FF-7, AES-2

FF-7) $1 = \gcd(x^3+x^2+1,\ x^5+x^2+1)$

$$
\begin{array}{r|l}
x^3+x^2+0x+1 & x^5+0x^4+0x^3+x^2+0x+1 \\
 & \underline{x^5+x^4\qquad\quad+x^2} \\
 & 0\quad x^4\qquad+x^2\qquad+1 \\
 & \underline{x^4+x^3\qquad+x} \\
 & 0\quad x^3+x^2+x+1 \\
 & \underline{x^3+x^2\qquad+1} \\
 & x
\end{array}
\quad\Rightarrow\quad x^2+x+1
$$

$$(x^5+x^2+1) = (x^2+x+1)(x^3+x^2+1) + (x)$$

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

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

$$1 = (x^3+x^2+1) + (x^2+x)\left((x^5+x^2+1) + (x^2+x+1)(x^3+x^2+1)\right)$$

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

$$1 = (x^3+x^2+1)(x^4+x+1)$$

Inverse of x^3+x^2+1 is x^4+x+1

AES-2) $x^4+x+1 = (x+1)(x^3+x^2) + (x^2+x+1)$

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

$$(x^2+x+1) = (x+1)(x) + 1$$

$$\perp = (x^2+x+1) + (x+1)(x)$$

$$\perp = (x^2+x+1) + (x+1)\left((x^3+x^2)+(x)(x^2+x+1)\right)$$

$$\perp = (x^2+x+1) + (x+1)(x^3+x^2) + (x+1)(x)(x^2+x+1)$$

$$\perp = (x+1)(x^3+x^2) + (x^2+x+1)(x^2+x+1)$$

$$\perp = (x+1)(x^3+x^2) + (x^2+x+1)\left(0+(x+1)(x^3+x^2)\right)$$

$$\perp = (x+1)(x^3+x^2) + (x^2+x+1)(x+1)(x^3+x^2)$$

$$\perp = (x+1)(x^3+x^2) + (x^3+1)(x^3+x^2)$$

$$\perp = (x^3+x^2)\left((x+1)+(x^3+1)\right)$$

$$\perp = (x^3+x^2)(x^3+x)$$

$$(x^3+x^2)^{-1} = (x^3+x) = 1010$$

$$(y^3+y)(y^3+y^2+1) + (y^3+1)$$

$$= y^6+y^5+y^3+y^4+y^3+y+y^3+1$$

$$= y^2+y+1+y^3+y+1$$

$$= y^3+y^3 = 1100$$

$$SBOX(1100) = 1100$$