Homework Set 8

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. If you feel comfortable with the steps, you can also **let SageMath do the work** for you (see the example code included on our website).

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.

Armin Straub
straub@southalabama.edu

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 2, 3 & 4

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

Problem 5

Example 7. What is the output of the AES-128 ByteSub applied to the byte $(0011\ 1001)_2$?

Solution. (using lookup table) Using the table at `https://en.wikipedia.org/wiki/Rijndael_S-box`, row $(0011)_2=(3)_{16}$, column $(1001)_2=(9)_{16}$, we find that the byte is transformed into $(12)_{16}=(0001\ 0010)_2$.

Solution. (doing the math) $(0011\ 1001)_2$ represents the polynomial $x^5+x^4+x^3+1$.

Its inverse is $(x^5+x^4+x^3+1)^{-1}=x^5+x^4+x^2+1$ in $\mathrm{GF}(2^8)$ (see Example 4 for the details of this computation), which is $\boldsymbol{c}=(0011\ 0101)_2$.

$$\begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \underbrace{\begin{bmatrix}1\\0\\1\\0\\1\\1\\0\\0\end{bmatrix}}_{\boldsymbol{c}} + \begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix} = \begin{bmatrix}1\\1\\1\\1\\1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\1\\1\\1\\1\\1\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\0\\1\\1\\1\\1\end{bmatrix} + \begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\1\end{bmatrix} + \begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\\1\\0\\0\\0\end{bmatrix}$$

[This is just the usual matrix-vector product modulo 2. The highlighted columns are the ones which get added up during this matrix-vector product.]

Hence, the output of ByteSub is the byte $(0001\ 0010)_2$.

Problem 6

Example 8. What are the multiplicative orders of 2 and 4 modulo 7?

Solution. Since $\phi(7)=6$, the possible orders of residues modulo 7 are $1,2,3,6$.

Since $2^2=4\not\equiv 1$, $2^3\equiv 1 \pmod 7$, the multiplicative order of $2 \pmod 7$ is 3.

Since $4^2\equiv 2\not\equiv 1$, $4^3\equiv 1 \pmod 7$, the multiplicative order of $4 \pmod 7$ is 3.

Alternatively. For the second part, we could have also used that, if $x \pmod m$ has (multiplicative) order k, then x^a has order $\frac{k}{\gcd(k,a)}$. Therefore, $4=2^2$ has multiplicative order $\frac{3}{\gcd(3,3)}=3$ modulo 7.

Armin Straub
straub@southalabama.edu

Problem 7

Example 9. Suppose 4 has multiplicative order 17 modulo m. What is the multiplicative order of 64 modulo m?

Solution. Recall that, if $x \pmod m$ has (multiplicative) order k, then x^a has order $\frac{k}{\gcd(k,a)}$.
Therefore, $64 = 4^3$ has multiplicative order $\frac{17}{\gcd(17,3)} = 17$ modulo m.

Problem 8

Example 10. Suppose 2 has multiplicative order 21 modulo m. What is the multiplicative order of 8 modulo m?

Solution. Recall that, if $x \pmod m$ has (multiplicative) order k, then x^a has order $\frac{k}{\gcd(k,a)}$.
Therefore, $8 = 2^3$ has multiplicative order $\frac{21}{\gcd(21,3)} = 7$ modulo m.

Armin Straub
straub@southalabama.edu