GF(2^4)

- can be constructed from
  $m(x) = x^4 + x + 1$
- elements are polynomials
  - modulo $m(x)$
  - modulo 2

$a_3x^3 + a_2x^2 + a_1x + a_0 \xrightarrow{4\text{ bits}} a_3a_2a_1a_0$

$x^3 + x + 1 \qquad\qquad 1011$

- addition

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

$1011 \oplus 1100 \qquad 0111$

- multiplication

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

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

$-(x^6+x^3+x^2)$

$x^5+x^4-x^3$

$-(x^5+x^2+x)$

$x^4-x^3-x^2-x$

$-(x^4+x+1)$

$-x^3-x^2-2x-1$ remainder

$= -x^3-x^2-2x-1$

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

$1011 \cdot 1100 = 1101$