

COMSM2004 : Introduction

B. Warinschi and N.P. Smart

Department of Computer Science,
University Of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB
United Kingdom.

January 30, 2009

Outline

Course Outline

Finite Fields of Char 2

Advanced Cryptography

In this course we will look in more depth at some of the topics considered in COMS30124

We assume

- ▶ You are familiar with the material in COMS30124
- ▶ Can write small programs in C/C++
 - ▶ In fact in C++, but the only non-C bit of C++ we will use will be the I/O stream library

Advanced Cryptography

We will look at

- ▶ Stream Cipher Design
- ▶ Differential Cryptanalysis of Block Ciphers
- ▶ Cryptographic Hash Functions
- ▶ Digital Signatures
- ▶ Zero-Knowledge Proofs
- ▶ Advanced Protocols (Voting, Ecash etc)
- ▶ Elliptic Curve Cryptography

But first we need to recap on some finite field stuff from COMS30124 and introduce finite fields in characteristic two

Fields

A **Field** is a set with two operations $(G, \times, +)$ such that

- ▶ $(G, +)$ is an abelian group, identity denoted by 0.
- ▶ $(G \setminus \{0\}, \times)$ is an abelian group
- ▶ $(G, \times, +)$ satisfies the **distributive law**

Distributive law

For all $f, g, h \in (G, \times, +)$

$$f \times (g + h) = (f \times g) + (f \times h).$$

Examples

Rational numbers, real numbers, complex numbers, integers modulo p .

Fields

We define the set of invertible elements of $\mathbb{Z}/N\mathbb{Z}$ as

$$(\mathbb{Z}/N\mathbb{Z})^* = \{a \in \mathbb{Z}/N\mathbb{Z} : \gcd(a, N) = 1\}.$$

The set $(\mathbb{Z}/N\mathbb{Z})^*$ is always a group with respect to multiplication and clearly has size $\phi(N)$.

When N is a prime p we have

$$\mathbb{Z}/N\mathbb{Z}^* = \{1, \dots, p-1\}.$$

We define the sets

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, \dots, p-1\} \quad \text{and} \quad \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^* = \{1, \dots, p-1\}.$$

We call \mathbb{F}_p a **finite field** of **characteristic p** .

Finite fields are of central importance in **coding theory** and **cryptology**.

Characteristic Two Fields

Of particular interest are fields of char 2.

Take an **irreducible** binary polynomial f of degree n and let \mathbb{F}_{2^n} denote all the binary polynomials of degree $< n$.

Addition in \mathbb{F}_{2^n} is defined as

- ▶ $a \oplus b = a + b \pmod{2}$
- ▶ Note this means $-a = a$.

Multiplication in \mathbb{F}_{2^n} is defined as

- ▶ $a \otimes b = a \cdot b \pmod{f}$.
- ▶ Inversion is performed by a variant of the Euclidean algorithm for polynomials.

Characteristic Two Fields

Often write

$$\mathbb{F}_{2^n} = \mathbb{F}_2[x]/f$$

to denote working modulo f .

Set of non-zero elements denoted by $\mathbb{F}_{2^n}^*$

- ▶ This is the **multiplicative subgroup** of the field

Char 2 Example

Let $f = x^6 + x + 1$ (this is **irreducible**) The finite field of 2^6 elements can then be identified with

- ▶ Bit strings of length six bits
- ▶ Binary polynomials of degree less than or equal to five

$$a = 001101 = x^3 + x^2 + 1$$

$$b = 101011 = x^5 + x^3 + x + 1$$

$$a \oplus b = 100110 = x^5 + x^2 + x$$

- ▶ Since the two x^3 and the two 1 terms cancel, as we are working mod two.
- ▶ Notice, we are simply taking the exclusive-or of the bit string representation.

Char 2 Example

Recap $f = x^6 + x + 1$, $a = 001101 = x^3 + x^2 + 1$,
 $b = 101011 = x^5 + x^3 + x + 1$.

Since f is sparse reduction mod f done using rewriting, as
 $x^6 = x + 1 \pmod{f}$,

$$\begin{aligned}a \otimes b &= (x^3 + x^2 + 1) \cdot (x^5 + x^3 + x + 1) \\&= x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 \\&= x^6 \cdot (x^2 + x + 1) + x^4 + x^3 + x^2 + x + 1 \\&= (x + 1) \cdot (x^2 + x + 1) + x^4 + x^3 + x^2 + x + 1 \\&= (x^3 + 1) + (x^4 + x^3 + x^2 + x + 1) \\&= x^4 + x^2 + x.\end{aligned}$$

i.e. $a \otimes b = 010110 = x^4 + x^2 + x$.

Char 2 Example

Since f is assumed irreducible, every polynomial $a \neq 0$ is coprime to f .

Hence, using a binary polynomial version of the extended GCD algorithm we can find u and v so that

$$u \cdot a + v \cdot f = 1 \pmod{2}.$$

In which case $a^{-1} = u$ in \mathbb{F}_{2^n} .

If $a = x^3 + x^2 + 1$ and $f = x^6 + x + 1$ then taking $u = x^5 + x^3$ and $v = x^2 + x + 1$ gives us

$$\blacktriangleright u \cdot a + v \cdot f = 1 \pmod{2}$$

and so

$$\blacktriangleright a^{-1} = u = x^5 + x^3 = 101000.$$

Choice of Defining Polynomial

All char 2 fields of the same degree n are **isomorphic**.

- ▶ This means it does not depend on which polynomial f we take.
- ▶ Different f 's give different representations of the same thing.

Let $f(x)$ and $g(y)$ be irreducible polynomials of degree n . Then there are polynomials $r(x)$ and $s(y)$ such that one can map one field into the other via

- ▶ $x \pmod{f(x)} \longrightarrow s(y) \pmod{g(y)}$
- ▶ $y \pmod{g(y)} \longrightarrow r(x) \pmod{f(x)}$

This means we can select the best irreducible polynomial f for our own implementation.

- ▶ Requires the mapping $s(y)$ only when talking to someone else's implementation which uses $g(y)$ instead.

Primitive Polynomials

Let $f(X)$ be an irreducible binary polynomial of degree n .

Let θ denote a root of $f(X)$

- ▶ i.e.

$$\mathbb{F}_{2^n} = \mathbb{F}_2[\theta]$$

Such an $f(X)$ is called **primitive** if θ generates $\mathbb{F}_{2^n}^*$

- ▶ i.e. as a set

$$\mathbb{F}_{2^n}^* = \{\theta^i : i = 0, \dots, 2^n - 1\}$$

Primitive polynomials are important when we look at Linear Feedback Shift Registers

Primitive Polynomials

The number of primitive polynomials of degree n is

$$\lambda(n) = \phi(2^n - 1)/n$$

Hence there are a lot:

- ▶ If $n = 4$ then $\lambda(n) = 2$
- ▶ If $n = 5$ then $\lambda(n) = 6$
- ▶ If $n = 6$ then $\lambda(n) = 6$
- ▶ If $n = 14$ then $\lambda(n) = 756$
- ▶ If $n = 15$ then $\lambda(n) = 1800$
- ▶ If $n = 16$ then $\lambda(n) = 2048$
- ▶ If $n = 20$ then $\lambda(n) = 24000$
- ▶ If $n = 21$ then $\lambda(n) = 84672$
- ▶ If $n = 22$ then $\lambda(n) = 120032$

The Rijndael Field

Of additional interest is the following field of degree 8

- ▶ It is used in Rijndael and some error correcting code systems

Identify **bytes** (8 bits) with elements of the field of degree 8

Defining polynomial f given by

$$f = x^8 + x^4 + x^3 + x + 1$$

Write numbers (base 16) to represent the elements

- ▶ $0x01 \longrightarrow 1$
- ▶ $0x02 \longrightarrow x$
- ▶ $0x03 \longrightarrow x + 1$
- ▶ $0x05 \longrightarrow x^2 + 1$
- ▶ etc