Primality testing & Prime Number Generation

Nitin Saxena

Department of CSE
Indian Institute of Technology Kanpur

NWCNS 2019
PSIT Kanpur

Outline

The Problem

- Given an integer n, test whether it is prime.
- Easy Solution: Divide n by all numbers between 2 and $(n-1)$.
- What is the deal about primality testing then ??

The Problem

- Given an integer n, test whether it is prime.
- Easy Solution: Divide n by all numbers between 2 and $(n-1)$.
- What is the deal about primality testing then ??

The Problem

- Given an integer n, test whether it is prime.
- Easy Solution: Divide n by all numbers between 2 and $(n-1)$.
- What is the deal about primality testing then ??

EFFICIENTLY SOLVING A PROBLEM

- Given n we want a polynomial time primality test, one that runs in atmost $(\log n)^c$ steps.
- Note that practically $(\log n)^{\log\log\log n}$ steps is efficient enough for the prime numbers we encounter in real life!
- Nevertheless, the notion of polynomial time elegantly captures the theoretical complexity of a problem.

Notation:

- $(\log n)$ is logarithm base 2. Natural log is $(\ln n)$.
- $\tilde{O}(\log^c n)$ denotes $\log^c n \cdot (\log\log n)^{O(1)}$.

Efficiently Solving a Problem

- Given n we want a polynomial time primality test, one that runs in atmost $(\log n)^c$ steps.
- Note that practically $(\log n)^{\log\log\log n}$ steps is efficient enough for the prime numbers we encounter in real life!
- Nevertheless, the notion of polynomial time elegantly captures the theoretical complexity of a problem.

Notation:

- $(\log n)$ is logarithm base 2. Natural log is $(\ln n)$.
- $\tilde{O}(\log^c n)$ denotes $\log^c n \cdot (\log\log n)^{O(1)}$.

Efficiently Solving a Problem

- Given n we want a polynomial time primality test, one that runs in atmost $(\log n)^c$ steps.
- Note that practically $(\log n)^{\log\log\log n}$ steps is efficient enough for the prime numbers we encounter in real life!
- Nevertheless, the notion of polynomial time elegantly captures the theoretical complexity of a problem.

Notation:

- $(\log n)$ is logarithm base 2. Natural log is $(\ln n)$.
- $\tilde{O}(\log^c n)$ denotes $\log^c n \cdot (\log\log n)^{O(1)}$.

Efficiently Solving a Problem

- Given n we want a polynomial time primality test, one that runs in atmost $(\log n)^c$ steps.
- Note that practically $(\log n)^{\log\log\log n}$ steps is efficient enough for the prime numbers we encounter in real life!
- Nevertheless, the notion of polynomial time elegantly captures the theoretical complexity of a problem.

Notation:

- $(\log n)$ is logarithm base 2. Natural log is $(\ln n)$.
- $\tilde{O}(\log^c n)$ denotes $\log^c n \cdot (\log\log n)^{O(1)}$.

Efficiently Solving a Problem

- Given n we want a polynomial time primality test, one that runs in atmost $(\log n)^c$ steps.
- Note that practically $(\log n)^{\log\log\log n}$ steps is efficient enough for the prime numbers we encounter in real life!
- Nevertheless, the notion of polynomial time elegantly captures the theoretical complexity of a problem.

Notation:

- $(\log n)$ is logarithm base 2. Natural log is $(\ln n)$.
- $\tilde{O}(\log^c n)$ denotes $\log^c n \cdot (\log\log n)^{O(1)}$.

Outline

Eratosthenes Sieve

Proposed by Eratosthenes (ca. 300 BC).

1. List all numbers from 2 to n in a sequence.
2. Take the smallest uncrossed number and cross out all its multiples (except itself).
3. At the end all the uncrossed numbers are primes.

Eratosthenes Sieve

Proposed by Eratosthenes (ca. 300 BC).

1. List all numbers from 2 to n in a sequence.
2. Take the smallest uncrossed number and cross out all its multiples (except itself).
3. At the end all the uncrossed numbers are primes.

Eratosthenes Sieve

Proposed by Eratosthenes (ca. 300 BC).

1. List all numbers from 2 to n in a sequence.
2. Take the smallest uncrossed number and cross out all its multiples (except itself).
3. At the end all the uncrossed numbers are primes.

Eratosthenes Sieve

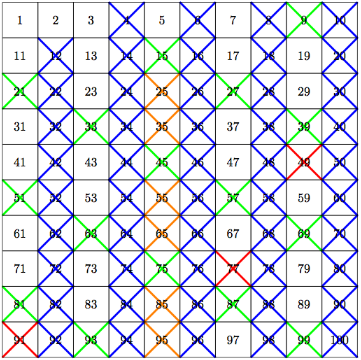
Proposed by Eratosthenes (ca. 300 BC).

1. List all numbers from 2 to n in a sequence.
2. Take the smallest uncrossed number and cross out all its multiples (except itself).
3. At the end all the uncrossed numbers are primes.

Eratosthenes Sieve

Proposed by Eratosthenes (ca. 300 BC).

1. List all numbers from 2 to n in a sequence.
2. Take the smallest uncrossed number and cross out all its multiples (except itself).
3. At the end all the uncrossed numbers are primes.



TIME COMPLEXITY

- To test primality $\sqrt{n}$ many steps would be enough.
- Not efficient by our standards!
  As input size is $O(\log n)$.

Time Complexity

- To test primality $\sqrt{n}$ many steps would be enough.
- Not efficient by our standards!
  As input size is $O(\log n)$.

Time Complexity

- To test primality $\sqrt{n}$ many steps would be enough.
- Not efficient by our standards!
  As input size is $O(\log n)$.

Outline

Density of primes

- Suppose we want a prime number *close* to n.
- Eratosthenes sieve is a way to generate it. But it's slow.
- Fortunately, the primes are abundant in nature. If $\pi(x)$ is the number of primes below x then *precise* estimates on $\pi(x)/x$ are known.

Rosser (1941)

showed that $\frac{1}{\ln x+2} < \frac{\pi(x)}{x} < \frac{1}{\ln x-4}$, for $x \geq 55$.

- Thus, if we randomly pick a $(\log n)$-bit number N, then with high probability it will be prime!

Density of primes

- Suppose we want a prime number *close* to n.
- Eratosthenes sieve is a way to generate it. But it's slow.
- Fortunately, the primes are abundant in nature. If $\pi(x)$ is the number of primes below x then *precise* estimates on $\pi(x)/x$ are known.

Rosser (1941)

showed that $\frac{1}{\ln x+2} < \frac{\pi(x)}{x} < \frac{1}{\ln x-4}$, for $x \geq 55$.

- Thus, if we randomly pick a $(\log n)$-bit number N, then with high probability it will be prime!

Density of primes

- Suppose we want a prime number *close* to n.
- Eratosthenes sieve is a way to generate it. But it's slow.
- Fortunately, the primes are abundant in nature. If $\pi(x)$ is the number of primes below x then *precise* estimates on $\pi(x)/x$ are known.

Rosser (1941)

showed that $\frac{1}{\ln x+2} < \frac{\pi(x)}{x} < \frac{1}{\ln x-4}$, for $x \geq 55$.

- Thus, if we randomly pick a $(\log n)$-bit number N, then with high probability it will be prime!

Density of primes

- Suppose we want a prime number *close* to n.
- Eratosthenes sieve is a way to generate it. But it's slow.
- Fortunately, the primes are abundant in nature. If $\pi(x)$ is the number of primes below x then *precise* estimates on $\pi(x)/x$ are known.

Rosser (1941)

showed that $\frac{1}{\ln x+2} < \frac{\pi(x)}{x} < \frac{1}{\ln x-4}$, for $x \geq 55$.

- Thus, if we randomly pick a $(\log n)$-bit number N, then with high probability it will be prime!

Ring based primality tests

- All the advanced primality tests associate a ring R to n and study its properties.
- The favorite rings are:
  1. $\mathbb{Z}_n$ – Integers modulo n.
  2. $\mathbb{Z}_n[\sqrt{3}]$ – Quadratic extensions.
  3. $\mathbb{Z}_n[x,y]/(y^2 - x^3 - ax - b)$ – Elliptic curves.
  4. $\mathbb{Z}_n[x]/(x^r - 1)$ – Cyclotomic rings.

Ring based primality tests

- All the advanced primality tests associate a ring R to n and study its properties.
- The favorite rings are:
  1. $\mathbb{Z}_n$ – Integers modulo n.
  2. $\mathbb{Z}_n[\sqrt{3}]$ – Quadratic extensions.
  3. $\mathbb{Z}_n[x,y]/(y^2 - x^3 - ax - b)$ – Elliptic curves.
  4. $\mathbb{Z}_n[x]/(x^r - 1)$ – Cyclotomic rings.

Ring based primality tests

- All the advanced primality tests associate a ring R to n and study its properties.
- The favorite rings are:
  1. $\mathbb{Z}_n$ – Integers modulo n.
  2. $\mathbb{Z}_n[\sqrt{3}]$ – Quadratic extensions.
  3. $\mathbb{Z}_n[x,y]/(y^2 - x^3 - ax - b)$ – Elliptic curves.
  4. $\mathbb{Z}_n[x]/(x^r - 1)$ – Cyclotomic rings.

Ring based primality tests

- All the advanced primality tests associate a ring R to n and study its properties.
- The favorite rings are:
  1. $\mathbb{Z}_n$ – Integers modulo n.
  2. $\mathbb{Z}_n[\sqrt{3}]$ – Quadratic extensions.
  3. $\mathbb{Z}_n[x, y]/(y^2 - x^3 - ax - b)$ – Elliptic curves.
  4. $\mathbb{Z}_n[x]/(x^r - 1)$ – Cyclotomic rings.

Ring based primality tests

- All the advanced primality tests associate a ring R to n and study its properties.
- The favorite rings are:
  1. $\mathbb{Z}_n$ – Integers modulo n.
  2. $\mathbb{Z}_n[\sqrt{3}]$ – Quadratic extensions.
  3. $\mathbb{Z}_n[x,y]/(y^2 - x^3 - ax - b)$ – Elliptic curves.
  4. $\mathbb{Z}_n[x]/(x^r - 1)$ – Cyclotomic rings.

Ring based primality tests

- All the advanced primality tests associate a ring R to n and study its properties.
- The favorite rings are:
  1. $\mathbb{Z}_n$ – Integers modulo n.
  2. $\mathbb{Z}_n[\sqrt{3}]$ – Quadratic extensions.
  3. $\mathbb{Z}_n[x, y]/(y^2 - x^3 - ax - b)$ – Elliptic curves.
  4. $\mathbb{Z}_n[x]/(x^r - 1)$ – Cyclotomic rings.

Outline

Fermat's Little Theorem (FLT)

Theorem (Fermat, 1660s)

If n is prime then for every a, $a^n = a \pmod{n}$.

- Basically, for all $a \in \mathbb{Z}_n^*$, $a^{n-1} = 1$.
- This property is not sufficient for primality (Carmichael, 1910).
- But it is the starting point!
- Eg. $561 = 3 \times 11 \times 17$.

Fermat's Little Theorem (FLT)

Theorem (Fermat, 1660s)

If n is prime then for every a, $a^n = a \pmod{n}$.

- Basically, for all $a \in \mathbb{Z}_n^*$, $a^{n-1} = 1$.
- This property is not sufficient for primality (Carmichael, 1910).
- But it is the starting point!
- Eg. $561 = 3 \times 11 \times 17$.

Fermat's Little Theorem (FLT)

Theorem (Fermat, 1660s)

If n is prime then for every a, $a^n = a \pmod{n}$.

- Basically, for all $a \in \mathbb{Z}_n^*$, $a^{n-1} = 1$.
- This property is not sufficient for primality (Carmichael, 1910).
- But it is the starting point!
- Eg. $561 = 3 \times 11 \times 17$.

Fermat's Little Theorem (FLT)

Theorem (Fermat, 1660s)

If n is prime then for every a, $a^n = a \pmod n$.

- Basically, for all $a \in \mathbb{Z}_n^*$, $a^{n-1} = 1$.
- This property is not sufficient for primality (Carmichael, 1910).
- But it is the starting point!
- Eg. $561 = 3 \times 11 \times 17$.

Fermat's Little Theorem (FLT)

Theorem (Fermat, 1660s)

If n is prime then for every a, $a^n = a \pmod{n}$.

- Basically, for all $a \in \mathbb{Z}_n^*$, $a^{n-1} = 1$.
- This property is not sufficient for primality (Carmichael, 1910).
- But it is the starting point!
- Eg. $561 = 3 \times 11 \times 17$.

Lucas Test

Theorem (Lucas, 1876)

n is prime iff $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $a^{\frac{n-1}{p}} \neq 1$ for all primes $p|(n-1)$.

- Suppose $(n-1)$ is smooth and we know its prime factors.
- Do the above test for a random a.
- Algebraic fact: For prime n, the group $\mathbb{Z}_n^*$ is cyclic and of size $n-1$.

Lucas Test

Theorem (Lucas, 1876)

n is prime iff $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $a^{\frac{n-1}{p}} \neq 1$ for all primes $p|(n-1)$.

- Suppose $(n-1)$ is smooth and we know its prime factors.
- Do the above test for a random a.
- Algebraic fact: For prime n, the group $\mathbb{Z}_n^*$ is cyclic and of size $n-1$.

Lucas Test

Theorem (Lucas, 1876)

n is prime iff $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $a^{\frac{n-1}{p}} \neq 1$ for all primes $p|(n-1)$.

- Suppose $(n-1)$ is smooth and we know its prime factors.
- Do the above test for a random a.
- Algebraic fact: For prime n, the group $\mathbb{Z}_n^*$ is cyclic and of size $n-1$.

Lucas Test

Theorem (Lucas, 1876)

n is prime iff $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $a^{\frac{n-1}{p}} \neq 1$ for all primes $p | (n-1)$.

- Suppose $(n-1)$ is smooth and we know its prime factors.
- Do the above test for a random a.
- Algebraic fact: For prime n, the group $\mathbb{Z}_n^*$ is cyclic and of size $n-1$.

Lucas Test

Theorem (Lucas, 1876)

n is prime iff $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $a^{\frac{n-1}{p}} \neq 1$ for all primes $p|(n-1)$.

- Suppose $(n-1)$ is smooth and we know its prime factors.
- Do the above test for a random a.
- Algebraic fact: For prime n, the group $\mathbb{Z}_n^*$ is cyclic and of size $n-1$.

Lucas Test

Theorem (Lucas, 1876)

n is prime iff $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $a^{\frac{n-1}{p}} \neq 1$ for all primes $p | (n-1)$.

- Suppose $(n-1)$ is smooth and we know its prime factors.
- Do the above test for a random a.
- Algebraic fact: For prime n, the group $\mathbb{Z}_n^*$ is cyclic and of size $n-1$.

Pocklington-Lehmer Test

Theorem (Pocklington, 1914)

If $\exists a \in \mathbb{Z}_n$ *such that* $a^{n-1} = 1$ *and* $gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ *for any distinct primes* $p_1, \ldots, p_t | (n-1)$. *Then any divisor of* n *is of the form* $1 + kp_1 \cdots p_t$.

- Suppose $\prod_{i=1}^{t} p_t \geq \sqrt{n}$ and we have them.
- The above test is done for a random a.

Pocklington-Lehmer Test

Theorem (Pocklington, 1914)

If $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ for any distinct primes $p_1, \ldots, p_t | (n-1)$. Then any divisor of n is of the form $1 + kp_1 \cdots p_t$.

- Suppose $\prod_{i=1}^{t} p_t \geq \sqrt{n}$ and we have them.
- The above test is done for a random a.

Pocklington-Lehmer Test

Theorem (Pocklington, 1914)

If $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ for any distinct primes $p_1, \ldots, p_t | (n-1)$. Then any divisor of n is of the form $1 + kp_1 \cdots p_t$.

- Suppose $\prod_{i=1}^{t} p_t \geq \sqrt{n}$ and we have them.
- The above test is done for a random a.

Pocklington-Lehmer Test

Theorem (Pocklington, 1914)

If $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ for any distinct primes $p_1, \ldots, p_t | (n-1)$. Then any divisor of n is of the form $1 + kp_1 \cdots p_t$.

- Suppose $\prod_{i=1}^{t} p_t \geq \sqrt{n}$ and we have them.
- The above test is done for a random a.

Pocklington-Lehmer Test

Theorem (Pocklington, 1914)

If $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ for any distinct primes $p_1, \ldots, p_t | (n-1)$. Then any divisor of n is of the form $1 + kp_1 \cdots p_t$.

- Suppose $\prod_{i=1}^{t} p_t \geq \sqrt{n}$ and we have them.
- The above test is done for a random a.

Pocklington-Lehmer Test

Theorem (Pocklington, 1914)

If $\exists a \in \mathbb{Z}_n$ such that $a^{n-1} = 1$ and $gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ for any distinct primes $p_1, \ldots, p_t | (n-1)$. Then any divisor of n is of the form $1 + kp_1 \cdots p_t$.

- Suppose $\prod_{i=1}^{t} p_t \geq \sqrt{n}$ and we have them.
- The above test is done for a random a.

Solovay-Strassen: First randomized test

Theorem (Strengthening FLT)

An odd number n is prime iff for all $a \in \mathbb{Z}_n$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$.

- Jacobi symbol $\left(\frac{a}{n}\right)$ is computable in time $\tilde{O}(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$.
- Algebraic fact: Quadratic residuosity in finite fields.

Solovay-Strassen: First randomized test

Theorem (Strengthening FLT)

An odd number n is prime iff for all $a \in \mathbb{Z}_n$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$.

- Jacobi symbol $\left(\frac{a}{n}\right)$ is computable in time $\tilde{O}(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$.
- Algebraic fact: Quadratic residuosity in finite fields.

Solovay-Strassen: First randomized test

Theorem (Strengthening FLT)

An odd number n is prime iff for all $a \in \mathbb{Z}_n$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$.

- Jacobi symbol $\left(\frac{a}{n}\right)$ is computable in time $\tilde{O}(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$.
- Algebraic fact: Quadratic residuosity in finite fields.

Solovay-Strassen: First randomized test

Theorem (Strengthening FLT)

An odd number n is prime iff for all $a \in \mathbb{Z}_n$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$.

- Jacobi symbol $\left(\frac{a}{n}\right)$ is computable in time $\tilde{O}(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$.
- Algebraic fact: Quadratic residuosity in finite fields.

Solovay-Strassen: First randomized test

Theorem (Strengthening FLT)

An odd number n is prime iff for all $a \in \mathbb{Z}_n$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$.

- Jacobi symbol $\left(\frac{a}{n}\right)$ is computable in time $\tilde{O}(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$.
- Algebraic fact: Quadratic residuosity in finite fields.

Solovay-Strassen: First randomized test

Theorem (Strengthening FLT)

An odd number n is prime iff for all $a \in \mathbb{Z}_n$, $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$.

- Jacobi symbol $\left(\frac{a}{n}\right)$ is computable in time $\tilde{O}(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$.
- Algebraic fact: Quadratic residuosity in finite fields.

Pépin's Test

This is a test specialized for Fermat numbers $F_k = 2^{2^k} + 1$.

Theorem (Pépin, 1877)

F_k is prime iff $3^{\frac{F_k - 1}{2}} = -1 \pmod{F_k}$.

This yields a deterministic polynomial time primality test for Fermat numbers.

Algebraic fact: In the prime case 3 is a generator!

Pépin's Test

This is a test specialized for Fermat numbers $F_k = 2^{2^k} + 1$.

Theorem (Pépin, 1877)

F_k is prime iff $3^{\frac{F_k - 1}{2}} = -1 \pmod{F_k}$.

This yields a deterministic polynomial time primality test for Fermat numbers.

Algebraic fact: In the prime case 3 is a generator!

Pépin's Test

This is a test specialized for Fermat numbers $F_k = 2^{2^k} + 1$.

Theorem (Pépin, 1877)

F_k is prime iff $3^{\frac{F_k-1}{2}} = -1 \pmod{F_k}$.

This yields a deterministic polynomial time primality test for Fermat numbers.

Algebraic fact: In the prime case 3 is a generator!

Pépin's Test

This is a test specialized for Fermat numbers $F_k = 2^{2^k} + 1$.

Theorem (Pépin, 1877)

F_k is prime iff $3^{\frac{F_k - 1}{2}} = -1 \pmod{F_k}$.

This yields a deterministic polynomial time primality test for Fermat numbers.

Algebraic fact: In the prime case 3 is a generator!

Miller-Rabin: Practical test

Strengthening FLT further [Miller, 1975]

An odd number $n = 1 + 2^s \cdot t$ (odd t) is prime iff for all $a \in \mathbb{Z}_n$, the sequence $a^{2^{s-1} \cdot t}, a^{2^{s-2} \cdot t}, \ldots, a^t$ has either a -1 or all 1's.

- We check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
- Algebraic fact: Over a field there are at most *two* square-roots.

Miller-Rabin: Practical test

Strengthening FLT further [Miller, 1975]

An odd number $n = 1 + 2^s \cdot t$ (odd t) is prime iff for all $a \in \mathbb{Z}_n$, the sequence $a^{2^{s-1}\cdot t}, a^{2^{s-2}\cdot t}, \ldots, a^t$ has either a -1 or all 1's.

- We check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
- Algebraic fact: Over a field there are at most *two* square-roots.

Miller-Rabin: Practical test

Strengthening FLT further [Miller, 1975]

An odd number $n = 1 + 2^s \cdot t$ (odd t) is prime iff for all $a \in \mathbb{Z}_n$, the sequence $a^{2^{s-1}\cdot t}, a^{2^{s-2}\cdot t}, \ldots, a^t$ has either a -1 or all 1's.

- We check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
- Algebraic fact: Over a field there are at most *two* square-roots.

Miller-Rabin: Practical test

Strengthening FLT further [Miller, 1975]

An odd number $n = 1 + 2^s \cdot t$ (odd t) is prime iff for all $a \in \mathbb{Z}_n$, the sequence $a^{2^{s-1}\cdot t}, a^{2^{s-2}\cdot t}, \ldots, a^t$ has either a -1 or all 1's.

- We check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
- Algebraic fact: Over a field there are at most *two* square-roots.

Miller-Rabin: Practical test

Strengthening FLT further [Miller, 1975]

An odd number $n = 1 + 2^s \cdot t$ (odd t) is prime iff for all $a \in \mathbb{Z}_n$, the sequence $a^{2^{s-1} \cdot t}, a^{2^{s-2} \cdot t}, \ldots, a^t$ has either a -1 or all 1's.

- We check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
- Algebraic fact: Over a field there are at most *two* square-roots.

Miller-Rabin: Practical test

Strengthening FLT further [Miller, 1975]

An odd number $n = 1 + 2^s \cdot t$ (odd t) is prime iff for all $a \in \mathbb{Z}_n$, the sequence $a^{2^{s-1} \cdot t}, a^{2^{s-2} \cdot t}, \ldots, a^t$ has either a -1 or all 1's.

- We check the above equation for a random a.
- This gives a randomized test that takes time $\tilde{O}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
- Algebraic fact: Over a field there are at most *two* square-roots.

Riemann Hypothesis and Primality

Generalized Riemann Hypothesis [Piltz, 1884]

Let Dirichlet L-function be the analytic continuation of $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. For every Dirichlet character χ and every complex number s with $L(\chi, s) = 0$: if $\text{Re}(s) \in (0, 1]$ then $\text{Re}(s) = \frac{1}{2}$.

- By taking χ to be the character modulo n it can be shown: the GRH implies that there exists an $a \leq 2\log^2 n$ such that $\left(\frac{a}{n}\right) \neq 1$ (Ankeny 1952; Miller 1975; Bach 1980s).
- This magical small a would be a witness of the compositeness of n.
- Thus, GRH derandomizes both Solovay-Strassen and Miller-Rabin primality tests.

This a also factors Carmichael numbers!

Riemann Hypothesis and Primality

Generalized Riemann Hypothesis [Piltz, 1884]

Let Dirichlet L-function be the analytic continuation of $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. For every Dirichlet character χ and every complex number s with $L(\chi, s) = 0$: if $\mathrm{Re}(s) \in (0, 1]$ then $\mathrm{Re}(s) = \frac{1}{2}$.

- By taking χ to be the character modulo n it can be shown: the GRH implies that there exists an $a \leq 2\log^2 n$ such that $\left(\frac{a}{n}\right) \neq 1$ (Ankeny 1952; Miller 1975; Bach 1980s).
- This magical small a would be a witness of the compositeness of n.
- Thus, GRH derandomizes both Solovay-Strassen and Miller-Rabin primality tests.

This a also factors Carmichael numbers!

Riemann Hypothesis and Primality

Generalized Riemann Hypothesis [Piltz, 1884]

Let Dirichlet L-function be the analytic continuation of $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. For every Dirichlet character χ and every complex number s with $L(\chi, s) = 0$: if $\mathrm{Re}(s) \in (0, 1]$ then $\mathrm{Re}(s) = \frac{1}{2}$.

- By taking χ to be the character modulo n it can be shown: the GRH implies that there exists an $a \leq 2\log^2 n$ such that $\left(\frac{a}{n}\right) \neq 1$ (Ankeny 1952; Miller 1975; Bach 1980s).
- This magical small a would be a witness of the compositeness of n.
- Thus, GRH derandomizes both Solovay-Strassen and Miller-Rabin primality tests.

This a also factors Carmichael numbers!

Riemann Hypothesis and Primality

Generalized Riemann Hypothesis [Piltz, 1884]

Let Dirichlet L-function be the analytic continuation of $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. For every Dirichlet character χ and every complex number s with $L(\chi, s) = 0$: if $\mathrm{Re}(s) \in (0, 1]$ then $\mathrm{Re}(s) = \frac{1}{2}$.

- By taking χ to be the character modulo n it can be shown: the GRH implies that there exists an $a \leq 2\log^2 n$ such that $\left(\frac{a}{n}\right) \neq 1$ (Ankeny 1952; Miller 1975; Bach 1980s).
- This magical small a would be a witness of the compositeness of n.
- Thus, GRH derandomizes both Solovay-Strassen and Miller-Rabin primality tests.

This a also factors Carmichael numbers!

Riemann Hypothesis and Primality

Generalized Riemann Hypothesis [Piltz, 1884]

Let Dirichlet L-function be the analytic continuation of $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. For every Dirichlet character χ and every complex number s with $L(\chi, s) = 0$: if $\mathrm{Re}(s) \in (0, 1]$ then $\mathrm{Re}(s) = \frac{1}{2}$.

- By taking χ to be the character modulo n it can be shown: the GRH implies that there exists an $a \leq 2\log^2 n$ such that $\left(\frac{a}{n}\right) \neq 1$ (Ankeny 1952; Miller 1975; Bach 1980s).
- This magical small a would be a witness of the compositeness of n.
- Thus, GRH derandomizes both Solovay-Strassen and Miller-Rabin primality tests.

This a also factors Carmichael numbers!

Riemann Hypothesis and Primality

Generalized Riemann Hypothesis [Piltz, 1884]

Let Dirichlet L-function be the analytic continuation of $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. For every Dirichlet character χ and every complex number s with $L(\chi, s) = 0$: if $\mathrm{Re}(s) \in (0, 1]$ then $\mathrm{Re}(s) = \frac{1}{2}$.

- By taking χ to be the character modulo n it can be shown: the GRH implies that there exists an $a \leq 2\log^2 n$ such that $\left(\frac{a}{n}\right) \neq 1$ (Ankeny 1952; Miller 1975; Bach 1980s).
- This magical small a would be a witness of the compositeness of n.
- Thus, GRH derandomizes both Solovay-Strassen and Miller-Rabin primality tests.

This a also factors Carmichael numbers!

Outline

Lucas-Lehmer Test

This is a test specialized for Mersenne primes $M_k = 2^k - 1$.

Theorem (Lucas-Lehmer, 1930)

M_k is prime iff $(2+\sqrt{3})^{\frac{M_k+1}{2}} = -1$ in $(\mathbb{Z}/M_k)[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes. `On 21-Dec-2018 GIMPS found largest known prime` $2^{82,589,933} - 1$.
- Generalization: Whenever $(n+1)$ has small prime factors one can test n for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $\left(\frac{D}{n}\right) = -1$.
- More generalization: Whenever $(n^2 \pm n + 1)$ has small prime factors one can test n for primality. But then we have to go to cubic extensions (Williams 1978).

Lucas-Lehmer Test

This is a test specialized for Mersenne primes $M_k = 2^k - 1$.

Theorem (Lucas-Lehmer, 1930)

M_k is prime iff $(2+\sqrt{3})^{\frac{M_k+1}{2}} = -1$ in $(\mathbb{Z}/M_k)[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes. `On 21-Dec-2018 GIMPS found largest known prime` $2^{82,589,933} - 1$.
- Generalization: Whenever $(n+1)$ has small prime factors one can test n for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $\left(\frac{D}{n}\right) = -1$.
- More generalization: Whenever $(n^2 \pm n + 1)$ has small prime factors one can test n for primality. But then we have to go to cubic extensions (Williams 1978).

Lucas-Lehmer Test

This is a test specialized for Mersenne primes $M_k = 2^k - 1$.

Theorem (Lucas-Lehmer, 1930)

M_k is prime iff $(2+\sqrt{3})^{\frac{M_k+1}{2}} = -1$ in $(\mathbb{Z}/M_k)[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes. On 21-Dec-2018 GIMPS found largest known prime $2^{82,589,933} - 1$.
- Generalization: Whenever $(n+1)$ has small prime factors one can test n for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $\left(\frac{D}{n}\right) = -1$.
- More generalization: Whenever $(n^2 \pm n + 1)$ has small prime factors one can test n for primality. But then we have to go to cubic extensions (Williams 1978).

Lucas-Lehmer Test

This is a test specialized for Mersenne primes $M_k = 2^k - 1$.

Theorem (Lucas-Lehmer, 1930)

M_k is prime iff $(2+\sqrt{3})^{\frac{M_k+1}{2}} = -1$ in $(\mathbb{Z}/M_k)[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes. `On 21-Dec-2018 GIMPS found largest known prime` $2^{82,589,933} - 1$.
- Generalization: Whenever $(n+1)$ has small prime factors one can test n for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $\left(\frac{D}{n}\right) = -1$.
- More generalization: Whenever $(n^2 \pm n + 1)$ has small prime factors one can test n for primality. But then we have to go to cubic extensions (Williams 1978).

Lucas-Lehmer Test

This is a test specialized for Mersenne primes $M_k = 2^k - 1$.

Theorem (Lucas-Lehmer, 1930)

M_k is prime iff $(2+\sqrt{3})^{\frac{M_k+1}{2}} = -1$ in $(\mathbb{Z}/M_k)[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes. On 21-Dec-2018 GIMPS found largest known prime $2^{82,589,933} - 1$.
- Generalization: Whenever $(n+1)$ has small prime factors one can test n for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $\left(\frac{D}{n}\right) = -1$.
- More generalization: Whenever $(n^2 \pm n + 1)$ has small prime factors one can test n for primality. But then we have to go to cubic extensions (Williams 1978).

Lucas-Lehmer Test

This is a test specialized for Mersenne primes $M_k = 2^k - 1$.

Theorem (Lucas-Lehmer, 1930)

M_k is prime iff $(2+\sqrt{3})^{\frac{M_k+1}{2}} = -1$ in $(\mathbb{Z}/M_k)[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes. `On 21-Dec-2018 GIMPS found largest known prime` $2^{82,589,933} - 1$.
- Generalization: Whenever $(n+1)$ has small prime factors one can test n for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $\left(\frac{D}{n}\right) = -1$.
- More generalization: Whenever $(n^2 \pm n + 1)$ has small prime factors one can test n for primality. But then we have to go to cubic extensions (Williams 1978).

Outline

Elliptic Curve Based Tests

- An elliptic curve over $\mathbb{Z}_n$ is the set of points:

$$E_{a,b}(\mathbb{Z}_n) = \{(x,y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + ax + b\}$$

- When n is prime: $E_{a,b}(\mathbb{Z}_n)$ is an abelian group.
- $\#E_{a,b}(\mathbb{Z}_n)$ can be computed in deterministic polynomial time (Schoof 1985).
- When n is prime: number of points on a random elliptic curve is uniformly distributed in the interval $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2 5]$ (Lenstra 1987).

Elliptic Curve Based Tests

- An elliptic curve over $\mathbb{Z}_n$ is the set of points:

$$E_{a,b}(\mathbb{Z}_n) = \{(x,y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + ax + b\}$$

- When n is prime: $E_{a,b}(\mathbb{Z}_n)$ is an abelian group.
- $\#E_{a,b}(\mathbb{Z}_n)$ can be computed in deterministic polynomial time (Schoof 1985).
- When n is prime: number of points on a random elliptic curve is uniformly distributed in the interval $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2 5]$ (Lenstra 1987).

Elliptic Curve Based Tests

- An elliptic curve over $\mathbb{Z}_n$ is the set of points:

$$E_{a,b}(\mathbb{Z}_n) = \left\{(x,y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + ax + b\right\}$$

- When n is prime: $E_{a,b}(\mathbb{Z}_n)$ is an abelian group.
- $\#E_{a,b}(\mathbb{Z}_n)$ can be computed in deterministic polynomial time (Schoof 1985).
- When n is prime: number of points on a random elliptic curve is uniformly distributed in the interval $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2 5]$ (Lenstra 1987).

Elliptic Curve Based Tests

- An elliptic curve over $\mathbb{Z}_n$ is the set of points:

$$E_{a,b}(\mathbb{Z}_n) = \left\{(x,y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + ax + b\right\}$$

- When n is prime: $E_{a,b}(\mathbb{Z}_n)$ is an abelian group.
- $\#E_{a,b}(\mathbb{Z}_n)$ can be computed in deterministic polynomial time (Schoof 1985).
- When n is prime: number of points on a random elliptic curve is uniformly distributed in the interval $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2 5]$ (Lenstra 1987).

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \le \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \le (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \le q$ we get that:
$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$
- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \le \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \le (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \le q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

1. Pick a random elliptic curve E over $\mathbb{Z}_n$ and a random point $A \in E$.
2. Compute $\#E(\mathbb{Z}_n)$. If $\#E(\mathbb{Z}_n)$ is odd then output COMPOSITE.
3. Let $\#E(\mathbb{Z}_n) =: 2q$. Prove the primality of q recursively.
4. If q is prime and $q \cdot A = O$ then output PRIME else output COMPOSITE.

Proof of Correctness:

- Firstly, note that conjecturally there are "many" numbers between $[(\sqrt{n}-1)^2, (\sqrt{n}+1)^2]$ that are twice a prime and for a random E, $\#E(\mathbb{Z}_n)$ will hit such numbers whp when n is prime.
- Suppose n is composite with a prime factor $p \leq \sqrt{n}$ but the Step 4 condition holds.
- Since $\#E(\mathbb{Z}_p) \leq (p+1+2\sqrt{p}) < \frac{n+1-2\sqrt{n}}{2} \leq q$ we get that:

$$q \text{ is prime and } q \cdot A = O \Rightarrow A = O \text{ in } E(\mathbb{Z}_p)$$

- Thus, A will factor n.

Goldwasser-Kilian Test

- This is the first randomized test that never errs when n is composite (1986).
- Time complexity (Atkin-Morain 1993): $\tilde{O}(\log^4 n)$.
- But its proof assumed a conjecture about the density of primes in the interval $\left[\frac{n+1-2\sqrt{n}}{2}, \frac{n+1+2\sqrt{n}}{2}\right]$.
- Currently, it is not even known if there is always a prime between m^2 and $(m+1)^2$ (Legendre's conjecture).

Goldwasser-Kilian Test

- This is the first randomized test that never errs when n is composite (1986).
- Time complexity (Atkin-Morain 1993): $\tilde{O}(\log^4 n)$.
- But its proof assumed a conjecture about the density of primes in the interval $\left[\frac{n+1-2\sqrt{n}}{2}, \frac{n+1+2\sqrt{n}}{2}\right]$.
- Currently, it is not even known if there is always a prime between m^2 and $(m+1)^2$ (Legendre's conjecture).

Goldwasser-Kilian Test

- This is the first randomized test that never errs when n is composite (1986).
- Time complexity (Atkin-Morain 1993): $\tilde{O}(\log^4 n)$.
- But its proof assumed a conjecture about the density of primes in the interval $\left[\frac{n+1-2\sqrt{n}}{2}, \frac{n+1+2\sqrt{n}}{2}\right]$.
- Currently, it is not even known if there is always a prime between m^2 and $(m+1)^2$ (Legendre's conjecture).

Goldwasser-Kilian Test

- This is the first randomized test that never errs when n is composite (1986).
- Time complexity (Atkin-Morain 1993): $\tilde{O}(\log^4 n)$.
- But its proof assumed a conjecture about the density of primes in the interval $\left[\frac{n+1-2\sqrt{n}}{2}, \frac{n+1+2\sqrt{n}}{2}\right]$.
- Currently, it is not even known if there is always a prime between m^2 and $(m+1)^2$ (Legendre's conjecture).

Adleman-Huang Test

- Using hyperelliptic curves they made Goldwasser-Kilian test unconditional (1992).
- Time complexity: $O(\log^c n)$ where $c > 30$!

Adleman-Huang Test

- Using hyperelliptic curves they made Goldwasser-Kilian test unconditional (1992).
- Time complexity: $O(\log^c n)$ where $c > 30$!

Outline

Adleman-Pomerance-Rumeli Test

- Recall how Lucas-Lehmer-Williams tested n for primality when $(n-1), (n+1), (n^2-n+1)$ or (n^2+n+1) was smooth.
- What can we do when $(n^m - 1)$ is smooth? Maybe go to some m-th extension of $\mathbb{Z}_n$?
- This question inspired the APR test (1980). Speeded up by Cohen and Lenstra (1981).
- Deterministic algorithm with time complexity $\log^{O(\log\log\log n)} n$.
- Is conceptually the most complex algorithm of all.
- Attempts to find a prime factor of n using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$.

Adleman-Pomerance-Rumeli Test

- Recall how Lucas-Lehmer-Williams tested n for primality when $(n-1), (n+1), (n^2-n+1)$ or (n^2+n+1) was smooth.
- What can we do when (n^m-1) is smooth? Maybe go to some m-th extension of $\mathbb{Z}_n$?
- This question inspired the APR test (1980). Speeded up by Cohen and Lenstra (1981).
- Deterministic algorithm with time complexity $\log^{O(\log\log\log n)} n$.
- Is conceptually the most complex algorithm of all.
- Attempts to find a prime factor of n using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$.

Adleman-Pomerance-Rumeli Test

- Recall how Lucas-Lehmer-Williams tested n for primality when $(n-1), (n+1), (n^2-n+1)$ or (n^2+n+1) was smooth.
- What can we do when (n^m-1) is smooth? Maybe go to some m-th extension of $\mathbb{Z}_n$?
- This question inspired the APR test (1980). Speeded up by Cohen and Lenstra (1981).
- Deterministic algorithm with time complexity $\log^{O(\log\log\log n)} n$.
- Is conceptually the most complex algorithm of all.
- Attempts to find a prime factor of n using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$.

Adleman-Pomerance-Rumeli Test

- Recall how Lucas-Lehmer-Williams tested n for primality when $(n-1), (n+1), (n^2-n+1)$ or (n^2+n+1) was smooth.
- What can we do when $(n^m - 1)$ is smooth? Maybe go to some m-th extension of $\mathbb{Z}_n$?
- This question inspired the APR test (1980). Speeded up by Cohen and Lenstra (1981).
- Deterministic algorithm with time complexity $\log^{O(\log\log\log n)} n$.
- Is conceptually the most complex algorithm of all.
- Attempts to find a prime factor of n using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$.

Adleman-Pomerance-Rumeli Test

- Recall how Lucas-Lehmer-Williams tested n for primality when $(n-1), (n+1), (n^2-n+1)$ or (n^2+n+1) was smooth.
- What can we do when (n^m-1) is smooth? Maybe go to some m-th extension of $\mathbb{Z}_n$?
- This question inspired the APR test (1980). Speeded up by Cohen and Lenstra (1981).
- Deterministic algorithm with time complexity $\log^{O(\log\log\log n)} n$.
- Is conceptually the most complex algorithm of all.
- Attempts to find a prime factor of n using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$.

Adleman-Pomerance-Rumeli Test

- Recall how Lucas-Lehmer-Williams tested n for primality when $(n-1), (n+1), (n^2-n+1)$ or (n^2+n+1) was smooth.
- What can we do when (n^m-1) is smooth? Maybe go to some m-th extension of $\mathbb{Z}_n$?
- This question inspired the APR test (1980). Speeded up by Cohen and Lenstra (1981).
- Deterministic algorithm with time complexity $\log^{O(\log\log\log n)} n$.
- Is conceptually the most complex algorithm of all.
- Attempts to find a prime factor of n using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$.

Agrawal-Kayal-S (AKS) Test

Theorem (A Generalization of FLT)

If n is a prime then for all $a \in \mathbb{Z}_n$, $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$.

- This was the basis of the AKS test proposed in 2002.
- It was the first unconditional, deterministic and polynomial time primality test.

Agrawal-Kayal-S (AKS) Test

Theorem (A Generalization of FLT)

If n is a prime then for all $a \in \mathbb{Z}_n$, $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$.

- This was the basis of the AKS test proposed in 2002.
- It was the first unconditional, deterministic and polynomial time primality test.

Agrawal-Kayal-S (AKS) Test

Theorem (A Generalization of FLT)

If n is a prime then for all $a \in \mathbb{Z}_n$, $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$.

- This was the basis of the AKS test proposed in 2002.
- It was the first unconditional, deterministic and polynomial time primality test.

AKS Test

1. If n is a prime power, it is composite.
2. Select an r such that $\mathrm{ord}_r(n) > 4\log^2 n$ and work in the ring $R := \mathbb{Z}_n[x]/(x^r - 1)$.
3. For each a, $1 \le a \le \ell := \lceil 2\sqrt{r}\log n \rceil$, check if $(x+a)^n = (x^n + a)$.
4. If yes then n is prime else composite.

AKS Test

1. If n is a prime power, it is composite.
2. Select an r such that $\mathrm{ord}_r(n) > 4\log^2 n$ and work in the ring $R := \mathbb{Z}_n[x]/(x^r - 1)$.
3. For each a, $1 \le a \le \ell := \lceil 2\sqrt{r}\log n \rceil$, check if $(x+a)^n = (x^n + a)$.
4. If yes then n is prime else composite.

AKS Test

1. If n is a prime power, it is composite.
2. Select an r such that $\mathrm{ord}_r(n) > 4\log^2 n$ and work in the ring $R := \mathbb{Z}_n[x]/(x^r - 1)$.
3. For each a, $1 \le a \le \ell := \lceil 2\sqrt{r}\log n \rceil$, check if $(x+a)^n = (x^n + a)$.
4. If yes then n is prime else composite.

AKS Test

1. If n is a prime power, it is composite.
2. Select an r such that $\mathrm{ord}_r(n) > 4\log^2 n$ and work in the ring $R := \mathbb{Z}_n[x]/(x^r - 1)$.
3. For each a, $1 \le a \le \ell := \lceil 2\sqrt{r}\log n \rceil$, check if $(x+a)^n = (x^n + a)$.
4. If yes then n is prime else composite.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r} \rangle$. $t := \# I \geq \mathrm{ord}_r(n) \geq 4\log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r - 1}{x - 1}$ modulo p.
  $\# J \geq 2^{\min\{t, \ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r} \rangle$. $t := \#I \geq \mathrm{ord}_r(n) \geq 4\log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ modulo p.

  $\#J \geq 2^{\min\{t,\ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r} \rangle$. $t := \#I \geq \mathrm{ord}_r(n) \geq 4 \log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ modulo p.

  $\#J \geq 2^{\min\{t,\ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r}\rangle$. $t := \#I \geq \mathrm{ord}_r(n) \geq 4\log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)}\rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ modulo p.
  $\#J \geq 2^{\min\{t,\ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r}\rangle$. $t := \#I \geq \mathrm{ord}_r(n) \geq 4\log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)}\rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ modulo p.
  $\#J \geq 2^{\min\{t,\ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r}\rangle$. $t := \#I \geq \mathrm{ord}_r(n) \geq 4\log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)}\rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ modulo p.
  $\#J \geq 2^{\min\{t,\ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r}\rangle$. $t := \#I \geq \mathrm{ord}_r(n) \geq 4\log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)}\rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ modulo p.
  $\#J \geq 2^{\min\{t,\ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS Test: The Proof

- Suppose all the congruences hold and p is a prime factor of n.
- The group $I := \langle n, p \pmod{r} \rangle$. $t := \#I \geq \mathrm{ord}_r(n) \geq 4\log^2 n$.
- The group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ where $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ modulo p.
  $\#J \geq 2^{\min\{t,\ell\}} > 2^{2\sqrt{t}\log n} \geq n^{2\sqrt{t}}$.
- *Proof:* Let $f(x), g(x)$ be two different products of $(x+a)$'s, having degree $< t$. Suppose $f(x) = g(x) \pmod{p, h(x)}$.
- The test tells us that $f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has atleast t roots in the field $\mathbb{F}_p[x]/(h(x))$, which is a contradiction.

AKS TEST: THE PROOF

THE TWO GROUPS

Group $I := \langle n, p \pmod{r} \rangle$ is of size $t > 4\log^2 n$.
Group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ is of size $> n^{2\sqrt{t}}$.

- There exist tuples $(i,j) \neq (i',j')$ such that $0 \leq i,j,i',j' \leq \sqrt{t}$ and $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{r}$.
- The test tells us that for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x^{n^i \cdot p^j})$ and $f(x)^{n^{i'} \cdot p^{j'}} = f(x^{n^{i'} \cdot p^{j'}})$.
- Thus, for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x)^{n^{i'} \cdot p^{j'}}$.
- As J is a cyclic group: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{\#J}$.
- As $\#J$ is large, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Hence, $n = p$ a prime.

AKS Test: The Proof

The Two Groups

Group $I := \langle n, p \pmod{r} \rangle$ is of size $t > 4\log^2 n$.
Group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ is of size $> n^{2\sqrt{t}}$.

- There exist tuples $(i,j) \neq (i',j')$ such that $0 \leq i,j,i',j' \leq \sqrt{t}$ and $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{r}$.
- The test tells us that for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x^{n^i \cdot p^j})$ and $f(x)^{n^{i'} \cdot p^{j'}} = f(x^{n^{i'} \cdot p^{j'}})$.
- Thus, for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x)^{n^{i'} \cdot p^{j'}}$.
- As J is a cyclic group: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{\#J}$.
- As $\#J$ is large, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Hence, $n = p$ a prime.

AKS Test: The Proof

The Two Groups

Group $I := \langle n, p \pmod{r} \rangle$ is of size $t > 4\log^2 n$.
Group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ is of size $> n^{2\sqrt{t}}$.

- There exist tuples $(i,j) \neq (i',j')$ such that $0 \leq i, j, i', j' \leq \sqrt{t}$ and $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{r}$.
- The test tells us that for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x^{n^i \cdot p^j})$ and $f(x)^{n^{i'} \cdot p^{j'}} = f(x^{n^{i'} \cdot p^{j'}})$.
- Thus, for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x)^{n^{i'} \cdot p^{j'}}$.
- As J is a cyclic group: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{\#J}$.
- As $\#J$ is large, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Hence, $n = p$ a prime.

AKS Test: The Proof

The Two Groups

Group $I := \langle n, p \pmod{r} \rangle$ is of size $t > 4\log^2 n$.
Group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ is of size $> n^{2\sqrt{t}}$.

- There exist tuples $(i,j) \neq (i',j')$ such that $0 \leq i,j,i',j' \leq \sqrt{t}$ and $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{r}$.
- The test tells us that for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x^{n^i \cdot p^j})$ and $f(x)^{n^{i'} \cdot p^{j'}} = f(x^{n^{i'} \cdot p^{j'}})$.
- Thus, for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x)^{n^{i'} \cdot p^{j'}}$.
- As J is a cyclic group: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{\#J}$.
- As $\#J$ is large, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Hence, $n = p$ a prime.

AKS Test: The Proof

The Two Groups

Group $I := \langle n, p \pmod{r} \rangle$ is of size $t > 4\log^2 n$.
Group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ is of size $> n^{2\sqrt{t}}$.

- There exist tuples $(i,j) \neq (i',j')$ such that $0 \leq i,j,i',j' \leq \sqrt{t}$ and $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{r}$.
- The test tells us that for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x^{n^i \cdot p^j})$ and $f(x)^{n^{i'} \cdot p^{j'}} = f(x^{n^{i'} \cdot p^{j'}})$.
- Thus, for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x)^{n^{i'} \cdot p^{j'}}$.
- As J is a cyclic group: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{\#J}$.
- As $\#J$ is large, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Hence, $n = p$ a prime.

AKS Test: The Proof

The Two Groups

Group $I := \langle n, p \pmod r\rangle$ is of size $t > 4\log^2 n$.
Group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)}\rangle$ is of size $> n^{2\sqrt{t}}$.

- There exist tuples $(i,j) \neq (i',j')$ such that $0 \leq i,j,i',j' \leq \sqrt{t}$ and $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod r$.
- The test tells us that for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x^{n^i \cdot p^j})$ and $f(x)^{n^{i'} \cdot p^{j'}} = f(x^{n^{i'} \cdot p^{j'}})$.
- Thus, for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x)^{n^{i'} \cdot p^{j'}}$.
- As J is a cyclic group: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{\#J}$.
- As $\#J$ is large, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Hence, $n = p$ a prime.

AKS Test: The Proof

The Two Groups

Group $I := \langle n, p \pmod{r} \rangle$ is of size $t > 4\log^2 n$.
Group $J := \langle (x+1), \ldots, (x+\ell) \pmod{p, h(x)} \rangle$ is of size $> n^{2\sqrt{t}}$.

- There exist tuples $(i,j) \neq (i',j')$ such that $0 \leq i,j,i',j' \leq \sqrt{t}$ and $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{r}$.
- The test tells us that for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x^{n^i \cdot p^j})$ and $f(x)^{n^{i'} \cdot p^{j'}} = f(x^{n^{i'} \cdot p^{j'}})$.
- Thus, for all $f(x) \in J$, $f(x)^{n^i \cdot p^j} = f(x)^{n^{i'} \cdot p^{j'}}$.
- As J is a cyclic group: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \pmod{\#J}$.
- As $\#J$ is large, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Hence, $n = p$ a prime.

AKS Test: Time Complexity

- Each congruence $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$ can be tested in time $\tilde{O}(r \log^2 n)$.
- The algorithm takes time $\tilde{O}(r^{\frac{3}{2}} \cdot \log^3 n)$.
- Recall that r is the least number such that $\mathrm{ord}_r(n) > 4\log^2 n$.
- Prime number theorem gives $r = O(\log^5 n)$ and thus, time $\tilde{O}(\log^{10.5} n)$.
- **Proof:** Stare at the product:

$$\Pi := (n-1)(n^2-1)\cdots(n^{\lfloor 4\log^2 n \rfloor} - 1)$$

AKS Test: Time Complexity

- Each congruence $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$ can be tested in time $\tilde{O}(r \log^2 n)$.
- The algorithm takes time $\tilde{O}(r^{\frac{3}{2}} \cdot \log^3 n)$.
- Recall that r is the least number such that $\mathrm{ord}_r(n) > 4\log^2 n$.
- Prime number theorem gives $r = O(\log^5 n)$ and thus, time $\tilde{O}(\log^{10.5} n)$.
- **Proof:** Stare at the product:

$$\Pi := (n-1)(n^2-1)\cdots(n^{\lfloor 4\log^2 n \rfloor} - 1)$$

AKS Test: Time Complexity

- Each congruence $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$ can be tested in time $\tilde{O}(r \log^2 n)$.
- The algorithm takes time $\tilde{O}(r^{\frac{3}{2}} \cdot \log^3 n)$.
- Recall that r is the least number such that $\mathrm{ord}_r(n) > 4\log^2 n$.
- Prime number theorem gives $r = O(\log^5 n)$ and thus, time $\tilde{O}(\log^{10.5} n)$.
- **Proof:** Stare at the product:

$$\Pi := (n-1)(n^2-1)\cdots(n^{\lfloor 4\log^2 n\rfloor}-1)$$

AKS Test: Time Complexity

- Each congruence $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$ can be tested in time $\tilde{O}(r \log^2 n)$.
- The algorithm takes time $\tilde{O}(r^{\frac{3}{2}} \cdot \log^3 n)$.
- Recall that r is the least number such that $\mathrm{ord}_r(n) > 4\log^2 n$.
- Prime number theorem gives $r = O(\log^5 n)$ and thus, time $\tilde{O}(\log^{10.5} n)$.
- **Proof:** Stare at the product:

$$\Pi := (n-1)(n^2-1)\cdots(n^{\lfloor 4\log^2 n \rfloor} - 1)$$

AKS Test: Time Complexity

- Each congruence $(x+a)^n = (x^n + a) \pmod{n, x^r - 1}$ can be tested in time $\tilde{O}(r \log^2 n)$.
- The algorithm takes time $\tilde{O}(r^{\frac{3}{2}} \cdot \log^3 n)$.
- Recall that r is the least number such that $\mathrm{ord}_r(n) > 4\log^2 n$.
- Prime number theorem gives $r = O(\log^5 n)$ and thus, time $\tilde{O}(\log^{10.5} n)$.
- **Proof:** Stare at the product:

$$\Pi := (n-1)(n^2-1)\cdots(n^{\lfloor 4\log^2 n\rfloor} - 1)$$

AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

$\#\left\{\textit{prime } p \leq x \mid \exists \textit{ prime } q \geq p^{\frac{2}{3}}, q|(p-1)\right\} \sim \frac{x}{\log x}$.

- Fouvry's theorem gives $r = O(\log^3 n)$ and thus, time $\tilde{O}(\log^{7.5} n)$.
- **Proof:** A "Fouvry prime" $r = \tilde{O}(\log^3 n)$ with $\mathrm{ord}_r(n) \leq 4\log^2 n$ has to divide the product:

$$\Pi' := (n-1)(n^2-1)\cdots(n^{O(\log n)}-1)$$

- But we can find a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ not dividing Π'.
- Thus, there is a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ satisfying $\mathrm{ord}_r(n) > 4\log^2 n$.

AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

$\#\left\{\textit{prime } p \leq x \mid \exists \textit{ prime } q \geq p^{\frac{2}{3}}, q|(p-1)\right\} \sim \frac{x}{\log x}$.

- Fouvry's theorem gives $r = O(\log^3 n)$ and thus, time $\tilde{O}(\log^{7.5} n)$.
- **Proof:** A "Fouvry prime" $r = \tilde{O}(\log^3 n)$ with $\text{ord}_r(n) \leq 4\log^2 n$ has to divide the product:

$$\Pi' := (n-1)(n^2-1)\cdots(n^{O(\log n)}-1)$$

- But we can find a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ not dividing Π'.
- Thus, there is a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ satisfying $\text{ord}_r(n) > 4\log^2 n$.

AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

$\#\left\{\textit{prime } p \leq x \mid \exists \textit{ prime } q \geq p^{\frac{2}{3}}, q|(p-1)\right\} \sim \frac{x}{\log x}.$

- Fouvry's theorem gives $r = O(\log^3 n)$ and thus, time $\tilde{O}(\log^{7.5} n)$.
- **Proof:** A "Fouvry prime" $r = \tilde{O}(\log^3 n)$ with $\mathrm{ord}_r(n) \leq 4\log^2 n$ has to divide the product:

$$\Pi' := (n-1)(n^2-1)\cdots(n^{O(\log n)}-1)$$

- But we can find a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ not dividing Π'.
- Thus, there is a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ satisfying $\mathrm{ord}_r(n) > 4\log^2 n$.

AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

$\#\left\{\text{prime } p \le x \mid \exists \text{ prime } q \ge p^{\frac{2}{3}}, q|(p-1)\right\} \sim \frac{x}{\log x}$.

- Fouvry's theorem gives $r = O(\log^3 n)$ and thus, time $\tilde{O}(\log^{7.5} n)$.
- **Proof:** A "Fouvry prime" $r = \tilde{O}(\log^3 n)$ with $\mathrm{ord}_r(n) \le 4\log^2 n$ has to divide the product:

$$\Pi' := (n-1)(n^2-1)\cdots(n^{O(\log n)}-1)$$

- But we can find a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ not dividing Π'.
- Thus, there is a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ satisfying $\mathrm{ord}_r(n) > 4\log^2 n$.

AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

$\#\left\{prime\ p \leq x \mid \exists\ prime\ q \geq p^{\frac{2}{3}}, q|(p-1)\right\} \sim \frac{x}{\log x}$.

- Fouvry's theorem gives $r = O(\log^3 n)$ and thus, time $\tilde{O}(\log^{7.5} n)$.
- **Proof:** A "Fouvry prime" $r = \tilde{O}(\log^3 n)$ with $\mathrm{ord}_r(n) \leq 4\log^2 n$ has to divide the product:

$$\Pi' := (n-1)(n^2-1)\cdots(n^{O(\log n)}-1)$$

- But we can find a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ not dividing Π'.
- Thus, there is a "Fouvry prime" $r = \tilde{O}(\log^3 n)$ satisfying $\mathrm{ord}_r(n) > 4\log^2 n$.

AKS Test: Variants

- Original AKS test took time $\tilde{O}(\log^{12} n)$. The above improvement used ideas from Hendrik Lenstra Jr.
- Lenstra and Pomerance (2003) further reduced the time complexity to $\tilde{O}(\log^{6} n)$.

AKS Test: Variants

- Original AKS test took time $\tilde{O}(\log^{12} n)$. The above improvement used ideas from Hendrik Lenstra Jr.
- Lenstra and Pomerance (2003) further reduced the time complexity to $\tilde{O}(\log^{6} n)$.

Outline

Questions

Can we reduce the number of a's for which the test is performed?

Conjecture: (Bhattacharjee-Pandey 2001; AKS 2004)

Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$ iff n is prime.

Evidence:

- Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
- The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.

Could this test be used for *factoring* integers? (Agrawal, S, Srivastava, MFCS 2016)

Thank you!

Questions

Can we reduce the number of a's for which the test is performed?

Conjecture: (Bhattacharjee-Pandey 2001; AKS 2004)

Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$ iff n is prime.

Evidence:

- Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
- The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.

Could this test be used for *factoring* integers? (Agrawal, S, Srivastava, MFCS 2016)

Thank you!

Questions

Can we reduce the number of a's for which the test is performed?

Conjecture: (Bhattacharjee-Pandey 2001; AKS 2004)

Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$ iff n is prime.

Evidence:

- Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
- The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.

Could this test be used for *factoring* integers? (Agrawal, S, Srivastava, MFCS 2016)

Thank you!

Questions

Can we reduce the number of a's for which the test is performed?

Conjecture: (Bhattacharjee-Pandey 2001; AKS 2004)

Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$ iff n is prime.

Evidence:

- Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
- The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.

Could this test be used for *factoring* integers? (Agrawal, S, Srivastava, MFCS 2016)

Thank you!

Questions

Can we reduce the number of a's for which the test is performed?

Conjecture: (Bhattacharjee-Pandey 2001; AKS 2004)

Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$ iff n is prime.

Evidence:

- Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
- The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.

Could this test be used for *factoring* integers? (Agrawal, S, Srivastava, MFCS 2016)

Thank you!

Questions

Can we reduce the number of a's for which the test is performed?

Conjecture: (Bhattacharjee-Pandey 2001; AKS 2004)

Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$ iff n is prime.

Evidence:

- Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
- The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.

Could this test be used for *factoring* integers? (Agrawal, S, Srivastava, MFCS 2016)

Thank you!

Questions

Can we reduce the number of a's for which the test is performed?

Conjecture: (Bhattacharjee-Pandey 2001; AKS 2004)

Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1) \pmod{n, x^r - 1}$ iff n is prime.

Evidence:

- Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
- The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.

Could this test be used for *factoring* integers? (Agrawal, S, Srivastava, MFCS 2016)

Thank you!