\[ \phi(n) \text{ is a function of } \prod_{i=1}^{k} p_i^{e_i} \]

\( \phi(n) \) - Euler\'s totient function

\[ n = \prod_{i=1}^{k} p_i^{e_i} \]
\[
\mathbb{Z} = \{ a \cdot b, a, b, -a, -b, \ldots, a^n, b^n, -a^n, -b^n, \ldots \}
\]

If \( a, b \in \mathbb{Z} \), then define \( a \cdot b \) to be the integer under multiplication.

\[
\mathbb{Z}^* = \mathbb{Z} - \{0\} = \{a \cdot b, a, b, -a, -b, \ldots, a^n, b^n, -a^n, -b^n, \ldots : a, b \neq 0\}
\]
is $z_1 = z^*_n$ ?

$\rightarrow$ all elements are from $\mathbb{Z}_n^*$

$\rightarrow$ each element is computed from 1 element of $\mathbb{Z}_n^*$

$\rightarrow$ so?

(1) all elements of $z'_1$ are distinct

$\rightarrow z'_1 \neq z^*_n$

(2) some duplicates
has to show all factors with \( n \)

now no factors with \( n \)

\[(b - b) (a + b) = (a - b) \]

\[\overline{ab = b + 8} \quad \text{equal, because} \]

\[ab = a + b\]

\[a \neq b \]

\[\text{and} \]

\[\text{such that } b \neq b\]

\[\text{Suppose } \exists \text{ 2 numbers } b, b \in \mathbb{Z} \]
If $a \in \mathbb{Z}$, then there exists $b \in \mathbb{Z}$ such that $a \cdot b \equiv 1 \pmod{m}$.
\[ 8 \equiv 2 \equiv 4 \pmod{8} \]

\[ \{1, 2, 4, 7, 8, 11, 13, 14\} \]

\[ 3 \cdot 5 = 15 \]

\[ \phi(6) = \{1, 2, 4, 5, 7, 8\} \]

Euclid's Theorem

\[ n \leq 2^\alpha \cdot 3^\beta \cdot \ldots \cdot \text{prime factors} \]

If \( a \equiv b \mod{n} \), then \( a^\phi(n) \equiv b^\phi(n) \mod{n} \)
(a, b) median. (a_1, b_1) median = A median

\[ A = c \]

\[ \text{Same as } b_0 \cdot b_1 \cdot b_2 \cdot \ldots = C \text{ mod } n \]

Multiply all elements
\[ a_{n+1} = \frac{1}{a_n} \]

\[ C = A \]

\[ a < \bar{a}, \bar{a} = \text{mean} \]

\[ a < \bar{a} \Rightarrow \text{median} = A \text{ mean} \]

\[ a, 0.6, b, c \]
RA ruling

If \((m^n)^p = n \mod q\) then find \(d \) such that \(e.d = 1 \mod \phi(n)\). Choose a common key.

\[ e.d = k.q(n) + 1 \]

\[ e.d = 1 \mod \phi(n) \]
\[ m < n \]

\[
\text{med} = k \varphi(n) + 1 \]

\[
= m \underbrace{\varphi(n) \cdot \varphi(n) \cdots \varphi(n)}_{k \text{ times}} + 1
\]

\[
= m \quad \text{mod} \ n
\]
RSA works when $m \in \mathbb{Z}_n^*$

but what if $m \in \mathbb{Z}_n$

- does it work... (how)?
Choose a, find d, e, d = 1 (mod φ(n))

\[ \varphi(n) = n \cdot \Phi(n) \]

such that

\[ ax + by = \varphi(n) \]

\[ \therefore \]

Extended Euclidean Algorithm:

evaluated at 
\[
\begin{align*}
\text{If } y \in o_p \Rightarrow d = (y, y) \\
\text{so } d = y \\
\text{hence } d = y
\end{align*}
\]

\[
\begin{align*}
\forall \epsilon > 0, \exists \delta > 0 \text{ such that } d < \delta \Rightarrow y \in o_p \\
\text{hence } y = 1
\end{align*}
\]
If not check new $n+1, n+2, \ldots$

Test for prime $n$

Now pick a large # at random

Prime #

And a final $p_j$'s

One of these $p, q$, we get $e, d$
Proverbially, probably to shy
4. da best many times

2. Miller Analog Test

1. Forward test of personality