Esercizi di Matematica Discreta

Luca De Paulis

20 luglio 2020

INDICE

1 CONGRUENZE LINEARI

1.1 TEOREMI E DEFINIZIONI UTILI

Definizione 1.1.1 (Congruenza lineare)
Siano $a, b, n \in \mathbb{Z}$, $n > 0$. Allora la congruenza

$$ax \equiv b \pmod{n}$$

si dice congruenza lineare.

Proposizione 1.1.2 (Condizione necessaria e sufficiente per la risolubilita')
Siano $a, b, n \in \mathbb{Z}$, $n > 0$. *Allora la congruenza*

$$ax \equiv b \pmod{n}$$

ha soluzione se e solo se $\text{mcd}(a, n) \mid b$.

Definizione 1.1.3 (Invertibilità e inverso)
Siano $a \in \mathbb{Z}$.
Allora si dice che a è invertibile modulo n se esiste $y \in \mathbb{Z}$ tale che

$$ay \equiv 1 \pmod{n}.$$

In particolare tra tutti gli y che soddisfano la relazione precedente, il numero y tale che $0 \leqslant y < n$ si dice inverso di a modulo n.

Proposizione 1.1.4 (Condizione necessaria e sufficiente per l'invertibilità)
Siano $a, n \in \mathbb{Z}$, $n > 0$.
Allora a *è invertibile modulo* n *se e solo se* $\text{mcd}(a, n) \mid 1$.

Proposizione 1.1.5 (Risoluzione di una congruenza lineare)
Siano $a, b, n \in \mathbb{Z}$, $n > 0$.
Allora per risolvere l'equazione $ax \equiv b \pmod{n}$ *possiamo ricondurci ad uno dei seguenti tre casi:*

(1) : $\text{mcd}(a, n) = 1$. *L'equazione ha soluzione*

$$x \equiv by \pmod{n},$$

dove y *è l'inverso di* a *modulo* n*;*

(2) : $\text{mcd}(a, n) \mid b$. *L'equazione è equivalente all'equazione*

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\frac{n}{d}\right);$$

(3) : $\text{mcd}(a, n) \nmid b$. *L'equazione non ha soluzione.*

1.2 ESERCIZI

Esempio 1.2.1. Proviamo a risolvere la congruenza

$$57x \equiv 81 \ (21)\,.$$

Innanzitutto notiamo che il coefficiente della x e il termine noto sono maggiori del modulo, dunque possiamo semplificarli:

$$\begin{aligned} 57 = 2 \cdot 21 + 15 &\implies 57 \equiv 15 \ (21) \\ 81 = 3 \cdot 21 + 18 &\implies 57 \equiv 18 \ (21) \end{aligned}$$

La congruenza diventa quindi

$$15x \equiv 18 \ (21)\,.$$

Notiamo che $\mathrm{mcd}(15, 21) = 3 \mid 18$, quindi la congruenza ha soluzione (per la proposizione 1.1.2) e possiamo applicare la regola (ii) della proposizione , ottenendo

$$5x \equiv 6 \ (7)\,.$$

A questo punto $\mathrm{mcd}(5, 7) = 1$, dunque 5 e' invertibile modulo 7 e possiamo trovare l'inverso a tentativi (dato che 7 e' piccolo).

$$\begin{aligned} &5 \cdot 1 \equiv 5 \not\equiv 1 \ (7) \\ &5 \cdot 2 \equiv 10 \equiv 3 \not\equiv 1 \ (7) \\ &5 \cdot 3 \equiv 15 \equiv 1 \ (7) \end{aligned}$$

dunque 3 e' l'inverso di 5 modulo 7.

Moltiplicando entrambi i membri dell'equazione per 3 otteniamo quindi

$$\begin{aligned} &3 \cdot 5x \equiv 6 \cdot 3 \ (7) \\ \iff &x \equiv 18 \equiv 4 \ (7)\,. \end{aligned}$$

La soluzione della congruenza e' quindi $x \equiv 4 \ (7)$.