

Review. $\text{GF}(p^n)$ is “the” finite field with p^n elements.

Recall that, in the construction of $\text{GF}(p^n)$, the polynomial $m(x)$ has to be such that it cannot be factored modulo p . We also require that $m(x)$ needs to be **irreducible** mod p .

For instance. The polynomial $x^2 + 2x + 1$ can always be factored as $(x + 1)^2$.

On the other hand. For the polynomials $m(x) = x^2 + x + 1$ things are more interesting:

- $x^2 + x + 1$ cannot be factored over \mathbb{Q} because the roots $\frac{-1 \pm \sqrt{-3}}{2}$ are not rational.
- However, $x^2 + x + 1 \equiv (x + 2)^2$ modulo 3, so it can be factored modulo 3.
- On the other hand, $x^2 + x + 1$ is irreducible modulo 2 (that is, it cannot be factored: the only linear factors are x and $x + 1$, but x^2 , $x(x + 1)$ and $(x + 1)^2$ are all different from $x^2 + x + 1$ modulo 2).

In general, it follows from the formula $\frac{-1 \pm \sqrt{-3}}{2}$ for the roots that $x^2 + x + 1$ can be factored modulo a prime $p > 2$ if and only if $\sqrt{-3}$ exists as a residue modulo p . In other words, if and only if -3 is a quadratic residue modulo p .

For instance. Modulo $p = 7$, we have $-3 \equiv 2^2$ and $\frac{1}{2} \equiv 4$, so that $\frac{-1 \pm \sqrt{-3}}{2} \equiv 4 \cdot (-1 \pm 2) \equiv 2, 4$. Indeed, we have the factorization $(x - 2)(x - 4) = x^2 - 6x + 8 \equiv x^2 + x + 1$ modulo 7.

Example 136. 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.

- List all 8 elements.
- Reduce $x^5 + 1$ in $\text{GF}(2^3)$.
- Multiply each element of $\text{GF}(2^3)$ with $x^2 + x$.
- What is the inverse of $x^2 + x$ in $\text{GF}(2^3)$?

Solution.

- 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. See next part.]
- We divide $x^5 + 1$ by $x^3 + x + 1$ (long division!) to find $x^5 + 1 = (x^2 - 1)(x^3 + x + 1) + (-x^2 + x + 2)$. It follows that $x^5 + 1$ reduces to $-x^2 + x + 2 \equiv x^2 + x$ in $\text{GF}(2^3)$.
Important. We can simplify things by performing the long division modulo 2. We then find $x^5 + 1 \equiv (x^2 + 1)(x^3 + x + 1) + (x^2 + x)$.
- We multiply the polynomials as usual, then reduce as in the previous part.
For instance, $(x^2 + x)(x^2 + x + 1) \equiv x^4 + x$ and, by long division, $x^4 + x \equiv x(x^3 + x + 1) + x^2$, which reduces to just x^2 in $\text{GF}(2^3)$.

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

- We are looking for an element y such that $y(x^2 + x) = 1$ in $\text{GF}(2^3)$. Looking at the table, we see that $y = x + 1$ has that property. Hence, $(x^2 + x)^{-1} = x + 1$ in $\text{GF}(2^3)$.
Important. To find the inverse, we essentially tried all possibilities. That’s not sustainable. Instead, we can (and should!) proceed as we did for computing the inverse of residues modulo n . That is, we should use the Euclidean algorithm as indicated in the next examples. Here, this is just one step: modulo 2, we have $x^3 + x + 1 \equiv (x + 1) \cdot (x^2 + x) + 1$, so that $(x^2 + x)^{-1} = x + 1$ in $\text{GF}(2^3)$.

The (extended) Euclidean algorithm with polynomials

Example 137.

- (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:

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

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 138. (HW) Find the inverses of $x^2 + 1$ and $x^3 + 1$ in $\text{GF}(2^8)$, constructed as in AES.

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

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

$$\boxed{x^8 + x^4 + x^3 + x + 1} \equiv (x^6 + x^4 + x) \cdot \boxed{x^2 + 1} + 1$$

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

- (b) 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

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

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