Chapter 2: The Galois Fields GF(p) .

Chapter Contents.

- More discussion of the modulo-n ring Z_n
- If n=prime, Z_n is not just a ring, it is also a *field*.
- The non-zero elements of Z_n form a multiplicative group of order n-1 when n = prime.
- This multiplicative group is *cyclic* and has at least one generator.
- If n is prime, then for any element **a** of Z_n we have $\mathbf{a}^n = \mathbf{a}$.
- Big Fact: Galois Fields GF(p) are equivalent to Z_p and Z/(p)
- There are several useful relations which apply to elements of GF(p):

$\mathbf{a}^p = \mathbf{a}$
$p\mathbf{a} = \mathbf{0}$
$(\mathbf{a} + \mathbf{b})^p = \mathbf{a}^p + \mathbf{b}^p$
$(\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d} + \ldots)^p = \mathbf{a}^p + \mathbf{b}^p + \mathbf{c}^p + \mathbf{d}^p + \ldots$

Chapter 2: The Galois Fields GF(p) .

Note: throughout this Chapter, we shall assume that p is some prime number, p = 2,3,5,7,11,13,...

More Discussion of Z_n = { mod-n,+,•}

In Chapter 1 we first showed that the set of numbers { 0,1,2,3,...n-1} formed a cyclic additive group which we called { mod-n,+}. A short list of properties was then presented for { mod-n,+}. One such property, for example, was that fact that n**a** = **0** for any a in the group.

The next step was to upgrade this additive group to ring status by endowing it with the modulo • multiplicative operation. This ring was called Z_n = { mod-n,+,•}, and the proof that it really is a ring was presented in full detail. In fact, it is a "ring with identity".

Finally, at the end of Chapter 1 we showed that Z_n is a *field* when n is prime. This means that all non-zero elements have inverses. This leads to the next claim:

Claim: The ring Z_n has n elements which are {**0**,**1**,**2**,**3**...**n-1**}, and we have modulo-n operations + and •. The claim is that, if you consider the subset of the n-1 non-zero elements {**1**,**2**,**3**...**n-1**}, this set forms a *group* under the mod-n • operation, provided that n is a *prime number*. Although the modulo operation is mod-n, the order of this group is n-1, since order is the number of elements in a group.

Proof: We already know that Z_n is a ring with identity, so it is just the inverses that are missing. But since Z_n is a field for prime n, we know these inverses all exist. QED.

Claim : The group just mentioned, {**1**,**2**,**3**...**n-1**} under operation •, is a *cyclic* group! It follows from this claim that there is at least one generator g, so we can write the group as

$\{1, g, g^2, g^3, ...g^{n-2}\}$ where $g^{n-1} = 1$, or $g^n = g$ order = n-1

Proof: It will later be shown that all Galois Fields are cyclic under •.

Fact : If n is prime, then for any element a of Z_n we have: $\mathbf{a}^n = \mathbf{a}$.

Proof: Let our arbitrary element be $a = g^k$. Then $a^n = (g^k)^n = g^{kn} = (g^n)^k = (g)^k = a$, QED.

Example: Let n = 5 = prime, then the 4 elements of our multiplicative group are {1,2,3,4}. These are the non-zero elements of the ring (and field) Z_5. An acceptible generator is 2, since (remember mod-5)

$2^1 = 2$ $2^2 = 4$ $2^3 = 8 = 3$ $2^4 = 16 = 1$

So we can write out our elements using this generator as:

$\{1,2,4,3\} = \{1, 2, 2^2, 2^3\}$ where $2^4 = 1$

Moreover, we can confirm that $a^4 = a$ for all elements of the group:

$1^4 = 1$ $2^4 = 16 = 1$ $3^4 = 81 = 1$ $4^4 = 256 = 1$

It is important to realize that not every element is a generator. Back in Chapter 1 we showed, once one element is known to be a generator, all elements (other than 1) are generators, provided the *order* of the cyclic group is prime. But here, the order is n-1 which is likely not to be prime. It is n that we want to be prime here.

In fact, we showed that g^m is definitely not a generator if order/m = integer. To verify this, our order is n-1 = 4, so we suspect that $g^m = 2^2 = 4$ will not be a generator. Let us check this:

$4^1 = 4$ $4^2 = 16 = 1$ $4^3 = 64 = 4$ $4^4 = 256 = 1$

Sure enough, we are missing half the elements of our group. Element 4 generates a cyclic subgroup of order 2, which we know has to divide evenly into our group order of 4. On the other hand, since 3 does not divide evenly into 4, we are not surprised that $2^3 = 8 = 3$ *is* a viable generator.

$3^1 = 3$ $3^2 = 9 = 4$ $3^3 = 27 = 2$ $3^4 = 81 = 1$

The relation between GF(p) and Z_p

We have made the claim in Chapter 1 that finite fields (ie, Galois Fields) with q elements exist only if q is of the form p^m where p is a prime number, and m is a positive integer. For example,

these fields exist: GF(2), GF(3), GF($4 = 2^2$), GF(5), ...

these fields do not exist: GF(6 = 2*3), GF(15 = 3*5), ...

Furthermore, for a given order q, we claim there is only one such field. So if you find a field of order 5, it has to be GF(5).

We know that for *any* positive integer q, we can write down a pair of "modulo-q" tables for the two operations + and •. Here, for example, are the tables for q = 5:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

For any integer q, we get similar tables. So we have a set of q elements and two operations + and •, and the thing is "closed" under each operation, and distributive holds, and there is an identity, so for any q

the set of elements forms a "ring with identity". This is Z_q. If every element has an inverse, then this thing advances to the front of the class and is proclaimed to be a *field*.

The + table is always boring, since it just contains the q elements cyclically permuted on each new line.

The • table is more interesting. Notice in the above table that a 1 appears in every row except the first row. This means that every element except 0 has an inverse, so our modulo thing is a field when q = 5. In fact, each row except the first is just a reordering of the elements.

Since we have formed a finite field with 5 elements, it must be equivalent to GF(5).

More generally, since we have already identified a set of fields Z_p for any prime p, these must be the GF(p). Recall that these are equivalent also to the residue class fields Z/(p). Thus, we have arrived at this

Super Big Fact: For p = prime, GF(p) = Z_p = Z/(p).

If q is not a prime, this does not work. For example, here is the • table for q = 4.

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Notice that the third row does not contain 1, so the element 2 has no multiplicative inverse. This "modulo-4 ring with identity" has four elements, but it is *not* a field.

We know that the field GF(4) = GF(2^2) exists. So we now know that the + and • tables for GF(4) are *not* the modulo arithmetic tables we have been talking about above. The correspondence between GF(p) and modulo-p only holds when p = a prime number.

So we summarize this section as follows:

Facts about GF(p)

Fact: The non-zero elements of GF(p) form a cyclic group under • of order p-1. There exists at least one element to serve as the generator. For example, for p=5 we have

$$\{2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8 = 3\} = \{1,2,4,3\}$$

Proof: No proof yet. This will come in Chapter 4.

Fact: For any element of GF(p), we claim that $\mathbf{a}^p = \mathbf{a}$, where **a** = **0**,**1**,**2**....**(p-1).** This fact is very useful later on when we consider the elements of GF(p) as coefficients of a polynomial defined on GF(p).

Proof: We already proved this in the section about Z_n above.

Fact: We claim that $p\mathbf{a} = \mathbf{0}$ for any element **a** of GF(p).

Proof: This is because GF(p) = Z_p is a cyclic additive group, see lengthy discussion in Chapter 1.

Example : We are used to the above result in the case of GF(p=2), the binary world, where we say **x** + **x** = 2**x** = **0**. Our usual proof here is to just exhaust the possibilities: **1** + **1** = **0** and **0** + **0** = **0**.

Fact: $(\mathbf{a} + \mathbf{b})^p = \mathbf{a}^p + \mathbf{b}^p$ when **a**,**b** are elements of GF(p), p = prime.

Proof: If you use the binomial theorem to expand the left side, you get p+1 terms and the coefficients are the binomial coefficients **Error!**) for m = 0,1,2....p Except for the first and last term in the binomial expansion, all these coefficients are proportional to p, and since $p\mathbf{n} = \mathbf{0}$ for any field element **n**, we see that all the cross terms having these coefficients must vanish.

Admittedly the result above conflicts with our usual intuition (field = reals) about what $(a+b)^p$ ought be be equal to.

Example: $(\mathbf{1} + \mathbf{x})^p = \mathbf{1} + \mathbf{x}^p$, where x is some element in GF(p), p = prime.

The above fact can be generalized as follows:

Fact: $(a + b + c + d + \ldots)^p = a^p + b^p + c^p + d^p + \ldots$ for a,b,c,d... in GF(p).

Proof: just apply the binomial theory proof a bunch of times.

Conclusion: In this chapter we have identified the Galois Fields GF(p) to be the Z_p . We have not yet nailed down the fields GF(p^m). This is where the notion of polynomials comes into play. As a hint, we note that if you divide a polynomial by some polynomial of degree m, and this polynomial is defined over GF(p), then there are exactly p^m possible remainders you can get. If we can somehow identify each of these remainders with a row of a residue class ring chart, then we may be on our way to constructing a representation of GF(p^m) which is analogous to Z/(p) for GF(p). Whereas integers sufficed for GF(p) and gave us p remainders, we have to go to polynomials to get p^m remainders.