\[ \phi(n) = \# \text{ values } 1, 2, 3, \ldots, n \text{ relatively prime with } n. \]

\[ \phi(p^k) = p^k - p^{k-1}, \quad p \in \text{Prime} \]

\[ = p^k(1 - p^{-1}) = p^k \left( \frac{p-1}{p} \right) \]

If \( \gcd(m, n) = 1 \), \( \phi(mn) = \phi(m) \phi(n) \)

\[ n = \prod_{\text{Prime factorized}} p_i^{a_i} \]

\[ \phi(n) = \prod_{\text{Prime factorized}} (p_i^{a_i} - p_i^{a_i-1}) \]

\[ = \prod_{\text{Prime factorized}} p_i^{a_i} \left( \frac{p_i-1}{p_i} \right) \]

\[ n = 96 \]

\[ \text{primes} = 2, 3 \]

\[ 96 \times \frac{1}{2} \times \frac{2}{3} = \sqrt{32} \]

The keys affine cipher

w/ alphabet size of \( n \)

\[ = n \phi(n) \]

\[ \uparrow \quad \uparrow \]

# choices \# choices

for b for c

Only over \# unique primes in factorization of \( n \).
(1) Euler's Theorem

2) Miller-Rabin Primality Test

Start w/ a set \( S = \{q_1, q_2, \ldots, q_{\phi(n)}\} \)

where \( q_i \in \{1, 2, 3, \ldots, n\} \) \& \( \gcd(q_i, n) = 1 \) \( q_i \)'s unique.

Reduced Residue System Mod n

- If \( n = 6 \), \( S = \{1, 5\} \)
- If \( n = 15 \), \( S = \{1, 2, 4, 7, 8, 11, 13, 14\} \)

Pick any value \( a \), \( \gcd(a, n) = 1 \) and create a set \( T = \{a, aq_1, aq_2, aq_3, \ldots, aq_{\phi(n)}\} \)

- If \( a = 3 \), \( n = 6 \), \( T = \{3, 6\} \)
- If \( a = 4 \), \( n = 15 \), \( T = \{4, 8, 16, 28, 32, 44, 57, 56\} \)

Prove all elements in \( T \mod n \) are equivalent to elements in \( S \).

\( \Rightarrow \) 1) All values in \( T \) are unique mod n

2) All values in \( T \) are relatively prime to n.

Proof of #2: \( \gcd(a, n) = 1 \), \( \gcd(q_i, n) = 1 \)

\( \Rightarrow \) \( \gcd(aq_i, n) = 1 \).
Proof by contradiction for #1

Assume \( \exists a_i, a_j \in S \mid a_i \neq a_j \) but

\[ a a_i \equiv a a_j \pmod{n} \]

\[ a a_i - a a_j = 0 \pmod{n} \]

\[ a(a_i - a_j) \equiv 0 \pmod{n} \]

\[ \Rightarrow n \mid a(a_i - a_j) \]

If \( a \mid bc \), and \( \gcd(a, b) = 1 \), then \( a \mid c \).

Because \( \gcd(a, n) = 1 \Rightarrow n \mid (a_i - a_j) \)

Contradiction 1 \( \leq a_i, a_j \leq n-1 \land a_i \neq a_j \)

So 1 \( \leq |a_i - a_j| \leq n-2 \)

\[ \prod_{i=1}^{\phi(n)} a_{a_i} \equiv \prod_{i=1}^{\phi(n)} q_i \pmod{n} \]

Product of items in S

Product of items in \( \frac{\phi(n)}{\phi(n)} \)

\[ a \times \prod_{i=1}^{\phi(n)} q_i \equiv \prod_{i=1}^{\phi(n)} q_i \pmod{n} \]

Let \( Z = \prod_{i=1}^{\phi(n)} a_i \)

\[ a^Z \equiv Z \pmod{n} \]

\[ a^{\phi(n)} Z - Z \equiv 0 \pmod{n} \]

\[ Z^{(a^{\phi(n)} - 1)} \equiv 0 \pmod{n} \]

\[ n \mid \{ Z^{(a^{\phi(n)} - 1)} \} \]

Because \( \gcd(n, Z) = 1 \), it follows that \( n \mid (a^{\phi(n)} - 1) \)
\[ \phi(n) - 1 \equiv 0 \pmod{n} \]
\[ \phi(n) \equiv 1 \pmod{n} \]

Euler's Theorem

What is the remainder when
\[ 67^{201} \]
is divided by 15
\[ 67^{201} \equiv 7^{201} \pmod{15} \]

\[ \gcd(7, 15) = 1, \text{ so by Euler's Theorem} \]
\[ \phi(15) \]
\[ 7^{8} \equiv 1 \pmod{15} \]

\[ 7^{201} = 7^{200+1} \equiv 7^{8 \times 25 \times 1} \]
\[ \equiv (7^{8})^{25} \times 7 \pmod{15} \]
\[ \equiv \overbrace{25 \times 7} \]
\[ \equiv 7 \pmod{15} \]
Primality Testing

Probabilistic Algorithm:
- if the Miller-Rabin says "no," the number is definitely composite.
- if the alg. says "yes" it really means "is Probably Prime"

\[ \gcd(a, n) = 1 \quad a^{n-1} \equiv 1 \pmod{n} \]

Is this true for composites? Or how often is it true for composites?

If \( n \) is composite, \( \phi(n) < n-1 \)

\[ a^{a^{n-1}} \equiv a \pmod{n} \]

Could be 1, we don't know

Turns out it's rarely equal to 1 for composites.

For a random composite \( n \), random int a \( \gcd(a, n) = 1 \), probability this is 1 is \( \frac{1}{2} \).
Original Idea

\[ \text{isPrime}(\text{int } n) \]
\[ a = \text{randint}(1, n-1) \]
\[ \text{if } (\gcd(a, n) \neq 1) \]
\[ \text{return false} \]
\[ \text{ans} = \text{pow}(a, n-1) \bmod n \]
\[ \text{return ans} = 1 ? \]

Fix #1

\[ \text{isPrime}(\text{int } n, \text{int rep}) \]
\[ \text{for } (i = 0; i < \text{rep}; i++) \]
\[ a = \text{randint}(1, n-1) \]
\[ \text{if } (\gcd(a, n) \neq 1) \]
\[ \text{return false; } \]
\[ \text{ans} = \text{pow}(a, n-1) \bmod n \]
\[ \text{if } (\text{ans} \neq 1) \text{ return false; } \]
\[ \text{return true; } // \text{ is probably prime} \]

Probability a composite makes it through this is \( \frac{1}{100} \)
The rep of 100 makes it crazy small

\[ \frac{1}{2^{\text{rep}}} \]

\[ \text{This isn't Miller-Rabin...} \]
\[ \text{We'll get there on Monday.} \]