Homework Set 7 (Lecture 23)

Problem 1

The process is the same as for the last two problems.

Again, the amount of computation varies considerably depending on which element we are inverting. Below we illustrate one intermediate, one laborious case as well as one that takes very little work.

Example 3. Consider the AES finite field $\mathrm{GF}(2^8)$ constructed from the polynomial $x^8+x^4+x^3+x+1$. We represent the 2^8 elements in that field in the natural way using 8 bits. What is the inverse of 00111001?

Solution. We are asked for the inverse of $x^5+x^4+x^3+1$.

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

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

Backtracking through this, again reducing modulo 2 along the way, we find that Bézout's identity takes the form

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

We therefore conclude that $(x^5+x^4+x^3+1)^{-1}=x^5+x^4+x^2+1$ in $\mathrm{GF}(2^8)$.

Encoded as bits, the inverse of 00111001 is 00110101.

Example 4. Consider the AES finite field $\mathrm{GF}(2^8)$ constructed from the polynomial $x^8+x^4+x^3+x+1$. We represent the 2^8 elements in that field in the natural way using 8 bits. What is the inverse of 11011111?

Solution. We are asked for the inverse of $x^7+x^6+x^4+x^3+x^2+x+1$.

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

$$\begin{aligned} \boxed{x^8+x^4+x^3+x+1} &\equiv (x+1)\cdot\boxed{x^7+x^6+x^4+x^3+x^2+x+1}+(x^6+x^5+x^4+x^3+x)\\ \boxed{x^7+x^6+x^4+x^3+x^2+x+1} &\equiv x\cdot\boxed{x^6+x^5+x^4+x^3+x}+(x^5+x^3+x+1)\\ \boxed{x^6+x^5+x^4+x^3+x} &\equiv (x+1)\cdot\boxed{x^5+x^3+x+1}+(x^2+x+1)\\ \boxed{x^5+x^3+x+1} &\equiv (x^3+x^2+x)\cdot\boxed{x^2+x+1}+1 \end{aligned}$$

Backtracking through this, again reducing modulo 2 along the way, we find that Bézout's identity takes the form

$$\begin{aligned} 1 &\equiv \boxed{x^5+x^3+x+1}+(x^3+x^2+x)\cdot\boxed{x^2+x+1}\\ &\equiv \boxed{x^5+x^3+x+1}+(x^3+x^2+x)\left(\boxed{x^6+x^5+x^4+x^3+x}+(x+1)\cdot\boxed{x^5+x^3+x+1}\right)\\ &\equiv (x^4+x+1)\cdot\boxed{x^5+x^3+x+1}+(x^3+x^2+x)\cdot\boxed{x^6+x^5+x^4+x^3+x}\\ &\equiv (x^4+x+1)\cdot\left(\boxed{x^7+x^6+x^4+x^3+x^2+x+1}+x\cdot\boxed{x^6+x^5+x^4+x^3+x}\right)\\ &\quad +(x^3+x^2+x)\cdot\boxed{x^6+x^5+x^4+x^3+x}\\ &\equiv (x^4+x+1)\cdot\boxed{x^7+x^6+x^4+x^3+x^2+x+1}+(x^5+x^3)\cdot\boxed{x^6+x^5+x^4+x^3+x}\\ &\equiv (x^4+x+1)\cdot\boxed{x^7+x^6+x^4+x^3+x^2+x+1}\\ &\quad +(x^5+x^3)\left(\boxed{x^8+x^4+x^3+x+1}+(x+1)\cdot\boxed{x^7+x^6+x^4+x^3+x^2+x+1}\right)\\ &\equiv (x^6+x^5+x^3+x+1)\cdot\boxed{x^7+x^6+x^4+x^3+x^2+x+1}+(x^5+x^3)\cdot\boxed{x^8+x^4+x^3+x+1} \end{aligned}$$

We therefore conclude that $(x^7+x^6+x^4+x^3+x^2+x+1)^{-1}=x^6+x^5+x^3+x+1$ in $\mathrm{GF}(2^8)$.

Encoded as bits, the inverse of 11011111 is 01101011.

Example 5. Consider the AES finite field $\mathrm{GF}(2^8)$ constructed from the polynomial $x^8+x^4+x^3+x+1$. We represent the 2^8 elements in that field in the natural way using 8 bits. What is the inverse of 10001101?

Solution. We are asked for the inverse of $x^7+x^3+x^2+1$.

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

$$\boxed{x^8+x^4+x^3+x+1} \equiv x\cdot\boxed{x^7+x^3+x^2+1}+1$$

We therefore are able to immediately conclude that $(x^7+x^3+x^2+1)^{-1}=x$ in $\mathrm{GF}(2^8)$.

Encoded as bits, the inverse of 10001101 is 00000010.

Problems 2, 3 & 4

You find the answers to these problems at the very beginning of Lecture 23.