MTH 201: Calculus

Module 2A: Intro to modular arithmetic

Prof. Talbert

GVSU

August 11, 2020

Agenda for today

- Review + QA over Daily Prep (Division Algorithm, the % operator)
- Lecture + activity: Writing a program to implement the shift cipher
- Lecture + activity: The multiplicative (decimation) cipher
- Wrap up + feedback

Q+A from Daily Prep

- Insert questions here

Modular arithmetic and the shift cipher

1. User: Input a word to encrypt and a key K (positive integer)
2. For each letter in the word:
    1. Convert to number n between 0 and 25
    2. Compute _____
    3. Convert back to letter

Now look at a **Jupyter notebook with some Python code** that does this.

`https://bit.ly/2XP25DO`

The multiplicative (decimation) cipher

Just like the shift cipher except multiply by the key instead of add.

1. User: Input a word to encrypt and a key K (positive integer)
2. For each letter in the word:
    1. Convert to number n between 0 and 25
    2. Compute $(n \times K) \,\%\, 26$
    3. Convert back to letter

Now look at a **Jupyter notebook with some Python code** that does this.

Recapping the highlights

- The Division Algorithm gives us a way of dividing any two integers and getting a quotient and a remainder
- That remainder is really important in CS and cryptography; % is an operator that captures
- We can implement all kinds of ciphers in code using %
- However the math gets complicated, for example in finding "fractions"

NEXT TIME...

All due dates are on the course calendar