# Solutions 7

**#1** Verify that $x^3 + x + 1$ is irreducible in $(\mathbf{Z}/2)[x]$.

Since $1^3 + 1 + 0 = 1 \neq 0$ and $0^3 + 0 + 1 = 1 \neq 0$, the equation $x^3 + x + 1 = 0$ has no roots in $\mathbf{Z}/2$. By the Division Algorithm, this means that $x^3 + x + 1$ is irreducible in $(\mathbf{Z}/2)[x]$.

**#2** In the field $K = (\mathbf{Z}/2)[x]/(x^2 + x + 1)$ let $\alpha$ be the image of $x$, and compute in reduced form $\alpha^5$.

Compute the reduction of $x^5$ modulo $x^2 + x + 1$ (by dividing)

$$(x^5) - (x^3 + x^2 + 1)(x^2 + x + 1) = x + 1$$

Therefore, $\alpha^5 = \alpha + 1$.

**#3** In the field $K = (\mathbf{Z}/2)[x]/(x^3 + x + 1)$ let $\alpha$ be the image of $x$, and compute in reduced form $(1 + \alpha + \alpha^2)^{-1}$.

Run the Euclidean Algorithm on $x^3 + x + 1$ and $x^2 + x + 1$:

$$\begin{array}{lcl} (x^3 + x + 1) & -(x+1)(x^2 + x + 1) & = x \\ (x^2 + x + 1) & -(x+1)(x) & = 1 \end{array}$$

Then, going backwards:

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

Thus, looking at this equation modulo $x^3 + x + 1$, we see that $x^2$ is the multiplicative inverse of $x^2 + x + 1$ modulo $x^3 + x + 1$. That is,

$$(\alpha^2 + \alpha + 1)^{-1} = \alpha^2$$