Строение конечных полей

Задача 1.

Для алгоритма шифрования AES преобразовать байт 01100101 в обратный с помощью поля $GF(2^8)$, построенное на основе неприводимого многочлена $x^8 + x^4 + x^3 + x + 1$.

Решение 1.

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

$$01100101 \longrightarrow x^6 + x^5 + x^2 + 1 = g(x)$$

$$\begin{array}{l|l}
x^8+x^4+x^3\ +x\ +1 & x^6+x^5+x^2+1 \\
\underline{x^8+x^7+x^4+x^2} & x^2+x+1 \\
\quad x^7+x^3+x^2\ +x+1 & \\
\quad \underline{x^7+x^6+x^3\ +x} & \\
\qquad x^6+x^2\ +1 & \\
\qquad \underline{x^6+x^5+x^2+1} & \\
\qquad\quad x^5 &
\end{array}
\qquad
\begin{array}{l|l}
x^6+x^5+x^2+1 & x^5 \\
\underline{x^6} & x+1 \\
\quad x^5+x^2+1 & \\
\quad \underline{x^5} & \\
\qquad x^2+1 &
\end{array}$$

$$\begin{array}{l|l}
x^5 & x^2+1 \\
\underline{x^5+x^3} & x^3+x \\
\quad x^3 & \\
\quad \underline{x^3+x} & \\
\qquad x &
\end{array}
\qquad
\begin{array}{l|l}
x^2+1 & x \\
\underline{x^2} & x \\
\quad 1 &
\end{array}$$

$$1 = x^2+1+x\cdot x = x^2+1+x(x^5+(x^2+1)(x^3+x)) = x\cdot x^5+(x^2+1)(x^4+x^2+1) = x\cdot x^5+(g(x)+x^5(x+1))(x^4+x^2+1) =$$

$$= g(x)(x^4+x^2+1) + x^5(x+1)(x^4+x^2+1) + x\cdot x^5 = g(x)(x^4+x^2+1) + x^5(x^5+x^4+x^3+x^2+1) =$$

$$= g(x)(x^4+x^2+1) + (f(x) + g(x)(x^2+x+1))(x^5+x^4+x^3+x^2+1) =$$

$$= f(x)(x^5+x^4+x^3+x^2+1) + g(x)(x^7+x^5+x^2+x)$$

$$\Downarrow$$

$$g(x)^{-1} = x^7 + x^5 + x^2 + x \longrightarrow 10100110$$

Задача 2.

Проверить, является ли факторкольцо $\mathbb{Z}_5[x]/\langle x^4+2x^2+3\rangle$ полем. Если да, то сколько в нём элементов? Если нет, показать, почему это не поле.

Решение 2. $\mathbb{Z}_5[x]/\langle x^4+2x^2+3\rangle$ – поле $\iff x^4+2x^2+3$ неприводимый над $\mathbb{Z}_5$.

Попробуем разложить в произведение многочленов первой и третей степени. Если раскладывается на многочлен первой степени, то есть корни.

- $x=0: \quad 0+0+3=3\neq 0$
- $x=1: \quad 1+2+3=1\neq 0$
- $x=2: \quad 16+8+3=1+3+3=7=2\neq 0$
- $x=3: \quad 3^4+2\cdot 3^2+3=(-2)^4+2\cdot(-2)^2+3=2\neq 0$
- $x=4: \quad 4^4+2\cdot 4^2+3=(-1)^4+2\cdot(-1)^2+3=1\neq 0$

Нет корней, значит не раскладывается произведение многочленов первой и третей степени. Остается проверить раскладывается ли x^4+2x^2+3 на произведение двух неприводимых многочленов второй степени. Пусть:

$$(ax^2+bx+c)(dx^2+ex+f)=x^4+2x^2+3$$

Б.О.О. положим $a=1$ (можно всегда вынести коэффициент из первого многочлена и занести во второй).

$$(x^2+bx+c)(dx^2+ex+f)=x^4+2x^2+3$$

$$dx^4+(e+bd)x^3+(f+eb+cd)x^2+(ce+bf)x+fc=x^4+2x^2+3$$

$$\begin{cases} d=1\\ e+bd=0\\ f+eb+cd=2\\ ce+bf=0\\ fc=3\end{cases}\iff\begin{cases} d=1\\ e+b=0\\ f+eb+c=2\\ ce+bf=0\\ fc=3\end{cases}\iff\begin{cases} d=1\\ e=-b=4b\\ f+4b^2+c=2\\ -bc+bf=0\\ fc=3\end{cases}\iff\begin{cases} d=1\\ e=4b\\ f+4b^2+c=2\\ b(f-c)=0\\ fc=3\end{cases}\iff$$

$$\iff\left[\begin{array}{l}\begin{cases} d=1\\ b=0\\ e=0\\ f+c=2\\ fc=3\end{cases}\\ \begin{cases} d=1\\ f=c\\ e=4b\\ 2c+4b^2=2\\ c^2=3\end{cases}\end{array}\right.\iff\left[\begin{array}{l}\begin{cases} d=1\\ b=0\\ e=0\\ f=2+4c\\ c(2+4c)=3\end{cases}\\ \begin{cases} d=1\\ f=c\\ e=4b\\ 2c+4b^2=2\\ c^2=3\end{cases}\end{array}\right.\iff\left[\begin{array}{l}\begin{cases} d=1\\ b=0\\ e=0\\ f=2+4c\\ c(1+2c)=4\end{cases}\\ \begin{cases} d=1\\ f=c\\ e=4b\\ 2c+4b^2=2\\ c^2=3\end{cases}\end{array}\right.\iff\left[\begin{array}{l}\begin{cases} d=1\\ b=0\\ e=0\\ f=2+4c\\ 2c^2+c+1=0\end{cases}\\ \begin{cases} d=1\\ f=c\\ e=4b\\ 2c+4b^2=2\\ c^2=3\end{cases}\end{array}\right.$$

Либо должно выполняться $2c^2 + c + 1 = 0$, либо $c^2 = 3$.

$2c^2 + c + 1 = 0 \iff b^2 - 4ac = 1 - 4 \cdot 2 \cdot 1 = 1 + 2 = 3$ – квадратичный вычет

То есть два варианта сводятся к вопросу, является ли 3 квадратичным вычетом по модулю 5.

Проверим по критерию Эйлера: $3^{\frac{5-1}{2}} = 3^2 = 9 = -1 \iff 3$ не квадратичный вычет по модулю 5.

Значит система не имеет решений, то есть $x^4 + 2x^2 + 3$ неприводимый над $\mathbb{Z}_5$.

$\mathbb{Z}_5[x]/\langle x^4 + 2x^2 + 3 \rangle$ – поле.