Appunti sui numeri complessi e i polinomi.

Roberto Catenacci

Versione del 7 Marzo 2011

Indice

1 Equazioni quadratiche.

Una equazione quadratica in x è una equazione della forma: $ax^2 + bx + c = 0$ dove a, b, c sono numeri reali e $a \neq 0$. Non è difficile risolverla; quando $\Delta = b^2 - 4ac \geq 0$ (la stessa formula vale anche se $\Delta < 0$, ma ne parleremo dopo) si ha:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Ci sono due tipi di equazioni quadratiche; quelle che hanno soluzioni *razionali* (ovvero che si possono scrivere nella forma m/n con m e n numeri interi relativi e $n \neq 0$) e quelle le cui soluzioni sono *irrazionali.* Le soluzioni sono razionali quando Δ è il quadrato di un numero razionale. Esempi di numeri irrazionali sono $\sqrt{2}$,$\sqrt{3}, \pi$.

Dimostriamo che $\sqrt{2}$ è irrazionale. Supponiamo che sia razionale; allora $\sqrt{2} = m/n$, *con* m *e* n *senza fattori comuni*; elevando al quadrato si ha: $m^2 = 2n^2$. Questo significa che m^2 è un numero pari e quindi anche m lo è (questa ultima osservazione deriva dal fatto che il quadrato di un numero dispari è un numero dispari, infatti $(2k + 1)^2 = 4k^2 + 4k + 1$; ora usiamo anche il seguente fatto: se la proposizione A implica la proposizione B, allora la proposizione non-B implica la proposizione non-A. (m dispari implica m^2 dispari allora m^2 non-dispari cioè pari implica m non-dispari cioè pari). Allora $m = 2k$ e quindi $4k^2 = 2n^2$ cioè $n^2 = 2k^2$ così n^2 è pari e anche n lo è. Allora sia m che n sono numeri pari e quindi hanno in comune almeno il fattore 2.

Questa è una contraddizione perchè abbiamo supposto che m *e* n *siano senza fattori comuni.* La contraddizione si risolve *solo negando l'assunto* che $\sqrt{2}$ sia razionale. Il ragionamento precedente è un esempio di **dimostrazione per assurdo**, il metodo consiste nell'assumere falsa la proposizione che si vuole dimostrare e cercare di ottenere una contraddizione. Questo risultato si generalizza abbastanza facilmente: **le radici n-esime dei numeri interi sono numeri irrazionali a meno che il numero non sia una n-esima potenza.** Dimostreremo questo teorema (che useremo nel corso di Algebra) più sotto, dopo aver discusso alcune proprietà dei polinomi.

La formula risolutiva delle equazioni di secondo grado data sopra implica che una tale equazione ha, al più, due soluzioni. Se $\Delta = b^2 - 4ac = 0$ l'equazione ha una sola soluzione *(meglio dire due soluzioni coincidenti)*, se $\Delta = b^2 - 4ac > 0$ l'equazione ha due soluzioni distinte. Se $\Delta = b^2 - 4ac < 0$ l'equazione non ha soluzioni reali; introducendo i **numeri complessi** si possono estrarre le radici quadrate dei numeri negativi e si ripristina la simmetria: una equazione di grado *due* ha sempre *due* soluzioni (distinte o coincidenti).

Due equazioni $a_1x^2 + b_1x + c_1 = 0$ e $a_2x^2 + b_2x + c_2 = 0$ hanno le stesse soluzioni se e solo se sono proporzionali, cioè se esiste una costante $k \neq 0$ tale che

$$ka_1 = a_2, kb_1 = b_2, kc_1 = c_2.$$

Questa osservazione è utile perchè ci consente di scrivere subito, senza risolvere l'equazione, la somma e il prodotto delle sue soluzioni: siano α e β le soluzioni dell'equazione $ax^2+bx+c = 0$. Anche l'equazione:

$$a(x - \alpha)(x - \beta) = ax^2 - a(\alpha + \beta)x + a\alpha\beta = 0$$

ha ovviamente le stesse soluzioni, e quindi, confrontando con l'equazione originaria, si trova:

$$\alpha + \beta = -b/a \text{ e } \alpha\beta = c/a.$$

Esempio: data l'equazione $8x^2 - 9x + 2 = 0$, trovare una equazione che abbia come soluzioni i quadrati delle soluzioni dell'equazione data. Siano α e β le soluzioni: si ha $\alpha + \beta = 9/8$ e $\alpha\beta = 1/4$. Notiamo anche che $(\alpha^2 + \beta^2) = (\alpha + \beta)^2 - 2\alpha\beta = 49/64$ e $\alpha^2\beta^2 = 1/16$. Quindi l'equazione richiesta, *trovata senza risolvere l'equazione di partenza*, è $x^2 - (\alpha^2 + \beta^2)x + \alpha^2\beta^2 = x^2 - \frac{49}{64}x + \frac{1}{16} = 0$.

Questo metodo funziona per trovare equazioni le cui radici siano **funzioni simmetriche** (una funzione f di α e β è simmetrica se $f(\alpha, \beta) = f(\beta, \alpha)$) delle radici dell'equazione data; infatti **tutte** le funzioni simmetriche si possono scrivere in funzione delle due funzioni simmetriche elementari $f_1(\alpha, \beta) = \alpha + \beta$ e $f_2(\alpha, \beta) = \alpha\beta$.

Esempio: $\alpha^3 + \beta^3 = (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta)$.

2 Numeri complessi.

Per introdurre i numeri complessi si parte di solito dal fatto che l'equazione $x^2 + 1 = 0$ non ha soluzioni nel campo dei numeri reali. Si *inventa* allora una soluzione dell'equazione data e la si chiama i. Si tratta poi i come un normale numero a cui si applicano le solite regole di calcolo algebrico e allora si ottiene $i^2 = -1$. Si scrivono poi tutti i simboli del tipo $a + ib$ con a e b numeri reali e si postulano per essi le usuali regole di calcolo algebrico: ecco i **numeri complessi**.

Un modo più *convincente* per introdurre i numeri complessi è quello di farli discendere direttamente dalle coppie di numeri reali.

Indichiamo con $\mathbb{R}$ il campo dei numeri reali con le solite operazioni e con $\mathbb{C}$ il campo dei numeri complessi.

Un **numero complesso** è una coppia ordinata di numeri reali $(a, b) \in \mathbb{R} \times \mathbb{R}$, cioè

$$\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}.$$

Definiamo $\forall\, (a, b), (c, d) \in \mathbb{C}$ le seguenti operazioni :

i) **somma**: $(a, b) + (c, d) = (a + b, c + d)$;

ii) **prodotto**: $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Viene naturale **identificare** $a \in \mathbb{R}$ con la coppia $(a, 0) \in \mathbb{C}$, cioè ogni numero reale può essere pensato come numero complesso $\Rightarrow \mathbb{C}$ è un "ampliamento" di $\mathbb{R}$, cioè $\mathbb{R} \subset \mathbb{C}$.

L'elemento $(0, 1) \in \mathbb{C}$, si denota con i ed è detto **unità immaginaria**. Si ha

$$i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (-1, 0) = -1.$$

Prendiamo $(a, b) \in \mathbb{C}$:

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (0, 1) \cdot (b, 0) = a + ib,$$

cioè ogni numero complesso può essere scritto nella forma $a + ib$, detta **forma algebrica**, a è chiamata **parte reale**, ib è la **parte immaginaria**. Le operazioni tra numeri complessi scritti in forma algebrica si eseguono con le regole del calcolo letterale:

$$(a + ib) + (c + id) = a + ib + c + id = (a + c) + i(b + d);$$
$$(a + ib) \cdot (c + id) = ac + iad + ibc + i^2bd = ac + iad + ibc - bd$$
$$= (ac - bd) + i(ad + bc).$$

Dato $z = a + ib$, si definisce il numero **complesso coniugato**

$$\overline{z} = a - ib.$$

I numeri complessi $\neq 0$ (ovvero quelli per cui $a^2 + b^2 \neq 0$) hanno un inverso:

$$\frac{1}{z} = \frac{\overline{z}}{z\overline{z}} = \frac{a - ib}{a^2 + b^2}$$

Infatti

$$z \cdot \frac{1}{z} = (a + ib) \cdot \frac{a - ib}{a^2 + b^2} = 1$$

Per mettere in forma algebrica una frazione con un numero complesso a denominatore, si può moltiplicare numeratore e denominatore per il coniugato del numero, osservando che $z\overline{z} = (a + ib) \cdot (a - ib) = a^2 - iab + iab - i^2b = a^2 + b^2$.

Rappresentazione geometrica dei numeri complessi

Fissiamo nel piano un sistema di riferimento cartesiano Oxy. Un numero complesso (a, b) può essere pensato come punto del piano π (**piano complesso**): a rappresenta l'ascissa e b l'ordinata.

Osservazioni.

1) Se $z \in \mathbb{R} \Rightarrow z = (a, 0) \Rightarrow z$ sta sull'asse x (detto **asse reale**).

2) Se $z = ib$, cioè z è immaginario puro $\Rightarrow z = (0, b)$ sta sull'asse y (detto **asse immaginario**).

3) La moltiplicazione per i equivale quindi a una rotazione di 90° in senso antiorario.

- **Forma trigonometrica di un numero complesso:**

sia $z = a + ib$ un numero complesso e sia P la sua immagine sul piano π. Associamo a z due "coordinate polari" (ρ, θ):

1) $\rho = \sqrt{a^2 + b^2}$ è detto **modulo** di z ed è la lunghezza del segmento che congiunge l'origine con il punto P;

2) θ è detto **anomalia** o **argomento** di z, è l'angolo tra ρ e il semiasse positivo delle x ed **è individuato a meno di multipli di** 2π**.**

Dalla trigonometria si ha che

$$a = \rho \cos\theta \text{ e } b = \rho \sin\theta$$

Si ottiene quindi:

$$\cos\theta = \frac{a}{\rho} = \frac{a}{\sqrt{a^2+b^2}} \text{ e } \sin\theta = \frac{b}{\rho} = \frac{b}{\sqrt{a^2+b^2}}.$$

Dalle formule precedenti si ottiene:

$$\boxed{a+ib = \rho\,(\cos\theta + i\sin\theta)},$$

detta **forma trigonometrica** del numero complesso $a+ib$.

Due numeri complessi non nulli $z_1 = \rho_1(\cos\theta_1 + i\sin\theta_1)$ e $z_2 = \rho_2(\cos\theta_2 + i\sin\theta_2)$ sono uguali se $\rho_1 = \rho_2$ e $\theta_1 = \theta_2 + 2k\pi$, con k intero.

- **Teorema**. Dati $z_1, z_2 \in \mathbb{C}$, il loro prodotto è

$$z_1 \cdot z_2 = \rho_1\rho_2\,[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)].$$

- Tale regola vale anche per un numero qualsiasi di fattori. Se i fattori sono uguali, si ha la **formula di De Moivre**:

$$[\rho\,(\cos\theta + i\sin\theta)]^n = \rho^n\,(\cos n\theta + i\sin n\theta)\,,\ \ n\in\mathbb{N}.$$

Esempio:

$$(1+i)^{14} = (\sqrt{2}(\cos\pi/4 + i\sin\pi/4))^{14} = 128(\cos(-\pi/2) + i\sin(-\pi/2)) = -128i$$

infatti $14\pi/4 = 7\pi/2 = 4\pi - \pi/2$ (provate solo a pensare di dover fare il calcolo senza la formula di De Moivre per capirne l'importanza !).

Se si conviene di porre $[\rho\,(\cos\theta + i\sin\theta)]^0 = 1$, e, per $\rho \neq 0$,

$$[\rho\,(\cos\theta + i\sin\theta)]^{-n} = \frac{1}{[\rho\,(\cos\theta + i\sin\theta)]^n} = \rho^{-n}\,[(\cos\theta - i\sin\theta)]^n = \left[\rho^{-n}\,(\cos(-n\theta) + i\sin(-n\theta)\right]$$

quindi la formula di De Moivre vale per $n\in\mathbb{Z}$.

- **Radici n-esime dei numeri complessi.**

Sia $z\in\mathbb{C}$ e $n\in\mathbb{N}$. I numeri $w\in\mathbb{C}$ tali che $w^n = z$, si dicono **radici n-esime** di z.

Prendiamo $z = \rho\,(\cos\theta + i\sin\theta)$ e sia $w = r(\cos\varphi + i\sin\varphi)$ una radice n-esima di z. Si deve avere

$$\begin{gathered} w^n = z \Rightarrow r^n(\cos n\varphi + i\sin n\varphi) = \rho\,(\cos\theta + i\sin\theta) \\ \Rightarrow r^n = \rho \text{ e } n\varphi = \theta + 2k\pi,\ k\in\mathbb{Z} \\ \Rightarrow r = \sqrt[n]{\rho} \text{ (radice aritmetica) e } \varphi = \frac{\theta}{n} + \frac{2k\pi}{n},\ k\in\mathbb{Z}. \end{gathered}$$

L'ultima formula dà infiniti valori per φ, ma solo n sono distinti ($k = 0, 1, ..., n-1$ poi si ripetono a meno di multipli di 2π).

Teorema. $z = \rho\,(\cos\theta + i\sin\theta)$ ammette n radici n-esime w distinte date dalla formula

$$(\sharp) \qquad \boxed{w = \sqrt[n]{z}^* = \sqrt[n]{\rho}\left[\cos\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right) + i\sin\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)\right]},$$

nella quale si pone $k = 0, 1, 2, ..., n-1$.

(L'asterisco serve solo a distinguere la radice complessa da quella aritmetica).

Gli n numeri forniti da ($\sharp$), hanno lo stesso modulo $\sqrt[n]{\rho}$, quindi le loro immagini sul piano complesso stanno su una circonferenza di centro l'origine e raggio $\sqrt[n]{\rho}$.

Scegliamo $z = 1 = 1 + 0i = 1(\cos 0 + i\sin 0)$. Utilizzando ($\sharp$), troviamo le n **radici n-esime dell'unità**:

$$\begin{aligned}\epsilon_k = \sqrt[n]{1}^* &= \sqrt[n]{1}\left[\cos\left(0 + \frac{2k\pi}{n}\right) + i\sin\left(0 + \frac{2k\pi}{n}\right)\right] \\ &= \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \text{ con } k = 0, 1, 2, ..., n-1.\end{aligned}$$

Le radici n-esime dell'unità si rappresentano geometricamente come vertici di un poligono regolare di n lati, inscritto in una circonferenza di raggio 1, con un vertice nel punto $(1, 0)$.

Le radici n-esime dell'unità servono anche per calcolare le radici n-esime di qualsiasi numero: basta moltiplicare una qualsiasi radice complessa del numero per le radici n-esime dell'unità. Infatti sia ζ una qualunque radice n-esima di z, ponendo $\zeta_k = \zeta\epsilon_k$ si ottengono tutte le radici di z, infatti:

$$(\zeta_k)^n = (\zeta\epsilon_k)^n = \zeta^n\epsilon_k^n = z$$

Esempi.

- Calcolare le tre radici cubiche complesse di 8.

Scriviamo 8 in forma trigonometrica:

$$8 = 8 + 0i = 8(\cos 0 + i\sin 0).$$
$$w_k = \sqrt[3]{8}^* = \sqrt[3]{8}\left(\cos\frac{2k\pi}{3} + i\sin\frac{2k\pi}{3}\right),\ k = 0, 1, 2.$$

Quindi
$w_0 = 2(\cos 0 + i\sin 0) = 2;$
$$w_1 = 2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right) = 2\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = -1 + i\sqrt{3};$$
$$w_2 = 2\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right) = 2\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = -1 - i\sqrt{3}.$$
Le tre radici cubiche di 8 sono: 2, $-1 + i\sqrt{3}$ e $-1 + i\sqrt{3}$.

- Calcolare le quattro radici quarte di $-1+i\sqrt{3}$.

Si ha:

$$\rho=\sqrt{1+3}=2,\ \cos\theta=-\frac{1}{2}\ \text{e}\ \sin\theta=\frac{\sqrt{3}}{2}\Rightarrow\theta=\frac{2\pi}{3}$$
$$\Rightarrow -1+i\sqrt{3}=2\left(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\right).$$

Applicando la $(\sharp)$ con $k=0,1,2,3$, si ha

$$w_k=\sqrt[4]{-1+i\sqrt{3}}^{*}=\sqrt[4]{2}\left[\cos\left(\frac{\pi}{6}+\frac{k\pi}{2}\right)+i\sin\left(\frac{\pi}{6}+\frac{k\pi}{2}\right)\right].$$

$$w_0=\sqrt[4]{2}\left[\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\right]=\sqrt[4]{2}\left(\frac{\sqrt{3}}{2}+i\frac{1}{2}\right)=\frac{\sqrt[4]{2}}{2}\left(\sqrt{3}+i\right);$$
$$w_1=\sqrt[4]{2}\left[\cos\left(\frac{\pi}{6}+\frac{\pi}{2}\right)+i\sin\left(\frac{\pi}{6}+\frac{\pi}{2}\right)\right]=\sqrt[4]{2}\left(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\right)$$
$$=\sqrt[4]{2}\left(-\frac{1}{2}+i\frac{\sqrt{3};}{2}\right)=\frac{\sqrt[4]{2}}{2}\left(-1+i\sqrt{3}\right);$$
$$w_2=\sqrt[4]{2}\left[\cos\left(\frac{\pi}{6}+\pi\right)+i\sin\left(\frac{\pi}{6}+\pi\right)\right]=\sqrt[4]{2}\left(\cos\frac{7\pi}{6}+i\sin\frac{7\pi}{6}\right)$$
$$=\sqrt[4]{2}\left(-\frac{\sqrt{3}}{2}-i\frac{1}{2}\right)=\frac{\sqrt[4]{2}}{2}\left(-\sqrt{3}-i\right);$$
$$w_3=\sqrt[4]{2}\left[\cos\left(\frac{\pi}{6}+\frac{3\pi}{2}\right)+i\sin\left(\frac{\pi}{6}+\frac{3\pi}{2}\right)\right]=\sqrt[4]{2}\left(\cos\frac{5\pi}{3}+i\sin\frac{5\pi}{3}\right)$$
$$=\sqrt[4]{2}\left(\frac{1}{2}-i\frac{\sqrt{3};}{2}\right)=\frac{\sqrt[4]{2}}{2}\left(1-i\sqrt{3}\right).$$

- Calcolare le sei radici seste dell'unità.

Si ha:

$$\epsilon_k=\sqrt[6]{1}^{*}=\cos\frac{2k\pi}{6}+i\sin\frac{2k\pi}{6},\ \text{con}\ k=0,1,2,3,4,5.$$

Quindi
$\epsilon_0=\cos 0+i\sin 0=1;$
$\epsilon_1=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}=\frac{1}{2}+i\frac{\sqrt{3}}{2};$
$\epsilon_2=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=-\frac{1}{2}+i\frac{\sqrt{3}}{2};$
$\epsilon_3=\cos\pi+i\sin\pi=-1;$

$\epsilon_4 = \cos\dfrac{4\pi}{3} + i\sin\dfrac{4\pi}{3} = -\dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}$;
$\epsilon_5 = \cos\dfrac{5\pi}{3} + i\sin\dfrac{5\pi}{3} = \dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}$.
Le sei radici trovate sono i vertici di un esagono regolare.

• **Formula di Eulero.**

Consideriamo la funzione esponenziale di variabile complessa $f(z) = e^z$, $z \in \mathbb{C}$, definita formalmente con la stessa serie che si usa per definire l'esponenziale reale.
Valgono le consuete proprietà delle potenze:

$$e^z \cdot e^w = e^{z+w}; \qquad e^z/e^w = e^{z-w}; \qquad (e^z)^n = e^{nz},$$

con $z, w \in \mathbb{C}$, $n \in \mathbb{Z}$.
Se $z = x + iy$, con $x, y \in \mathbb{R}$, si trova, scrivendo esplicitamente le serie coinvolte,

$$e^z = e^{x+iy} = e^x \cdot e^{iy} = e^x(\cos y + i\sin y).$$

Quindi è

$$\boxed{e^{iy} = (\cos y + i\sin y)}.$$

Quest'ultima è la **formula di Eulero**.
Si ha

$$e^{2\pi i} = \cos 2\pi + i\sin 2\pi = 1 + 0i = 1$$

e

$$e^{z+2\pi i} = e^z \cdot e^{2\pi i} = e^z,$$

cioè l'esponenziale e^z è periodica di periodo $2\pi i$.
Inoltre

$$e^{-iy} = \cos(-y) + i\sin(-y) = \cos y - i\sin y.$$

Esempio.
$i = 0 + 1i = \cos\dfrac{\pi}{2} + i\sin\dfrac{\pi}{2} = e^{\frac{\pi}{2}i}$;
$-1 = -1 + 0i = \cos\pi + i\sin\pi = e^{\pi}$.

3 Radici n - esime dell'unità.

Abbiamo visto che le radici n - esime dell'unità sono espresse dagli n numeri complessi:

$$\epsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \text{con } k = 0, 1, 2, ..., n-1.$$

E' facile verificare, utilizzando la definizione e la formula del prodotto di numeri complessi in forma trigonometrica:

$$z_1 \cdot z_2 = \rho_1\rho_2\left[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\right]$$

che l'insieme delle radici n - esime dell'unità è un **gruppo abeliano**; il prodotto è dato esplicitamente da:

$$\epsilon_k \cdot \epsilon_h = \epsilon_j \text{ dove } j = (k+h) \bmod n$$

E' chiaro che l'elemento neutro del gruppo è $\epsilon_0 = 1$ e che l'inverso di ϵ_k è:

$$(\epsilon_k)^{-1} = \epsilon_{n-k}$$

Un altro risultato utile è:

$$(\epsilon_k)^{-1} = \overline{\epsilon_k}$$

Questo gruppo è **ciclico**, ovvero tutti i suoi elementi sono potenze positive di un qualche suo elemento, detto allora **generatore**. Si verifica subito infatti che, per ogni n :

$$\epsilon_k = (\epsilon_1)^k$$

Vogliamo ora capire, dato n, quali sono i generatori del gruppo delle radici n - esime (oltre ovviamente ϵ_1). Il punto di partenza è la seguente osservazione: sia ϵ_k una radice n - esima, se $MCD(n,k) = d$ allora ϵ_k è anche radice $\frac{n}{d}$ - esima. Infatti basta calcolare:

$$(\epsilon_k)^{\frac{n}{d}} = \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)^{\frac{n}{d}} = \cos\left(\frac{2k\pi}{n}\frac{n}{d}\right) + i\sin\left(\frac{2k\pi}{n}\frac{n}{d}\right) = \cos\frac{2k\pi}{d} + i\sin\frac{2k\pi}{d} = 1$$

Perchè k è per ipotesi divisibile per d. Diamo ora la seguente definizione: ϵ_k è **radice primitiva** se è radice n - esima ma non radice m - esima con $1 \leq m < n$. Ovvero se $(\epsilon_k)^n = 1$, ma $(\epsilon_k)^m \neq 1$ per $1 \leq m < n$. Ovviamente ϵ_1 **è sempre primitiva**. Si vede subito che ϵ_k è primitiva se e solo se $MCD(n,k) = 1$. La dimostrazione procede per assurdo; se infatti $MCD(n,k) \neq 1$ l'osservazione precedente implica che ϵ_k non è primitiva, infatti $(\epsilon_k)^{\frac{n}{d}} = 1$ e $\frac{n}{d} < n$. Viceversa se ϵ_k non è primitiva, allora $(\epsilon_k)^m = 1$ per qualche m, $1 \leq m < n$. Ovvero, essendo ϵ_1 sempre primitiva, esiste un intero h tale che $km = hn$. Questo implica che $MCD(n,k) \neq 1$, perchè se fosse 1, per un teorema dimostrato in corsi precedenti, esisterebbero due interi x, y tali che $nx + ky = 1$ e quindi, moltiplicando per m si ha:

$$m = nmx + kmy = nmx + nhy = n(mx + hy)$$

e questo è assurdo perchè $1 \leq m < n$ implica che m non possa essere divisibile per n.

Esempio: consideriamo le radici seste dell'unità (vedi più sopra)**:** $MCD(6,k)=1$ per $k=1,5$ e infatti si vede subito che $\epsilon_3=-1$ è anche radice quadrata, mentre ϵ_2 e ϵ_4 sono anche radici cubiche: $\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^3=\left(-\frac{1}{2}-i\frac{\sqrt{3}}{2}\right)^3=1$.

Possiamo ora concludere facilmente che i generatori sono tutte e sole le radici primitive, infatti solo per le radici primitive le potenze distinte sono proprio n.

Si mostra anche un altro fatto interessante: **ogni radice n - esima è d - esima primitiva per ogni d divisore di n.** Sia infatti $(\epsilon_k)^n=1$ e sia d il più piccolo intero positivo per cui $(\epsilon_k)^d=1$ (questo d si dice **periodo** o **ordine** di ϵ_k) allora dividendo n per d si ha $n=qd+r$ (con $0\leq r<d$) allora si avrebbe

$$1=(\epsilon_k)^n=(\epsilon_k)^{qd}(\epsilon_k)^r=\left((\epsilon_k)^d\right)^q(\epsilon_k)^r=(\epsilon_k)^r$$

E quindi deve essere $r=0$ perchè altrimenti d non sarebbe il più piccolo e quindi d deve essere divisore di n. Osserviamo anche che segue che se n è primo e quindi non ha divisori non banali, tutte le radici $\neq 1$ sono primitive. Viceversa è ovvio che se d divide n ogni radice d - esima è anche n - esima.

Concludiamo con altre interessanti proprietà delle radici n -esime dell'unità:

$$\sum_0^{n-1}\epsilon_k=\sum_1^n\epsilon_k=0$$

Infatti si ha, posto $\sum_0^{n-1}\epsilon_k=S$, $\epsilon_1 S=S$ (osservando che $\epsilon_1\epsilon_{n-1}=\epsilon_n=\epsilon_0$) e quindi $S=0$.

$$\prod_0^{n-1}\epsilon_k=\prod_1^n\epsilon_k=1 \text{ se } n \text{ è dispari e } -1 \text{ se } n \text{ è pari}$$

Infatti

$$\prod_1^n\epsilon_k=\prod_1^n(\epsilon_1)^k=(\epsilon_1)(\epsilon_1)^2\ldots(\epsilon_1)^n=(\epsilon_1)^{\frac{n(n+1)}{2}}$$

Allora se n è dispari, $n=2m+1$, e quindi $\frac{n(n+1)}{2}=nm$ e allora

$$(\epsilon_1)^{nm}=((\epsilon_1)^n)^m=1,$$

mentre se n è pari, $n=2m$, e quindi $\frac{n(n+1)}{2}=m(n+1)$ e allora

$$(\epsilon_1)^{m(n+1)}=(\epsilon_1)^{nm}(\epsilon_1)^m=(\epsilon_1)^m=\cos\frac{2m\pi}{n}+i\sin\frac{2m\pi}{n}=\cos\frac{2m\pi}{2m}+i\sin\frac{2m\pi}{2m}=-1$$

4 Polinomi.

Un **polinomio** a coefficienti reali (o complessi) nella indeterminata x è un'espressione

$$P(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$$

con $a_0, a_1, ..., a_n \in \mathbb{R}$ (o $\mathbb{C}$), $a_n \neq 0$, detti **coefficienti** del polinomio e $n \in \mathbb{N}$, detto **grado** del polinomio: $n = \deg P(x)$. Se $a_n = 1$, il polinomio è detto **monico**. L'insieme dei polinomi in x su $\mathbb{R}$ (o $\mathbb{C}$) è denotato con $\mathbb{R}[x]$ (o $\mathbb{C}[x]$). Il **polinomio nullo**, è per definizione, il numero 0 (ad esso, secondo la nostra definizione, non si potrebbe attribuire un grado, perchè non c'è nessun n per cui a_n è diverso da zero; si conviene, per convenzione, attribuirgli qualsiasi grado vogliamo). Un **polinomio costante** è il polinomio nullo oppure un polinomio di grado 0.

Due polinomi in x sono uguali se hanno uguali i coefficienti delle potenze di x corrispondenti. I polinomi si sommano e si moltiplicano secondo le regole note del calcolo letterale. Si usa denotare con $\mathbb{R}_{\leq n}[x]$ (o $\mathbb{C}_{\leq n}[x]$) l'insieme dei polinomi di grado al più n, includendo anche il polinomio nullo.

- **Algoritmo della divisione.**

Dati due polinomi $A(x)$, $B(x) \in \mathbb{R}[x]$, sono determinati in modo unico i polinomi $Q(x)$ (**quoziente**) e $R(x)$ (**resto**) in $\mathbb{R}[x]$, tali che

$$A(x) = B(x)Q(x) + R(x)$$

con $R(x) = 0$ oppure $\deg R(x) < \deg B(x)$.
Se $\deg A(x) = n$, $\deg B(x) = m$:
i) se $m \leqslant n \Rightarrow \deg Q(x) = n - m$ e $\deg R(x) < m$;
ii) se $m > n \Rightarrow Q(x) = 0$ e $R(x) = A(x)$.
Se nel polinomio $A(x) \in \mathbb{R}[x]$, x è sostituita da un $c \in \mathbb{R}$, il risultato è un elemento di $\mathbb{R}$ (e lo stesso vale se invece di $\mathbb{R}$ lavoriamo in $\mathbb{C}$).
Esempio.
$A(x) = x^3 - 2x^2 + 2 \in \mathbb{R}[x]$
$A(3) = 27 - 18 + 2 = 11 \in \mathbb{R}$.

- **Teorema del resto**. Siano $A(x) \in \mathbb{R}[x]$ e $B(x) = x - c$, con $c \in \mathbb{R}$. Il resto della divisione di $A(x)$ per $B(x)$ è $A(c)$.

Infatti $A(x) = (x - c)Q(x) + R(x)$ e ponendo $x = c$ si ottiene $A(c) = R(c) = R(x)$ perchè il grado del resto deve essere, in questo caso, zero (il grado del resto è minore del grado del polinomio divisore) e quindi $R(x)$ è un polinomio costante.
Esempio.
$A(x) = x^3 - 2x^2 + 2$, $B(x) = x - 3$.
$R(x) = A(3) = 11$.
Il risultato si può facilmente verificare eseguendo la divisione tra i due polinomi.
Dati $A(x), B(x) \in \mathbb{R}[x]$ con $B(x) \neq 0$, diciamo che $A(x)$ è **divisibile** per $B(x)$ se $A(x) = B(x)Q(x)$, cioè se il resto della divisione è 0.
$c \in \mathbb{R}$ si dice **radice** (o **zero**) di un polinomio $A(x) \in \mathbb{R}[x]$ se $A(c) = 0$.

- **Teorema di Ruffini**. Se $A(x) \in \mathbb{R}[x]$ e $c \in \mathbb{R}$, allora c è radice di $A(x) \Leftrightarrow A(x)$ è divisibile per $(x-c)$.

- **Teorema fondamentale dell'algebra**. Ogni polinomio $P(x) \in \mathbb{C}[x]$ di grado $n \geqslant 1$, ha sempre n radici in $\mathbb{C}$.

Un polinomio a coefficienti reali non è detto che abbia sempre radici reali, ma chiaramente se z è una radice, anche $\overline{z}$ lo è. Ne consegue che un polinomio a coefficienti **reali** di grado **dispari** deve avere sempre almeno una radice reale. Questo fatto deriva anche da un noto teorema di analisi (Teorema degli zeri di Bolzano): un polinomio a coefficienti reali è una funzione reale continua e, se ha grado dispari, per $x \to \pm\infty$ tende all'infinito con valori di segno discordi; deve quindi passare per zero.

Se il polinomio è **monico** e le radici sono $x_1, ..., x_n$ allora possiamo scomporre il polinomio nella forma

$$P(x) = (x-x_1)(x-x_2)...(x-x_n).$$

Se una radice compare k volte nella scomposizione, diciamo che ha **molteplicità algebrica** k. In questo caso essa è radice non solo del polinomio, ma anche delle sue derivate fino all'ordine $k-1$.

Se il polinomio non è monico basta riscriverlo così:

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n = a_n(\frac{a_0}{a_n} + \frac{a_1}{a_n}x + a_2x^2 + ... + x^n) = a_n(x-x_1)(x-x_2)...(x-x_n)$$

dove ora le radici sono quelle del polinomio monico $\frac{a_0}{a_n} + \frac{a_1}{a_n}x + a_2x^2 + ... + x^n$.

- L'insieme dei polinomi a coefficienti interi, razionali, reali o complessi è un **anello commutativo con unità** con le operazioni di somma e prodotto usuali.

- Un polinomio $P(x)$ è una **unità** se esiste un altro polinomio $Q(x)$ tale che $P(x)Q(x) = 1$. Se i coefficienti sono in un campo le unità sono tutti e soli i polinomi costanti diversi da zero.

- Un polinomio $P(x) \neq 0$ si dice **irriducibile** se non è una unità, e quando $P(x) = A(x)B(x)$, almeno uno dei due polinomi $A(x)$ e $B(x)$ è una unità.

La riducibilità o meno di un polinomio dipende ovviamente dall'anello in cui si considerano i coefficienti. Ad esempio il polinomio x^2-2 è riducibile sui reali: $x^2-2 = \left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right)$, mentre è irriducibile sui razionali (perchè $\sqrt{2}$ non è un razionale). Ancora x^2+2 è riducibile sui complessi: $x^2+2 = \left(x-\sqrt{2}i\right)\left(x+\sqrt{2}i\right)$, mentre è irriducibile sui reali (perchè $\sqrt{2}i$ non è un reale)

I polinomi irriducibili sui complessi sono solo quelli di grado 1 (segue dal teorema fondamentale dell'algebra) mentre sui reali sono quelli di grado 1 e quelli di grado due **senza radici reali**. Infatti tutti i polinomi di grado maggiore di due sono riducibili sui reali: possiamo ridurci

sempre al caso di grado pari (se è di grado dispari abbiamo visto che ha almeno una radice reale α e quindi basta dividere per $x-\alpha$) e, in questo caso, le radici reali o complesse appaiono a coppie, β e $\overline{\beta}$. Il polinomio è quindi divisibile per il polinomio **reale**:

$$P(x) = (x-\beta)\left(x-\overline{\beta}\right) = x^2 - \left(\beta+\overline{\beta}\right)x + \beta\overline{\beta}$$

Ad esempio, calcolando le radici quarte di -1, che sono:

$$\left(\frac{1}{2}+\frac{1}{2}i\right)\sqrt{2},\ \left(\frac{1}{2}-\frac{1}{2}i\right)\sqrt{2},\ -\left(\frac{1}{2}-\frac{1}{2}i\right)\sqrt{2},\ -\left(\frac{1}{2}+\frac{1}{2}i\right)\sqrt{2},$$

si trova:

$$x^4+1 = \left(x^2 - x\sqrt{2}+1\right)\left(x^2+x\sqrt{2}+1\right)$$

Per i polinomi a coefficienti **interi** vale un interessante risultato

- **Teorema delle radici razionali:** sia $P(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ un polinomio a coefficienti interi e supponiamo che $r = \frac{c}{d}$ con c e d primi fra loro, sia una radice razionale di $P(x)$. Allora c divide a_0 e d divide a_n.

  Dimostrazione. Si ha quindi:

  $$a_0 + a_1\frac{c}{d} + a_2\left(\frac{c}{d}\right)^2 + ... + a_n\left(\frac{c}{d}\right)^n = 0$$

  Moltiplicando per d^n si ottiene:

  $$-a_nc^n = a_{n-1}c^{n-1}d + ... + a_1cd^{n-1} + a_0d^n$$

  ne consegue che a_nc^n è divisibile per d, ma siccome d non divide c allora deve dividere a_n. Analogamente possiamo scrivere invece:

  $$a_nc^n + a_{n-1}c^{n-1}d + ... + a_1cd^{n-1} = -a_0d^n$$

  E dedurre come sopra che c deve dividere a_0.

- Questo teorema ha una conseguenza molto interessante: consideriamo l'equazione $x^n - a = 0$ con a intero. Se $x = \frac{c}{d}$ fosse una soluzione razionale, il teorema dimostrato sopra implica che $d = 1$ perchè $a_n = 1$, e quindi $x = r$ deve essere un intero. Allora necessariamente a è una potenza n - esima di un intero. Quindi $\sqrt[n]{a}$ **è razionale se e solo se** a **è una potenza** n **- esima di un intero**. Questo risultato sarà utilizzato nel corso di Algebra.

5 Polinomi ciclotomici.

I **polinomi ciclotomici** sono polinomi che hanno come radici le radici primitive n - esime dell'unità; sono molto interessanti e hanno importantissime applicazioni in algebra teorica (teoria dei campi finiti) e applicata all'informatica (codici correttori di errori).

- **Definizione.** Sia n un numero intero positivo; la funzione di Eulero di n, indicata con $\varphi(n)$ è il numero dei numeri minori di n e primi con n. E' una funzione molto importante e la utilizzeremo nel corso di algebra. Nella sezione dedicata alle radici dell'unità abbiamo dimostrato che $\varphi(n)$ è anche il numero delle radici n - esime primitive.

- **Definizione.** L'n - esimo polinomio ciclotomico $\Phi_n(x)$ è il polinomio monico di grado $\varphi(n)$ che ha come radici le radici n - esime primitive:

$$\Phi_n(x) = \prod_{k=1}^{\varphi(n)} (x - \alpha_k)$$

dove denotiamo con α_k le radici n - esime **primitive**. Se si considera il polinomio $x^n - 1$, le sue radici sono tutte le radici n - esime, quindi abbiamo la fattorizzazione

$$x^n - 1 = \prod_{k=1}^{n} (x - \epsilon_k)$$

dove ora ϵ_k è una qualsiasi radice n -esima. Quindi $\Phi_n(x)$ divide $x^n - 1$. Sia ora ϵ_k una qualsiasi radice n -esima e sia d il suo periodo (se $d = n$ la radice è primitiva), cioè $(\epsilon_k)^d = 1$, abbiamo già visto che d **deve dividere** n e che, in questo caso, ϵ_k è anche una radice d - esima primitiva.

Abbiamo allora, raggruppando in $\Phi_d(x)$ tutte le radici n - esime di periodo d

$$x^n - 1 = \prod_d \Phi_d(x)$$

Dove il prodotto è esteso a tutti i d divisori di n. Per $n = 1$ otteniamo ovviamente

$$\Phi_1(x) = x - 1$$

Se p è un numero primo,

$$x^p - 1 = \Phi_1(x)\Phi_p(x) = (x - 1)\,\Phi_p(x)$$

Per cui

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + ... + x^{p-1}$$

Dalle formule precedenti possiamo allora ottenere facilmente i primi polinomi ciclotomici:

$$\Phi_1(x) = x - 1 \tag{1}$$
$$\Phi_2(x) = 1 + x \tag{2}$$
$$\Phi_3(x) = 1 + x + x^2 \tag{3}$$
$$\Phi_4(x) = 1 + x^2 \tag{4}$$
$$\Phi_5(x) = 1 + x + x^2 + x^3 + x^4 \tag{5}$$
$$\Phi_6(x) = 1 - x + x^2 \tag{6}$$
$$\Phi_7(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \tag{7}$$
$$\Phi_8(x) = 1 + x^4 \tag{8}$$

Si può dimostrare che i polinomi ciclotomici hanno sempre coefficienti interi e sono irriducibili sui razionali. Contrariamente alle apparenze i coefficienti non sono solo $-1, 0, 1$. Ad esempio, il primo polinomio ciclotomico in cui appare anche un coefficiente 2 è $\Phi_{105}(x)$. Notate che $105 = 3 \times 5 \times 7$ è il più piccolo intero che è il prodotto di tre primi dispari distinti...e ciò non è per niente casuale...