VE475 Introduction to Cryptography
Homework 3

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

June 1, 2019

Ex. 1 - Finite fields

1. Assume $X^2 + 1$ is reducible in $\mathbb{F}_3[X]$, then the possible factors of $X^2 + 1$ are X, $X + 1$, and $X + 2$.

$$
\begin{aligned}
X \cdot X &= X^2 \neq X^2 + 1 \\
X \cdot (X + 1) &= X^2 + X \neq X^2 + 1 \\
X \cdot (X + 2) &= X^2 + 2X \neq X^2 + 1 \\
(X + 1) \cdot (X + 1) &= X^2 + 2X + 1 \neq X^2 + 1 \\
(X + 1) \cdot (X + 2) &= X^2 + 3X + 2 \neq X^2 + 1 \\
(X + 2) \cdot (X + 2) &= X^2 + 4X + 4 \neq X^2 + 1
\end{aligned}
$$

   So, $X^2 + 1$ is irreducible in $\mathbb{F}_3[X]$.

2.

3.