Independence of the Miller-Rabin and Lucas Probable Prime Tests

Alec Leng
Mentor: David Corwin

PRIMES Conference, 5/21/2016

Primality Testing

Definition

A **primality test** is an algorithm that helps determine if a number is prime or not

Why do we care?

- Modern public-key cryptographic algorithms (e.g. RSA) rely on large prime numbers

The Fermat Primality Test

Fermat's Little Theorem

If p is a prime number, and a is relatively prime to p, then:

$$a^{p-1} \equiv 1 \pmod{p}.$$

- Using Fermat's Little Theorem, we can form a primality test.
- If for some a, $a^{n-1} \not\equiv 1 \pmod{n}$, n is composite.

The Fermat Primality Test

Fermat's Little Theorem

If p is a prime number, and a is relatively prime to p, then:

$$a^{p-1} \equiv 1 \pmod{p}.$$

- Using Fermat's Little Theorem, we can form a primality test.
- If for some a, $a^{n-1} \not\equiv 1 \pmod{n}$, n is composite.
- Even if $a^{n-1} \equiv 1 \pmod{n}$, n is not necessarily prime.
- If n is actually composite, we call a a **nonwitness** for n's compositness.

The Fermat Primality Test

Fermat's Little Theorem

If p is a prime number, and a is relatively prime to p, then:

$$a^{p-1} \equiv 1 \pmod{p}.$$

- Using Fermat's Little Theorem, we can form a primality test.
- If for some a, $a^{n-1} \not\equiv 1 \pmod{n}$, n is composite.
- Even if $a^{n-1} \equiv 1 \pmod{n}$, n is not necessarily prime.
- If n is actually composite, we call a a **nonwitness** for n's compositness.
- The Fermat test is a **probabilistic** primality test, since it determines if a number is composite or "probably prime".
- A **deterministic** test determines for sure if a number is prime or not.

The Fermat Primality Test

Examples

Let $n = 15$. Notice that $4^{14} \equiv (4^2)^7 \equiv 16^7 \equiv 1^7 \equiv 1 \pmod{15}$.
So 4 is a nonwitness.
$6^{14} \equiv 6 \not\equiv 1 \pmod{15}$.
So 15 is composite.
Let $n = 561 = 3 \cdot 11 \cdot 17$. Then, every integer relatively prime to 561 is a nonwitness!

The Fermat Primality Test

Examples

Let $n = 15$. Notice that $4^{14} \equiv (4^2)^7 \equiv 16^7 \equiv 1^7 \equiv 1 \pmod{15}$.
So 4 is a nonwitness.
$6^{14} \equiv 6 \not\equiv 1 \pmod{15}$.
So 15 is composite.
Let $n = 561 = 3 \cdot 11 \cdot 17$. Then, every integer relatively prime to 561 is a nonwitness!

- Unfortunately, there are plenty of numbers like 561.

Definition

A **Carmichael number** is a composite, n, where every a is a nonwitness.

The Miller-Rabin Test

Stronger Criterion

If p is prime, let $p - 1 = 2^k q$. Then, for any a relatively prime to p, one of the following is true:

$$a^{2^i q} \equiv -1 \pmod{p}, \text{ for } i < k, \text{ or } a^q \equiv 1 \pmod{p}.$$

Examples

Let $n = 561$ again. Then, $561 - 1 = 2^4 \cdot 35$.
According to Wolfram Alpha:

The Miller-Rabin Test

Stronger Criterion

If p is prime, let $p-1=2^kq$. Then, for any a relatively prime to p, one of the following is true:

$$a^{2^iq}\equiv -1 \pmod{p},\ \text{for } i<k,\ \text{or } a^q\equiv 1 \pmod{p}.$$

Examples

Let $n=561$ again. Then, $561-1=2^4\cdot 35$.
According to Wolfram Alpha:

- $2^{35}\equiv 263 \pmod{561}$
- $2^{2\cdot 35}\equiv 166 \pmod{561}$
- $2^{2^2\cdot 35}\equiv 67 \pmod{561}$
- $2^{2^3\cdot 35}\equiv 1 \pmod{561}$

The Lucas Probable Prime Test

The Lucas test generalizes the Fermat test to the “quadratic integers”. Typically, these are just things of the form $a + b\sqrt{D}$, for integers a, b, and D, where D is square-free.

Examples

Consider real numbers in the form $a + b\sqrt{7}$, where a and b are integers. With these “integers”:

- We can multiply: $(a + b\sqrt{7})(c + d\sqrt{7}) = ac + 7bd + (ad + bc)\sqrt{7}$.
- We can add and subtract: $(a + b\sqrt{7}) \pm (c + d\sqrt{7}) = (a \pm c) + (b \pm d)\sqrt{7}$.
- We can take mods: $7 + 4\sqrt{7} \equiv 1 + \sqrt{7} \pmod{3}$.

The Lucas Probable Prime Test

The Lucas test is a Fermat using these "quadratic integers".

Fermat's Little Theorem

If p is a prime number, and a is relatively prime to p, then:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Lucas Test Condition

Let τ be a specific type of quadratic integer. Then, if p is a prime,

$$\tau^{p \pm 1} \equiv 1 \pmod{p}.$$

Definition

A **Lucas-Carmichael** number is a composite number n, such that for every τ defined by a Lucas series, $\tau^{n \pm 1} \equiv 1 \pmod{n}$.

Numbers with High Nonwitnesses

For each test, and for each number of prime factors (2 or 3), these are the numbers with the most nonwitnesses:

▸▸

Miller-Rabin: (results due to Shyam Narayanan):

- Numbers of the form $(2k+1)(4k+1)$
- Certain Carmichael Numbers with three prime factors

(Strong) Lucas Test: (results essentially due to David Amirault)

- Lucas-Carmichael Numbers with two prime factors
- Certain Lucas-Carmichael Numbers with three prime factors

Numbers with High Nonwitnesses

- We wrote several programs to search for numbers with many nonwitnesses.
- To reduce the number of possible integers we checked, we proved several technical lemmas to classify possible candidates.
- After searching all possible numbers $< 2^{30}$, no numbers with many nonwitnesses were found.

Independence of the Tests

Theorem

If we choose our quadratic integers well, there are no numbers with "high" nonwitnesses for both the (Strong) Lucas and Miller-Rabin tests.

- Idea of proof:
- Case for two prime factors can be taken care of relatively easily.
- Carmichael Numbers have $p - 1|n - 1$.
- If we choose our integers well, Lucas-Carmichael numbers have $p \pm 1|n + 1$.
- If both of these are true, then $p + 1|n + 1$.
- There are no numbers with three prime factors and $p - 1|n - 1$, $p + 1|n + 1$.

Further Research

⏩ Return to classifications

- Are Carmichael and Lucas-Carmichael numbers always the "worst cases" for a number with k prime factors?
- Can any number be both a Carmichael number and a Lucas-Carmichael number?
- Can we find a way to use one test to eliminate composites with high non-witnesses for the other test?

Acknowlegments

Thank you to

- My mentor, David Corwin,
- Stefan Wehmeier from Mathworks, for suggesting the project,
- The PRIMES program and faculty,
- And my parents, for their love and support.