

EXAMPLE OF EUCLID'S ALGORITHM FOR POLYNOMIALS

We will use Euclid's algorithm and back-substitution to determine the (monic!) gcd of $T^8 - 1$ and $T^5 + 2T^3 + 2$ in $\mathbf{F}_3[T]$ and to express the gcd as an $\mathbf{F}_3[T]$ -linear combination of the two polynomials.

Remember: all computations are being carried out in $\mathbf{F}_3[T]$.

By Euclid's algorithm in $\mathbf{F}_3[T]$,

$$\begin{aligned} T^8 - 1 &= (T^5 + 2T^3 + 2)(T^3 + T) + (T^4 + T^3 + T + 2) \\ T^5 + 2T^3 + 2 &= (T^4 + T^3 + T + 2)(T + 2) + (2T^2 + 2T + 1) \\ (T^4 + T^3 + T + 2) &= (2T^2 + 2T + 1)(2T^2 + 2) + 0. \end{aligned}$$

The last nonzero remainder is $2T^2 + 2T + 1$, whose monic multiple is $T^2 + T + 2$, so the greatest common divisor of $T^8 - 1$ and $T^5 + 2T^3 + 2$ is $T^2 + T + 2$. As a check on this, we show that $T^2 + T + 2$ is a factor of both $T^8 - 1$ and $T^5 + 2T^3 + 2$ in $\mathbf{F}_3[T]$:

$$T^8 - 1 = (T^2 + T + 2)(T^6 + 2T^5 + 2T^4 + 2T^2 + T + 1), \quad T^5 + 2T^3 + 2 = (T^2 + T + 2)(T^3 + 2T^2 + T + 1).$$

To write $T^2 + T + 2$ as an $\mathbf{F}_3[T]$ -linear combination of $T^8 - 1$ and $T^5 + 2T^3 + 2$, we back-substitute into Euclid's algorithm, starting with the last nonzero remainder:

$$\begin{aligned} 2T^2 + 2T + 1 &= T^5 + 2T^3 + 2 - (T^4 + T^3 + T + 2)(T + 2) \\ &= T^5 + 2T^3 + 2 - (T^8 - 1 - (T^5 + 2T^3 + 2)(T^3 + T))(T + 2) \\ &= (T^5 + 2T^3 + 2)(1 + (T^3 + T)(T + 2)) - (T^8 - 1)(T + 2) \\ &= (T^5 + 2T^3 + 2)(T^4 + 2T^3 + T^2 + 2T + 1) - (T^8 - 1)(T + 2). \end{aligned}$$

Now multiply both sides by 2 to make the left side monic:

$$T^2 + T + 2 = (T^5 + 2T^3 + 2)(2T^4 + T^3 + 2T^2 + T + 2) + (T^8 - 1)(T + 2).$$