1B03 – LINEAR ALGEBRA 1 (C01) WS19 Lecture 35

Last Time Row Space, Column Space, Null Space of A

To find bases for these:

- Reduce A to its RREF R
- For null(A): solve $A\bar{x} = \bar{0}$ i.e. $[A \mid 0]$ i.e. $[R \mid 0]$
- For row(A): use the non-zero rows of R
- For col(A): use the columns of A corresponding to the pivot columns of R (with leading 1s)

Note Dependence structure amongst columns same for A and R.

10.14 Cryptography – $\underbrace{\text{encoding}}_{\text{enciphering}}$ and $\underbrace{\text{decoding}}_{\text{deciphering}}$

Given letters, first encode as #s:

A	B	C	D	E	F	G	H	I	J	K	L
1	2	3	4	5	6	7	8	9	10	11	12

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25	0

Hill n- Cipher

- Convert "plaintext" message into #s (use chart)
- Split up string of #s in n-tuples $[b_1\ b_2\ \dots\ b_n]$

  (Repeat last digit enough times if length of message not a multiple of n.)

- We fix A, $n \times n$, enciphering matrix (some rules about what A can be — see later)
- Replace each submessage $[b_1\ \dots\ b_n]$ by $\leftarrow$ plaintext vector

$$A \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$ – another n-tuple called ciphertext vectors

- Change ciphertext vectors back into text ("ciphertext")
- Send ciphertext.

(we'll only use $n=2$.)

Example Encipher ENCODE using the Hill 2-cipher & $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$.

Solution ENCODE

5 14 3 15 4 5

Plaintext vectors $P_1 = \begin{bmatrix} 5 \\ 14 \end{bmatrix}$, $P_2 = \begin{bmatrix} 3 \\ 15 \end{bmatrix}$, $P_3 = \begin{bmatrix} 4 \\ 5 \end{bmatrix}$.

Encoding: $AP_1 = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 15 \\ 19 \end{bmatrix}$ O S

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 9 \\ 18 \end{bmatrix} \begin{matrix} I \\ R \end{matrix}$$

Send OSIRLI.

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 12 \\ 9 \end{bmatrix} \begin{matrix} L \\ I \end{matrix}$$

ciphertext vectors

Example Encipher END using $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$.

Solution 3 letters so add last letter on end: ENDD

$\underbrace{5\ 14}\ 4\ 4$

So
$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 15 \\ 19 \end{bmatrix} \begin{matrix} O \\ S \end{matrix}$$

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \end{bmatrix} \begin{matrix} L \\ H \end{matrix}$$

Send OSLH.

Potential Problem Encipher GET OUT using $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$

GET OUT

$$\begin{bmatrix} 7 \\ 5 \end{bmatrix}\begin{bmatrix} 20 \\ 15 \end{bmatrix}\begin{bmatrix} 21 \\ 20 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 7 \\ 5 \end{bmatrix} = \begin{bmatrix} 21 \\ 12 \end{bmatrix} \begin{matrix} U \\ L \end{matrix}$$

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 20 \\ 15 \end{bmatrix} = \begin{bmatrix} 60 \\ 35 \end{bmatrix} \begin{matrix} ? \\ ? \end{matrix} \quad \begin{matrix} H \\ I \end{matrix}$$

$$\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 21 \\ 20 \end{bmatrix} = \begin{bmatrix} 63 \\ 41 \end{bmatrix} \equiv \begin{bmatrix} 11 \\ 15 \end{bmatrix} \begin{matrix} K \\ O \end{matrix}$$

So $60 \longrightarrow 60 - 26 = 34 \longrightarrow 34 - 26 = 8$ H

$35 \longrightarrow 35 - 26 = 9$ I

$\equiv$ is "equivalent to"
i.e. differ by a multiple of 26 in each place

Send ULHIKO.

Modular Arithmetic

If m is a <u>positive</u> integer, a, b integers we say "a is equivalent to b modulo m" written $a = b \pmod{m}$ if $a - b$ is a multiple of m.

Examples $\underbrace{6 = 2 \pmod 4}_{6-2=4} = \underbrace{10}_{6-10=-4} \pmod 4 = \underbrace{-14}_{6-(-14)=20} \pmod 4$

etc. : there are infinitely many b with $6 = b \pmod 4$.

We define <u>residue</u> of a modulo m to be the

$$b \in \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

(It is a Fact that there is only one.)

Careful: It's not quite the "remainder" – see Example below.

Examples The residue of 6 modulo 4 is 2 (it's the b in $\{0, 1, 2, 3\}$ with $6 = b \pmod 4$)

The residue of 63 modulo 26 is 11 (see above)

The residue of -7 modulo 26 is 19. $\left(\mathbb{Z}_{26} = \{0, \ldots, 25\}\right)$

$\longrightarrow -\frac{7}{26} = 0(26) - 7$ So remainder here is -7. We want a # in $\mathbb{Z}_{26}$.

How do work this out? Add / subtract multiples of m until we land in $\mathbb{Z}_m$:

Use **Fact** For any integer k

$$\underbrace{a = (a \pm km) \pmod m}_{\text{says } a-(a\pm km) \text{ is a multiple of } m}$$

says $a - (a \pm km)$ is a multiple of m
$= \pm km$.

We can also multiply #s:

Examples Find 3×4, 5×7 and 11×19 modulo 26.

Solution

$3\times 4 = 12 = 12 \pmod{26}$

$5 \times 7 = 35 = (35-26) \pmod{26}$
$= 9 \bmod 26$

This says, in the world of $\mathbb{Z}_{26}$ "$5\times 7 = 9$"

$11 \times 19 = 209 = (209-208) = 1 \pmod{26}$

This says "$11\times 19 = 1$"

(Take away "easy" multiples of 26.) → It will probably help to remember 26, 52, (78), 104, 130, 156, (182), 204.

Can also keep taking away multiples → e.g. $209 = (209-104) \pmod{26}$
$= 105 \pmod{26} = (105-104) \pmod{26} = 1 \pmod{26}$ → do whatever is easiest!

Definition If $b \in \mathbb{Z}_m$, then b^{-1} is the number in $\mathbb{Z}_m$ with $bb^{-1} = b^{-1}b = 1 \pmod m$

b^{-1} is called the <u>reciprocal</u> of b modulo m.

Example 11 is the reciprocal of 19 modulo 26

19 " " " " 11 " "

<u>Fact</u> (about mod 26) $b \in \mathbb{Z}_{26}$ has a reciprocal exactly when it does NOT have EITHER 2 OR 13 as a (regular) divisor.

Why? (Not on syllabus!)

<u>Note</u> 2 & 13 are the "prime divisors" of 26 i.e. the prime #s that divide 26.

So really this fact is a special case of:

<u>Fact</u> If $s \in \mathbb{Z}_m$, then s has a reciprocal modulo m exactly when p does not divide s for every prime p that divides m.

Which in turn is a fancier way of saying:

<u>Fact</u> If $s \in \mathbb{Z}_m$, then s has a reciprocal modulo m exactly when s does not share any divisors with m (except 1).

(It's just easier to check the prime ones — if k divides both s and m and p divides k, then p also divides both s and m.)

So to see that this last <u>Fact</u> is true, take $s \in \mathbb{Z}_m$ and suppose that it does have a reciprocal $r \in \mathbb{Z}_m$ i.e.

$sr \equiv 1 \pmod{m}$ i.e. $sr - 1 = lm$ for some integer l.

Now if s and m share a divisor $k > 0$, then

$s = kt$ and $m = ku$ for integers t, u.

Then $ktr - 1 = lku$

$\Rightarrow k(tr - lu) = 1$

$\Rightarrow k = 1$ (and $tr - lu = 1$) since k and $tr - lu$ are both integers and $k > 0$

So the only divisor k that s and m can share is 1, if s is going to have a reciprocal modulo m.

The fact that $s \in \mathbb{Z}_m$ <u>does</u> have a reciprocal $s^{-1} \in \mathbb{Z}_m$ if the only divisor it shares with m is 1 follows from (for example) a sophisticated version of Euclid's Algorithm — dig deeper if you're interested.