Data and Network Security

Course Code: IT-4542

Polynomial Arithmetic

111: $x^2 + x + 1 = 1.x^2 + 1.x^1 + 1.x^0$

101: $x^2 + 1 = 1.x^2 + 0.x^1 + 1.x^0$

011: $0.x^2 + 1.x^1 + 1.x^0$

This ploy of representing a bit pattern with a polynomial will allow us to create a finite field with bit patterns.

In general,

$$a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0$$

Coefficients $a_0, a_1, \ldots, a_n$ are drawn from some designated set S. S is called the coefficient set.

When an $a_n \neq 0$, we have a polynomial of degree n.

Polynomial Arithmetic

- A zeroth-degree polynomial is called a constant polynomial.
- Polynomial arithmetic deals with the addition, subtraction, multiplication, and division of polynomials.
- Note that we have no interest in evaluating the value of a polynomial for any value of the variable x.

Arithmetic Operations on Polynomials

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_1x + b_0 \\ f(x) + g(x) &= a_2x^2 + (a_1 + b_1)x + (a_0 + b_0) \end{aligned}$$

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_3x^3 + b_0 \\ f(x) - g(x) &= -b_3x^3 + a_2x^2 + a_1x + (a_0 - b_0) \end{aligned}$$

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_1x + b_0 \\ f(x) \times g(x) &= a_2b_1x^3 + (a_2b_0 + a_1b_1)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0 \end{aligned}$$

Arithmetic Operations on Polynomials

$$\begin{aligned} f(x) &= a_2x^2 + a_1x + a_0 \\ g(x) &= b_1x + b_0 \\ f(x) \,/\, g(x) &= ? \end{aligned}$$

Let's say we want to divide the polynomial $8x^2 + 3x + 2$ by the polynomial $2x + 1$:

$$\frac{8x^2 + 3x + 2}{2x + 1} = 4x - 0.5 + \frac{2.5}{2x + 1}$$

Arithmetic Operations on Polynomials Whose Coefficients Belong to a Finite Field

Let's consider the set of all polynomials whose coefficients belong to the finite field Z_7

Z_7:	0	1	2	3	4	5	6
AI:	0	6	5	4	3	2	1
MI:	–	1	4	5	2	3	6

$$
\begin{aligned}
f(x) &= 5x^2 + 4x + 6 \\
g(x) &= 2x + 1 \\
f(x) + g(x) &= 5x^2 + 6x
\end{aligned}
$$

$$
\begin{aligned}
f(x) &= 5x^2 + 4x + 6 \\
g(x) &= 2x + 1 \\
f(x) - g(x) &= 5x^2 + 2x + 5
\end{aligned}
$$

$$
\begin{aligned}
f(x) &= 5x^2 + 4x + 6 \\
g(x) &= 2x + 1 \\
f(x) \times g(x) &= 3x^3 + 6x^2 + 2x + 6
\end{aligned}
$$

$$
\begin{aligned}
f(x) &= 5x^2 + 4x + 6 \\
g(x) &= 2x + 1 \\
f(x) \,/\, g(x) &= 6x + 6 \\
5x^2 + 4x + 6 &= (2x + 1) \times (6x + 6)
\end{aligned}
$$

Dividing Polynomials Defined Over a Finite Field

We say that a polynomial is defined over a field (polynomial over a field) if all its coefficients are drawn from the field.

Let's now consider polynomials defined over $GF(2)$ or $Z_2 = \{0, 1\}$. Note that the 2 is the first prime.

Note: addition is XOR, multiply is AND

0	+	0	=	0	0	X	0	=	0	0	−	0	=	0					
0	+	1	=	1	0	X	1	=	0	1	−	0	=	1					
1	+	0	=	1	1	X	0	=	0	0	−	1	=	0	+	1	=	1
1	+	1	=	0	1	X	1	=	1	1	−	1	=	1	+	1	=	0

Arithmetic Operations On Polynomials Over $GF(2)$

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

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

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

Arithmetic Operations On Polynomials Over $GF(2)$

$$
\begin{aligned}
f(x) &= x^2 + x + 1 \\
g(x) &= x + 1 \\
f(x) \ / \ g(x) &= x + \frac{1}{x + 1}
\end{aligned}
$$

Polynomials Over a Field Constitute a Ring

- The group operator is polynomial addition. Z_p
- The polynomial 0 is the identity element with respect to polynomial addition.
- Polynomial addition is associative and commutative.
- The set of all polynomials over a given field is closed under polynomial addition.
- Polynomial multiplication distributes over polynomial addition.
- Polynomial multiplication is associative.

Therefore, the set of all polynomials over a field constitutes a ring. Such a ring is also called the polynomial ring.

Polynomials Over a Field Constitute a Ring

- Since polynomial multiplication is commutative, the set of polynomials over a field is actually a commutative ring.
- In general, for polynomials defined over a field, the division of a polynomial $f(x)$ of degree m by another polynomial $g(x)$ of degree $n \leq m$ can be expressed by

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

$$f(x) = q(x)g(x) + r(x)$$

- When $r(x)$ is zero, we say that $g(x)$ divides $f(x)$ that is $g(x)|f(x)$.

Irreducible Polynomials – Prime Polynomials

- When $g(x)$ divides $f(x)$ without leaving a remainder, we say $g(x)$ is a factor of $f(x)$.

- A polynomial $f(x)$ over a field F is called irreducible if $f(x)$ cannot be expressed as a product of two polynomials, both over F and both of degree lower than that of $f(x)$.

- An irreducible polynomial is also referred to as a prime polynomial.

Example of Modular Polynomial Arithmetic in GF(2^3)

$$(x^2 + x + 1) \times (x^2 + 1) \ mod \ (x^3 + x + 1)$$

$$\begin{aligned} &= (x^4 + x^3 + x^2) + (x^2 + x + 1) \ mod \ (x^3 + x + 1) \\ &= (x^4 + x^3 + x + 1) \ mod \ (x^3 + x + 1) \\ &= -x^2 - x \\ &= x^2 + x \end{aligned}$$

$$\frac{(x^4 + x^3 + x + 1)}{(x^3 + x + 1)} = x + 1 + \frac{-x^2 - x}{x^3 + x + 1}$$

How large is the set of polynomials when multiplications are carried out modulo $x^3 + x + 1$?

With multiplications modulo $x^3 + x + 1$, we have only the following eight polynomials in the set of polynomials over GF(2^3):

0

1

x

x^2

$x + 1$

$x^2 + 1$

$x^2 + x$

$x^2 + x + 1$

How large is the set of polynomials when multiplications are carried out modulo $x^3 + x + 1$?

this set as $GF(2^3)$ where the exponent of 2 (which in this case is 3) is the degree of the modulus polynomial.

$GF(2^3)$ is a Finite Field?

- $GF(2^3)$ is an abelian group under the operation of polynomial addition.
- $GF(2^3)$ is also a commutative ring.
- $GF(2^3)$ is an integral domain because of the fact that the set contains the multiplicative identity element 1 and because if for $a \in GF(2^3)$ and $b \in GF(2^3)$ we have

  $a \times b = 0 \bmod (x^3 + x + 1)$

  then either $a = 0$ or $b = 0$.

- $GF(2^3)$ is a finite field because it is a finite set and because it contains a unique multiplicative inverse for every non-zero element.

$GF(2^3)$ is a Finite Field?

- $GF(2^3)$ contains a unique multiplicative inverse for every non-zero element.
- Therefore, $GF(2^3)$ is a finite field.
- $GF(2^n)$ is a finite field for every n.
- AES arithmetic is based on $GF(2^8)$. It uses the following irreducible polynomial

$$x^8 + x^4 + x^3 + x + 1$$

- AES obviously contains 256 distinct polynomials.

Representing the Individual Polynomials in $GF(2^n)$ by Binary Code Words

- Think of the polynomials as bit strings

$$
\begin{aligned}
0 &\Rightarrow 000 \\
1 &\Rightarrow 001 \\
x &\Rightarrow 010 \\
x^2 &\Rightarrow 100 \\
x+1 &\Rightarrow 011 \\
x^2+1 &\Rightarrow 101 \\
x^2+x &\Rightarrow 110 \\
x^2+x+1 &\Rightarrow 111
\end{aligned}
$$

$GF(2^n)$:

Addition is XOR

The bitwise operations needed to directly multiply two bit patterns are specific to the irreducible polynomial that defines a given $GF(2^n)$.

$$5 + 13 = 0000\ 0101 + 0000\ 1101 = 0000\ 1000 = 8$$
$$76 + 22 = 0100\ 1100 + 0001\ 0110 = 0101\ 1010 = 90$$
$$7 - 3 = 0000\ 0111 - 0000\ 0011 = 0000\ 0100 = 4$$
$$7 + 3 = 0000\ 0111 + 0000\ 0011 = 0000\ 0100 = 4$$

- Subtraction is the same as addition in GF(2^8).

  [Each "number" is its own additive inverse in GF(2^8).]
- The order of a finite field refers to the number of elements in the field. So the order of GF(2^n) is 2^n.

Direct Bitwise Operations for Multiplications in $GF(2^8)$

- In AES, this field is derived using the following irreducible polynomial of degree 8:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

- Note: in GF(2^8):

$$x^8 \bmod m(x) = x^4 + x^3 + x + 1$$

$$f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

$$f(x)\times x = b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x$$

$$
\begin{aligned}
& (f(x) \times x) \ \ mod \ \ m(x) \\
= \ & (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \ mod \ m(x) \\
= \ & (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \quad + \quad (x^8 \ mod \ m(x)) \\
= \ & (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + (x^4 + x^3 + x \ + 1) \\
= \ & (b_6b_5b_4b_3b_2b_1b_00) \quad \otimes \quad (00011011)
\end{aligned}
$$

Summary of How a Multiplication is Carried out in GF(2^8)

- Multiply B with 00000001: do nothing
- Multiply B with 00000010:
  - If B's MSB is 0: left shift B by 1 bit
  - If B's MSB is 1: left shift B by 1 bit then XOR it with 00011011
- Multiply B with 00000100: do the above twice and so on
- Example:

$B \times 10000011$

$= B \times (00000001 + 00000010 + 10000000)$

$= (B \times 00000001) + (B \times 00000010) + (B \times 10000000)$

$= (B \times 00000001) \otimes (B \times 00000010) \otimes (B \times 10000000)$

Multiplicative Inverses in GF(2^8)

- 10000000 mod 100011011 = 10000011
- 10010101 mod 100011011 = 10001010

Multiplicative Inverses in GF(2^3)

	Additive Inverse	Multiplicative Inverse
000	000	-----
001	001	001
010	010	101
011	011	110
100	100	111
101	101	010
110	110	011
111	111	100

Irreducible polynomial $x^3 + x + 1$

Using a Generator to Represent the Elements of GF(2^n)

- If g is a generator element, then every element of $GF(2^n)$, except for the 0 element, can be expressed as some power of g.
- Example: for $GF(2^3)$, Irreducible polynomial $x^3 + x + 1$

$$g^3 + g + 1 = 0$$

$$g^3 = -g - 1 = g + 1$$

$$0$$

$$\begin{aligned} g^0 &= 1 \\ g^1 &= g \\ g^2 &= g^2 \\ g^3 &= g + 1 \end{aligned}$$

$$
\begin{aligned}
g^4 &= g(g^3) = g(g+1) &&= g^2 + g \\
g^5 &= g(g^4) = g(g^2+g) = g^3 + g^2 &&= g^2 + g + 1 \\
g^6 &= g(g^5) = g(g^2+g+1) = g^3 + g^2 + g &&= g^2 + 1 \\
\\
g^7 &= g(g^6) = g(g^2+1) = g^3 + g &&= 1 \\
&\vdots
\end{aligned}
$$

- Note: the powers g^0 through g^6 of the generator element, along with the element 0, correspond to the eight polynomials of GF(2^3) [note $g = x$]
- The higher powers of g obey the relationship $g^k = g^{k \bmod 7}$
- 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 ($2^n - 1$).

If g is the generator element of a finite field of the form GF(2^n), then all the powers of g from g^0 through $g^{2\wedge(n)-2}$, along with the element 0, correspond to the elements of the finite field.

Using the generator notation allows the multiplications of the elements of the finite field to be carried out without reference to the irreducible polynomial.