Scribe Notes for *Algorithmic Number Theory*
Class 14—June 5, 1998

Scribes: Nick Loehr, Lynn W. Jones, and Hussein Suleman

Abstract

In today's class, we began discussion of finite fields. In particular, we are interested in the representation of the elements of finite fields and algorithms for performing arithmetic with them.

1 Homework Assignment 3

Duxing presented an elegant proof and solution to finding the number of solutions to $x^2 = x$ in $\mathbb{Z}/(n)$. Cara demonstrated two ways of applying Theorem 5.8.1 to find the Legendre symbol

$$\left(\frac{958816}{129527}\right).$$

2 Finite Extensions of Fields

If k is a field and $f \in k[X]$ is an irreducible polynomial over k, then we can define a new field

$$k' = k[X]/(f).$$

Since k' has no zero divisors, it is indeed a field, with $k \subset k'$. The elements of k' are the equivalence classes of $k[X]$ modulo f. Moreover, k' is a vector space over k, of dimension equal to the degree of f.

The polynomial f splits into linear factors in k'. Thus, all (deg f) roots of f are present in k'.

Basic Facts about Finite Fields of Characteristic p

If we fix a prime number p to be the characteristic of a finite field, the following properties will hold.

1. $\mathbb{Z}/(p)$ is a *prime field* and is a subfield of any field of characteristic p. In other words, in any field of characteristic p, there is a subfield isomorphic to $\mathbb{Z}/(p)$. This subfield is generated additively by the multiplicative identity 1.

2. There is a finite field of cardinality $q = p^n$ for every $n \geq 1$. Let $\mathbb{F}_q$ denote this field. The field $\mathbb{F}_q$ is unique up to isomorphism. In other words, every field of the same cardinality has the same algebraic structure.

3. $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$. Thus, any element in $\mathbb{F}_q^*$ raised to the $q - 1$ power equals 1 in the field.

4. $\mathbb{F}_q$ is the smallest extension field of $\mathbb{F}_p$ containing all the roots of $X^{q-1} - 1$. Also, $\mathbb{F}_q$ is a vector space over $\mathbb{F}_p$ of dimension n.

5. Suppose $m < n$ and $m \mid n$. Then $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$. There is a unique isomorphic copy of $\mathbb{F}_{p^m}$ in $\mathbb{F}_{p^n}$, and $\mathbb{F}_{p^n}$ is a vector space of dimension n/m over $\mathbb{F}_{p^m}$. Thus $\mathbb{F}_{p^n}$ is an extension of $\mathbb{F}_{p^m}$. Conversely, if $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$, then $m \mid n$.

6. The subfields of $\mathbb{F}_{p^n}$ form a lattice under inclusion.

Example 2.1. The lattice below illustrates the inclusion relationships among the subfields of the finite field $\mathbb{F}_{p^n}$ for $n = 30$.

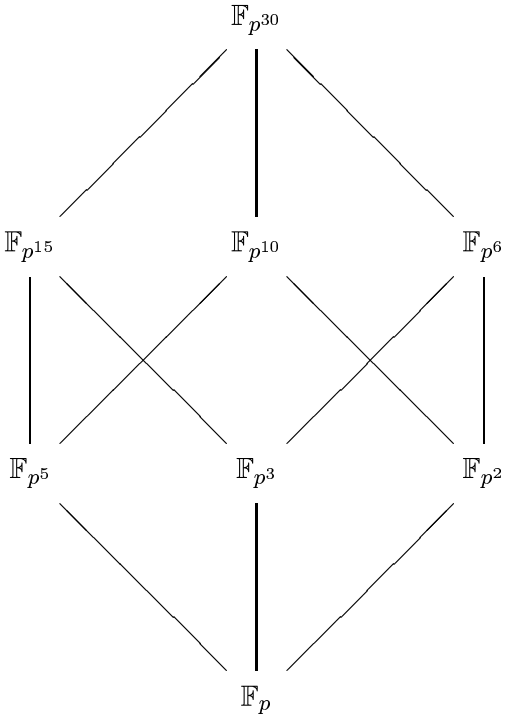

Figure 1: Lattice of subfields of $\mathbb{F}_{p^{30}}$.

3 Models of Finite Fields

From an algorithmic point of view, it is important to find efficient representations of finite fields. To represent $\mathbb{F}_{p^n}$, note that we can always find an irreducible polynomial $f \in \mathbb{Z}/(p)[X]$ of degree n. Suppose this polynomial is $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Then we can represent $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_p$ with basis $\{1, X, X^2, \ldots, X^{n-1}\}$. Every element of the finite field $\mathbb{F}_{p^n}$ can be thought of as a linear combination (with coefficients from $\mathbb{Z}/(p)$) of the elements of the basis. Now, any model to represent the elements of $\mathbb{F}_{p^n}$ must completely define the operations of addition and multiplication. Depending on the particular data representation model employed, some operations are simple while others require table lookups. The following discussion considers different data representations and the tables that need to be generated in each case.

3.1 Naive Model

Each element of the finite field $\mathbb{F}_{p^n}$ is stored as a vector of coefficients used to generate the equivalent linear combination of the basis elements. Then addition is defined as vector addition modulo p. Multiplication of the polynomials, however, results in powers of X that are larger than n, necessitating reduction modulo f. To perform multiplication efficiently, a table of possible powers of X can be precalculated. This will be in the form of an $n \times n$ table, indexed by i and j, where $0 \le i \le n-1$ and $0 \le j \le n-1$, with the ij-entry being

$$X^i \cdot X^j \texttt{ mod } f.$$

The space complexity of this table is $\Theta(n^3 \lg p)$ bits.

3.2 Better Model

The multiplication table generated by the naive model contains a lot of redundancy because a single product can be generated by many different pairs of operands. However, we only need to calculate all powers of X that are possible as a result of multiplication of any two powers of X in the range $[0 \ldots n-1]$.

Thus, we need a one-dimensional table indexed by k, where $0 \le k \le 2n-2$, with the k'th entry being

$$X^k \texttt{ mod } f.$$

This table requires $\Theta(n^2 \lg p)$ bits.

3.3 Alternate Model

Suppose that $f(X)$ is not only irreducible but also *primitive*, i.e., the root X of f generates the cyclic group $\mathbb{F}_q^*$. Then we can represent nonzero elements of the finite field as powers of X, viz.

$$\mathbb{F}_q = \{0\} \cup \{X^i \mid 0 \le i < q-1\}.$$

Multiplication in this representation is very easy, since $X^i \cdot X^j = X^{i+j} = X^{(i+j) \bmod (q-1)}$. Similarly, division is easy since $(X^i)^{-1} = X^{-i} = X^{(q-1)-i}$. However, to perform addition in this model, it is necessary to store a table of size p^n, in which the i'th entry contains $X^i + 1$ written as a power of X. The space required for this table is $\Theta(p^n \lg p^n) = \Theta(np^n \lg p)$ bits.

Example 3.1. Let $p = 2$, $n = 3$, and $f(X) = X^3 + X + 1$. It is easy to check that f is irreducible over $\mathbb{Z}/(2) = \mathbb{F}_2$ and also primitive. If we represent $\mathbb{F}_8$ as $\mathbb{F}_2[X]/(f)$, then

$$\mathbb{F}_8 = \{0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1\}.$$

Table 1 gives the multiplication table stored by the better model for this choice of f. Observe that the entries for $0 \le i < n$ are trivial and could be omitted in a computer implementation of this model.

Table 2 gives the addition table stored by the alternate model for this choice of f. The middle column is used initially to derive the values in the right column; in an actual computer implementation, only the right column would be stored. Note that zero must be treated specially in this model, since 0 is not a power of X.

i	$X^i \bmod f$
0	1
1	X
2	X^2
3	$X+1$
4	X^2+X

Table 1: Multiplication table for $\mathbb{F}_8$ using the better model.

X^i	$X^i \bmod f$	X^i+1
0	0	$1 = X^0$
$1 = X^0$	1	0
X^1	X	X^3
X^2	X^2	X^6
X^3	$X+1$	X^1
X^4	X^2+X	X^5
X^5	X^2+X+1	X^4
X^6	X^2+1	X^2

Table 2: Addition table for $\mathbb{F}_8$ using the alternate model.

3.4 Addition in the alternate model

Consider the addition of field elements a and b using the representation in the alternate model. Since addition is trivial if $a = 0$ or $b = 0$, assume both a and b are nonzero. Then $a = X^i$ and $b = X^j$ for some i and j. Assume with no loss of generality that $i \geq j$. Then, using the distributive law,

$$a + b = X^i + X^j = X^j(X^{i-j} + 1) = X^{j+k},$$

where $X^k = X^{i-j} + 1$ is obtained from the table. Thus, adding two field elements can be done with one table lookup and two integer additions of exponents (to compute $i - j$ and $j + k$).

Example 3.2. Continuing the previous example, we have

$$X^5 + X^3 = X^3(X^2 + 1) = X^3(X^6) = X^9 = X^2.$$

We got the equality $X^2 + 1 = X^6$ directly from the addition table. The equality $X^9 = X^2$ follows since X generates the multiplicative group of nonzero elements of $\mathbb{F}_8$, hence X has order $7 = 8 - 1$ and $X^7 = 1$. As a check, note that $X^5 = X^2 + X + 1$ and $X^3 = X + 1$ from the middle column of Table 2. So

$$X^5 + X^3 = (X^2 + X + 1) + (X + 1) = X^2,$$

in agreement with the first result.

4 Next Time

In the next class, we will revisit the Euclidean algorithm and use it to find the greatest common divisors of polynomials over finite fields.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, The MIT Press, Cambridge, Massachusetts, 1996.