Instructions

- Use Latex (Submit only pdf file, Mention Name, Roll No. in title)
- Private submission on Piazza (Ask TA for help with submission)
- Select appropriate folder (e.g. hw2)
- Subject of post: `<HW#>_<Roll#>`

How many keys?

- Take the number formed by the 2^{nd} last and 3^{rd} last digits of your roll-number (say r)
- [1]Assume Affine Cipher defined over $\mathbb{Z}_r$
- Find number of possible keys for "your" Affine Cipher?
- Note: if $r < 15$, take $r = 58$.

[1]Recall definition of $\mathbb{Z}_m$ from class

Euler Phi Function

- Find out about the Euler Phi Function and how it is related to the affine cipher.
- Now solve Problem-1 using it.

Bijection

- Consider the two sets $X = \{x_1, x_2, \cdots, x_n\}$ and $Y = \{y_1, y_2, \cdots, y_n\}$, and a function $f : X \to Y$.
  Show that if X and Y have the same cardinality and if f is an injection, then f is a bijection.

Euclidean GCD

Implement the Euclidean GCD Algorithm in `python`.

Involutory Key

- A key is called involutory when $e_K = d_K$
- Let an Affine Cipher be defined over $\mathbb{Z}_m$ with key $K = (a, b)$.
- Prove that K is an involutory key if and only if

$$a^{-1} \mod m = a$$

and

$$b(a+1) \equiv 0 \mod m$$

- Now find all involutory keys in $\mathbb{Z}_{15}$ for the Affine Cipher