Lecture A – Finite fields

Chloe Martindale

2023

These notes are **Additional Content**, and are only intended for students going for the 90-100 range. Students who prefer to skip the additional content should skip these notes.

A.1 Finite fields

The Pohlig-Hellman attack on the discrete logarithm problem in $\mathbb{F}_p^*$, for p prime, can be thwarted by choosing a prime p such that there is at least one large prime dividing $p-1$.

But, this is a bit of a problem for the ideas we had for efficient computations mod p: remember we were also using Sun-Tzu's Remainder Theorem to make our computations more efficient for encryption.

So, we need a bit more choice in how to set up our cryptosystems: Instead of just using exponentiation mod p we can use exponetiation in some more general contexts. To figure out which contexts will work, we let's first enumerate what we're actually using in for example Diffie-Hellman and ElGamal.

- We need to be able to exponentiate efficiently.
- We need to be able to multiply and add elements together (efficiently).
- We need elements to have inverses that we can compute.
- We need an element (we've been calling it g) of finite order.

The first three properties in the list are all true in any *field*, and the last property will hold if our field is finite. So, instead of just using integers mod p, we want to extend our cryptographic algorithms to be for more general finite fields. What are these exactly?

Definition A.1. A set k is a *field* with respect to binary operations

$$\cdot : k \times k \to k$$

and

$$+ : k \times k \to k$$

if the following axioms are satisfied:

(F1) $(k, +)$ is an abelian group.

(F2) $(k - \{0\}, \cdot)$ is an abelian group.

(F3) For every $a, b \in k$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Examples

- $\mathbb{Z}/p\mathbb{Z}$ for p prime.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Non-examples

- $\mathbb{Z}$ (e.g. 2 has no multiplicative inverse).
- $\mathbb{Z}/4\mathbb{Z}$ (e.g. multiplication is not a binary operation on $\mathbb{Z}/4\mathbb{Z} - \{0\}$: $2 \cdot 2 \equiv 0 \pmod 4 \notin (\mathbb{Z}/4\mathbb{Z}) - \{0\}$.)
- $\mathbb{Z}/n\mathbb{Z}$ for composite n. (Try to extend the reasoning for $\mathbb{Z}/4\mathbb{Z}$ to this case).

If we look at our list of examples above, given that we need a field to be finite, we're left with only $\mathbb{Z}/p\mathbb{Z}$, that we were using already. So how do we construct more examples? To see this, consider for a moment how you first constructed from .

$$\mathbb{C} = \mathbb{R} + i\mathbb{R} = \{a + ib : a, b \in \mathbb{R}\},$$

where is abstractly defined as a number such that $i^2 + 1 = 0$.

We can use the same trick to construct extensions of the fields $\mathbb{Z}/p\mathbb{Z}$. We first see an example.

Example. Define

$$(\mathbb{Z}/2\mathbb{Z}) + \alpha(\mathbb{Z}/2\mathbb{Z}) = \{n + \alpha m : n, m \in \mathbb{Z}/2\mathbb{Z}\},$$

where $\alpha^2 + \alpha + 1 = 0$. This set contains four elements:

$$(\mathbb{Z}/2\mathbb{Z}) + \alpha(\mathbb{Z}/2\mathbb{Z}) = \{0, 1, \alpha, 1 + \alpha\},$$

and we claim that it is a field. Let us first write out an addition table to see why it is an additive group.

+	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

From this table we can read off the desired (nonobvious) group properties: the sum of any two elements lands back in the desired set, every element has an additive inverse (since every element has a 0 in its column), and it is abelian since the table is symmetric about the diagonal.

Now we do the same to check that $((\mathbb{Z}/2Z) + \alpha(\mathbb{Z}/2\mathbb{Z})) - \{0\}$ is a multiplicative group.

$\cdot$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$1+\alpha$	1
$1+\alpha$	$1+\alpha$	1	α

Again, from this table we can read off the desired (nonobvious) group properties: the product of any two nonzero elements lands in the set of nonzero elements, every element has a multiplicative inverse (since every element has a 1 in its column), and it is abelian since the table is symmetric about the diagonal.

You can also check distributivity (F3) but we leave that as an exercise. So here we have a field with 4 elements. It is certainly not the same thing as $\mathbb{Z}/4\mathbb{Z}$ since that is not a field, so we have successfully constructed a new field. We can construct more examples by including higher degrees of α that satisfy different polynomials, and of course using different primes p. However, such a construction won't always work, let's see an example where this goes wrong.

Non-example Let

$$L = \mathbb{Z}/2\mathbb{Z} + \alpha\mathbb{Z}/2\mathbb{Z} + \alpha^2\mathbb{Z}/2\mathbb{Z} + \alpha^3\mathbb{Z}/2\mathbb{Z} = \{a + b\alpha + c\alpha^2 + d\alpha^3 : a, b, c, d \in \mathbb{Z}/2\mathbb{Z}\},$$

where $\alpha^4 + \alpha^2 + 1$. This set has 16 elements:

$$\begin{aligned} L = \{&0, 1, \alpha, 1+\alpha \\ &\alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1 \\ &\alpha^3, \alpha^3+1, \alpha^3+\alpha, \alpha^3+\alpha+1 \\ &\alpha^3+\alpha^2, \alpha^3+\alpha^2+1, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1\}. \end{aligned}$$

In this case $L - \{0\}$ is *not* a multiplicative group, since for example

$$(1+\alpha+\alpha^2)\cdot(1+\alpha+\alpha^2) \equiv 1+\alpha^2+\alpha^4 = 0 \pmod 2 \notin L - \{0\}.$$

What goes wrong in this example that didn't go wrong for the first example? The problem is our defining equation $\alpha^4 + \alpha^2 + 1$ can be factorized, giving nonzero elements that can be multiplied to give 0; these elements will also not have multiplicative inverses. To make this more formal we first introduce some notation.

Notation We notate the set $\mathbb{Z}/p\mathbb{Z} + \alpha\mathbb{Z}/p\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z}/p\mathbb{Z}$, where α is a root of the degree n polynomial $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$, by

$$(\mathbb{Z}/p\mathbb{Z})[x]/(f(x)).$$

(Recall: a degree n polynomial $f(x)$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$ is given by $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$, where the coefficients c_i are integers mod p and $c_n \neq 0$.)

In this notation, our first example above would be written

$$(\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1).$$

To check if something is a field, we can use the following theorem:

Theorem A.1. *Let p be a prime and $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ a polynomial. Then $(\mathbb{Z}/p\mathbb{Z})[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible. It has $p^{deg(f)}$ elements.*

This theorem is actually part of a bigger theorem called the *classification of finite fields*, which we won't go into, but just for your enjoyment, here are some more facts about this construction:

- Every finite field is of the form given in the theorem above.
- For every prime p and $n \in \mathbb{Z}_{>0}$ there exists a finite field of order p^n, and it is unique up to isomorphism.

This (semi) uniqueness of a finite field of a certain order hopefully motivates the following notation.

Notation A finite field of order p^n is denoted by $\mathbb{F}_{p^n}$. The *multiplicative group* $\mathbb{F}_{p^n} - \{0\}$ associated to such a field is denoted by $\mathbb{F}_{p^n}^*$.

So, when confronted with the notation $\mathbb{F}_{p^n}$ and asked to do calculations in that field, your first thought should be: which irreducible degree n polynomial $f(x)$ defines this field? Once you know that, you can write down elements of your field and do calculations with them.

Going back to the use of finite fields in cryptography, you can hopefully see now that you can get a large computation space even with small primes if your take your n to be very large: even $\mathbb{F}_{2^n}$ can work if n is large enough. We can then take a $g \in \mathbb{F}_{2^n}^*$ of large prime order and perform our Diffie-Hellman with this g. Because $\mathbb{F}_{2^n}$ can be viewed as a vector space over $\mathbb{F}_2$, you then can do a lot of your additions just in $\mathbb{Z}/2\mathbb{Z}$ in parallel and this speeds up the computations massively. However, it turns out if you choosen small p (e.g. $p = 2$) and large n, then index calculus is extra effective – in fact in this particular instance it is polynomial time!