CMSC 389T HW3 SOLUTION

Phong Dinh and William Gasarch

Jan 6, 2017

Problem 3

Find ALL pairs of numbers $a, b \in \{0, \ldots, 25\}$ such that the coding and decoding tables for x goes to $ax + b \pmod{26}$ are the same.

<u>Solution</u>:

We start with affine cipher: $y \equiv ax + b \pmod{26}$. NOTE that a is relatively prime with 26.

$$\begin{aligned} y &\equiv ax + b \pmod{26} \\ \Leftrightarrow y - b &\equiv ax \pmod{26} \\ \Leftrightarrow a^{-1}(y-b) &\equiv a^{-1}ax \pmod{26} (a^{-1} \text{ is the multiplicative inverse of a}) \\ \Leftrightarrow a^{-1}y - a^{-1}b &\equiv x \pmod{26} (a^{-1} \text{ is mul. inv. of a} \Rightarrow a^{-1}a \equiv 1 \pmod{26}) \end{aligned}$$

Now, since we want the encoding the decoding tables are identical, then we have

$$a^{-1}x + a^{-1}b \equiv y \pmod{26}$$

Since

$$y \equiv ax + b \pmod{26}$$

We get

$$a^{-1}x + a^{-1}b \equiv ax + b \pmod{26} \tag{1}$$

Since (1) is true for all $a, b \in \{0, \ldots, 25\}$, we get

$$\begin{cases} a \equiv a^{-1} \pmod{26} \\ b \equiv -a^{-1}b \pmod{26} \end{cases}$$

(Continued on next page)

Lets look at the equation

$$a \equiv a^{-1} \pmod{26}$$

$$a^2 \equiv 1 \pmod{26}$$

$$a^2 - 1 \equiv 0 \pmod{26}$$

$$(a-1)(a+1) \equiv 0 \pmod{26}$$

One is tempted to say AHA- $a = -1 \equiv 25$ or $a = 1$. DONE. While this is true the reasoning is not quite right. Over the reals if $\alpha\beta = 0$ then you MUST have $\alpha = 0$ or $\beta = 0$. but over mod 26 you can have something like $6 \times 13 \equiv 0$.

So there might be solutions where either $a - 1$ is even and $a + 1 = 13$ or $a + 1$ is evern and $a - 1 = 13$. We leave it to the reader to show that neither is possible.

So $a = 1$ and $a = 25$ are the ONLY possibilities for a.

Alternatively you can go through all a relatively prime to 26 and see which ones give $a^2 \equiv 1$.

- When $a = 1$, then we have

$$\begin{aligned} b &\equiv -b \pmod{26} \\ \Leftrightarrow 2b &\equiv 0 \pmod{26} \end{aligned}$$

  There are only two possible values for b that satisfies this equation: $b = 0$ and $b = 13$. NOTE that this is the result that we achieved from previous homework. The reason is $a = 1$ means it is really a shift cipher.

- When $a = 25$, then

$$\begin{aligned} b &\equiv -25b \pmod{26} \\ \Leftrightarrow 26b &\equiv 0 \pmod{26} \end{aligned}$$

  Since this statement is always true, then for $a = 25$, b could be anything in $\{0, \ldots, 25\}$.

We conclude that all possible pairs for (a, b) are $(1, 0), (1, 13), (25, 1), \ldots, (25, 25)$.
If you missed a lot of pairs and didn't show work at all, you will lose credits. If you just get $(1, 0)$ and $(1, 13)$ and did explain how you got those answers, you've earned half credit. If you wrote a program to check all possible solutions and ended up with the same result, that is still okay.