Daily Post Sol^{n}s

1) Sage – demo overflow

2) $2 \not\equiv 4 \pmod{10}$, $5 \not\equiv 0 \pmod{10}$, but $2 \cdot 5 \equiv 0 \equiv 4 \cdot 5 \pmod{10}$

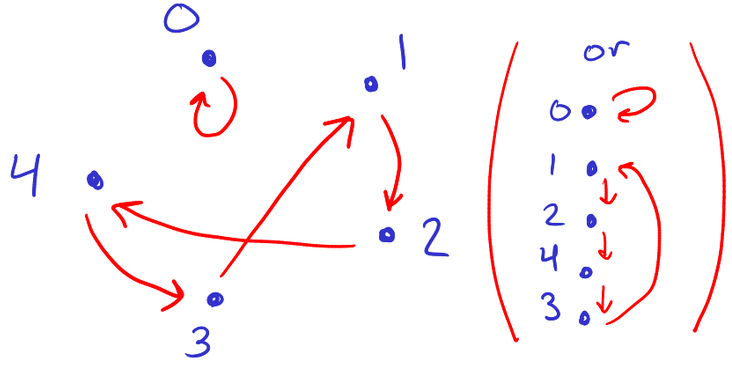
can't cancel the 5 ✡

3) mod 11: $10^{12} \equiv (-1)^{12} \equiv 1 \not\equiv 10^1$ can't reduce exponent mod 11 ✡

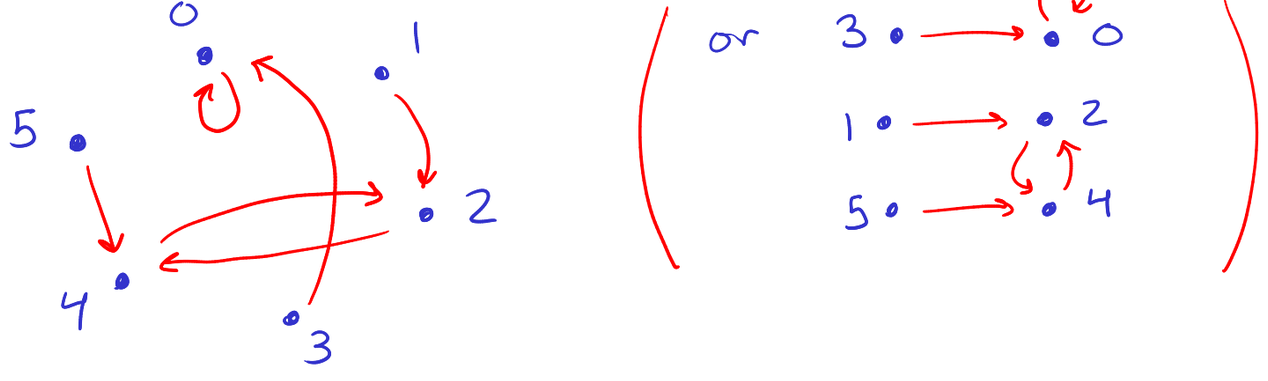
4) mod 13: $13131312^{50\,000} \equiv 12^{50\,000} \equiv (-1)^{50\,000} \equiv 1$

mod 8: $3^{50\,000} \equiv (3^2)^{25\,000} \equiv 1^{25\,000} \equiv 1$

6) mod 5: $x \mapsto 2x$



7) mod 6: $x \mapsto 2x$



A	B	C	...	Z
00	01	02		25

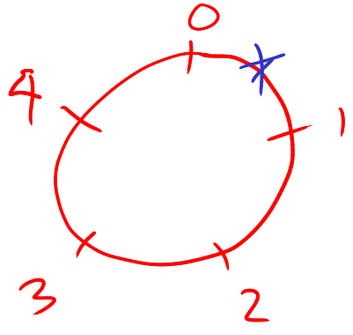
Affine cipher. $\text{key} = (\alpha, \beta) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2 = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Encryption: $m \longmapsto \alpha m + \beta \pmod{n}$

keyspace size $= 26^2$

BUT! not all keys work.

Ex. $n = 5$ $\quad \text{key} = (2,0) = (\alpha, \beta)$



m	2m = ciphertext
0	0
1	2
2	4
3	1
4	3

inverse

Pair: What is the decryption fn?

c	m = 3c
0	0
1	3
2	1
3	4
4	2

$3 \cdot 2 \cdot c \equiv 1 c \equiv c$

$2 \cdot 3 \equiv 1 \pmod{5}$

↺ inverses (multiplicative inverse)

So mult. by 3 "undoes" mult. by 2.

A good name for 3 is "that which, when multiplied by 2, gives 1".

ie. $3 \equiv \frac{1}{2} \equiv 2^{-1} \pmod 5$

Pairs: Which a are invertible (have a multiplicative inverse) mod n?

eg. mod 5: 2 has an inverse
0 does not

Consider mod 5, 6 as good examples

mod 5: invertible: 1, 2, 3, 4 not: 0

mod 6: invertible: 1, 5 not: 0, 2, 3, 4

Def^n. Let $a \in \mathbb{Z}/n\mathbb{Z}$. The **multiplicative inverse of a** is the element (if it exists) which multiplies by a to give 1.

We denote it by a^{-1} or $\frac{1}{a}$ and write the property as

$$\boxed{a^{-1} \cdot a \equiv 1 \pmod{n}}$$

If the invere exists, we say a is **invertible**.
If it does not, we say a is **not invertible**.

Ex. (A) $2^{-1} \equiv 3 \pmod 5$ and $3^{-1} \equiv 2 \pmod 5$ because $2 \cdot 3 \equiv 1 \pmod 5$.

(B) $2 \bmod 26$ is not invertible.

Think: • Any multiple of 2 is **even** & **stays even** when reducing.

• try to solve $2x \equiv 1 \pmod{26}$ but $\underset{\text{even}}{2x} + 26k = \underset{\text{odd}}{1}$ $\rightarrow\leftarrow$

Affine cipher: encryption: $m \longmapsto \alpha m + \beta \mod n$

decryption: $c \longmapsto \alpha^{-1}(c - \beta) \mod n$

only works if α is invertible!

What about matrices?

Reminder $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Mod n: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \equiv (ad-bc)^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod n$

$\equiv$ if determinant is invertible

Hill Cipher. key: $A \in M_{d\times d}(\mathbb{Z}/n\mathbb{Z}) =$ $d \times d$ matrices w/ entries mod n

Encryption: $\vec{m} \longmapsto A\vec{m}$

Decryption: $\vec{c} \longmapsto A^{-1}\vec{c}$

where $\vec{m} \in (\mathbb{Z}/n\mathbb{Z})^d$

d-dim^l vector

d = dimension.

Need: $\det(A)$ invertible

Example. $A = \begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix}$ mod 26

$\det = -3$

$$A^{-1} = \frac{1}{-3}\begin{pmatrix} 3 & -2 \\ -3 & 1 \end{pmatrix} \qquad (-3)\cdot(-9) = 27 \equiv 1 \pmod{26}$$

$$= -9\begin{pmatrix} 3 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -8 \\ 1 & -9 \end{pmatrix}$$

HI $\xrightarrow{\text{vector}}$ $\begin{pmatrix} 7 \\ 8 \end{pmatrix}$

Encryption: $\vec{c} = A \cdot \vec{m} = \begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 23 \\ 19 \end{pmatrix}$

Decryption: $\vec{m} = A^{-1}\vec{c} = \begin{pmatrix} -1 & -8 \\ 1 & -9 \end{pmatrix} \begin{pmatrix} 23 \\ 19 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix}$ YAY!

Proposition. Let $a \in \mathbb{Z}/n\mathbb{Z}$. There's at most one b s.t. $ba \equiv 1 \pmod n$. $\pmod n$

Pf. Sps a has two inverses, b and b'.

Then $x \mapsto ax$ and $x \mapsto bx$ ($ax \mapsto bax = x$) are inverse functions of each other.

So $x \mapsto ax$ is bijective.

But $ab \equiv 1 \equiv ab'$. This is a failure of injectivity.

This contradicts $x \mapsto ax$ being bijective. ∎

Puzzle: How to efficiently compute $a^{(\text{big exp})} \bmod n$?