

This is a brief summary on finite fields.

INFORMAL DEFINITION: A *field* is a set of “numbers” that can be added, subtracted, multiplied, and divided.

Examples:

- \mathbb{Q} = rational numbers
- \mathbb{R} = real numbers
- \mathbb{C} = complex numbers
- \mathbb{Z}_p when p is prime
- \mathbb{Z} is not a field. Why?
- \mathbb{N} is not a field. Why?

In algorithms we want finite fields, because computers do not handle well infinite objects since they can only store an approximation of an infinite object. Only \mathbb{Z}_p in the above list is a finite field.

Definition 1 A *field* is a structure $(F, +, \cdot, 0, 1)$ in which F is a nonempty set, $0, 1 \in F$ are some some special elements and such that for every $x, y, z \in F$,

1. $(x + y) + z = x + (y + z)$

2. $x + y = y + x$

3. $x + 0 = x$

4. *there is $-x$ such that $x + (-x) = 0$*

5. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

6. $x \cdot y = y \cdot x$

7. $x \cdot 1 = x$

8. *if $x \neq 0$, there is x' such that $x \cdot x' = 1$*

9. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

For what n do we have a field with n elements? The answer is the following important theorem.

Theorem 2 (1) *If p is a prime and k is a natural number, then there is a field with p^k elements. Moreover there is just one such field, which is called $GF[p^k]$.*

(2) *For all other integers n that are not a power of a prime number, there is no field with n elements.*

Example: there is a field with 125 elements.

No field with 35 elements.

How does $GF[p^k]$ look like?

1. Start with Z_p - recall that this is a field.

2. Consider $Z_p[x]$ - set of polynomials with coefficients in Z_p .

3. Choose $p(x)$ a polynomial in $Z_p[x]$ irreducible of degree k .
4. $GF[p^k]$ is $Z_p[x] \bmod p(x)$ - that is we take all polynomials with coefficients in Z_p of degree at most $k - 1$ and we add and multiply them modulo $p(x)$.

Example: $GF[2^8]$

- we take $p(x) = x^8 + x^4 + x^3 + x + 1$, this is irreducible and of degree 8.
- how many polynomials are there $\bmod p(x)$?

they have degree 7

they are of the form

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0.$$

Each $b_i \in Z_2$, so each b_i is either 0 or 1.

So there are 2^8 polynomials.

Each such polynomial can be represented by the sequence of its coefficients.

$$x^7 + x^6 + x^3 + x + 1 \leftrightarrow 11001011.$$

So, we have a 1-to-1 and onto mapping of the set of polynomials of degree 7 with coefficients in Z_2 into the set of bytes.

- **addition**

$$(x^7 + x^6 + x^3 + x + 1) + (x^4 + x^3 + 1) = (x^7 + x^6 + x^4 + x).$$

so

$$11001011 + 00011001 = 11010010.$$

So addition is bitwise-XOR.

- **multiplication**

Multiplication is a little more complex, so let's see first a particular case.

Let's look first at multiplication by x . For example,

$$\begin{aligned}
 (x^7 + x^6 + x^3 + x + 1) \times (x) &= x^8 + x^7 + x^4 + x^2 + x \\
 &= (x^8 + x^4 + x^3 + x + 1) + (x^7 + x^3 + x^2 + 1) \\
 &= (x^7 + x^3 + x^2 + 1) \pmod{p(x)}.
 \end{aligned}$$

So, $11001011 \times 00000010 = 10001101$.

Multiplication method with shift-left + XOR

first we shift=left and append a 0:

$$11001011 \rightarrow 110010110$$

If the first bit is 0 (which is not the case in our example) we stop (because the degree is less than 8 so we don't need to reduce $\pmod{p(x)}$).

If the first bit is 1, then we XOR with $p(x)$

$$\begin{aligned}
 &110010110 \oplus \\
 &100011011 \\
 &= 010001101.
 \end{aligned}$$

We discard the leading 0, and this is the result.

Using the above procedure, we can do multiplication with *any* polynomial.

For example:

To multiply with x^2 , we multiply with x and then again we multiply with x .

To multiply with, say, $x^2 + x$, multiply with x^2 , then with x , and add the results.

And so on.