MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 4: Problems for Homework 5

Homework 5: Do the following problems from the textbook: 3.13 #9, 10, 12, 15, 25, 26, 27. Also do the problems below.

Problem 1. In the ring $\mathbb{Z}_2[x]$, let $\xi = x^5+x^2+1$. Show that the polynomial ξ is irreducible (hint: the only irreducible polynomials of degree 2 or less are x, $x+1$, and x^2+x+1. If ξ were reducible, it should have one of these as a factor).

Problem 2. Consider the field $\mathbb{Z}_2[x]/(\xi)$, where $\xi = x^5+x^2+1$. In this field, we write $abcde$ as a notation for $ax^4+bx^3+cx^2+dx+e$, where a, b, c, d, e are elements of $\mathbb{Z}_2$. For example, 11010 is a notation for the element $1x^4+1x^3+0x^2+1x+0 = x^4+x^3+x$. Compute the following. Make sure to write all of your answers either as polynomials of degree less than 5, or as a sequence of 5 binary digits.

(a) $11010 + 01111$.

(b) $11010 \cdot 01111$.

(c) 11010^{-1}.