# Primality Tests

## Cryptography - Applied Number Theory

**CSE 496**
**Second Presentation**

**Baran Solmaz**

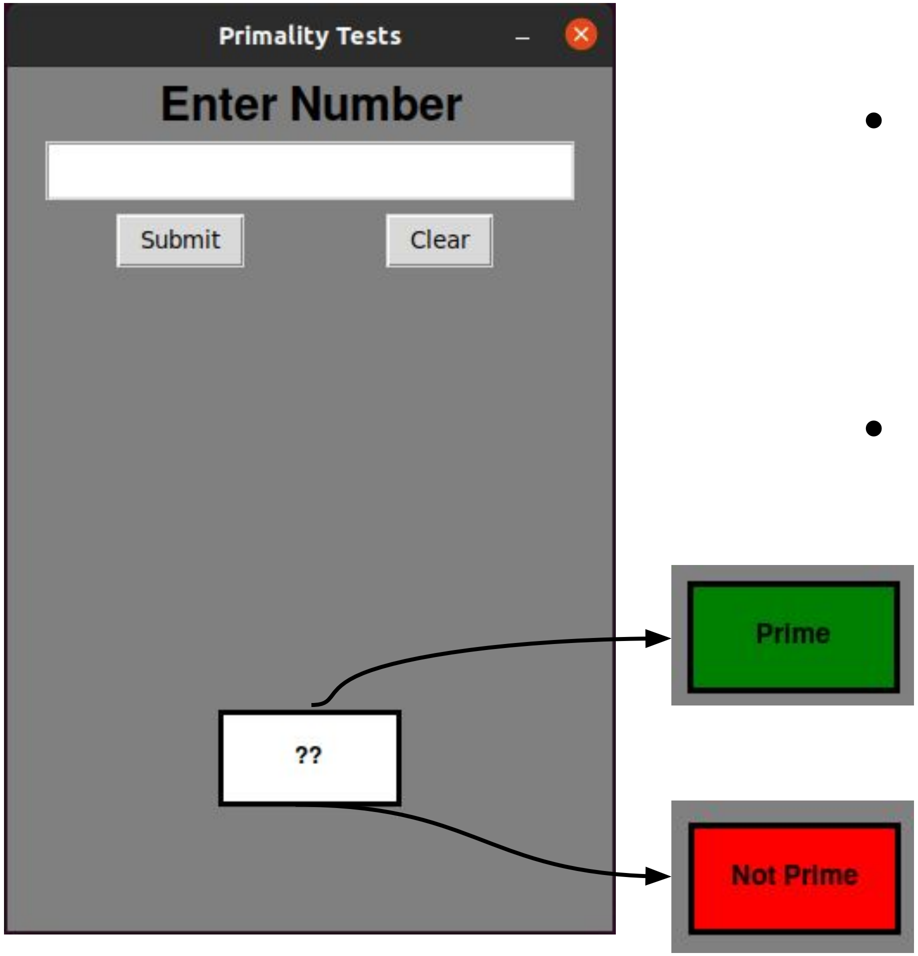
**Project Advisor: Dr. Tülay AYYILDIZ AKOĞLU**

**May 2023**

# Contents

- Project Summary
- Additional Information
- Current Status
- Solution Approaches
- Future Plans
- References

# Project Summary

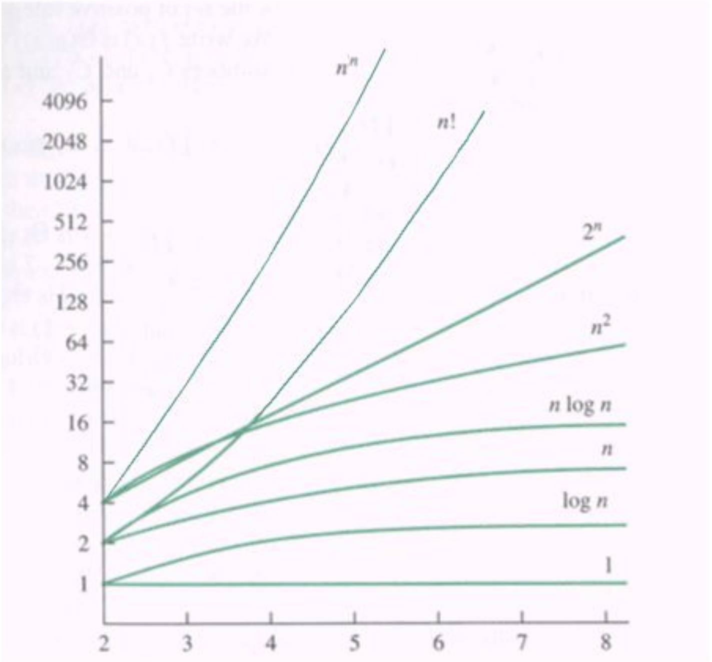



- Project Description:
  - Takes natural number,
  - Checks whether it is prime or not.
- Aim:
  - Handling Pseudo-primes.

# Additional Information

- Reason

| | Time Complexity |
|---|---|
| School Method | $O(n)$ |
| Optimized School Method | $O(\sqrt{n})$ |
| Fermat's Test | $O(k * log(n))$ |
| Miller-Rabin Test | $O(k * log(n))$ |
| AKS Test | $O(log(n)^6)$ |




- AKS Test

$$(X+a)^n \equiv X^n + a \,(mod\, n)$$

n: number to be checked for primality
a: any number that coprime to n
X: unknown variable

- Improved version of Fermat's Test

# Current Status

- GUI
- Test Implementations
  - Fermat’s Test
  - Miller-Rabin Primality Test
- Solution Approaches
  - Carmichael Control
  - Strong Pseudoprime Control

# Solution Approaches - I

- Carmichael Control

Definition: Carmichael numbers are composite numbers n such that

$$a^{n-1} \equiv 1 \, mod \, n$$

for every a coprime to n.

561 = 3 * 11 * 17

$$2^{560} \equiv 1 \, (mod \, 561)$$

$$447^{560} \equiv 375 \, (mod \, 561)$$

447 = 3 * 149

$$19^{560} \equiv 1 \, (mod \, 561)$$

$$22^{560} \equiv 154 \, (mod \, 561)$$

# Solution Approaches - I

- Carmichael Control

$$a^{n-1} \equiv 1 \, mod \, n$$

for every a coprime to n.

561 = 3 * 11 * 17

$$2 \leq X < 561$$

Has common divisor : 240
Coprime : 319

$$\sqrt{n} \quad \sim 11$$

$$\sqrt{\sqrt{n}} \quad \sim 3$$

41041 = 7 * 11 * 13 * 41

$$2 \leq X < 41041$$

Has common divisor : 12240
Coprime : 28799

$$\sqrt{n} \quad \sim 60$$

$$\sqrt{\sqrt{n}} \quad \sim 4$$

- Unique interval for bigger integers

# Solution Approaches - II

- Strong Pseudoprime Control
  - AKS Test:

$$(X+a)^n \equiv X^n + a \,(mod\, n)$$

Ex1:

$$(X+2)^5 \equiv X^5 + 2 \,(mod\, 5)$$

$$\cancel{X^5} + \cancel{10X^4} + \cancel{40X^3} + \cancel{80X^2} + \cancel{80X} + 32$$

$$\equiv$$

$$\cancel{X^5} + 2 \,(mod\, 5)$$

$$32 \equiv 2 \,(mod\, 5)$$

$$2 \equiv 2 \,(mod\, 5)$$

5 is prime.

Ex2:

$$(X+3)^4 \equiv X^4 + 3 \,(mod\, 4)$$

$$\cancel{X^4} + \cancel{12X^3} + 54X^2 + \cancel{108X} + 81$$

$$\equiv \cancel{X^4} + 3 \,(mod\, 4)$$

$$2X^2 + 1 \equiv 3 \,(mod\, 4)$$

4 is not prime.

# Future Plans

- Implementing Solution Approaches
- Improving Solution Approaches
- Efficient Thread Control

# References

- Carmichael Numbers - OEIS
- Carmichael Numbers - GFG
- Carmichael Numbers - Wikipedia
- Strong Pseudoprimes - OEIS
- Strong Pseudoprimes - Wikipedia
- Wilson’s Theorem - GFG
- AKS Test - Primes is in P - Agrawal,Kayal,Saxena
- AKS - Mathworld Wolfram
- Graph of Function Growths