Lezione 09 - 20/10/2022

Teorema cinese del resto

Il sistema di congruenze

$$\begin{cases} x \equiv c_1 \mod r_1 \\ x \equiv c_2 \mod r_2 \\ ... \\ x \equiv c_s \mod r_s \end{cases}$$

con $(r_i, r_j) = 1,\ i \neq j$, **ha soluzione unica** $\bmod r_1 \cdot r_2 \cdot ... \cdot r_s$**.**

<u>Dimostrazione</u>: poniamo $R = r_1 \cdot r_2 \cdot ... \cdot r_s,\ R_k = \dfrac{R}{r_k}$.

Ovviamente si ha che $(R_k, r_k) = 1$, quindi la congruenza

$$R_k x \equiv c_k \mod r_k$$

ammette un'unica soluzione $\bar{x}_k \mod r_k$. Pongo

$$\bar{x} = R_1\bar{x}_1 + R_2\bar{x}_2 + ... + R_s\bar{x}_s$$

e dico che $\bar{x}$ risolve il sistema di congruenze. Infatti la **k-esima equazione** è

$$\begin{aligned} x &\equiv c_k \mod r_k \\ \bar{x} &= R_1\bar{x}_1 + R_2\bar{x}_2 + ... + R_s\bar{x}_s \\ &\equiv R_k\bar{x}_k \equiv c_k \mod r_k \end{aligned}$$

Per provare l'unicità $\bmod r_1 \cdot ... \cdot r_s$, supponiamo che $\bar{y}$ sia un'altra soluzione:

$$\bar{x} \equiv c_k \equiv \bar{y} \mod r_k,\ \forall k$$

quindi

$$\begin{aligned} \bar{x} - \bar{y} &\equiv 0 \mod r_k,\ \forall k \\ \text{ovvero } \bar{x} - \bar{y} &\equiv 0 \mod r_1 \cdot ... \cdot r_s \end{aligned}$$

ovvero $\bar{x} \equiv \bar{y} \mod r_1 \cdot ... \cdot r_s$.

Esempio:

$$\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 2 \mod 5 \\ x \equiv 1 \mod 3 \end{cases}$$

si ha che:

- $R = 5 \cdot 8 \cdot 3 = 120$
- $R_1 = 15$
- $R_2 = 24$
- $R_3 = 40$

che forma il seguente sistema

$$\begin{cases} R_1 x \equiv c_1 \mod r_1 \\ R_2 x \equiv c_2 \mod r_2 \\ R_3 x \equiv c_3 \mod r_3 \end{cases}$$

ovvero

$$\begin{cases} 15x \equiv 1 \mod 8 \\ 24x \equiv 2 \mod 5 \\ 40x \equiv 1 \mod 3 \end{cases}$$

ricaviamo ora le $\overline{x}_k$

$$\begin{array}{lllllll} 15x \equiv 1 \mod 8 & \rightarrow & -x \equiv 1 \mod 8 & \rightarrow & x \equiv -1 \equiv 7 \mod 8 & \overline{x}_1 = 7 \\ 24x \equiv 2 \mod 5 & \rightarrow & -x \equiv 2 \mod 5 & \rightarrow & x \equiv -2 \equiv 3 \mod 5 & \overline{x}_2 = 3 \\ 40x \equiv 1 \mod 3 & \rightarrow & x \equiv 1 \mod 3 & & & \overline{x}_3 = 1 \end{array}$$

quindi

$$\begin{aligned} \overline{x} &= R_1\overline{x}_1 + R_2\overline{x}_2 + R_3\overline{x}_3 \mod 120 \\ &= 15 \cdot 7 + 24 \cdot 3 + 40 \cdot 1 = 105 + 72 + 40 \\ &= 217 \equiv 97 \mod 120 \end{aligned}$$

e quindi tutte le soluzioni sono del tipo $x = 97 + 120k$.

Proposizione

Siano r, s interi ≥ 2, $(r, s) = 1$. Allora la corrispondenza

$$f : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$$

data da

$$f(x \bmod rs) = (x \bmod r, x \bmod s)$$

è **biunivoca** e **rispetta le operazioni**.

> ⚠️ Più avanti diremo che f è un **isomorfismo di anelli**.

Esempio:

$$\begin{aligned}
\mathbb{Z}_6 \to& \mathbb{Z}_3 \times \mathbb{Z}_2 \\
\bar{0} \mapsto& (\bar{0}, \bar{0}) \\
\bar{1} \mapsto& (\bar{1}, \bar{1}) \\
\bar{2} \mapsto& (\bar{2}, \bar{0}) \\
\bar{3} \mapsto& (\bar{0}, \bar{1}) \\
\bar{4} \mapsto& (\bar{1}, \bar{0}) \\
\bar{5} \mapsto& (\bar{2}, \bar{1})
\end{aligned}$$

Dove quello che si trova prima di '$\mapsto$' è inteso in $\bmod 6$, mentre quello che si trova nelle parentesi è inteso rispettivamente alle posizioni nella coppia $\bmod 3$ e $\bmod 2$.

Esempio:

$$\bar{3} + \bar{5} = \bar{8} = \bar{2}$$
$$(\bar{0}, \bar{1}) * (\bar{2}, \bar{1}) = (\bar{2}, \bar{0})$$

Dimostrazione di f biunivoca: Poichè $|\mathbb{Z}_{rs}| = |\mathbb{Z}_r| \times |\mathbb{Z}_s| = rs$, basta vedere che f è **suriettiva**.

Dire che f è suriettiva significa dire che dato $\bar{a} \in \mathbb{Z}_r$, $\bar{b} \in \mathbb{Z}_s$, esiste $x \in \mathbb{Z}_{rs}$ tale che

$$\begin{cases} x \equiv a \mod r \\ x \equiv b \mod s \end{cases} \tag{1}$$

ma questo è garantito dal **teorema cinese dei resti**: il sistema (1) ha soluzione **unica** $\mod rs$.

Esempio:

$$\begin{cases} 2x \equiv 8 \mod 9 \\ 2x \equiv 6 \mod 15 \end{cases}$$
$$\begin{cases} x \equiv 40 \mod 9 \\ x \equiv 48 \mod 15 \end{cases}$$
$$\begin{cases} x \equiv 4 \mod 9 \\ x \equiv 3 \mod 15 \rightarrow \begin{cases} x \equiv 3 \mod 5 \\ x \equiv 3 \mod 3 \ (*) \end{cases} \end{cases}$$

Sia ha che $x \equiv 0 \mod 3 \Rightarrow 0, 3, 6$ e $(*)$ si può riscrivere come $x = 3k$. Il sistema però non è risolubile.

Teorema di Eulero-Fermat

Ricordiamo prima la **funzione di Eulero**:

$$\phi(n) = |\{x \in \mathbb{N} : 1 \leq x < n,\ (x, n) = 1)\}|$$
$$\phi(rs) = \phi(r)\phi(s) \quad \text{se } (r, s) = 1$$
$$\phi(p^k) = p^k - p^{k-1}$$

e ricordiamo il **piccolo teorema di Fermat**:

$$a^p \equiv a \mod p$$
$$\text{se } (a, p) = 1 \quad a^p \equiv 1 \mod p$$

Teorema: **Teorema di Eulero-Fermat**

Sia $(a, n) = 1$

$$a^{\phi(n)} = 1 \mod n$$

> ⚠️ Se p è **primo**, $\phi(p) = p - 1$, quindi il **piccolo teorema di Fermat** è un caso speciale di **teorema di Eulero-Fermat**

Dimostrazione: per prima cosa proviamo che se p è **primo** e $p \nmid a$ allora

$$a^{\phi(p^k)} \equiv 1 \mod p^k$$

Procediamo per **induzione su k**:

- $k = 1$, si ottiene il **piccolo teorema di Fermat**
- Supponiamo la tesi vera per k e dimostriamola per $k+1$

$$\begin{aligned} &a^{\phi(p^k)} \equiv 1 \mod p^k, \text{ ovvero} \\ &a^{\phi(p^k)} = 1 + hp^k \\ &\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p \cdot \phi(p^k) \end{aligned}$$

dunque

$$\begin{aligned} a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} = (1 + hp^k)^p = \\ &= 1 + \binom{p}{1} hp^k + \binom{p}{2} (hp^k)^2 + ... + \binom{p}{p-1} (hp^k)^{p-1} + (hp^k)^p \equiv 1 \end{aligned}$$

dove tutti gli $hp^k \equiv 0 \mod p^{k+1}$.

In generale, $n = p_1^{h_1} ... p_s^{h_s}$

$$\phi(n) = \phi(p_1^{h_1}) ... \phi(p_s^{h_s}) \; (*)$$

Da quanto già visto risulta

$$a^{\phi(p_i^{h_i})} \equiv 1 \mod p_i^{h_i} \; (\blacksquare)$$

Inoltre da $(*)$ si ha che $\phi(p_i^{h_i}) \mid \phi(n)$.

Elevando ambo i membri per $(\blacksquare)$ alla $\dfrac{\phi(n)}{\phi(p_i^{h_i})}$ otteniamo

$$a^{\phi(n)} \equiv 1 \mod p_i^{h_i}$$

Ma allora $a^{\phi(n)} \equiv 1 \mod \underbrace{p_1^{h_1} ... p_s^{h_s}}_{=n}$.