Tre metodi per calcolare il polinomio $f_{\cos 2\pi/n}$

AL310 – 2016/17

November 7, 2016

In questa nota, il polinomio $\Psi_n(X) = f_{2\cos 2\pi/n}(X) \in \mathbf{Z}[X]$ indica il polinomio minimo del numero algebrico $2\cos 2\pi/n = \zeta_n + \bar{\zeta}_n$ dove $\zeta_n = e^{2\pi i/n}$ è una radice primitiva n–esima dell'unità.

Inoltre indichiamo con $\Phi_n(X) = f_{\zeta_n}(X)$ l'n–esimo polinomio ciclotomico.

Fatti che utilizzeremo:

1. $\Phi_n(X) \in \mathbf{Z}[X]$ è monico, irriducibile e $\deg \Phi_n = \varphi(n)$;
2. $\bar{\zeta}_n = \zeta_n^{n-1} = \zeta_n^{-1}$;
3. $[\mathbf{Q}[\zeta_n] : \mathbf{Q}] = \deg \Phi_n = \varphi(n)$;
4. $[\mathbf{Q}[\cos 2\pi/n] : \mathbf{Q}] = \deg \Psi_n = \frac{1}{2}\varphi(n)$;
5. $2^{-\varphi(n)/2}\Psi_n(2X) = f_{2\cos 2\pi/n}(X)$.

1 Il sistema lineare

Si parte dall'identità $\Phi_n(\zeta_n) = 0$ che può essere usata come strumento per scrivere tutti gli elementi di $\mathbf{Q}[\zeta_n]$ nella forma

$$a_0 + a_1\zeta_n + \cdots + a_{\varphi(n)-1}\zeta_n^{\varphi(n)-1}.$$

Vogliamo determinare i numeri interi $A_0, \ldots, A_M$ tali che

$$\Psi_n(X) = A_0 + A_1X + \cdots + A_MX^M,$$

dove $M = \frac{1}{2}\varphi(n)$. Si parte dall'identità:

$$\Psi_n(2\cos\frac{2\pi}{n}) = \Psi_n\left(\zeta_n + \zeta_n^{n-1}\right) = 0.$$

che può essere scritta come

$$A_0 + A_1\left(\zeta_n + \zeta_n^{\varphi(n)-1}\right) + \cdots + A_M\left(\zeta_n + \zeta_n^{\varphi(n)-1}\right)^M = 0$$

e, in quanto elemento di $\mathbf{Q}[\zeta_n]$, la quantità sopra può essere riscritta nella forma seguente:

$$c_0 + c_1\zeta_n + \cdots + c_{n-1}\zeta_n^{n-1} = 0.$$

dove per ogni j, $0 \le j < \varphi(n)$, $c_j = c_j(A_0, A_1, \ldots, A_M)$ è lineare (i.e. una combinazione lineare degli A_j) nelle variabili $A_0, A_1, \ldots, A_M$. Risolvendo il sistema lineare

$$\begin{cases} c_0(A_0, A_1, \ldots, A_M) & = & 0 \\ c_1(A_0, A_1, \ldots, A_M) & = & 0 \\ & \vdots & \\ c_{\varphi(n)-1}(A_0, A_1, \ldots, A_M) & = & 0 \end{cases}$$

si ottengono i coefficienti $A_0, A_1, \ldots, A_M$.

ESEMPIO DEL CALCOLO DI Ψ_9: Il nono polinomio ciclotomico è $\Phi_9(X) = \Phi_3(X^3) = X^6 + X^3 + 1$ da cui deduciamo: $\zeta_9^6 = -1 - \zeta_9^3$. Il grado $\deg \Psi_9 = 3$. Pertanto$\Psi_9(X) = A_0 + A_1X + A_2X^2 + X^3$. Sostituendo $2\cos\frac{2\pi}{9} = \zeta_9 + \zeta_9^8$, otteniamo

$$A_0 + A_1\left(\zeta_9 + \zeta_9^8\right) + +A_2\left(\zeta_9 + \zeta_9^8\right)^2 + \left(\zeta_9 + \zeta_9^8\right)^3.$$

Facendo i calcoli otteniamo:

$$(A_0 + A_2 - 1) + (A_1 - A_2 + 3)\,\zeta_9 + (-A_1 + A_2 - 8)\,\zeta_9^2 + (-A_2)\,\zeta_9^4 + (-A_1 - 3)\,\zeta_9^5.$$

Da cui otteniamo il sistema lineare:

$$\begin{cases} A_0 + A_2 - 1 &= 0 \\ A_1 - A_2 + 3 &= 0 \\ -A_1 + A_2 - 3 &= 0 \\ -A_2 &= 0 \\ -A_1 - 3 &= 0 \end{cases}$$

che ha per soluzioni $A_0 = 1, A_1 = -3, A_2 = 0$. Infine $\Psi(X) = X^3 - 3X + 1$.

2 il trucco ciclotomico

Questo metodo consiste nell'utilizzo della seguente identità:

$$X^M \Psi\left(X + \frac{1}{X}\right) = \Phi_n(X).$$

Tale identità segue dal fatto che la quantità di sinitra è un polinomio monico a coefficienti razionali di grado $2M$. Inoltre $\Psi_n\left(\zeta_n + \zeta_n^{-1}\right) = \Psi_n\left(2\cos\frac{2\pi}{n}\right) = 0$. Dall'unicità del polinomio minimo segue l'identità con il polinomio ciclotomico.

Se scriviamo

$$\Phi_n(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{2M-1}X^{2M-1} + X^{2M} \quad \text{e} \quad \Psi(X) = A_0 + A_1 X + \cdots + A_{M-1}X^{M-1} + X^M,$$

allora

$$\begin{aligned} X^M \Psi_n\left(X + \frac{1}{X}\right) &= A_0 X^M + A_1 X^{M-1}\left(X^2+1\right) + \cdots + A_{M-1}X(X^2+1)^{M-1} + \left(X^2+1\right)^M \\ &= b_0 + b_1 X + \cdots + b_{2M-1}X^{2M-1} + X^{2M} \end{aligned}$$

dove, per ogni j, $0 \le j < 2M$, $b_j = b_j(A_0, A_1, \ldots, A_M)$ è lineare (i.e. una combinazione lineare) nelle variabili $A_0, A_1, \ldots, A_M$. Risolvendo il sistema lineare

$$\begin{cases} b_0(A_0, A_1, \ldots, A_M) &= \alpha_0 \\ b_1(A_0, A_1, \ldots, A_M) &= \alpha_1 \\ &\vdots \\ b_{2M-1}(A_0, A_1, \ldots, A_M) &= \alpha_{2M-1} \end{cases}$$

si ottengono i coefficienti $A_0, A_1, \ldots, A_M$. Si noti che non è difficile verificare che $b_0 = 1$, $b_1 = 2A_{M-1}$, $b_2 = M$

ESEMPIO DEL CALCOLO DI $f_{2\cos\frac{2\pi}{9}}$: L'identità $X^3\Psi_3\left(X + \frac{1}{X}\right) = \Phi_9(X)$ è equivalente a

$$X^6 + X^3 + 1 = X^6 + A_2X^5 + (A_1+3)\,X^4 + (A_0 + A_2)\,X^3 + (A_1+3)\,X^2 + A_2X + 1$$

da cui deduciamo $A_2 = 0$, $A_1 = -3$, $A_2 = 1$ e $f_{\cos\frac{2\pi}{9}}(X) = X^3 - 3X + 1$.

3 per ottenere un multiplo del polinomio minimo

Se si sfrutta il fatto che $\zeta_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ e si considera l'identità $\Phi_n(\zeta_n) = 0$. Scriviamo

$$\Re\Phi_n(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}) = \Re\left(\alpha_0 + \alpha_1\zeta_n + \cdots + \alpha_{2M-1}\zeta_n^{2M-1} + \zeta_n^{2M}\right) = 0$$

e osserviamo che $\Re\zeta_n^k = \cos\frac{k\pi}{n}$.

Affermiamo che per ogni $k \in \mathbf{N}$ esistono due polinomi $g_k(X), h_k(X) \in \mathbf{Z}[X]$ tali che $\cos k\alpha = g_k(\cos\alpha)$ e $\sin k\alpha = \sin\alpha h_k(\cos\alpha)$. Ciò è chiaro per $k = 1$. Inoltre dalla formula di duplicazione per il coseno, si ottiene $\cos 2\alpha = 2\cos^2\alpha - 1$ e $\sin 2\alpha = 2\sin\alpha\cos\alpha$. In generale,

$$\begin{aligned} \cos(k+1)\alpha &= \cos\alpha\cos k\alpha - \sin\alpha\sin k\alpha = \cos\alpha \times g_k(\cos\alpha) - (1-\cos^2\alpha)h_k(\cos k\alpha) \\ \sin(k+1)\alpha &= \sin\alpha\cos k\alpha + \cos\alpha\sin k\alpha = \sin\alpha \times (g_k(\cos\alpha) + \cos\alpha h_k(\cos k\alpha)). \end{aligned}$$

Quindi g_k e h_k soddisfano le relazioni ricorsive:

$$\begin{cases} g_1(X) = X \\ g_{k+1}(X) = X \times g_k(X) - (1 - X^2)h_k(X), \end{cases} \qquad \begin{cases} h_1(X) = X \\ h_{k+1}(X) = g_k(X) + X \times h_k(X). \end{cases}$$

E' anche facile dimostrare per induzione che $\deg g_k = k$ e $\deg h_k = k - 1$.

Da questa osservazione deduciamo:

$$\alpha_0 + \alpha_1 g_1(\cos \frac{2\pi}{n}) + \cdots + \alpha_{2M-1} g_{2M-1}(\cos \frac{2\pi}{n}) + g_{2M}(\cos \frac{2\pi}{n}) = 0$$

Quindi, il polinomio

$$U_n(X) := \alpha_0 + \alpha_1 g_1(X) + \cdots + \alpha_{2M-1} g_{2M-1}(X) + g_{2M}(X) \in \mathbf{Z}[X]$$

ha la proprietà di avere $\cos \frac{2\pi}{n}$ come radice. Pertanto $\Psi_n(X)$ divide $U_n(X)$.

ESEMPIO DEL CALCOLO DI $f_{\cos \frac{2\pi}{9}}$: Partendo dall'identità $\Phi_9(X) = X^6 + X^3 + 1$, otteniamo

$$U_9(X) = 1 + g_3(X) + g_6(X) = 1 + (4X^3 - 3X) + (32X^6 - 48X^4 + 18X^2 - 1)$$

Quindi, fattorizzando U_9, si ottiene: $U_9(X) = 32X^6 - 48X^4 + 4X^3 + 18X^2 - 3X = X(4X^2 - 3)(8X^3 - 6X + 1)$. Sapendo che $\deg \Psi_9 = 3$, deduciamo che $\Psi_9(X/2) = X^3 - \frac{3}{4}X + \frac{1}{8}$.

Si noti che dall'identità $\zeta_n^n = 1$ si deduce anche che, per $n > 1$, $\Psi_n \mid \gcd(g_n, h_n)$.

4 la trigonometria

ANCORA DA SCRIVERE

ESEMPIO DEL CALCOLO DI $f_{\cos \frac{2\pi}{9}}$