Lezione 07 - 14/10/2022

Ripasso - Elementi invertibili

Ricordiamo che se A è un **anello commutativo con unità**, un elemento $a \in A$ si dice **invertibile** se

$$\exists b \in A : ab = 1$$

Esempio: In $\mathbb{Z}$ gli elementi invertibili sono ± 1.
Osserviamo inoltre che gli elementi invertibili di A **formano un gruppo rispetto al prodotto**. Infatti basta verificare che il prodotto di elementi invertibili è invertibile: Se a, b sono invertibili, esistono

$$c, d \in A : ac = 1 \quad bd = 1$$

ma allora

$$(ab)(cd) = acbd = 1 \cdot 1 = 1$$

Osservazione: $\{\pm 1\}$ è un gruppo rispetto al prodotto. La tabella moltiplicativa è:

	1	-1
1	1	-1
-1	-1	1

Proposizione

$\bar{a} \in \mathbb{Z}_n$ è invertibile se e solo se $(a, n) = 1$

Corollario

$\{\bar{a} \in \mathbb{Z}_n : 0 < a < n,\ (a, n) = 1\}$ è un gruppo (che spesso viene denotato con $\mathbb{U}_n$)

<u>Dimostrazione</u>: supponiamo che $(a, n) = 1$. Scriviamo l'**identità di bezout**:

$$ab + ns = 1$$

prendiamo le classi resto $\bmod n$

$$\begin{aligned} \overline{ab + ns} &= \overline{1} \\ \overline{a}\overline{b} + \underbrace{\overline{ns}}_{=\overline{0}} &= \overline{1} \\ \overline{a}\overline{b} &= \overline{1} \end{aligned}$$

Dunque $\overline{a}$ è invertibile e $\overline{b}$ è l'**inverso**.
Viceversa, se $\overline{a}$ è **invertibile**, esiste $\overline{b} \in \mathbb{Z}_n$ con $\overline{a}\overline{b} = \overline{1}$, cioè

$$\begin{aligned} &ab \equiv 1 \mod n \\ &ab - 1 = kn \\ &\underbrace{ab - kn = 1}_{\text{identità di bezout}} \Rightarrow (a, n) = 1 \end{aligned}$$

<u>Esempi esercizi</u>:

1. Trovare gli **elementi invertibili** in $\mathbb{Z}_{42}$

$$42 = 2 \cdot 3 \cdot 7$$
$$\{\overline{1}, \overline{5}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{37}, \overline{41}\}$$

   Procedimento:

   - Si prende il modulo
   - Si fattorizza
   - Si prendono i fattori che non hanno multipli in comune

2. Trovare l'inverso di $\overline{31}$ in $\mathbb{Z}_{42}$

$$
\begin{aligned}
42 &= 31 + 11 \\
31 &= 11 \cdot 2 + 9 \\
11 &= 9 \cdot 1 + 2 \\
9 &= 2 \cdot 4 + 1
\end{aligned}
$$

Scriviamo ora l'identità di bezout

$$
\begin{aligned}
1 &= 9 - 2 \cdot 4 \\
&= 9 - (11 - 9) \cdot 4 \\
&= 9 \cdot 5 - 11 \cdot 4 \\
&= (31 - 11 \cdot 2)5 - 11 \cdot 4 \\
&= 31 \cdot 5 - 11 \cdot 14 \\
&= 31 \cdot 5 - (42 - 31) \cdot 14 \\
&= 31 \cdot 19 - 42 \cdot 14
\end{aligned}
$$

Quindi l'inverso di $\overline{31}$ è $\overline{19}$ in $\mathbb{Z}_{42}$ in quanto $\overline{31} \cdot \overline{19} = \overline{1}$.

Spoiler - la cardinalità di Un

Definizione: funzione ϕ di Eulero

$$\phi(n) = |\{a \in \mathbb{N}, 1 \leq a <, (a, n) = 1\}|$$

Teorema: $\phi(n)$ si calcola a partire dalla fattorizzazione di n usando le due segenti regole:

1. Se p **primo**, $\phi(p^n) = p^n - p^{n-1}$
2. Se $(r, s) = 1$, $\phi(rs) = \phi(r) \cdot \phi(s)$

Esempio:

- Calcolo di $\phi(42)$

$$
\begin{aligned}
\phi(42) = \phi(2 \cdot 3 \cdot 7) &\overset{(2)}{=} \phi(2)\phi(3)\phi(7) \\
&\overset{(1)}{=} (2-1)(3-1)(7-1) = 1 \cdot 2 \cdot 6 = 12
\end{aligned}
$$

- Calcolo di $\phi(100)$

$$\begin{aligned}\phi(100) = \phi(2^2 \cdot 2^5) &= \phi(2^2)\phi(2^5) \\ &= (2^2 - 2)(5^2 - 2) = (4-2)(25-5) = 40\end{aligned}$$

Congruenze lineari

Una **congruenza lineare** è un'equazione della forma

$$ax \equiv b \mod n$$

con $a, b \in \mathbb{Z},\ n \in \mathbb{N}$.

> ⚠️ Può essere pensata come l'equazione $\bar{a}\bar{x} = \bar{b}$ in $\mathbb{Z}_n$

Proposizione

Una congruenza $ax \equiv b \mod n$ ha soluzione se e solo se $(a, n) \mid b$.

<u>Dimostrazione</u>:

$$ax \equiv b \mod n \iff ax - b = kn \iff ax - kn = b$$

ovvero, la congruenza $ax \equiv b \mod n$ ha soluzione se e solo se l'**equazione diofantea** $ax - kn = b$ **ha soluzione**, che accade se e solo se $(a, n) \mid b$.

Proposizione

Sia $ax \equiv b \mod n$ una **congruenza lineare** con $(a, n) \mid b$. Se x_0 è una soluzione, **tutte le soluzioni** sono del tipo

$$x_0 + h \cdot \underbrace{\frac{n}{(a, n)}}_{\text{è un intero}}, \quad h \in \mathbb{Z}$$

tra queste le soluzioni con $0 \leq h < (a, n)$ sono **a due a due non congruenti** e **ogni altra soluzione è congruente a una di esse**.

<u>Esempio</u>: $2x \equiv 4 \mod 8$ con $d = (a, n) = 2$.

Le soluzioni fondamentali sono: $x_0,\ x_0 + 4$. Ad esempio:

- $x_0 = 2$

- $x_0 = 4$

Proviamo che $x_0 + h \cdot \dfrac{n}{d}$ (abbiamo posto $d = (a, n)$) è una soluzione:

$$\begin{aligned} a(x_0 + h \cdot \frac{n}{d}) &= ax_0 + ah \cdot \frac{n}{d} \\ &\equiv b + \underbrace{\text{m.c.m}(a,n) \cdot h}_{\text{è un multiplo di n}} \\ &\equiv b \mod n \end{aligned}$$

Proviamo ora che **ogni soluzione è di questo tipo**: siano x_0, x_0' due soluzioni, allora

$$\begin{aligned} &ax_0 = b + hn,\ ax_0' = b + kn \\ &a(x_0 - x_0') = (h-k)n \\ &\frac{a}{d}(x_0 - x_0') = (h-k)\frac{a}{d} \end{aligned}$$

$$\begin{aligned} (\frac{a}{d}, \frac{n}{d}) = 1 \quad & \frac{n}{d} \mid x_0 - x_0' \\ & x_0 - x_0' = h \cdot \frac{n}{d} \\ & x_0 = x_0' + h \cdot \frac{n}{d} \end{aligned}$$

Resta da vedere che le soluzioni $x_0 + h \cdot \dfrac{n}{d} \quad 0 \leq h < d$

1. Sono **a due a due non congruenti**
2. Che **ogni altra soluzione è congruente a una di loro**

<u>Dimostrazione per 1.</u>: Supponiamo per assurdo che

$$x_0 + h_1 \cdot \frac{n}{d} \equiv x_0 + h_2 \cdot \frac{n}{d} \mod n, \quad 0 \leq h_1 < h_2 < d \ (1)$$

allora

$$h_1 \cdot \frac{n}{d} \equiv h_2 \cdot \frac{n}{d} \mod n$$

dunque

$$h_1 \equiv h_2 \mod \frac{n}{n/d}$$

e qundi $h_1 \equiv h_2 \mod d$ che è **assurdo** per (1).

> ℹ️ Si ricorda che per la proprietà 5 delle congruenze
>
> $$ac \equiv bc \mod n$$
> $$a \equiv b \mod \frac{n}{(n, c)}$$

Dimostrazione per 2: prendiamo una soluzione $x_0 + h \cdot \dfrac{n}{d}$ e dividiamo h per d:

$$h = dq + r \quad 0 \leq r < d$$
$$x_0 + h \cdot \frac{n}{d} = x_0 + (dq + r)\frac{n}{d} = x_0 + nq + r\frac{n}{d} \equiv x_0 + r\frac{n}{d} \mod n$$

Corollario

Se $(a, n) = 1$, la congruenza $ax \equiv b \mod n$ **ammette soluzione unica** $\mod n$.

Esempio:

$$5x \equiv 16 \mod 7$$
$$\overline{5}\overline{x} = \overline{16} = \overline{2} \text{ in } \mathbb{Z}_7$$

L'inverso di $\overline{5}$ in $\mathbb{Z}_7$ è $\overline{3}$

$$\overline{3} \cdot \overline{5}\overline{x} = \overline{3} \cdot \overline{2}$$
$$\overline{x} = \overline{6}$$
$$x = 6 + 7k, \; k \in \mathbb{Z}$$

> ⚠️ Devo trovare l'inverso di $\overline{5}$ per isolare la $\overline{x}$.

Sistemi di congurenze lineari

Vogliamo ora risolvere sistemi di congruenze lineari del tipo

$$\begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \\ ... \\ a_s x \equiv b_s \mod n_s \end{cases}$$

Supponiamo dapprima $(n_i, n_j) = 1,\ i \neq j$.

Supponiamo inoltre $d_i = (a_i, n_i) \mid b_i$.

Se divido per d_i ciascuna equazione, ottengo un sistema del tipo:

$$\begin{cases} a'_1 x \equiv b'_1 \mod n'_1 \\ a'_2 x \equiv b'_2 \mod n'_2 \\ ... \\ a'_s x \equiv b'_s \mod n'_s \end{cases}$$

con $a_i = \dfrac{a_i}{d_i}$, $b_i = \dfrac{b_i}{d_i}$ e $n_i = \dfrac{n_i}{d_i}$.

Ma allora $(a'_i, n'_i) = 1$ quindi a'_i è invertibile in $\mathbb{Z}_n$ e quindi il sistema può riscriversi nella forma

$$\begin{cases} x \equiv c_1 \mod n'_1 \\ ... \\ x \equiv c_s \mod n'_s \end{cases}$$

con $c_i = a_i'^{-1},\ (n'_i, n'_j) = 1,\ i \neq j$.

Esempio:

$$\begin{cases} 1025x \equiv 5312065 \mod 8 \\ 36x \equiv 322 \mod 5 \\ 4x \equiv 7 \mod 3 \end{cases}$$

si trasforma in

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

soluzione

$$\begin{aligned} x &= 1 + 8n \\ 1 + 8n &\equiv 2 \mod 5 \\ 8n &\equiv 1 \mod 5 \\ 3n &\equiv 1 \mod 5 \\ n &\equiv 2 \mod 5 \end{aligned}$$

$$\begin{aligned} n &= 2 + 5m \\ x &= 1 + 8n = 1 + 8(2 + 5m) = \\ &= 17 + 40m \end{aligned}$$

$$\begin{aligned} 17 + 40m &\equiv 1 \mod 3 \\ 2 + m &\equiv 1 \mod 3 \\ m &\equiv -1 \mod 3 \\ m &\equiv 2 \mod 3 \\ m &= 2 + 3s \end{aligned}$$

$$\begin{aligned} x &= 17 + 40m = 17 + 40(2 + 3s) = \\ &= 97 + 120s \end{aligned}$$