These are notes for a *second* course in linear algebra. It is presumed that you are comfortable with (at least)

1. How to multiply and add matrices
2. How to represent systems of linear equations using matrices
3. How to find the row reduced echelon form and rank of a matrix
4. How to use the row reduced echelon form to solve a system of equations
5. The structure of the set of solutions to a system of equations
6. What it means for a matrix to be invertible and how to tell if one is from the row reduced echelon form
7. How to use the inverse of a matrix to solve a system of linear equations

We will (very) briefly review these concepts and the computations behind them. However, if you have not seen these before, you should learn them thoroughly before taking on these notes.

A typical *first* course in linear algebra will cover all of these topics and more. The other topics will also help with this course, but will generally find greater and more in depth coverage here. While it is not as essential that you remember them now, nevertheless, it would help to also know

1. How to compute determinants of square matrices
2. How to find the eigenvalues and eigenvectors of a square matrix, or determine that they don't exist
3. How to determine if a matrix is diagonalizable, and, if it is, how to diagonalize it.

We will review these concepts as we encounter them.

## 1. Systems of linear equations - Review

Recall that a system of linear equations is a set of equations such as

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m &= b_2 \\ \vdots \qquad\qquad & \quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m &= b_n \end{aligned}$$

where $n$ and $m$ are positive integers, the $x_i$ are variables, and the $a_{ij}$ and $b_i$ are constants. The equations are taken to be ordered as a first equation, second equation, and so forth, where the $i^{th}$ equation has coefficients $a_{ij}$. To solve a system of linear equations is to find values for $x_1, \ldots, x_m$ which make all the equations true simultaneously.

**Example 1:** We wish to find $a, b, c, d, e$ so that

$$\begin{aligned} 3\,a + 0\,b + 0\,c + 1\,d + 1\,e &= 0 \\ -\,a + 1\,b + 1\,c + 0\,d + 1\,e &= 0 \\ -2\,a + 0\,b + 0\,c + 0\,d - 2\,e &= 0 \end{aligned}$$

There are several different ways to solve a system of equations, depending on the structure of the system. We will review Gaussian Elimination here, as it will be the only method we will need.

The idea behind Gaussian elimination is to replace the system you start with by an *equivalent* system which you can solve easily, where

**Definition 1** (Informal)**.** *Two systems of linear equations are equivalent if they have the same set of solutions.*

There are several operations we can perform on a system of linear equations which will produce a different, but equivalent, system of equations:

(1) Multiplying the coefficients (and $b_i$) of the $i^{th}$ row by a *non-zero* number $\lambda$
(2) Switching the $j^{th}$ equation with the $i^{th}$ equation, and
(3) Adding the $i^{th}$ equation to the $j^{th}$ equation

Note that each of these operations is reversible: to reverse the first we divide the same equation by $\lambda \neq 0$; to reverse the second, switch the equations back; to reverse the third, subtract the $i^{th}$ equation (which is unchanged) from the new $j^{th}$ equation.

While these operations always yield an equivalent system, it isn't clear that all equivalent systems of equations can be joined by a sequence of these operations. Can they? We'll answer this later.

Since the coefficients of the system (and the $b_i$) are all that define the system, we only need to keep track of what happens to the coefficients. Thus, in Math 237 we introduce the (augmented) matrix for the system of equations:

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1m} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2m} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nm} & b_n \end{array}\right]$$

Recall that a matrix with $n$ rows and $m$ columns is an $n \times m$ matrix.

The operations on systems above have corresponding operations on the augmented matrices. In the same order, these operations correspond to

(Type I) Replacing the each entry $a_{ik}$ in the $i^{th}$ row by $\lambda a_{ik}$ for some *non-zero* number $\lambda$
(Type II) Switching the $j^{th}$ row with the $i^{th}$ row, and
(Type III) Replacing the entry $a_{jk}$ by $a_{ik} + a_{jk}$ for some $i$ and $j$.

As above these operations are reversible. Matrices that can be obtained, one from the other, by a sequence of these operations are called *row equivalent*.

The basic result of an elementary linear algebra class – the one upon which most everything else is based – is that each matrix is row equivalent to one in row-reduced echelon form. Intuitively, a matrix is in echelon form if the first non-zero entry in each row occurs to the left of the first non-zero entries of the rows below it. Formally,

**Definition 2.** *An $n \times m$ matrix $\mathbf{M}$ is in row-reduced echelon form (RREF) if*

a) *there is a number $0 \leq k \leq \min\{n, m\}$, called the* rank *of $\mathbf{M}$, and*
b) *if $k > 0$, columns $1 \leq i_1 < i_2 < \cdots < i_k \leq m$*

*such that*

1) *The entry $a_{r\,i_r}$ is called a* pivot.
2) *If $a_{rs} \neq 0$ then there is a pivot $a_{ij}$ with $i \geq r$ and $j \leq s$.*

**Definition 3.** *An $n \times m$ matrix $\mathbf{M}$ is in row-reduced echelon form (RREF) if*

*there is a number $0 \leq k \leq \min\{n, m\}$, called the* rank *of $\mathbf{M}$,*

*such that*

1) *The entries in the rows after the $k^{th}$ are all $0$'s: $a_{ij} = 0$ for $i > k$ and any $j$.*
2) *For each $r \in \{1, \ldots, k\}$, the first non-zero entry, called a* pivot, *equals $1$. That is, there is a number $i_r \in \{1, \ldots, m\}$ such that $a_{rj} = 0$ for $j < i_r$ and $a_{r\,i_r} = 1$.*
3) *The numbers $i_r$ satisfy $1 \leq i_1 < i_2 < \cdots < i_k \leq m$, when $k > 0$,*
4) *For each $r \in \{1, \ldots, k\}$, the entries in the $i_r^{th}$ column other than $a_{r\,i_r} = 1$* all *equal $0$.*

**(Question 1.1)** This definition is hard to digest. Verify that the conditions require that the pivots occur in a "staircase" pattern where each pivot occurs the right of the pivots in the rows above it, and that all the entries the the left and below a pivot are equal to 0.

**Example 1 (cont.):** The system of equations above has augmented matrix:

$$\left[\begin{array}{ccccc|c} 3 & 0 & 0 & 1 & 1 & 0 \\ -1 & 1 & 1 & 0 & 1 & 0 \\ -2 & 0 & 0 & 0 & -2 & 0 \end{array}\right]$$

We perform the following operations (where $R2$ is row 2):

(1) Divide $R1$ by 3: $R1 \longleftarrow \frac{1}{3}R1$
(2) Add (the new) $R1$ to $R2$: $R2 \longleftarrow R1 + R2$
(3) Add $2R1$ to $R3$: $R3 \longleftarrow 2\,R1 + R3$

to get the matrix

$$\left[\begin{array}{ccccc|c} 1 & 0 & 0 & 1/3 & 1/3 & 0 \\ 0 & 1 & 1 & 1/3 & 4/3 & 0 \\ 0 & 0 & 0 & 2/3 & -4/3 & 0 \end{array}\right]$$

This isn't in RREF yet since the first entry in the third row isn't equal to 1, and the entries above it in the same column aren't zeros. So we proceed:

(1) $R3 \longleftarrow \frac{3}{2}R3$
(2) $R2 \longleftarrow R2 - \frac{1}{3}R3$
(3) $R1 \longleftarrow R1 - \frac{1}{3}R3$

to get the following matrix in RREF (with pivots boxed for emphasis)

$$\left[\begin{array}{ccccc|c} \boxed{1} & 0 & 0 & 0 & 1 & 0 \\ 0 & \boxed{1} & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & \boxed{1} & -2 & 0 \end{array}\right]$$

which corresponds to the equivalent system:

$$\begin{aligned} a + e &= 0 \\ b + c + 2e &= 0 \\ d - 2e &= 0 \end{aligned}$$

We can solve for the variable corresponding to the pivot columns: $a = -e$, $b = -c - 2e$ and $d = 2e$. Thus,

$$\begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \alpha \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} -1 \\ -2 \\ 0 \\ 2 \\ 1 \end{bmatrix}$$

Thus there are an infinite set of solutions to this equation.

**Example 2:** This time we wish to solve for $a, b, c$ in a system of linear equations with augmented matrix

$$\left[\begin{array}{ccc|c} 2 & -3 & 1 & 3 \\ 1 & 1 & 0 & 0 \\ -2 & 0 & -2 & 0 \end{array}\right]$$

**(Question 1.2)** Show that this matrix has RREF

$$\left[\begin{array}{ccc|c} \boxed{1} & 0 & 0 & 3/4 \\ 0 & \boxed{1} & 0 & -3/4 \\ 0 & 0 & \boxed{1} & -3/4 \end{array}\right]$$

and thus the only solution is $a = 3/4$, $b = -3/4$, and $c = -3/4$.

We make a few observations (which, ignoring differences in notation and description, should just be review!):

(1) The vertical line in an augmented matrix is there to identify the coefficients ($a_{ij}$'s) from the constants ($b_i$'s) and serves no other purpose. The matrix of coefficients is the matrix to the

left of the line:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix}$$

If we let

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} \qquad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Then solving the system of linear equations is the same as solving the matrix equation

$$\mathbf{Ax} = \mathbf{b}$$

for the vector $\mathbf{x}$ given the matrix $\mathbf{A}$ and the vector $\mathbf{b}$ (where the multiplication $\mathbf{Ax}$ is matrix multiplication).

(2) When we use row operations to convert the augmented matrix $[\mathbf{A}|\mathbf{b}]$ into a matrix in RREF from, the part of the new matrix to the left of the line is a matrix in RREF which results from applying the same operations to the coefficient matrix $\mathbf{A}$.

(3) If we convert the augmented matrix $[\mathbf{A}|\mathbf{b}]$ into a matrix in RREF form, and the last column contains a pivot, the system has no solutions[1]. Indeed, if there is a pivot in the last column, then there there is a row of the RREF matrix from $\mathbf{A}$ consisting only of 0's but for which the entry to the right of $|$ is 1. This corresponds to a system including the equation $0 = 1$, and thus has no solution.

(4) However, if we convert the augmented matrix $[\mathbf{A}|\mathbf{b}]$ into a matrix in RREF form, and the last column of the resulting matrix is not a pivot column, then the system has at least one solution. Suppose after applying row operations to $[\mathbf{A}|\mathbf{b}]$ we get an RREF matrix $[\mathbf{A}'|\mathbf{c}]$ and there is no pivot in the last column. Suppose further that the $j_1, \ldots, j_l^{th}$ columns of $\mathbf{A}'$ are all its *non-pivot* columns, for some $l > 0$. Then every solution to the set of equations has the form

$$\mathbf{x} = \mathbf{C} + \alpha_1 \mathbf{k}_1 + \cdots + \alpha_l \mathbf{k}_l$$

where $\mathbf{C}$ is a vector computed from $\mathbf{c}$, the $\alpha_i$ are each numbers, and each $\mathbf{k}_r$ is a vector which satisfies $\mathbf{Ak}_r = \mathbf{0}$ (i.e. solves the *homogeneous equation* for $\mathbf{A}$) *and* has $j_r^{th}$ entry equal to 1, while all higher entries are 0. (This is the situation in Example 1!)

(5) Furthermore, if every column in $\mathbf{A}'$ (from the preceding item) is a pivot column then there can be at most one solution. This is the situation in Example 2.

(6) For the system $\mathbf{Ax} = \mathbf{b}$ to have a single solution for *every* $\mathbf{b}$, the preceding entries require that 1) every column in the RREF matrix from $\mathbf{A}$ contain a pivot, and 2) every row in that matrix also contains a pivot. The latter ensures that a pivot never occurs in the last column of the RREF matrix from $[\mathbf{A}|\mathbf{b}]$, since for each row there must be a pivot to the left of the dividing line. Thus, the number of rows and columns must equal the number of pivots, and so the matrix $\mathbf{A}$ must be a square matrix. Furthermore, the RREF matrix from $A$ must be the $n \times n$ identity matrix $\mathbf{I}_n$, as it is the only RREF matrix with a pivot in every row and column.

[1] some would say the system is *inconsistent*

In this case, there is a matrix $\mathbf{A}^{-1}$ such that $\mathbf{A}^{-1}\mathbf{A} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{I}_n$ and we can use matrix multiplication to compute the unique solution to $\mathbf{A}\mathbf{x} = \mathbf{b}$ via $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$. So in this case, the homgeneous equations $\mathbf{A}\mathbf{x} = \mathbf{0}$ has only $\mathbf{0}$ as a solution.

We say $\mathbf{A}$ is invertible and $\mathbf{A}^{-1}$ is its inverse.

**Example 3:** Now let's consider how to solve the following system of equations, whose coefficients come from the complex numbers $\mathbb{C}$:

$$\begin{aligned} 2z_1 + (1+i)z_2 - 10i\, z_3 &= 10i \\ z_1 + 2i\, z_2 + 30z_3 &= 30 + 10i \\ (2+i)z_1 + (-1+i)z_2 + 20i\, z_3 &= -10 + 40\, i \end{aligned} \quad \Longrightarrow \left[\begin{array}{ccc|c} 2 & 1+i & -10\, i & 10\, i \\ 1 & 2i & 30 & 30 + 10\, i \\ 2+i & -1+i & 20\, i & -10 + 40\, i \end{array}\right] \tag{1}$$

How can we solve this system over $\mathbb{C}$? That is, what are the solutions when we allow the $z_i$ to be complex[2]? Can we simply follow the previous procedure?

Before we proceed, lets **(Re-)View the complex numbers:** The complex numbers are an extension of the real numbers that include numbers whose squares are negatives. In particular, we add a number $i$ with $i^2 = -1$. In order for this to work, we will need to be able to multiply any two numbers together, such as $b \in \mathbb{R}$ and $i$, so there must be numbers $b\, i$. Furthermore, we must be able to add any two numbers, so there must be numbers of the form $a + b\, i$ when $a \in \mathbb{R}$. For numbers of this form, we add and multiply like usual, remembering that $i^2 = -1$:

$$(2 - 3i) + (-1 + 7i) = (2 - 1) + (-3 + 7)\, i = 1 + 4\, i$$

$$\begin{aligned} (1 + 2\, i)(\sqrt{2} - 3\, i) &= (\sqrt{2} - 3\, i) + 2\, i(\sqrt{2} - 3\, i) \\ &= \sqrt{2} - 3\, i + 2\sqrt{2}\, i - 6\, i^2 \\ &= \sqrt{2} - 3\, i + 2\sqrt{2}\, i + 6 \\ &= (\sqrt{2} + 6) + (2\sqrt{2} - 3)\, i \end{aligned}$$

which has the form $a + b\, i$ for the real numbers $a = 6 + \sqrt{2}$ and $b = 2\sqrt{2} - 3$.

**(Question 1.3)** Compute $i^n$ for $n = 0, 1, 2, 3, 4, 5, 6, \ldots$.

**(Question 1.4)** Let $1 = 1 + 0\, i$ and $0 = 0 + 0\, i$. Show that these behave like usual: that is if $z = a + b\, i$ is a complex number, then $1 \cdot z = z$ and $0 + z = z$

.

**(Question 1.5)** Verify that $\begin{bmatrix} 10\, i \\ 0 \\ 1 \end{bmatrix}$ is a solution to the system in (**??**).

**(Question 1.6)** Let $z = a + b\, i$ and $w = c + d\, i$ where $a, b, c, d \in \mathbb{R}$. Verify that

$$z + w = (a + c) + (b + d)i$$

and

$$z \cdot w = (ac - bd) + (ad + bc)\, i$$

[2] It is customary to use "z" for a variable that can be a complex number

**Theoretical note:** This doesn't actually define the complex numbers because saying that they are the set of all $a + b\,i$ presupposes that we know what $i$. Saying that $i^2 = -1$ doesn't define $i$ since there is no real number has this property (that's why it was historically derided as "imaginary"). To define the complex number $\mathbb{C}$ we should only use the real numbers and sets theory. One way to formally define the complex numbers is

**Definition 4.** *The complex numbers* $\mathbb{C}$ *is the set* $\mathbb{R}^2 = \{\, (a, b) \mid a, b \in \mathbb{R} \,\}$ *equipped with the following addition and multiplication*

$$(a, b) + (c, d) = (a + c, b + d)$$

*and*

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

*The complex number* $(0, 1)$ *is denoted by* $i$*. Numbers of the form* $(a, 0)$ *are called* real*, while numbers of the form* $(0, b)$ *are called* imaginary *The* real *part of* $z = (a, b)$ *is the real number* $\operatorname{Re} z = (a, 0)$*, while the imaginary part of* $z$ *is* $\operatorname{Im} z = (0, b)$*.*

Let's verify that it captures what we wanted:

**(Question 1.7)** Show that $(a, b) = (a, 0) + (b, 0) \cdot (0, 1)$ using the rules above.

We write the expression $(a, 0) + (b, 0) \cdot (0, 1)$ as $a + b\,i$.

**(Question 1.8)** Using this notation, explain why numbers of the form $(a, 0)$ are called *real* and how this is related to the real numbers. Explain why $(a, 0)$ is called the real part of $z = a + b\,i$.

After seeing this correspondence, we also see that the multiplication and addition in the definition are lifted directly from the computation of the multiplication and addition using $a + b\,i$ and $c + d\,i$.

The identification of $\mathbb{C}$, as a set[3] with $\mathbb{R}^2$ gives us a way to depict elements of $\mathbb{C}$ as ordered pairs in the plane. Using the distance formula, we can define the magnitude for the complex number $z = a + b\,i$ as the distance (a real number!) from $(0, 0)$ to $(a, b)$:

$$|z| = \sqrt{a^2 + b^2}$$

This is sometimes also called the *modulus* of $z$.

**(Question 1.9)** Plot the real and imaginary complex numbers in $\mathbb{R}^2$. What are we doing in $\mathbb{R}^2$ when we find real and imaginary parts of a complex number?

**(Question 1.10)** Show that $|a + 0\,i| = |a|$, where the $|\cdot|$ on the right side is the absolute value, as usual for $\mathbb{R}$

We can also consider the complex number which results when we take the mirror image in the real axis (the $x$-axis in $\mathbb{R}^2$): if $z = a + b\,i$ then the conjugate of $z$ is $\overline{z} = a - b\,i$.

**(Question 1.11)** If you know that $z = \overline{z}$, what does it imply about $z$? Can you draw any conclusion from knowing $z = -\overline{z}$? Explain you answers algebraically (that is from the formulas above) and geometrically (that is, using that $z \leftrightarrow \overline{z}$ is a reflection in the real axis)

**(Question 1.12)** Show, algebraically, that

[3] that is, ignoring the multiplication

(1) $\overline{\overline{z}} = z$ for all $z \in \mathbb{C}$
(2) $\overline{z+w} = \overline{z} + \overline{w}$ for all $z, w \in \mathbb{C}$
(3) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$, for all $z, w \in \mathbb{C}$
Then verify (1) and (2) geometrically as well.

**(Question 1.13)** Show that the product $z\overline{z}$ equals $|z|^2 = a^2+b^2$, and thus equals 0 only if $z = 0+0\,i$.

This last property of the conjugate allows us to find a multiplicative inverse for any non-zero complex number by multiplying by the conjugate divided by the conjugate. We illustrate with an example:

$$\begin{aligned}(2-3i)^{-1} &= \frac{1}{2-3i}\\ &= \left(\frac{1}{2-3i}\right)\left(\frac{2+3i}{2+3i}\right)\\ &= \frac{2+3i}{(2-3i)(2+3i)}\\ &= \frac{2+3i}{2^2+3^2}\\ &= \frac{2}{13} + \frac{3}{13}\,i\end{aligned}$$

**(Question 1.14)** Follow the procedure above to verify

$$\frac{1}{a+b\,i} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\,i$$

when $a + b\,i \neq 0$ (where is this constraint in the formula?)

Now we return to out motivating question. Can we find the solutions to the system of linear equations in (**??**)?

**(Question 1.15)** By repeating the usual row reduction procedure for the system in (**??**), while using the arithmetic of complex numbers, show that we obtain the following matrix in RREF:

$$\left[\begin{array}{ccc|c} 1 & 0 & -8+6\,i & -8+16\,i \\ 0 & 1 & -3-19\,i & -3-19\,i \\ 0 & 0 & 0 & 0 \end{array}\right]$$

and then confirm that the solutions are

$$\begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} -8+16\,i \\ -3-19\,i \\ 0 \end{bmatrix} + \alpha \begin{bmatrix} 8-6\,i \\ 3+19\,i \\ 1 \end{bmatrix}$$

What sort of number can $\alpha$ be?

Since this is exactly the same procedure as in Example 1 and Example 2, we obtain the same conclusions: as long as we allow complex numbers in our matrices all our previous conclusions – about when there are solutions, and whether the solutions are unique, and when a matrix has an inverse – remain true over the complex numbers! We don't need to do any additional work!

Nevertheless, there is a difference in the examples above. In Example 3, the coefficients were complex numbers, but since we can add, substract, multiply and divide complex numbers we were able to solve the system as long as we allow complex numbers in the solutions. In Example 1, the coefficients in the system of linear equations are all integers but the solutions turn out to have all have integer entries when $\alpha$ and $\beta$ are integers. Thus, this system can be solved and understood if we are limited to using integers alone.

However, in Example II, the coefficients are also all integers, but the (only) solution consists of rational numbers. IF WE MUST STAY IN THE INTEGERS THEN THE SYSTEM HAS NO SOLUTION!

In fact, this is the reason for introducing rational numbers historically. The simplest linear equation with integer coefficients is one such as

$$3x = b$$

It can only have an integer solution if $b$ is divisible by 3. Thus $3x = 6$ has a solution, but not because we are dividing by 3. WE still can't divide. Instead, the solution comes from rewriting the equation as $3(x-2) = 0$ and using the fact that the product of two integers is 0 if and only if one of them is 0. When $b$ is not divisible by 3, there is no integer solution. By introducing the rationals we get solutions to all these equations.

Similarly, we can't necessarily find a row reduced echelon form for a matrix of integers, if we aren't ever allowed to divide by integers other than ±1:

$$\begin{bmatrix} 8 & 7 \\ 12 & 5 \end{bmatrix} \overset{R2-R1\to R2}{\longrightarrow} \begin{bmatrix} 8 & 7 \\ 4 & -2 \end{bmatrix} \overset{R1-2\,R2\to R1}{\longrightarrow} \begin{bmatrix} 0 & 11 \\ 4 & -2 \end{bmatrix} \overset{R2,R1\to R1,R2}{\longrightarrow} \begin{bmatrix} 4 & -2 \\ 0 & 11 \end{bmatrix}$$

We can go no further, since we can't divide by 4 or 11.

Here's another, somewhat more complicated example,

**Example 4:** Before we start, we fix some notation. Let

$$\mathbb{Z}/26\mathbb{Z} = \{0, 1, \ldots, 25\}$$

We can equip $\mathbb{Z}/26\mathbb{Z}$ with an addition and a multiplication by using modular arithmetic: that is, take the sum or product of the numbers in the integers, divide by 26, and take the remainder as your result. For example,

(1) Since $19 + 15 = 34$ in the integers, and 34 divide by 26 leaves a remainder of 8, we have $19 + 15 = 8$ in $\mathbb{Z}/26\mathbb{Z}$.
(2) Since $7 \cdot 17 = 119$ in the integers, we have $7 \times 17 = 15$ in $\mathbb{Z}/26\mathbb{Z}$. $(119 = 4 \cdot 26 + 15)$

Since these operations derive from the integers, they have all the same basic properties as addition and multiplication of integers. However, they also have some properties that are different: for example, in $\mathbb{Z}/26\mathbb{Z}$ we can divide by 3.

Dividing by 3 is the same as multiplying by $3^{-1}$ where $3^{-1}$ is the number such that $3 \cdot 3^{-1} = 1$. In $\mathbb{Z}/26\mathbb{Z}$, $3 \cdot 9 = 1$ since 27 leaves a remainder of 1 when divided by 26. Thus, if we wish to solve $3x = 7$ in $\mathbb{Z}/26\mathbb{Z}$, we can do so by multiplying by 9: $x = (9 \cdot 3)x = 9 \cdot (3x) = 9 \cdot 7 = 11$ (since $63 = 2 \cdot 26 + 11$).

Now consider the matrix with entries in $\mathbb{Z}/26\mathbb{Z}$:

$$\mathbf{A} = \begin{bmatrix} 6 & 1 \\ 7 & 6 \end{bmatrix}$$

and multiply vectors with entries in $\mathbb{Z}/26\mathbb{Z}$ by this matrix, using the usual method for matrix multiplication and the remainder arithmetic above. For example,

$$\begin{bmatrix} 6 & 1 \\ 7 & 6 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} = \begin{bmatrix} 14 \\ 19 \end{bmatrix}$$

Similarly, we can construct systems of equations with coefficients in $\mathbb{Z}/26\mathbb{Z}$ and try to solve them for elements in $\mathbb{Z}/26\mathbb{Z}$:

$$\left[\begin{array}{cc|c} 6 & 1 & 14 \\ 7 & 6 & 19 \end{array}\right]$$

Now $7 \cdot 15 = 1$, $6 \cdot 15 = 12$ and $19 \cdot 15 = 25$. So multiplying the second row by 15, and switching it into the first row we get

$$\left[\begin{array}{cc|c} 1 & 12 & 25 \\ 6 & 1 & 14 \end{array}\right] \xrightarrow{R2-6R1\to R2} \left[\begin{array}{cc|c} 1 & 12 & 25 \\ 0 & 7 & 20 \end{array}\right] \xrightarrow{15\cdot R2\to R2} \left[\begin{array}{cc|c} 1 & 12 & 25 \\ 0 & 1 & 14 \end{array}\right] \xrightarrow{R1-12\cdot R2\to R1} \left[\begin{array}{cc|c} 1 & 0 & 13 \\ 0 & 1 & 14 \end{array}\right]$$

and we recover the original vector. Note how the ability to invert 7 within $\mathbb{Z}/26\mathbb{Z}$ allows us to do this computation. In fact, this matrix has an inverse, which we can compute using the usual formula for inverses of $2 \times 2$ matrices:

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Longrightarrow \mathbf{A}^{-1} = D^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

where $D$ is the determinant of $A$. For our example, $D = 6 \cdot 6 - 7 \cdot 1 = 3$ in $\mathbb{Z}/26\mathbb{Z}$ (all our computations have to be in this set!), and we've seen that $3^{-1} = 9$. Thus over $Z/26\mathbb{Z}$ we have

$$\begin{bmatrix} 6 & 1 \\ 7 & 6 \end{bmatrix}^{-1} = 3^{-1} \begin{bmatrix} 6 & 25 \\ 19 & 6 \end{bmatrix} = \begin{bmatrix} 9 \cdot 6 & 9 \cdot 25 \\ 9 \cdot 19 & 9 \cdot 6 \end{bmatrix} = \begin{bmatrix} 2 & 17 \\ 15 & 2 \end{bmatrix}$$

which can be checked is the inverse matrix.

**(Question 1.16)** Suppose, instead, we try to use the matrix

$$\mathbf{A} = \begin{bmatrix} 1 & 3 \\ 7 & 9 \end{bmatrix}$$

(1) Show that the determinant of this matrix is $9 - 21 = -12 = 14 \neq 0$ in $\mathbb{Z}/26\mathbb{Z}$.
(2) Show that we cannot invert 14 in $\mathbb{Z}/26\mathbb{Z}$ (*Hint:* in $\mathbb{Z}/26\mathbb{Z}$, we have $14 \cdot 13 = 0$, but $13 \neq 0$. What would be the only solution to $14x = 0$ if $14^{-1}$ existed?)
(3) This shows that the formula for $\mathbf{A}^{-1}$ doesn't work. However, maybe there is another way to find an inverse. Find two different vectors solving $\mathbf{Ax} = \mathbf{0}$ and explain why this rules out the existence of $\mathbf{A}^{-1}$.

**Takeaway:** When we try to solve equations with integer coefficients we may need to use rational numbers since division by an integer requires us to have rationals. However, allowing rational numbers also allows us to have systems with rational coefficients. Similarly, allowing complex numbers allows us to have systems with complex coefficients. In these cases, we don't need to look for solutions in larger sets of numbers *because we can divide by (non-zero) numbers in this set*!

So over the rationals and over the complex numbers, we can use the techniques of elementary linear algebra such as finding row reduced echelon form matrices to solve system of linear equations. However, over other sets of numbers such as the integers or $\mathbb{Z}/26\mathbb{Z}$, these techniques don't work. The difference is whether we can always find a (multiplicative) inverse for a non-zero number.