Lezione 12 Algebra I

Federico De Sisti

2024-11-07

1 Divisione Euclidea

Teorema 1
$a, b \in \mathbb{Z}$ con $b \neq 0$ allora $\exists q, r \in \mathbb{Z}$ tale che
$\cdot a = qb + r$
$\cdot\ 0 \leq r < |b|$

Dimostrazione
Procediamo per passi
$1) a, b \in \mathbb{Z}_{>0}$

$$A = \{k \in \mathbb{Z} | kb > a\}.$$

Osserviamo che $A \neq \emptyset$
Infatti $(a+1)b = ab + b > ab \geq a \Rightarrow a+ \in A$
Per il principio del buon ordinamento di $\mathbb{N}$

$$\Rightarrow \exists m := min\{k\} \in \mathbb{Z}^{+}.$$

Definiamo

$$q := m - 1 \in \mathbb{Z}^{+}.$$

$q \notin A$ *e* $q + 1 \in A$
$qb \leq a < (q+1)b = qb + b$
$\Rightarrow 0 \leq a - qb < b$
Definiamo $r = a - qb$ *e otteniamo:*
$0 \leq r < b$
$a = qb + r$
2) $a \in \mathbb{Z}$ $b > 0$
Se $a \geq 0$ *(ok per 1)*
Se $a < 0 \Rightarrow -a > 0$
$\Rightarrow -a = qb + r$ *con* $0 \leq r < b$
$\Rightarrow a = (-q)b - r$
Se $r = 0$ *abbiamo finito*
Se invece $0 < r < b$
definiamo $r' = b - r \Rightarrow 0 < r' < b$
$a = (-q)b - b + \frac{b-r}{r'}$
$\Rightarrow a = (-q-1)b + r' = q'b + r'$
3) $a \in \mathbb{Z}, b < 0$
$\Rightarrow -b > 0$
$a = q(-b) + r$ *con* $0 \leq r < -b$
$\Rightarrow a = (-q)b + r \quad 0 \leq r < |b|$ $\square$

2 Esercizi delle schede

$\begin{cases} x \equiv 50 \ mod(110) \\ x \equiv 47 mod(73) \end{cases}$

Dal teorema cinese del resto sappiamo che esiste un'unica soluzione modulo il prodotto $mod(110 * 73) = mod(8030)$

Come lo costruisco?

$\bar{x} = 50 \cdot 73 \cdot m_1 + 47 \cdot 110 \cdot m_2$

L'idea è di infilare al posto di m_1 l'inverso di 73 $mod(110)$

$$\begin{cases} 73 \cdot m_1 \equiv 1 \ (110) \\ 110 \cdot m_2 \equiv 1 \ (73) \end{cases} .$$

Bisogna determinare m_1, m_2

Idea: Sfruttare l´identità di Bezoit: $(n_1) + (n_2) = (MCD(n_1, n_2)) = (1)$

obiettivo: $n_1 \cdot e + n_2 \cdot s = 1$

Nel nostro caso cerco $110 \cdot r + 73 \cdot s = 1 \quad r, s \in \mathbb{Z}$

Perché è importante $110 \cdot r \equiv 1 \ mod(73)$

$73 \cdot s \equiv 1 \ mod(110)$

Il nuovo obiettivo è determinare r, s

Procedo con la divisione euclidea tra 110 e 73

$$110 = 73 + 37$$
$$73 = 2 \cdot 37 - 1$$
$$\Rightarrow 1 = 2 \cdot 37 - 73$$
$$\Rightarrow 2 \cdot (110 - 73) - 73 = 1$$
$$\Rightarrow 2 \cdot 110 - 3 \cdot 73$$

Quindi:

$1 = 2 \cdot 110 - 3 \cdot 73$

da cui

$$m_1 = -3$$
$$m_2 = 2$$

$$\bar{x} \equiv 5 - \cdot 73 \cdot (-3) + 47 \cdot 110 \cdot (2) \equiv -620 \ mod(8030).$$

8===D

Nuovo Esercizio

$\begin{cases} x \equiv_6 2 \\ x \equiv_{10} 3 \end{cases}$ Non possiamo sfruttare il teorema cinese del resto

$$x \equiv_6 2$$
$$\Updownarrow$$
$$x = 2 + 6k \quad k \in \mathbb{Z}$$
$$\Updownarrow$$
$$x = 2(1 + 3k)$$

$$x \equiv_{10} 3$$
$$\Updownarrow$$
$$x = 3 + 10h \quad h \in \mathbb{Z}$$
$$\Updownarrow$$
$$x = 2(5h + 1) + 1$$

Dunque dalla prima congruenza segue

$$x \equiv_2 0.$$

dalla seconda

$$x \equiv_2 1.$$

8===D

Nuovo Esercizio

$\begin{cases} 3x \equiv_{15} 6 \\ 7x \equiv_9 2 \end{cases}$

Non posso usare TCB studio $3x \equiv_{15} 6$

$$3x \equiv 6 + 15k$$
$$\Updownarrow$$
$$3x = 3(2 + 5k)$$
$$\Updownarrow$$
$$x = 2 + 5k$$

$\begin{cases} x \equiv_5 2 \\ 7x \equiv_9 2 \end{cases}$

Ora $MCD(3, 9) = 1$ Vorrei sfruttare TCR, per farlo dobbiamo eliminare i coefficienti

Noto che 7 e 9 sono coprimi $\Rightarrow [7] \in U_9$ (invertibili modulo 9)

Cerchiamo l'inverso moltiplicativo di $[7] \in U_9$

ovvero cerco $s \in \mathbb{Z}$ tale che $7s \equiv_9 1$

Utilizzo la divisione euclidea

$$
\begin{gathered}
9 = 7 + 2 \\
7 = 3 \cdot 2 + 1 \\
\Rightarrow 1 = 7 - 3 \cdot 2 \\
\Rightarrow 1 = 7 - 3 \cdot (9 - 7) \\
\Rightarrow 1 = 4 \cdot 7 - 3 \cdot 9
\end{gathered}
$$

Quindi $s = 4$

$$
\begin{gathered}
7x \equiv_9 2 \\
\Updownarrow \\
4 \cdot 7 \equiv_9 4 \cdot 2 \\
\Updownarrow \\
x \equiv_9 8
\end{gathered}
$$

Il sistema è quindi equivalente a

$$
\begin{cases} x \equiv_5 2 \\ x \equiv_9 8 \end{cases}
$$

Applico TCR
La soluzione esiste ed è unica modulo (45)
Soluzione:

$$\bar{x} \equiv_{45} 2 \cdot 9 \cdot m_1 - 1 \cdot 5 \cdot m_2.$$

Dove : $\begin{cases} 5m_2 \equiv_9 1 \\ 9m_1 \equiv_5 1 \end{cases}$ Divisione euclidea

$$
\begin{gathered}
9 = 5 + 4 \\
5 = 4 + 1 \\
1 = 5 - 4 \\
1 = 5 - (9 - 5) \\
1 = 2 \cdot 5 - 9
\end{gathered}
$$

$\Rightarrow m_2 = 2 \;\; m_1 = -1$

$$\bar{x} \equiv_{45} -18 - 10 \equiv_{45} -28.$$

3 Azioni di gruppi

Definizione 1
Un'azione di un gruppo $(G,\cdot)$ su un insieme X è un'applicazione

$$G \times X \to X$$
$$(g,x) \to g.x$$

tale che
1) $e.x = x$
2) $(f \cdot g).x = f(g.x) \quad \forall f, g \in G \quad \forall x \in X$

Esempi:
1)$(G,*)$ gruppo scelgo $X = G$ agisce per moltiplicazione sinistra

$$G \times X \to X$$
$$(g,x) = g \underset{\circ}{*} x$$

2) $G = S_n \quad X = \{1, \ldots, n\}$

$$\mathrm{S}_n \times X \to X$$
$$(\sigma, x) \to \sigma(x)$$

3) $n, m \in \mathbb{Z}^+$
$G := GL_n(\mathbb{R}) \times GL_n(\mathbb{R})$
$X = Mat_{n,m}(\mathbb{R})$

$$G \times X \to X$$
$$(AB, C) \to BCA^{-1}$$

4) $G = GL_n(\mathbb{R}) \;\; X = \mathbb{R}^n$

$$\mathrm{G} \times X \to X$$
$$(\mathrm{A,v}) \to Av$$

5) $G = GL_n(\mathbb{R}) \quad X = Mat_{n,m}(\mathbb{R})$

$$G \times X \to X$$
$$(A, C) \to ACA^{-1}$$

6) $(G,\cdot)$ gruppo $X = G$

$$G \times X \to X$$
$$(g, x) \to g * x * g^{-1}$$

Definizione 2
Data un'azione di un gruppo G su un insieme X si dice transitiva se

$$\forall x, y \in X \ \ g \in G \text{ tale che } g.x = y.$$

Definizione 3
Un'azione si dice semplicemente transitiva se

$$\forall x, y \in X \quad g \in G \text{ tale che } g.x = y.$$

Esercizio:
1) Dimostrare che gli esempi dati sono azioni
2) stabilire quali degli esempi sono semplicemente transitivi, transitivi o nessuna delle due

Notazione 1
Scriveremo $G \curvearrowright X$ per indicare che il gruppo G agisce sull'inseme X

Definizione 4
$G \curvearrowright X$, Dato $x \in X$ definiamo:
· l'orbita di x come il sottoinsieme

$$O_x = \{g.x | g \in G\} \subseteq X.$$

lo stabilizzatore di x il sottogruppo:

$$Stab_x = \{g \in G | g.x = x\} \subseteq G.$$

Esercizio:
Dimostra che lo stabilizzatore di ogni elemento è sempre un sottogruppo (non necessariamente normale
Esercizio:
Sia G gruppo finito ($|G| < +\infty$) con $G \curvearrowright X$, per ogni $x \in X$ si ha:
1) $|Stab_x| < +\infty$ (banale)
2) $|O_x| < +\infty$
3) $|G| = |O_x||Stab_x|$
Suggerimento:
2) Abbiamo un'applicazione suriettiva
$G \to O_x$

$g \to g.x$

3) L'idea è di dimostrare che esiste una corrispondenza biunivoca fra gli elementi dell'orbita e i laterali sinistri dello stabilizzatore, poi concludete ricordando che $[G : Stab_x] = \frac{|G|}{|Stab_x|}$ (numero di laterali sinistri)
Idea(per la corrispondenza biunivoca)
Verificare che $\forall g, f \in G$

$$g \equiv f mod(Stab_x)$$
$$\Updownarrow$$
$$g.x = f.x$$

> **Teorema 2** (Cauchy)
> *Sia G un gruppo finito, Sia p primo tale che $p \mid |G|$*
> *Allora esistono (almeno) $p-1$ elementi di ordine p in G*

Dimostrazione
1) In generale se $G \curvearrowright X$ allora X è unione disgiunta di orbite
Definiamo la relazione di equivalenza su$X$come$x\tilde{y} \Leftrightarrow g \in G$ tale che $g.x = y$.
Basta dimostrare che è una relazione d'equivalenza
2) $X = \{(g_1, \ldots, g_n) \in G \times \ldots \times G | g \cdot \ldots \cdot g_p = e\}$
Vogliamo definire un'azione del gruppo ciclico $C_p =< p >$ su X

$$C_p \times X \to X$$
$$\rho.(g_1, \ldots, g_p) \to (g_2, g_3, \ldots, g_p, g_1)$$

Verifichiamo che l'azione sia ben definita ovvero che
$\rho.(g_1, \ldots, g_p) \in X \quad \forall (g_1, \ldots, g_p) \in X$

$$g_2 \cdot \ldots \cdot g_p g_1 = (g_1^{-1} g_1)(g_2 \cdot \ldots \cdot g_p) g_1 = g_1^{-1}(g_1 \cdot \ldots \cdot g_p) g_1 = g_1^{-1} g_1 = e.$$

3) Studio $|X|$ abbiamo $|X| = |G|^{p-1}$ infatti:
$\forall (g_1, \ldots, g_{p-1}, g_p) \in X$ dove $_p = (g_1, \ldots, g_{p-1})^{-1} \Rightarrow$ in particolare $p||X|$
4)Studiamo le orbite dell'azione $C_p \curvearrowright X$, Sappiamo che $|C_p| = |O_x||Stab_x| \; \forall x \in X$
Quindi $|O_x| = 1 \quad \vee \quad |O_x| = p$
5) Dato che X è unione disgiunta di orbite e $p||X|$
Allora il numero di orbite formate da (x) unico elemento è un multiplo di p
6) Studio tali orbite
L'orbita $O_{(g_1, \ldots, g_p)}$ è formata da un singolo elemento se e solo se
$g_1 = g_2 = \ldots = g_p$ □
Dunque abbiamo una corrispondenza biunivoca

$$\{O_x : \; |O_x| = 1\} \; \leftrightarrow \; \{g \in G | g^p = e\}.$$

Quindi p divide $|\{g \in G | g^p = e\}|$
d'ora in poi $A = \{g \in G | g^p = e\}$

7)$A \neq \emptyset$ poiché $e \in A$

$$A = \{e\} \cup \{g \in G | ord(g) = p\}.$$

Quindi modulo (p) abbiamo

$$0 \equiv_p 1 + |\{g \in G | ord(g) = 1\}|.$$

Quindi l'insieme di elementi di ordine p in G è non uvoto e

$$|\{g | ord(g) = p\} \equiv_p p - 1.$$

Deduciamo

$$|\{g \in G | ord(g) = p\} = kp - 1 \geq p - 1.$$

con $k \in Z^+$

4 Torniamo alle schede

$\begin{cases} 3x \equiv_{15} 6 \\ 21x \equiv_{49} 13 \end{cases}$ La prima congruenza è equivalente a $x \equiv_5 2$

$MCD(21, 49) = 7$

La seconda congruenza significa

$$21x = 13 + 49k \quad k \in \mathbb{Z}.$$

$$21x - 49k = 13$$
$$7(3x - 7k) = 13$$

Osservazione:

Se $MCD(a, n) \not| b$

allora $ax \equiv_n b$ non ammette soluzioni

Infatti: $d = MCD(a, n)$

con $d \not| b$ allora

con d divide il membro di sinistra ma non quello di destra

Esercizio

G gruppo $g \in G \quad ord(g) = n$

Allora, $g^h = g^k$ se e solo se $h \equiv_n k$

Soluzione

Assumiamo che $g^h = g^k$ Divisione Euclidea

$h - k = qn + r$ con $0 \leq r < n$

Assurdo se $0 < r < n \;\; r = 0$

$h - k = qn \Rightarrow h \equiv_n k$

Esercizio
per quali $n, m \in \mathbb{Z}$ si ha $2^n + 2^m$ divisibile per 9 **Soluzione**
Studio

$$2^n + 2^m \equiv_9 0$$
$$\Updownarrow 2^n \equiv_9 -2^m$$
$$\Updownarrow$$
$$2^{n-m} \equiv_9 -1$$
$$\Updownarrow$$
$$2^{n-m} \equiv_9 8$$
$$\Updownarrow$$
$$2^{n-m} \equiv_9 2^3$$

Sfruttiamo l'esercizio precedente con $G = U_9$
La congruenza è verificata se e solo se

$$n - m \equiv 3 \ mod(ord_{U_9}([2])).$$