◎ガロア体のデータ表現

ガロア体の表現には，べき乗表現とベクトル表現があります．

ガロア体の乗算，除算はべき乗表現，加算はベクトル表現で行います．

原始多項式 $p(x)=x^8+x^4+x^3+x^2+x^0$，$p(\alpha)=0$ の原始元 α で生成されるガロア体のべき乗表現とベクトル表現の関係は次のとおりです．

べき乗	ベクトル								
	α^7	α^6	α^5	α^4	α^3	α^2	α^1	α^0	
−	0	0	0	0	0	0	0	0	
α^0	0	0	0	0	0	0	0	1	
α^1	0	0	0	0	0	0	1	0	
α^2	0	0	0	0	0	1	0	0	+
α^3	0	0	0	0	1	0	0	0	
α^4	0	0	0	1	0	0	0	0	
α^5	0	0	1	0	0	0	0	0	
α^6	0	1	0	0	0	0	0	0	
α^7	1	0	0	0	0	0	0	0	
α^8	0	0	0	1	1	1	0	1	← $\alpha^8+\alpha+\alpha^3+\alpha^2+\alpha^0=0$　$\alpha^8=\alpha^4+\alpha^3+\alpha^2+\alpha^0$
α^9	0	0	1	1	1	0	1	0	← $\alpha^9=\alpha\cdot\alpha^8=\alpha^5+\alpha^4+\alpha^3+\alpha$
α^{10}	0	1	1	1	0	1	0	0	← $\alpha^{10}=\alpha\cdot\alpha^9=\alpha^6+\alpha^5+\alpha^4+\alpha^2$
α^{11}	1	1	1	0	1	0	0	0	← $\alpha^{11}=\alpha\cdot\alpha^{10}=\alpha^7+\alpha^6+\alpha^5+\alpha^3$
α^{12}	1	1	0	0	1	1	0	1	← $\alpha^{12}=\alpha\cdot\alpha^{11}=\alpha^8+\alpha^7+\alpha^6+\alpha^4$
									$=(\alpha^4+\alpha^3+\alpha^2+\alpha^0)+\alpha^7+\alpha^6+\alpha^4=\alpha^7+\alpha^6+\alpha^3+\alpha^2+\alpha^0$
	⋮								
α^{254}	1	0	0	0	1	1	1	0	
α^{255}	0	0	0	0	0	0	0	1	← $\alpha^{255}=\alpha\cdot\alpha^{254}=\alpha^8+\alpha^4+\alpha^3+\alpha^2$
									$=(\alpha^4+\alpha^3+\alpha^2+\alpha^0)+\alpha^4+\alpha^3+\alpha^2=\alpha^0$

◎ガロア体の計算

・乗算

$\alpha^n\cdot\alpha^m=\alpha^{(n+m)}$　n+m>254 なら $\alpha^{(n+m-255)}$

$\alpha^{52}\cdot\alpha^{250}=\alpha^{(52+250-255)}=\alpha^{47}$

・除算

$\alpha^n/\alpha^m=\alpha^{(n-m)}$　n−m<0 なら $\alpha^{(n-m+255)}$

$\alpha^{100}/\alpha^{12}=\alpha^{(100-12)}=\alpha^{88}$

・加算（減算）

ベクトル表現した値で EX-OR を取る。

$\alpha^{12}+\alpha^{10}=\alpha^{12}-\alpha^{10}=11001101 \oplus 01110100 = 10111001=\alpha^{60}$