NMAI057 – Linear algebra 1

Tutorial 7

Fields

Date: November 10, 2021 TA: Denys Bulavka

Problem 1. Simplify the following expressions:

(a) $((2^{-1}+1)4)^{-1}, 4/3$ over $\mathbb{Z}_5$,

(b) $6+7, -7, 6\cdot 7, 7^{-1}, 6/7$ over $\mathbb{Z}_{11}$.

<u>Solution</u>:

(a) The finite field $\mathbb{Z}_5$ is defined as the set of all residues in $\mathbb{Z}$ after division by 5 together with the operations of addition and multiplication modulo 5. Performing addition modulo 5 is straightforward. For the remaining operations in $\mathbb{Z}_5$, we use the multiplication table modulo 5:

$\mathbb{Z}_5, \cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that we can see that the set $\mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ together with multiplication modulo 5 is a group – the so-called multiplicative group modulo 5. This is not surprising as the definition of a field requires that $\mathbb{T}$ with the addition operation $+$ and multiplication operation $\cdot$ on $\mathbb{T}$ satisfy i) distributivity of addition and multiplication, ii) that $(\mathbb{T},+)$ is a group with neutral element 0, and iii) that $(\mathbb{T}\setminus\{0\},\cdot)$ is also a group. It is the property iii) that we see in the above multiplication table.

In order to simplify the expressions over $\mathbb{Z}_5$, we find the multiplicative inverses using the multiplication table as follows. For any $a \in \mathbb{Z}_5 \setminus \{0\}$, we find in the corresponding row the element 1 and the column index b must be the multiplicative inverse a^{-1} of a since $a \cdot b = 1$ in $\mathbb{Z}_5$. We get:

$$((2^{-1}+1)4)^{-1} = ((3+1)4)^{-1} = (4\cdot 4)^{-1} = (1)^{-1} = 1 \text{ in } \mathbb{Z}_5$$

and

$$4/3 = 4\cdot 3^{-1} = 4 \cdot 2 = 3 \text{ in } \mathbb{Z}_5.$$

(b) We proceed similarly as for $\mathbb{Z}_5$ but we will not construct the whole multiplication table for $\mathbb{Z}_{11}$. We get

$$\begin{aligned} 6+7 &= 6+7 \pmod{11} = 2 \text{ in } \mathbb{Z}_{11}, \\ -7 &= 11-7 \pmod{11} = 4 \text{ in } \mathbb{Z}_{11}. \\ 6\cdot 7 &= 6\cdot 7 \pmod{11} = 42 \pmod{11} = 9 \text{ in } \mathbb{Z}_{11}. \end{aligned}$$

When computing the multiplicative inverse of 7, we can proceed as when constructing the row of the multiplication table modulo 11 corresponding to 7. However, we stop the computation in the moment when we see the element 1:

$$\begin{aligned} 7\cdot 1 &= 7, \\ 7\cdot 2 &= 3, \\ 7\cdot 3 &= 10, \\ 7\cdot 4 &= 6, \\ 7\cdot 5 &= 2, \\ 7\cdot 6 &= 9, \\ 7\cdot 7 &= 5, \\ 7\cdot 8 &= 1. \end{aligned}$$

Thus,

$$7^{-1} = 8 \text{ in } \mathbb{Z}_{11}.$$

We use this value also when simplifying the last expression:

$$6/7 = 6\cdot 7^{-1} = 6\cdot 8 = 48 \pmod{11} = 4 \text{ in } \mathbb{Z}_{11}.$$

Problem 2. Over $\mathbb{Z}_5$, find the set of all solutions of the system

$$\begin{aligned} 3x+2y+z &= 1 \\ 4x+y+3z &= 3 \end{aligned}$$

and compute its cardinality.

Solution:

We proceed as for systems over $\mathbb{R}$ but we use the appropriate arithmetic. Moreover, we can use the ability to eliminate elements in the column below the current pivot via adding an appropriate multiple of the row with pivot to the rows below it. By adding the first row multiplied by 2 to the second row, we get

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 4 & 1 & 3 & 3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 3 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) .$$

We set the free variables to parameters $y, z \in \mathbb{Z}_5$ and express

$$x = 3^{-1}(1-2y-z) = 2(1+3y+4z) = 2+y+3z \ .$$

Thus, the solution set of the system is

$$\{(2,0,0)^T + y(1,1,0)^T + z(3,0,1)^T \mid y,z \in \mathbb{Z}_5\} .$$

There are $25 = 5 \cdot 5$ possible choices for the values of the parameters y a z, and the cardinality of the solution set is 25.

Problem 3. Find the multiplicative inverses 9^{-1} and 12^{-1} in $\mathbb{Z}_{31}$.

Solution:

We could proceed as for $\mathbb{Z}_{11}$ but the computation might take 31 steps in case we would have to compute the whole row for 9 in the multiplication table modulo 31. There is a more efficient method exploiting the extended Euclidean algorithm. The output of the extended Euclidean algorithm is the $\mathrm{GCD}(9,31)$ together with a pair of integer values $a, b \in \mathbb{Z}$ such that

$$1 = \mathrm{GCD}(9,31) = a \cdot 9 + b \cdot 31 .$$

Thus, we can use $a \pmod{31}$ as the multiplicative inverse of 9 in $\mathbb{Z}_{31}$. On input $(9,31)$, the extended Euclidean algorithm will perform the following steps:

$$\begin{aligned}
a_0 &= 31,\\
a_1 &= 9,\\
a_2 &= 4 = 31 - 3 \cdot 9,\\
a_3 &= 1 = 9 - 2 \cdot 4 = 7 \cdot 9 - 2 \cdot 31.
\end{aligned}$$

The final value a_3 is the $\mathrm{GCD}(9,31)$ (which we knew to be equal to 1 since 31 is a prime). Moreover, we have expressed 1 as a sum of integer multiples of 9 and 31. We can derive that

$$1 = 7 \cdot 9 - 2 \cdot 31 = 7 \cdot 9 - 2 \cdot 31 \pmod{31} = 7 \cdot 9 \pmod{31} .$$

Thus, $9^{-1} = 7$ in $\mathbb{Z}_{31}$.

For 12, we get:

$$\begin{aligned}
a_0 &= 31,\\
a_1 &= 12,\\
a_2 &= 7 = 31 - 2 \cdot 12,\\
a_3 &= 5 = 12 - 7 = 3 \cdot 12 - 31,\\
a_4 &= 2 = 7 - 5 = 31 - 2 \cdot 12 - 3 \cdot 12 + 31 = 2 \cdot 31 - 5 \cdot 12,\\
a_5 &= 3 = 5 - 2 = 3 \cdot 12 - 31 - 2 \cdot 31 + 5 \cdot 12 = 8 \cdot 12 - 3 \cdot 31,\\
a_6 &= 1 = 3 - 2 = 8 \cdot 12 - 3 \cdot 31 - 2 \cdot 31 + 5 \cdot 12 = 13 \cdot 12 - 5 \cdot 31.
\end{aligned}$$

Again, we have expressed 1 as a sum of integer multiples of 12 and 31. We can derive that

$$1 = 13 \cdot 12 - 5 \cdot 31 = 13 \cdot 12 - 5 \cdot 31 \pmod{31} = 13 \cdot 12 \pmod{31} .$$

Thus, $12^{-1} = 13$ in $\mathbb{Z}_{31}$.

Problem 4. Over $\mathbb{Z}_7$, compute the matrix power A^{100} for $A = \left(\begin{smallmatrix} 3 & 2 \\ 1 & 4 \end{smallmatrix}\right)$.

Solution:

Note that the sequence of matrices A^i for $i = 1, \dots, \infty$ must be cyclic when computed over a finite field. We compute some of the initial terms of this sequence:

$$\begin{aligned}
A = A^1 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} , \\
A^2 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} , \\
A^3 &= \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} , \\
A^4 &= \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} , \\
A^5 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} , \\
A^6 &= \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \\
A^7 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = A .
\end{aligned}$$

We see that the period of the sequence is 6 over $\mathbb{Z}_7$. Thus,

$$A^{100} = A^{100 \pmod 6} = A^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} .$$

Problem 5. For $n \in \mathbb{N}$ and an asociative operation $\cdot$ let $a^n = a \cdot a \cdot \ldots \cdot a$, where the element a appears n times in the product.

- Determine values $2^{101}, 3^{1\,001}$ and $4^{1\,000\,001}$ in the field $\mathbb{Z}_{17}$.
- Determine $5^{100}, 8^{200}, 11^{300}$ and 18^{400} in the field $\mathbb{Z}_{19}$.

Problem 6. Solve the following system of equations over $\mathbb{Z}_5, \mathbb{Z}_7$ and $\mathbb{R}$.

$$\begin{array}{rcrcrcl}
x_1 & + & 2x_2 & + & 4x_3 & = & 3 \\
3x_1 & + & x_2 & + & 2x_3 & = & 4 \\
2x_1 & + & 4x_2 & + & x_3 & = & 3
\end{array}$$

Problem 7. Invert the following matrices over fields $\mathbb{Z}_3$ and $\mathbb{Z}_5$

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

- $\mathbf{C} = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.
- $\mathbf{D} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$.
- $\mathbf{E} = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 1 & 2 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 2 & 0 & 0 \end{pmatrix}$.

Problem 8. Invert the following matrix over $\mathbb{Z}_{11}$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Problem 9. Find a matrix $\mathbf{A}$, that over $\mathbb{Z}_5$ satisfies

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