MATH 314 Fall 2023 - Class Notes

9/5/2023 11/2/2023

Scribe: Name Brian Righini

Summary: Miller Rabin primality test.

Miller-Rabin Primality Test

Take an odd integer $n > 1$ to be tested for primality. Let $n - 1 = 2^s \cdot d$ where s is the largest integer such that 2^s divides $n - 1$, and d is an odd integer.

- **Witness Generation:** Choose a random integer a such that $2 \leq a \leq n - 2$.
- **Exponentiation:** Compute $x = a^d \mod n$.
- **Primality Test:**
  - If $x \equiv 1 \mod n$ or $x \equiv -1 \mod n$, then n passes the test for this particular a.
  - If x is neither 1 nor -1 after the exponentiation, proceed to the next steps.
- **Repeated Squaring:** For $r = 1, 2, \ldots, s - 1$, compute $x = x^2 \mod n$.
- **Final Test:**
  - If $x \equiv 1 \mod n$, n is likely composite.
  - If $x \equiv -1 \mod n$, n passes the test for this particular a.
  - If x never becomes congruent to $\pm 1 \mod n$ in the repeated squaring process, n is likely composite.
- **Repeat the Test:** Repeat steps 2-6 with a different random a to decrease the probability of error.
- **Conclusion:**
  - If n passes all tests for different random bases, then n is considered "probably prime" with a high level of confidence.
  - If n fails the test for any a, then n is composite.

Miller-Rabin Primality Test Example

Example of the Miller-Rabin primality test to check if $n = 35$ is likely to be a prime number using $a = 3$.

- **Witness Generation:** Choose a random integer $a = 3$ such that $2 \leq a \leq n - 2$.
- **Exponentiation:** Compute $x = a^d \mod n$.

  For $d = 17$:

  $$x = 3^{17} \mod 35$$
  $$x = 129140163 \mod 35$$
  $$x = 13$$

- **Primality Test:**
  - If $x \equiv 1 \mod n$ or $x \equiv -1 \mod n$, then n passes the test for this particular a.
  - If x is neither 1 nor -1 after the exponentiation, proceed to the next steps.
- **Repeated Squaring:** For $r = 1, 2, \ldots, s - 1$, compute $x = x^2 \mod n$.

  For $r = 1$:

  $$x = 13^2 \mod 35$$
  $$x = 169 \mod 35$$
  $$x = 4$$

- **Final Test:**
  - If $x \equiv 1 \mod n$, n is likely composite.
  - If $x \equiv -1 \mod n$, n passes the test for this particular a.
  - If x never becomes congruent to $\pm 1 \mod n$ in the repeated squaring process, n is likely composite.
- **Conclusion:**
  - If n passes all tests for different random bases, then n is considered "probably prime" with a high level of confidence.
  - If n fails the test for any a, then n is composite.