=32

1、给定 GF(2^5)的本原多项式$p(x) = x^5 + x^2 + 1$，写出 GF(2^5)的生成过程。GF(2^5)中的元素用多项式和数值两种形式来表示。

2、对于 GF(2^8)和本原多项式$p(x) = x^8 + x^4 + x^3 + x^2 + 1$，计算 GF($2^8$)中的元素 10 和 120 的乘积。（10 和 120 为十进制表示形式）

解：1. GF(2^5)中元素有：

00000 → 0
00001 → 1
00010 → x
00100 → x^2
00101 → x^2+1
00110 → x^2+x
00111 → x^2+x+1
01000 → x^3
01001 → x^3+1
01010 → x^3+x
01011 → x^3+x+1
01100 → x^3+x^2
01101 → x^3+x^2+1
01110 → x^3+x^2+x
01111 → x^3+x^2+x+1
10000 → x^4
10001 → x^4+1
10010 → x^4+x
10011 → x^4+x+1
10100 → x^4+x^2
10101 → x^4+x^2+1
10110 → x^4+x^2+x
10111 → x^4+x^2+1
11000 → x^4+x^3
11001 → x^4+x^3+1
11010 → x^4+x^3+x
11011 → x^4+x^3+x+1
11100 → $x^4+x^3+x^2$
11101 → $x^4+x^3+x^2+1$
11110 → $x^4+x^3+x^2+x$
11111 → $x^4+x^3+x^2+x+1$

生成过程

① 00000 → 0
② 00001 → 1
③ 00010 → x
④ x^2 → 00100
⑤ x^3 → 01000
⑥ x^4 → 10000
⑦ x^5 → x^2+1 → 00101
⑧ x^6 → x^3+x → 01010
⑨ x^4+x^2 → 10100
⑩ x^5+x^3 → x^3+x^2+1 → 01101
⑪ x^4+x^3+x → 11010
⑫ $x^5+x^4+x^2$ → x^4+1 → 10001
⑬ x^5+x → x^2+x+1 → 00111
⑭ x^3+x^2+x → 01110
⑮ $x^4+x^3+x^2$ → 11100
⑯ $x^5+x^4+x^3$ → $x^4+x^3+x^2+1$ → 11101
⑰ $x^5+x^4+x^3+x$ → $x^4+x^3+x^2+x+1$ → 11111
⑱ $x^5+x^4+x^3+x^2+x$ → x^4+x^3+x+1 → 11011
⑲ $x^5+x^4+x^2+x$ → x^4+x+1 → 10011
⑳ x^5+x^2+x → $x+1$ → 00011
㉑ x^2+x → 00110
㉒ x^3+x^2 → 01100
㉓ x^4+x^3 → 11000
㉔ x^5+x^4 → x^4+x^2+1 → 10101
㉕ x^5+x^3+x → x^3+x^2+x+1 → 01111

㉖ $x^4+x^3+x^2+x \to 11110$

㉗ $x^5+x^4+x^3+x^2 \to x^4+x^3+1 \to 11001$

㉘ $x^5+x^4+x \to x^4+x^2+x+1 \to 10111$

㉙ $x^5+x^3+x^2+x \to x^3+x+1 \to 01011$

㉚ $x^4+x^2+x \to 10110$

㉛ $x^5+x^3+x^2 \to x^3+1 \to 01001$

㉜ $x^4+x \to 10010$

2. GF(28) 中 $(19)_{10} = (00001010)_2$

$= x^3+x$

$(120)_{10} = (01111000)_2 = x^6+x^5+x^4+x^3$

$(10)_{10} \times (120)_{10} = (x^3+x)(x^6+x^5+x^4+x^3) \bmod P(x)$

$= (x^9+x^8+x^7+x^6+x^7+x^6+x^5+x^4) \bmod P(x)$

$= (x^9+x^8+x^5+x^4) \bmod P(x)$

$= x^4+x^2+x+1 = (00001111)_2$

$$
\begin{array}{r|l}
 & 1 \quad / \\
\hline
x^8+x^4+x^3+x^2+1 & x^9+x^8+x^5+x^4 \\
 & x^9+x^5+x^4+x^3+x \\
\hline
 & x^8+x^3+x \\
 & x^8+x^4+x^3+x^2+1 \\
\hline
 & x^4+x^2+x+1
\end{array}
$$