$GF(2^4)$

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

now: inversion (crucial non-linear step in AES)

AES

$GF(2^8)$

$m(x) = x^8 + x^4 + x^3 + x + 1$

EG $(x^2+1)^{-1}$ in $GF(2^4)$

Euclid

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

Bezout

$$1 = x^2 + 1 + x \cdot x$$
$$= x^2 + 1 + x\left(x^4 + x + 1 + (x^2+1)(x^2+1)\right)$$
$$= (x^3 + x + 1)(x^2+1) + x(x^4 + x + 1)$$

$$\Rightarrow (x^2+1)^{-1} = x^3 + x + 1 \text{ in } GF(2^4)$$

$$(0101)^{-1} = 1011$$