Semester II 2026

MA135/MA160 - Algebra II



OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Ilia Pirashvili, PhD

With special thanks to Prof. Aisling McCluskey & Dr. Róisín Hill

Lecture 20: Systems of linear equations

Cryptography - review

Recall, from semester 1, 1-letter encryption (1-letter base units affine cipher). For example, suppose

$$f_E(x) = 3x + 2 \mod 26,$$

let

A	B	C	D	E	$\ldots$	X	Y	Z
0	1	2	3	4	$\ldots$	23	24	25

and let the plaintext be

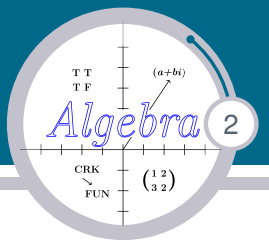
B	L	U	E
1	11	20	4

. Then

$$f_E(1) = 3(1) + 2 = 5 \leftrightarrow F$$
$$f_E(11) = 3(11) + 2 = 35 \equiv (35 - 26) \mod 26 = 9 \mod 26 \leftrightarrow J$$
$$f_E(20) = 3(20) + 2 = 62 \equiv (62 - 52) \mod 26 = 10 \mod 26 \leftrightarrow K$$
$$f_E(4) = 3(4) + 2 = 14 \leftrightarrow O$$

So $\underbrace{BLUE}_{\text{plaintext}}$ is encrypted as $\underbrace{FJKO}_{\text{cyphertext}}$.

Decryption



More generally, the encryption function takes the form

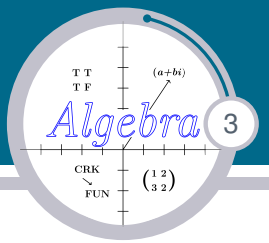
$$f_E(x) = \alpha x + \beta, \quad \text{where } \alpha, \beta \in \mathbb{Z}_{26} \text{ are given, } x \in \mathbb{Z}_{26}.$$

Private key is (α, β).
If we know α and β, we can decrypt the cyphertext using

$$f_D(x) = \alpha^{-1}(x - \beta).$$

For example, if $f_E(x) = 3x + 2$, then $f_D(x) = 3^{-1}(x - 2)$. Since $3(9) = 27 \equiv 1 \bmod 26$, $3^{-1} \equiv 9 \bmod 26$ and so $f_D(x) = 9(x - 2)$.

Decryption example

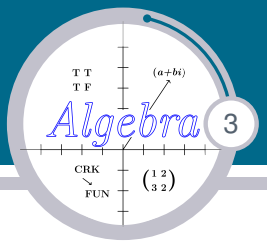


Let's decrypt

F	J	K	O
5	9	10	14

with $f_D(x) = 9(x - 2)$:

Decryption example



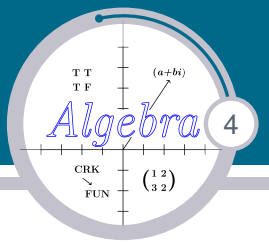
Let's decrypt

F	J	K	O
5	9	10	14

with $f_D(x) = 9(x-2)$:

$$f_D(5) = 9(5-2) = 27 \equiv (27-26) \bmod 26 = 1 \bmod 26 \leftrightarrow B$$
$$f_D(9) = 9(9-2) = 63 \equiv (63-52) \bmod 26 = 11 \bmod 26 \leftrightarrow L$$
$$f_D(10) = 9(10-2) = 72 \equiv (72-52) \bmod 26 = 20 \bmod 26 \leftrightarrow U$$
$$f_D(14) = 9(14-2) = 108 \equiv (108-104) \bmod 26 = 4 \bmod 26 \leftrightarrow E$$

Encrypting 2-letters at a time



Now let's consider encrypting "BLUE" using a 2-letter base units affine cipher. Here we take two letters at a time :

$$\begin{pmatrix} B \\ L \end{pmatrix} \to \begin{pmatrix} 1 \\ 11 \end{pmatrix}, \quad \begin{pmatrix} U \\ E \end{pmatrix} \to \begin{pmatrix} 20 \\ 4 \end{pmatrix} \quad \text{and we encrypt} \begin{pmatrix} 1 \\ 11 \end{pmatrix} \quad \text{and} \begin{pmatrix} 20 \\ 4 \end{pmatrix}$$

For this, the encryption process uses 2×2 matrices over $\mathbb{Z}_{26}$ (denoted by $M_2(\mathbb{Z}_{26})$) as follows:

$$f_E(X) = \alpha X + \beta, \quad \text{where } X = \begin{pmatrix} x \\ y \end{pmatrix}, \beta = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

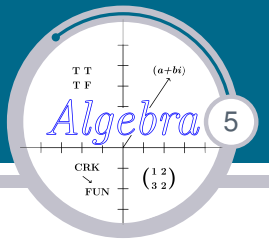
For example, if

$$\alpha = \begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix}, \quad \text{and } \beta = \begin{pmatrix} 2 \\ 3 \end{pmatrix},$$

then

$$f_E \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \quad \text{for } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 11 \end{pmatrix}, \begin{pmatrix} 20 \\ 4 \end{pmatrix}.$$

Encrypt “BLUE” (cont.)

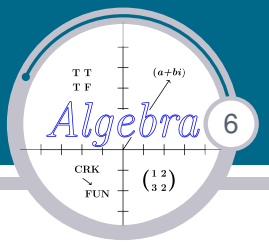


$$f_E\begin{pmatrix}1\\11\end{pmatrix} = \begin{pmatrix}4 & 5\\1 & 5\end{pmatrix}\begin{pmatrix}1\\11\end{pmatrix}+\begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}4+55\\1+55\end{pmatrix}+\begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}59\\56\end{pmatrix}+\begin{pmatrix}2\\3\end{pmatrix}$$
$$= \begin{pmatrix}61\\59\end{pmatrix} \equiv \begin{pmatrix}61-52\\59-52\end{pmatrix} \bmod 26 = \begin{pmatrix}9\\7\end{pmatrix} \bmod 26.$$

$$f_E\begin{pmatrix}20\\4\end{pmatrix} = \begin{pmatrix}4 & 5\\1 & 5\end{pmatrix}\begin{pmatrix}20\\4\end{pmatrix}+\begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}80+20\\20+20\end{pmatrix}+\begin{pmatrix}2\\3\end{pmatrix} = \begin{pmatrix}100\\40\end{pmatrix}+\begin{pmatrix}2\\3\end{pmatrix}$$
$$= \begin{pmatrix}102\\43\end{pmatrix} \equiv \begin{pmatrix}102-78\\43-26\end{pmatrix} \bmod 26 = \begin{pmatrix}24\\17\end{pmatrix} \bmod 26.$$

$$\begin{pmatrix}9\\7\end{pmatrix} \leftrightarrow \begin{pmatrix}J\\H\end{pmatrix}, \begin{pmatrix}24\\17\end{pmatrix} \leftrightarrow \begin{pmatrix}Y\\R\end{pmatrix} \quad \text{and } \underbrace{\text{BLUE}}_{\text{plaintext}} \rightarrow \underbrace{\text{JHYR}}_{\text{ciphertext}}.$$

Encryption example



$$f_E \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix},$$

Encrypt “GALWAY” using the above function

$$\begin{pmatrix} G \\ A \end{pmatrix} \to \begin{pmatrix} 6 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} L \\ W \end{pmatrix} \to \begin{pmatrix} 11 \\ 22 \end{pmatrix}, \quad \begin{pmatrix} A \\ Y \end{pmatrix} \to \begin{pmatrix} 0 \\ 24 \end{pmatrix}.$$

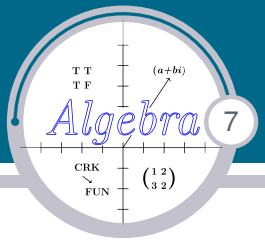
$$\begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 6 \\ 0 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 24 \\ 6 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 26 \\ 9 \end{pmatrix} = \begin{pmatrix} 0 \\ 9 \end{pmatrix} \mod 26,$$

$$\begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 11 \\ 22 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 44+110 \\ 11+110 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 156 \\ 124 \end{pmatrix} = \begin{pmatrix} 0 \\ 20 \end{pmatrix} \mod 26,$$

$$\begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 0 \\ 24 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 120 \\ 120 \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 122 \\ 123 \end{pmatrix} = \begin{pmatrix} 18 \\ 19 \end{pmatrix} \mod 26,$$

$$\begin{pmatrix} 0 \\ 9 \end{pmatrix} \to \begin{pmatrix} A \\ J \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 20 \end{pmatrix} \to \begin{pmatrix} A \\ U \end{pmatrix}, \quad \begin{pmatrix} 18 \\ 19 \end{pmatrix} \to \begin{pmatrix} S \\ T \end{pmatrix}, \quad \underbrace{\text{GALWAY}}_{\textit{plantext}} \to \underbrace{\text{AJAUST}}_{\textit{ciphertext}}$$

Exercise: encryption

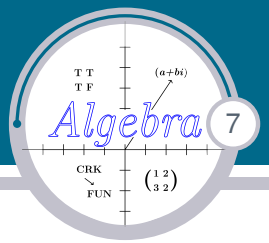


Using the function

$$f_E \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

encrypt “RENT”.

Exercise: encryption



Using the function

$$f_E\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

encrypt “RENT”.

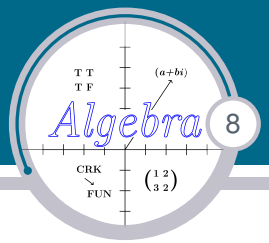
$$\begin{pmatrix} R \\ E \end{pmatrix} \to \begin{pmatrix} 17 \\ 4 \end{pmatrix}, \quad \begin{pmatrix} N \\ T \end{pmatrix} \to \begin{pmatrix} 13 \\ 19 \end{pmatrix}.$$

$$\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 34+12 \\ 17+20 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 47 \\ 38 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 12 \end{pmatrix} \mod 26,$$

$$\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}\begin{pmatrix} 13 \\ 19 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 26+57 \\ 13+95 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 84 \\ 109 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 5 \end{pmatrix} \mod 26,$$

$$\begin{pmatrix} 21 \\ 12 \end{pmatrix} \to \begin{pmatrix} V \\ M \end{pmatrix}, \quad \begin{pmatrix} 6 \\ 5 \end{pmatrix} \to \begin{pmatrix} G \\ F \end{pmatrix}. \quad \underbrace{\text{“RENT”}}_{\text{plaintext}} \to \underbrace{\text{“VMGF”}}_{\text{ciphertext}}.$$

Decryption



The enciphering function using a 2-letter base units affine cipher over $\mathbb{Z}_{26}$ takes the form

$$f_E(X) = \alpha X + \beta.$$

The deciphering function that decodes the ciphertext is

$$f_D(X) = \alpha^{-1}(X - \beta), \quad \text{assuming } \alpha^{-1} \text{ exists.}$$

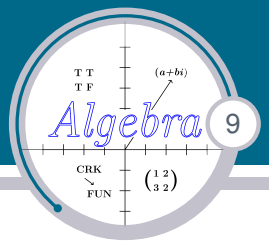
So how do we find α^{-1} where α is a 2×2 matrix over $\mathbb{Z}_{26}$? Example:

$$\alpha = \begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix} \implies \alpha^{-1} = (\det(\alpha))^{-1} \begin{pmatrix} 5 & -5 \\ -1 & 4 \end{pmatrix} \qquad \text{(F\&T, p20)}$$

Now, $\det(\alpha) = 4(5) - 5(1) = 15$. We need 15^{-1} mod 26, i.e., we need a number such that $15n \equiv 1 \bmod 26$.

We try $3, 5, 7, \ldots$ (as n must be odd), and find $15(7) = 105 = 104 + 1 = 26(4) + 1$ so $15(7) \equiv 1 \bmod 26$, and $15^{-1} = 7 \bmod 26$.

Decryption (cont)



Thus

$$\alpha^{-1} = \begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix}^{-1} = 7 \begin{pmatrix} 5 & -5 \\ -1 & 4 \end{pmatrix} = \begin{pmatrix} 35 & -35 \\ -7 & 28 \end{pmatrix}$$
$$\equiv \begin{pmatrix} 35-26 & -35+52 \\ -7+26 & 28-26 \end{pmatrix} \bmod 26 = \begin{pmatrix} 9 & 17 \\ 19 & 2 \end{pmatrix} \bmod 26$$

We add or subtract multiples of 26 until each entry in α^{-1} is ≥ 0 and ≤ 25.

Decryption (cont)

For the encryption function

$$f_E \begin{pmatrix} x \\ y \end{pmatrix} = \alpha \begin{pmatrix} x \\ y \end{pmatrix} + \beta$$

$$\text{i.e., } f_E \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

the decryption function is

$$f_D \begin{pmatrix} x \\ y \end{pmatrix} = \alpha^{-1} \left(\begin{pmatrix} x \\ y \end{pmatrix} - \beta \right),$$

$$\text{i.e., } f_D \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 9 & 17 \\ 19 & 2 \end{pmatrix} \left(\underbrace{\begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \end{pmatrix}}_{\text{calculate first}} \right),$$

Let's check if this will decode "AJAUST" to find "GALWAY"

Decryption example

$$f_D\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}9 & 17\\19 & 2\end{pmatrix}\left(\begin{pmatrix}x\\y\end{pmatrix} - \begin{pmatrix}2\\3\end{pmatrix}\right),$$

$$\begin{pmatrix}A\\J\end{pmatrix} \to \begin{pmatrix}0\\9\end{pmatrix}, \quad \begin{pmatrix}A\\U\end{pmatrix} \to \begin{pmatrix}0\\20\end{pmatrix}, \quad \begin{pmatrix}S\\T\end{pmatrix} \to \begin{pmatrix}18\\19\end{pmatrix}$$

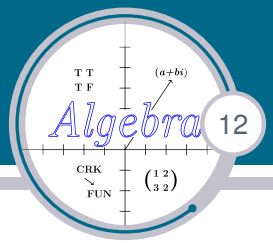
$$\begin{pmatrix}9 & 17\\19 & 2\end{pmatrix}\left(\begin{pmatrix}0\\9\end{pmatrix} - \begin{pmatrix}2\\3\end{pmatrix}\right) \equiv \begin{pmatrix}9 & 17\\19 & 2\end{pmatrix}\begin{pmatrix}-2+26\\6\end{pmatrix} \mod 26$$

$$= \begin{pmatrix}9(24)+17(6)\\19(24)+2(6)\end{pmatrix} = \begin{pmatrix}318\\468\end{pmatrix} \equiv \begin{pmatrix}318-12(26)\\468-18(26)\end{pmatrix} \mod 26 = \begin{pmatrix}6\\0\end{pmatrix} \mod 26$$

$$\begin{pmatrix}9 & 17\\19 & 2\end{pmatrix}\left(\begin{pmatrix}0\\20\end{pmatrix} - \begin{pmatrix}2\\3\end{pmatrix}\right) \equiv \begin{pmatrix}9 & 17\\19 & 2\end{pmatrix}\begin{pmatrix}-2+26\\17\end{pmatrix} \mod 26$$

$$= \begin{pmatrix}9(24)+17(17)\\19(24)+2(17)\end{pmatrix} = \begin{pmatrix}505\\490\end{pmatrix} \equiv \begin{pmatrix}505-19(26)\\490-18(26)\end{pmatrix} \mod 26 = \begin{pmatrix}11\\22\end{pmatrix} \mod 26$$

Decryption example (cont.)

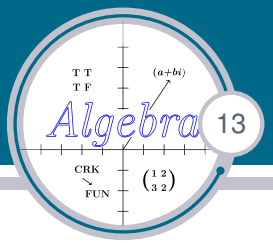


$$\begin{pmatrix} 9 & 17 \\ 19 & 2 \end{pmatrix} \left(\begin{pmatrix} 18 \\ 19 \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right) = \begin{pmatrix} 9 & 17 \\ 19 & 2 \end{pmatrix} \begin{pmatrix} 16 \\ 16 \end{pmatrix}$$

$$= \begin{pmatrix} 9(16) + 17(16) \\ 19(16) + 2(16) \end{pmatrix} = \begin{pmatrix} 416 \\ 336 \end{pmatrix} \equiv \begin{pmatrix} 416 - 16(26) \\ 336 - 12(26) \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ 24 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} 6 \\ 0 \end{pmatrix} \to \begin{pmatrix} G \\ A \end{pmatrix}, \quad \begin{pmatrix} 11 \\ 22 \end{pmatrix} \to \begin{pmatrix} L \\ W \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 24 \end{pmatrix} \to \begin{pmatrix} A \\ Y \end{pmatrix}.$$

Exercise: decryption



Find the decryption function for the encryption function

$$f_E \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

and decode “VMGF”. First, find α^{-1} and f_D.

Exercise: decryption

Find the decryption function for the encryption function

$$f_E \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

and decode “VMGF”. First, find α^{-1} and f_D.

$$\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}^{-1} = (2(5) - 3(1))^{-1} \begin{pmatrix} 5 & -3 \\ -1 & 2 \end{pmatrix} = 7^{-1} \begin{pmatrix} 5 & -3 \\ -1 & 2 \end{pmatrix}.$$

We need to find n such that $7n \equiv 1 \bmod 26$. By checking $n = 3, 5, 7 \ldots$ we find that $7(15) \equiv 1 \bmod 26$, so $7^{-1} = 15 \bmod 26$.

$$\begin{aligned} \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}^{-1} &= 15 \begin{pmatrix} 5 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 75 & -45 \\ -15 & 30 \end{pmatrix} \\ &= \begin{pmatrix} 75 - 52 & -45 + 52 \\ -15 + 26 & 30 - 26 \end{pmatrix} \bmod 26 = \begin{pmatrix} 23 & 7 \\ 11 & 4 \end{pmatrix} \bmod 26 \end{aligned}$$

Exercise: decryption (cont)

$$f_D\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 23 & 7 \\ 11 & 4 \end{pmatrix}\left(\begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right),$$

$$\begin{pmatrix} V \\ M \end{pmatrix} \to \begin{pmatrix} 21 \\ 12 \end{pmatrix}, \quad \begin{pmatrix} G \\ F \end{pmatrix} \to \begin{pmatrix} 6 \\ 5 \end{pmatrix}.$$