Università di Pisa - CdL in Informatica

Un sistema di congruenze con parametro

a cura di Alessio Del Vigna

Pisa, 06 Giugno 2019

Esercizio 1. Discutere la risolubilità del sistema di congruenze seguente, al variare del parametro intero a:

$$\begin{cases} ax \equiv 3 \pmod{17} \\ a^x \equiv 4 \pmod{17} \end{cases}.$$

Soluzione. La prima congruenza è risolubile se e solo se $\mathrm{mcd}\,(a, 17) \mid 3$, ossia se e solo se $\mathrm{mcd}\,(a, 17) = 1$. Questo equivale a dire che a deve essere invertibile in $\mathbb{Z}/(17)$. Tutti gli elementi invertibili modulo un numero primo si possono sempre esprimere come potenza di un fissato elemento invertibile[1]. Nel nostro caso, ossia $\mathbb{Z}/(17)$, ogni elemento invertibile è potenza di 3: questo fatto può essere verificato anche a mano. Di conseguenza varrà che $a \equiv 3^c \pmod{17}$ per un opportuno esponente $1 \leq c \leq 16$[2]. Osservato inoltre che $4 \equiv 3^{12} \pmod{17}$, possiamo riscrivere la seconda congruenza come

$$3^{cx} \equiv 3^{12} \pmod{17} \Leftrightarrow cx \equiv 12 \pmod{16},$$

poiché l'ordine di 3 modulo 17 è proprio 16, essendo 3 una radice primitiva. L'ultima congruenza ammette soluzione se e solo se $\mathrm{mcd}\,(c, 16) \mid 12$, ossia se e solo se $\mathrm{mcd}\,(c, 16)$ è 1, 2 o 4. Ricordando che $1 \leq c \leq 16$, la precedente condizione equivale a $c \neq 8$ e $c \neq 16$, ossia $a \not\equiv 16 \pmod{17}$ e $a \not\equiv 1 \pmod{17}$.
Rimane adesso da studiare la risolubilità del sistema. Si osservi che:

(i) se $a \not\equiv 0 \pmod{17}$, la prima congruenza ha come insieme soluzione $x \equiv 3\alpha \pmod{17}$, dove α è un inverso di a modulo 17.

(ii) la seconda congruenza equivale a $cx \equiv 12 \pmod{16}$, e se $a \not\equiv 1 \pmod{17}$ e $a \not\equiv 16 \pmod{17}$ ha come insieme soluzione l'insieme di tutti i numeri congrui tra loro modulo un divisore di 16 (quale divisore dipende da c, ossia da a, ovviamente).

In ogni caso, il sistema che ne risoluta ha come modulo della prima congruenza 17 e come modulo della seconda congruenza un divisore di 16. I moduli sono primi tra loro, quindi il sistema è risolubile se e solo se sono verificate le condizioni

$$a \not\equiv 0 \pmod{17} \quad \wedge \quad a \not\equiv 1 \pmod{17} \quad \wedge \quad a \not\equiv 16 \pmod{17}.$$

[1] Per chi avesse visto l'argomento, dato un primo p, il gruppo moltiplicativo degli elementi invertibili modulo p, ossia $\mathbb{Z}/(p)^*$, è un gruppo ciclico. Questo significa che esiste un elemento invertibile $g \in \mathbb{Z}/(p)^*$, detto *radice primitiva*, tale che ogni elemento $a \in \mathbb{Z}/(p)^*$ si scrive come $a = g^c$, per un opportuno esponente c.

[2] Per il piccolo teorema di Fermat, $a^{p-1} \equiv 1 \pmod{p}$ per ogni a invertibile modulo p, così che c può essere limitato tra 1 e $p - 1$.