1ZC3

Last Day Modular Arithmetic

We create in integers, equivalence classes (i.e. congruence classes i.e. residue classes)

$a \equiv b \mod p$ means $a = b + np$, $n \in \mathbb{Z}$

(alternate notation $a = b \mod p$, or $a =_p b$)

eg $2 \mod 6$ is $2 \equiv 8 \equiv 14 \equiv -4 \equiv -10 \equiv +62 \mod 6$.

all represent same residue class mod 6

"same number"

Usually represent each class by its "least residue"
the lowest +ve, or 0 integer in the class!

eg. "mod 6" $\left.\begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 \end{matrix}\right\} = \mathbb{Z}_6$ space!

In general "mod p" classes form $\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$

Note: If $a \equiv b \mod p$ & $c \equiv d \mod p$

$$a + c \equiv b + d \mod p$$

Proof

$$a \equiv b \mod p \iff a = b + np$$

$$c \equiv d \mod p \iff c = d + mp$$

$$
\begin{aligned}
b + d &= a - np + c - mp \\
&= a + c - np - mp \\
&= (a+c) + (-m-n)p \\
&\equiv a+c \mod p
\end{aligned}
$$

Subtraction works same way!

How about multn?

$$
\begin{aligned}
ac &= (b+np)(d+mp) \\
&= bd + \underbrace{ndp + bmp + (nmp)p}_{\text{Integer multiple of } p} \\
&\equiv bd \mod p
\end{aligned}
$$

eg let work in $\mathbb{Z}_5$

$$2 \cdot 4 = 8 \equiv 3 \mod 5$$

$$22 \cdot (-1) = -22 \equiv 3 \mod 5$$

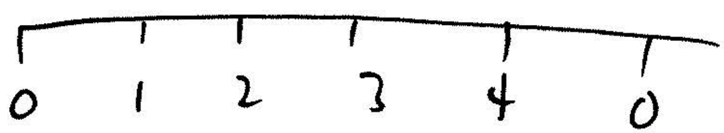
$+25$
$\equiv 0$

---

division & inverse "mod p"

a^{-1} is defined as the element of $\mathbb{Z}_p$ such that $a a^{-1} \equiv 1 \mod p$.

eg. In $\mathbb{Z}_5$



$$1^{-1} = \frac{1}{1} = 1 \qquad 2^{-1} = \frac{1}{2} \equiv 3 \qquad 2 \cdot 3 = 6 \equiv 1 \mod p$$

e.g. Working in $\mathbb{Z}/_5$ (i.e. "mod 5")

Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

Is A invertible?

What is A^{-1} (if anything?)

<u>Solution</u> $\det(A) = 1(4) - 2(3) = 4 - 6 = -2 \equiv 3 \bmod 5$

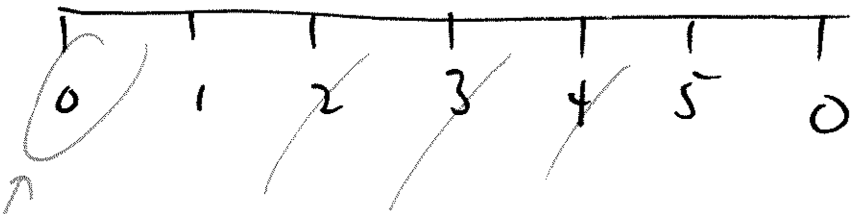
$\not\equiv 0 \bmod 5 \Rightarrow$ <u>A^{-1} exists!</u>

<u>(if $\det(A) \equiv 0 \bmod p \Leftrightarrow$ no inverse)</u>

<u>Rule</u> as <u>before</u> $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \cdot (ad - bc)^{-1}$

So in "mod 6", $\mathbb{Z}_6$

$6 = 2 \cdot 3$



none!

no inverse!

Only 1 & 5 have inv. mod 6

Modular Math & Matrices: All our matrix rules & constructions work as usual *if* we're careful to follow $\mathbb{Z}_p$ rules!

<u>Note</u> $aa^{-1} \equiv 1 \bmod p$ (if a^{-1} <u>exists</u>)

$aa^{-1} = 1 + np$

<u>then</u> $(aa^{-1} - np) = 1$ if $a=2$, $p=6$

$\Rightarrow aa^{-1} - np$ is <u>even</u>

so 2^{-1} <u>DNE</u>

If a, p have a <u>common</u> <u>factor</u> k

$\Rightarrow$ 1 is divisible by k $\Downarrow$ ie <u>no</u> <u>a^{-1}</u> <u>exists</u>!

ie If <u>greatest</u> <u>common</u> <u>divisor</u> $\gcd(a,p) \neq 1$

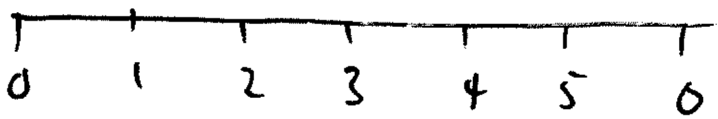
$\Rightarrow$ <u>no inverse</u>

<u>Can</u> <u>show</u> opposite is <u>true too</u>! $\gcd(a,p) = 1$

$\Rightarrow$ <u>inverse exists</u>

$3^{-1} = \frac{1}{3} \equiv 2$ $\qquad$ $4^{-1} \equiv (-1)^{-1} \equiv -1 \equiv 4 \mod p$

eg. In $\mathbb{Z}/_6$



$1^{-1} \equiv 1 \mod 6$ $\qquad$ $5^{-1} \equiv (-1)^{-1} \equiv -1 \equiv 5 \mod 6.$

$2^{-1} = ?$

$2\cdot 1 = 2$ $\qquad$ $2\cdot 3 \equiv 0 \mod 6$

$2\cdot 2 = 4$ $\qquad$ $2\cdot 4 = 8 \equiv 2 \mod 6$

$2\cdot 0 = 0$ $\qquad$ $2\cdot 5 = 10 \equiv 4 \mod 6$

2^{-1} DNE!

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} \cdot (\cancel{3^{-1}}) \quad 2 \bmod 5$$

$$\equiv \begin{bmatrix} 8 & -4 \\ -6 & 2 \end{bmatrix} \bmod 5$$

$$\equiv \begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix} \bmod 5 = A^{-1}$$

Cryptography App: The Hill Cypher

1) Write alphabet to integer!

A	B	C	.....	M	N	......	Y	Z
1	2	3		13	14		25	0

"mod 26"

$\mathbb{Z}_{26}$

Set!

2) Break Message in to n-length Vectors!

eg "Yo" $= \begin{bmatrix} 25 \\ 15 \end{bmatrix}$

3) Multiply Each vector by A invertible mod 26.

$\Rightarrow$ Encrypted!

4) Mult. by A^{-1} to decrypt!