ALGEBRA 2
Esercizi 9 - 24 novembre 2023

Esercisi sull'algoritmo di Berlekamp

1. Un modo "veloce" per calcolare il resto della divisione di un polinomio g per un polinomio f (in $\mathbb{Z}_p[x]$) usando le congruenze.
   Consideriamo ad esempio il caso $f = x^3 + 6 \in \mathbb{Z}_7[x]$. Vogliamo trovare il resto di x^{20} quando viene diviso per f.
   Vale: $f \equiv 0 \mod f$. Quindi $x^6 \equiv -6 \mod f$. Poiché $-6 = 1$ in $\mathbb{Z}_7$, abbiamo: $x^3 \equiv 1 \mod f$.
   Per calcolare il resto della divisione di x^{20} per f possiamo allora procedere così:
   $$x^{20} \equiv x^2(x^{18}) \equiv x^2(x^3)^4 \equiv x^2 \cdot 1^4 \equiv x^2 \mod f$$
   pertanto il resto della divisione di x^{20} per f è x^2.
   Usando questa osservazione, dire quanti fattori irriducibili ha il polinomio $f \in \mathbb{Z}_7[x]$.

2. Calcolare la fattorizzazione in fattori irriducibili del polinomio $x^4 + 1 \in \mathbb{Z}_3[x]$.

3. Trovare la fattorizzazione in fattori irriducibili del polinomio $x^4 + x^3 + x + 1 \in \mathbb{Z}_3[x]$.

4. Dire se il polinomio $x^4 + 2x^3 + x + 2 \in \mathbb{Z}_3[x]$ ha fattori multipli e dire quanti sono i suoi fattori irriducibili.

5. Provare che il $x^2 + 1 \in \mathbb{Z}_3[x]$ è irriducibile. Allora l'anello quoziente $K = \mathbb{Z}_3[x]/(x^2 + 1)$ è un campo. Provare che è perfetto. Trovare poi la radice cubica di $[x + 2] \in K$.

6. Trovare tutti i fattori irriducibili di $x^{p^2} - x^p \in \mathbb{Z}_p[x]$ (non usare Berlekamp).

7. Trovare, usando Berlekamp e anche il fatto che $(a + b)^p = a^p + b^p$ in un anello di caratteristica p, la fattorizzazione del polinomio $x^{80} + 1 \in \mathbb{Z}_2[x]$.