Università degli studi di Roma Tre
Corso di Laurea in Matematica, a.a. 1999/2000
Matematica Applicata 2
Sesto test

CERCARE DI RISOLVERE IL MASSIMO NUMERO DEI SEGUENTI PROBLEMI

1. Fattorizzare il polinomio $x^6 + x^5 + x^2 + 1$ su $\mathbb{F}_3$ usando l'algoritmo di Berlekamp.

2. Si consideri il polinomio $F(x) = x^3 - x^2 - 7x - 3 \in \mathbb{F}_{17}[x]$.
   a. Si trovi un polinomio F-riduttore di grado due usando l'algoritmo di Berlekamp.
   b. Si determinino i $c \in \mathbb{F}_{17}$ tali che $\gcd(F(x), H(x) - c) \neq 1$ (dove $H(X)$ è il polinomio F-riduttore trovato nel punto (a)) usando il metodo di Zassenhaus.

3. Si determini, usando l'algoritmo di Berlekamp, il numero dei irriducibili di $x^4 + 1$ su $\mathbb{F}_p$, per ogni numero primo dispari p.

4. Supponiamo di lavori nel campo $\mathbb{F}_{17}$.
   a. Si calcoli la piu' piccola radice primitiva di $\mathbb{F}_{17}$.
   b. Supponiamo che Alice e Bernardo vogliano sfruttare $\mathbb{F}_{17}$ a la sua piu' piccola radice primitiva per scambiarsi una Chiave in modo sicuro. Si spieghi come possono fare usando il metodo di Diffie–Hellman e si faccia un esempio concreto scegliendo i parametri a piacere.
   c. Si dia un esempio di come funziona il Crittosistema ElGamal in $\mathbb{F}_{17}$ scegliendo a piacere i dati.