{i=0}^{N} a_i (-1)^i \qquad \pmod{11},$$

da cui i criteri di divisibilità per 3, 9 e 11 proposti dall'esercizio.
Inoltre

$$n = \sum_{i=1}^{N} a_i 10^i + a_0,$$

ove il primo addendo è multiplo di 10 e dunque di 5. Dunque

$$n \equiv a_0 \pmod 5,$$

e, d'altra parte, 5 divide a_0 se e solo se $a_0 \in \{0, 5\}$.
Ne consegue il criterio di divisibilità per 5.
Infine, per ogni intero r tale che $1 \leq r \leq N$,

$$n = \sum_{i=r}^{N} a_i 10^i + \sum_{i=0}^{r-1} a_i 10^i,$$

ove il primo addendo è multiplo di 10^r, e dunque di 2^r. Pertanto

$$n \equiv \sum_{i=0}^{r-1} a_i 10^i \pmod{2^r},$$

da cui il criterio di divisibilità per 2^r. In particolare, il caso in cui $r = 1$ ci rivela che n è pari se e solo se a_0 è pari.