

## Finite fields

Two of my sources are

<https://engineering.purdue.edu/kak/compsec/Lectures.html>

<http://www.cs.utsa.edu/~wagner/laws/FFM.html>

Start with some notes from the first one, early chapters from Prof. Kak's course on cryptography.

### Definitions

A **group** is a set of objects plus a binary operation (operator  $o$ ), with the following properties. If  $a, b \in G$ , then the operations exhibit:

- Closure:  $a o b = c \Rightarrow c \in G$
- Associativity:  $(a o b) o c = a o (b o c)$
- Identity element:  $a o i = a$
- Inverse element:  $a o b = i$

A common notation is to use  $\{G, +\}$ , (even if the operation is not really like addition). If  $a + i = a$ , call  $i$  the identity element and typically use 0 for it.

An **Abelian group** is:

- Commutative:  $a o b = b o a$

A **Ring** is a group with the multiplication operator  $\times$  (even if the operation is not really like multiplication). It may be designated as  $\{R, +, \times\}$  and exhibits:

- Closure:  $a \times b \in R$
- Associativity:  $(a \times b) \times c = a \times (b \times c)$
- Distributivity:  $a \times (b + c) = (a \times c) + (a \times b)$

Often the  $\times$  is dropped:  $a(b + c) = ac + ab$ .

A ring *may* be

- Commutative:  $ab = ba$

An **integral domain**  $\{R, +, \times\}$  is a commutative ring that also has

- Multiplicative identity element:  $a \times 1 = a$

If  $ab = 0$ , then either  $a = 0$  or  $b = 0$ .

A **Field**  $\{F, +, \times\}$  is an integral domain that has, for every  $a$  a multiplicative inverse  $b$

- Multiplicative inverse:  $ab = 1$

1 is its own multiplicative inverse.

According to wikipedia

[https://en.wikipedia.org/wiki/Finite\\_field](https://en.wikipedia.org/wiki/Finite_field)

In mathematics, a finite field or Galois field ... is a field that contains a finite number of elements. As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules.

You can read all about it there. I *think* this conveys the general idea.

## Polynomial arithmetic

We switch to a new topic. The connection with fields will be apparent shortly.

A polynomial is an expression of the form:

$$\sum_0^n a_n x^n$$

where the coefficients come from some set  $S$ , for example, the integers:

$$x^5 + 9x^3 + 2x^2 + 1$$

This is a polynomial *of degree 5*.

Polynomial arithmetic deals with addition, multiplication, etc. of polynomials. Consider this example of division for polynomials with cofactors from the real numbers:

$$\frac{8x^2 + 3x + 2}{2x + 1}$$

The first term of the quotient is  $4x$  (because  $4x \times 2x = 8x^2$ ) and

$$4x \times (2x + 1) = 8x^2 + 4x$$

so we subtract that from the numerator and the remainder is  $-x + 2$  and dividing again

$$\frac{-x + 2}{2x + 1}$$

The second term of the quotient is  $-0.5$  (because  $-0.5 \times 2 = -1$  and

$$-0.5 \times (2x + 1) = -x - 0.5$$

Subtracting  $-0.5$  from 2 leaves a remainder of 2.5.

## Additive and multiplicative inverses

Now, suppose we start doing arithmetic with polynomials whose coefficients belong to a finite field. Example:  $Z_7$  which can also be called  $GF(7)$ .

We construct such a field simply by doing all our arithmetic modulo 7. If a value is greater than or equal to 7, we divide by 7 and set the value equal to the remainder.

We will be doing division and subtraction mod 7. For division that means finding a multiplicative inverse for the denominator and *multi-*  
*plying* the numerator by that. Similarly, for subtraction we find the additive inverse of the second term and *add* that to the first term.

### Additive inverses

$$1 + 6 = 0 \text{ mod } 7$$

$$2 + 5 = 0 \text{ mod } 7$$

$$3 + 4 = 0 \text{ mod } 7$$

So, for example, subtracting 3 is the same as adding 4

### Multiplicative inverses.

1 is its own inverse

$$2 \times 4 = 8 = 1 \text{ mod } 7$$

$$3 \times 5 = 15 = 1 \text{ mod } 7$$

$$6 \times 6 = 36 = 1 \text{ mod } 7$$

so 6 is also its own multiplicative inverse.

Example

$$\frac{5x^2 + 4x + 6}{2x + 1}$$

We first divide 5 by 2. Since 4 is the multiplicative inverse of 2 we multiply  $5 \times 4 = 20 = 6 \pmod{7}$ . So the first term of the quotient is  $6x$  and

$$6x \times (2x + 1) = 5x^2 + 6x$$

We need to subtract  $4x - 6x$  which we do by adding  $4x + 1x = 5x \pmod{7}$ . Hence we now have the remainder

$$\frac{5x + 6}{2x + 1}$$

We did this division  $5/2$  before: we got 6.

$$6 \times (2x + 1) = 5x + 6$$

which leaves no remainder. The answer is  $6x + 6$ .

Hence we can write:

$$(6x + 6)(2x + 1) = 5x^2 + 4x + 6$$

That can be done pretty easily without paper. Multiplication is definitely easier than division.

We call  $(6x + 6)$  and  $(2x + 1)$  the factors of  $(5x^2 + 4x + 6)$ .

## GF(2)

Now we're getting closer to the main point. We will be doing binary arithmetic and the coefficients of the polynomials come only from 0 and 1. Therefore, the polynomials are of the form

$$\sum_0^n x^n$$

There are no coefficients now. Either a term is zero or it is  $x$  to some power like  $x^n$ .

GF(2) consists of the set  $\{0,1\}$ .

We define **addition**

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 0$$

Addition is the same as logical XOR.

**subtraction**

$$0 - 0 = 0$$

$$1 - 0 = 1$$

$$0 - 1 = 1$$

$$1 - 1 = 0$$

Notice here that (i)  $1 - 1 = 0$  because (from the first table) the arithmetic inverse of 1 is just 1 since  $1 \oplus 1 = 0$ , so  $1 - 1 = 1 + 1 = 0$ . For a similar reason  $0 - 1 = 1$ .

Another reason is that in moving 0 to  $-1$  we move by one unit.

**multiplication**

$$0 \times 0 = 0$$

$$0 \times 1 = 0$$

$$1 \times 0 = 0$$

$$1 \times 1 = 1$$

Multiplication is the same as logical AND.

Let us work with two such polynomials:

$$(x^4 + x^3 + x + 1), \text{ and } (x^3 + x^2)$$

Addition::

$$(x^4 + x^3 + x + 1) + (x^3 + x^2)$$

What to do with  $2x^3$ ? We do the addition mod 2, and so obtain zero for the coefficient of  $x^3$ . And the important rule is: we *do not* "carry the one."

$$= x^4 + x^2 + x + 1$$

Multiplication:

$$(x^2 + x + 1)(x + 1) = x^3 + x^2 + x + x^2 + x + 1$$

Here, there are two of  $x^2$  and two of  $x$  which all cancel.

$$= x^3 + 1$$

I have a question at this point, why don't we treat this as

$$(0x^3 + 1x^2 + 1x + 1)(0x^3 + 0x^2 + 1x + 1)$$

and use the rules for multiplying 0 and 1 above? In any event, we don't.

**division**

$$\frac{x^2 + x + 1}{x + 1}$$

We can do this formally, or we can guess. The formal method is to divide  $x^2/x$  which is equal to  $x$  so then

$$x \times (x + 1) = x^2 + x$$

Subtraction gives 1, and the answer is  $x$  with a remainder of  $1/x + 1$ .

When

$$\frac{f(x)}{g(x)}$$

leaves no remainder, we say that  $g(x)$  is a factor of  $f(x)$  (and the quotient is another factor).

## Irreducible polynomial

An irreducible or prime polynomial is one without factors. To restate this, to say that a given polynomial  $p(x)$  is irreducible means that there do not exist:

$$f(x) \times g(x) = p(x)$$

The set of polynomials over  $GF(2)$  forms a ring, called the polynomial ring.

There are only two irreducible polynomials of degree 3 in  $GF(2)$  and they are:

$$x^3 + x + 1$$

$$x^3 + x^2 + 1$$

It is claimed that you cannot find  $f(x)$  and  $g(x)$  such that  $f(x) \times g(x)$  is equal to either of these, and these are the only polynomials in  $GF(2)$  with that property.

Now that's a challenge. Suppose we build up possible factors of these expressions, starting with

$$1$$

and continuing with polynomials with greatest term  $x^1$ . There are two:

$$x$$

$$x + 1$$

Now consider polynomials with greatest term  $x^2$  formed by multiplying these last:

$$x(x) = x^2$$

$$x(x + 1) = x^2 + x$$

$$(x + 1)(x + 1) = x^2 + 1$$



Now consider all products with greatest term  $x^3$  by multiplying factors that we have generated so far:

$$\begin{aligned}
x(x^2) &= x^3 \\
x(x^2 + x) &= x^3 + x^2 \\
x(x^2 + 1) &= x^3 + x \\
(x + 1)(x^2) &= x^3 + x^2 \\
(x + 1)(x^2 + x) &= x^3 + x \\
(x + 1)(x^2 + 1) &= x^3 + x^2 + x + 1
\end{aligned}$$

And that's it. There is no way to generate any other polynomial with greatest term  $x^3$ , and since these two do not appear in our results, there is no way to factor either  $x^3 + x + 1$  or  $x^3 + x^2 + 1$ .

Proving something similar for higher degrees might be a challenge, but see Kak's proof, below.

### **Modulo an irreducible polynomial**

We will now consider all polynomials defined over  $GF(2)$  modulo the irreducible polynomial  $x^3 + x + 1$ .

When multiplication results in a polynomial whose degree equals or exceeds that of the irreducible polynomial, we will take for our result the remainder modulo that polynomial.

Example:

$$\begin{aligned}
&(x^2 + x + 1) \times (x^2 + 1) \mod x^3 + x + 1 \\
&= x^4 + x^2 + x^3 + x + x^2 + 1 \mod x^3 + x + 1 \\
&= x^4 + x^3 + x + 1 \mod x^3 + x + 1
\end{aligned}$$

What is

$$\frac{x^4 + x^3 + x + 1}{x^3 + x + 1}$$

well

$$x(x^3 + x + 1) = x^4 + x^2 + x$$

which when subtracted from the numerator leaves  $x^3 - x^2 + 1$  so we have

$$\frac{x^3 - x^2 + 1}{x^3 + x + 1}$$

Now the quotient is 1 with a remainder of  $-x^2 - x$ .

Recall that  $-1 = 1$ , because 1 is its own additive inverse:  $1 + 1 = 0$  so  $1 = 0 - 1$ . We have then  $x^2 + x$ .

Restate the result:

$$\frac{x^4 + x^3 + x + 1}{x^3 + x + 1} = x + 1 + \frac{x^2 + x}{x^3 + x + 1}$$

Let's check:

$$\begin{aligned} & (x^3 + x + 1) \times (x + 1) \\ &= x^4 + x^3 + x^2 + x + x + 1 \\ &= x^4 + x^3 + x^2 + 1 \end{aligned}$$

which falls short of the original numerator  $x^4 + x^3 + x + 1$  by exactly  $x^2 + x$ .

There is a less error-prone way to do this kind of modulo operation and we will see it in the next chapter.

Polynomials defined over  $GF(2)$  modulo the irreducible polynomial  $x^3 + x + 1$  consist of the finite set:

$$0$$

$$\begin{aligned}
&1 \\
&x \\
&x + 1 \\
&x^2 \\
&x^2 + 1 \\
&x^2 + x \\
&x^2 + x + 1
\end{aligned}$$

It's starting to look familiar.

000  
001  
010  
011  
100  
101  
110  
111

There are only eight of them. We refer to this set as  $GF(2^3)$ . 3 is the degree of the modulus polynomial.