CR1 – Crittografia 1

Alfonso Pesiri - Fabrizio Zaccari

Tutorato 6 – 30 Aprile 2008

Esercizio 1. Sia $p^n = 4, 8, 25, 27, 32$. In ciascuno di questi casi, svolgere i seguenti punti:

1. Calcolare tutti i polinomi monici irriducibili di grado n su $\mathbb{F}_p$;
2. Dopo aver fissato un polinomio f monico irriducibile, trovare l'ordine ed il polinomio minimo di tutti gli elementi di $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[x]/(f)$;
3. Trovare tutte le radici primitive del gruppo moltiplicativo $\mathbb{F}_{p^n}^*$;
4. Trovare tutti i sottocampi di $\mathbb{F}_{p^n}$.

Esercizio 2. Determinare il numero di polinomi irriducibili monici primitivi di grado 12 in $\mathbb{F}_5[x]$. Qual'è la probabilità che preso casualmente un polinomio monico di grado 12 su $\mathbb{F}_5[x]$ esso sia irriducibile?

Esercizio 3. Sia dato il polinomio $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$.

1. Dimostrare che $f(x)$ è irriducibile;
2. Costruire $\mathbb{F}_{16}$;
3. Trovare un generatore $g \in \mathbb{F}_{16}^*$ e scrivere tutti gli elementi di $\mathbb{F}_{16}^*$ come potenze di g.

Esercizio 4. Si consideri il campo $\mathbb{F}_2$. Dopo aver scritto tutti i polinomi irriducibili di grado ≤ 4, dimostrare che $x^5 + x^2 + 1$ è irriducibile.

Esercizio 5. Mostrare che tutti i polinomi del tipo $x^p + x + 1$ sono riducibili in $\mathbb{F}_p$, per ogni $p \geq 3$.