Homework Set 6 (Lecture 22)

Problems 7 & 8

Problems 7 and 8 are asking for inverses in $\mathrm{GF}(2^3)$ and $\mathrm{GF}(2^4)$. The process is the same, so we give examples for the case of $\mathrm{GF}(2^4)$.

As these examples illustrate, the amount of computation varies depending on which element we are inverting. If your calculation was particularly simple, or if you would like extra practice, let the homework system generate a new problem for you.

Example 1. Consider the finite field $\mathrm{GF}(2^4)$ constructed from the polynomial x^4+x+1. We represent the 16 elements in that field in the natural way using 4 bits. What is the inverse of 0101?

Solution. We are asked for the inverse of x^2+1.

We use the extended Euclidean algorithm and 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

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

We therefore conclude that $(x^2+1)^{-1}=x^3+x+1$ in $\mathrm{GF}(2^4)$.

Encoded as bits, the inverse of 0101 is 1011.

Example 2. Consider the finite field $\mathrm{GF}(2^4)$ constructed from the polynomial x^4+x+1. We represent the 16 elements in that field in the natural way using 4 bits. What is the inverse of 0111?

Solution. We are asked for the inverse of x^2+x+1.

We use the extended Euclidean algorithm and reduce modulo 2 at each step:

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

We therefore are able to immediately conclude that $(x^2+x+1)^{-1}=x^2+x$ in $\mathrm{GF}(2^4)$.

Encoded as bits, the inverse of 0111 is 0110.

Armin Straub
straub@southalabama.edu