Use an affine cipher with key $k = (9, 11)$

1. You want to encrypt the message $x =$"MY CABBAGES"
   (You should first remove any spaces)
   (a) First encode message as numbers in $\mathbb{Z}_{26}$
   (b) Encrypt plaintext using affine cipher using the key k
   (c) Convert cipher text to letters
   (d) What message do you send?

2. Decrypt the message $y =$"FPHYAVLPCJALIL"

3. Explain why $k = (4, 17)$ would not work as an affine key

Note: WolframAlpha can perform modular arithmetic

Encoding in Unicode and UTF-8

- The Unicode standard assigns a character a unique value in the range

$$0 - 2^{32} = 4,294,967,296$$

- Each value can be stored in 4-bytes (each byte is 8-bits)
- `https://unicode.org/charts/`
- Not very efficient if the characters used most often have low Unicode values
- UTF-8 is a system to encode Unicode values using 1–4 bytes per character
  Requires using leading bits to indicate how many bytes the character uses

Some desirable properties for any cryptosystem

Kerckhoff’s Principle: A cryptosystem should be secure when the attacker knows all the details of the encryption and decryption algorithms but does not know the secret key.

i.e. No security through obscurity of the method

Definition: A cryptosystem is *unconditionally secure* if it cannot be broken, even with infinite computational resources.