Емельянов Семён
Александрович

9303

930306

Вариант: 16

① а) Получите линейное представление НОД многочленов $f(x) = x^7 + x^4 + x^3 + x + 1$ и $g(x) = x^6 + x^4 + x + 1$ над полем $GF(2)$

б) Разложите $f(x)$ на неприводимые сомножители

② Пусть α - примитивной элемент поля $GF(25) \cong$
$\cong Z_5[x]/(x^2 + 4x + 2)$
Найдите $L(n)$ - решения уравнения $1 + \alpha^n = \alpha^{L(n)}$ для $n = 1, 8$ и 13

$V = g + n \pmod{111}$

$g = 10$ для 9303

1 a) $f(x) = x^7 + x^4 + x^3 + x + 1$

$g(x) = x^6 + x^4 + x + 1$

$$\begin{array}{l|l} x^7+x^4+x^3+x+1 & x^6+x^4+x+1 \\ \cline{2-2} x^7+x^5+x^2+x & x \\ \hline x^5+x^4+x^3+x^2+1 & \end{array}$$

$$\begin{array}{l|l} x^6+x^4+x+1 & x^5+x^4+x^3+x^2+1 \\ \cline{2-2} x^6+x^5+x^4+x^3+x & x+1 \\ \hline x^5+x^3+1 & \\ x^5+x^4+x^3+x^2+1 & \\ \hline \end{array}$$

$$\begin{array}{l|l} x^5+x^4+x^3+x^2+1 & x^4+x^2 \\ \cline{2-2} x^5+x^3 & x+1 \\ \hline x^4+x^2+1 & \\ -\ x^4+x^2 & \\ \hline \end{array}$$

$$\begin{array}{l|l} x^4+x^2 & 1 \\ \cline{2-2} -\ x^4+x^2 & x^4+x^2 \\ \hline 0 & \end{array}$$

$f(x) \cdot U(x) + g(x) V(x) = d(x)$

$$\begin{cases} f(x) = g(x)\, q_1 + r_1 \\ g(x) = r_1 \cdot q_2 + r_2 \\ r_1 = r_2 \cdot q_3 + r_3 \\ r_2 = r_3 q_4 + r_4 \end{cases}$$

$r_3 = d = r_1 - r_2 q_3$

$r_1 = f(x) - g(x) q_1$

$r_2 = g(x) - r_1 q_2 = g(x) - q_2 (f(x) - g(x) q_1)$

$d = f(x) - g(x) q_1 - q_3 (g(x) - q_2 (f(x) - g(x) q_1)) =$

$= f(x) (1 + q_3 q_2) + g(x) (-q_1 - q_3 - q_1 q_2 q_3)$

$f(x) (1 + (x+1)^2) + g(x) (-x - x - 1 - x(x+1)^2) =$

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

Ответ: $f(x) \cdot x^2 + g(x)(1 + x + x^3)$

б) $f(x) = x^7+x^4+x^3+x+1$

$$
\begin{array}{r|l}
x^7+x^4+x^3+x+1 & x^3+x^2+1 \\
\cline{2-2}
-\ x^7+x^6+x^4 \qquad\qquad & x^4+x^3+x^2+x+1 \\
\hline
x^6+x^3+x+1 & \\
-\ x^6+x^5+x^3 \qquad\quad & \\
\hline
x^5+x+1 & \\
-\ x^5+x^4+x^2 \qquad & \\
\hline
x^4+x^2+x+1 & \\
-\ x^4+x^3+x \qquad & \\
\hline
x^3+x^2+1 & \\
-\ x^3+x^2+1 & \\
\hline
0 &
\end{array}
$$

1

Неприворимый многочлен, но если не строить таблицу для неприворимого многочленов, то можно разделить данный многочлен на неприворимый многочлен старшая степень которого равна 2, убедиться, что при делении останется остаток следовательно, многочлен неприворимый

Неприворимые многочлены

$n=1$ x, $x+1$

$n=2$ x^2+x+1

$n=3$ x^3+x^2+1

x^3+x+1

$n=4$ $x^4+x^3+x^2+x+1$

x^4+x^3+1

x^4+x+1

Ответ: $(x^3+x^2+1)(x^4+x^3+x^2+x+1)$

② $GF(25) = Z_5[x]/(x^2+4x+2)$

$\alpha^0 = 1$

$\alpha = x$

$\alpha^2 = -4x-2 = x+3$

$\alpha^3 = x^2+3x = x+3+3x = 4x+3$

$\alpha^4 = 4x^2+3x = 4(x+3)+3x = 4x+12+3x = 2x+2$

$\alpha^5 = 2x^2+2x = 2(x+3)+2x = 2x+6+2x = 4x+1$

$\alpha^6 = 4x^2+x = 4(x+3)+x = 4x+12+x = 2$

$\alpha^7 = 2x$

$\alpha^8 = 2x^2 = 2(x+3) = 2x+1$

$\alpha^9 = 2x^2+x = 2(x+3)+x = 2x+6+x = 3x+1$

$\alpha^{10} = 3x^2+x = 3(x+3)+x = 3x+9+x = 4x+4$

$\alpha^{11} = 4(x+3)+4x = 4x+12+4x = 3x+2$

$\alpha^{12} = 3(x+3)+2x = 3x+9+2x = 4$

$\alpha^{13} = 4x$

$\alpha^{14} = 4(x+3) = 4x+2$

$\alpha^{15} = 4(x+3)+2x = 4x+12+2x = x+2$

$\alpha^{16} = x+3+2x = 3x+3$

$\alpha^{17} = 3(x+3)+3x = 3x+9+3x = x+4$

$\alpha^{18} = (x+3)+4x = 3$

$\alpha^{19} = 3x$

$\alpha^{20} = 3(3+x) = 9+3x = 3x+4$

$\alpha^{21} = 3(3+x)+4x = 9+3x+4x = 7x+9 = 2x+4$

$\alpha^{22} = 2(x+3)+4x = 2x+6+4x = x+1$

$\alpha^{23} = (x+3)+x = 2x+3$

$\alpha^{24} = 2(x+3)+3x = 1$

$1+\alpha^0 = 2 = \alpha^6$

$1+\alpha^1 = x+1 = \alpha^{22}$

$1+\alpha^2 = x+4 = \alpha^{17}$

$1+\alpha^3 = 4x+4 = \alpha^{10}$

$1+\alpha^4 = 2x+3 = \alpha^{23}$

$1+\alpha^5 = 4x+2 = \alpha^{14}$

$1+\alpha^6 = 3 = \alpha^{18}$

$1+\alpha^7 = 2x+1 = \alpha^8$

$1+\alpha^8 = 2x+2 = \alpha^4$

$1+\alpha^9 = 3x+2 = \alpha^{11}$

$1+\alpha^{10} = 1+4x+4 = 4x = \alpha^{13}$

$1+\alpha^{11} = 3x+3 = \alpha^{16}$

$1+\alpha^{12} = 0 = -\infty$

$1+\alpha^{13} = 4x+1 = \alpha^5$

$1+\alpha^{14} = 4x+3 = \alpha^3$

$1+\alpha^{15} = x+3 = \alpha^2$

$1+\alpha^{16} = 3x+4 = \alpha^{20}$

$1+\alpha^{17} = x = \alpha^1$

$1+\alpha^{18} = 4 = \alpha^{12}$

$1+\alpha^{19} = 3x+1 = \alpha^9$

$1+\alpha^{20} = 3x = \alpha^{19}$

$1+\alpha^{21} = 2x = \alpha^7$

$1+\alpha^{22} = x+2 = \alpha^{15}$

$1+\alpha^{23} = 2x+4 = \alpha^{21}$

n	1	8	13
L(n)	22	4	5

Ответ