2022 FALL MATH 5310 HOMEWORK 5 SOLUTIONS
DUE: SEP 26TH

SANGHOON KWAK

Question 1 (Artin 3.1.2)**.** Find the inverse of 5 modulo p, for $p = 7, 11, 13$ and 17.

Solution.

$$5^{-1} \equiv 3 \mod 7, \qquad 5^{-1} \equiv 9 \mod 11, \qquad 5^{-1} \equiv 8 \mod 13, \qquad 5^{-1} \equiv 7 \mod 17. \quad //$$

Question 2 (Artin 3.1.4)**.** Consider the system of linear equations $\begin{bmatrix} 6 & -3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$.

(a) Solve the system in $\mathbb{F}_p$ when $p = 5, 11$ and 17.
(b) Determine the number of solutions when $p = 7$.

Solution. (a) Note that we can get the inverse of the coefficient matrix using the formula:

$$\begin{bmatrix} 6 & -3 \\ 2 & 6 \end{bmatrix}^{-1} = ((6)(6) - (-3)(2)) \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix} = (42)^{-1} \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix},$$

where $(42)^{-1}$ is the multiplicative inverse in $\mathbb{F}_p$. Since all $5, 11, 17$ are relatively prime to 42, the inverse exists. Therefore, the solution of the system is:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = (42)^{-1} \begin{bmatrix} 6 & 3 \\ -2 & 6 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = (42)^{-1} \begin{bmatrix} 21 \\ 0 \end{bmatrix},$$

which is $\begin{bmatrix} 3 \\ 0 \end{bmatrix}$ in $\mathbb{F}_5$, $\begin{bmatrix} 6 \\ 0 \end{bmatrix}$ in $\mathbb{F}_{11}$, and $\begin{bmatrix} 9 \\ 0 \end{bmatrix}$ in $\mathbb{F}_{17}$.

(b) Note that 42 has no inverse in $\mathbb{F}_7$. Indeed, the system is dependent:

$$\begin{bmatrix} 6 & -3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix} \qquad \overset{\text{mod } 7}{\equiv} \qquad \begin{bmatrix} -1 & -3 \\ 2 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} -4 \\ 8 \end{bmatrix},$$

so any pair of $(x_1, x_2) \in \mathbb{F}_7 \times \mathbb{F}_7$ satisfying $x_1 + 3x_2 = 4$ is a solution. Therefore, there are 7 solutions to this system when $p = 7$.

//

Question 3 (Artin 3.1.5)**.** Determine the primes p such that the matrix

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & -1 \\ -2 & 0 & 2 \end{bmatrix}$$

is invertible, when its entries are considered to be in $\mathbb{F}_p$.

Solution. Recall a matrix is invertible if and only if its determinant is multiplicative invertible in $\mathbb{F}_p$. Computing the determinant of A, we get $\det A = 10$, so A is invertible if and only if $p \neq 2, 5$. //

Question 4 (Artin 3.1.6)**.** Solve completely the systems of linear equations $AX = 0$ and $AX = B$, where

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}, \qquad \text{and} \qquad B = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$$

(a) in $\mathbb{Q}$,
(b) in $\mathbb{F}_2$,
(c) in $\mathbb{F}_3$,
(d) in $\mathbb{F}_7$.

Solution. First, using the formula for matrix inverse, we get

$$A^{-1} = 3^{-1} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix},$$

so we can conclude A^{-1} exists only in $\mathbb{Q}$, $\mathbb{F}_2$, and $\mathbb{F}_7$. Using this, the solutions for (a), (b), (d) are: $X = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}^T$ for $AX = 0$, and $X = \begin{bmatrix} \frac{1}{3} & \frac{2}{3} & -\frac{4}{3} \end{bmatrix}^T$, $X = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^T$, and $X = \begin{bmatrix} 5 & 3 & 1 \end{bmatrix}^T$ for $AX = B$ of (a), (b), and (d) respectively.

For (c), setting the augmented matrix from the given systems $AX = 0$ and $AX = B$ we get:

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 \end{array}\right] \qquad \text{and} \qquad \left[\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right]$$

respectively. Reducing those into row echelon form:

$$\left[\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \qquad \text{and} \qquad \left[\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 2 \end{array}\right].$$

Therefore, the solutions for $AX = 0$ for (c) are: $(0, 0, 0), (2, 1, 1)$ and $(1, 2, 2)$ but $AX = B$ has no solution. //

Question 5 (Artin 3.2.2)**.** Which of the following subsets is a subspace of the vector space $F^{n \times n}$ of $n \times n$ matrices with coefficients in F?

(a) symmetric matrices ($A = A^t$),
(b) invertible matrices,
(c) upper triangular matrices.

Solution. (a) Yes, as the zero matrix is symmetric, and the transpose operation commutes with addition and scalar multiplication.
(b) No, as the zero matrix is not invertible.
(c) Yes, as the zero matrix is upper triangular, and being upper triangular is closed under addition and scalar multiplication. //

Question 6 (Bonus; Artin 3.1.11)**.** Prove that the set of symbols $\{a + bi | a, b \in \mathbb{F}_3\}$ forms a field with nine elements, if the laws of composition are made to mimic addition and multiplication of complex numbers. Will the same method work for $\mathbb{F}_5$? For $\mathbb{F}_7$? Explain.

Proof. The key idea is that every nonzero element of $C_p\{a + bi | a, b, \in \mathbb{F}_p\}$ is invertible under multiplication if and only if p does not divide $a^2 + b^2$ for every $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p \setminus (0, 0)$. This is because $(a + bi)(a - bi) = a^2 + b^2$, so

$$(a + bi)^{-1} = (a^2 + b^2)^{-1}(a - bi).$$

When $p = 3$, we have $x^2 \equiv 0, 1 \mod 3$ so 3 divides $a^2 + b^2$ if and only if both a, b are divisible by 3. This means that for every $(a, b) \neq (0, 0)$, $a^2 + b^2$ is not divisible by 3, so the set C_3 forms a field.

When $p = 5$, this fails as 5 divides $1^2 + 2^2 = 5$, so in particular $1 + 2i$ is not invertible.

When $p = 7$, we have $x^2 \equiv 0, 1, 2, 4 \mod 7$, so 7 divides $a^2 + b^2$ if and only if $a \equiv b \equiv 0 \mod 7$. Therefore, for every $(a, b) \neq (0, 0)$, $a^2 + b^2$ is not divisible by 7, so the set C_7 forms a field. $\square$