Lezione 17 Algebra I

Federico De Sisti

2024-11-26

1 Ricordo (Lagrange)

$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ tale che $a_n \not\equiv_p 0$ con $p > 1$ primo
Allora $f(x) \equiv_p 0$ ammette al più n soluzioni

Corollario 1 (Esercizio)
Dimostrare che se p primo e $d|(p-1)$ allora $x^d - 1 \equiv_p 0$ ammette esattamente d soluzioni

Dimostrazione (Soluzione)
Abbiamo che se $d(p-1)$ allora $(x^d-1)|(x^{p-1}-1)$
$\Rightarrow x^{p-1} = (x^d - 1)f(x)$
dove f è di grado $(p-1-d)$
Ora $x^{p-1} \equiv_p 1$ ammette $p-1$ soluzioni distinte per il piccolo teorema di Fermat.
Le soluzioni sono $1, 2, \ldots, p-1$
Se una di tali soluzioni non risolve $f(x) \equiv_p 0$ allora risolve $x^d - 1 \equiv_p 0$ (Sto usando il fatto che $\mathbb{Z}/(p)$ è un dominio d'integrità [prodotto commutativo e se il prodotto tra due numeri è 0 allora o uno o l'altro sono 0])
Dato che $f(x) \equiv_p 0$ ammette al più $p-1-d$ soluzioni distinte deduciamo che $x^d - 1 \equiv_p$ ammette almeno $d = (p-1) - (p-1-d)$ soluzioni distinte in $\mathbb{Z}/(p)$.
D'altra parte per l'esercizio precedente ne ammette al più d, e quindi segue la tesi. □

Corollario 2 (Esercizio)
$p > 1$ primo, $d|(p-1)$ Allora, esistono esattamente $\phi(d)$ interi, distinti in U_p, di ordine d in U_p

Dimostrazione (Soluzione)
Introduco $S_d = \{k \in \mathbb{Z} | ord_{U_p}([k]) = d, \quad 1 \leq k \leq p-1\}$
La tesi è equivalente a dimostrare che $|S_d| = \phi(d)$
Abbiamo una partizione $\{1, \ldots, p-1\} = \bigcup_{d|p-1} S_d$
Quindi $p - 1 = \sum_{d|(p-1)} |S_d|$
Ricordo:
$n = \sum_{d|n} \phi(d)$ (esercizio delle vecchie schede)
Scegliendo $n = p-1$ deduciamo
$\sum_{d|p-1} |S_d| = \sum_{d|p-1} \phi(d)$
Basta allora dimostrare che $|S_d| \leq \phi(d) \quad \forall d|p-1$
Se $S_d = \emptyset \Rightarrow |S_d| = 0 \leq \phi(d)$
Se $S_d \neq \emptyset \Rightarrow \exists a \in S_d$
$\Rightarrow \{a, a^2, a^3, \ldots, a^d\}$ sono tutti distinti mod(p) infatti

$$a^i \equiv_p a^k$$
$$\Updownarrow$$
$$i \equiv_d j$$

Quindi $a, a^2, \ldots, a^n$ *sono tutte e sole le soluzioni di* $x^d - 1 \equiv_p 0$ *Quindi gli elementi di ordine* d *in* U_p *sono della forma* a^j *per qualche* $j \in \{1, \ldots, j\}$
Ma $ord([a^j]) = \frac{d}{MCD(j,d)}$ *(esercizio di una riga)*
Quindi $|S_d| = \phi(d)$

□

Corollario 3
Esercizio] $p > 1$ *primo:*
Allora esistono esattamente $\phi(p-1)$ *radici primitive distinte*

Dimostrazione (Soluzione)
Basta applicare l'esercizio precedente, scegliendo $d = p - 1$ □

Esercizio
$p > 1$ primo
dimostrare che $Aut(C_p) \cong C_{p-1}$
Soluzione:
Sappiamo che $Aut(C_p) \cong U_p \cong C_{p-1}$
Dove la prima congruenza la sappiamo da teoremi precedenti, la seconda viene data dal precedente corollario

Congettura 1 (Gauss, 1801)
Esistono infiniti primi per cui 10 *è una radice primitiva*

Congettura 2 (E. Artin, 1927)
$a \in \mathbb{Z}$, $a \neq \pm 1$
Assumiamo che a *non sia un quadrato perfetto, Allora esistono infiniti primi per cui* a *è una radice prima*

Osservazione
Oggi sappiamo che la congettura di Artin è vera per infiniti interi a, ma non è noto quali **Esercizio:** $p > 1$ primo
Sia $a = x^2$ con $x \in \mathbb{Z}$
Dimostrare che se $[a] \in U_p$
allora $ord_{U_p}([a] \not= p - 1$
Esercizio [classificazione dei gruppi di ordine pq]
Dimostrare che tutti i gruppi non ciclici di ordine pq con $p \neq q$ primi, sono fra

loro isomorfi e non abeliani
Soluzione
Dato G tale che $|G| = pq$ Avevamo dimostrato che $\exists! Q \in Syl_q(G) \ \Rightarrow \ Q \trianglelefteq G$
Inoltre $\exists P \in Syl_p(G) \Rightarrow P \leq G$
Abbiamo verificato che:
$\cdot P \cap Q = \{e\}$
$\cdot |PQ| = |G| \Rightarrow PQ = G$
$\Rightarrow G \cong Q \rtimes_\phi P \cong C_q \rtimes_\phi C_p$