Algebra n. 3 - NOTE ALLA LEZIONE 27

Dimostrazione del **Lemma 27.11**:

Sia a un intero non divisibile per p. Allora $[a]_p$ è un elemento invertibile, e quindi cancellabile, dell'anello $\mathbb{Z}_p$. Pertanto, dati due elementi distinti x e y di $\mathbb{Z}_p$, si ha che $ax = [a]_p x \neq [a]_p y = ay$. Nel momento in cui x e y appartengono a P, non sono l'uno l'opposto dell'altro, ossia $x \neq -y$, da cui, analogamente a sopra, si deduce che $ax \neq -ay$. Ne consegue che, all'interno di aP, non esistono coppie del tipo ax, $-ax$. In altri termini, due elementi distinti di aP non possono essere uno l'opposto dell'altro. D'altra parte, dalla cancellabilità di $[a]_p$ segue, come abbiamo visto, che gli elementi di aP sono tanti quanti P, ossia esattamente $\frac{p-1}{2}$. Quindi in ognuna delle $\frac{p-1}{2}$ coppie del tipo ax, $-ax$ è presente esattamente un elemento di aP. L'altro appartiene necessariamente ad aQ.

Una volta individuato, tra 1 e -1, il numero che è *congruo* ad $\left(\frac{a}{p}\right)$ modulo p, è chiaro che a quel numero il simbolo di Legendre $\left(\frac{a}{p}\right)$ sarà necessariamente *uguale*: infatti esso assume uno di quei valori, e questi sono non congrui modulo p. Si noti qui l'importanza di supporre p dispari.

Nota al **Teorema 27.12**:

L'enunciato del Teorema si può riformulare in forma equivalente affermando che il prodotto dei due simboli di Legendre $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$ è uguale a 1 se e solo se uno tra p e q è congruo a 1 modulo 4, se e solo se uno tra $\frac{p-1}{2}$ e $\frac{q-1}{2}$ è pari, se e solo se il loro prodotto è pari, se e solo se $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$.

Dimostrazione del **Teorema 27.12**:

Il numero μ conta gli elementi del tipo $q[x]_p$, con $1 \leq x \leq \frac{p-1}{2}$, (si noti che questi sono a due a due distinti, dato che q e p sono coprimi) che appartengono a Q, ossia coincidono con uno degli elementi $[-x]_p$, con $1 \leq x \leq \frac{p-1}{2}$. Anziché contare le classi $[x]_p$ con la proprietà considerata, si possono, equivalentemente, contare i loro rappresentanti canonici x. Questi sono precisamente i numeri interi x compresi tra 1 e $\frac{p-1}{2}$ tali che qx sia congruo, modulo p, ad uno dei numeri $-\frac{p-1}{2},\ldots,-1$.

Non può esistere più di un intero y tale che $-\frac{p}{2} < qx - py < 0$, in quanto, se y' è un altro intero tale che $-\frac{p}{2} < qx - py' < 0$, allora $-\frac{p}{2} < qx - py - (qx - py') < \frac{p}{2}$, ossia $-\frac{p}{2} < py' - py < \frac{p}{2}$, possibile solo se $y = y'$.

Una prima espressione del numero ν si ricava, naturalmente, scambiando, nell'espressione di μ, i numeri p e q. D'altra parte, però, è indifferente contare le coppie (x, y) oppure le coppie (y, x), dato che, come appena osservato, ogni x è associato ad uno e un solo y. Scambiando quindi, nell'espressione precedentemente ottenuta per ν, anche x e y, si perviene a quella indicata nel testo.