CAPITOLO 1

Riassunto esercitazione del 9 marzo: polinomi

Per iniziare:

ESERCIZIO 0.1. Calcolare con l'algoritmo di Euclide il MCD fra i seguenti polinomi in $\mathbb{Q}[x]$: $f(x) = x^5 + x^3 + x^2 + 1$, $g(x) = x^4 - x^3 + x - 1$. Esprimere il massimo comune divisore come combinazione 'di Bezout' di $f(x)$ e $g(x)$.

ESERCIZIO 0.2. Calcolare con l'algoritmo di Euclide il MCD fra i seguenti polinomi in $\mathbb{Q}[x]$: $f(x) = x^5 + x^3 + x^2 + 1$, $g(x) = x^4 + x - 1$. Esprimere il massimo comune divisore come combinazione 'di Bezout' di $f(x)$ e $g(x)$.

1. Polinomi irriducibili di grado basso in $\mathbb{Z}_3[x]$

Premessa importante: per i polinomi di grado due e tre in $K[x]$ (K campo), la proprietà di essere irriducibili equivale al fatto di non avere radici in K. Questo è FALSO per polinomi di grado più alto: per esempio possiamo avere un polinomio di grado quattro senza radici in K che non è irriducibile perché si spezza come prodotto di due polinomi di grado due (che non hanno radici). Pensiamo a $x^4 + 2x^2 + 1$ in $\mathbb{R}[x]$. Questo polinomio non ha radici in $\mathbb{R}$, come si vede dal fatto che è sempre strettamente maggiore di zero. Eppure non è irriducibile, perché si spezza in $\mathbb{R}[x]$ come $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$.

Dunque, per trovare i polinomi irriducibili di grado due e tre in $\mathbb{Z}_3[x]$ basta cercare i polinomi di grado due e tre che non hanno radici in $\mathbb{Z}_3$. Partiamo dal grado due: possiamo restringerci a polinomi monici, ossia della forma $x^2 + ax + b$ con $a, b \in \mathbb{Z}_3$. Sono 9 polinomi da studiare. Si guarda quali hanno [0] come radice, quali hanno [1] come radice, quali hanno [2] come radice (d'ora in avanti ometteremo le parentesi quadre per gli elementi di $\mathbb{Z}_3$) e.. i rimanenti sono irriducibili. Ecco qui gli irriducibili (verificato in classe):

$$x^2 + 1 \quad x^2 + x + 2 \quad x^2 + 2x + 2$$

Nota: che gli irriducibili dovessero essere tre si poteva anche capire facendo il prodotto a due a due dei tre polinomi monici di primo grado di $\mathbb{Z}_3[x]$. Si ottengono 6 polinomi che, per costruzione, NON sono irriducibili. Gli altri $9 - 6 = 3$ polinomi devono essere irriducibili.

ESERCIZIO 1.1. Elencare i polinomi irriducibili monici di grado 3 in $\mathbb{Z}_3[x]$. [Traccia per la risposta: sono 8, come si può scoprire controllando quali fra i 27 polinomi della forma $x^3 + ax^2 + bx + c$ non hanno radici. Da qui si arriva anche subito a poterli elencare. Osservazione: che sono 8 lo si potrebbe anche dire contando quanti sono tutti i possibili prodotti di un polinomio irriducibile di grado due per un polinomio di grado 1, e poi contando i prodotti di tre polinomi di grado 1...]

ESERCIZIO 1.2. Controllare di sapere quali sono i i polinomi irriducibili monici di grado 2 e 3 in $\mathbb{Z}_2[x]$. Se non lo avete già visto, fate anche questo esercizio...

2. Fattorizzare in $Q[x]$: il lemma di Gauss e alcune tecniche utili

Teorema 2.1 ('Lemma di Gauss'). *Sia $f(x)$ un polinomio a coefficienti interi. Se $f(x) = a(x)b(x)$ in $\mathbb{Q}[x]$ allora vale anche $f(x) = a_1(x)b_1(x)$ con $a_1(x), b_1(x) \in \mathbb{Z}[x]$ e con $a_1(x) = ka(x)$, $b_1(x) = tb(x)$, con $k, t \in \mathbb{Q}$.*

Quindi, per dimostrare che $f(x) \in \mathbb{Z}[x]$ è irriducibile in $\mathbb{Q}[x]$ basta dimostrare che è irriducibile in $\mathbb{Z}[x]$. D'altra parte, se abbiamo un polinomio $q(x)$ in $\mathbb{Q}[x]$ possiamo ottenerne uno a coefficienti interi moltiplicando per il minimo comune multiplo dei denominatori dei coefficienti. Questo polinomio è fattorizzabile in $\mathbb{Z}[x]$ se e solo se $q(x)$ è fattorizzabile in $\mathbb{Q}[x]$. Dunque **saper fattorizzare in $\mathbb{Q}[x]$ è un problema equivalente a saper fattorizzare in $\mathbb{Z}[x]$**. Vedere il Childs per approfondire.

Ecco alcuni criteri che possono essere utili per scoprire se un polinomio in $\mathbb{Z}[x]$ è irriducibile o no.

2.1. Criterio 1: trovare una radice.

Se si trova una radice e il polinomio ha grado maggiore strettamente di 1 , allora non è irriducibile...((come si diceva sopra per i polinomi di grado due o tre vale anche il viceversa)).

Criterio: se $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, con $a_n \neq 0$, $a_0 \neq 0$, ha una radice in $\mathbb{Q}$, allora questa radice deve essere un numero razionale $\frac{r}{s}$ tale che:

- r divide a_0 (r può essere anche negativo !)
- s divide a_n (s può essere anche negativo !)

Non possono esserci altre radici razionali.

Esercizio 2.2. Controllare se $x^6 + 5x^3 + 4x^2 + 25x + 10$ ha radici razionali.

Esercizio 2.3. Controllare se $x^3 - 4x^2 + 7x - 6$ ha radici razionali. Qual è la fattorizzazione in irriducibili di tale polinomio?

2.2. Criterio 2: ridurre modulo p.

Se $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $a_n \neq 0$, posso scegliere un numero primo p **che sia primo con** a_n e 'leggere' il polinomio in $\mathbb{Z}_p[x]$ (chiameremo questo polinomio $\overline{f}(x)$).

Criterio (dimostrato in classe): se $\overline{f}(x)$ si spezza in $\mathbb{Z}_p[x]$ allora $f(x)$ non è irriducibile in $\mathbb{Z}[x]$ (e dunque in $\mathbb{Q}[x]$).

Esercizio 2.4. Scoprire se $x^4 + x + 1$ è irriducibile in $\mathbb{Q}[x]$. [provate a leggerlo in $\mathbb{Z}_2[x]$..]

Esercizio 2.5. Scoprire se $x^5 + 2x^2 + x + 1$ è irriducibile in $\mathbb{Q}[x]$. [provate a leggerlo in $\mathbb{Z}_3[x]$..] E cosa dite di $x^5 + 9x^4 + 27x^3 + 2x^2 + 4x + 7$?

Esercizio 2.6. Scoprire se $5x^5 - 12x^4 + 6x^3 + 3x^2 + 2x + 11$ è irriducibile in $\mathbb{Q}[x]$.

2.3. Criterio 3: il criterio di Eisenstein.

Teorema 2.7 (Criterio di Eisenstein). *Consideriamo $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $a_n \neq 0$. Se esiste un primo p tale che*

- *p non divide a_n*
- *p divide a_{n-1}, a_{n-1}, ..., a_1 e a_0*
- *p^2 non divide a_0 (insomma a_0 è diviso da p ma non da p^2)*

allora $f(x)$ è irriducibile in $\mathbb{Z}[x]$ e dunque in $\mathbb{Q}[x]$.

Una traccia della dimostrazione è stata data in classe.

Esercizio 2.8. Dimostrare che $x^4 - 8x^2 - 16x + 10$ è irriducibile in $\mathbb{Q}[x]$.

Osservazione importante: grazie al criterio di Eisenstein possiamo dire che in $\mathbb{Q}[x]$, a differenza di quel che accade in $\mathbb{R}[x]$ e in $\mathbb{C}[x]$, ci sono polinomi irriducibili di ogni grado. Vogliamo un polinomio irriducibile di grado 237? Basta prendere $x^{237}+2$ che è irriducibile per Eisenstein... oppure, se vogliamo stupire, prendiamo $4x^{237} + 3x^7 + 12x^4 + 15x + 6$ (come mostrate che è irriducibile?).

Esercizio 2.9 (Eisenstein 'col trucco'). Dimostrare che $x^4 + 4x + 1$ è è irriducibile in $\mathbb{Q}[x]$.

Soluzione: Sembrerebbe che Eisenstein non si possa applicare. Però facciamo un 'cambio di variabile' e poniamo $x = y + 1$. Il polinomio $(y + 1)^4 + 4(y + 1) + 1$ è irriducibile..come si vede con Eisenstein (per calcolarlo bisogna ricordarsi il binomio di Newton). Da questo si può ricavare (visto in classe) che era irriducibile anche il polinomio di partenza... □

Esercizio 2.10 (ancora Eisenstein 'col trucco'). Dimostrare che, per ogni p primo, il polinomio $x^{p-1} + x^{p-2} + \cdots + x + 1$ è irriducibile in $\mathbb{Q}[x]$.

3. Qualche esercizio sulle radici di 1

Sia p primo. Il polinomio $x^{p-1} + x^{p-2} + \cdots + x + 1$ si chiama *polinomio ciclotomico* p-esimo. Le sue radici in $\mathbb{C}$ sono esattamente le radici complesse p-esime dell'unità diverse da 1. Infatti si verifica subito che vale $x^p - 1 = (x^{p-1} + x^{p-2} + \cdots + x + 1)(x - 1)$ e il polinomio $x^p - 1$ ha per radici in $\mathbb{C}$ esattamente tutte le radici p-esime dell'unità. La fattorizzazione appena mostrata è una fattorizzazione in irriducibili in $\mathbb{Q}[x]$, come sappiamo dall' esercizio 2.10.

Se p non è primo cosa succede? Prendiamo $x^{10}-1$. Le sue radici in $\mathbb{C}$ sono esattamente le radici decime di 1. Fra queste ci sono però le radici quadrate di 1 e anche le radici quinte. Questo ci dice che x^5-1 e x^2-1 dividono $x^{10}-1$. Quindi se vogliamo fattorizzare in irriducibili $x^{10}-1$ in $\mathbb{Q}[x]$ come possiamo procedere? Sappiamo che x^5-1 si fattorizza in irriducibili come $(x^4+x^3+x^2+x+1)(x-1)$, sempre per l'esercizio 2.10. Inoltre x^2-1 si fattorizza in irriducibili come $(x + 1)(x - 1)$. Allora, prendendo gli irriducibili che compaiono in queste due fattorizzazioni, abbiamo che $(x^4+x^3+x^2+x+1)(x-1)(x+1)$ deve dividere $x^{10} - 1$ in $\mathbb{Q}[x]$. Svolgendo la divisione troviamo che

$$x^{10} - 1 = (x^4 + x^3 + x^2 + x + 1)(x - 1)(x + 1)(x^4 - x^3 + x^2 - x + 1)$$

Il nuovo polinomio che è comparso, $x^4 - x^3 + x^2 - x + 1$, risulta irriducibile, dunque abbiamo trovato la fattorizzazione in irriducibili di $x^{10} - 1$ in $\mathbb{Q}[x]$.

Esercizio 3.1. Dimostrare che $x^4 - x^3 + x^2 - x + 1$ è irriducibile in $\mathbb{Q}[x]$.

In generale, se stiamo considerando il polinomio $x^n - 1$ e se $d|n$ allora, visto che le radici d-esime di 1 sono anche radici n-esime, sappiamo che $x^d - 1$ divide $x^n - 1$.

Studiamo più da vicino le radici n-esime di 1. Sia α una radice n-esima di 1 . Se, per un certo c che divide n, vale che $\alpha^c = 1$ allora α è radice anche del polinomio $x^c - 1$. Altrimenti si dice che α è una radice n-esima *primitiva* di 1: la prima potenza positiva di α che ci fa ottenere 1 è proprio α^n.

Il polinomio $x^4-x^3+x^2-x+1$ visto prima ha per radici esattamente le radici decime primitive di 1. [1]

[1]In generale si può dimostrare (non in questo corso !) che il polinomio ottenuto facendo il prodotto di tutti gli $x - \alpha$ al variare di α fra le radici n-esime primitive è **a coefficienti interi** ed è irriducibile in $\mathbb{Q}[x]$. Tale polinomio si chiama *polinomio ciclotomico n-esimo* (il caso $n = p$ primo lo conosciamo bene, è $x^{p-1} + x^{p-2} + \cdots + x + 1$, nel caso $n = 10$ come abbiamo visto è $x^4 - x^3 + x^2 - x + 1$).

Esercizio 3.2. Qual è il massimo comune divisore fra $x^{15}-1$ e $x^{70}-1$?[Studiare le radici, come abbiamo visto in classe per un esempio analogo]

Esercizio 3.3. In generale, dati due interi positivi n, m, qual è il $MCD(x^n-1, x^m-1)$? [Risposta: $x^{MCD(n,m)}-1$, come si vede studiando le radici in comune....]

4. Teorema cinese del resto per polinomi

Teorema 4.1. *Sia K un campo. Siano $a_1(x), a_2(x), \ldots, a_n(x)$ polinomi in $K[x]$ e siano $m_1(x), m_2(x), \ldots, m_n(x)$ polinomi in $K[x]$ a due a due coprimi.*

Allora esiste un unico polinomio $f(x) \in K[x]$ di grado minore o uguale al grado di $m_1(x)m_2(x)\cdots m_n(x)$ e tale che

$$
\begin{gathered}
f(x) \equiv a_1(x) \bmod m_1(x) \\
f(x) \equiv a_2(x) \bmod m_2(x) \\
\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots \\
f(x) \equiv a_n(x) \bmod m_n(x)
\end{gathered}
$$

Dimostrato in classe.

Corollario 4.2. *Se $n_0, n_1, \ldots n_d$ sono interi* **distinti** *e $s_0, s_1, \ldots s_d$ sono interi, esiste un unico polinomio $q(x) \in \mathbb{Q}[x]$ di grado $\leq d$ tale che $q(n_i) = s_i$ per ogni $i = 0, 1, \ldots, d$.*

Dimostrazione. Applicazione del teorema cinese, visto che

$$f(x) \equiv s_i \bmod x - n_i$$

equivale a dire $f(n_i) = s_i$. $\square$