Primality Testing and the Miller-Rabin Algorithm

FA 2018 Cryptography Seminar

J. David Taylor

October 12, 2018

Why Primality Testing?

- Suppose Bob wants to implement RSA.

Why Primality Testing?

- Suppose Bob wants to implement RSA.
- Bob needs a pair of large prime numbers!

Why Primality Testing?

- Suppose Bob wants to implement RSA.
- Bob needs a pair of large prime numbers!
- If p, q are composite, then Bob will need to know how to factor them,

Why Primality Testing?

- Suppose Bob wants to implement RSA.
- Bob needs a pair of large prime numbers!
- If p, q are composite, then Bob will need to know how to factor them, and the cipher will be less secure.

Why Primality Testing?

- The prime number theorem tells us that

$$\text{The number of primes } \leq N \approx \frac{N}{\log N}$$

.

Why Primality Testing?

- The prime number theorem tells us that

$$\text{The number of primes } \leq N \approx \frac{N}{\log N}$$

.

- If Bob can efficiently distinguish prime numbers from composite numbers, then Bob can choose large numbers at random and check which are prime.

Why Primality Testing?

- The prime number theorem tells us that

$$\text{The number of primes } \leq N \approx \frac{N}{\log N}$$

.

- If Bob can efficiently distinguish prime numbers from composite numbers, then Bob can choose large numbers at random and check which are prime.
- Bob wants an efficient algorithm that detects composite numbers.

Fermat's Little Theorem

Theorem

Let p be a prime number, then $a^p \equiv a \mod p$ for every integer a.

Fermat's Little Theorem

Theorem

Let p be a prime number, then $a^p \equiv a \mod p$ for every integer a.

Example: Let
$n = 3198793773747935533262006864371310149095233 5301.$

Fermat's Little Theorem

Theorem

Let p be a prime number, then $a^p \equiv a \mod p$ for every integer a.

Example: Let
$n = 3198793773747935533262006864371310149095233 5301.$

The congruence (mod n)

$$2^{n-1} \equiv 128126595355135906413360121624715183605316 0074$$

tells Bob that n is not prime!

Witnesses

Let a, n be integers. We say that a is a witness for (the compositeness of) n if $a^n \not\equiv a \mod n$.

Witnesses

Let a, n be integers. We say that a is a witness for (the compositeness of) n if $a^n \not\equiv a \mod n$.

For example, 2 is a witness for 6, but 3 isn't.

Witnesses

Let a, n be integers. We say that a is a witness for (the compositeness of) n if $a^n \not\equiv a \mod n$.

For example, 2 is a witness for 6, but 3 isn't.

Idea: Try numbers less than n until you find a witness or try all of them

Carmichael Numbers

- Composite numbers with no witnesses are called Carmichael numbers.

Carmichael Numbers

- Composite numbers with no witnesses are called Carmichael numbers.
- (Korselt) Theorem: A positive composite integer n is Carmichael iff n is square-free and $p-1|n-1$ for every prime $p|n$.

Carmichael Numbers

- Composite numbers with no witnesses are called Carmichael numbers.
- (Korselt) Theorem: A positive composite integer n is Carmichael iff n is square-free and $p-1|n-1$ for every prime $p|n$.
- First seven Carmichael numbers are 561, 1105, 1729, 2465, 2821, 6601, and 8911.

Carmichael Numbers

- Composite numbers with no witnesses are called Carmichael numbers.
- (Korselt) Theorem: A positive composite integer n is Carmichael iff n is square-free and $p-1|n-1$ for every prime $p|n$.
- First seven Carmichael numbers are 561, 1105, 1729, 2465, 2821, 6601, and 8911.
- (Alfred, Granville, Pomerance) Theorem: There are infinitely many Carmichael numbers

Miller-Rabin Criterion

Let $p = 2^k q + 1$ be an odd prime number with q odd.

Miller-Rabin Criterion

Let $p = 2^k q + 1$ be an odd prime number with q odd.

Let a be an integer coprime to p.

Miller-Rabin Criterion

Let $p = 2^k q + 1$ be an odd prime number with q odd.

Let a be an integer coprime to p. Then

- $a^q \equiv 1 \mod p$,

Miller-Rabin Criterion

Let $p = 2^k q + 1$ be an odd prime number with q odd.

Let a be an integer coprime to p. Then

- $a^q \equiv 1 \mod p$, or
- one of $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to $-1 \mod p$.

Miller-Rabin Criterion

Let $p = 2^k q + 1$ be an odd prime number with q odd.

Let a be an integer coprime to p. Then

- $a^q \equiv 1 \mod p$, or
- one of $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to $-1 \mod p$.

Essentially, $a^{2^k q} = a^{p-1} \equiv 1 \mod p$,

Miller-Rabin Criterion

Let $p = 2^k q + 1$ be an odd prime number with q odd.

Let a be an integer coprime to p. Then

- $a^q \equiv 1 \mod p$, or
- one of $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to $-1 \mod p$.

Essentially, $a^{2^k q} = a^{p-1} \equiv 1 \mod p$, so either q kills a

Miller-Rabin Criterion

Let $p = 2^k q + 1$ be an odd prime number with q odd.

Let a be an integer coprime to p. Then

- $a^q \equiv 1 \mod p$, or
- one of $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to $-1 \mod p$.

Essentially, $a^{2^k q} = a^{p-1} \equiv 1 \mod p$, so either q kills a or some number in the list is a non-trivial square root of 1.

Miller-Rabin Primality Test

We'll test n with potential witness a:

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"
2. factor $n - 1 = 2^k q$ with q odd.

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"
2. factor $n - 1 = 2^k q$ with q odd.
3. set $a = a^q \mod n$

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"
2. factor $n - 1 = 2^k q$ with q odd.
3. set $a = a^q \mod n$
4. if $a \equiv 1 \mod n$, return "fail"

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"
2. factor $n - 1 = 2^k q$ with q odd.
3. set $a = a^q \mod n$
4. if $a \equiv 1 \mod n$, return "fail"
5. for $i = 0, \ldots, k - 1$,

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"
2. factor $n - 1 = 2^k q$ with q odd.
3. set $a = a^q \mod n$
4. if $a \equiv 1 \mod n$, return "fail"
5. for $i = 0, \ldots, k - 1$,

   if $a \equiv -1 \mod n$, return "fail"

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"
2. factor $n - 1 = 2^k q$ with q odd.
3. set $a = a^q \mod n$
4. if $a \equiv 1 \mod n$, return "fail"
5. for $i = 0, \ldots, k - 1$,

   if $a \equiv -1 \mod n$, return "fail"

   set $a = a^2 \mod n$

Miller-Rabin Primality Test

We'll test n with potential witness a:

1. if $2|n$ or $1 < \gcd(a, n) < n$, return "composite"
2. factor $n - 1 = 2^k q$ with q odd.
3. set $a = a^q \mod n$
4. if $a \equiv 1 \mod n$, return "fail"
5. for $i = 0, \ldots, k - 1$,

   if $a \equiv -1 \mod n$, return "fail"

   set $a = a^2 \mod n$
6. return "composite"

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Step 3 $a = 2^{35} \equiv 263 \mod 561$

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Step 3 $a = 2^{35} \equiv 263 \mod 561$

Step 5 The loop 0,1,2,3

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Step 3 $a = 2^{35} \equiv 263 \mod 561$

Step 5 The loop 0,1,2,3

$263 \not\equiv -1$

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Step 3 $a = 2^{35} \equiv 263 \mod 561$

Step 5 The loop 0,1,2,3

$263 \not\equiv -1$

$263^2 \equiv 166$

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Step 3 $a = 2^{35} \equiv 263 \mod 561$

Step 5 The loop 0,1,2,3

$263 \not\equiv -1$

$263^2 \equiv 166$

$166^2 \equiv 67$

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Step 3 $a = 2^{35} \equiv 263 \mod 561$

Step 5 The loop 0,1,2,3

$263 \not\equiv -1$

$263^2 \equiv 166$

$166^2 \equiv 67$

$67^2 \equiv 1$

Miller-Rabin Example

Let's test $n = 561$ with $a = 2$.

Step 2 $560 = 2^4 \cdot 35$

Step 3 $a = 2^{35} \equiv 263 \mod 561$

Step 5 The loop 0,1,2,3

$263 \not\equiv -1$

$263^2 \equiv 166$

$166^2 \equiv 67$

$67^2 \equiv 1$

Step 6 return "composite"

MRT Analysis

If n is an odd composite number, then at least 75% of the integers in $[1, n-1]$ will show that n is composite via the Miller-Rabin Test.

MRT Analysis

If n is an odd composite number, then at least 75% of the integers in $[1, n-1]$ will show that n is composite via the Miller-Rabin Test.

If the Generalized Riemann Hypothesis is true, then some $a \leq 2(\log n)^2$ suffices.

MRT Analysis

If n is an odd composite number, then at least 75% of the integers in $[1, n-1]$ will show that n is composite via the Miller-Rabin Test.

If the Generalized Riemann Hypothesis is true, then some $a \leq 2(\log n)^2$ suffices.

In practice, (1) choose a large number n, then (2) try random a's in the MRT until you get a sufficently high probability that n is prime.

MRT Analysis

If n is an odd composite number, then at least 75% of the integers in $[1, n-1]$ will show that n is composite via the Miller-Rabin Test.

If the Generalized Riemann Hypothesis is true, then some $a \leq 2(\log n)^2$ suffices.

In practice, (1) choose a large number n, then (2) try random a's in the MRT until you get a sufficently high probability that n is prime.

The runtime for each n is between quadratic and quartic depending on implementation.

AKS Primality Test

The paper "PRIMES is in P" by Agrawal, Kayal, and Saxena presents an algorithm that can be modified to have runtime of $\mathcal{O}(\log^6 n)$.

AKS Primality Test

The paper "PRIMES is in P" by Agrawal, Kayal, and Saxena presents an algorithm that can be modified to have runtime of $\mathcal{O}(\log^6 n)$.

The AKS algorithm is deterministic and proves that n is or is not prime.

AKS Primality Test

The paper "PRIMES is in P" by Agrawal, Kayal, and Saxena presents an algorithm that can be modified to have runtime of $\mathcal{O}(\log^6 n)$.

The AKS algorithm is deterministic and proves that n is or is not prime.

In practice, MRT's speed makes it preferable to AKS.

AKS Primality Test

The paper "PRIMES is in P" by Agrawal, Kayal, and Saxena presents an algorithm that can be modified to have runtime of $\mathcal{O}(\log^6 n)$.

The AKS algorithm is deterministic and proves that n is or is not prime.

In practice, MRT's speed makes it preferable to AKS.

AKS uses: Let a, n be coprime with $n \geq 2$. Then n is prime iff

$$(x + a)^n \equiv (x^n + a) \mod n$$

(as polynomials).

I've been informed that having no pictures is unacceptable ;-)

...Meow