Lezione 11 Algebra I

Federico De Sisti

2024-11-05

1 Svolgimento esercizi

Ossercazione:
Quali sono gli elementi di oridne 21 in S_{13}?
Ricordo che in S_4, gli elementi $(12)(34), (13)(24), (14)(23)$ hanno ordine 2
gli elementi di ordine 21 sono $(3-ciclo)(7-ciclo)$ sono $\frac{13!}{126}$
$(3-ciclo)(3-ciclo)(7-ciclo)$ sono $\frac{13!}{126}$
Nelle note del corso trovi soluzioni degli esercizi

2 Funzione di Eulero

$\phi : \mathbb{Z}_{>0} \to \mathbb{Z}$
$\quad n \to |U_n|$
Ricordo:
$\phi(1) = 1$
$\phi(\rho) = \rho - 1$
$\phi(\rho^k) = \rho^k - \rho^{k-1}$
$\phi(n \cdot m) = \phi(n)\phi(m) \quad$ se $MCD(n,m) = 1$

Lemma 1
$n > 1, a \in \mathbb{Z}$ t.c. $MCD(n,a) = 1$
sia $\{a_1, \dots, a_{\phi(n)}\}$ l'insieme dei numeri positivi minori di n coprimi con n distinti fra loro.
Allora $\{[a_1], \dots, [a_{\phi(n)}] = \{[aa_1], \dots, [aa_{\phi(n)}]\}$ (Classi in $Z/(n)$)

Dimostrazione
Basta verificare che gli elementi delle classi $[aa_i] \ \ \forall\ 0 < i < \phi(n)$
Siano tutte distinte tra loro e aa_i sia coprimo con $n \ \forall\ 0 < i < \phi(n)$
Se per assurdo $[aa_i] = [aa_j] \quad i \neq j \Rightarrow aa_i \equiv aa_j \ mod(n) \Rightarrow a \equiv a_j \ mod(n)$
Assurdo perché $1 \leq a_i, a_j < n$ per ipotesi e dunque $a_i - a_j \notin (n)$
$$\begin{cases} MCD(a,n) = 1 \\ MCD(a_i, n) = 1 \end{cases} \Rightarrow MCD(a, a_i) = 1$$
$\square$

Teorema 1 (Eulero 1760)
$n > 1, a \in \mathbb{Z}$ tale che $MCD(a,n) = 1$
Allora
$$a^{\phi(n)} \equiv 1 \ mod(n).$$

Nota
Se n è primo ritroviamo il piccolo teorema di Fermat

Dimostrazione
Considero la situazione del lemma:
$A = \{a_1, \dots, a_{\phi(n)}\}$
Insieme degli interi positivi minori di n e coprimi con n distinti tra loro
Dal lemma segue che

$$a_1 \cdot \dots \cdot a_{\phi(n)} \equiv (aa_1) \cdot \dots \cdot (aa_{\phi(n)})\ mod(n).$$

$$\equiv a^{\phi(n)} \cdot a_1 \cdot \dots \cdot a_{\phi(n)}\ mod(n).$$

Dal momento che $MCD(a_i, n) = 1$
abbiamo: $1 \equiv a^{\phi(n)}\ mod(n)$ □

Esempio
Se volessi calcolare le ultime 3 cifre di 2024^{2025} Studiamo la congruenza

$$x \equiv 2024^{2025}\ mod(1000)$$

È equivalente al sistema (Teorema cinese del resto):

$$\begin{cases} x \equiv 2024^{2025}\ mod(2^3) \\ x \equiv 2024^{2025}\ mod(5^3) \end{cases}$$

Alternativamente mi accorgo che la prima equazione è equivalente a

$$x \equiv 24^{2025}\ mod(1000).$$

$\phi(1000) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$
$\Rightarrow 24^{400} \equiv 1 mod(n)$
Ma questo implica che la congruenza che devo studiare è:

$$\Rightarrow x \equiv 24^{2025} mod(1000).$$

$$\Rightarrow \begin{cases} x \equiv 24^{2025}\ mod(8) \\ x \equiv 24^{2025}\ mod(125) \end{cases} \Rightarrow \begin{cases} x \equiv 0\ mod(8) \\ x \equiv 24^{2025}\ mod(125) \end{cases}.$$

Dove nell'ultimo passaggio abbiamo utilizzato il fatto che $8|24$ e $24^{\phi(125)} \equiv 24^{100} \equiv 1\ mod(125)$
Alla fine dovremmo ricostruire la soluzione in $\mathbb{Z}/(1000)$ che sarà unica per il teorema cinese del resto

3 Teorema cinese del resto

Problema
Dato un sistema di congruenze
$$\begin{cases} x \equiv= a_1\ mod(n_1) \\ \vdots \\ x \equiv= a_r\ mod(n_r) \end{cases}$$

con $MCD(n_i, n_j) = 1 \ \ \forall i \neq j$
Come ricostruire l'unica soluzione $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \ldots \cdot n_r)$
$\bar{x} \equiv a_i \ mod(n_i) \ \forall i \in \{1, \ldots, r\}$

Idea

Definiamo:
$n := n_1 \cdot n_r$
$N_i := \frac{n}{n_i}$
$\bar{x} := a_1 N_1^{\phi(n_1)} + \ldots + a_r N_r^{\phi(n_r)}$
Ora $\bar{x} \equiv a_i N^{\phi(n)} \ mod(n) \Rightarrow \bar{x} = a_i mod(n_i) \ \ \forall i$

Teorema 2 (TCR)
Damp il sistema
$$\begin{cases} x \equiv a_1 \ mod(n) \\ \ldots x \equiv a_r \ mod(n_r) \end{cases}$$
con $MCD(n_i, n_j) = 1 \ \ \forall i \neq j$
Allora esiste un'unica classe $[\bar{x}] \in \mathbb{Z}/(n_1 \cdot \ldots \cdot n_r)$ *tale che*
$\bar{x} \equiv a_i \ mod(n_i) \ \ \forall i \in \{1, \ldots, r\}$

Dimostrazione (Alternativa al teorema di Eulero)
$n := n_1 \ldots \cdot n_r$
$N_i = \frac{n}{n_i}$
$\bar{x} := a_1 N_1 m_1 + \ldots a_r N_r m_r$
dove gli m_i *sono univocamente determinati dalla condizione* $N_i m_i \equiv 1 mod(n_i)$
Infatti
$$\bar{x} \equiv a_i N_i m_i \ mod(n_i) \Rightarrow \bar{x} \equiv a_i mod(n_i).$$
Osserviamo che $MCD(N_i, n_i) = 1$ *Per ipotesi*
Quindi $[N_i] \in U_{n_i}$ *e* $[m_i]$ *è l'unico inverso di* $[N_i]$ *in* U_{n_i} $\square$

Osservazione

Per risolvere i sistemi di congruenze "basta" saper trovare gli inversi degli elementi in gruppi U_{n_i}

Esercizi dalle schede

Esercizio (Gauss)

Dato un intero $n > 1$ dimostrare che $n = \sum_{d|n} \phi(d)$ (somma di tutti i divisori positivi di n

Dimostrazione

$S_d := \{m \in \mathbb{Z} | MCD(m, n) = d, 1 \leq m \leq n\}$
Osserviamo che
$\{1, \ldots, n\} = \bigcup_d S_d$
$\Rightarrow n = \sum_{d|n} |S_d|$
$MCD(m, n) = d \ \Leftrightarrow MCD(\frac{m}{d}, \frac{n}{d}) = 1$
Quindi $|S_d| = \phi(\frac{n}{d})$
$n = \sum_{d|n} |S_d| = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d)$

$\square$

Esempio
$n = 15$
Voglio ripetere la dimostrazione per ottenere $15 = \sum_{d|15} \phi(d)$
$S_1 = \{1, 2, 4, 7, 8, 11, 13, 14\} \Rightarrow \phi(15/1) = 8$
$S_3 = \{3, 6, 9, 12\} \Rightarrow \phi(15/3) = 4$
$S_5 = \{5, 10\$ \Rightarrow \phi(15/5) = 2$
$S_{15} = \{15\} \Rightarrow \phi(15/15) = 1$
Esempio
$n.1$ Allora la somma di tutti gli interi positivi minori di n coprimi con n vale $\frac{1}{2}n\phi(n) \in \mathbb{Z}$
Dimostrazione
Chiamiamo $a_1, \dots, a_{\phi(n)}$ *tali interi:*
Studio $\sum_{i=1}^{\phi(n)} a_i$
Osserviamo che $MCD(a, n) = 1 \Leftrightarrow MCD(n - a_i, n) = 1$
Quindi
$\{a_1, \dots, a_{\phi(n)}\} = \{n - a_1, \dots n - a_{\phi(n)}\}$
$\Rightarrow \sum_{i=1}^{\phi(n)} a_i = \sum_{i=1}^{\phi(n)} (n - a_i) = n\phi(n) - \sum_{i=1}^{\phi(n)} a_i \Rightarrow 2\sum_{i=1}^{\phi(n)} a_i = n\phi(n)$ □

3.1 Teorema di Wilson/Lagrange

Ricordo

Teorema 3 (Wilson)
p primo. Allora
$(p - 1)! \equiv (p - 1)\ mod(p)$

Teorema 4 (Lagrange)
$m > 1$ intero tale che
$(m - 1)! \equiv (m - 1)\ mod(m)$
Allora m è primo

Dimostrazione
Per assurdo, se m non è primo allora esiste un intero $d|m$ tale che $1 < d < m$
Osserviamo che:
$d < m \Rightarrow d|(m - 1)!$
dall'ipotesi segue che

$$m|(m - 1)! + 1.$$

$\Rightarrow d|(m + 1)! + 1$
Quindi $\begin{cases} d|(m-1)! \\ d|(m-1)! + 1 \end{cases} \quad => d|1$ *che è un assurdo* □
Esercizio
p primo dispari. Allora

$$p \equiv 1\ mod(.$$