MATH 195: CRYPTOGRAPHY
HOMEWORK #11

Problem R4. *Let* $c_0, c_1, c_2, c_3 \in \mathbb{F}_{256}$ *be such that* $c_0 + c_1 + c_2 + c_3 = 1$ *and put*

$$c = c_0 + c_1 Y + c_2 Y^2 + c_3 Y^3 \in \mathbb{F}_{256}[Y].$$

Prove:

(a) $c \equiv 1 \pmod{Y+1}$.
(b) $c^4 \equiv 1 \pmod{Y^4+1}$.
(c) *The inverse of* $(c \bmod Y^4+1)$ *equals*

$$\begin{aligned} &c_0(c_0^2+c_2^2) + c_2(c_1^2+c_3^2) + (c_1(c_0^2+c_2^2) + c_3(c_1^2+c_3^2))Y \\ &\quad + \left(c_2(c_0^2+c_2^2) + c_0(c_1^2+c_3^2)\right)Y^2 + \left(c_3(c_0^2+c_2^2) + c_1(c_1^2+c_3^2)\right)Y^3. \end{aligned}$$

Problem R5. *Recall that we define the map*

$$\begin{aligned} M &: \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4 \\ M(g) &\equiv c \cdot g \pmod{Y^4+1}. \end{aligned}$$

where we identify the word space $\mathbb{F}_{256}^4$ *with the set of polynomials*

$$\begin{aligned} \mathbb{F}_{256}^4 &= \{g \in \mathbb{F}_{256}[Y] : \deg g < 4\} \\ (a_0, a_1, a_2, a_3) &= a_0 + a_1 Y + a_2 Y^2 + a_3 Y^3. \end{aligned}$$

Here we let $c \in \mathbb{F}_{256}^4$ *be*

$$c = (X, 1, 1, X+1) = X + Y + Y^2 + (X+1)Y^3,$$

where

$$\mathbb{F}_{256} = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1).$$

Prove that M^4 *is the identity map on the set of words, and that* $M^{-1} = M^3$ *is given by*

$$M^{-1}(g) \equiv d \cdot g \pmod{Y^4+1}$$

for all words g, *where*

$$d = (X^3 + X^2 + X) + (X^3+1)Y + (X^3+X^2+1)Y^2 + (X^3+X+1)Y^3.$$

[Hint: Do problem R4 before trying this problem.]

Problem R6. *Find all words* $w \in \mathbb{F}_{256}^4$ *with* $M(w) = w$. *Find a pair of words* v, w *with*

$$M(v) = w, \quad M(w) = v$$

where $w \neq v$.

Date: April 16, 2002.
R4, R5, R6.