Day 04 – Ciphers Using Modular Arithmetic

Last time

**Theorem 1** (Quotient-Remainder Theorem). *Given an integer* $A$ *and a positive integer* $B$. *Then there exist integers* $q, r$ *obtained through long division* such that $A = B \cdot q + r$ *where* $0 \leq r < B$.

*Here, $q$ is quotient and $r$ is remainder. We say* $r = A \mod B$.

If $a, b$ are two integers with the same remainder under modulo $m$, then we say $a$ and $b$ are congruent modulo $m$ and write $a \equiv b \mod m$. 
Definition 1 (Inverse in modular arithmetic). If \( A \cdot C = 1 \mod B \) then \( C \) is the modular inverse of \( A \) under mod \( B \). Denote \( C = A^{-1} \mod B \).

If \( A^{-1} \) exists then we say that \( A \) is invertible under modulo \( B \).

Use the multiplication table to find the inverses under mod 26.
**Definition:** Let $d, n$ be integers. We say “$d$ divides $n$” or “$n$ is divisible by $d$” if there exist an integer $r$ such that $n = d \cdot r$. We write $d | n$ to denote that $d$ divides $n$. In this case, we also say that $d$ is a divisor of $n$.

Suppose we have two non-zero integers $m, n$. Then the common divisor of $m$ and $n$ is a positive integer $d$ such that $d | m$ and $d | n$.

The greatest common divisor (GCD) of two positive integers $m$ and $n$ is a common divisor $d$ such that for every other common divisor $d'$ of $m$ and $n$, $d' | d$. We write $d = \gcd(m, n)$.

If $\gcd(m, n) = 1$ then $m$ and $n$ are said to be relatively prime or coprime.

**Theorem 2.** $a$ is invertible under modulo $n$ if and only if $\gcd(a, n) = 1$. 
Affine cipher

A key is given by a pair of integers \((a, b)\) where

- \(a\) relatively prime to 26 and
- \(0 \leq b \leq 25\).

For each plaintext number \(x\) and ciphertext number \(y\),

- Encryption function \(y = E(x) = ax + b \mod p\)
- Decryption function \(x = D(y) = a^{-1}(y - b) \mod 26\)

Example. Encrypt the word S W O R D using the affine cipher mod 26 for \(a = 9\) and \(b = 15\).

<table>
<thead>
<tr>
<th>plaintext</th>
<th>S</th>
<th>W</th>
<th>O</th>
<th>R</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x)</td>
<td>18</td>
<td>22</td>
<td>14</td>
<td>17</td>
<td>3</td>
</tr>
<tr>
<td>(y = ax + b \mod 26)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ciphertext</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example. Decrypt the ciphertext S Y L N H knowing it was encrypted using affine cipher mod 26 for \(a = 19\) and \(b = 13\).

<table>
<thead>
<tr>
<th>ciphertext</th>
<th>S</th>
<th>Y</th>
<th>L</th>
<th>N</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>(y)</td>
<td>18</td>
<td>24</td>
<td>11</td>
<td>13</td>
<td>7</td>
</tr>
<tr>
<td>(x = a^{-1}(y - b) \mod 26)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>plaintext</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Modulo arithmetic on matrices

Definition. Let $A, B$ be $m \times n$ matrices with integer entries. We say that $A$ and $B$ are congruent modulo $m$ if

$$a_{i,j} \equiv b_{i,j} \mod m$$

for all entries $a_{i,j}, b_{i,j}$. We write $A \equiv B \mod m$.

Example. In modulo 5, consider $A = \begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$.

- $A + 2B \mod 5 =$

- $AB \mod 5 =$

- $BA \mod 5 =$

Definition. Let $m$ be a given modulus and let $A$ be an $n \times n$ matrix with integer entries. $A$ is said to be invertible modulo $m$ if there exists an $n \times n$ matrix $B$ such that

$$AB = I \mod m \quad \text{and} \quad BA = I \mod m.$$

We write “$A^{-1} = B \mod m$” to denote $B$ is the inverse of $A$ modulo $m$. 
**Definition.** The **determinant** of $A$ modulo $m$ is $\det(A)$ reduced mod $m$.

**Example.** Find the determinant of $A = \begin{bmatrix} 3 & 4 \\ -9 & 8 \end{bmatrix}$ under mod 10.

**Theorem 3.** If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an integer entries then the determinant of $A$ under modulo $m$ is given by

$$
\det(A) = ad - bc \mod m.
$$

$A$ is invertible modulo $m$ if and only if $\det(A)$ is relatively prime to $m$. In this case, the inverse is given by

$$
A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \mod m
$$

**Example.** Find the inverse of $A = \begin{bmatrix} 1 & 4 \\ 8 & 11 \end{bmatrix}$ under mod 26.