

1. Per il primo punto si può usare il lemma sulle antcatene, però bisogna formularlo.
 - (a) Provare che un ideale monomiale è finitamente generato.
 - (b) Provare che ogni ideale di $k[x_1, \dots, x_n]$ può essere generato da un numero finito di elementi.
 - (c) Provare che ogni ideale di $k[x_1, \dots, x_n]$ ha una base di Gröbner finita.
2. Siano $f, g \in k[x_1, \dots, x_n]$. Supponiamo che il minimo comune multiplo di $\text{LM}(f)$ e $\text{LM}(g)$ è il prodotto $\text{LM}(f)\text{LM}(g)$. Provare che $S(f, g)$ riduce a 0 modulo $\{f, g\}$.
3. Sia $I \subset k[x_1, \dots, x_n]$ un ideale, e G una base di Gröbner di I rispetto all'ordine lessicografico, dove $x_1 >_{\text{lex}} x_2 > \dots >_{\text{lex}} x_n$. Sia $I_l = I \cap k[x_{l+1}, \dots, x_n]$. Provare che $G \cap k[x_{l+1}, \dots, x_n]$ è una base di Gröbner di I_l .
4. Sia k un campo e $T_1, \dots, T_n \subset k$ sottoinsiemi finiti. Poniamo $t_i = |T_i|$, $T = T_1 \times \dots \times T_n \subset k^n$, e

$$I(T) = \{f \in k[x_1, \dots, x_n] \mid f(p) = 0 \text{ per ogni } p \in T\}.$$

Sia

$$f_i(x_i) = \prod_{s \in T_i} (x_i - s).$$

Provare che f_1, \dots, f_n è una base di Gröbner di $I(T)$, rispetto a qualsiasi ordine monomiale.

5. (a) Sia $x \in \mathbb{R}$, $x > 1$. Siano $\frac{b_i}{c_i}$ i convergenti della frazione continua per x . Dimostrare che $|b_i^2 - c_i^2 x^2| < 2x$.
 - (b) In che modo questo risultato viene usato nell'algorithmo per fattorizzare un intero usando frazioni continue?
6. Sia $f \in \mathbb{F}_q[x]$. Sia $v \in \mathbb{F}_q[x]$ tale che $v^q \equiv v \pmod{f}$. Allora

$$f = \prod_{a \in \mathbb{F}_q} \text{mcd}(f, v - a).$$

7. Sia q una potenza di un primo dispari. Sia $\gamma \in \mathbb{F}_q^*$. Si sa che $\gamma^{\frac{q-1}{2}} = 1$ se e solo se γ è un quadrato, e $\gamma^{\frac{q-1}{2}} = -1$ se e solo se γ non è un quadrato. Fare vedere come su questo fatto si basa un metodo probabilistico per fattorizzare polinomi in $\mathbb{F}_q[x]$.
8. Sia $f \in \mathbb{Z}[x]$ e p un primo. Siano $g, h \in \mathbb{Z}[x]$ con
 - $\deg(g) + \deg(h) = \deg(f)$,
 - $\text{mcd}(h, g) = 1 \pmod{p}$,

- $f = gh \pmod{p^k}$ (per un certo $k > 0$).

Allora esistono $\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$ con

- $\deg(\tilde{g}) = \deg(g), \deg(\tilde{h}) = \deg(h)$,
- $\tilde{g} = g \pmod{p^k}, \tilde{h} = h \pmod{p^k}$,
- $f = \tilde{g}\tilde{h} \pmod{p^{k+1}}$.

Fare vedere come la dimostrazione dà un metodo per trovare \tilde{g}, \tilde{h} .