Galois field 2^3

A field satisfies various algebraic properties like closure, associativity and so on. An important distinction of a field is that each element of the field has a multiplicative inverse.

The order of a finite field is the number of elements in the field.

A familiar type of finite field can be constructed with order equal to a chosen prime number. Z_7 is such a field, constructed using standard addition and multiplication, modulo 7.

There are 7 elements in Z_7 but the multiplication table has 6 rows and 6 entries per row.

1	2	3	4	5	6
2	4	6	1	3	5
3	6	2	5	1	4
4	1	5	2	6	3
5	3	1	6	4	2
6	5	4	3	2	1

1					
2	4				
3	6	2			
4	1	5	2		
5	3	1	6	4	
6	5	4	3	2	1

The table on the right has the duplicate entries removed (since $ab = ba$).

Each row contains all of the elements of the field, as a consequence one and only one product is equal to 1, so each element has a multiplicative inverse, which is unique.

prime powers

Rather than being a prime number, alternatively the order can be a prime power, that is, an integer power of a prime. Wikipedia says that there are no other examples of finite fields beyond these two types.

In cryptography we are most interested in the field GF(2^8), but to make the arithmetic easier, we start by exploring GF(2^3).

The usual way to explain the construction is to talk about polynomials of the form

$$ax^2 + bx + c$$

where the cofactors are either 0 or 1 (that's the 2 part of the field's designation).

These are the seven field elements:

$$1$$

$$x$$

$$x + 1$$

$$x^2$$

$$x^2 + 1$$

$$x^2 + x$$

$$x^2 + x + 1$$

Unlike with Z, for GF(2^3), 0 is not an element.

There are three more rules for arithmetic. Addition is XOR with no carry:

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

$$1 + 1 = 0$$

A corollary is that subtraction is the same as addition.

Multiplication is polynomial multiplication:

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

followed by the XOR addition rule:

$$= x^2 + 1$$

The third and final rule is that if the result of multiplication is a polynomial of degree 3 (or higher), carry out "division" by an **irreducible polynomial** until the result is of degree 2 or less. There are two possible choices for the special polynomial:

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

$$x^3 + x + 1$$

We'll see how these are arrived at in the next section.

Division is repeated subtraction (addition). So, for example

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

$$x^3 \bmod (x^3 + x + 1) = x + 1$$

A nice trick for doing this is to use the binary equivalent:

```
1000 = x^3
1011 = x^3 + x + 1
----
0011
```

The result is $x+1$, as we said. Notice that even though 1000 is smaller than 1011 in binary, we still do the XOR operation, because it is of degree 3.

Continue doing XOR until the result is of degree 2 or less. For example, with x^4 we would do

```
10000 = x^4
10110 = x^4 + x^2 + x
-----
00011 = x^2 + x
```

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

Multiplication in the binary format is a left-shift. Times 2 is just left-shift one place. Times $4x$ is left-shift two places..

Times 3 is times 2, then XOR with times 1, the original number.

Now consider

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

One approach is

```
00101 = x^2 + 1
00111 = x^2 + x + 1
------
00101
01010
10100
-----
11011
```

The mod operation is:

```
11011
1011  = x^4 + x^2 + x
----
01101
 1011 = x^3 + x + 1
 ----
```

```
0110
```

We could have done repeated XOR of the polynomial $x^3 + x + 1$, but instead at the first step multiplied by x.

The answer is

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

There's another approach which is worth mentioning. We can take the intermediate result

$$= x^4 + x^3 + x + 1$$

and substitute $x^4 = x^2 + x$ and $x^3 = x + 1$ from above

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

irreducible polynomials

We want to find polynomials that do not have factors, that cannot be arrived at by multiplying together two polynomials.

For this multiplication we are not using the special rule mod rule, we are not working in the field yet. We are just looking. However, we do use XOR addition.

The degree 2 or smaller polynomials are

$$1$$

$$x + 1$$

$$x$$

Multiplying by 1 doesn't go anywhere.

To go to degree 2 multiply

$$x \cdot x = x^2$$

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

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

There is one more degree 2 polynomial that is not generated by this procedure:

$$x^2 + x + 1$$

Since this one has no "factors" in the field, it is irreducible, which is (somewhat) analogous to being prime. It could be used to form the field GF(2^2), which has three elements.

Next, multiplying all pairwise combinations of degree 1 with degree 2 to form degree 3 polynomials, there are eight results and six are unique. (We did this in the previous write-up, but repeat it here).

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

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

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

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

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

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

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

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

Two polynomials of degree 3 are not produced by this method. It is easier to see which they are if we write the results in binary:

```
1000 1010 1001
1100 1110 1111
```

The two missing polynomials, 1011 and 1101, are the irreducible ones.

$$x^3+x+1$$

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

We could choose either of these to form the field GF(2^3). We chose the first one, above.

multiplication table

Constructing a multiplication table is a bit of a pain, but it's a useful exercise. Start by re-computing the modulus result for x^3 and x^4:

```
1000 x^3
1011
----
0011 x + 1
```

$x^3 = x+1$ in this field, and $x^4 = x^2+x$ because

$$x^4 \bmod x^3+x+1 = x^2+x$$

```
10000 x^4
10110
-----
00110 x^2 + x
```

That was just a left-shift of the irreducible polynomial by one place (corresponding to multiplication by 010).

If there additional terms, say we had $x^3 + x$, the result is $x + 1$ from x^3 then XOR the other term(s): here the result is 1. Thus

$$x^3 + x \bmod x^3 + x + 1 = 1$$

And therefore, factoring, we find that $x^2 + 1$ and x are multiplicative inverses.

Let's start the table

1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x^2	.	.	.	.	.
$x+1$	x^2+x	.	.	.	.	.
x^2	$x+1$	.	.	.	.	.
x^2+1	1	.	.	.	.	.
x^2+x	x^2+x+1	.	.	.	.	.
x^2+x+1	x^2+1	.	.	.	.	.

The second column contains each of the elements multiplied by x. We used the fact that $x(x^2) = x^3 = x + 1$ as described above.

Also, $x(x^2 + x) = x^3 + x^2 = (x + 1)$ XOR x^2.

Finally $x(x^2 + x + 1) = x^3 + x^2 + x = (x + 1)$ XOR $x^2 + x = x^2 + 1$.

Each column and each row will turn out to contain all 7 elements of the field.

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

The same 7 elements fill each row and each column. Every polynomial has a unique inverse, and the inverses match (of course).

Having filled out and laborious re-checked the table, it's pretty clear that polynomials are not the way to do this sort of thing.

Instead, we write binary numbers

```
001   010   011   100   101   110   111
010   100   110
011   110   101
100   011
101
110
111
```

In filling out the second column, we have reached the first division operation.

$$100 * 010 = 1000 \rightarrow 011$$

$$101 * 010 = 1010 \rightarrow 001$$

It is very fast with pen and paper and not at all error-prone.

Two points: first, this is one way to find multiplicative inverses for a field like GF(2^3): exhaustive calculation. However, it is not practical for GF(2^8) with 65,000+ multiplications.

Second, the reason for choosing an irreducible polynomial becomes clear: we *must not* produce zero.

other methods

What about other approaches? There are at least three.

The one we use extensively elsewhere (in code) is based on knowledge that **0x03** is a primitive element or generator of the field GF(2^8), which

is to say that $(\mathbf{0x03})^8 = \mathbf{0x03}$. When wikipedia talks about the $q-1$ root of unity, this is what they refer to.

By this operation we can produce a table of powers, and then by inverting the table produce discrete logarithms, and then find logs which sum to the right number (i.e. 7). We'll see that below.

The second method is the extended Euclidean algorithm. And the third is the one we take up next.

Suppose we want to find the multiplicative inverse of x^2+x in GF(2^3). Write a general polynomial

$$(x^2+x)(ax^2+bx+c)$$

$$= ax^4+bx^3+cx^2+ax^3+bx^2+cx$$

group like terms:

$$= ax^4+(b+a)x^3+(c+b)x^2+cx$$

Now, just substitute for the values of x^4 and x^3 mod the irreducible polynomial x^3+x+1, namely

$$= a(x^2+x)+(b+a)(x+1)+(c+b)x^2+cx$$

so again re-group to obtain

$$= (a+b+c)x^2+(a+b+a+c)x+(a+b)$$

$$= (a+b+c)x^2+(b+c)x+(a+b)$$

The source

`https://math.stackexchange.com/questions/2357753/multiplicative-inverse`

has

$$= (b+c-a)x^2+(c-b)x+(a+b)$$

but subtraction is the same as addition, so these are equivalent.

Our goal is that the product should be equal to 1, that is to the polynomial with coefficients $(0, 0, 1)$ thus:

$$a + b + c = 0$$

$$b + c = 0$$

$$a + b = 1$$

Subtracting the second from the first, it is clear that $a = 0$.

If we supposed that $a = 1$ then we would have $b = 0, c = 0$ and $1 + 0 + 0 = 0$, a contradiction. Hence $a = 0$.

Then, $b = 1$ and $c = 1$ also, since $1 + 1 = 0$. Therefore, the inverse should be $x + 1$. Check it:

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

Divide by $x^3 + x + 1$ (or just add $x + 1$) and obtain 1 as the answer. It checks.

generators

Some elements are generators, some are not. I tried 011 because it works with GF(2^8):

```
0011
0011
----
0011
0110
----
0101  =>  0101
```

```
==========
0101
0011
----
0101
1010
----
1111
1011
----
0100  =>  101, 100
==========
0100
0011
----
0100
100
----
1100
1011
----
0111  =>  101, 100, 111
==========
0111
0011
----
0111
111
----
1001
1011
```

```
----
0010  =>  101, 100, 111, 010
===========
0010
0011
----
0010
0100
----
0110  =>  101, 100, 111, 010, 110
===========
0110
0011
----
0110
1100
----
1010
1011
----
0001  =>  101, 100, 111, 010, 110, 001
===========
0001
0011
-----
0011 =>  101, 100, 111, 010, 110, 001, 011
```

That's all seven, that's all we need. Here they are with their logarithms.

```
011, 101, 100, 111, 010, 110, 001, 011
  1,   2,   3,   4,   5,   6,   7,   8
```

Since the generator to the 0 power is equal to the generator to the 7 power, we need the logs to sum to 7.

As an example, the log of $x^2+x = 110$ is 6. The log of its multiplicative inverse must therefore be 1, which corresponds to 011. We showed already (by two approaches) that $011 = x + 1$ is the correct value.

Extended Euclidean algorithm review

Let us review the method in decimal first.

Construct two co-prime integers:

$$3 \cdot 7 \cdot 11 = 231$$

$$2 \cdot 5 \cdot 13 = 130$$

and then carry out Euclid's algorithm, keeping the quotient as well as the remainder from each step.

```
a   b   r   q
231 130 101 1
130 101 29  1
101  29 14  3
 29  14  1  2
 14   1  0  2
```

1 is the $GCD(130, 231)$, as we already knew.

Rewrite the results as subtractions

```
  r =   a - (q)  b
101 = 231 - (1)130
 29 = 130 - (1)101
 14 = 101 - (3) 29
  1 =  29 - (2) 14
```

```
0 =  14 - (1) 14
```

One can go forward or backward. I prefer to start from the equation with 1 on the left-hand side:

$$1 = 29 - (2)14$$

Substitute for 14 from the previous equation:

$$1 = 29 - (2)[101 - (3)29]$$

$$= (7)29 - (2)101$$

Then substitute for 29:

$$1 = (7)[130 - 101] - (2)101$$

$$= (7)130 - (9)101$$

And finally, substitute for 101:

$$1 = (7)130 - (9)[231 - 130]$$

$$= (16)130 - (9)231$$

We have thus written 1 as a *linear combination* of a and b.

Finally, do mod 231

$$1 = (16)130 \bmod 231$$

Our result is that 16 and 130 are multiplicative inverses mod 231

$$9 \cdot 231 = 2079 = 16 \cdot 130 - 1$$

There are other inverses revealed as well.

Finite field EEA

So then the question is: how to carry this out for a finite field like GF(2^3)?

If we have two polynomials $a(x)$ and $b(x)$ we can find their gcd, and then find two more polynomials $s(x)$ and $t(x)$ such that

$$gcd(a, b) = s(x)a(x) + t(x)b(x)$$

and if the gcd is 1 then they are co-prime and

$$1 = s(x)a(x) + t(x)b(x)$$

So if $a(x) = m(x)$ is the irreducible polynomial 1011, then certainly the gcd with any polynomial in the field is 1 so we should be able to find

$$1 = s(x)m(x) + t(x)b(x)$$

and then do modulo $m = 1011$ we have

$$1 = t(x)b(x)$$

example 1: $x^2 + x$

Recall that $x^2 + x$ is written as 110 I'm going to adopt the convention that elements of the field (degree 2 or less) will be written with as few digits as possible.

We seek gcd(1011,110). The smallest q that works is 10:

```
   a   b   q   qb   r
1011 110  10 1100 111
 110 111  01  111   1
------
111 = 1011 - 10 * 110
  1 =  110 - 01 * 111
    =  110 - 01[1011 - 10 * 110]
    =  11 * 110
    = (x + 1)(x^2 + x)
```

Note $q \cdot b > a$ is still OK.

Suppose we try $q = 11$:

```
   a   b   q   qb   r
1011 110  11 1010   1
------
  1 =  1011 - 11 * 110
    =  11 * 110
    = (x + 1)(x^2 + x)
```

We have that the multiplicative inverse of $x^2 + x$ is $x + 1$, which should not come as a surprise.

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

example 2: x

We want $\gcd(1101, 010)$.

We might pick $q = 100$ but notice $q = 101$ gives

```
   a   b   q   qb   r
1011 010 101 1010   1
------
  1 = 1011 - 101 * 010
    =  101 * 010
    =  (x^2 + 1)(x)
```

Refer back to above to the multiplication table or the logarithms section to confirm that x and $x^2 + 1$ are inverses. Does $q = 100$ work?

```
   a   b   q   qb   r
1011 010 100 1000  11
  10  11   1   11   1
------
 11 = 1011 - 100 * 010
  1 =   10 - 1 * 11
    =   10 - 1 * [1011 - 100 * 010]
    =  101 * 010
    =  (x^2 + 1)(x)
```

The answer is the same, $x^2 + 1$ and x are inverses.

example 3: $x^2 + x + 1$

```
gcd(m, x^2 + x + 1)

   a   b   q   qb   r
1011 111  10 1110 101
 111 101   1  101  10
 101  10  10  100   1

101 = 1011 - (10)111
 10 =  111 - (01)101
```

```
  1 =  101 - (10)10
    =  101 - (10)[111 - (01)101]
    =  (11)101 - (10)111
    =  (11)[1011 - (10)111] - (10)111
    = -(110)111 - (10)111
    =  (100)111
    = (x^2)(x^2 + x + 1)
```

Suppose we made a different choice for that first quotient:

```
gcd(m, x^2 + x + 1)

   a   b   q   qb   r
1011 111  11 1001  10
 111  10  11  110   1

  10 = 1011 - (11)111
   1 = 111  - (11)10
     = 111 - (11)[1011 - (11)111]
     = 111 + (101)111
     = 100(111)
     = (x^2)(x^2 + x + 1)
```

Provisionally, it seems that one can pick any multiplier that will get the degree right, and we obtain the correct answer.