Day 2 Notes

Emily Vogel

February 5, 2020

1 Abstract Theorems

1.1 A Divides B

Definition: We say 'a divides b' and write $a|b$ if $b = ka$ for some integer k.

1.1.1 Examples

$$2|18 \equiv 18 = 9 \times 2$$

In this case, $k = 9$.

$$2|0 \equiv 0 = 0 \times 2$$

In this case, $k = 0$. *Note: This means that $a/0$ for every a.*

1.2 B Modulo N

Definition: $a \equiv b \pmod{n}$ and say "a is congruent to b modulo n" if $n|(a - b)$.

1.2.1 Examples

$$33 \equiv 3 \pmod{10}$$

$$33 - 3 = 30$$

$$10|30$$

$$27 \equiv 42 \pmod{5}$$

$$27 - 42 = -15$$

$$5| - 15$$

1.3 Modulo Equivalency, Addition

If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a + b \equiv c + d \pmod{n}$.

1.3.1 Examples

$12 \equiv 22 \pmod{10}$ and $7 \equiv 37 \pmod{10}$ then...

$$12 + 7 \equiv 22 + 37 \pmod{10}$$

$$19 \equiv 59 \pmod{10}$$

1.3.2 Proof of Theorem

Since $a \equiv c \pmod{n}$, then $n|(a-c)$ so that means $a-c \equiv k \times n$ or $a = c+k \times n$
So:

$$a + b = (c + k \times n) + (d + l \times n)$$
$$= (c + d) + k \times n + l \times n$$
$$= c + d + n(k + l)$$

Is $a + b \equiv c + d \pmod{n}$?

$$(a + b) - (c + d) \equiv -n(k + l)$$

So yes, it is congruent.

1.4 Module Equivalency, Multiplication

If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \times b \equiv c \times d \pmod{n}$.

1.4.1 Proof of Theorem

$a = c + k \times n$ and $b = d + l \times n$. So:

$$a \times b = (c + k \times n) \times (d + l \times n)$$
$$= cd + cln + dkn + kln^2$$
$$= cd + n \times (cl + dk + kln)$$

So $ab = cd + nj$, where j is an integer so $ab \equiv cd \pmod{n}$.

1.5 Final Note

You can add, subtract, and multiply a and b but you can't always divide.

2 Affine Cipher (aka a better Caesar Cipher)

Pick a key, two integers α and β. Assume $0 \leq \alpha$, $\beta \leq 25$. For instance,

$$E(x) = \alpha x + \beta \pmod{26}$$

2.1 Encryption Example

$\alpha = 7$, $\beta = 20$ - *This is the key.* Plaintext is 'at' or 0 19.

$$E(0) = 7(0) + 20 \pmod{26}$$
$$= 20$$

or 'U'

$$E(19) = 7(19) + 20 \pmod{26}$$
$$= 153 \pmod{26}$$
$$= 23$$

or 'X'
Ciphertext is equal to 'UX'.

2.2 Decryption Example

$$y = E(x) = \alpha x + \beta \pmod{26}$$
$$y - \beta = \alpha x \pmod{26}$$

But we can't divide all numbers (can't take the mod of a fraction). So we must find a number α^{-1} where $\alpha^{-1}\alpha \equiv 1 \pmod{26}$. If α^{-1} exists, multiply both sides by α^{-1}. So:

$$\alpha^{-1}(y - \beta) \equiv \alpha^{-1}\alpha x \pmod{26}$$
$$\equiv x \pmod{26}$$

Which gives us:

$$D(y) = \alpha^{-1}(y - \beta)$$

By using the table in the schedule, if $\alpha = 7$ then $\alpha^{-1} = 15$.

$$D(y) = 15(y - 20) \pmod{26}$$
$$= 15y + 15 \times 6 \pmod{26}$$
$$= 15y + 12$$

Note: β went from -20 to 6 because we needed a positive number between 0 and 26, so we added 26 to the number. 15×6 *turned into 12 because we looked at the table to find the answer (not modulo 26).*

$$D(20) \equiv 15(20) + 12 \pmod{26}$$
$$\equiv 14 + 12 \pmod{26}$$

Which is equivalent to 'a'.

$$D(23) \equiv 15(23) + 12 \pmod{26}$$
$$\equiv 7 + 12 \pmod{26}$$

Which is equivalent to 't'.

2.2.1 Potential Problems

There can be one α that can map to multiple α^{-1}s. This means that the decrypted message could be wrong. What we do instead when we first pick an α is make sure the row contains only one 1. This leaves out the even numbers and the number 13 from being chosen.

3 Attacking the Affine Cipher

3.1 Ciphertext Only

You can use brute force for value pairs of α and β. This leaves 12 possibilities for α and 26 for β, for a total of $12 \times 26 = 312$ possibilities.

3.2 Chosen Plaintext

Pick α to be 0, or 'a'.

$$E(0) = \alpha(0) + \beta = \beta$$

Then pick α to be 1, or 'b'.

$$E(1) = \alpha(1) + \beta$$

$$E(1) - \beta = \alpha$$

3.3 Known Plaintext

Suppose 'it' maps to 'OH' (8, 19 -> 14, 7). We can use some principles in algebra to find the key α and β.

$$\alpha(8) + \beta \equiv 14 \pmod{26}$$

$$-\alpha(19) + \beta \equiv 7 \pmod{26}$$
$$= \alpha(-11) \equiv 7 \pmod{26}$$

or

$$= \alpha(15) \equiv 7 \pmod{26}$$

We pull up the table to find α^{-1} of 15, which is 7. So,

$$7 \times \alpha \times 15 \equiv 7 \times 7 \pmod{26}$$

$$\alpha \equiv 23$$

Now we plug it in to find β,

$$23(8) + \beta \equiv 14 \pmod{26}$$

$$2 + \beta \equiv 14 \pmod{26}$$
$$\beta \equiv 12$$