UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

# Algebra

Alessandro D'Andrea

## 5. Il teorema di Lagrange

# Richiami



- $\mathbb{Z}/n$ è un anello
- $(\mathbb{Z}/n)^\times$ è un gruppo rispetto alla moltiplicazione
- Oggi: **Congruenza modulo un sottogruppo e teorema di Lagrange**
  - Piccolo teorema di Fermat: se $p$ è primo, $a^p \equiv a \mod p$;
  - Teorema di Eulero: se gli elementi invertibili in $\mathbb{Z}/n$ sono in totale $\varphi(n)$, allora $a^{\varphi(n)} \equiv 1 \mod n$ non appena $\mathrm{MCD}(a, n) = 1$.

# Congruenza modulo $n$ in $\mathbb{Z}$



Ripercorriamo il concetto di congruenza modulo $n$. Scriviamo

$$a \equiv b \mod n$$

esattamente quando $n$ divide $b - a$. Equivalentemente possiamo dire che $b - a \in (n)$, che è un sottogruppo di $(\mathbb{Z}, +)$.

Proviamo ad adattare questa definizione a sottogruppi di gruppi più generali di $\mathbb{Z}$.

# Congruenza modulo $H < G$



Se abbiamo $H < G$, scriviamo

$$a \equiv b \mod H$$

se $a^{-1}b \in H$. Verifichiamo che la congruenza modulo $H$ è una relazione di equivalenza:

- $a \equiv a \mod H$ per ogni $a \in G$.
  - $a^{-1}a = 1 \in H$.
- Se $a \equiv b \mod H$, allora anche $b \equiv a \mod H$.
  - Se $a^{-1}b \in H$, allora anche $b^{-1}a = (a^{-1}b)^{-1} \in H$.
- Se $a \equiv b \mod H$ e $b \equiv c \mod H$, allora anche $a \equiv c \mod H$.
  - Sappiamo che $a^{-1}b, b^{-1}c \in H$. Moltiplicando, otteniamo $a^{-1}c = a^{-1}bb^{-1}c \in H$.

Come sono fatte le classi di congruenza?

# Classi laterali sinistre



Dire $a \equiv b \mod H$ è lo stesso che dire $a^{-1}b \in H$.

Ma $a^{-1}b = h \in H$ è equivalente a $b = ah$, dove $h \in H$.

Gli elementi nella classe di congruenza di $a$ sono tutti e soli quelli della forma $ah$, con $h \in H$.

L'insieme di questi elementi si indica con $aH$ e si chiama classe laterale sinistra di $H$, o semplicemente laterale di $H$.

# Partizione in classi laterali



Sono affermazioni equivalenti:

- $a \equiv b \mod H$;
- $a \in bH$;
- $b \in aH$;
- $aH = bH$.

Se $a, b$ sono elementi di $G$, allora sono possibili due situazioni:

- $a \equiv b \mod H$;
  - In questo caso $aH = bH$.
- $a \not\equiv b \mod H$;
  - In questo caso $aH \cap bH = \emptyset$.

Le classi laterali sinistre di $H$ costituiscono una partizione di $G$ in sottoinsiemi disgiunti.

Ciascuna classe laterale $aH$ ha tanti elementi quanti ne possiede $H$.
In effetti, se $ah_1 = ah_2$, allora $h_1 = h_2$.

# Un esempio in $S_3$



Abbiamo già visto due elementi di $S_3$:

$$\sigma : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} , \qquad \tau : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases} .$$

I $6 = 3!$ elementi di $S_3$ sono $1, \tau, \tau^2, \sigma, \tau\sigma, \tau^2\sigma$. Infatti:

$$\tau^2 : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases} , \qquad \tau\sigma : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases} , \qquad \tau^2\sigma : \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases} .$$

Il sottogruppo generato da $\sigma$ è $H = \{1, \sigma\}$. I suoi laterali sinistri sono $H$, $\tau H = \{\tau, \tau\sigma\}$ e $\tau^2 H = \{\tau^2, \tau^2\sigma\}$.

# Struttura degli omomorfismi



Se $\phi : G \to H$ è un omomorfismo di gruppi, abbiamo già visto che

$$\phi(a) = \phi(b) \iff 1 = \phi(a)^{-1}\phi(b) = \phi(a^{-1}b) \iff a^{-1}b \in \ker\phi.$$

Ricordando che

$$a^{-1}b \in \ker\phi \iff a \equiv b \mod \ker\phi,$$

vediamo che due elementi di $G$ possiedono la stessa immagine attraverso $\phi$ se e solo se si trovano nella stessa classe laterale di $\ker\phi < G$.

Una volta ripartito $G$ in classi laterali rispetto a $\ker\phi$, gli elementi di ciascun laterale hanno la stessa immagine, e ciascun laterale va in un elemento diverso.

# Teorema di Lagrange



Consideriamo un gruppo finito $G$ ($\leftarrow$ questo vuol dire che $G$ ha un numero finito di elementi), e un suo sottogruppo $H < G$.

Poiché $G$ è ripartito nell'unione disgiunta dei laterali sinistri di $H$, il numero di elementi di $G$ si ottiene sommando il numero di elementi di ciascun laterale di $H$.

Ricordando che i laterali possiedono tutti lo stesso numero di elementi, il numero di elementi di $G$ si ottiene moltiplicando il numero di elementi di $H$ per il numero dei laterali di $H$ in $G$.

Gergo: il numero di elementi di un gruppo $G$ è l'ordine di $G$, e si indica con $|G|$. Il numero dei laterali di un sottogruppo $H < G$ si chiama indice di $H$ in $G$ e si indica con $[G : H]$.

## Teorema (Lagrange)

*Se $H < G$ sono gruppi finiti, allora $|G| = [G : H]|H|$.*

# Alcune conseguenze



## Teorema (Lagrange)

*Se $H < G$ sono gruppi finiti, allora $|G| = [G : H]|H|$.*

- Se $H < G$, allora $|H|$ divide $|G|$.
- Se $g \in G$, allora l'ordine di $g$ divide $|G|$.
  - Il sottogruppo $(g)$ generato da $g$ è un sottogruppo di $G$;
  - pertanto $|(g)|$ divide $|G|$,
  - ma abbiamo visto che il numero di elementi di $(g)$ è esattamente l'ordine di $g$.
- Se $g \in G$, $g^{|G|} = 1$.
  - Se $d$ è l'ordine di $g$, sappiamo che $g^d = 1$;
  - Ma $d$ divide $|G|$, quindi $|G| = dn$ per qualche $n$,
  - e quindi $g^{|G|} = g^{dn} = (g^d)^n = 1^n = 1$.

# Gruppi di ordine primo



Che possiamo dire di un gruppo $G$ se $|G| = p$, con $p$ primo?

Gli elementi di $G$ hanno ordine che divide $p$, quindi hanno ordine 1 oppure ordine $p$.

L'unico elemento di ordine 1 è l'elemento neutro.

Se $g \neq 1$ è un elemento di $G$, allora deve avere ordine $p$. Allora $(g)$ ha $p$ elementi, e quindi $(g) = G$.

I gruppi di ordine primo sono ciclici. In particolare, sono abeliani.

- Se $1 \neq g \in G$, ogni elemento di $G$ è una potenza di $g$. Ma sappiamo che

$$g^m g^n = g^{m+n} = g^n g^m.$$

Indicheremo il gruppo ciclico con $p$ elementi con $C_p$.

# Piccolo teorema di Fermat



Se $G$ è un gruppo finito e $g \in G$, allora $g^{|G|} = 1$. (in notazione additiva, $|G|g = 0$).

- $G = (\mathbb{Z}/n, +)$. Poiché $|G| = n$, allora $n\overline{a} = \overline{0}$.
  - Lo sapevamo già: $n\overline{a} = \overline{an} = \overline{0}$.
- $G = (\mathbb{Z}/p^{\times}, \cdot)$, con $p$ primo. In questo caso $|G| = p - 1$, quindi $\overline{a}^{p-1} = \overline{1}$ se $\overline{a} \in G$.
  - Se $p$ non divide $a$, allora $a^{p-1} \equiv 1 \mod p$.
  - Moltiplicando per $a$, si ottiene $a^p \equiv a \mod p$, che è vero anche quando $p$ divide $a$.

## Teorema (Fermat)

*Se $p$ è un numero primo, $a^p \equiv a \mod p$ per ogni intero $a$.*

# La funzione $\varphi$ di Eulero



L'ordine del gruppo moltiplicativo $(\mathbb{Z}/n)^\times$ si indica con $\varphi(n)$.

- $\varphi(p) = p - 1$ quando $p$ è primo.
  - Ogni elemento è invertibile tranne $\overline{0}$.
- $\varphi(mn) = \varphi(m)\varphi(n)$ se $\mathrm{MCD}(m, n) = 1$.
  - Segue dal teorema cinese del resto. $\overline{a}$ è invertibile in $\mathbb{Z}/mn$ se esiste $\overline{h}$ tale che $\overline{a} \cdot \overline{h} = \overline{1}$ in $\mathbb{Z}/mn$.
  - Che $ah \equiv 1 \mod mn$ può essere verificato modulo $m$ e modulo $n$ separatamente.
  - Ma allora $a$ deve essere invertibile modulo $m$ (ci sono $\phi(m)$ scelte) e invertibile modulo $n$ (ci sono $\phi(n)$ scelte). In conclusione, ho $\phi(m)\phi(n)$ scelte per $\overline{a}$.
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ se $p$ è primo.
  - $\mathrm{MCD}(a, p^k) = 1$ è lo stesso che $\mathrm{MCD}(a, p) = 1$. Gli elementi di $\mathbb{Z}/p^k$ sono tutti invertibili tranne i multipli di $p$, che sono $p^{k-1}$.

# Come calcolare $\varphi(n)$ - I



Le proprietà

- $\varphi(p^k) = p^{k-1}(p-1)$ se $p$ è primo.
- $\varphi(mn) = \varphi(m)\varphi(n)$ se $\text{MCD}(m,n) = 1$.

permettono di calcolare facilmente $\varphi(n)$ per ogni $n$. Calcoliamo ad esempio $\varphi(5040)$.

- Fattorizziamo 5040 in primi: $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$.
- Calcoliamo $\varphi$ su ciascuna potenza di primo:
  - $\varphi(2^4) = 2^3(2-1) = 8$;
  - $\varphi(3^2) = 3^1(3-1) = 6$;
  - $\varphi(5) = 5^0(5-1) = 4$;
  - $\varphi(7) = 7^0(7-1) = 6$.
- Moltiplichiamo i valori ottenuti:

$$\varphi(5040) = \varphi(2^4)\varphi(3^2)\varphi(5)\varphi(7) = 8 \cdot 6 \cdot 4 \cdot 6 = 1152.$$

# Come calcolare $\varphi(n)$ - II



Si può automatizzare questa procedura nella formula

$$\varphi(n) = n \cdot \prod_{p|n, p \text{ primo}} 1 - \frac{1}{p}.$$

Nel caso di $n = 5040$, i primi che dividono $n$ sono $2, 3, 5, 7$. Pertanto

$$\begin{aligned}\varphi(5040) &= 5040 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) \\ &= 5040 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 5040 \cdot \frac{48}{210} = 24 \cdot 48 = 1152.\end{aligned}$$

# Teorema di Eulero



Se $G$ è un gruppo finito e $g \in G$, allora $g^{|G|} = 1$.

- Se $G = (\mathbb{Z}/n)^\times$, allora $|G| = \varphi(n)$.
- Pertanto, se $\overline{a} \in G$, $\overline{a}^{\varphi(n)} = \overline{1}$.

## Teorema (Eulero)

*Se* $\mathrm{MCD}(a, n) = 1$*, allora* $a^{\varphi(n)} \equiv 1 \mod n$.

Attenzione!!! Se $a$ non è primo con $n$, l'enunciato è sicuramente falso!!!