MATH 312

NOVEMBER 28, 2018

AFFINE TRANSFORMATIONS
AND EXAM REVIEW
Let \( a, m \in \mathbb{Z} \) with \( m > 0 \) and \((a, m) = 1\), then \( a^{\phi(m)} = 1 \mod m\).

The order of \( a \) is the least positive integer such that \( a^n = 1 \mod m \).

\( a \) is a \underline{primitive root} \( \mod m \) if the order of \( a \) is \( \phi(m) \).

\[ \phi(7) = 6 \quad a \mod 7 \mid 1 \ 2 \ 3 \ 4 \ 5 \ 6 \]

| order | 1 \ 3 \ 6 \ 3 \ 6 \ 2 |

3 and 5 are \underline{primitive roots} of \( 7 \).
where \( q^n \) exists since \( a \) and \( n \) are relatively prime. However, if we do not have access to the encoding key \( (a, b) \), then we cannot determine \( Da,b \) unless we can figure it out from an intercepted message.

Example: Suppose we have intercepted the following ciphertext:

23 16 07 03 25 08 06 25 10 17 20 07 24 10 12 05 20
08 17 25 12 08 06 25 23 25 07 12 25 08 06 25 04 05
11 07 21 25 23 05 10 08 06 25 23 08 07 12 23 06 17 16
25 20 08 25 12 16 12 17 23 25

This corresponds to

XQHDZI62KRUHYKMFUIRZMl6GZXZHMZl6
ZFLHZXFK1GZFHMXGROZUIZM6M6RXZ-

where the most common letters are Z and I.

The most frequent letters in English are...

To be continued on 11/28/2018
E and T, so we guess

\[ E_{a,b}(E) = 2 \quad \text{and} \quad E_{a,b}(T) = 1 \]

Thus \[ D_{a,b}(x) = cx + kd \] must take values if guess is right.

\[
\begin{align*}
(D_{a,b}(25) = 4) & \iff (25c + d = 4 \mod 26) \\
(D_{a,b}(19) = 19) & \iff (8c + d = 19 \mod 26)
\end{align*}
\]

Eliminate \(d\) by subtraction

\[
17c = -15 \mod 26 = 11 \mod 26
\]

Solve \(17x \equiv 1 \mod 26\)

\[
17x = 1 + k(26)
\]

Review Euclidean Algorithm

\[ 26 = 17 + 9 \quad 17 = 9 + 8 \quad 9 = 8 + 1 \]

\[
\begin{align*}
1 & = 9 - 8 = 9 - (17 - 9) = 2\cdot 9 - 17 = 2\cdot (26 - 17) - 17 = \\
1 & = 2\cdot 26 - 3\cdot 17 \quad \text{Thus} \; 17(-3) - 26(-2) = 1
\end{align*}
\]

Thus \(17^{-1} \mod 26 = -3 \mod 26 = 23 \mod 26\)

and \(D_{a,b}(y) = 19y + 23 \mod 26\) so if we have guessed correctly - then the decrypted message is

\[
\begin{align*}
1815000204190704050813001105171413190804071907041804060418140579
\end{align*}
\]

Exercise - Decipher the above message
Variation Enlarge alphabet to a larger number of symbols. Example Enlarge to 28 symbols by adding blank space = 26 and $? = 27$. The affine cipher is then of the form

$$f(x) = ax + b \pmod{28}$$

with decryption of the form $g(y) = cy + d \pmod{28}$
EXAM REVIEW

I will work a variety of problems as part of a review for the final in 312. I suggest that you also work a variety of problems from old UBC Math 312 finals kept on the math department website.

1. Use mathematical induction to show that $3^n < n!$ for $n \geq 7$.

   **Solution:** Let $n = 7$. Then $3^7 = 2187 < 5040 = 7!$

   Suppose $N! > 3^N$ for some $N \geq 7$, then

   $(N+1)! = (N+1) \cdot N! > (N+1) \cdot 3^N > 3 \cdot 3^N = 3^{N+1}$.

2. Show that if $n$ is a positive integer, then $(n+1, n^2-n+1)$ is either 1 or 3.

   **Solution:** Suppose $d | (n+1)$ and $d | (n^2-n+1)$, then

   $d | (n^2-n+1) - (n+1)(n-2) \Rightarrow d | (n^2-n+1 - (n^2-n-2))$

   $\Rightarrow d | (n^2-n+1 - n^2+n+2) \Rightarrow d | 3$. Thus $d = 1$ or 3.

   Case 1: $n = 2$  $n+1 = 3$  $n^2-n+1 = 3$  $d = 3$