Università di Pisa - CdL in Informatica

Un sistema di congruenze con parametro

Alessio Del Vigna

28 Marzo 2020

Esercizio 1. Sia a un numero intero, e si consideri il seguente sistema di congruenze:

$$\begin{cases} (6a-1)x \equiv 1 \pmod{21} \\ x \equiv a \pmod{35} \end{cases}.$$

(i) Discutere la risolubilità del sistema al variare di a.

(ii) Per i valori di a per cui il sistema ammette soluzione, risolvere il sistema.

Soluzione. (i) Cerchiamo una condizione necessaria alla risolubilità del sistema. Se il sistema ha una soluzione allora deve essere della forma $x = a + 35k$ per qualche intero k. Sostituendo nella prima si ha $6a^2 - a - 35k \equiv 1 \pmod{21}$, che implica $6a^2 - a - 1 \equiv 0 \pmod{7}$. Quest'ultima congruenza, con un po' di occhio, può essere riscritta come

$$a^2 + a - 6 = (a+3)(a-2) \equiv 0 \pmod{7}.$$

Dato che 7 è primo, vale la legge di annullamento del prodotto modulo 7 e quindi la precedente congruenza equivale a $a \equiv 2 \pmod{7} \vee a \equiv 4 \pmod{7}$. Abbiamo quindi mostrato che se il sistema ha soluzione allora necessariamente deve valere $a \equiv 2 \pmod{7} \vee a \equiv 4 \pmod{7}$, o, equivalentemente, che se $a \not\equiv 2 \pmod{7} \wedge a \not\equiv 4 \pmod{7}$ allora il sistema non ha soluzione.

Adesso supponiamo che $a \equiv 2 \pmod{7}$. Sostituendo nella prima congruenza si ottiene $11x \equiv 1 \pmod{21}$, ossia $x \equiv 2 \pmod{21}$. Dunque il sistema equivale a

$$\begin{cases} x \equiv 2 \pmod{21} \\ x \equiv a \pmod{35} \end{cases}, \qquad (\star)$$

ed è risolubile perché $(21, 35) = 7 \mid (2-a)$. Analogamente si dimostra che anche nel caso $a \equiv 4 \pmod{7}$ il sistema è risolubile.

(ii) Sia $a \equiv 2 \pmod{7}$ e il sistema associato $(\star)$. Dalla seconda congruenza scriviamo $x = a + 35k$ per un certo k intero. Sostituendo nella prima si arriva a $k \equiv \frac{a-2}{7} \pmod{3}$, da cui

$$x = 6a - 10 \pmod{105}.$$

Procedendo in modo analogo, nel caso $a \equiv 4 \pmod{7}$ si ottiene $x \equiv 6a - 55 \pmod{105}$.