**Inverses in the Field GF(2^8)**

Date: 11/07/2000 at 07:12:20

From: mmcl

Subject: Multiplicative Inverse in GF(2^8)

I have a 4x4 matrix of bytes:

[B0 B4 B8 B12]

[B1 B5 B9 B13]

[B2 B6 B10 B14]

[B3 B7 B11 B15]

I need to get the multiplicative inverse of this matrix in GF(2^8). Is

this the same as obtaining the inverse of a 4x4 matrix?

Date: 11/07/2000 at 13:40:17

From: Doctor Rob

Subject: Re: Multiplicative Inverse in GF(2^8)

Thanks for writing to Ask Dr. Math.

It is just the same, as long as you do all your arithmetic in GF(2^8).

Your first job is to figure out the map that carries bytes into field

elements, and vice versa. Map the byte matrix into a field element

matrix, do the inversion, then map the result back into bytes.

- Doctor Rob, The Math Forum

<http://mathforum.org/dr.math/>

Date: 11/09/2000 at 05:45:07

From: Maire McLoone

Subject: Re: Multiplicative Inverse in GF(2^8)

I would like to obtain the multiplicative inverse of each individual

byte in GF(2^8). How do I do this?

Date: 11/09/2000 at 11:28:45

From: Doctor Rob

Subject: Re: Multiplicative Inverse in GF(2^8)

Thanks for writing back.

The field GF(2^8) is usually defined in the following way. Find a

polynomial f(x) of degree 8 which is irreducible over GF(2). There are

30 of these to choose from. Then the polynomials of degree less than 8

over GF(2) form a set of size 2^8.

"Addition" is the usual addition of polynomials (reducing coefficients

modulo 2), and "multiplication" is the usual multiplication of

polynomials (reducing coefficients modulo 2), followed by a reduction

modulo f(x) (and further coefficient reduction modulo 2) until the

result has degree less than 8. Using these operations, this set forms

a field isomorphic to GF(2^8).

For example, suppose the polynomial were

f(x) = x^8 + x^6 + x^5 + x + 1

which is irreducible over GF(2). Then to add x^7 + x^3 + x + 1 and

x^4 + 1, you would get x^7 + x^4 + x^3 + x + 2, and reducing the

coefficients modulo 2, you get x^7 + x^4 + x^3 + x, which is the sum.

To multiply these same polynomials, you get:

x^11 + 2\*x^7 + x^5 + x^4 + x^3 + x + 1

-> x^11 + x^5 + x^4 + x^3 + x + 1

-> x^7 + x^2 + x

which is the product.

Now suppose one of the entries in your matrix is the byte 11001001.

You have to figure out whether this means

x^7 + x^6 + x^3 + 1

(so the bits from left to right are the coefficients of the powers of

x in decreasing order) or

x^7 + x^4 + x + 1

(so the bits from left to right are the coefficients of the powers of

x in increasing order). Then you have to determine what polynomial

f(x) is being used to do the arithmetic. Once you know these data, you

can construct the multiplicative inverses you seek in the following

way.

First figure out what polynomial a(x) the byte you want to invert is

equivalent to.

Given a polynomial a(x) whose inverse you seek, perform the Extended

Euclidean Algorithm on a(x) and f(x). If a(x) is not zero, you will

obtain polynomials r(x) and s(x) such that

r(x)\*a(x) + s(x)\*f(x) = 1

Then reduce this equation modulo f(x):

r(x)\*a(x) = 1 (mod f(x))

a(x) will be the multiplicative inverse of r(x).

Example: Inverse of x^4 + 1.

x^8 + x^6 + x^5 + x + 1 = (x^4+x^2+x+1)\*(x^4+1) + (x^2)

x^4 + 1 = (x^2)\*(x^2) + 1

and, working backwards,

1 = 1\*(x^4+1) + (x^2)\*(x^2)

= 1\*(x^4+1) + (x^2)\*([x^4+x^2+x+1]\*[x^4+1]+[x^8+x^6+x^5+x+1])

= (x^6+x^4+x^3+x^2+1)\*(x^4+1) + (x^2)\*(x^8+x^6+x^5+x+1)

so, reducing modulo f(x),

1 = (x^6+x^4+x^3+x^2+1)\*(x^4+1) (mod f(x))

Thus the multiplicative inverse sought is x^6 + x^4 + x^3 + x^2 + 1.

You can remove the need to work backwards by keeping track of some

auxiliary quantities as you perform the Euclidean Algorithm.

Remainder Quotient Auxiliary

x^8+x^6+x^5+x+1 0

x^4+1 1

x^2 x^4+x^2+x+1 x^4+x^2+x+1

1 x^2 x^6+x^4+x^3+x^2+1

The Auxiliary column always starts with 0 and 1. The Remainder column

always starts with f(x) and a(x). To fill in any subsequent row,

divide the remainders in the previous two rows, and put the quotient

in the Quotient column and the remainder in the Remainder column. Then

multiply the quotient times the Auxiliary number in the previous row

and add the Auxiliary number in the row before that, putting the

result in the Auxiliary column. When the remainder is reduced to 1,

the content of the Auxiliary column in that row is the inverse of

a(x). This is a version of the Extended Euclidean Algorithm which you

can use to advantage here.

Of course, once you have the inverse, you have to convert that

polynomial back to a byte.

- Doctor Rob, The Math Forum

<http://mathforum.org/dr.math/>