Day 04

Monday, April 9, 2018 9:03 AM

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 $r = A \mod B$.*

$A = B.q + r$

quotient remainder

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 $a \equiv b \mod m$.

Ex: -8 and 8 are congruent mod 16.

$8 = 16 \times 0 + 8$ → remainder 8

$-8 = 16 \times (-1) + 8$

$8 \equiv -8 \mod 16.$

Vernam cipher

. Randomize 2 short keys U and V.

Construct long key $K = U + V \mod 26.$

$$\begin{tikzcd}
\boxed{\text{plaintext}} \arrow[r, leftrightarrow] & \boxed{M} \arrow[r, bend left, "C = M + K \mod 26"] & \boxed{C} \arrow[l, bend left, "M = C - K \mod 26"] \arrow[r, leftrightarrow] & \boxed{\text{ciphertext}}
\end{tikzcd}$$

$A = 0$

$B = 1$

$C = 2$

$\vdots$

$Z = 25$

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

. look for $\underline{1}$ inside the table.

then row & column of this entry form a pair of inverses

$1^{-1} = 1$

$3^{-1} = 9$; $9^{-1} = 3$

$5^{-1} = 21$; $21^{-1} = 5$

$7^{-1} = 15$; $15^{-1} = 7$.

$11^{-1} = 19$; $19^{-1} = 11$

$17^{-1} = 23$; $23^{-1} = 17$

$25^{-1} = 25$

There are 12 invertible number in mod 26.

gcd (any of these 12, 26) = 1

These 12 numbers are co-prime to 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* $\gcd(a, m) = 1$.

Ex: $\gcd(60, 42)$

Find prime factorization of 60 & 42

$60 = 2^2 \times 3^1 \times 5^1$

$42 = 2^1 \times 3^1 \times 7^1$

To get the gcd, collect all the common primes and raise them to the lowest power in the factorization

$\gcd = 2^1 \times 3^1 = 6$

3

Ex: Solve for x:

(a) $7x + 5 = y \mod 26$

$7x = y - 5 \mod 26$

$\underbrace{15 \cdot 7}x = 15(y - 5) \mod 26$

$x = 15(y - 5) \mod 26$

(b) $8x + 5 = 10 \mod 26$

$8x = 5 \mod 26$

No soln.

Another alphabet has 29 letters

Choices for a: $29 - 1 = 28$ (1, 2, 3, ..., 28 b/c 29 is a prime number)

b: 29

$|K| = 28 \times 29$

Affine cipher

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

- a relatively prime to 26 and
- $0 \le b \le 25$.

a must have an inverse mod 26.

$|K| = 12 \times 26$

12 choices for a

26 choices for b.

For each plaintext number x and ciphertext number y,

- Encryption function $y = E(x) = ax + b \mod \cancel{n}$ 26
- 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**.

plaintext	S	W	O	R	D
x	18	22	14	17	3
$y = ax + b \mod 26$	21	5	11	12	16
ciphertext	V	F	L	M	Q

$9 \times 18 + 15 = 21$

$9 \times 22 + 15 = 31 = 5$

$9 \times 14 + 15 = \dots = 11$

$\vdots$

$a^{-1} = 11.$

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

ciphertext	S	Y	L	N	H
y	18	24	11	13	7
$x = a^{-1}(y - b) \mod 26$	3	17	4	0	12
plaintext	D	R	E	A	M

$a^{-1}(y - b)$

$11 \times (18 - 13) = 11 \times 5 = 3$

4

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 $A \equiv B \mod m$.

$$\begin{bmatrix} 3 & 8 \\ 11 & 15 \end{bmatrix} \equiv \begin{bmatrix} 19 & -8 \\ 43 & -1 \end{bmatrix} \bmod 16$$

$3 \equiv 19 \bmod 16$
$8 \equiv -8 \bmod 16$
$11 \equiv 43 \bmod 16$
$15 \equiv -1 \bmod 16$

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

- $A + 2B \mod 5 =$

$$\begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ \cancel{6}\,1 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 7 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 3 & 0 \end{bmatrix} \bmod 5$$

- $AB \mod 5 =$

$$\begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 10 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 5.$$

- $BA \mod 5 =$

$$\begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 5 \\ 10 & 11 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 5.$$

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.

5

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.

$$\det(A) = ad - bc = (3)(8) - (-9)(4) = 60$$
$$= 0 \bmod 10$$

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

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

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

$\det(A) = (11)(1) - (8)(4) = 5 \bmod 26.$

Here, $\gcd(5, 26) = 1$ then A is invertible.

$\det(A)^{-1} = 5^{-1} = 21 \bmod 26.$

$$A^{-1} = 21 \begin{bmatrix} 11 & -4 \\ -8 & 1 \end{bmatrix} = \dots = \begin{bmatrix} 23 & 20 \\ 14 & 21 \end{bmatrix} \bmod 26.$$

Check that 6 $A \cdot A^{-1} = I \bmod 26$

$A^{-1} \cdot A = I \bmod 26.$