Math 237

Module P

Section P.1 Section P.2 Section P.3 Section P.4

Module P: Applications of Linear Algebra

Math 237

Module P

Section P.1 Section P.2 Section P.3

Module P Section 1

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Definition P.1.1

In geology, a **phase** is any physically separable material in the system, such as various minerals or liquids.

A **component** is a chemical compound necessary to make up the phases; for historical reasons these are usually oxides such as Calcium Oxide (CaO) or Silicone Dioxide (SiO₂).

In a typical problem, a geologist knows how to build each phase from the components, and is interested in determining reactions among the different phases.

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4 Activity P.1.2 (~5 min) Consider the 3 components $c_1={\rm CaO},~c_2={\rm MgO},$ and $c_3={\rm SiO}_2,$ and the 5 phases

 $\begin{aligned} \mathbf{p}_1 &= \mathrm{Ca}_3\mathrm{MgSi}_2\mathrm{O}_8 & \mathbf{p}_2 &= \mathrm{Ca}\mathrm{MgSi}\mathrm{O}_4 & \mathbf{p}_3 &= \mathrm{CaSiO}_3 \\ \mathbf{p}_4 &= \mathrm{Ca}\mathrm{MgSi}_2\mathrm{O}_6 & \mathbf{p}_5 &= \mathrm{Ca}_2\mathrm{MgSi}_2\mathrm{O}_7 \end{aligned}$

Geologists will know

or more compactly,

$$\mathbf{p}_1 = \begin{bmatrix} 3\\1\\2 \end{bmatrix}, \mathbf{p}_2 = \begin{bmatrix} 1\\1\\1 \end{bmatrix}, \mathbf{p}_3 = \begin{bmatrix} 1\\0\\1 \end{bmatrix}, \mathbf{p}_4 = \begin{bmatrix} 1\\1\\2 \end{bmatrix}, \mathbf{p}_5 = \begin{bmatrix} 2\\1\\2 \end{bmatrix}.$$

Determine if the 5 phases are linearly dependent or linearly independent.

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.1.3 (~15 min) Recall our five phases:

or more compactly,

$$\mathbf{p}_1 = \begin{bmatrix} 3\\1\\2 \end{bmatrix}, \mathbf{p}_2 = \begin{bmatrix} 1\\1\\1 \end{bmatrix}, \mathbf{p}_3 = \begin{bmatrix} 1\\0\\1 \end{bmatrix}, \mathbf{p}_4 = \begin{bmatrix} 1\\1\\2 \end{bmatrix}, \mathbf{p}_5 = \begin{bmatrix} 2\\1\\2 \end{bmatrix}$$

Geologists want to find chemical reactions among the 5 phases; that is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\mathbf{p}_1 + x_2\mathbf{p}_2 + x_3\mathbf{p}_3 + x_4\mathbf{p}_4 + x_5\mathbf{p}_5 = 0.$$

.

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.1.3 (~15 min) Recall our five phases:

or more compactly,

$$\mathbf{p}_1 = \begin{bmatrix} 3\\1\\2 \end{bmatrix}, \mathbf{p}_2 = \begin{bmatrix} 1\\1\\1 \end{bmatrix}, \mathbf{p}_3 = \begin{bmatrix} 1\\0\\1 \end{bmatrix}, \mathbf{p}_4 = \begin{bmatrix} 1\\1\\2 \end{bmatrix}, \mathbf{p}_5 = \begin{bmatrix} 2\\1\\2 \end{bmatrix}$$

Geologists want to find chemical reactions among the 5 phases; that is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\mathbf{p}_1 + x_2\mathbf{p}_2 + x_3\mathbf{p}_3 + x_4\mathbf{p}_4 + x_5\mathbf{p}_5 = 0.$$

Part 1: Set up a system of equations that gives these chemical equations.

.

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.1.3 (~15 min) Recall our five phases:

or more compactly,

$$\mathbf{p}_1 = \begin{bmatrix} 3\\1\\2 \end{bmatrix}, \mathbf{p}_2 = \begin{bmatrix} 1\\1\\1 \end{bmatrix}, \mathbf{p}_3 = \begin{bmatrix} 1\\0\\1 \end{bmatrix}, \mathbf{p}_4 = \begin{bmatrix} 1\\1\\2 \end{bmatrix}, \mathbf{p}_5 = \begin{bmatrix} 2\\1\\2 \end{bmatrix}$$

Geologists want to find chemical reactions among the 5 phases; that is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\mathbf{p}_1 + x_2\mathbf{p}_2 + x_3\mathbf{p}_3 + x_4\mathbf{p}_4 + x_5\mathbf{p}_5 = 0.$$

Part 1: Set up a system of equations that gives these chemical equations. *Part 2:* Find a basis for the solution set.

.

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.1.3 (~15 min) Recall our five phases:

or more compactly,

$$\mathbf{p}_1 = \begin{bmatrix} 3\\1\\2 \end{bmatrix}, \mathbf{p}_2 = \begin{bmatrix} 1\\1\\1 \end{bmatrix}, \mathbf{p}_3 = \begin{bmatrix} 1\\0\\1 \end{bmatrix}, \mathbf{p}_4 = \begin{bmatrix} 1\\1\\2 \end{bmatrix}, \mathbf{p}_5 = \begin{bmatrix} 2\\1\\2 \end{bmatrix}$$

Geologists want to find chemical reactions among the 5 phases; that is, they want to find numbers x_1, x_2, x_3, x_4, x_5 such that

$$x_1\mathbf{p}_1 + x_2\mathbf{p}_2 + x_3\mathbf{p}_3 + x_4\mathbf{p}_4 + x_5\mathbf{p}_5 = 0.$$

Part 1: Set up a system of equations that gives these chemical equations. *Part 2:* Find a basis for the solution set. *Part 3:* Interpret each basis vector as a chemical equation.

Math 237

Section P.1

Activity P.1.4 (~10 mm) We found two basis vector $\begin{bmatrix} -1\\2\\-1\\-1\\0 \end{bmatrix}$ and $\begin{bmatrix} 0\\1\\1\\0\\-1 \end{bmatrix}$, corresponding to two chemical Activity P.1.4 ($\sim 10 \text{ min}$)

equations

$$\begin{aligned} & 2\textbf{p}_2 + 2\textbf{p}_3 = \textbf{p}_1 + \textbf{p}_4 \quad 2\text{CaMgSiO}_4 + 2\text{CaSiO}_3 = \text{Ca}_3\text{MgSi}_2\text{O}_8 + \text{CaMgSi}_2\text{O}_6 \\ & \textbf{p}_2 + \textbf{p}_3 = \textbf{p}_5 \qquad \text{CaMgSiO}_4 + \text{CaSiO}_3 = \text{Ca}_2\text{MgSi}_2\text{O}_7 \end{aligned}$$

Find a chemical equation among the five phases that does not involve $\mathbf{p}_2 = \mathrm{CaMgSiO}_4.$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Math 237

Module F

Section P.1 Section P.2 Section P.3

Module P Section 2

Math 237

Module I

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.2.1 (~10 min) A \$700,000,000,000 Problem:

In the picture below, each circle represents a webpage, and each arrow represents a link from one page to another.



Based on how these pages link to each other, write a list of the 7 webpages in order from most imptorant to least important.

Math 237

Module P Section P.1 Section P.2 Section P.3 Section P.4

Observation P.2.2 The \$700,000,000,000 Idea:

Links are endorsements.

- **1** A webpage is important if it is linked to (endorsed) by important pages.
- 2 A webpage distributes its importance equally among all the pages it links to (endorses).

Math 237

Module F

Section P.1 Section P.2 Section P.3

Example P.2.3

Consider this small network with only three pages. Let x_1, x_2, x_3 be the importance of the three pages respectively.



- x₁ splits its endorsement in half between x₂ and x₃
- **2** x_2 sends all of its endorsement to x_1
- **3** x_3 sends all of its endorsement to x_2 .

This corresponds to the **page rank** system

$$x_2 = x_1$$

$$\frac{1}{2}x_1 + x_3 = x_2$$

$$\frac{1}{2}x_1 = x_3$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Math 237

Module

Section P.1 Section P.2 Section P.3

Observation P.2.4



By writing this linear system in terms of matrix multiplication, we obtain the **page rank matrix** $A = \begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & 1 \\ \frac{1}{2} & 0 & 0 \end{bmatrix}$ and page rank vector $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$. Thus, computing the importance of pages on a network is equivalent to solving the matrix equation $A\mathbf{x} = 1\mathbf{x}$.

Math 237

Module I

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.2.5 (\sim 5 min) Thus, our \$700,000,000 problem is what kind of problem?

$$\begin{bmatrix} 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = 1 \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

- (a) An antiderivative problem
- (b) A bijection problem
- (c) A cofactoring problem
- (d) A determinant problem
- (e) An eigenvector problem

Math 237

Module P

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.2.6 (~10 min)

Find a page rank vector **x** satisfying $A\mathbf{x} = 1\mathbf{x}$ for the following network's page rank matrix A.

That is, find the eigenspace associated with $\lambda = 1$ for the matrix A, and choose a vector from that eigenspace.



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

Math 237

Module P Section P.1 Section P.2 Section P.3 Section P.4

Observation P.2.7
Row-reducing
$$A - I = \begin{bmatrix} -1 & 1 & 0 \\ \frac{1}{2} & -1 & 1 \\ \frac{1}{2} & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{bmatrix}$$
 yields the basic eigenvector $\begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}$.

Therefore, we may conclude that pages 1 and 2 are equally important, and both pages are twice as important as page 3.



Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4 Activity P.2.8 (\sim 5 min) Compute the 7 \times 7 page rank matrix for the following network.



For example, since website 1 distributes its endorsement equally between 2 and 4,

the first column is

 $\frac{1}{2}$

 $\frac{1}{2}$

0

Math 237

Module F

Section P.1 Section P.2 Section P.3

Activity P.2.9 (\sim 10 min) Find a page rank vector for the given page rank matrix.



Which webpage is most important?

Math 237

Module F

Section P.1 Section P.2 Section P.3

Observation P.2.10

Since a page rank vector for the network is given by \mathbf{x} , it's reasonable to consider page 2 as the most important page.



Based upon this page rank vector, here is a complete ranking of all seven pages from most important to least important:

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.2.11 (~10 min)

Given the following diagram, use a page rank vector to rank the pages 1 through 7 in order from most important to least important.



Math 237

Module F

Section P.1 Section P.2 Section P.3

Module P Section 3

Math 237

Module P Section P.1 Section P.2

Section P.3 Section P.4

Example P.3.1

In engineering, a **truss** is a structure designed from several beams of material called **struts**, assembled to behave as a single object.



Math 237

Module P Section P.1 Section P.2 Section P.3

Activity P.3.2 (~5 min)

Consider the representation of a simple truss pictured below. All of the seven struts are of equal length, affixed to two anchor points applying a normal force to nodes C and E, and with a 10000N load applied to the node given by D.



Which of the following must hold for the truss to be stable?

- a) All of the struts will experience compression.
- b) All of the struts will experience tension.
- c) Some of the struts will be compressed, but others will be tensioned.

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Observation P.3.3

Since the forces must balance at each node for the truss to be stable, some of the struts will be compressed, while others will be tensioned.



By finding vector equations that must hold at each node, we may determine many of the forces at play.

Math 237

Module P Section P.1

Section P.2 Section P.3

Remark P.3.4

For example, at the bottom left node there are 3 forces acting.



Let \mathbf{F}_{CA} be the force on *C* given by the compression/tension of the strut *CA*, let \mathbf{F}_{CD} be defined similarly, and let \mathbf{N}_{C} be the normal force of the anchor point on *C*.

For the truss to be stable, we must have

$$\mathbf{F}_{CA} + \mathbf{F}_{CD} + \mathbf{N}_{C} = \mathbf{0}.$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

Math 237

Module

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.3.5 (~10 min)

Using the conventions of the previous slide, and where L represents the load vector on node D, find four more vector equations that must be satisfied for each of the other four nodes of the truss.



Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Remark P.3.6

The five vector equations may be written as follows.



 $A : \mathbf{F}_{AC} + \mathbf{F}_{AD} + \mathbf{F}_{AB} = \mathbf{0}$ $B : \mathbf{F}_{BA} + \mathbf{F}_{BD} + \mathbf{F}_{BE} = \mathbf{0}$ $C : \mathbf{F}_{CA} + \mathbf{F}_{CD} + \mathbf{N}_{C} = \mathbf{0}$ $D : \mathbf{F}_{DC} + \mathbf{F}_{DA} + \mathbf{F}_{DB} + \mathbf{F}_{DE} + \mathbf{L} = \mathbf{0}$ $E : \mathbf{F}_{EB} + \mathbf{F}_{ED} + \mathbf{N}_{E} = \mathbf{0}$

Math 237

Module P Section P.1 Section P.2 Section P.3 Section P.4

Observation P.3.7



Each vector has a vertical and horizontal component, so it may be treated as a vector in \mathbb{R}^2 . Note that \mathbf{F}_{CA} must have the same magnitude (but opposite direction) as \mathbf{F}_{AC} .

$$\mathbf{F}_{CA} = x \begin{bmatrix} \cos(60^\circ) \\ \sin(60^\circ) \end{bmatrix} = x \begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix}$$
$$\mathbf{F}_{AC} = x \begin{bmatrix} \cos(-120^\circ) \\ \sin(-120^\circ) \end{bmatrix} = x \begin{bmatrix} -1/2 \\ -\sqrt{3}/2 \end{bmatrix}$$

Math 237

Module F

Section P.1 Section P.2 Section P.3

Activity P.3.8 (~5 min)

To write a linear system that models the truss under consideration with constant load 10000 newtons, how many variables will be required?



- a) 7: 5 from the nodes, 2 from the anchors
- b) 9: 7 from the struts, 2 from the anchors
- c) 11: 7 from the struts, 4 from the anchors
- d) 12: 7 from the struts, 4 from the anchors, 1 from the load
- e) 13: 5 from the nodes, 7 from the struts, 1 from the load

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Observation P.3.9

Since the angles for each strut are known, one variable may be used to represent each.



For example:

$$\mathbf{F}_{AB} = -\mathbf{F}_{BA} = x_1 \begin{bmatrix} \cos(0) \\ \sin(0) \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$\mathbf{F}_{BE} = -\mathbf{F}_{EB} = x_5 \begin{bmatrix} \cos(-60^\circ) \\ \sin(-60^\circ) \end{bmatrix} = x_5 \begin{bmatrix} 1/2 \\ -\sqrt{3}/2 \end{bmatrix}$$

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Observation P.3.10

Since the angle of the normal forces for each anchor point are unknown, two variables may be used to represent each.



$$\mathbf{N}_{C} = \begin{bmatrix} y_{1} \\ y_{2} \end{bmatrix} \qquad \qquad \mathbf{N}_{D} = \begin{bmatrix} z_{1} \\ z_{2} \end{bmatrix}$$

The load vector is constant.

$$\mathbf{L} = \begin{bmatrix} \mathbf{0} \\ -10000 \end{bmatrix}$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQ@

Remark P.3.11

Math 237

Module F

Section P.1 Section P.2 Section P.3 Each of the five vector equations found previously represent two linear equations: one for the horizontal component and one for the vertical.



$$C : \mathbf{F}_{CA} + \mathbf{F}_{CD} + \mathbf{N}_{C} = \mathbf{0}$$

$$\Leftrightarrow x_{2} \begin{bmatrix} \cos(60^{\circ}) \\ \sin(60^{\circ}) \end{bmatrix} + x_{6} \begin{bmatrix} \cos(0^{\circ}) \\ \sin(0^{\circ}) \end{bmatrix} + \begin{bmatrix} y_{1} \\ y_{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Using the approximation $\sqrt{3}/2\approx 0.866,$ we have

$$\Leftrightarrow x_2 \begin{bmatrix} 0.5\\0.866 \end{bmatrix} + x_6 \begin{bmatrix} 1\\0 \end{bmatrix} + y_1 \begin{bmatrix} 1\\0 \end{bmatrix} + y_2 \begin{bmatrix} 0\\1 \end{bmatrix} = \begin{bmatrix} 0\\0 \end{bmatrix}$$

イロト イポト イヨト イヨト

ъ

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.3.12 (~10 min)

Expand the vector equation given below using sine and cosine of appropriate angles, then compute each component (approximating $\sqrt{3}/2 \approx 0.866$).



$$D: \mathbf{F}_{DA} + \mathbf{F}_{DB} + \mathbf{F}_{DC} + \mathbf{F}_{DE} = -\mathbf{L}$$

$$\Leftrightarrow x_3 \begin{bmatrix} \cos(?)\\\sin(?) \end{bmatrix} + x_4 \begin{bmatrix} \cos(?)\\\sin(?) \end{bmatrix} + x_6 \begin{bmatrix} \cos(?)\\\sin(?) \end{bmatrix} + x_7 \begin{bmatrix} \cos(?)\\\sin(?) \end{bmatrix} = \begin{bmatrix} ?\\ ? \end{bmatrix}$$

$$\Leftrightarrow x_3 \begin{bmatrix} ?\\ ? \end{bmatrix} + x_4 \begin{bmatrix} ?\\ ? \end{bmatrix} + x_6 \begin{bmatrix} ?\\ ? \end{bmatrix} + x_7 \begin{bmatrix} ?\\ ? \end{bmatrix} = \begin{bmatrix} ?\\ ? \end{bmatrix}$$

Math 237

Section P.1

Section P.2 Section P.3

Observation P.3.13

The full augmented matrix given by the ten equations in this linear system is given below, where the elevent columns correspond to $x_1, \ldots, x_7, y_1, y_2, z_1, z_2$, and the ten rows correspond to the horizontal and vertical components of the forces acting at A, \ldots, E .

Γ1	-0.5	0.5	0	0	0	0	0	0	0	0	ך 0
0	-0.866	-0.866	0	0	0	0	0	0	0	0	0
-1	0	0	-0.5	0.5	0	0	0	0	0	0	0
0	0	0	-0.866	-0.866	0	0	0	0	0	0	0
0	0.5	0	0	0	1	0	1	0	0	0	0
0	0.866	0	0	0	0	0	0	1	0	0	0
0	0	-0.5	0.5	0	-1	1	0	0	0	0	0
0	0	0.866	0.866	0	0	0	0	0	0	0	10000
0	0	0	0	-0.5	0	-1	0	0	1	0	0
LΟ	0	0	0	0.866	0	0	0	0	0	1	0

Math 237

Section P.2

Section P.3 Section P.4

Observation P.3.14

This matrix row-reduces to the following.

	Γ1	0	0	0	0	0	0	0	0	0	0	–5773.7]
	0	1	0	0	0	0	0	0	0	0	0	-5773.7
	0	0	1	0	0	0	0	0	0	0	0	5773.7
	0	0	0	1	0	0	0	0	0	0	0	5773.7
	0	0	0	0	1	0	0	0	0	0	0	-5773.7
\sim	0	0	0	0	0	1	0	0	0	-1	0	2886.8
	0	0	0	0	0	0	1	0	0	-1	0	2886.8
	0	0	0	0	0	0	0	1	0	1	0	0
	0	0	0	0	0	0	0	0	1	0	0	5000
	Γo	0	0	0	0	0	0	0	0	0	1	5000]

Math 237

Module P Section P.1 Section P.2 Section P.3





Thus we know the truss must satisfy the following conditions.

$$x_{1} = x_{2} = x_{5} = -5882.4$$
$$x_{3} = x_{4} = 5882.4$$
$$x_{6} = x_{7} = 2886.8 + z_{1}$$
$$y_{1} = -z_{1}$$
$$y_{2} = z_{2} = 5000$$

In particular, the negative x_1, x_2, x_5 represent tension (forces pointing into the nodes), and the postive x_3, x_4 represent compression (forces pointing out of the nodes). The vertical normal forces $y_2 + z_2$ counteract the 10000 load.

Math 237

Module F

- Section P.
- Section F
- Section I
- Section P.4

Module P Section 4

Math 237

Module P Section P.1

Section P.2 Section P.3

Definition P.4.1

Cryptography is the practice and study of encoding messages so that only the intended receiver can decode them.

For example, the ROT13 cipher both encodes and decodes messages by shifting each letter thirteen places in the alphabet, cycling from Z back to A. This may be accomplished by converting each letter to a number

$$\mathtt{A}\equiv \mathtt{1}, \mathtt{B}\equiv \mathtt{2}, \ldots, \mathtt{Y}\equiv \mathtt{25}, \mathtt{Z}\equiv \mathtt{0}$$

and adding 13 (modulo 26):

$$\text{HELLO} \equiv \begin{bmatrix} 8\\5\\12\\12\\12\\15\end{bmatrix} \overset{\leftrightarrow}{\underset{ROT13}{\leftrightarrow}} \begin{bmatrix} 21\\18\\25\\25\\2\end{bmatrix} \equiv \text{URYYB}$$

Math 237

Module P Section P.1

Section P.2 Section P.3

Activity P.4.2 (~10 min)

Suppose your instructor saw another student passing a note that said

MFUT DIFBU PO UIF UFTU

How could the instructor decode this message, taking advantage of the fact that THE is one of the most commonly used words in the English language?

Math 237

Module P Section P.1 Section P.2 Section P.3 Section P.4

Observation P.4.3

Frequency analysis is a common tool used in breaking **substitution ciphers** that simply substitute letters for other letters. In the message

MFUT DIFBU PO UIF UFTU

the common word THE is encoded as UIF, and the most common letters in the English language E,T match the most common letters used in this message: F,U.

This suggests the following partial decryption:

-ET- -HE-T -- THE TE-T

By considering the context, or the fact that all letters were shifted the same amount, or perhaps by an analysis of other messages sent using the same code, the completed message may be revealed:

LETS CHEAT ON THE TEST

Math 237

Module P Section P.1 Section P.2 Section P.3 Section P.4

Remark P.4.4

To defeat naive frequency analysis attacks, one method that may be used is to create a rule that converts groups of letters into new groups of letters, rather than converting single letters individually.

So to send the message

LETS CHEAT ON THE TEST

one might first break it into three-letter pieces.

LET SCH EAT ONT HET EST

Math 237

Module P Section P.1 Section P.2 Section P.3 Section P.4

Remark P.4.5

Each piece then may be converted to a Euclidean vector in \mathbb{R}^3 , which may be linearly transformed by multiplying by a matrix A with det(A) = 1 = det(A⁻¹).

For
$$A = \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix}$$
:
LET $\equiv \begin{bmatrix} 12 \\ 5 \\ 20 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \\ 20 \end{bmatrix} = \begin{bmatrix} -34 \\ -9 \\ 28 \end{bmatrix}$

Math 237

Module P Section P.1 Section P.2 Section P.3 Section P.4

Remark P.4.6

The resulting vector may be converted back into English letters by adding multiples of 26 to each component to obtain numbers between 0 and 25.

$$\begin{bmatrix} -34\\ -9\\ 28 \end{bmatrix} \equiv \begin{bmatrix} -34+52\\ -9+26\\ 28-26 \end{bmatrix} = \begin{bmatrix} 18\\ 17\\ 2 \end{bmatrix} \equiv \mathbb{RPB}$$

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Observation P.4.7

This process may be done all at once by converting the entire message into a matrix:

 $LET SCH \dots \equiv \begin{bmatrix} 12 & 19 \\ 5 & 3 & \dots \\ 20 & 8 \end{bmatrix}$ $\rightarrow \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 12 & 19 \\ 5 & 3 & \dots \\ 20 & 8 \end{bmatrix} = \begin{bmatrix} -34 & 27 \\ -9 & -29 & \dots \\ 28 & -3 \end{bmatrix}$ $\equiv \begin{bmatrix} 18 & 1 \\ 17 & 23 & \dots \\ 2 & 23 \end{bmatrix} \equiv RQB AVV \dots$

Math 237

Module I

Section P.1 Section P.2 Section P.3

Section P.4

Activity P.4.8 (~10 min)

encoding

Complete the following encoding of the entire message given below, using the $\begin{bmatrix} 3 & 2 & 3 \end{bmatrix}$

matrix
$$A = \begin{bmatrix} 5 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix}$$
.
LET SCH EAT ONT HET EST $\equiv \begin{bmatrix} 12 & 19 \\ 5 & 3 & \dots \\ 20 & 8 \end{bmatrix}$

$$\rightarrow \begin{bmatrix} 3 & -2 & -3 \\ -2 & 3 & 0 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 12 & 19 \\ 5 & 3 & \dots \\ 20 & 8 \end{bmatrix} = \begin{bmatrix} -34 & 27 \\ -9 & -29 & \dots \\ 28 & -3 \end{bmatrix}$$
$$\equiv \begin{bmatrix} 18 & 1 \\ 17 & 23 & \dots \\ 2 & 23 \end{bmatrix} \equiv RQB \text{ AWW ESI ILY FYF UUI}$$

Math 237

Module F

Section P.1 Section P.2 Section P.3 Section P.4

Activity P.4.9 (~10 min)

Reverse this process by using the decoding matrix, $A^{-1} = \begin{bmatrix} 6 & 4 & 9 \\ 4 & 3 & 6 \\ 3 & 2 & 5 \end{bmatrix}$.

$$RQB AWW ESI ILY FYF UUI \equiv \begin{bmatrix} 18 & 1 \\ 17 & 23 & \dots \\ 2 & 23 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} 6 & 4 & 9 \\ 4 & 3 & 6 \\ 3 & 2 & 5 \end{bmatrix} \begin{bmatrix} 18 & 1 \\ 17 & 23 & \dots \\ 2 & 23 \end{bmatrix} = \begin{bmatrix} 194 & 305 \\ 135 & 211 & \dots \\ 98 & 164 \end{bmatrix}$$
$$\equiv \begin{bmatrix} 12 & 19 \\ 5 & 3 & \dots \\ 20 & 8 \end{bmatrix} \equiv \text{LET SCH EAT ONT HET EST}$$