4.2.6. Вычисление в поле Галуа

Напомним некоторые определения из алгебраических основ:

Поле F_p – это множество p элементов, на котором определены операции сложения и умножения, обладающие свойствами коммуникативности, ассоциативности и дистрибутивности, при этом относительно этих двух операций существуют нейтральные элементы и $\forall a$ существует обратный элемент относительно операции сложения, $\forall b \neq 0$ существует обратный элемент относительно операции умножения.

Пусть $f(\lambda)$ – неприводимый многочлен над полем F, для него существует конечное расширение поля F, содержащее все корни многочлена $f(\lambda)$ – поле разложения.

Группа – это непустое множество G с алгебраической операцией * на нем, для которой выполняются аксиомы:

1. Операция * ассоциативна $\forall a,b,c \in G: a*(b*c)=(a*b)*c$.
2. В G $\exists e$ единичный элемент такой, что $\forall a \in G: a*e=e*a=a$.
3. $\forall a \in G\ \exists a^{-1} \in G: a * a^{-1} = a^{-1} * a = e$.

Если дополнительно группа удовлетворяет аксиоме:

4. $\forall a,b \in G: a * b = b * a$.

То это абелева (коммуникативная) группа.

Кольцом называется множество R с двумя бинарными операциями $(+,\cdot)$ такими, что:

1. R – абелева группа относительно операции $+$.
2. Операция умножения ассоциативна: $\forall a, b, c \in R: (ab)c = a(bc)$;
3. Выполняется закон дистрибутивности $\forall a,b,c \in R: a(b+c)=cb+ac$.

Кольцо классов вычетов Z_p называется полем Галуа порядка p и обозначается $GF(p)$ (где p – простое). В поле Галуа определены операции $+,-,*,/$.

Теорема 1.

Поле Галуа $GF\left(p^n\right)$ есть поле разложения всякого неприводимого многочлена $f(\lambda)$ степени n над полем $F_p = GF(p)$.

Арифметика поля Галуа широко используется в криптографии. Данное поле содержит только числа конечного размера, при делении отсутствуют ошибки округления. Многие криптосистемы основаны на $GF(p)$, где p – большое простое число.

Криптографы также используют арифметику по модулю неприводимых многочленов степени n, коэффициентами которых являются целые числа по модулю q, где q – простое число. Эти поля называются $GF(q^n)$.

Пример (байтовые операции)

Рассмотрим поле Галуа $GF(2^8)$. Оно может интерпретироваться как работа с битами одного байта, который будет рассматриваться как элемент этого конечного поля с бинарными операциями: $\oplus, \cdot$.

Сложение: $\oplus$ – это поразрядное суммирование по модулю 2.

Умножение – это умножение полиномов, соответствующих байтам, но по модулю неприводимого двоичного полинома $m(x) = x^8 + x^4 + x^3 + x + 1$ ($11B_{16}$).

Элемент этого поля может быть представлен в полиномиальном виде:

$b(x) = b_7 x^7 + ... + b_1 x + b_0$, где b_i – i-ый бит байта b.

Например: $b = 87_{10} = 1010111_2$, тогда $b(x) = x^6 + x^4 + x^2 + x + 1$.

Сложение: $(87+131)_{10} = (x^6 + x^4 + x^2 + x + 1) \oplus (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$.

Умножение: умножение на x эквивалентно побитовому сдвигу влево на один бит. Операция умножения $b(x) \cdot x$ с последующим приведением по модулю полинома $m(x)$ обозначается $xtime(b)$. Умножение на x^i эквивалентно побитовому сдвигу влево на i бит и равносильна k-кратной композиции $xtime(b)$.

$(87 \cdot 19)_{10} = (x^6 + x^4 + x^2 + x + 1) \cdot (x^4 + x + 1)$

Умножаем $(x^6 + x^4 + x^2 + x + 1)$ на $1 = x^0$, то есть сдвигаем на 0 бит, получаем: $(x^6 + x^4 + x^2 + x + 1)$.

Умножаем $(x^6 + x^4 + x^2 + x + 1)$ на $x = x^1$, то есть сдвигаем на 1 бит, получаем: $(x^7 + x^5 + x^3 + x^2 + x)$.

Чтобы умножить $(x^6 + x^4 + x^2 + x + 1)$ на x^4 надо произвести умножение на $x^0 \div x^4$, и результат сложить. Поэтому:

Умножаем $(x^7 + x^5 + x^3 + x^2 + x)$ на x: $(x^8 + x^6 + x^4 + x^3 + x^2)$, приводим по $m(x) = x^8 + x^4 + x^3 + x + 1$ и получаем: $(x^6 + x^2 + x + 1)$.

Умножаем $(x^6 + x^2 + x + 1)$ на x: $(x^7 + x^3 + x^2 + x)$.

Умножаем $(x^7 + x^3 + x^2 + x)$ на x: $(x^8 + x^4 + x^3 + x^2)$, приводим по $m(x) = x^8 + x^4 + x^3 + x + 1$ и получаем: $(x^2 + x + 1)$.

В итоге получаем:

$$(87 \cdot 19)_{10} = (x^6 + x^4 + x^2 + x + 1) \cdot (x^4 + x + 1) =$$
$$= (x^2 + x + 1) \oplus (x^7 + x^5 + x^3 + x^2 + x) \oplus (x^6 + x^4 + x^2 + x + 1) =$$
$$= x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x.$$

Другой способ умножения:

$$(87\cdot 19)_{10} = \left(x^6 + x^4 + x^2 + x + 1\right)\cdot\left(x^4 + x + 1\right) = x^{10} + x^8 + x^6 + x^5 + x^4 + \\ + x^7 + x^5 + x^3 + x^2 + x + \\ + x^6 + x^4 + x^2 + x + 1 = \\ = x^{10} + x^8 + x^7 + x^3 + 1.$$

Полученный результат приводим по модулю $m(x) = x^8 + x^4 + x^3 + x + 1$:

$$x^{10} + x^8 + x^7 + x^3 + 1 \mod (x^8 + x^4 + x^3 + x + 1) = \\ = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$$

Следовательно, $(87\cdot 19)_{10} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$.

<u>И ещё один способ умножения</u>:

Представляем 87 и 19 в двоичном виде: $(87)_{10} = (1010111)_2$, $(19)_{10} = (10011)_2$. Представляем 19 в виде $(19)_{10} = (10011)_2 = (10000)_2 \oplus (00010)_2 \oplus (00001)_2$. Тогда

$$(87\cdot 19)_{10} = (1010111)_2 \cdot (10000)_2 \oplus (1010111)_2 \cdot (00010)_2 \oplus (1010111)_2 \cdot (00001)_2.$$

Для удобства перейдём к записи в столбик:

```
  1010111 0000      ← это (1010111)2 · (10000)2
⊕  000 1010111 0    ← это (1010111)2 · (00010)2
⊕  0000 1010111     ← это (1010111)2 · (00001)2
   10110001001      ← это (1010111)2 · (10011)2
```

Обозначим соответствующий полученному результату полином за $s_0(x)$: $s_0(x) = x^{10} + x^8 + x^7 + x^3 + 1$. Пусть *maxdegree* ($p(x)$) – максимальная степень полинома $p(x)$. Тогда *maxdegree* ($s_0(x)$) = 10, *maxdegree* ($m(x)$) = 8.

Т.к. *maxdegree* ($s_0(x)$) ≥ *maxdegree* ($m(x)$), то теперь полученный результат нужно привести по модулю $m(x) = x^8 + x^4 + x^3 + x + 1$. Для этого складываем по модулю 2 полученный результат с полиномом $m(x)$, умноженным на x^k, где k = *maxdegree* ($s_0(x)$) – *maxdegree* ($m(x)$) = 10 – 8 = 2:

```
   10110001001
⊕  100011011 00     ← это m(x) · x^2 = (100011011)2 · (100)2
   00111100101
```

Обозначим соответствующий полученному результату полином за $s_1(x)$: $s_1(x) = x^8 + x^7 + x^6 + x^5 + x^2 + 1$

Т.к. снова *maxdegree* ($s_1(x)$) ≥ *maxdegree* ($m(x)$), то выполняем аналогичное сложение с полиномом $m(x)$, умноженным на x^0:

```
   111100101
⊕  100011011        ← это m(x) · x^0 = (100011011)2 · (1)2
   011111110
```

Теперь получили полином $s_2(x)$: $s_2(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$. Для него *maxdegree* ($s_2(x)$) < *maxdegree* ($m(x)$), поэтому $s_2(x)$ является результатом умножения 87_{10} на 19_{10}:

$(87\cdot 19)_{10} = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$. •

Пример (операции с 4-байтовыми векторами)

Любой многочлен принадлежащий $GF(2^8)$ степени не больше 3 может быть представлен 4-х байтовым вектором.

Сложение 4-х байтовых векторов производится $\oplus$ побитово.

Умножение: с последующим приведением по модулю полинома $M(x) = x^4 + 1$.

Пусть дано два многочлена: $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, $b(x) = b_3x^3 + b_2x^2 + b_1x + b_0$. Их произведение равно $c(x) = c_6x^6 + ... + c_1x + c_0$, где:

$$c_0 = a_0 \cdot b_0$$
$$c_1 = a_1 \cdot b_0 \oplus a_0 \cdot b_1$$
$$c_2 = a_2 \cdot b_0 \oplus a_1 \cdot b_1 \oplus a_0 \cdot b_2$$
$$c_3 = a_3 \cdot b_0 \oplus a_2 \cdot b_1 \oplus a_1 \cdot b_2 \oplus a_0 \cdot b_3$$
$$c_4 = a_3 \cdot b_1 \oplus a_2 \cdot b_2 \oplus a_1 \cdot b_3$$
$$c_5 = a_3 \cdot b_2 \oplus a_2 \cdot b_3$$
$$c_6 = a_3 \cdot b_3$$

Далее приводим $c(x)$ по модулю $M(x)$ и окончательно получаем, что если $d(x) = a(x) \otimes b(x)$, то:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

Примерами алгоритмов шифрования, основанных на вычисление в поле Галуа является RIJNDAEL (AES), A5/1.