Exercise Part 6
Coding Theory, Finite Fields, and AES

Hans Georg Schaathun

10th August 2015

1 Wednesday 29 October 2014

Exercise 1 *Write the following numbers in Hexadecimal:*

1. *321*
2. *1519*

Exercise 2 *Write the following numbers in Octal:*

1. *321*
2. *721*
3. *1519*

Exercise 3 *Write the following hexadecimal numbers in decimal:*

1. *17A2*

Exercise 4 *Write the following octal numbers in decimal:*

1. *077*
2. *03771*

Exercise 5 *Write down the decryption keys for the following transposition encryption keys:*

1. $(4, 5, 1, 3, 2)$
2. $(7, 4, 6, 1, 5, 3, 2)$

Solution:

1. $(3, 5, 4, 1, 2)$
2. $(4, 7, 6, 2, 5, 3, 1)$

Exercise 6 *Find the inverse matrices over* $\mathbb{Z}^5$ *for*

$$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix} \tag{1}$$

You can use Gaussian ellimination in the same way as you would over the reals.

2 Tuesday 4 November 2014

Exercise 7 *Calculate*

1. *Over* $\mathbb{Z}_2$*:* $x^8 + x^6 + x^5 + x^2 + x + 1 \mod x^4 + 1 =$
2. *Over* $\mathbb{Z}_2$*:* $x^6 + x^4 + x^3 + 1 \mod x^4 + x + 1 =$
3. *Over* $\mathbb{Z}_3$ $x^5 + 2x^4 + x^2 + 2 \mod x^3 + 2x + 1 =$

Exercise 8 *Calculate*

1. *Over* $\mathbb{Z}_2$ $(x^3 + x + 1)(x + 1) \mod (x^2 + x + 1)$
2. *Over* $\mathbb{Z}_2$ $(x^3 + x^2 + 1)(x^4 + x^3 + 1) \mod (x^2 + x + 1)$
3. *Over* $\mathbb{Z}_3$ $(x^2 + 2x + 1)(x^4 + x^3 + 2x + 2) \mod (x^3 + 2x + 1)$

3 Thursday 6 November 2014

Exercise 9 *Consider the following matrices:*

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \textit{over } \mathbb{Z}_2,$$

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \textit{over } \mathbb{Z}_3,$$

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 4 & 1 \\ 1 & 0 & 2 \end{bmatrix} \quad \textit{over } \mathbb{Z}_5,$$

Find A^{-1}*.*

4 Friday 7 November 2014