S.Giuseppe

Scomposizioni polinomiali

(pubblicazione web del 19-03-2013)

In questa pagina ci occupiamo dei polinomi ciclotomici, una categoria particolare di polinomi irriducibili a cui ci conduce lo studio sui numeri interi, trattato nel libro: "N esp1 - Un ordinamento possibile dei numeri primi".
Un concetto fondamentale di cui si deve tenere conto è lo stretto legame che intercorre tra aritmetica e algebra.
Ne sia esempio la numerazione posizionale decimale: la scrittura di un numero altro non è che la scrittura semplificata di un polinomio.
Ad esempio, nel seguente caso si ha:

$$1234057 = 1\cdot10^6+2\cdot10^5+3\cdot10^4+4\cdot10^3+0\cdot10^2+5\cdot10+7$$

Alla base dello studio dei polinomi ci sono i polinomi completi e ordinati di grado n, a coefficienti tutti uguali a 1:

$$f(x) = x^n + x^{n-1} + \ldots + x^2 + x + 1$$

Per questi polinomi è sempre possibile stabilire se sono scomponibili o irriducibili e, nel caso in cui sono scomponibili, è sempre possibile ricavare i loro divisori.
I divisori irriducibili di questi polinomi monici sono denominati

polinomi ciclotomici

Ecco l'elenco ordinato dei primi 100:

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\Phi_6(x) = x^2 - x + 1$

>>> per continuare l'elenco cliccare qui

In determinati casi i polinomi di questo elenco illimitato si possono ottenere senza che sia necessario alcun calcolo: è sufficiente attenersi a delle regole.
Per scomporre i polinomi completi f(x) sono fondamentali i polinomi ciclotomici elencati sopra, ma si deve tenere presente il loro ordine.
Se n è il grado del polinomio completo f(x), i suoi termini sono p=n+1 e p indica il suo ordine:

$$f_p(x) = x^n + x^{n-1} + \ldots + x^2 + x + 1 \quad (p=n+1)$$

Se p è numero primo $f_p(x)$ è irriducibile, per cui esso stesso è un polinomio ciclotomico.
Se p invece non è primo, $f_p(x)$ è scomponibile e, per trovare tutti i suoi fattori polinomiali, ci viene in aiuto la scomposizione in fattori primi del numero p. Vediamo in che modo, facendo degli esempi pratici.

* Scomponiamo il polinomio: $f_4(x) = x^3 + x^2 + x + 1$
Questo polinomio completo di 3° grado ha ordine 4 (p=4); per scomporlo troviamo i divisori del 4: $D_4=\{1, 2, 4\}$
Da qui ne segue che i divisori di $f_4(x)$ sono i polinomi ciclotomici di ordine 1, 2 e 4: $\Phi_1(x)$, $\Phi_2(x)$, $\Phi_4(x)$
Ma $\Phi_1(x)$ ha la funzione di elemento neutro e non va considerato (in linea generale).
Procediamo con la scomposizione del polinomio, prendendo i polinomi ciclotomici $\Phi_2(x)$ e $\Phi_4(x)$ dalla tabella:

$$f_4(x) = \Phi_2(x)\cdot\Phi_4(x) \quad >>> \quad x^3 + x^2 + x + 1 = (x+1)(x^2+1)$$

* Scomponiamo il polinomio completo di ordine 12: $f_{12}(x) = x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
I divisori di 12 sono: $D_{12}=\{1, 2, 3, 4, 6, 12\}$, quindi i divisori del polinomio $f_{12}(x)$ sono i polinomi ciclotomici:

$$\Phi_2(x) = x + 1 \ ; \ \Phi_3(x) = x^2 + x + 1 \ ; \ \Phi_4(x) = x^2 + 1 \ ; \ \Phi_6(x) = x^2 - x + 1 \ ; \ \Phi_{12}(x) = ?$$

Poiché il polinomi ciclotomico $\Phi_{12}(x)$ non è nella tabella, lo dobbiamo ricavare dall'uguaglianza:

$$x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 = (x+1)\cdot(x^2+x+1)\cdot(x^2+1)\cdot(x^2-x+1)\cdot\Phi_{12}(x)$$

eseguendo delle divisioni tra polinomi.
Tuttavia, in questo caso, le divisioni, certamente lunghe e tediose, non è necessario eseguirle: il polinomio ciclotomico $\Phi_{12}(x)$ è tra quelli che si possono ricavare in modo semplice, applicando le regole: $\Phi_{12}(x) = x^4 - x^2 + 1$
Quindi: $x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 = (x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1)$

* Scomponiamo il polinomio di ordine 3025: $f_{3025}(x) = x^{3024} + x^{3023} + \ldots + x^2 + x + 1$
Anche in questo caso si arriva rapidamente al risultato richiesto, perché tutti i polinomi irriducibili della scomposizione si possono ricavare applicando le regole.

Dato che $D_{3025} = \{1, 5, 11, 25, 55, 121, 275, 605, 3025\}$, i divisori ciclotomici di $f_{3025}(x)$ sono:

$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

$\Phi_{11}(x) = x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$

$\Phi_{25}(x) = x^{20}+x^{15}+x^{10}+x^5+1$

$\Phi_{55}(x) = x^{40}-x^{39}+x^{35}-x^{34}+x^{30}-x^{28}+x^{25}-x^{23}+x^{20}-x^{17}+x^{15}-x^{12}+x^{10}-x^6+x^5-x+1$

$\Phi_{121}(x) = x^{66}+x^{55}+x^{44}+x^{33}+x^{22}+x^{11}+1$

$\Phi_{275}(x) = x^{200}-x^{195}+x^{175}-x^{170}+x^{150}-x^{140}+x^{125}-x^{115}+x^{100}-x^{85}+x^{75}-x^{60}+x^{50}-x^{30}+x^{25}-x^5+1$

$\Phi_{605}(x) = x^{440}-x^{429}+x^{385}-x^{374}+x^{330}-x^{308}+x^{275}-x^{253}+x^{220}-x^{187}+x^{165}-x^{132}+x^{110}-x^{66}+x^{55}-x^{11}+1$

$\Phi_{3025}(x) = x^{2200}-x^{2145}+x^{1925}-x^{1870}+x^{1650}-x^{1540}+x^{1375}-x^{1265}+x^{1100}-x^{936}+x^{825}-x^{660}+x^{550}-x^{330}+x^{275}-x^{55}+1$

Quindi: $f_{3025}(x) = \Phi_5(x)\cdot\Phi_{11}(x)\cdot\Phi_{25}(x)\cdot\Phi_{55}(x)\cdot\Phi_{121}(x)\cdot\Phi_{275}(x)\cdot\Phi_{605}(x)\cdot\Phi_{3025}(x)$

Questa breve trattazione sui polinomi ciclotomici ci serve per introdurre un teorema, di sicuro interesse, che ho indicato con la sigla VTL-$(Wn)_b$.

Teorema VTL - $(Wn)_b$