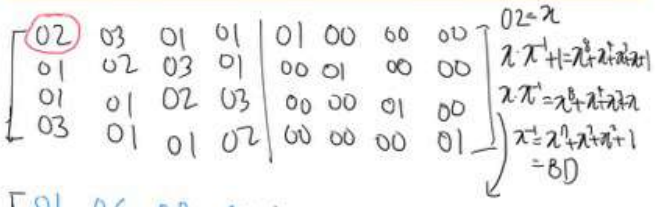
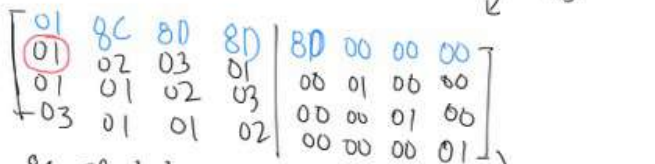
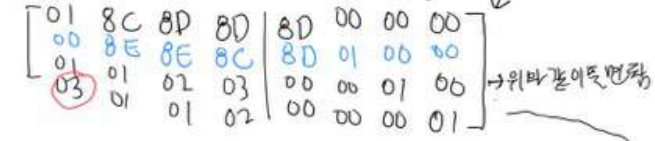
역행렬 구하기 -20192233 백건철





8C = x⁷+x³+x², 8C−02 = x⁷+x³+x²+x = 8E
8D = x⁷+x³+x²+1 8D−03 = x⁷+x³+x²+x = 8E
8D−01 = x⁷+x³+x² = 8C



→위와 같이 변형

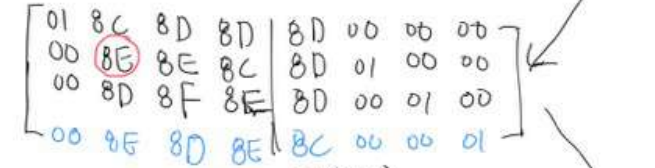
01=1 f(x)=3 =x+1

8C = x⁷+x³+x² 8C·3 = (x⁷+x³+x²)(x+1) = x⁸+x⁴+x³+x⁷+x³+x²
= x⁸+x⁷+x⁴+x² = x⁷+x³+x²+x+1
8D = x⁷+x³+x²+1 = 10001111 = 8F

8D·3 = (x⁷+x³+x²+1)(x+1) = x⁸+x⁴+x³+x⁷+x³+x²+x+1
= x⁸+x⁷+x⁴+x³+x+1
= x⁷+x³+x²+1 = 10001100 = 8C

01 8C 8D 8D | 8D 00 00 00
→ 03 8F 8C 8C | 8C 00 00 00

8F−01 = x⁷+x³+x²+x = 8E, 8C−01 = x⁷+x³+x²+1 = 8D,
8C−02 = x⁷+x³+x²+x = 8E

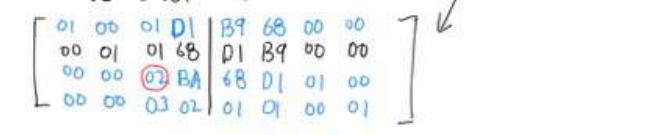


$(x^8+x^7+x^3+x+1) = (x^8+x^3+x^2+x)\cdot x+(x^7+x+1)$
$x^7+x^3+x^2+x = 0\cdot x^8+x^7+x^3+x^2+x+1\cdot x^7+x^3+x^2+x = 0\cdot m(x)+1\cdot f(x)$
$x^7+x+1 = (x^8+x^7+x^3+x+1)+x(x^7+x^3+x^2+x)$
$= m(x)+x\cdot f(x)$
$(x^7+x^3+x^2+x) = (x^7+x+1)(x^6+x^4+x^3)+x$
$x^7+x+1 = (x^8+x^7+x^3+x+1)+x(x^7+x^3+x^2+x)$
$= m(x)+x\cdot f(x)$
$x = (x^7+x^3+x^2+x)+(x^6+x^4+x^3)(x^7+x+1)$
$= f(x)+(x^6+x^4+x^3)(m(x)+x f(m)) = f(x)+(x^6+x^4+x^3)m(x)+(x^6+x^4+x^3)f(x)$
$= m(x)+(x^6+x^4+x^3+1)f(x)$

$x^8+x^7+x^3+x+1 = m(x)$
$x^7+x^3+x^2+x = f(x)$

$(x^7+x+1) = x(x+1)+1$
$1 = (x^7+x+1)+(x+1)x = m(x)+x f(x)+(x+1)(m(x)+(x^6+x^4+x^3)f(x))$
$= x\,m(x)+(x^7+x^6+x^4+x^3+1)f(x)$
$\Rightarrow (x^7+x^6+x^4+x^3+1)f(x) = 1 \pmod{m(x)}$
$(x^7+x^6+x^4+x)^{-1} = x^7+x^6+x^4+x+1 = B9$

00 01 01 6B | D1 B9 00 00
→ 00 8C 8C 5C | 34 6B 00 00
→ 00 8D 8D 34 | E5 0B 00 00
→ 00 8E 8E 8C | 0B 01 00 00



$$\left[\begin{array}{cccc|cccc} 01 & 00 & 01 & D1 & B9 & 68 & 00 & 00 \\ 00 & 01 & 01 & 68 & D1 & B9 & 00 & 00 \\ 00 & 00 & 02 & BA & 68 & D1 & 01 & 00 \\ 00 & 00 & 03 & 02 & 01 & 01 & 00 & 01 \end{array}\right]$$

$02=x \quad x'=x^3+x^2+x^2+1=8D$

$$\left[\begin{array}{cccc|cccc} 01 & 00 & 01 & D1 & B9 & 68 & 00 & 00 \\ 0D & 01 & 61 & 68 & D1 & B9 & 00 & 60 \\ 00 & 00 & 01 & 5D & 34 & E5 & 8D & 00 \\ 00 & 00 & 03 & 02 & 01 & 01 & 00 & 01 \end{array}\right]$$

$$\begin{array}{cccc|cccc} 00 & 00 & 01 & 5D & 34 & E5 & 8D & 00 \\ \rightarrow 00 & 00 & 03 & E7 & 5C & 34 & 8C & 00 \end{array}$$

$$\left[\begin{array}{cccc|cccc} 01 & 00 & 00 & 8C & 8D & 8D & 8D & 00 \\ 00 & 01 & 00 & 35 & E5 & 5C & 8D & 00 \\ 00 & 00 & 01 & 5D & 34 & E5 & 8D & 00 \\ 00 & 00 & 00 & E5 & 5D & 35 & 8C & 01 \end{array}\right]$$

$E5=x^7+x^6+x^5+x^2+1$

$M(x)=x^8+x^7+x^2+x+1$

$f(x)=x^6+x^5+x^2+1$

$x^8+x^7+x^2+x+1=(x^2+x^7+x^5+x^2+1)x+(x^7+x^6+x^2+1)$

$\begin{cases} (x^2+x^7+x^5+x^2+1)\Rightarrow f(x) \\ x^7+x^6+x^2+1=M(x)+xf(x) \end{cases}$

$x^7+x^6+x^5+x^2+1=(x^7+x^6+x^4+1)+(x^5+x^2+x^2)$

$\begin{cases} x^7+x^6+x^4+1=M(x)+xf(x) \\ x^5+x^2+x^2=(x^7+x^6+x^5+x^2+1)+(x^7+x^6+x^4+1)=f(x)+M(x)+xf(x) \end{cases}$

$=M(x)+(x+1)f(x)$

$x^7+x^6+x^4+1=(x^5+x^4+x^2)x^2+1$

$\begin{cases} x^5+x^4+x^2=M(x)+(x+1)f(x) \\ 1=(x^7+x^6+x^4+1)+x^2(x^5+x^4+x^2)=M(x)+xf(x)+x^2\{M(x)+(x+1)f(x)\} \end{cases}$

$=(x^2+1)M(x)+(x^3+x^2+x)f(x)$

$(x^3+x^2+x)f(x)=1 \pmod{M(x)}$

$f(x)^{-1}=(x^2+x^2+x)=0E$

$$\left[\begin{array}{cccc|cccc} 01 & 00 & 00 & 8C & 8D & 8D & 8D & 00 \\ 00 & 01 & 00 & 35 & E5 & 5C & 8D & 00 \\ 00 & 00 & 01 & 5D & 34 & E5 & 8D & 00 \\ 00 & 00 & 00 & 01 & 0D & 0D & 09 & 0E \end{array}\right]$$

$$\begin{array}{cccc|cccc} 00 & 00 & 00 & 01 & 0D & 0D & 09 & 0E \\ \rightarrow 00 & 00 & 00 & 8C & 86 & 86 & 80 & 09 \\ 00 & 00 & 00 & 35 & 52 & 52 & 86 & 0D \\ 00 & 00 & 00 & 5D & EC & EC & 83 & 0B \end{array}$$

$$\left[\begin{array}{cccc|cccc} 01 & 00 & 00 & 00 & 0E & 0B & 0D & 09 \\ 00 & 01 & 00 & 00 & 09 & 0E & 0B & 0D \\ 00 & 00 & 01 & 00 & 0D & 09 & 0E & 0B \\ 00 & 00 & 00 & 01 & 0D & 0D & 09 & 0E \end{array}\right]$$

$\Rightarrow$ 역행렬 $=\left[\begin{array}{cccc} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0D & 0D & 09 & 0E \end{array}\right]$