INF 240 - Exercise problems - 3
Solutions

Nikolay Kaleyski

Exercise 1. *Since* 7 *is a prime, the finite field* $\mathbb{F}_7$ *is the same thing as* $\mathbb{Z}_7$*; the Cayley tables therefore merely express addition and multiplication modulo* 7*. The table for addition has the form*

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	6	0	1	2	3	4	5
2	5	6	0	1	2	3	4
3	4	5	6	0	1	2	3
4	3	4	5	6	0	1	2
5	2	3	4	5	6	0	1
6	1	2	3	4	5	6	0

Table 1: Addition table for $\mathbb{F}_7$

and the one for multiplication takes the form

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	2	4
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 2: Multiplication table for $\mathbb{F}_7$

The inverse table can be extracted from the addition and multiplication tables above (by e.g. finding the row that contains the neutral element for a given column), or can be computed manually. Note that 0 *does not have a multiplicative inverse, and this is true for any field. The result is:*

Exercise 2. *1. Writing the coefficients from the least to the most significant,* $p_1(x) = x^5 + 3x^4 + 6x^2 + 2x + 1$ *gives the vector*

$$(1, 2, 6, 0, 3, 1)$$

while $p_2(x) = 6x^4 + 3x^3 + x^2 + x + 5$ *gives the vector*

$$(5, 1, 1, 3, 6).$$

x	$-x$	x^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Table 3: Inverse table for $\mathbb{F}_7$

Should we need to have both vectors of the same length, we can always expand the vector corresponding to $p_2(x)$ by adding extra terms with zero coefficients; in other words, we can imagine that $p_2(x)$ has the form $p_2(x) = 0x^5 + 6x^4 + 3x^3 + x^2 + x + 5$ and write its vector as

$$(5, 1, 1, 3, 6, 0).$$

2. The degree of a polynomial is its largest exponent with a non-zero coefficient. So, in our case, $\deg(p_1(x)) = 5$ *and* $\deg(p_2(x)) = 4$.

3. A monic polynomial is one whose largest exponent has coefficient 1. *In this case $p_1(x)$ is monic but $p_2(x)$ is not.*

4.

$$p_1(x)+p_2(x) = x^5+(6+3)x^4+(6+1)x^2+(2+1)x+5+1 = x^5+2x^4+3x+6.$$

$$\begin{aligned}
&(x^5 + 3x^4 + 6x^2 + 2x + 1)(6x^4 + 3x^3 + x^2 + x + 5) = \\
&6x^9+3x^8+x^7+x^6+5x^5+4x^8+2x^7+3x^6+3x^5+x^4+x^6+4x^5+6x^4+6x^3+2x^2+ \\
&5x^5 + 6x^4 + 2x^3 + 2x^2 + 3x + 6x^4 + 3x^3 + x^2 + x + 5 = \\
&6x^9 + (3 + 4)x^8 + (1 + 2)x^7 + (1 + 3 + 1)x^6 + (5 + 3 + 4 + 5)x^5+ \\
&(1 + 6 + 6 + 6)x^4 + 6 + (2 + 3)x^3 + (2 + 2 + 1)x^2 + (3 + 1)x + 5 = \\
&6x^9 + 3x^7 + 5x^6 + 3x^5 + 5x^4 + 4x^3 + 3x^2 + 5x + 5.
\end{aligned}$$

To get the additive inverse of a polynomial, we simply replace every coefficient with its additive inverse:

$$-p_1(x) = 6x^5 + 4x^4 + x^2 + 5x + 6,$$

$$-p_2(x) = x^4 + 4x^3 + 6x^2 + 6x + 2.$$

Dividing with remainder, we get

$$p_1(x) = p_2(x)(6x + 1) + (5x^3 + 6x^2 + 6x + 3).$$

Exercise 3. *Let*

$$M = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

be an arbitrary 3-by-3 matrix. Consider e.g. the product

$$MI = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}.$$

Suppose we want to compute the value of F. By the definition of matrix multiplication, since F is on the second row and third column, we take the second row of M, viz. (def), and the third column of I, viz. (001), and compute $F = d \cdot 0 + e \cdot 0 + 1 \cdot f = f$. In the same way, we can verify that $A = a$, $B = b$, etc., and hence $MI = M$. In the same way, one can verify that $IM = M$ as well.

2. We have e.g.

$$A + B = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 & 2 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 0 & 3 \\ 4 & 2 & 0 \end{pmatrix}.$$

3. We have e.g.

$$AB = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 & 2 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}.$$

To compute e.g. A (which is on the first row and first column), we take the first row of A, and combine it with the first column of B:

$$A = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 2 = 2$$

Similarly, we have

$$B = 1 \cdot 2 + 0 \cdot 0 + 1 \cdot 1 = 3$$

$$C = 1 \cdot 2 + 0 \cdot 2 + 1 \cdot 0 = 2$$

$$D = 2 \cdot 0 + 0 \cdot 1 + 1 \cdot 2 = 2$$

$$E = 2 \cdot 2 + 0 \cdot 0 + 1 \cdot 1 = 5$$

$$F = 2 \cdot 2 + 0 \cdot 2 + 1 \cdot 0 = 4$$

$$G = 2 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 = 1$$

$$H = 2 \cdot 2 + 1 \cdot 0 + 0 \cdot 1 = 4$$

$$I = 2 \cdot 2 + 1 \cdot 2 + 0 \cdot 0 = 6$$

so that

$$AB = \begin{pmatrix} 2 & 3 & 2 \\ 2 & 5 & 4 \\ 1 & 4 & 6 \end{pmatrix}.$$

4. The additive inverse of a matrix is obtained by simply replacing all of its elements with their additive inverses; for instance, we get

$$-A = \begin{pmatrix} -1 & 0 & -1 \\ -2 & 0 & -1 \\ -2 & -1 & 0 \end{pmatrix}.$$

Exercise 4. *The computations here are exactly the same as in the previous exercise, except one has to modulate numbers larger than 5 or smaller than 0. In this case, we have e.g.*

$$A + B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 0 & 3 \\ 4 & 2 & 0 \end{pmatrix}$$

and

$$AB = \begin{pmatrix} 2 & 3 & 2 \\ 2 & 0 & 4 \\ 1 & 4 & 1 \end{pmatrix}.$$

Exercise 5. *We prove the statement by induction on k, the number of the terms in the expression. From Theorem 1.46, we already know that the statement is true for $k = 2$. Let us assume that we know the statement is true is for all k from 1 up to some l and we want to prove that it is true for $l+1$. We can write*

$$(a_1 + a_2 + a_3 + \cdots + a_l + a_{l+1})^{p^n} = (\underbrace{(a_1 + a_2 + \cdots + a_l)}_{A} + \underbrace{a_{l+1}}_{B})^{p^n}.$$

Since we know that the statement is true for $k = 2$ terms, we can apply it to $(A+B)^{p^n}$ above to get

$$(A+B)^{p^n} = A^{p^n} + B^{p^n} = (a_1 + a_2 + \cdots + a_l)^{p^n} + a_{l+1}^{p^n}.$$

But since the statement is true for l, we know that

$$(a_1 + a_2 + \cdots + a_l)^{p^n} = a_1^{p^n} + a_2^{p^n} + \cdots + a_l^{p^n}$$

and hence

$$(a_1 + a_2 + a_3 + \cdots + a_l + a_{l+1})^{p^n} = a_1^{p^n} + a_2^{p^n} + \cdots + a_l^{p^n} + a_{l+1}^{p^n}$$

which justifies the induction step and completes the proof.