BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Some HW04 Solutions

October 17, 2020

HW04, Problem 2

October 17, 2020

HW04, Problem 2a

Alice and Bob are using the Rail Fence Cipher with 4 rows. Show how Alice encodes

The rail fence cipher.

Show all steps. Give the answer in blocks of 5 all caps for readability. (The last block will be smaller than 5.)

HW04, Problem 2a

Alice and Bob are using the Rail Fence Cipher with 4 rows. Show how Alice encodes

The rail fence cipher.

Show all steps. Give the answer in blocks of 5 all caps for readability. (The last block will be smaller than 5.)

Let's write it on the rails:

T						*L*						*C*					
	H				*I*		*F*				*E*		*I*				*R*
		E		*A*				*E*		*C*				*P*		*E*	
			R						*N*						*H*		

HW04, Problem 2a

Alice and Bob are using the Rail Fence Cipher with 4 rows. Show how Alice encodes

The rail fence cipher.

Show all steps. Give the answer in blocks of 5 all caps for readability. (The last block will be smaller than 5.)

Let's write it on the rails:

T						L						C					
	H				I		F				E		I				R
		E		A				E		C				P		E	
			R						N						H		

We then get
TLCHI FEIRE AECPE RNH

HW04, Problem 2b

Alice and Bob are using the Rail Fence Cipher with 4 rows. State the rail fence cipher (with 4 rows) in MOD terminology (as I did on the slides).

HW04, Problem 2b

Alice and Bob are using the Rail Fence Cipher with 4 rows. State the rail fence cipher (with 4 rows) in MOD terminology (as I did on the slides).

First list out the letters in positions $\equiv 1 \pmod 6$.
Second list out the letters in positions $\equiv 0, 2 \pmod 6$.
Third list out the letters in positions $\equiv 3, 5 \pmod 6$.
Fourth list out the letters in positions $\equiv 4 \pmod 6$.

HW04, Problem 2c

Give the modern view of the 5-row rail cipher, in terms of mods.

HW04, Problem 2c

Give the modern view of the 5-row rail cipher, in terms of mods.

This one I leave to you. I might put it on the **midterm** or **final**

HW04, Problem 4a

This problem is MOD 13.
Fill in the XXX in the following statement:
The 2×2 matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

has an inverse mod 13 IFF XXX.
(XXX can't be something like *the determinant is not a number of Shen-type*, it has to be about a, b, c, d.)

HW04, Problem 4a

This problem is MOD 13.
Fill in the XXX in the following statement:
The 2×2 matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

has an inverse mod 13 IFF XXX.
(XXX can't be something like *the determinant is not a number of Shen-type*, it has to be about a, b, c, d.)

XXX is $ad - bc$ is rel prime to 13.
Equivalent to
XXX is $ad - bc \not\equiv 0 \pmod{13}$

HW04, Problem 4b

This problem is MOD 13.
Give an example of a 2×2 matrix that DOES have an inverse mod 13 and give the inverse.

HW04, Problem 4b

This problem is MOD 13.
Give an example of a 2×2 matrix that DOES have an inverse mod 13 and give the inverse.

So many work that it would be hard to come up with one that DOESN"T work.

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$1 \times 4 - 2 \times 3 = 4 - 6 = -2 \equiv 11 \not\equiv 0$.
The final answer uses the formula for inverses BUT NOTE THAT you DO NOT us $\frac{1}{11}$ IN THE FINAL ANSWER. You use what it is mod 13 which is WELL LETS SEE:
$13 = 11 \times 1 + 2$
$11 = 2 \times 5 + 1$.
$1 = 11 - 2 \times 5 = 11 - (13 - 11) \times 5 = 11 \times 6 - 13 \times 5$
$1 \equiv 11 \times 6 \pmod{13}$. So the inverse of 11 mod 13 is 6.

HW04, Problem 4c

This problem is MOD 13.
Does there exist a 2×2 matrix with all entries DIFFERENT and in $\{1, \ldots, 12\}$ that DOES NOT have an inverse mod 13? If YES then give such a matrix, if NO then explain why not.

HW04, Problem 4c

This problem is MOD 13.
Does there exist a 2×2 matrix with all entries DIFFERENT and in $\{1, \ldots, 12\}$ that DOES NOT have an inverse mod 13? If YES then give such a matrix, if NO then explain why not.

YES: Here is such a matrix.

$$\begin{pmatrix} 6 & 3 \\ 4 & 2 \end{pmatrix}$$

The determinant is $6 \times 2 - 3 \times 4 = 0 \equiv 0 \pmod{13}$.