Coding and Cryptography Fall 2016
Mission #7
Due Friday, November 4th

Katherine E. Stange

October 26, 2016

Note: This is an individual mission. You may meet with group members (optionally) if you'd like to give each other feedback and help, or collaborate on creating proofs.

Overview:

1. The goal of this Mission is to write the textbook chapter on finite fields, including some example problems. I have given a suggested outline below.
2. It is crucial that you cite resources. If you collaborate with someone on a proof or problem, you should cite them there (a simple "Collaborated with so-and-so." will suffice). If you use internet or book resources (including our own textbook) in any way, cite them and explain how (e.g., read the webpage (give URL) to get background information). This is very important. Everything you write must be intellectually your own property, even if you learned the method somewhere else. Cite where you learned the method and then write **after** not **during** your interaction with the resource.
3. In class I'll arrange working pairs for those who wish to collaborate or give feedback with other people in the class.
4. I will grade on whether, as a publisher, I would be happy with this as a textbook chapter in a textbook aimed at students in this course.

The rest of this document serves as a template for the chapter. Please remove anything in red in this document, and replace with appropriate material as explained.

1 Introduction

Give a couple of sentences of introduction saying what we will be studying (in a general way – what type of thing is it?) and why. We will use finite fields when we study coding theory and in a brief introduction to elliptic curve cryptography, among other things.

2 What is a field?

Explain in general terms what a ring and field are.

2.1 The fields axioms

Then give the field axioms (you can steal them from the worksheets directly if you want).

2.2 Common examples

Give common examples of fields and non-fields, e.g. which of the real numbers, complex numbers, rationals, integers, etc. are fields? Explain why or why not.

2.3 When is $\mathbb{Z}/n\mathbb{Z}$ a field?

Remind the reader that $\mathbb{Z}/n\mathbb{Z}$ is a ring, and explain under what circumstance it is a field. Explain exactly what goes wrong when it is not, and why. Give examples to illustrate the point, showing explicitly what goes wrong or not.

3 Finite fields from polynomials

The purpose of this section is to give an explanation of how to generate a ring $(\mathbb{Z}/n\mathbb{Z})[X]/(f(X))$ using a modulus n and a polynomial modulus $f(X)$. First, define the polynomial ring $(\mathbb{Z}/n\mathbb{Z})[X]$ as the collection of polynomials with coefficients in $\mathbb{Z}/n\mathbb{Z}$. Give examples. How many elements does this ring have? Then, define the ring $(\mathbb{Z}/n\mathbb{Z})[X]/(f(X))$ by further working modulo $f(X)$. Tell me exactly what the elements are, and how to combine them with addition and multiplication (i.e. what are the rules for working in the ring? give examples). State a theorem about how many elements this ring has, and write a nice proof.

3.1 The field of four elements

Use this method to create $\mathbb{F}_4$, and show its addition, subtraction, multiplication and division tables. Point out why it is a field, and not just a ring.

3.2 When is $(\mathbb{Z}/n\mathbb{Z})[X]/(f(x))$ a field?

First, define what it means for a polynomial of $(\mathbb{Z}/n\mathbb{Z})[X]$ to be irreducible. Give examples and non-examples, with justification. State a theorem demonstrating that $(\mathbb{Z}/n\mathbb{Z})[X]/(f(X))$ is a field if and only if n is prime and $f(X)$ is irreducible. Prove the 'only if' direction.

3.3 Examples

Generate a novel example of a finite field (not one you've seen anywhere else).

3.4 Finding inverses

Explain that it is possible to find inverses using the Euclidean algorithm, just as one does in modular arithmetic. Demonstrate the process with a novel example (not one you've seen anywhere else).

4 Some example problems

The purpose of this section is to give students some practice problem examples. Give nicely written, completely justified and explanatory solutions, much as you would hope to find in a textbook.

1. Determine the complete list of irreducible polynomials of degree at most 3 working with coefficients modulo 2. Explain your method.
2. For any field K, we write K^* for its invertible elements, i.e. everything except 0. For the field $(\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1)$, find a multiplicative generator of K^*. Justify.
3. Diffie-Hellman Key Exchange could be performed with any finite field, if it has a multiplicative generator for its invertible elements. Give a concrete example demonstration over a finite field of nine elements, with concrete elements, i.e. pick Alice and Bob's secrets, etc.
4. How many elements does a 5-dimensional vector space over $\mathbb{F}_9$, the field of nine elements, have? Justify.