Numero dei polinomi irriducibili a coefficienti in un campo finito

Maurizio Cornalba

3/5/2014

Sia $q = p^h$, dove p è un numero primo e h è un intero positivo. Indichiamo con μ la funzione di Möbius:

$$\mu(m) = \begin{cases} 1 & \text{se } m = 1 \\ (-1)^k & \text{se } m \text{ è prodotto di } k \text{ primi distinti} \\ 0 & \text{altrimenti} \end{cases}$$

Vogliamo dimostrare il seguente risultato, dovuto a Gauss.

Teorema 1. *Il numero dei polinomi monici irriducibili di grado n a coefficienti in $\mathbb{F}_q$ è*

$$\frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$$

Sia P un polinomio monico irriducibile di grado n e sia α una sua radice. Allora $\mathbb{F}_q[\alpha]$ ha grado n su $\mathbb{F}_q$ e quindi è isomorfo a $\mathbb{F}_{q^n}$. Poiché $\mathbb{F}_{q^n}$ è una estensione galoisiana di $\mathbb{F}_q$ ne segue che P ha n radici distinte in $\mathbb{F}_{q^n}$. Osserviamo anche che se due polinomi monici irriducibili hanno una radice comune essi coincidono, per l'unicità del polinomio minimo. Dunque il numero che dobbiamo calcolare è

$$\frac{1}{n} \mathcal{R}_n$$

dove $\mathcal{R}_n$ è il numero degli elementi di $\mathbb{F}_{q^n}$ che hanno grado n su $\mathbb{F}_q$. In altre parole

$$\mathcal{R}_n = \#\Big(\mathbb{F}_{q^n} \smallsetminus \bigcup_{\substack{K \text{ sottocampo} \\ \text{proprio di } \mathbb{F}_{q^n}}} K\Big)$$

Scriviamo $n = \prod_{i=1}^{\ell} p_i^{e_i}$, dove $p_1, \ldots, p_\ell$ sono primi distinti. Notiamo che i sottocampi di $\mathbb{F}_{q^n}$ contenenti $\mathbb{F}_q$ sono quelli della forma $\mathbb{F}_{q^{(n/d)}}$, dove d è un divisore di n, e che tra questi i sottocampi propri massimali sono i campi $F_i = \mathbb{F}_{q^{(n/p_i)}}$. Dunque

$$\mathcal{R}_n = \#\Big(\mathbb{F}_{q^n} \smallsetminus \bigcup_{i=1}^{\ell} F_i\Big) \tag{1}$$

Per calcolare la cardinalità dell'unione degli F_i useremo un risultato combinatorio classico. Siano $X_1, \ldots, X_\ell$ insiemi finiti. Se $i_1, \ldots, i_s \in \{1, \ldots, \ell\}$ poniamo $X_{i_1 \ \ldots \ i_s} = X_{i_1} \cap X_{i_2} \cap \cdots \cap X_{i_s}$. Il risultato di cui faremo uso è il seguente

Lemma 1.

$$\#\Big(\bigcup_{i=1}^{\ell} X_i\Big) = \sum_{s=1}^{\ell} (-1)^{s-1} \sum_{i_1 < i_2 < \cdots < i_s} \#(X_{i_1 \ \ldots \ i_s})$$

Dimostrazione. Ragioniamo per induzione su ℓ. Se $\ell = 2$ l'enunciato si riduce a $\#(X_1 \cup X_2) = \#(X_1) + \#(X_2) - \#(X_1 \cap X_2)$. Se supponiamo il risultato dimostrato per unioni di meno di ℓ insiemi possiamo scrivere

$$\begin{aligned}
\#\Big(\bigcup_{i=1}^{\ell} X_i\Big) &= \#\Big(\bigcup_{i=1}^{\ell-1} X_i\Big) + \#(X_\ell) - \#\Big(\Big(\bigcup_{i=1}^{\ell-1} X_i\Big) \cap X_\ell\Big) \\
&= \sum_{s=1}^{\ell-1}(-1)^{s-1} \sum_{i_1<\cdots<i_s<\ell} \#(X_{i_1\ \dots\ i_s}) + \#(X_\ell) - \#\Big(\bigcup_{i=1}^{\ell-1} X_i \cap X_\ell\Big) \\
&= \sum_{s=1}^{\ell-1}(-1)^{s-1} \sum_{i_1<\cdots<i_s<\ell} \#(X_{i_1\ \dots\ i_s}) + \#(X_\ell) \\
&\quad - \sum_{s=1}^{\ell-1}(-1)^{s-1} \sum_{i_1<\cdots<i_s<\ell} \#(X_{i_1\ \dots\ i_s\ \ell}) \\
&= \sum_{s=1}^{\ell}(-1)^{s-1} \sum_{i_1<i_2<\cdots<i_s} \#(X_{i_1\ \dots\ i_s})
\end{aligned}$$

□

Applichiamo il lemma appena dimostrato alla (1) osservando che, quando $i_1, \dots, i_s$ sono distinti,

$$F_{i_1\ \dots\ i_s} = F_{i_1} \cap F_{i_2} \cap \cdots \cap F_{i_s} = \mathbb{F}_{q^{\frac{n}{p_{i_1}\cdots p_{i_s}}}}$$

Si ottiene

$$\begin{aligned}
\mathcal{R}_n &= q^n + \sum_{s=1}^{\ell}(-1)^s \sum_{i_1<\cdots<i_s} \#\Big(\mathbb{F}_{q^{\frac{n}{p_{i_1}\cdots p_{i_s}}}}\Big) \\
&= q^n + \sum_{s=1}^{\ell}(-1)^s \sum_{i_1<\cdots<i_s} q^{\frac{n}{p_{i_1}\cdots p_{i_s}}} \\
&= q^n + \sum_{s=1}^{\ell} \sum_{i_1<\cdots<i_s} \mu(p_{i_1}\cdots p_{i_s}) q^{\frac{n}{p_{i_1}\cdots p_{i_s}}}
\end{aligned}$$

Ponendo $\frac{n}{p_{i_1}\cdots p_{i_s}} = d$ e ricordando che $\mu(m) = 0$ quando nella fattorizzazione di m vi sono primi ripetuti, ciò equivale a

$$\mathcal{R}_n = q^n + \sum_{d\Big|n, d\neq n} \mu\left(\frac{n}{d}\right) q^d = \sum_{d\Big|n} \mu\left(\frac{n}{d}\right) q^d$$

che è quanto andava dimostrato.