Semester II 2026

MA135/MA160 - Algebra II



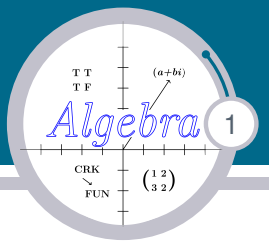
OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Ilia Pirashvili, PhD

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

Lecture 21: Systems of linear equations

Exercise: encryption (from yesterday)

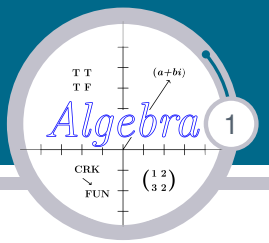


Using the function

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

encrypt “RENT”.

Exercise: encryption (from yesterday)



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

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

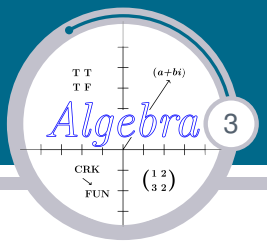
So how do we find α^{-1} where α is a 2×2 matrix over $\mathbb{Z}_{26}$? Example:

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

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)

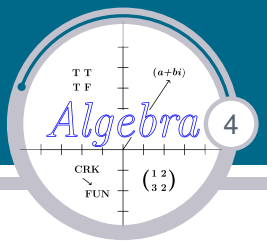


Thus

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

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

Decryption (cont)



For the encryption function

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

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

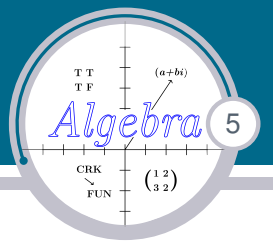
the decryption function is

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

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

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

Decryption example



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

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

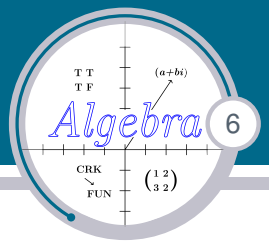
$$\begin{pmatrix}9 & 17\\19 & 2\end{pmatrix}\left(\begin{pmatrix}0\\9\end{pmatrix} - \begin{pmatrix}2\\3\end{pmatrix}\right) \equiv \begin{pmatrix}9 & 17\\19 & 2\end{pmatrix}\begin{pmatrix}-2+26\\6\end{pmatrix} \mod 26$$

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

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

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

Decryption example (cont.)

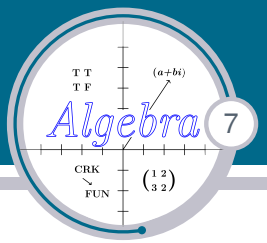


$$\begin{pmatrix} 9 & 17 \\ 19 & 2 \end{pmatrix} \left(\begin{pmatrix} 18 \\ 19 \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right) = \begin{pmatrix} 9 & 17 \\ 19 & 2 \end{pmatrix} \begin{pmatrix} 16 \\ 16 \end{pmatrix}$$

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

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

Exercise: decryption

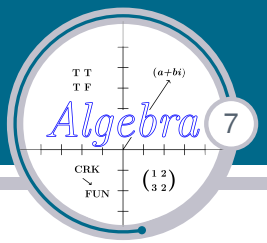


Find the decryption function for the encryption function

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

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.

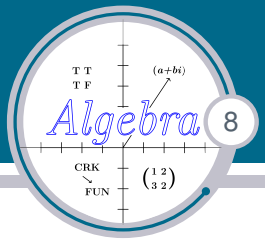
$$\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}^{-1} = \frac{1}{2(5) - 3(1)} \begin{pmatrix} 5 & -3 \\ -1 & 2 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 5 & -3 \\ -1 & 2 \end{pmatrix}.$$

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 $7^{-1} = 15 \bmod 26$.

$$\begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}^{-1} = 15 \begin{pmatrix} 5 & -3 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 75 & -45 \\ -15 & 30 \end{pmatrix}$$

$$= \begin{pmatrix} 75 - 52 & -45 + 52 \\ -15 + 26 & 30 - 26 \end{pmatrix} \bmod 26 = \begin{pmatrix} 23 & 7 \\ 11 & 4 \end{pmatrix} \bmod 26$$

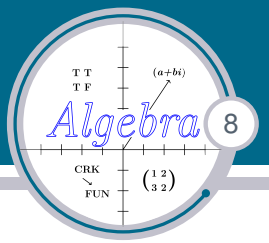
Exercise: decryption (cont)



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

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

Exercise: decryption (cont)



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

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

$$\begin{pmatrix}23 & 7\\11 & 4\end{pmatrix}\left(\begin{pmatrix}21\\12\end{pmatrix} - \begin{pmatrix}1\\1\end{pmatrix}\right) = \begin{pmatrix}23 & 7\\11 & 4\end{pmatrix}\begin{pmatrix}20\\11\end{pmatrix} = \begin{pmatrix}23(20)+7(11)\\11(20)+4(11)\end{pmatrix}$$

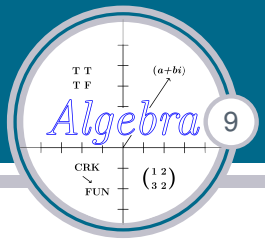
$$= \begin{pmatrix}537\\264\end{pmatrix} = \begin{pmatrix}537-520\\264-260\end{pmatrix} \bmod 26 = \begin{pmatrix}17\\4\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}23 & 7\\11 & 4\end{pmatrix}\left(\begin{pmatrix}6\\5\end{pmatrix} - \begin{pmatrix}1\\1\end{pmatrix}\right) = \begin{pmatrix}23 & 7\\11 & 4\end{pmatrix}\begin{pmatrix}5\\4\end{pmatrix} = \begin{pmatrix}23(5)+7(4)\\11(5)+4(4)\end{pmatrix}$$

$$= \begin{pmatrix}143\\71\end{pmatrix} = \begin{pmatrix}143-130\\71-52\end{pmatrix} \bmod 26 = \begin{pmatrix}13\\19\end{pmatrix} \bmod 26.$$

$$\begin{pmatrix}17\\4\end{pmatrix} \to \begin{pmatrix}R\\E\end{pmatrix}, \quad \begin{pmatrix}13\\19\end{pmatrix} \to \begin{pmatrix}N\\T\end{pmatrix}. \quad \underbrace{\text{VMGF}}_{\text{cybertext}} \to \underbrace{\text{RENT}}_{\text{plaintext}}$$

Exam



- Final exam will be two hours long and has six questions.
- You are expected to attempt all question.
- Three of the questions (totaling 50%) will be on Algebra, one on each area.
- Exam scripts and Formulae and Tables will be provided.
- You are expected to take your own calculator. Make sure its a basic, non-programmable one.