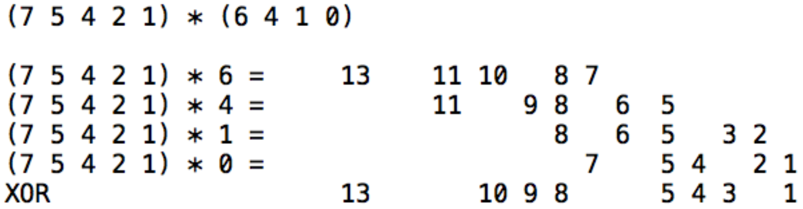
# Generators, logarithms, inverses

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

### Improved multiplication, and generators for GF(2e8)

Following the reference, we first take another look at multiplication.

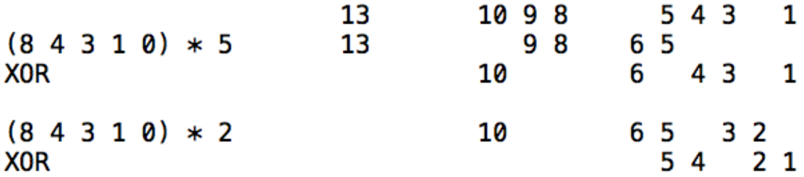
Previously, we multiplied **0xb6 * 0x53** by doing $(7, 5, 4, 2, 1) * (6, 4, 1, 0)$



```
(7 5 4 2 1) * (6 4 1 0)

(7 5 4 2 1) * 6 =     13    11 10   8 7
(7 5 4 2 1) * 4 =           11    9 8   6  5
(7 5 4 2 1) * 1 =                   8   6  5   3 2
(7 5 4 2 1) * 0 =                     7    5 4   2 1
XOR                   13       10 9 8      5 4 3   1
```

followed by the modulus operation by repeated $\oplus$ at the end:

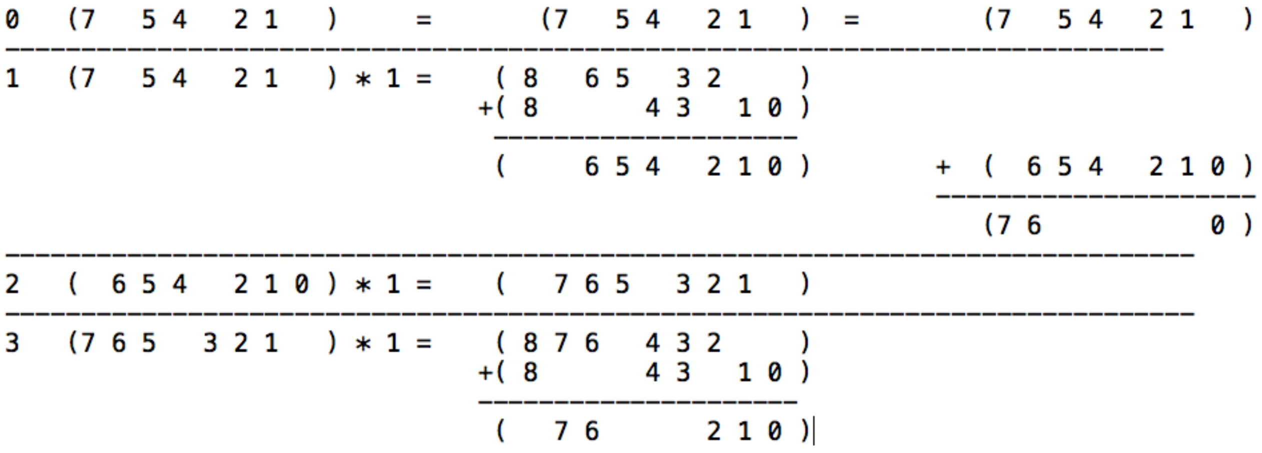


```
                      13       10 9 8      5 4 3   1
(8 4 3 1 0) * 5       13          9 8    6 5
XOR                            10        6   4 3   1

(8 4 3 1 0) * 2                10        6 5   3 2
XOR                                        5 4   2 1
```

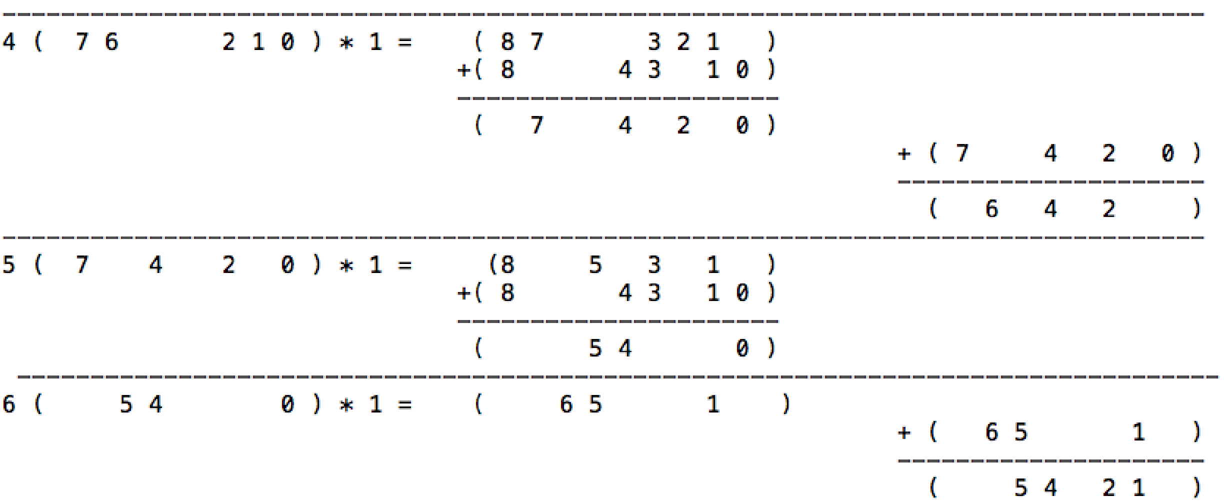
The following is given as a more efficient version. Whenever a value in the program exceeds 255, we do an XOR with the irreducible polynomial.

Again we have $(7, 5, 4, 2, 1) * (6, 4, 1, 0)$. In the first phase (round 0) we have just $(7, 5, 4, 2, 1) * 0$. In the round 1 we multiply by 1 (i.e. $x$) to give $(8, 6, 5, 3, 2)$, which we immediately XOR with the special polynomial $m(x) = (8, 4, 3, 1, 0)$, and then XOR that with what we had from phase 0.



```
0   (7   5 4   2 1   )     =     (7   5 4   2 1   )  =      (7   5 4   2 1   )
----------------------------------------------------------------------------
1   (7   5 4   2 1   ) * 1 =    ( 8   6 5   3 2     )
                               +( 8       4 3   1 0 )
                                --------------------
                                (     6 5 4   2 1 0 )      + (  6 5 4   2 1 0 )
                                                           ---------------------
                                                             (7 6           0 )
-------------------------------------------------------------------------------
2   (  6 5 4   2 1 0 ) * 1 =    (   7 6 5   3 2 1   )
-------------------------------------------------------------------------------
3   (7 6 5   3 2 1   ) * 1 =    ( 8 7 6   4 3 2     )
                               +( 8       4 3   1 0 )
                               ---------------------
                                (   7 6       2 1 0 )
```

In round 2 we bump up the multiplicand by a factor of 2 again (of course, it was reduced by the modulus in the previous round). We do the same again in round 3, and find we have again exceeded the modulus. So we do another XOR.



```
--------------------------------------------------------------------------------
4 (  7 6       2 1 0 ) * 1 =    ( 8 7       3 2 1   )
                               +( 8       4 3   1 0 )
                               ----------------------
                                (   7     4   2   0 )
                                                          + ( 7     4   2   0 )
                                                          ---------------------
                                                            (   6   4   2     )
--------------------------------------------------------------------------------
5 (  7    4    2   0 ) * 1 =     (8     5   3   1   )
                               +( 8       4 3   1 0 )
                               ----------------------
                                (       5 4       0 )
 --------------------------------------------------------------------------------
6 (     5 4        0 ) * 1 =    (     6 5       1     )
                                                          + (   6 5       1   )
                                                          ---------------------
                                                            (     5 4   2 1   )
```

In round 4, we increase by a factor of 2, divide by the special number, and XOR what we accumulated before. In round 6, we increase by a factor of 2 and do the modulus thing, In round 6, we increase by 2-fold and do the XOR thing. The result is $(5, 4, 2, 1)$, which is the same as what we got before.

### Generators in fields

According to the reference a

> A generator is an element whose successive powers take on every element except the zero.

Having faith that one exists we try various possibilities for $Z_{13}$: powers of 5

$$5$$

$$5^2 = 25 \quad \mathrm{mod}\ 13 = 12$$

$$5^3 = 5 \times 12 \quad \mathrm{mod}\ 13 = 8$$

$$5^4 = 5 \times 8 = 40 \quad \mathrm{mod}\ 13 = 1$$

So now the pattern will repeat, and we have only 4 values.

You could try 4

$$4$$

$$4^2 = 16 \quad \mathrm{mod}\ 13 = 3$$

$$4^3 = 4 \times 3 = 12 \quad \mathrm{mod}\ 13 = 12$$

$$4^4 = 4 \times 12 = 48 \quad \mathrm{mod}\ 13 = 9$$

$$4^5 = 4 \times 9 = 45 \quad \mathrm{mod}\ 13 = 6$$

$$4^6 = 4 \times 6 = 24 \quad \mathrm{mod}\ 13 = 9$$

$$4^7 = 4 \times 9 = 36 \quad \mathrm{mod}\ 13 = 10$$

$$4^8 = 4 \times 10 = 40 \quad \mathrm{mod}\ 13 = 1$$

so we terminate with only 8 values.

Persevere!

$$2 \times 1 = 2$$

$$2 \times 2 = 4$$

$$2 \times 3 = 8$$

$$2 \times 4 = 16 \quad \mathrm{mod}\ 13 = 3$$

$$2 \times 3 = 6$$

$$2 \times 6 = 12$$

$$2 \times 12 = 24 \quad \mathrm{mod}\ 13 = 11$$

$$\begin{gathered}
2 \times 11 = 22 \quad \text{mod } 13 = 9 \\
2 \times 9 = 18 \quad \text{mod } 13 = 5 \\
2 \times 5 = 10 \\
2 \times 10 = 20 \quad \text{mod } 13 = 7 \\
2 \times 7 = 14 \quad \text{mod } 13 = 1
\end{gathered}$$

We see that 2 will generate:

$$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$$

That is all the values we need.

Generators are hard to discover.

Here is an example from Kak, lecture 7. Recall that the polynomials defined over $GF(2^3)$ modulo the irreducible polynomial $x^3 + x + 1$ consist of the finite set:

$$\begin{gathered}
0, \quad 1, \quad x, \quad x+1 \\
x^2, \quad x^2+1, \quad x^2+x, \quad x^2+x+1
\end{gathered}$$

Kak says:

> The generator g is that element which symbolically satisfies $g^3+g+1=0$, implying that such an element will obey $g^3 = -g - 1 = g + 1$

.

The first element is 0, then the generator gives us

$$\begin{gathered}
g^0 = 1 \\
g^1 = g \\
g^2 = g^2 \\
g^3 = g + 1 \\
g^4 = g(g^3) = g(g+1) = g^2 + g \\
g^5 = g(g^4) = g(g^2+g) = g^3 + g^2 = g^2 + g + 1 \\
g^6 = g(g^5) = g(g^2+g+1) = g^3 + g^2 + g = g^2 + 1 \\
g^7 = g(g^6) = g(g^2+1) = g^3 + g = 1
\end{gathered}$$

Kak again:

> Since every polynomial in $GF(2^n)$ is represented by a power of $g$, multiplying any two polynomials in $GF(2^n)$ becomes trivial  we just have to add the exponents of $g$ modulo ($2^n$ minus 1). .. using the generator notation allows the multiplications of the elements of the finite field to be carried out without reference to the irreducible polynomial.

### Generator for GF(2e8)

For $GF(2^8)$, **0x03** $= 3$ is a generator.

**0x03 * 0x03 = 0011 * 0011 = 0110 $\oplus$ 0011 = 0101 = 0x05**

**0x03 * 0x05 = 1010 $\oplus$ 0101 = 1111 = 0x0f**

**0x03 * 0x0f = 0000 1111 $\oplus$ 0001 1110 = 0001 0001 = 0x11**

**0x03 * 0x11 = 0010 0010 $\oplus$ 0001 0001 = 0011 0011 = 0x33**

**0x03 * 0x33 = 0110 0110 $\oplus$ 0011 0011 = 0101 0101 = 0x55**

**0x55 * 0x11 = 1010 1010 $\oplus$ 0101 0101 = 1111 1111 = 0xff**

The next step is the first one to involve the modulus: The first term is the shifted **0xff**.

**0x03 * 0x11 = 1 1111 1110 $\oplus$ 1 0001 1011 = 1110 0101**

**1110 0101 $\oplus$ 1111 1111 = 0001 1010 = 0x1a**

Another way to do the last step

$$255 * 2 = 510, \qquad \bmod 256 = 254, \quad \oplus\ 27 = 229, \quad \oplus\ 255 = 26$$

Here is part of it. Somehow it comes around.

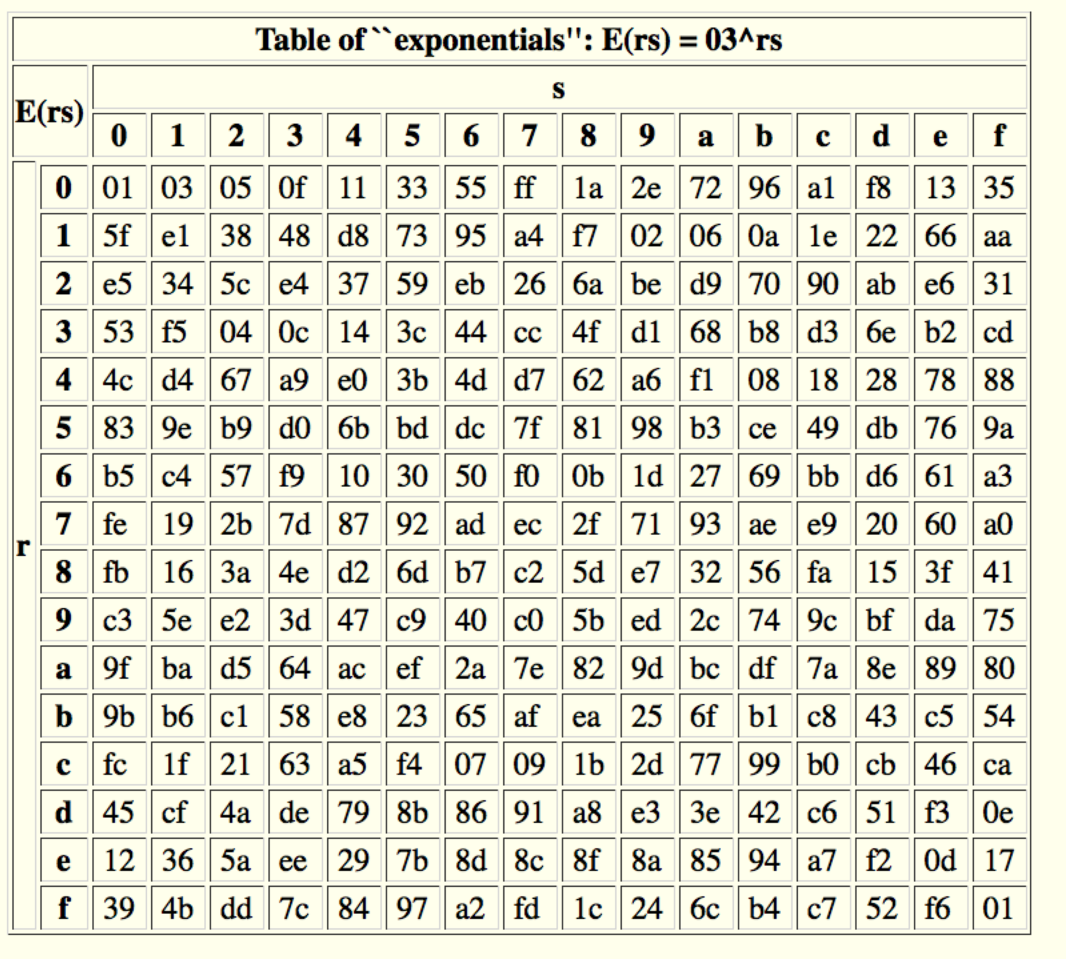


Table of ``exponentials'': E(rs) = 03^rs

| E(rs) | | s | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| r | 0 | 01 | 03 | 05 | 0f | 11 | 33 | 55 | ff | 1a | 2e | 72 | 96 | a1 | f8 | 13 | 35 |
| | 1 | 5f | e1 | 38 | 48 | d8 | 73 | 95 | a4 | f7 | 02 | 06 | 0a | 1e | 22 | 66 | aa |
| | 2 | e5 | 34 | 5c | e4 | 37 | 59 | eb | 26 | 6a | be | d9 | 70 | 90 | ab | e6 | 31 |
| | 3 | 53 | f5 | 04 | 0c | 14 | 3c | 44 | cc | 4f | d1 | 68 | b8 | d3 | 6e | b2 | cd |
| | 4 | 4c | d4 | 67 | a9 | e0 | 3b | 4d | d7 | 62 | a6 | f1 | 08 | 18 | 28 | 78 | 88 |
| | 5 | 83 | 9e | b9 | d0 | 6b | bd | dc | 7f | 81 | 98 | b3 | ce | 49 | db | 76 | 9a |
| | 6 | b5 | c4 | 57 | f9 | 10 | 30 | 50 | f0 | 0b | 1d | 27 | 69 | bb | d6 | 61 | a3 |
| | 7 | fe | 19 | 2b | 7d | 87 | 92 | ad | ec | 2f | 71 | 93 | ae | e9 | 20 | 60 | a0 |
| | 8 | fb | 16 | 3a | 4e | d2 | 6d | b7 | c2 | 5d | e7 | 32 | 56 | fa | 15 | 3f | 41 |
| | 9 | c3 | 5e | e2 | 3d | 47 | c9 | 40 | c0 | 5b | ed | 2c | 74 | 9c | bf | da | 75 |
| | a | 9f | ba | d5 | 64 | ac | ef | 2a | 7e | 82 | 9d | bc | df | 7a | 8e | 89 | 80 |
| | b | 9b | b6 | c1 | 58 | e8 | 23 | 65 | af | ea | 25 | 6f | b1 | c8 | 43 | c5 | 54 |
| | c | fc | 1f | 21 | 63 | a5 | f4 | 07 | 09 | 1b | 2d | 77 | 99 | b0 | cb | 46 | ca |
| | d | 45 | cf | 4a | de | 79 | 8b | 86 | 91 | a8 | e3 | 3e | 42 | c6 | 51 | f3 | 0e |
| | e | 12 | 36 | 5a | ee | 29 | 7b | 8d | 8c | 8f | 8a | 85 | 94 | a7 | f2 | 0d | 17 |
| | f | 39 | 4b | dd | 7c | 84 | 97 | a2 | fd | 1c | 24 | 6c | b4 | c7 | 52 | f6 | 01 |

There is a hard way and an easy way to use the table. The hard way is the following. Let's check the multiplication we did before: **0xb6** × **0x53**. The answer was **0x36**.

Scour through the table to find the entry that is equal to **0xb6** and find it indexed as the power **0xb1**. Similarly look up **0x53**, we find it indexed as the power **0x30**.

Multiply by adding the powers: **0xb1** + **0x30** = **0xe1** (Do the addition modulo 256 if necessary). Index into the table by the power **0xe1** and find **0x36** . That's the same answer we got before.

The easy way, of course, is to make another table, of logarithms. Take every pair **index, value** from the table of exponentials that we have, and switch it so the value becomes a new index and the index a new value. Use the new index and value to construct the table of logarithms. Just do the lookup for the first part of the method in the logarithms table.

### multiplicative inverse

As I mentioned in the previous chapter, I used Kak's method to find all 65536 possible products of the numbers in the field $GF(2^8)$. In the process I verified that for any product $p$ (except 0) and any factor $a$ there exists one and only one $b$ such that $a \times b = p$.

This is also true for $p = 1$. Every number has a multiplicative inverse.

If two numbers produce $p = 1$ when they are multiplied together, then their powers must add to give 255. (0 is not generated as any power of the generator, the list of powers repeats after 255 values).

If we look in the table of logarithms for **0x53** we find **0x30**, and if we look for **0xca** and find **0xcf**. Add them to obtain **0x30 + 0xcf = 0xff**. Look in the table of exponentials and see the **0xff** indeed corresponds to **0x01**.