Primality & Prime Number Generation

Nitin Saxena

CSE, Indian Institute of Technology
Kanpur

Dec 2014
UPMC Paris
1. **The problem**

2. **The high school method**

3. **Prime generation & testing**

4. **Studying integers modulo n**

5. **Studying quadratic extensions mod n**

6. **Studying elliptic curves mod n**

7. **Studying cyclotomic extensions mod n**

8. **Questions**
OUTLINE

1 The problem
2 The high school method
3 Prime generation & testing
4 Studying integers modulo n
5 Studying quadratic extensions mod n
6 Studying elliptic curves mod n
7 Studying cyclotomic extensions mod n
8 Questions
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. $(\ln n)$ is natural log.
- $O^{\sim}(\log^c n)$ 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 at most $(\log n)^c$ steps.
- Note that practically $\left(\log n\right)^{\log \log \log n}$ 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. $(\ln n)$ is natural log.
- $O^\sim(\log^c n)$ 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. $(\ln n)$ is natural log.
- $O^{\sim}(\log^c n)$ 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 at most $(\log n)^c$ 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. $(\ln n)$ is natural log.
- $O^\sim(\log^c n)$ 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. $(\ln n)$ is natural log.
- $O^\sim(\log^c n)$ denotes $\log^c n \cdot (\log \log n)^{O(1)}$. 
OUTLINE

1. The problem
2. The high school method
3. Prime generation & testing
4. Studying integers modulo n
5. Studying quadratic extensions mod n
6. Studying elliptic curves mod n
7. Studying cyclotomic extensions mod n
8. Questions
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.
The high school method

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 $O(\log n)$. 
The high school method

**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

1 The problem
2 The high school method
3 Prime generation & testing
4 Studying integers modulo n
5 Studying quadratic extensions modulo n
6 Studying elliptic curves modulo n
7 Studying cyclotomic extensions modulo n
8 Questions
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 $\frac{\pi(x)}{x}$ 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:
  - $\mathbb{Z}_n$ – Integers modulo $n$.
  - $\mathbb{Z}_n[\sqrt{3}]$ – Quadratic extensions.
  - $\mathbb{Z}_n[x, y]/(y^2 - x^3 - ax - b)$ – Elliptic curves.
  - $\mathbb{Z}_n[x]/(x^r - 1)$ – 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.
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

1. THE PROBLEM
2. THE HIGH SCHOOL METHOD
3. PRIME GENERATION & TESTING
4. STUDYING INTEGERS MODULO N
5. STUDYING QUADRATIC EXTENSIONS MOD N
6. STUDYING ELLIPTIC CURVES MOD N
7. STUDYING CYCLOTOOMIC EXTENSIONS MOD N
8. QUESTIONS
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!
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!
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!
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!
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 \( p \mid (n-1) \).

- Suppose \( (n-1) \) is smooth and we know its prime factors.
- Do the above test for a random \( a \).
Lucas Test

**Theorem (Lucas, 1876)**

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

- Suppose \((n - 1)\) is smooth and we know its prime factors.
- Do the above test for a random \(a\).
Lucas Test

Theorem (Lucas, 1876)

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

- Suppose \((n - 1)\) is smooth and we know its prime factors.
- Do the above test for a random \(a\).
**Lucas Test**

**Theorem (Lucas, 1876)**


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

- Suppose \((n - 1)\) is smooth and we know its prime factors.
- Do the above test for a random \(a\).
**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 $a$. 
Theorem (Pocklington, 1914)

If \( \exists a \in \mathbb{Z}_n \) such that \( a^{n-1} \equiv 1 \mod n \) and \( \gcd(a^{n-1} / p_i - 1, n) = 1 \) for any distinct primes \( p_1, \ldots, p_t \mid (n - 1) \). 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 \( \gcd(a^{n-1}/p_i - 1, n) = 1 \) for any distinct primes \( p_1, \ldots, p_t \mid (n-1) \). 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 \( a \).
Theorem (Pocklington, 1914)

If \( \exists a \in \mathbb{Z}_n \) such that \( a^{n-1} = 1 \) and \( \gcd\left(a^{\frac{n-1}{p_i}} - 1, n\right) = 1 \) for any distinct primes \( p_1, \ldots, p_t \mid (n-1) \). 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 \( \gcd\left(a^{n-1}/p_i - 1, n\right) = 1 \) 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 $a^{n-1} \equiv 1 \pmod{n}$ and $\gcd\left(a^{\frac{n-1}{p_i}} - 1, n\right) = 1$ 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 $O^\sim(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random $a$.
- This gives a randomized test that takes time $O^\sim(\log^2 n)$.
- It errs with probability at most $\frac{1}{2}$. 
**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 $O^\sim(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random $a$.
- This gives a randomized test that takes time $O^\sim(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$. 

**SOLOVAY-STRASSEN: First randomized test**

Studying integers modulo $n$
**Studying integers modulo n**

**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 $O^{\sim}(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random $a$.
- This gives a randomized test that takes time $O^{\sim}(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$.  

---

Nitin Saxena (IIT-K)  
Primality & Prime Generation  
Paris 2014  
16 / 37
**SOLOVAY-STRASSEN**: First randomized test

**Theorem (Strengthening FLT)**

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

- Jacobi symbol $(\frac{a}{n})$ is computable in time $O^\sim(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random $a$.
- This gives a randomized test that takes time $O^\sim(\log^2 n)$.
- It errs with probability atmost $\frac{1}{2}$. 
SOLOVAY-STRASSEN: First randomized test

Theorem (Strengthening FLT)

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

- Jacobi symbol $(a/n)$ is computable in time $O^\sim(\log^2 n)$.
- Solovay-Strassen (1977) check the above equation for a random $a$.
- This gives a randomized test that takes time $O^\sim(\log^2 n)$.
- It errs with probability at most $\frac{1}{2}$. 
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.
 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.
**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.
Studying integers modulo $n$

**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 $a^{2^{s-1} \cdot t}$, $a^{2^{s-2} \cdot t}$, ... , $a^t$ 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 $O^\sim(\log^2 n)$.
- It errs with probability at most $\frac{1}{4}$.
- The most popular primality test!
**Studying integers modulo n**

**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 $a^{2^s-1} \cdot t$, $a^{2^s-2} \cdot t$, ..., $a^t$ 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 $O(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
Studying integers modulo $n$

**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 $O^\sim(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
**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 $O^\sim(\log^2 n)$.
- It errs with probability atmost $\frac{1}{4}$.
- The most popular primality test!
**Studying integers modulo n**

**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 \( O^{\sim}(\log^2 n) \).
- It errs with probability atmost \( \frac{1}{4} \).
- The most popular primality test!
Studying integers modulo \( n \)

**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 \( \chi \) 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 \( \chi \) 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 $\chi$ 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 $\chi$ 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 $(\frac{a}{n}) \neq 1$ (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 $\chi$ 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 $\chi$ 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 $(\frac{a}{n}) \neq 1$ (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!
Studying integers modulo $n$

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 $\chi$ 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 $\chi$ 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 $(\frac{a}{n}) \neq 1$ (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 $\chi$ 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 $\chi$ 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 $(\frac{a}{n}) \neq 1$ (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 $\chi$ 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 $\chi$ 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

1. THE PROBLEM
2. THE HIGH SCHOOL METHOD
3. PRIME GENERATION & TESTING
4. STUDYING INTEGERS MODULO N
5. STUDYING QUADRATIC EXTENSIONS MOD N
6. STUDYING ELLIPTIC CURVES MOD N
7. STUDYING CYCLOTOMIC EXTENSIONS MOD N
8. QUESTIONS
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 $\mathbb{Z}_n[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes.
- Generalization: Whenever $(n + 1)$ has small prime factors one can test $n$ for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $(\frac{D}{n}) = -1$.
- 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 $(2 + \sqrt{3})^{M_k+1}/2 = -1$ in $\mathbb{Z}_n[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes.
- **Generalization:** Whenever $(n + 1)$ has small prime factors one can test $n$ for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $(D/n) = -1$.
- **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 $\mathbb{Z}_n[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes.
- Generalization: Whenever $(n + 1)$ has small prime factors one can test $n$ for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $(\frac{D}{n}) = -1$.
- 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 $\mathbb{Z}_n[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes.
- **Generalization**: Whenever $(n + 1)$ has small prime factors one can test $n$ for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $(\frac{D}{n}) = -1$.
- 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 $\left(2 + \sqrt{3}\right)\frac{M_k+1}{2} = -1$ in $\mathbb{Z}_n[\sqrt{3}]$.

- This yields a deterministic polynomial time primality test for Mersenne primes.
- **Generalization**: Whenever $(n + 1)$ has small prime factors one can test $n$ for primality by working in $\mathbb{Z}_n[\sqrt{D}]$ where $(\frac{D}{n}) = -1$.
- **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

1. THE PROBLEM

2. THE HIGH SCHOOL METHOD

3. PRIME GENERATION & TESTING

4. STUDYING INTEGERS MODULO N

5. STUDYING QUADRATIC EXTENSIONS MOD N

6. STUDYING ELLIPTIC CURVES MOD N

7. STUDYING CYCLOTOMIC EXTENSIONS MOD N

8. QUESTIONS
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 $[(\sqrt{n} - 1)^2, (\sqrt{n} + 1)^2]$ (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 $[(\sqrt{n} - 1)^2, (\sqrt{n} + 1)^2]$ (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 $[(\sqrt{n} - 1)^2, (\sqrt{n} + 1)^2]$ (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 $[\sqrt{n} - 1)^2, (\sqrt{n} + 1)^2]$ (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:
  - $q$ is prime and $q \cdot A = O \Rightarrow A = O$ 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:
  
  $q$ is prime and $q \cdot A = O \Rightarrow A = O$ 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:
  
  $q$ is prime and $q \cdot A = O \Rightarrow A = O$ 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: $q$ is prime and $q \cdot A = O \Rightarrow A = O$ 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:
  
  $q$ is prime and $q \cdot A = O \Rightarrow A = O$ in $E(\mathbb{Z}_p)$
- Thus, $A$ will factor $n$.  

Nitin Saxena (IIT-K)  Primality & Prime Generation  Paris 2014  24 / 37
**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:
  
  $q$ is prime and $q \cdot A = O \Rightarrow A = O$ 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:
  - $q$ is prime and $q \cdot A = O \Rightarrow A = O$ 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:
  
  $q$ is prime and $q \cdot A = O \Rightarrow A = O$ 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:
  
  $q$ is prime and $q \cdot A = O \Rightarrow A = O$ in $E(\mathbb{Z}_p)$
- Thus, $A$ will factor $n$. 

Nitin Saxena (IIT-K)  
Primality & Prime Generation  
Paris 2014  
24 / 37
Goldwasser-Kilian Test

- This is the first randomized test that never errs when $n$ is composite (1986).
- 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): $O \sim (\log^4 n)$.
- 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): \( O^\sim(\log^4 n) \).
- 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): \( O(\log^4 n) \).
- 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

- Time complexity: $O(\log^c n)$ where $c > 30$!
Adleman-Huang Test

- Time complexity: $O(\log^c n)$ where $c > 30$!
OUTLINE

1. The problem

2. The high school method

3. Prime generation & testing

4. Studying integers modulo n

5. Studying quadratic extensions modulo n

6. Studying elliptic curves modulo n

7. Studying cyclotomic extensions modulo n

8. Questions
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 $\mathbb{Z}_n$?
- Deterministic algorithm with time complexity $\log^O(\log \log \log n) \cdot n$.
- Is conceptually the most complex algorithm of all.
- Attempts to find a prime factor of $n$ using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$. 
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 $\mathbb{Z}_n$?
- 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 $\mathbb{Z}_n$?


- 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 $\mathbb{Z}_n$. 

**Studying cyclotomic extensions mod $n$**
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 \( \mathbb{Z}_n \)?
- 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 \( a \in \mathbb{Z}_n \), \((x + a)^n = (x^n + a) (mod \ n, x^r - 1)\).

- 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 \( \text{ord}_r(n) > 4 \log^2 n \) and work in the ring \( R := \mathbb{Z}_n[x]/(x^r - 1) \).
3. For each \( a, 1 \leq a \leq \ell := \lceil 2\sqrt{r \log n} \rceil \), 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 \( \text{ord}_r(n) > 4 \log^2 n \) and work in the ring \( R := \mathbb{Z}_n[x]/(x^r - 1) \).

3. For each \( a \), \( 1 \leq a \leq \ell := \lceil 2 \sqrt{r \log n} \rceil \), 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 $\text{ord}_r(n) > 4 \log^2 n$ and work in the ring $R := \mathbb{Z}_n[x]/(x^r - 1)$.

3. For each $a$, $1 \leq a \leq \ell := \lceil 2\sqrt{r \log n} \rceil$, 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 $\text{ord}_r(n) > 4 \log^2 n$ and work in the ring $R := \mathbb{Z}_n[x]/(x^r - 1)$.

3. For each $a$, $1 \leq a \leq \ell := \lceil 2\sqrt{r \log n} \rceil$, 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 \( I := \langle n, p \pmod{r} \rangle \). \( t := \#I \geq \text{ord}_r(n) \geq 4 \log^2 n \).
- 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 \( p \).

\[ \#J \geq 2^{\min\{t, \ell\}} > 2^{2\sqrt{t} \log n} \geq n^2 \sqrt{\ell}. \]

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 \( f(x^n \cdot p^j) = g(x^n \cdot p^j) \pmod{p, h(x)} \).
- But this means that \( f(z) - g(z) \) has at least \( t \) 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 $I := \langle n, p \pmod{r} \rangle$. $t := \#I \geq \text{ord}_r(n) \geq 4 \log^2 n$.
- 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 at least $t$ 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 $I := \langle n, p \pmod{r} \rangle$. $t := \#I \geq \text{ord}_r(n) \geq 4 \log^2 n$.
- 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 $f(x^{ni \cdot pj}) = g(x^{ni \cdot pj}) \pmod{p, h(x)}$.
- But this means that $f(z) - g(z)$ has at least $t$ 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 \( I := \langle n, p \pmod{r} \rangle \). \( t := \#I \geq \text{ord}_r(n) \geq 4 \log^2 n \).
- 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 \( p \).
  \[ \#J \geq 2\min\{t, \ell\} > 2^{\sqrt{t} \log n} \geq n^{2\sqrt{t}}. \]
- 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 at least \( t \) 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 \( I := \langle n, p \pmod{r} \rangle \). \( t := \# I \geq \text{ord}_r(n) \geq 4 \log^2 n \).
- 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 at least \( t \) 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 $I := \langle n, p \pmod{r} \rangle$. $t := \#I \geq \text{ord}_r(n) \geq 4 \log^2 n$.
- 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 at least $t$ 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 $I := \langle n, p \pmod{r} \rangle$. $t := \#I \geq \text{ord}_r(n) \geq 4 \log^2 n$.
- 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 \( I := \langle n, p \ (\text{mod} \ r) \rangle \). \( t := \# I \geq \text{ord}_r(n) \geq 4 \log^2 n \).
- The group \( J := \langle (x + 1), \ldots, (x + \ell) \ (\text{mod} \ p, h(x)) \rangle \) 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 \( f(x) = g(x) \ (\text{mod} \ p, h(x)) \).
- The test tells us that \( f(x^{n^i \cdot p^j}) = g(x^{n^i \cdot p^j}) \ (\text{mod} \ p, h(x)) \).
- But this means that \( f(z) - g(z) \) has at least \( t \) roots in the field \( \mathbb{F}_p[x]/(h(x)) \), which is a contradiction.
AKS Test: The Proof

**The Two Groups**

Group $I := \langle n, p \ (\text{mod } r) \rangle$ is of size $t > 4 \log^2 n$.

Group $J := \langle (x + 1), \ldots, (x + \ell) \ (\text{mod } p, h(x)) \rangle$ 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 $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \ (\text{mod } r)$.

- 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: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \ (\text{mod } \#J)$.

- 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 $I := \langle n, p \ (\text{mod} \ r) \rangle$ is of size $t > 4 \log^2 n$.

Group $J := \langle (x + 1), \ldots, (x + \ell) \ (\text{mod} \ p, h(x)) \rangle$ 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 $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \ (\text{mod} \ r)$.
- 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: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \ (\text{mod} \ \#J)$.
- 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 $I := \langle n, p \mod r \rangle$ is of size $t > 4 \log^2 n$.

Group $J := \langle (x + 1), \ldots, (x + \ell) \mod p, h(x) \rangle$ 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 $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \mod r$.

- 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: $n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \mod \#J$.

- 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 \( I := \langle n, p \ (\text{mod} \ r) \rangle \) is of size \( t > 4 \log^2 n \).

Group \( J := \langle (x + 1), \ldots, (x + \ell) \ (\text{mod} \ p, h(x)) \rangle \) 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 \(n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \ (\text{mod} \ r)\).

- 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: \( n^i \cdot p^j \equiv n^{i'} \cdot p^{j'} \ (\text{mod} \ \#J) \).

- 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 \(O^{\sim}(r \log^2 n)\).
- The algorithm takes time \(O^{\sim}(r^3 \cdot \log^3 n)\).
- Recall that \(r\) is the least number such that \(\text{ord}_r(n) > 4 \log^2 n\).
- Prime number theorem gives \(r = O(\log^5 n)\) and thus, time \(O^{\sim}(\log^{10.5} n)\).
- 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 \(O^\sim(r \log^2 n)\).
- The algorithm takes time \(O^\sim(r^{3/2} \cdot \log^3 n)\).
- Recall that \(r\) is the least number such that \(\text{ord}_r(n) > 4 \log^2 n\).
- Prime number theorem gives \(r = O(\log^5 n)\) and thus, time \(O^\sim(\log^{10.5} n)\).

**Proof:** Stare at the product:

\[ \prod := (n - 1)(n^2 - 1) \cdots (n^{\lfloor 4 \log^2 n \rfloor} - 1) \]
AKS Test: Time Complexity

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

\[
\prod := (n - 1)(n^2 - 1) \cdots (n^{\lfloor 4 \log^2 n \rfloor} - 1)
\]
AKS Test: Time Complexity

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

**Proof:** Stare at the product:

\[
\prod := (n - 1)(n^2 - 1) \cdots (n^{\lfloor 4 \log^2 n \rfloor} - 1)
\]
AKS Test: Time Complexity

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

\[
\Pi := (n - 1)(n^2 - 1) \cdots \left(n^{\left\lfloor 4 \log^2 n \right\rfloor} - 1\right)
\]
AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

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

- Fouvry’s theorem gives \( r = O(\log^3 n) \) and thus, time \( O^\sim(\log^{7.5} n) \).
- **Proof**: A “Fouvry prime” \( r = O^\sim(\log^3 n) \) 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” \( r = O^\sim(\log^3 n) \) not dividing \( \Pi' \).
- Thus, there is a “Fouvry prime” \( r = O^\sim(\log^3 n) \) satisfying \( \text{ord}_r(n) > 4 \log^2 n \).
AKS Test: Better Time Complexity

**Theorem (Fouvry 1985)**

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

- Fouvry’s theorem gives \( r = O(\log^3 n) \) and thus, time \( O^\sim(\log^{7.5} n) \).
- **Proof:** A “Fouvry prime” \( r = O^\sim(\log^3 n) \) 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” \( r = O^\sim(\log^3 n) \) not dividing \( \Pi' \).
- Thus, there is a “Fouvry prime” \( r = O^\sim(\log^3 n) \) satisfying \( \text{ord}_r(n) > 4 \log^2 n \).
AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

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

- Fouvry’s theorem gives \( r = O(\log^3 n) \) and thus, time \( O^{\sim}(\log^{7.5} n) \).
- **Proof:** A “Fouvry prime” \( r = O^{\sim}(\log^3 n) \) 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” \( r = O^{\sim}(\log^3 n) \) not dividing \( \Pi' \).
- Thus, there is a “Fouvry prime” \( r = O^{\sim}(\log^3 n) \) satisfying \( \text{ord}_r(n) > 4 \log^2 n \).
AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

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

- Fouvry’s theorem gives \( r = O(\log^3 n) \) and thus, time \( O^{\sim}(\log^{7.5} n) \).
- **Proof:** A “Fouvry prime” \( r = O^{\sim}(\log^3 n) \) 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” \( r = O^{\sim}(\log^3 n) \) not dividing \( \Pi' \).
- Thus, there is a “Fouvry prime” \( r = O^{\sim}(\log^3 n) \) satisfying \( \text{ord}_r(n) > 4 \log^2 n \).
AKS Test: Better Time Complexity

Theorem (Fouvry 1985)

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

- Fouvry’s theorem gives $r = O(\log^3 n)$ and thus, time $O(\log^{7.5} n)$.
- **Proof:** A “Fouvry prime” $r = O(\log^3 n)$ 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” $r = O(\log^3 n)$ not dividing $\Pi'$.
- Thus, there is a “Fouvry prime” $r = O(\log^3 n)$ satisfying $\text{ord}_r(n) > 4 \log^2 n$. 

Nitin Saxena (IIT-K) Primality & Prime Generation Paris 2014 34 / 37
AKS Test: Variants

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

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

1 THE PROBLEM
2 THE HIGH SCHOOL METHOD
3 PRIME GENERATION & TESTING
4 STUDYING INTEGERS MODULO N
5 STUDYING QUADRATIC EXTENSIONS MOD N
6 STUDYING ELLIPTIC CURVES MOD N
7 STUDYING CYCLOTOMIC EXTENSIONS MOD N
8 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?

Thank you!
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?

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?

Thank you!
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?

Thank you!
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?

Thank you!
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?

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

$$(x - 1)^n \equiv (x^n - 1) \pmod{n, x^r - 1} \iff n \text{ is prime}.$$  

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?

Thank you!

Nitin Saxena (IIT-K)
Primality & Prime Generation
Paris 2014