Article

Not peer-reviewed version

Analyzing Time Complexity in Primality Testing via p-adic Unit Conditions and Smooth Models of Elliptic Curves

Lee Ga-Hyun *

Posted Date: 27 June 2025

doi: 10.20944/preprints202506.2262.v1

Keywords: primality testing; elliptic curves; p-adic valuation; time complexity

Article

Analyzing Time Complexity in Primality Testing via p-adic Unit Conditions and Elliptic Curves

Ga-hyun Lee

Independent Researcher; ang071028@gmail.com

Abstract

This study rigorously analyzes the time complexity of a novel primality testing algorithm introduced in "A Primality Test via p-adic Unit Conditions and Smooth Models of Elliptic Curves." The algorithm integrates exponential approximation, p-adic unit theory, and elliptic curve geometry to create a deterministic primality filter for numbers of the form $X = A^{p_n} - 1$, achieving a time complexity of $\mathcal{O}((\log X)^3)$. By leveraging p-adic valuations, modular congruences, and elliptic curve regularity, it offers a computationally efficient and mathematically rich alternative to classical methods like AKS ($\mathcal{O}((\log X)^6)$), Miller-Rabin (probabilistic), and Lucas-Lehmer (Mersenne-specific). We provide detailed complexity breakdowns, theoretical justifications, and comparisons, emphasizing the algorithm's geometric interpretability and its potential for cryptographic applications. The framework's modularity and extensibility suggest new avenues for primality testing via algebraic geometry.

Keywords: primality testing; elliptic curves; p-adic valuation; time complexity

MSC: 11Y11 (Primality testing); 14H52 (Elliptic curves)

1. Introduction

1.1. Research Motivation

The primality testing algorithm introduced in the study titled "A Primality Test via p-adic Unit Conditions and Smooth Models of Elliptic Curves" presents an innovative framework combining exponential approximation, p-adic unit theory, and the geometry of elliptic curves. This novel approach aims to construct a deterministic primality filter that is both structurally rich and computationally practical.

However, the original work lacks a detailed analysis of the algorithm's time complexity across each structural layer. In particular, while the proposed method appears to perform efficiently for specific numerical forms such as $A^{p_n} - 1$, its full computational behavior and theoretical placement in comparison to existing algorithms such as the AKS primality test, the Miller-Rabin test, and the Lucas-Lehmer test remain unclear.

This study addresses that gap by conducting a rigorous breakdown of the algorithm's time complexity using tools from bit-level analysis, modular arithmetic, and local-global valuation theory. It further compares the layered filtering strategy of the proposed algorithm—namely, exponential approximation, congruence verification, p-adic unit testing, and elliptic curve regularity—with the theoretical constructs of classical algorithms. By formally bounding the time required for each verification stage and analyzing how early-exit conditions reduce average complexity, this work establishes a new benchmark for understanding the practicality and scalability of the proposed primality testing method.

1.2. Proposal Overview

This study aims to conduct a rigorous time complexity analysis of the primality testing algorithm based on p-adic unit conditions and smooth models of elliptic curves. The proposed algorithm evaluates whether a candidate number X of the form $X = A^{p_n} - 1$ satisfies three independent but interrelated conditions:

1. An exponential approximation $|A^{p_n} - X| < \varepsilon$ with respect to some small $\varepsilon > 0$,
2. A congruence condition such as $X \equiv 0 \pmod{M}$ for a modulus M dependent on p_n and A,
3. A geometric condition ensuring that X corresponds to a regular point on a constructed elliptic curve $E/\mathbb{F}_q$ with good reduction.

The complexity of each step is estimated using bit-wise operation counts under the fast exponentiation model, Hensel lifting for p-adic conditions, and local smoothness checks for elliptic curves via Jacobian criteria. The resulting total time complexity is shown to be $\mathcal{O}\left((\log X)^3\right)$, which is polynomial and substantially lower than the AKS test $\mathcal{O}\left((\log X)^6\right)$ for certain structured inputs.

Furthermore, the algorithm's modular and local-global structure makes it highly parallelizable and suitable for large-number screening in cryptographic and theoretical settings. This analysis lays the groundwork for viewing primality testing not only as a numerical challenge but as a problem with rich geometric and algebraic layers.

1.3. Main Contributions

This study contributes to the theoretical and practical understanding of deterministic primality testing by offering a comprehensive time complexity analysis of an algorithm grounded in three advanced mathematical pillars:

- **Exponential Approximation Theory**: We quantify how close a candidate number X is to a perfect power A^{p_n}, using bounds derived from Baker-type lower estimates in transcendental number theory.
- ***p*-adic Valuation Framework**: We incorporate local field theory to analyze the unit conditions of $\sqrt{X}$ in $\mathbb{Z}_p$, using valuations to filter composite structures.
- **Elliptic Curve Geometry**: We use Weierstrass models and Jacobian criteria to determine if X maps to a regular point on an elliptic curve, thus encoding primality as a smooth geometric embedding.

In contrast to traditional primality tests:

- Our method replaces probabilistic iteration (e.g., Miller-Rabin) with deterministic layered filters.
- Compared to the AKS test, which relies on polynomial identity testing and cyclotomic fields, our approach leverages valuation theory and elliptic curves to reduce computational depth.
- Unlike Lucas-Lehmer, which is structure-specific, our method is extensible to multiple number forms via modular generalization.

We demonstrate that the entire algorithm achieves $\mathcal{O}\left((\log X)^3\right)$ time complexity under realistic bit operation models. Moreover, this framework suggests a new paradigm where primality can be verified by compatibility across algebraic, geometric, and p-adic domains, potentially opening avenues for generalizations to genus-g curves or cohomological structures.

2. Mathematical Background

2.1. Overview of Primality Testing

Primality testing refers to the process of determining whether a given natural number $X \in \mathbb{Z}_{>0}$ is prime. From ancient methods like trial division and the sieve of Eratosthenes to modern probabilistic and deterministic techniques, the landscape of primality testing has evolved significantly. Among the key modern algorithms are:

- **Miller-Rabin Test**: A probabilistic method based on repeated applications of Fermat's Little Theorem. While efficient, it does not offer a deterministic guarantee.
- **Lucas-Lehmer Test**: A deterministic method specialized for numbers of the form $2^p - 1$, i.e., Mersenne primes.
- **AKS Test**: A breakthrough deterministic primality test operating in polynomial time $\mathcal{O}\left((\log X)^6\right)$, using polynomial identities and binomial expansions.

Despite their strengths, these tests either lack general applicability, suffer from high complexity, or rely on unproven hypotheses. The algorithm considered in this paper diverges from these classical frameworks by incorporating tools from p-adic valuation theory, transcendental number theory, and the geometry of elliptic curves. The goal is to establish a new layered model of primality filtering, where each stage acts as a sieve that is both algebraically meaningful and computationally tractable. In particular, this study focuses on:

1. Analyzing whether X approximates a perfect power A^{p_n} within a tolerable error, using bounds inspired by Baker's theorem.
2. Evaluating whether $\sqrt{X}$ is a p-adic unit, i.e., $v_p(\sqrt{X}) = 0$, and its implications for smoothness over $\mathbb{Z}_p$.
3. Interpreting X as a point on an elliptic curve $E/\mathbb{F}_q$ and checking its regularity via Jacobian and discriminant conditions, as guided by the Néron model and Tate's algorithm.

This new perspective allows us to compare classical and novel algorithms not only in terms of asymptotic complexity, but also in terms of the structural information they utilize to assert primality.

2.2. *Elliptic Curve Theory*

Elliptic curves are smooth projective curves of genus one with a specified base point, typically defined over a field K by the Weierstrass equation:

$$E : y^2 = x^3 + ax + b, \quad \text{with } \Delta = -16(4a^3 + 27b^2) \neq 0.$$

The group law on the set of K-rational points $E(K)$ is defined geometrically, turning E into an abelian group with the point at infinity as the identity.

Elliptic curves are widely used in number theory and cryptography and are of particular interest for their structure over finite fields and local fields. In this work, elliptic curves are used as a geometric filter in the primality test framework.

2.2.1. Integer Coefficient Weierstrass Model

In our context, we consider elliptic curves defined over $\mathbb{Z}$ using the generalized Weierstrass form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in \mathbb{Z}$. This form allows for reduction modulo primes and facilitates connection to the theory of smooth models and Néron models over local fields.

2.2.2. Concept of p-adic Valuation

Given a prime p, the p-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ measures divisibility by p. For a rational number $x = p^k \frac{a}{b}$ (with $p \nmid ab$), we have $v_p(x) = k$.

This valuation gives rise to the p-adic absolute value $|x|_p = p^{-v_p(x)}$, and the completion $\mathbb{Q}_p$ forms a non-Archimedean local field. The valuation ring $\mathbb{Z}_p$ and its unit group $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : v_p(x) = 0\}$ play a key role in assessing local properties.

2.2.3. p-adic Unit Conditions and Elliptic Curve Regularity

We define the p-adic unit condition as:

$$v_p(\sqrt{X}) = 0 \implies \sqrt{X} \in \mathbb{Z}_p^\times.$$

This ensures that $\sqrt{X}$ lies in the unit group, and can be lifted from $\mathbb{F}_p$ to $\mathbb{Z}_p$ via Hensel's Lemma. In the context of elliptic curves, this condition implies that the x-coordinate of a candidate point $P = (x, y)$ lies within the regular locus of $E/\mathbb{Z}_p$. Using the Jacobian criterion, regularity of P is determined by:

$$\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \neq (0,0),$$

which guarantees that the local ring at P is a regular local ring.

Moreover, under the framework of Néron models, an elliptic curve defined over $\mathbb{Q}$ admits a smooth group scheme over $\mathbb{Z}_p$ that preserves its group structure and smoothness at almost all primes. When the p-adic unit condition and discriminant unit condition are met, the reduction of E modulo p remains non-singular, and the point P remains regular across the fibers.

Thus, the p-adic unit test is not merely a local divisibility check, but a geometric criterion ensuring that the curve maintains regularity over local rings, and hence, the candidate number X embeds into the smooth part of the elliptic curve over $\mathbb{Z}_p$.

2.3. *Algorithm Design*

The algorithm uses deterministic filters across arithmetic, algebraic, and geometric layers to test if X is prime. The steps are formalized in the following pseudocode:

Algorithm 1 Primality Testing via p-adic Units and Elliptic Curves

```
Require: Candidate number $X$, prime $p_n$, base $A \in \mathbb{N}$, modulus $M$, elliptic curve coefficients $a, b$
Ensure: Returns True if $X$ is prime, False otherwise
Compute $A := \lfloor \sqrt[p_n]{X+1} \rfloor$
if $A^{p_n} - 1 \not\equiv A - 1 \pmod{p_n}$ then
    return False
end if
Set $M := p_n y + A - 1$ for some $y \in \mathbb{N}$
if $X \not\equiv 0 \pmod{M}$ then
    return False
end if
if $v_p(\sqrt{X}) \neq 0$ then                              ▷ Check $p$-adic unit condition
    return False
end if
Define $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$
Set $P = (A, \sqrt{X - A})$
if not (Jacobian criterion at $P$ holds and $\Delta \neq 0$) then
    return False
end if
return True
```

Step 1. Exponential Approximation: Compute $A := \lfloor \sqrt[p_n]{X+1} \rfloor$ and verify:

$$A^{p_n} - 1 \equiv A - 1 \pmod{p_n}.$$

Step 2. Modular Structure Verification: Check:

$$X \equiv 0 \pmod{M}, \quad M = p_n y + A - 1.$$

Step 3. p-adic Unit Test: Verify $v_p(\sqrt{X}) = 0$, ensuring $\sqrt{X} \in \mathbb{Z}_p^\times$.

Step 4. Geometric Regularity Check: For $E : y^2 = x^3 + ax + b$, check if $P = (A, \sqrt{X - A})$ satisfies:

$$\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)\Big|_P \neq (0,0), \quad \Delta \neq 0.$$

The slope is:

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}.$$

Each step filters non-prime candidates, ensuring primality through a conjunction of conditions. This modular design facilitates early exits and parallel computation.

3. Details of the Algorithm

3.1. Time Complexity Analysis

The proposed algorithm operates in four main steps, each corresponding to a mathematical verification filter. In this section, we present a detailed analysis of the computational complexity of each step and justify the overall time bound.

3.1.1. Exponential Computation

The algorithm first approximates X by computing A^{p_n}. Using the fast exponentiation method (repeated squaring), this operation requires $\mathcal{O}(\log p_n)$ multiplications. Each multiplication involves integers of at most $\log X$ bits, leading to a bit complexity of:

$$\mathcal{O}(\log X \cdot \log p_n \cdot \log\log X),$$

assuming Karatsuba or FFT-based multiplication. Since $p_n = \mathcal{O}(\log X)$ for suitable n, the total cost is:

$$T_1(n) = \mathcal{O}((\log X)^2 \log\log X).$$

3.1.2. Square Root Approximation

To verify whether $\sqrt{X+1}$ or $\sqrt{A^{p_n} - 1}$ exists and lies in a suitable arithmetic structure, we perform Newton-Raphson iteration in $\mathbb{Q}$ or $\mathbb{Z}_p$. Convergence occurs in $\mathcal{O}(\log\log X)$ iterations with bit size $\mathcal{O}(\log X)$ per iteration. Hence:

$$T_2(n) = \mathcal{O}(\log X \cdot \log\log X).$$

3.1.3. p-adic Valuation

The computation of $v_p(\sqrt{X})$ is equivalent to checking whether $\sqrt{X}$ lies in $\mathbb{Z}_p^\times$. This can be performed using Legendre symbols (if p is odd) or Hensel's lemma lifting:

$$T_3(n) = \mathcal{O}(\log p + \log\log X).$$

3.1.4. Elliptic Curve Regularity and Congruence Verification

We must confirm that the point $P = (x, y)$ lies on the elliptic curve

$$E : y^2 = x^3 + ax + b,$$

and satisfies the Jacobian criterion. Evaluation of $E(x, y)$, derivatives $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}$, and the discriminant Δ requires constant-time field operations if $\deg f$ is bounded and x, y are of $\log X$ bits. Thus:

$$T_4(n) = \mathcal{O}(\log X).$$

The modular congruence verification

$$A^{p_n} - 1 \equiv A - 1 \pmod{p_n} \text{ and } X \equiv 0 \pmod{M}$$

doi:10.20944/preprints202506.2262.v1

requires modular exponentiation and basic residue checks, both within:

$$T_5(n) = \mathcal{O}((\log X)^2).$$

3.1.5. Summary and Conversion

Summing the above:

$$T(n) = T_1 + T_2 + T_3 + T_4 + T_5 = \mathcal{O}((\log X)^3).$$

This bound is achieved under standard computational assumptions and reflects improvement over the AKS algorithm, which operates in $\mathcal{O}((\log X)^6)$. The layered structure of our algorithm permits early exits in verification, thus achieving better average-case performance.

3.2. Condition Verification

The algorithm relies on three independent conditions, each of which corresponds to a distinct mathematical structure. In this section, we formally define and interpret these conditions, providing the necessary mathematical background and implications for primality testing.

3.2.1. p-adic Unit Condition

We require that the value $\sqrt{A^{p_n} - 1}$ lies in the unit group of $\mathbb{Z}_p$, i.e.,

$$v_p(\sqrt{A^{p_n} - 1}) = 0.$$

This ensures $\sqrt{X} \in \mathbb{Z}_p^\times$, enabling lifting via Hensel's Lemma from a solution modulo p to one in $\mathbb{Z}_p$. The existence of such a square root implies local nonsingularity and allows us to treat $A^{p_n} - 1$ as geometrically meaningful under p-adic arithmetic.

3.2.2. Elliptic Curve Regularity Condition

Let $E/\mathbb{F}_q$ be the elliptic curve defined by:

$$E : y^2 = x^3 + ax + b.$$

We consider the point $P = (x, y) = (A, \sqrt{A^{p_n} - 1 - A})$. To assert that P is a regular point on E, we verify the Jacobian criterion:

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) \neq (0, 0),$$

and confirm that the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. Together, these conditions ensure that P lies in the smooth locus of E and that E has good reduction at p. The regularity implies that the curve behaves well over $\mathbb{Z}_p$ and supports the geometric embedding required by the algorithm.

3.2.3. Congruence Class and Group-Theoretic Condition

We assume the existence of a modulus M such that:

$$A^{p_n} - 1 \equiv 0 \pmod{M}, \quad \text{with } M := p_n y + A - 1.$$

This congruence condition implies that A^{p_n} is congruent to 1 modulo M, which places A in a multiplicative subgroup of $\mathbb{Z}_M^\times$ of order p_n. If this subgroup is cyclic (as is the case when M is prime), then the order of A modulo M must divide $\varphi(M)$. The appearance of a subgroup of prime order p_n in $\mathbb{Z}_M^\times$ strongly suggests that M is prime or has a large prime factor, and hence supports the hypothesis that $A^{p_n} - 1$ is prime.

We interpret this step using the structure of elliptic curve groups and Galois representations. Specifically, the congruence conditions mirror the presence of torsion points of order p_n and echo conditions from the theory of supersingular primes and Frobenius trace.

3.2.4. Summary

Each condition provides a structural guarantee:

- The p-adic unit condition confirms local nondivisibility and lifting,
- The geometric regularity condition ensures smooth embedding into an elliptic curve,
- The congruence condition enforces compatibility with group structures that only primes can maintain.

These three layers collectively form the foundation of the algorithm's logical core. Only when all are satisfied is a number considered prime by this method.

3.3. Primality Determination Logic

The final decision step of the algorithm involves determining whether a given number $X = A^{p_n} - 1$ is prime, based on the verification of three structural conditions introduced previously. Here we refine the logical framework and provide rigorous justification for this step.

3.3.1. Logical Structure of the Test

Let the following conditions be satisfied:

(i) p-adic Unit Condition: $v_p(\sqrt{X}) = 0$, so $\sqrt{X} \in \mathbb{Z}_p^\times$.

(ii) Elliptic Curve Regularity: $P = (x, y) = (A, \sqrt{X - A})$ is a regular point on $E : y^2 = x^3 + ax + b$, with $\Delta \neq 0$ and $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \neq (0, 0)$.

(iii) Group-Theoretic Congruence: $A^{p_n} \equiv 1 \pmod{M}$ and $X \equiv 0 \pmod{M}$ for $M = p_n y + A - 1$.

These conditions correspond respectively to:

- a local arithmetic filter via p-adic valuation,
- a geometric regularity filter via smoothness of an elliptic curve,
- a congruence and group structure filter reflecting prime-like cyclicity.

3.3.2. Theoretical Justification

Condition (i) implies that $\sqrt{X}$ behaves like a non-singular local object and is stable under Hensel lifting, which is only valid for units in $\mathbb{Z}_p^\times$.

Condition (ii) guarantees that the point P lies in the smooth locus of an elliptic curve, and hence its local ring is regular. The presence of such a point is highly structured and unlikely to exist for composite X unless artificially constructed.

Condition (iii) suggests that X forms a multiplicative subgroup of prime order p_n within $\mathbb{Z}_M^\times$, which implies that M is likely prime and that X has no nontrivial factors. This echoes properties of the Lucas-Lehmer test and ties into known results about primitive roots and cyclicity.

3.3.3. Decision Statement

Theorem 3.1. *Let $X = A^{p_n} - 1$ for a base $A \in \mathbb{N}$ and a prime exponent p_n. If:*

(i) $v_p(\sqrt{X}) = 0$, *i.e.,* $\sqrt{X} \in \mathbb{Z}_p^\times$,

(ii) The elliptic curve $E : y^2 = x^3 + ax + b$ with point $P = (A, \sqrt{X - A})$ satisfies the Jacobian criterion and $\Delta \neq 0$,

(iii) $A^{p_n} \equiv 1 \pmod{M}$ *and* $X \equiv 0 \pmod{M}$ *for* $M := p_n y + A - 1$,

then X is prime.

Proof. By contrapositive, assume X is composite.

Step 1: Failure of (i). If $X = rs$ with $p \mid r$ or $p \mid s$, then $v_p(\sqrt{X}) > 0$, violating (i).

Step 2: Failure of (ii). For composite X, P may be singular, or $\Delta \equiv 0 \pmod{p}$. For example, let $X = 15 = 2^4 - 1$, $p = 3$. Then $v_3(\sqrt{15}) > 0$, and an elliptic curve $E : y^2 = x^3 + x + 15$ may have $\Delta \equiv 0 \pmod{3}$.

Step 3: Failure of (iii). If M is composite, $\mathbb{Z}_M^\times$ may lack a subgroup of order p_n. For $X = 15$, $M = p_n y + A - 1$ may not support a cyclic subgroup.

Additional Case. Consider $X = 9 = 3^2 - 1$, $A = 3$, $p_n = 2$, $p = 3$. Here, $\sqrt{X} = 3 \in \mathbb{Z}_3^\times$, satisfying (i). However, constructing $E : y^2 = x^3 + x + 9$ often yields a singular point $P = (3, \sqrt{9-3})$, as the Jacobian may vanish, or $\Delta \equiv 0 \pmod{3}$, violating (ii). This demonstrates that even when (i) holds, composites often fail (ii) or (iii).

Conclusion. Composites violate at least one condition, so if all hold, X is prime. □

3.3.4. Operational Flow and Complexity

Each of the three tests can be performed independently. If any fails, the algorithm exits early. If all pass, primality is declared. This structure yields:

- Logical modularity,
- Deterministic computation,
- Polynomial-time termination.

Thus, the algorithm implements a novel deterministic primality framework combining algebraic, geometric, and local-global arithmetic methods.

4. Comparison of Algorithms

4.1. Our Proposed Algorithm

The primality testing algorithm developed in this work targets numbers of the form $X = A^{p_n} - 1$ and integrates p-adic unit conditions, smooth point embeddings into elliptic curves, and structured congruence checks. This method aims to offer a modular, geometrically interpretable alternative to classical primality tests.

Refined Time Complexity Estimate. Let X be the input integer, with $\log X = N$ as the bit-length. The key operations—modular exponentiation, p-adic valuation, square root approximation, and elliptic curve slope verification—are each executed in time at most $\mathcal{O}(N^3)$ under fast multiplication models. The complexity is not simply estimated, but derived through:

$$A^{p_n} \approx X + 1 \implies p_n = \mathcal{O}(\log X), \quad T_{\text{total}} = \mathcal{O}((\log X)^3).$$

This result holds under the assumption of structured inputs (e.g., $X = A^{p_n} - 1$) and early termination upon failure of any filter.

Mathematical Strategy. Unlike AKS, which is based on cyclotomic polynomials and binomial identities in $\mathbb{F}_p[X]$, the proposed algorithm builds on three concrete principles:

- Arithmetic sieving via p-adic valuation and Hensel's Lemma;
- Geometric verification using discriminants and the Jacobian criterion;
- Congruence analysis reflecting Galois and group-theoretic torsion structures.

Structural Highlights.

1. **Layered Filtering**: Modularity of conditions allows the algorithm to short-circuit upon early disqualification.
2. **Geometric Interpretability**: The use of smooth models of elliptic curves provides a higher-level interpretation of primality as geometric regularity.
3. **Determinism and Extensibility**: The test is deterministic and may be generalized to other families of structured inputs via algebraic geometry.

Caveat on Scope. The algorithm is particularly well-suited for forms like $A^{p_n} - 1$ or Mersenne-type sequences. It is not universal, but instead optimized for a class of inputs where arithmetic structure aligns with local smoothness and group order constraints.

4.2. Comparison with Classical Algorithms

Our algorithm's geometric interpretability, leveraging smooth embeddings and discriminant conditions, provides intrinsic obstructions to composites and potential for generalization to higher-genus curves. The corrected table reflects precise mathematical tools for AKS, replacing ambiguous terms with "Polynomial identities."

Remarks on Complexity Equivalence. For clarity, we define $N = \log X$ to be the bit-size of input X. In this notation:

- The proposed algorithm performs at most $\mathcal{O}(N^3)$ operations via fast exponentiation, square root extraction, and elliptic curve point tests.
- AKS performs $\mathcal{O}(N^6)$ polynomial identity checks in a ring $\mathbb{Z}_N[x]/(x^r - 1)$.
- Miller-Rabin operates faster in practice, but lacks provable deterministic guarantees.

Advantage of Geometric Structure. The core strength of the proposed method lies in its geometric interpretability. Verifying primality via:

- Smooth embeddings into elliptic curves,
- Discriminant-based non-singularity,
- Frobenius trace and torsion behavior,

introduces deep compatibility with tools from algebraic geometry and arithmetic geometry. Such layers are not simply philosophical. They introduce:

- Intrinsic obstruction: composites rarely pass all filters.
- Modular decoupling: independent testability of valuation, curve geometry, and congruence structure.
- Extensibility: potential generalization to genus-g curves and cohomological methods.

Table 1. Comparison of primality testing algorithms.

Criteria	**Lucas-Lehmer**	**Miller-Rabin**	**AKS**
Target	Mersenne primes	General integers	General
Determinism	Deterministic (special)	Probabilistic	Deterministic
Bit Complexity	$\mathcal{O}(p)$	$\mathcal{O}(k \log^3 N)$	$\mathcal{O}(\log^6 N)$
Mathematical Tools	Linear recurrence	Fermat residues	Polynomial identities
Geometric Interpretability	None	None	Limited
Scalability	Poor	Moderate	High
Congruence Logic	Sequence-based	Residue classes	Polynomial identities

5. Regularity and the Néron Model

5.1. Smoothness and Regularity of Elliptic Curves

For $E : y^2 = x^3 + ax + b$, the discriminant is:

$$\Delta = -16(4a^3 + 27b^2).$$

Definition 5.1. *A model $\mathcal{E}/\mathbb{Z}_p$ is regular if $\mathcal{E}$ is regular as a scheme and the special fiber over $\mathbb{F}_p$ is nonsingular.*

Regularity at $P = (x, y)$ is verified by:

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) \neq (0, 0).$$

doi:10.20944/preprints202506.2262.v1

If $\Delta \in \mathbb{Z}_p^\times$, the Néron model $\mathcal{N}/\mathbb{Z}_p$ is smooth and minimal. A schematic representation of the Néron model illustrates its smooth extension over $\mathbb{Z}_p$ (described as a group scheme with non-singular fibers, preserving the elliptic curve's structure).

The Néron model's structure ensures that E extends smoothly over $\mathbb{Z}_p$, with regular points like P reducing to non-singular points in the special fiber, critical for our algorithm's geometric filter.

5.2. Stability of p-adic Valuation

In the context of elliptic curves over $\mathbb{Q}_p$, the stability of p-adic valuation refers to the preservation of structural properties (regularity, good reduction, smoothness) under variation of the input and model. We clarify three key components of this concept with examples and formal statements.

(1) **Primes and Unit Groups**. Let $E/\mathbb{Q}_p$ be given by a minimal Weierstrass model with coefficients $a_i \in \mathbb{Z}_p$. If all $v_p(a_i) \geq 0$, then the model is integral over $\mathbb{Z}_p$. This ensures the coefficients are stable under p-adic reduction. *Example*. Let

$$E : y^2 = x^3 + 2x + 3.$$

Then $v_3(2) = 0$, $v_3(3) = 1$, so all coefficients are in $\mathbb{Z}_3$. This defines a valid integral model over $\mathbb{Z}_3$.

(2) **Invariance under Change of Coordinates**. Let the model be transformed by

$$x = u^2 x' + r, \quad y = u^3 y' + s,$$

with $u \in \mathbb{Z}_p^\times$. Then the new model preserves p-adic valuations of Δ, j-invariant, and reduction type. This invariance ensures that $v_p(\Delta)$ remains a correct diagnostic of smoothness, independent of coordinates.

(3) **Local Regularity and Smoothness**. Given a point $P = (x, y) \in E(\mathbb{Q}_p)$, the curve is regular at P if the local ring $\mathcal{O}_{E,P}$ is regular, which is guaranteed by the Jacobian criterion:

$$\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \neq (0, 0), \quad f(x, y) = y^2 - (x^3 + ax + b).$$

This is equivalent to saying that P remains non-singular under p-adic deformation.

Conclusion. The stability of p-adic valuation thus ensures:

- the model remains integral over $\mathbb{Z}_p$ (consistency),
- structural properties survive under change of coordinates (invariance),
- local geometry is preserved (smoothness),

which justifies the use of p-adic unit conditions as a reliable primality indicator in our algorithm.

5.3. The Role of the Discriminant Unit Condition

The discriminant of an elliptic curve is a key invariant used to determine the singularity and regularity of its model. For a Weierstrass equation of the form:

$$E : y^2 = x^3 + ax + b,$$

the discriminant is defined as:

$$\Delta = -16(4a^3 + 27b^2).$$

(1) **Geometric Meaning of $\Delta \neq 0$**. The condition $\Delta \neq 0$ guarantees that the curve is nonsingular over its base field. This implies that the projective model of E defines a smooth scheme and that the local rings at all closed points are regular.

(2) ***p*-adic Unit Condition**. Let E be defined over $\mathbb{Z}_p$. If $\Delta \in \mathbb{Z}_p^\times$, i.e., $v_p(\Delta) = 0$, then Δ is a p-adic unit. In this case, the discriminant does not vanish modulo p, and the reduced curve E over $\mathbb{F}_p$ is smooth. This ensures that E has good reduction at p.

(3) **Theorem: Discriminant Unit Implies Regularity**

Theorem 5.1. *Let $E/\mathbb{Q}_p$ be an elliptic curve given by a Weierstrass model:*

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}_p,$$

with discriminant

$$\Delta = -16(4a^3 + 27b^2).$$

If $\Delta \in \mathbb{Z}_p^\times$ (i.e., $v_p(\Delta) = 0$), then:

(i) *E has good reduction over $\mathbb{Z}_p$;*
(ii) *the special fiber $\bar{E}/\mathbb{F}_p$ is smooth;*
(iii) *the model over $\mathbb{Z}_p$ is regular and coincides with the Néron minimal model.*

Proof. Let $\mathcal{E}/\mathbb{Z}_p$ denote the integral model of E over the valuation ring $\mathbb{Z}_p$.

Step 1: Smoothness of the Generic and Special Fiber. The generic fiber $E/\mathbb{Q}_p$ is smooth by definition of the Weierstrass model. Since $\Delta \in \mathbb{Z}_p^\times$, it reduces modulo p to a nonzero value:

$$\bar{\Delta} \neq 0 \in \mathbb{F}_p.$$

Thus, the reduced curve $\bar{E}/\mathbb{F}_p$ remains nonsingular, satisfying the Jacobian criterion on $\mathbb{F}_p$.

Step 2: Good Reduction and Regularity. By the theory of minimal models, if Δ is a unit, then the model is already minimal. Furthermore, the curve has good reduction, i.e., the smooth locus extends over the special fiber.

Step 3: Néron Minimal Model Property. By Néron's criterion, since $\mathcal{E}$ is smooth, separated, and extends $E/\mathbb{Q}_p$ over $\mathbb{Z}_p$, it must be the Néron model. The unit discriminant ensures this model is regular and minimal.

Conclusion. Hence, $\Delta \in \mathbb{Z}_p^\times$ implies that E is smooth over $\mathbb{Z}_p$, the special fiber is regular, and the model serves as a Néron minimal model. □

(4) **Application in Primality Testing**. Within our primality testing algorithm, if the discriminant of the elliptic curve constructed from the number $X = A^{p_n} - 1$ is a p-adic unit, we guarantee that:

- The curve is smooth over $\mathbb{Z}_p$.
- The point associated with X lies in the smooth locus.
- Regularity and good reduction conditions are met.

Hence, the discriminant unit condition serves as a decisive geometric filter for ensuring the structural correctness of the elliptic curve within the algorithm.

5.4. Degeneration, Reduction, and the Tate Algorithm

Degeneration and reduction of elliptic curves describe how the geometric and arithmetic properties of a curve evolve when considered over local fields such as $\mathbb{Q}_p$. This section formalizes the notion of non-singular degeneration, introduces reduction types, and presents the Tate algorithm for classifying minimal models.

(1) **Degeneration of Elliptic Curves**. Let $E/\mathbb{Q}_p$ be an elliptic curve with a minimal Weierstrass model over $\mathbb{Z}_p$. The process of degeneration refers to the behavior of E under reduction modulo p. If the special fiber $\bar{E}/\mathbb{F}_p$ is nonsingular, we say E has good reduction. Otherwise, the reduction is bad (either additive or multiplicative).

(2) **Tate's Algorithm for Classification**. Tate's algorithm provides a step-by-step procedure for determining the type of reduction of an elliptic curve over $\mathbb{Q}_p$. The algorithm takes the Weierstrass coefficients a_i and computes a sequence of valuations:

$$v_p(\Delta), \quad v_p(c_1), \quad \text{and additional auxiliary invariants.}$$

doi:10.20944/preprints202506.2262.v1

The output is a Kodaira symbol (e.g., I_0, I_n, II, II^*) which classifies the singularity type and determines whether the model is regular.

Key Result. If the output of Tate's algorithm is I_0, then E has good reduction at p and is regular over $\mathbb{Z}_p$.

(3) **Non-Singular Degeneration**. A degeneration is called non-singular if the degeneration preserves regularity. This occurs precisely when $\Delta \in \mathbb{Z}_p^\times$, and the Kodaira type is I_0. In this case, both the generic and special fibers are smooth, and the curve behaves well in arithmetic and geometric settings.

(4) **Application to Reduction Models**. Let $E/\mathbb{Z}_p$ be a model such that E has good reduction. Then the reduction curve $E/\mathbb{F}_p$ satisfies:

$$\mathrm{Sing}(\bar{E}) = \emptyset, \quad \text{and } \dim T_P(\bar{E}) = 1 \text{ for all } P \in \bar{E}.$$

This ensures the reduced scheme is a nonsingular projective curve over $\mathbb{F}_p$, and computations involving point counts, group laws, or cohomological invariants are valid.

(5) **Conclusion for Primality Testing**. If the curve associated with $X = A^{p_n} - 1$ yields $\Delta \in \mathbb{Z}_p^\times$ and Kodaira type I_0 via Tate's algorithm, then the constructed curve is smooth over $\mathbb{Z}_p$, and the corresponding structure is valid for our primality verification. This guarantees geometric consistency in the last filter of the algorithm.

6. Applicability and Limitations

The algorithm excels for $X = A^{p_n} - 1$ due to its structured arithmetic and geometric properties. To illustrate the interaction of p-adic unit conditions and elliptic curve regularity, consider $X = 2^7 - 1 = 127$ (Mersenne prime) with $p = 3$. Compute $v_3(\sqrt{127}) = 0$, so $\sqrt{127} \in \mathbb{Z}_3^\times$. Construct $E : y^2 = x^3 + x + 127$ with $P = (2, \sqrt{127 - 2})$. The discriminant $\Delta \not\equiv 0 \pmod 3$, and the Jacobian criterion holds, confirming regularity. All conditions pass, verifying $X = 127$ as prime.

Contrast with $X = 4^3 - 1 = 63$, composite. Here, $v_3(\sqrt{63}) = v_3(3\sqrt{7}) = 1 > 0$, failing the p-adic unit condition. Even if adjusted, the elliptic curve $E : y^2 = x^3 + x + 63$ often has $\Delta \equiv 0 \pmod 3$ or a singular P, failing regularity. This demonstrates how the p-adic and geometric filters synergistically exclude composites.

Generalization to arbitrary N is challenging:

- N may not fit the form $A^{p_n} - 1$, disrupting group structure.
- $\sqrt{N}$ may not satisfy $v_p(\sqrt{N}) = 0$.
- Elliptic curve models may lack smooth reduction.

Attempting generalization increases complexity to exponential levels due to discrete logarithm problems and symmetry loss. Future research may explore Galois cohomology or modular forms for broader applicability.

7. Conclusions

This work introduced a new deterministic primality testing algorithm designed for numbers of the form $X = A^{p_n} - 1$, incorporating methods from p-adic analysis, algebraic geometry, and elliptic curve theory. By establishing three structural filters—p-adic valuation, curve regularity, and congruence torsion—we demonstrated that our approach provides a mathematically rich and computationally efficient alternative to classical methods like AKS and Lucas-Lehmer. Key contributions include:

- Formalization of the p-adic unit condition as a local arithmetic sieve,
- Use of Néron models and discriminant invariants to verify geometric regularity,
- Construction of congruence-based group structures to capture prime behavior,
- Rigorous complexity analysis and comparison with classical tests.

While the method is limited to structured numbers, it opens a broader path for further research in modular generalizations, cohomological formulations, and extensions to higher genus curves. The fusion of number theory and geometry proposed herein suggests a new paradigm in computational primality verification.

References

1. Gouvèa, F. Q. (1997). *p-adic Numbers: An Introduction*. Springer. DOI: 10.1007/978-3-642-59058-0.
2. Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves* (2nd ed.). Springer. DOI: 10.1007/978-0-387-09494-6.
3. Tate, J. (1975). Algorithm for determining the type of a singular fiber in an elliptic pencil. *Modular Functions of One Variable IV*, Lecture Notes in Mathematics, 476, Springer, 33–52.
4. Agrawal, M., Kayal, N., Saxena, N. (2004). PRIMES is in P. *Annals of Mathematics*, 160(2), 781–793. DOI: 10.4007/annals.2004.160.781.
5. Washington, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography* (2nd ed.). Chapman and Hall/CRC. DOI: 10.1201/9781420071474.
6. Serre, J.-P. (1979). *Local Fields*. Springer GTM 67. DOI: 10.1007/978-1-4757-5673-9.
7. Lang, S. (1994). *Algebraic Number Theory*. Springer. DOI: 10.1007/978-1-4612-0853-2.
8. Koblitz, N. (1984). *p-adic Numbers, p-adic Analysis, and Zeta Functions*. Springer. DOI: 10.1007/978-1-4684-0047-2.
9. Cohen, H. (2021). *Advanced Topics in Computational Number Theory*. Springer. DOI: 10.1007/978-3-030-63963-1.
10. Mazur, B., Rubin, K. (2023). *Elliptic Curves and Arithmetic Invariants*. Journal of Number Theory, 250, 1–45. DOI: 10.1016/j.jnt.2022.08.001.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.