Mathematical Puzzles, Games and Other Diversions

Day 16

Derrick Chung

October 19, 2022

More on Modular Arithmetic

Addition, subtraction and multiplication work as expected.
What about division?

Definition

Given an integer a, then a number a^{-1} is called the *multiplicative inverse* of a modulo m if and only if $aa^{-1} = a^{-1}a = 1 \pmod{m}$.

Note that a has a multiplicative inverse modulo m if and only if a and m are relatively prime (i.e. no common factors other than 1).

List of inverses modulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

You can find a multiplicative inverse by checking all possibilities

A better way is by applying the *Euclidean algorithm*.

The Affine Cipher

The Affine Cipher

Messages are encrypted using addition AND multiplication.

The encryption function is:

$E(x) = (ax + b) \pmod{26}$.

The decryption function is:

$D(x) = a^{-1}(x - b) \pmod{26}$.

Initial considerations

- This only works when a has a multiplicative inverse.
- As a result, there are $12 \times 26 = 312$ possible encryption keys.
- Every decryption key is also an encryption key:
  $D(x) = a^{-1}(x - b) = a^{-1}x + a^{-1}(-b) \pmod{26}$.

The Affine Cipher (cont.)

Example

Let's encrypt PIZZA with the affine cipher $E(x) = 5x - 9$.

- As before, we first write it as numbers: 16 9 0 0 1.
- Multiplying each number by 5 and then subtracting 9 gives: 71 36 -9 -9 -4
- Taking the residue modulo 26 gives 19 10 17 17 22
- Converting back to letter gives us the encrypted word SJQQV

And to decrypt, we use $D(x) = 5^{-1}(x + 9)$

Simplifying: $D(x) = 21(x + 9)$ OR $\underbrace{(-5)}_{-5 \equiv 21}(x + 9) \pmod{26}$.

Applying that to the numbers for SJQQV gives us back PIZZA.

The Affine Cipher (cont.)

Example

Let's try to decrypt the word YUWOM that was encoded with

$$E(x) = 9x + 12 \pmod{26}$$

- Convert the letters to numbers: 25 21 23 15 13
- Calculate $D(x) = 9^{-1}(x - 12) \pmod{26}$

  $D(x) = 3(x - 12)$ OR $3x - 36 \equiv 3x - 10 \pmod{26}$.
- Apply $D(x)$ to each number: 13 1 7 9 3
- Convert the numbers back to letters: *MAGIC*

Exercise

If you receive the message MRCZJQ encoded with the same affine cipher key as above, what was the original intended message?

The Affine Cipher (cont.)

General Considerations

- The key space for the Affine cipher is way too small.
- Any mono-alphabetic substitution cipher is very vulnerable to known plaintext attack.
  - For a Caesar cipher, knowing one letter is enough.
  - For an affine cipher, knowing two letters is sufficient.
- They are also very vulnerable to frequency analysis.
- A similar function can quickly generate random numbers, but it's not secure.
- We have to do MUCH better.

Kerchoff's Principle (1883)

A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.