

Example 118. The polynomial $x^3 + x + 1$ is irreducible modulo 2, so we can use it to construct the finite field $\text{GF}(2^3)$ with 8 elements.

- (a) List all 8 elements, and multiply all of them with $x + 1$.
- (b) What is the inverse of $x + 1$?

Solution.

- (a) The elements are $0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1$.

[Note that $x^3 = -x - 1 = x + 1$ in $\text{GF}(2^3)$. That means all polynomials of degree 3 and higher can be reduced to polynomials of degree less than 3.]

When multiplying, we calculate, for instance: $(x + 1)x^2 = x^3 + x^2 = x^2 + x + 1$

Similarly: $(x + 1)(x^2 + 1) = (x + 1)x^2 + (x + 1) \equiv (x^2 + x + 1) + (x + 1) \equiv x^2$

Or: $(x + 1)(x^2 + x) = (x + 1)x^2 + (x + 1)x \equiv (x^2 + x + 1) + (x^2 + x) \equiv 1$

\times	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x

- (b) We are looking for an element y such that $y(x + 1) = 1$ in $\text{GF}(2^3)$. Looking at the table, we see that $y = x^2 + x$ has that property. Hence, $(x + 1)^{-1} = x^2 + x$ in $\text{GF}(2^3)$.

The (extended) Euclidean algorithm with polynomials

Example 119.

- (a) Apply the extended Euclidean algorithm to find the gcd of $x^2 + 1$ and $x^4 + x + 1$, and spell out Bezout's identity.
- (b) Repeat the previous computation but always reduce all coefficients modulo 2.
- (c) What is the inverse of $x^2 + 1$ in $\text{GF}(2^4)$? Here, $\text{GF}(2^4)$ is constructed using $x^4 + x + 1$.

Solution.

- (a) We use the extended Euclidean algorithm:

$$\begin{aligned} \gcd(x^2 + 1, x^4 + x + 1) & \quad \boxed{x^4 + x + 1} = (x^2 - 1) \cdot \boxed{x^2 + 1} + (x + 2) \\ & = \gcd(x + 2, x^2 + 1) \quad \boxed{x^2 + 1} = (x - 2) \cdot \boxed{x + 2} + 5 \\ & = 5 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$\begin{aligned} 5 & = 1 \cdot \boxed{x^2 + 1} - (x - 2) \cdot \boxed{x + 2} = 1 \cdot \boxed{x^2 + 1} - (x - 2) \cdot (\boxed{x^4 + x + 1} - (x^2 - 1) \cdot \boxed{x^2 + 1}) \\ & = (x^3 - 2x^2 - x + 3) \cdot \boxed{x^2 + 1} - (x - 2) \cdot \boxed{x^4 + x + 1} \end{aligned}$$

If we wanted to, we could divide both sides by 5.

- (b) We repeat the exact same computation but reduce modulo 2 at each step:

$$\begin{aligned} \boxed{x^4 + x + 1} & \equiv (x^2 + 1) \cdot \boxed{x^2 + 1} + x \\ \boxed{x^2 + 1} & \equiv = x \cdot \boxed{x} + 1 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$\begin{aligned} 1 & = 1 \cdot \boxed{x^2 + 1} + x \cdot \boxed{x} = 1 \cdot \boxed{x^2 + 1} + x \cdot (\boxed{x^4 + x + 1} + (x^2 + 1) \cdot \boxed{x^2 + 1}) \\ & = (x^3 + x + 1) \cdot \boxed{x^2 + 1} + x \cdot \boxed{x^4 + x + 1} \end{aligned}$$

- (c) We can now read off that $(x^2 + 1)^{-1} = x^3 + x + 1$ in $\text{GF}(2^4)$.

Example 120. (extra) Find the inverse of $x^2 + 1$ in $\text{GF}(2^8)$, constructed as in AES.

Solution. Recall that for AES, $\text{GF}(2^8)$ is constructed using $x^8 + x^4 + x^3 + x + 1$.

We use the extended Euclidean algorithm for polynomials, and reduce all coefficients modulo 2:

$$\begin{aligned} \gcd(x^2 + 1, x^8 + x^4 + x^3 + x + 1) & \quad \boxed{x^8 + x^4 + x^3 + x + 1} \equiv (x^6 + x^4 + x) \cdot \boxed{x^2 + 1} + 1 \\ & = 1 \end{aligned}$$

Hence, $(x^2 + 1)^{-1} = x^6 + x^4 + x$ in $\text{GF}(2^8)$.

Example 121. (extra)

- Apply the extended Euclidean algorithm to find the gcd of $x^3 + 1$ and $x^8 + x^4 + x^3 + x + 1$, and spell out Bezout's identity.
- Repeat the previous computation but always reduce all coefficients modulo 2.
- What is the inverse of $x^3 + 1$ in $\text{GF}(2^8)$, constructed using $x^8 + x^4 + x^3 + x + 1$?

Solution.

- The final result is that the gcd is 1, and Bezout's identity takes the form

$$(x^6 - x^3 + x^2 + x + 1)(x^3 + 1) - x(x^8 + x^4 + x^3 + x + 1) = 1.$$

(The computations are exactly as in the next step, except we do not reduce modulo 2.)

- We use the extended Euclidean algorithm, and always reduce modulo 2:

$$\begin{aligned} \boxed{x^8 + x^4 + x^3 + x + 1} & \equiv (x^5 + x^2 + x + 1) \cdot \boxed{x^3 + 1} + x^2 \\ \boxed{x^3 + 1} & \equiv x \cdot \boxed{x^2} + 1 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$\begin{aligned} 1 & \equiv 1 \cdot \boxed{x^3 + 1} - x \cdot \boxed{x^2} \equiv 1 \cdot \boxed{x^3 + 1} - x \cdot (\boxed{x^8 + x^4 + x^3 + x + 1} - (x^5 + x^2 + x + 1) \cdot \boxed{x^3 + 1}) \\ & \equiv x^6 + x^4 + x + 1. \end{aligned}$$

- Hence, $(x^3 + 1)^{-1} = x^6 + x^4 + x + 1$ in $\text{GF}(2^8)$.