Aritmetica, Tutorato 3

Rivediamo la dimostrazione della

Prop. Per ogni numero naturale $n > 0$,

$$\sum_{d \mid n} \varphi(d) = n.$$

dim. Lo mostriamo in due modi. In entrambi i casi, l'idea è la stessa: trovare un insieme $\mathcal{F}$ di cardinalità n che sappiamo partizionare in pezzi $\mathcal{F}_d$, uno per ogni d divisore di n, tali che $|\mathcal{F}_d| = \varphi(d)$.

Modo I Chiamiamo

$$\mathcal{F} := \left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n} \right\}$$

l'insieme delle frazioni positive e ≤ 1 di denominatore n. Riduciamo le frazioni ai minimi termini: ognuna delle frazioni ottenute sarà della forma i/d, dove

(i) d è un divisore di n, [abbiamo diviso num e den per un divisore di n]

(ii) $i \leq d$,

(iii) $(i,d) = 1$. [altrimenti, i/d sarebbe riducibile]

Viceversa, se i/d verifica (i), (ii), (iii) sopra, allora compare in $\mathcal{F}$: moltiplicando num. e den. per n/d otteniamo

$$i/d = \frac{\boxed{i \cdot \frac{n}{d}}}{n} \leftarrow \text{è } \leq 1 \text{ perché } i \leq d$$

Chiamiamo allora $\mathcal{F}_d$ l'insieme delle (nuove) frazioni in $\mathcal{F}$ con den. $= d$, per d un div. di n: per (i) e (iii) vale

$$\mathcal{F}_d = \{ i/d \mid i \leq d,\ (i,d) = 1 \},$$

e pertanto

$$|\mathcal{F}_d| = \# \{ i \in \mathbb{N} \mid i \leq d,\ (i,d) = 1 \}$$

che è $\varphi(d)$ per definizione. Inoltre, per (i), l'unione è disg. perché ogni frazione ha un unico den.!

$$\mathcal{F} = \bigsqcup_{\boxed{d \mid n}} \mathcal{F}_d$$

questo segue da (i)

da cui, passando alle cardinalità,

l'unione è disg.

$$\underset{\substack{\| \\ n}}{|\mathcal{F}|} = \sum_{d \mid n} \underset{\substack{\| \\ \varphi(d)}}{|\mathcal{F}_d|}$$

$$\Longrightarrow \quad n = \sum_{d \mid n} \varphi(d).$$

$\boxed{\text{Modo 2}}$ È del tutto analogo, ma usiamo un po' di teoria dei gruppi. In particolare, ricordiamo i

Fatti (i) G gruppo finito, $x \in G$ _ L'ordine di x divide $|G|$ ← È il th. di Lagrange

(*) (ii) $n \geq 1$ _ Per ogni divisore d di n, $\mathbb{Z}/_n$ ha esatt. $\varphi(d)$ elt. di ordine d.

In tal caso, il nostro $\mathcal{F}$ è $\mathbb{Z}/_n$ e, per ogni d divisore di n,

$$\mathcal{F}_d = \{x \in \mathbb{Z}/_n \mid x \text{ ha ordine } d\}.$$

Per (ii), vale $|\mathcal{F}_d| = \varphi(d)$ e, per (i),

l'unione è disg perché ogni elt. ha un unico ordine!

$$\mathcal{F} = \bigsqcup_{\boxed{d \mid n}} \mathcal{F}_d$$

per Lagrange, ogni $x \in \mathbb{Z}/_n$ sta in uno degli $\mathcal{F}_d$ con $d \mid n$.

Si conclude esattamente come prima (fatelo!) $\square$

Esercizio (i) Elencare gli elementi di $\mathbb{Z}/_8$ a seconda del loro ordine.

(ii) Elencare i sgp. di $\mathbb{Z}/_8$ a seconda del loro ordine.

dim. (i) Usiamo la Proposizione appena mostrata. Abbiamo, in $\mathbb{Z}/_8$,

ordine	# elt.
8	$\varphi(8) = 4$
4	$\varphi(4) = 2$
2	$\varphi(2) = 1$
1	$\varphi(1) = 1$

Gli elt. di ordine 8 sono gli invertibili (mod 8), i.e. i numeri dispari, perciò

(usando la notazione della Prop.)

$$\mathcal{F}_8 = \{[1]_8, [3]_8, [5]_8, [7]_8\}.$$

L'unico elt. di ordine 1 è l'identità di $\mathbb{Z}/_8$, ie la classe di 0, perciò

$$\mathcal{F}_1 = \{[0]_8\}.$$

Infine,

$$\mathcal{F}_2 = \{[4]_8\},$$

$$\mathcal{F}_4 = \{[2]_8, [6]_8\}.$$

(ii) Ricordiamo che ogni sgp. di un gp. ciclico è a sua volta ciclico. Perciò, basta guardare i sgp della forma $\langle x \rangle$, al variare di $x \in \mathbb{Z}/_8$. Abbiamo

- $\langle [0]_8 \rangle = \{[0]_8\} =: 0$
- $\langle [1]_8 \rangle = \mathbb{Z}/_8$ perché $[1]_8$ ha ordine 8, e lo stesso vale per gli altri elt. di $\mathcal{F}_8$
- $\langle [2]_8 \rangle = \{[0]_8, [2]_8, [4]_8, [6]_8\}$,

  $\langle [6]_8 \rangle = \{[0]_8, [6]_8, [4]_8, [2]_8\}$,

  perciò $[2]_8, [6]_8$ generano lo stesso sottogruppo, che indichiamo con $2\mathbb{Z}/_{8\mathbb{Z}}$;
- $\langle [4]_8 \rangle = \{[0]_8, [4]_8\} =: 4\mathbb{Z}/_{8\mathbb{Z}}$.

In conclusione, abbiamo i seguenti sgp:

$$\mathbb{Z}/_{8\mathbb{Z}} = \langle [1]_8 \rangle = \langle [3]_8 \rangle = \langle [5]_8 \rangle = \langle [7]_8 \rangle$$

$$2\mathbb{Z}/_{8\mathbb{Z}} = \langle [2]_8 \rangle = \langle [6]_8 \rangle$$

$$4\mathbb{Z}/_{8\mathbb{Z}} = \langle [4]_8 \rangle$$

$$0 = \langle [0]_8 \rangle$$

Notiamo che hanno ordine 8, 4, 2, 1 rispettivamente, per cui una tabella analoga a quella del punto (i) è

ordine del sgp	# di sgp
8	1
4	1
2	1
1	1

$\square$

L'analisi dei sottogruppi di $\mathbb{Z}/_8$ mostra un fatto interessante: per ogni divisore di 8, c'è un unico sgp di ordine quel divisore.
È vero in generale? Sì! Notiamo che avete in realtà dimostrato il fatto (*) per ogni gp. ciclico finito, cioè

Fatto (**) G ciclico, $|G|=n$. Se $d|n$, G ha esatt. $\varphi(d)$ elt. di ordine d.

Esercizio Per ogni $n \geq 1$, $\mathbb{Z}/_n$ ha esattamente un sgp di ordine d per ogni divisore d di n.

dim Fissiamo un div. d di n. Sappiamo che $\mathbb{Z}/_n$ ha esattamente $\varphi(d)$ elt. di ordine d: fissiamone uno, diciamo $x \in \mathbb{Z}/_n$, e consideriamo $H = \langle x \rangle$. Allora, $|H| = |\langle x \rangle|$ è l'ordine di x, cioè proprio d: questo mostra che $\mathbb{Z}/_n$ ha almeno un sgp di ordine d.
Vediamo che H è anche l'unico. Poiché H è ciclico di ordine d, per il fatto (**) ha esatt. $\varphi(d)$ elt. di ordine d, ma lo stesso vale per $\mathbb{Z}/_n$! Necessariamente, allora, se y è un elt. di ordine d di $\mathbb{Z}/_n$, vale $y \in H$.
Sia ora K un qualsiasi sgp di ordine d di $\mathbb{Z}/_n$: sappiamo che dev'essere ciclico, generato da un elt. di ordine d, diciamo $\bar{y} \in \mathbb{Z}/_n$. Ma per quanto appena osservato, dev'essere $\bar{y} \in H$, da cui $K = \langle \bar{y} \rangle \subset H$. D'altra parte, $|K| = |H| = d$, perciò si conclude $K = H$. $\square$

Esercizio Risolvere la congruenza

$$2^{3x} \equiv 5 \pmod{41}.$$

dim. Perché la congruenza abbia soluzione, 5 dev'essere una potenza di 2 (mod 41).

Si nota in effetti che

$$2^7 \equiv 2^6 \cdot 2 \equiv 64 \cdot 2$$

$$\equiv 23 \cdot 2 \equiv 46 \equiv 5 \ (41),$$

per cui la congruenza diventa

$$2^{3x} \equiv 2^7 \pmod{41}.$$

Calcoliamo ora l'ordine di 2 in $\mathbb{Z}/_{41}^{\times} = \{ [i]_{41} \mid (i, 41) = 1 \}$. Notiamo che

$$2^{10} \equiv 2^7 \cdot 2^3 \equiv 5 \cdot 8 \equiv -1 \ (41),$$

da cui

$$2^{20} \equiv (2^{10})^2 \equiv 1 \ (41).$$

Questo dice che l'ordine di 2 divide 20, ma è $\neq 10$: siccome ogni divisore proprio di 20 divide 10, se ne conclude che dev'essere 20. Infatti, se $d \mid 20$ e $d \neq 20$, scrivo $10 = dk$, e se avessi $2^d \equiv 1 \ (40)$ avrei anche

$$2^{10} = 2^{dk} = (2^d)^k \equiv 1^k \equiv 1 \ (41) \ \text{⚡}.$$

In conclusione, 2 ha ordine moltiplicativo 20 (mod 41). Questo dice che gli esponenti a cui elevare 2 per ottenere $2^7 \pmod{41}$ sono esattamente $[7]_{20}$, perciò

$$2^{3x} \equiv 2^7 \ (41) \iff 3x \equiv 7 \ (20).$$

A questo punto, siccome 7 è un inverso di 3 (mod 20), ottengo

$$\iff x \equiv 7 \cdot 7 \equiv 9 \ (20),$$

perciò le soluzioni sono gli $x \equiv 9 \ (20)$. $\square$

DN 4.4.11 Se p è un primo, n è un intero positivo, sia

$$N = \frac{(np)^p - 1}{np - 1}.$$

(i) $(N, np-1) = 1$

(ii) Se q è primo t.c. $q \mid N$,

- $(q, np) = 1$
- $o([np]_q)$ in $\mathbb{Z}/_q{}^\times$?

(iii) Se q è primo, $q \mid N$, allora $q \equiv 1 \ (p)$

(iv) Esistono ∞ primi $\equiv 1 \ (p)$.

dim Notiamo un fatto preliminare. La fattorizzazione del polinomio $X^p - 1$ come

$$X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$$

fornisce, sostituendo $X = np$,

$$(np)^p - 1 = (np-1) \cdot ((np)^{p-1} + \cdots + np + 1),$$

da cui

$$N = \frac{(np)^p - 1}{np - 1} = (np)^{p-1} + \cdots + np + 1.$$

(i) Per mostrare $(N, np-1) = 1$, supponiamo per assurdo che q sia un primo che divide entrambi N, $np-1$. Ne segue che

(1) $np \equiv 1 \ (q)$

(2) $N \equiv 0 \ (q) \Rightarrow (np)^{p-1} + \cdots + np + 1 \equiv 0 \ (q)$,

e sostituendo (1) in (2) si ha

$$1^{p-1} + \cdots + 1 + 1 = p \equiv 0 \ (q),$$

cioè $q = p$. Ma chiaramente p non divide $np-1$, quindi tale q non può esistere.

(ii) Per il primo punto, dobbiamo mostrare che, se $q \mid N$, $q \neq p$ e q non divide n. Se $q = p$ oppure $q \mid n$, vale in effetti $np \equiv 0 \ (q)$, da cui

$$N = \underset{\substack{|||\\0}}{(np)^{p-1}} + \cdots + \underset{\substack{|||\\0}}{np} + 1 \equiv 1 \ (q),$$

cioè $q \nmid N$.

Ora, per calcolare l'ordine di $[np]_q$ in $\mathbb{Z}/_{q}^{\times}$, notiamo che

$$N \equiv 0 \ (q) \implies N \cdot (np-1) = (np)^p - 1 \equiv 0 \ (q),$$

cioè $(np)^p \equiv 1 \ (q)$: quindi, l'ordine di $[np]_q$ divide p, ed è quindi necessariamente 1 o p. Ma il punto (i) dice

$$q \mid N \implies np - 1 \not\equiv 0 \ (q),$$

cioè $np \not\equiv 1 \ (q)$, e pertanto $[np]_q$ ha ordine p.

(iii) Poiché $[np]_q$ ha ordine p in $\mathbb{Z}/_{q}^{\times}$, dev'essere $p \mid q-1$ per il Piccolo Th. di Fermat (o, equiv., per il Th. di Lagr. applicato a $\mathbb{Z}/_{q}^{\times}$). Questo vuol dire proprio $q \equiv 1 \ (p)$.

(iv) Supponiamo per assurdo che i primi $\equiv 1 \ (p)$ siano finiti, diciamo $q_1, \dots, q_k$. Se poniamo $n = q_1 \cdots q_k$, otteniamo che

$$N = \frac{(np)^p - 1}{np - 1}$$

verifica $q \mid N \implies q \equiv 1 \ (p)$. Ora, un primo q che divida N esiste perché N è evidentemente $\neq 1$ [altr. $(np)^p - 1 = np - 1 \Rightarrow (np)^p = np$, cioè $np = 1$], ma tale q non può essere nessuno dei q_i, perché

$$(np)^p - 1 \equiv -1 \ (q_i)$$

per ogni i, siccome $q_i \mid n$, e N è un divisore di $(np)^p - 1$ [perciò, se $q_i \nmid (np)^p - 1$, non può dividere nemmeno N].

Abbiamo allora trovato un primo $q \neq q_1, \dots, q_k$ t.c. $q \equiv 1 \ (p)$, il che è assurdo. $\square$