Homework Set 7

Problems 1 & 2

Problems 1 and 2 are asking for products in $\mathrm{GF}(2^3)$ and $\mathrm{GF}(2^4)$. The process is the same, so we give an example for the case of $\mathrm{GF}(2^4)$.

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 product of 0111 and 1100?

Solution. We are asked for the product of x^2+x+1 and x^3+x^2 in $\mathrm{GF}(2^4)$.

We multiply the polynomials as usual to get $(x^2+x+1)(x^3+x^2)=x^5+2x^4+2x^3+x^2$. Modulo 2, this reduces to x^5+x^2. Finally, to reduce modulo x^4+x+1, we perform long division to get

$$\boxed{x^5+x^2}=x\cdot\boxed{x^4+x+1}-x.$$

Hence, reducing the remainder modulo 2, we get $x^5+x^2\equiv -x\equiv x$ in $\mathrm{GF}(2^4)$.

[Note that, to simplify computations, we can perform the steps of the long division modulo 2.]

Encoded as bits, the product of 0111 and 1100 therefore is 0010.

Problems 3 & 4

Problems 3 and 4 are asking for inverses in $\mathrm{GF}(2^3)$ and $\mathrm{GF}(2^4)$. Again, 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 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 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 3. 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.

Problem 5

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 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 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 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 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 6. 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 6, 7 & 8

You find the answers to these problems at the very beginning of Lecture 22.