Polinomi irriducibili su campi finiti

29 Ottobre 2009

Definizione 1. *Sia* $f(x) \in \mathrm{GF}(q)[x]$ *un polinomio. Si dice* campo di spezzamento *di* $f(x)$ *il più piccolo campo* $\mathbb{K}$ *con* $\mathrm{GF}(q) \leq \mathbb{K}$ *contenente tutte le radici di* $f(x)$.

Osserviamo che $f(x)$, nel suo campo di spezzamento, si scrive sempre come prodotto di fattori lineari. Ad esempio, consideriamo

$$f(x) = x^3 - x^2 + x - 1 \in \mathrm{GF}(3)[x].$$

Il polinomio $f(x)$ si fattorizza in $\mathrm{GF}(3)[x]$ come prodotto di irriducibili $f(x) = (x^2+1)(x-1) \in \mathbb{Z}_3[x]$. Osserviamo che il fattore $f_1(x) = (x^2+1)$ è irriducibile du $\mathrm{GF}(3)$; pertanto $\mathrm{GF}(9) \simeq \mathrm{GF}(3)(\alpha)$, ove α è una sua radice. Ne segue che

$$f(x) = (x-\alpha)(x+\alpha)(x-1)$$

in $\mathrm{GF}(9)$, cioè che $\mathrm{GF}(9)$ è il campo di spezzamento di $f(x)$.

Osserviamo che il campo di spezzamento di un polinomio irriducibile $f(x) \in \mathrm{GF}(q)[x]$ di grado n è $\mathrm{GF}(q^n)$.

Teorema 2. *Sia* $f(x) \in \mathrm{GF}(q)[x]$ *un polinomio irriducibile su* $\mathrm{GF}(q)$ *e supponiamo che* α *sia una sua radice, presa in una opportuna estensione algebrica. Allora, per ogni* $h(x) \in \mathrm{GF}(q)[x]$ *si ha* $h(\alpha) = 0$ *se, e solamente se,* $f(x)$ *divide* $h(x)$.

Dimostrazione. Per il teorema di estensione, l'insieme

$$I_\alpha = \{p(x) \in \mathrm{GF}(q)[x] : p(\alpha) = 0\}$$

è un ideale proprio. Chiaramente, $f(x) \in I_\alpha$. Poiché $\mathrm{GF}(q)[x]$ è un dominio ad ideali principali, esiste $g(x)$ tale che

$$I_\alpha = \{g(x)q(x) : q(x) \in \mathrm{GF}(q)[x]\}.$$

In particolare, $g(x)$ deve dividere $f(x)$ e $\deg g(x) \geq 1$. Per l'irrudicibilità di $f(x)$ abbiamo $g(x) = af(x)$, ove $a \in \mathrm{GF}(q)$. In particolare, anche $f(x)$ è un generatore di I_α. Ne segue che $f(x)$ divide ogni polinomio $h(x) \in I_\alpha$, ovvero ogni $h(x)$ con $h(\alpha) = 0$. □

Il seguente teorema consente di caratterizzare i polinomi irriducibili il cui grado divide un intero n prefissato.

Teorema 3. *Sia* $f(x) \in \mathrm{GF}(q)[x]$ *un polinomio irriducibile su* $\mathrm{GF}(q)$ *per cui* $\deg f(x) = m$. *Allora,* $f(x)$ *divide* $x^{q^n} - x$ *se, e solamente se,* m *divide* n.

Dimostrazione. Rammentiamo che per ogni $\xi \in \mathrm{GF}(q^n)$ si ha

$$\xi^{q^n} - \xi = 0;$$

pertanto gli elementi di $\mathrm{GF}(q^n)$ sono tutte e sole le radici del polinomio $g(x) = x^{q^n} - x$. Sia ora α una radice di $f(x)$ nel suo campo di spezzamento su $\mathrm{GF}(q)$.

- Supponiamo $f(x)$, polinomio irriducibile, divida $g(x) = x^{q^n} - x$. Allora, $\alpha^{q^n} = \alpha$, per cui $\alpha \in \mathrm{GF}(q^n)$. Ne segue che $\mathrm{GF}(q)(\alpha)$ è un sottocampo di $\mathrm{GF}(q^n)$. D'altro canto $[\mathrm{GF}(q)(\alpha) : \mathrm{GF}(q)] = m$ e $[\mathrm{GF}(q^n) : \mathrm{GF}(q)] = n$, per cui m deve dividere n.
- Se m divide n, allora $\mathrm{GF}(q^n)$ contiene $\mathrm{GF}(q^m)$ come sottocampo. Osserviamo che $[\mathrm{GF}(q)(\alpha) : \mathrm{GF}(q)] = m$, poiché $f(x)$ è irriducibile, per cui $\mathrm{GF}(q)(\alpha) = \mathrm{GF}(q^m)$. Conseguentemente $\alpha \in \mathrm{GF}(q^m) \subseteq \mathrm{GF}(q^n)$ e dunque $\alpha^{q^n} = \alpha$, cioè α è radice di $g(x) = x^{q^n} - x$. Per il Teorema 2, si ha che $f(x)$ divide $g(x)$.

□

Teorema 4. *Sia* n *un intero positivo. Il prodotto di tutti i polinomi monici irriducibili su* $\mathrm{GF}(q)$ *il cui grado divide* n *è*

$$g(x) = x^{q^n} - x.$$

Dimostrazione. Per il Teorema 3, tutti i polinomi monici irriducibili su $\mathrm{GF}(q)$ il cui grado divide n sono fattori di $g(x) = x^{q^n} - x$. Questi, chiaramente, sono *tutti* i fattori irriducibili di $g(x)$. D'altro canto

$$g'(x) = -1,$$

per cui $g(x)$ non ha radici multiple nel suo campo di spezzamento. Pertanto ogni polinomio monico che compare nella fattorizzazione di $g(x)$ vi appare un'unica volta. La tesi segue. □

Il Teorema 4 ha svariate conseguenze. Mostriamo dapprima come esso possa essere usato per contare il numero di polinomi irriducibili di grado n. Premettiamo un corollario.

Corollario 5. *Sia* $N_q(d)$ *il numero di polinomi monici irriducibili su* $\mathrm{GF}(q)[x]$ *aventi grado* d*. Allora, per ogni intero positivo* n*,*

$$q^n = \sum_{d|n} dN_q(d). \tag{1}$$

Dimostrazione. Per ogni d, poniamo

$$\mathfrak{F}_d = \{f(x) \in \mathrm{GF}(q)[x] : f(x) \text{ monico, irriducibile e } \deg f(x) = d\}.$$

Per il Teorema 4,

$$x^{q^n} - x = \prod_{d|n} \prod_{f(x)\in\mathfrak{F}_d} f(x). \tag{2}$$

Estraendo il grado, si ottiene

$$q^n = \deg(x^{q^n} - x) = \sum_{d|n} \sum_{f(x)\in\mathfrak{F}_d} \deg f(x) = \sum_{d|n} dN_q(d),$$

da cui discende la tesi. □

Problema: ricavare i valori di $N_q(d)$.

Ci servono alcuni strumenti di teoria dei numeri.

Definizione 6. *La funzione di Moebius* $\mu : \mathbb{Z} \to \{-1, 0, 1\}$ *è la funzione*

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ (-1)^k & \text{se } n \text{ è il prodotto di } k \text{ fattori primi distinti} \\ 0 & \text{se } n \text{ è divisibile per il quadrato di un primo.} \end{cases}$$

Il seguente teorema è un risultato preliminare, necessario per la formula d'inversione.

Teorema 7. *Per ogni* $n \in \mathbb{Z}$ *si ha*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1. \end{cases}$$

Dimostrazione.

- Per $n = 1$, allora la somma è $\mu(1) = 1$.

- Per $n > 1$ basta considerare i divisori d di n tali che $\mu(d) \neq 0$, cioè i d che sono prodotto di primi distinti. Siano $p_1, p_2, \ldots, p_k$ i fattori primi distinti di n; abbiamo

$$\begin{aligned}\sum_{d|n} \mu(d) = \; & \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq k} \mu(p_{i_1} p_{i_2}) + \cdots + \mu(p_1 p_2 \cdots p_k) = \\ & 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = \\ & (1 + (-1))^k = 0.\end{aligned}$$

□

Teorema 8 (Formula di inversione di Moebius)**.** *Siano* h *e* H *due funzioni da* $\mathbb{Z}$ *in un gruppo abeliano* $(G, +)$*. Allora,*

$$H(n) = \sum_{d|n} h(d) \tag{3}$$

se, e solamente se,

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right). \tag{4}$$

Dimostrazione. Osserviamo che se d è un divisore di n, allora anche $\frac{n}{d}$ lo è. In particolare,

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right).$$

D'altro canto, per la (3),

$$\sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|(n/d)} h(c).$$

Scambiando l'ordine delle sommatorie,

$$\sum_{d|n} \mu(d) \sum_{c|(n/d)} h(c) = \sum_{c|n} \sum_{d|(n/c)} \mu(d) h(c) = \sum_{c|n} h(c) \sum_{d|(n/c)} \mu(d).$$

Applicando ora il Teorema 7, tenuto conto che per $c \neq n$, $n/c > 1$,

$$\sum_{c|n} h(c) \sum_{d|(n/c)} \mu(d) = h(n).$$

Il viceversa è analogo. □

Teorema 9. *Il numero* $N_q(n)$ *di polinomi monici irriducibili in* $\mathrm{GF}(q)[x]$ *aventi grado* n *è dato da*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Dimostrazione. Usiamo il Teorema 8, ponendo $h(n) = nN_q(n)$ e $H(n) = q^n$: per (1), l'uguaglianza (3) è soddisfatta. Pertando, usando (4),

$$nN_q(n) = h(n) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) q^{n/d}.$$

□

A titolo di esempio calcoliamo il numero di polinomi monici irriducibili di grado 20 su $\mathrm{GF}(q)$. Poiché $20 = 2^2 \times 5$, i fattori d di 20 per cui $\mu(d) \neq 0$ sono $1, 2, 5, 10$. Ne segue

$$N_q(20) = \frac{1}{20} \left(q^{20} - q^{10} - q^4 + q^2\right).$$

Corollario 10. *Il numero di polinomi irriducibili di grado* n *su* $\mathrm{GF}(q)$ *si può stimare mediante:*

$$N_q(n) \geq \frac{1}{n} \left(q^n - \frac{q^n - q}{q - 1}\right).$$

In particolare $N_q(n) > 0$ *per ogni* q *ed* $n > 1$.

Dimostrazione. Si ha

$$\sum_{d|n} \mu(d) q^{n/d} = q^n + \sum_{d|n, d\neq 1} \mu(d) q^{n/d} \geq q^n - \sum_{d|n, d\neq 1} q^{n-d} \geq q^n - \sum_{i=1}^{n-1} q^i = q^n - \frac{q^n - q}{q - 1}.$$

La tesi segue. □

Una stima migliore sul numero di polinomi irriducibili è la seguente:

$$\frac{q^n}{n} - \frac{q(q^{n/2} - 1)}{n(q - 1)} \leq N_q(n) \leq \frac{q^n - q}{n}.$$

In generale, il significato dei risultati sopra presentati è che circa 1 polinomio su n di grado n, selezionato a caso, è irriducibile.

Come applicazione dei risultati sopra mostrati presentiamo un test di irriducibilità, dovuto a Ben–Or, per polinomi su campi finiti.

Teorema 11. *Un polinomio* $f(x) \in \mathrm{GF}(q)[x]$ *di grado* n *è irriducibile se, e solamente se, per ogni* $i = 1, \ldots n/2$, $h_i(x) = \gcd(f(x), x^{q^i} - x) = 1$.

Dimostrazione. Supponiamo che $f(x)$ sia riducibile; chiaramente $f(x)$ deve ammettere almeno un fattore irriducibile $f_1(x)$ di grado $d \leq n/2$. Ne segue che tale fattore deve dividere $g_d(x) = x^{q^d} - x$ con $d \leq n/2$; in particolare,

$$f_1(x) | \gcd(f(x), x^{q^d} - x) = h_d(x),$$

e, dunque, $h_d(x) \neq 1$. Viceversa, se $h_d(x) \neq 1$, allora abbiamo un fattore non banale di $f(x)$; pertanto $f(x)$ è riducibile. □

Esempio: consideriamo il polinomio

$$f(x) = x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1$$

in $\mathrm{GF}(3)$. Mostriamo che esso è irriducibile. Poiché $\deg f(x) = 7$, usando il Teorema 11 dobbiamo calcolare

$$\gcd(f(x), g_1(x)), \gcd(f(x), g_2(x)), \gcd(f(x), g_3(x)),$$

ove $g_1(x) = x^3 - x$, $g_2(x) = x^9 - x$ e $g_3(x) = x^{27} - x$. Possiamo procedere applicando l'algoritmo euclideo. Si verifica che tutti e tre i massimi comuni divisori sono 1. Ne segue che $f(x)$ è irriducibile in $\mathrm{GF}(3)[x]$. In particolare, si ha

$$\frac{\mathrm{GF}(3)}{(f(x))} \simeq \mathrm{GF}(3^7).$$