Corollari di aritmetica modulare

di Gabriel Antonio Videtta

31 luglio 2023

In questo breve documento dimostro ognuno dei seguenti teoremi di teoria dei numeri:

(i) il teorema di Wilson,

(ii) il teorema di Wolstenholme,

(iii) il teorema di Lagrange (per i polinomi).

Questi teoremi si dimostrano facilmente anche senza l'uso dei teoremi principali della teoria dei gruppi e degli anelli. Tuttavia, la loro vera natura è prettamente dovuta allo studio di queste due teorie – come si evince dalla brevità e dall'immediatezza delle dimostrazioni.

Il prerequisito fondamentale per approcciare questi tre teoremi è l'aver studiato il teorema di Lagrange di teoria dei gruppi (quantomeno per dimostrare i primi due teoremi)[1] e avere familiarità con gli anelli euclidei (per dimostrare il teorema di Lagrange).

Si presenta innanzitutto il seguente lemma:

Lemma 1. Sia p un numero primo. Sia $q \in \mathbb{Z}[x]$ il polinomio tale per cui:

$$q(x) = (x-1)(x-2)\cdots(x-(p-1)).$$

Allora, se

$$q(x) = x^{p-1} + a_{p-2}x^{p-2} + \ldots + a_1 x + a_0, \qquad a_i \in \mathbb{Z},\ 0 \leq i \leq p-1,$$

vale che $\hat{q}(x) = x^{p-1} - 1$, dove $\hat{q}$ è la proiezione in $\mathbb{Z}/p\mathbb{Z}$ di q.

Dimostrazione. Per il teorema di Lagrange, vale che $x^{p-1} - 1 \equiv 0\ (p)$ per ogni $x \in \mathbb{Z}/p\mathbb{Z}^*$, dal momento che $\mathbb{Z}/p\mathbb{Z}^*$ è un gruppo moltiplicativo di ordine $p-1$. Pertanto $\hat{q}$ e $x^{p-1}-1$ hanno le stesse radici e lo stesso grado, e sono dunque lo stesso polinomio, da cui la tesi. □

[1] Oppure il suo più semplice corollario, il piccolo teorema di Fermat.

Teorema (di Wilson)**.** Sia $p \in \mathbb{N}^+$. Allora $(p-1)! \equiv -1 \ (p)$ se e solo se p è primo.

Dimostrazione. Se $(p-1)! \equiv -1 \ (p)$, allora ogni elemento di $\mathbb{Z}/p\mathbb{Z}$ è invertibile, e quindi $\mathbb{Z}/p\mathbb{Z}$ sarebbe un campo; ciò è possibile se e solo se p è primo[2]. Se p è primo, per il *Lemma 1*, $\hat{q}(x) = x^{p-1} - 1$, e quindi p divide ogni a_i. Si osserva allora che $a_0 = (-1)^{p-1}(p-1)!$ e che deve dunque valere:

$$(-1)^{p-1}(p-1)! \equiv -1 \quad (p).$$

Sia che p sia uguale a 2, sia che p sia dispari, l'ultima equazione implica che:

$$(p-1)! \equiv -1 \quad (p),$$

da cui la tesi. □

Teorema (di Wolstenholme)**.** Sia $p \geq 5$ un numero primo. Allora il numeratore di:

$$S = 1 + \frac{1}{2} + \ldots + \frac{1}{p-1}$$

è divisibile per p^2.

Dimostrazione. Per il *Lemma 1*, p divide ogni a_i di q. Si osserva inoltre che a_1 è esattamente il numeratore di S.

Si computa q in p:

$$q(p) = p^{p-1} + a_{p-2}p^{p-2} + \ldots + a_1 p + a_0.$$

Analogamente:

$$q(p) = (p-1)(p-2)\cdots(p-(p-1)) = (p-1)! = (-1)^{p-1}a_0 = a_0,$$

dove si è usato che $p \geq 5$ è dispari. Quindi vale che:

$$p^{p-1} + a_{p-2}p^{p-2} + \ldots + a_1 p = 0,$$

da cui:

$$a_1 p = -(p^{p-1} + \ldots + a_2 p^2).$$

Poiché $p > 3$, p^3 divide il secondo membro dell'equazione, e quindi p^2 divide a_1, da cui la tesi. □

Teorema (di Lagrange, per i polinomi)**.** Sia q un polinomio in $\mathbb{Z}[x]$ e sia p un numero primo. Allora vale una delle seguenti due affermazioni:

- p divide ogni coefficiente di q,

[2]Infatti un campo è prima di tutto un dominio. Se p non fosse primo, $\mathbb{Z}/p\mathbb{Z}$ ammetterebbe divisori di zero.

- esistono al più $\deg q$ soluzioni incongruenti[3] di q in $\mathbb{Z}/p\mathbb{Z}$.

Dimostrazione. Si consideri la proiezione in $\mathbb{Z}/p\mathbb{Z}$ di q, indicata con $\hat{q}$. Poiché p è primo, $\mathbb{Z}/p\mathbb{Z}$ è un campo, e quindi $\mathbb{Z}/p\mathbb{Z}[x]$ è un anello euclideo. Pertanto, se $\hat{q}$ è diverso da 0, $\hat{q}$ ammette al più $\deg \hat{q}$ soluzioni in $\mathbb{Z}/p\mathbb{Z}$. In particolare vale che $\deg \hat{q} \leq \deg q$, e quindi $\hat{q}$ ammette al più $\deg q$ soluzioni in $\mathbb{Z}/p\mathbb{Z}$ (e quindi esistono al più $\deg q$ classi di resto che sono soluzione in $\mathbb{Z}/p\mathbb{Z}$). Se invece $\hat{q} = 0$, p deve dividere obbligatoriamente ogni coefficiente di q, da cui la tesi. □

[3]Due soluzioni x, $y \in \mathbb{Z}$ si dicono incongruenti se $x \not\equiv y \ (p)$.