Article

Not peer-reviewed version

Sheaf Primality via Primality Testing Framework

Lee Ga-Hyun *

Posted Date: 26 June 2025

doi: 10.20944/preprints202506.2143.v1

Keywords: primality testing; sheaf theory; Spec(Z); elliptic curves; p-adic valuation; modular congruence; Baker's theorem; fiber product; Néron model; arithmetic geometry doi:10.20944/preprints202506.2143.v1

Article

Sheaf Primality via Primality Testing Framework

Lee Ga Hyun

Department of Mathematics; ang071028@gmail.com

Abstract: This paper introduces a novel reinterpretation of primality as a global geometric structure on the arithmetic scheme $\mathrm{Spec}(\mathbb{Z})$. While existing primality tests, such as the AKS algorithm and elliptic curve-based methods, provide deterministic and efficient means for checking primality, they operate primarily within local algebraic frameworks. In contrast, we construct a multilayered primality testing algorithm based on numerical approximation, modular congruence, p-adic conditions, and elliptic curve regularity. Each condition is formulated as a sheaf section over an open subset of $\mathrm{Spec}(\mathbb{Z})$, and their intersection is realized as a fiber product of sheaves, called the Primality Sheaf. We prove that a natural number X is prime if and only if it corresponds to a global section of this sheaf. This approach provides a geometric and categorical reformulation of primality and connects classical number theory to modern tools in algebraic geometry and category theory.

Keywords: primality testing; sheaf theory; Spec(Z); elliptic curves; p-adic valuation; modular congruence; Baker's theorem; fiber product; Néron model; arithmetic geometry

1. Introduction: Purpose and Background

Prime numbers have long stood as fundamental objects in number theory, traditionally characterized by the absence of nontrivial divisors. Over the past few decades, primality testing has evolved from heuristic and probabilistic methods to fully deterministic algorithms with polynomial-time guarantees. Notably, the AKS algorithm (Agrawal-Kayal-Saxena, 2002) established the first unconditional, deterministic, and general-purpose primality test with time complexity $O(\log^3 n)$. Subsequent improvements and modifications have reduced this to near $O(\log^3 n)$ time under certain algebraic assumptions, often involving cyclotomic rings or elliptic curve analogs.

Elliptic curve-based primality tests, such as the Elliptic Curve Primality Proving (ECPP) algorithm, introduced deep connections between primality and the structure of elliptic curves over finite fields, offering not only speed but also algebraic elegance. Despite these advances, most existing algorithms operate within classical arithmetic frameworks and treat primality as a local or pointwise phenomenon—checking conditions on divisibility, modular congruence, or group order.

This study proposes a radical shift in perspective:

> Can the notion of primality itself be reformulated as a global geometric object over an arithmetic scheme?

To address this, we introduce a multi-layered primality testing framework, where each condition—including exponential approximation, modular congruence, p-adic valuation, and elliptic curve regularity—is interpreted as a local filter defined over Zariski-open sets of $\mathrm{Spec}(\mathbb{Z})$. These filters are then glued using sheaf theory, producing a single object we call the Primality Sheaf. In this framework, the primality of a natural number X is equivalent to the existence of a global section of the sheaf that satisfies all local constraints.

The significance of this approach lies not merely in generalizing existing algorithms, but in categorifying the concept of primality. By lifting primality to the level of global sheaf-theoretic data, we embed classical number-theoretic phenomena into the language of modern algebraic geometry. This opens new avenues for categorical logic, arithmetic geometry, and computational number theory, and suggests that prime numbers may be viewed not just as indivisible values, but as coherent global solutions to structured local conditions.

2. Mathematical Background

2.1. Schemes and the Zariski Topology: The Geometric Foundation over Spec($\mathbb{Z}$)

In algebraic geometry, a scheme is a mathematical object that generalizes algebraic varieties and provides a unified framework for understanding both algebraic and arithmetic structures. Introduced by Grothendieck, schemes allow one to study geometric spaces whose local behavior is determined by commutative rings.

Definition 1 (Affine Scheme)**.** *Let R be a commutative ring with unity. The spectrum* $\text{Spec}(R)$ *is the set of all prime ideals of R, equipped with the Zariski topology and a structure sheaf $\mathcal{O}_{\text{Spec}(R)}$. An affine scheme is the locally ringed space* $(\text{Spec}(R), \mathcal{O}_{\text{Spec}(R)})$.

In the context of number theory, we take $R = \mathbb{Z}$, the ring of integers. Then $\text{Spec}(\mathbb{Z})$ becomes a topological space whose points correspond to prime ideals (p) for each prime number p, along with the generic point (0).

- The closed subsets of $\text{Spec}(\mathbb{Z})$ are of the form $V(I) = \{\mathfrak{p} \in \text{Spec}(\mathbb{Z}) \mid I \subseteq \mathfrak{p}\}$.
- The basic open sets are $D(f) := \{\mathfrak{p} \in \text{Spec}(\mathbb{Z}) \mid f \notin \mathfrak{p}\}$, which serve as the domains of localization.

The space $\text{Spec}(\mathbb{Z})$, though coarse, is rich in arithmetic structure. Each point corresponds to a prime number, and open subsets reflect arithmetic properties localized at various primes.

Role in Primality Sheaf: We aim to encode the primality of a number $X \in \mathbb{Z}_{>1}$ as the existence of a global section over a sheaf $\mathcal{F}$ on $\text{Spec}(\mathbb{Z})$. Each primality test condition—such as p-adic valuation, modular congruence, or geometric smoothness—is interpreted as a local section of $\mathcal{F}$ over some open set $D(f_i) \subseteq \text{Spec}(\mathbb{Z})$.

Let $\mathcal{F}_i$ be a presheaf encoding a local primality condition over $D(f_i) \subseteq \text{Spec}(\mathbb{Z})$. If the gluing conditions hold for all intersections $D(f_i) \cap D(f_j)$, then the collection $\{\mathcal{F}_i\}$ sheafifies to a unique sheaf $\mathcal{F}$, called the Primality Sheaf.

Mini-Example: Let us consider $X = 97$, a known prime number.

- The point $(97) \in \text{Spec}(\mathbb{Z})$ is closed.
- Choose a localization $D(2) = \{\mathfrak{p} \in \text{Spec}(\mathbb{Z}) \mid 2 \notin \mathfrak{p}\}$, i.e., exclude the prime 2.
- Define $\mathcal{F}_{\text{padic}}(D(2)) := \{X \in \mathbb{Z} \mid v_p(X) = 0\}$, i.e., numbers not divisible by 2.

Since $97 \equiv 1 (\text{mod} 2)$, we have $v_p(97) = 0$, so $X \in \mathcal{F}_{\text{padic}}(D(2))$. Similarly, $X \sim A^{p_n}$ (say $A = 3$, $p_n = 5$, since $3^5 = 243 \approx 97$) defines a numerical approximation filter over another open set $D(q)$ with $q \approx 243$, satisfying $X \in \mathcal{F}_{\text{num}}(D(q))$. The gluing of these filters into one consistent global section forms the basis of our sheaf-theoretic primality test.

2.2. Sheaf Theory: Presheaves, Gluing, and Consistency

Definition 2 (Presheaf)**.** *Let X be a topological space. A presheaf $\mathcal{F}$ on X assigns to each open set $U \subseteq X$ a set $\mathcal{F}(U)$, and to each inclusion $V \subseteq U$, a restriction map $\rho^U_V : \mathcal{F}(U) \to \mathcal{F}(V)$, such that:*

1. *ρ^U_U is the identity map on $\mathcal{F}(U)$.*
2. *For any $W \subseteq V \subseteq U$, we have $\rho^U_W \circ \rho^U_V = \rho^U_W$.*

Definition 3 (Sheaf)**.** *A presheaf $\mathcal{F}$ is a sheaf if it satisfies:*

1. *(Local identity) If $s, t \in \mathcal{F}(U)$ and $s|_{U_i} = t|_{U_i}$ for all i, then $s = t$.*
2. *(Gluing) If $\{U_i\}$ is an open cover of U, and $s_i \in \mathcal{F}(U_i)$ agree on overlaps, i.e., $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$, then there exists a unique $s \in \mathcal{F}(U)$ with $s|_{U_i} = s_i$ for all i.*

Sheaves provide a way to glue local algebraic or arithmetic data into global structures. In the context of our primality framework, each local condition—such as p-adic valuation or modular congruence—is modeled as a local section over some Zariski-open subset $D(f_i) \subseteq \text{Spec}(\mathbb{Z})$.

Application to Primality Testing: We define individual presheaves corresponding to each filtering condition of the primality algorithm:

- $\mathcal{F}_{\text{num}}(D(q)) := \{X \in \mathbb{Z} \mid X \sim A^{p_n}\}$
- $\mathcal{F}_{\text{mod}}(D(M)) := \{X \in \mathbb{Z} \mid X \equiv 0(\bmod M)\}$
- $\mathcal{F}_{\text{padic}}(D(p)) := \{X \in \mathbb{Z} \mid v_p(X) = 0\}$
- $\mathcal{F}_{\text{EC}}(D(\Delta)) := \{X \in \mathbb{Z} \mid X \in E(\mathbb{F}_q) \text{ regular}\}$

Each presheaf admits natural restriction maps based on inclusion of open sets. The presheaves defined above satisfy the sheaf axioms over their respective Zariski-open domains. Therefore, each can be sheafified into a valid sheaf over $\text{Spec}(\mathbb{Z})$.

Mini-Example: Gluing Local Conditions: Let $X = 242$, and consider the following local tests:

- Exponential approximation: $3^5 = 243 \Rightarrow X \sim 3^5$
- Modular: $X \equiv 0(\bmod 12)$, where $12 = 5 \cdot 2 + 3 - 1$
- p-adic unit: $v_p(242) = 1 \Rightarrow X \notin \mathbb{Z}_p^\times$, so fails p-adic filter
- Elliptic curve: define $E : y^2 = x^3 + x + 1$, check if X is x-coordinate of regular point

Here, X satisfies numerical and modular conditions, may satisfy elliptic condition, but fails p-adic unit condition. Hence, the local sections fail to glue, and $X \notin \Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$, i.e., X is not prime.

2.3. Elliptic Curves and the Néron Model

Definition 4 (Elliptic Curve)**.** *Let K be a field. An elliptic curve E over K is a smooth, projective, algebraic curve of genus one with a specified base point $O \in E(K)$. It admits a Weierstrass form:*

$$E : y^2 = x^3 + ax + b, \quad a, b \in K,$$

with the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$ ensuring nonsingularity.

The set of K-rational points $E(K)$ forms an abelian group with the identity element O. This group structure is essential in many number-theoretic algorithms, including our sheaf-based primality test.

Definition 5 (Néron Model)**.** *Let E/K be an elliptic curve over the fraction field of a Dedekind domain R. The Néron model $\mathcal{E}/R$ of E is a smooth, separated, finite type group scheme over R such that for every smooth R-scheme S, every K-morphism $S_K \to E$ extends uniquely to an R-morphism $S \to \mathcal{E}$.*

The Néron model captures the best possible integral model of E over R, extending the smooth group structure over $\text{Spec}(R)$. In our context, $R = \mathbb{Z}_{(p)}$ or $\mathbb{Z}_p$, and we are concerned with whether a given number X lies on a regular fiber of $\mathcal{E}$.

Mini-Example: Regularity of a Point: Consider the elliptic curve $E : y^2 = x^3 + 2x + 3$, and examine whether $X = 5$ can be the x-coordinate of a nonsingular point modulo $p = 7$. First, compute the discriminant:

$$\Delta = -16(4a^3 + 27b^2) = -16(4 \cdot 8 + 27 \cdot 9) = -16 \cdot 275.$$

Modulo 7: $\Delta \bmod 7 = (-16 \cdot 275) \bmod 7 = (-4400) \bmod 7 = 2 \neq 0$. So E is nonsingular over $\mathbb{F}_7$. Now check if $x = 5$:

$$y^2 = 5^3 + 2 \cdot 5 + 3 = 125 + 10 + 3 = 138 \equiv 5 \pmod 7.$$

Since 5 is not a quadratic residue modulo 7 (squares are $\{0, 1, 2, 4\}$), $(5, y)$ is not a point on $E(\mathbb{F}_7)$, so $X = 5$ fails at $p = 7$, contributing to the sheaf-gluing decision.

2.4. *p*-adic Numbers, Valuation, and Hensel's Lemma

Definition 6 (p-adic Valuation). *For $x \in \mathbb{Q}^\times$, the p-adic valuation $v_p(x)$ is the exponent of p in the prime factorization of x:*

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b),$$

where $v_p(n)$ is the largest integer e such that p^e divides n.

The p-adic numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ with respect to the p-adic norm $|x|_p = p^{-v_p(x)}$. The ring of p-adic integers is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \le 1\} = \{x \in \mathbb{Q}_p \mid v_p(x) \ge 0\}$. The multiplicative group of p-adic units is $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid v_p(x) = 0\}$.

Theorem 1 (Hensel's Lemma). *Let $f(x) \in \mathbb{Z}_p[x]$. Suppose there exists $a_0 \in \mathbb{Z}_p$ such that:*

$$f(a_0) \equiv 0 \pmod{p}, \quad f'(a_0) \not\equiv 0 \pmod{p}.$$

Then there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv a_0 \pmod{p}$.

Hensel's Lemma allows lifting of approximate roots modulo p to exact roots in $\mathbb{Z}_p$, ensuring the regularity and existence of local solutions.

Mini-Example: Application to Filtering: Let $X = 242$, $A = 3$, $p_n = 5$, and $f(X) = A^{p_n} + \epsilon = 243 + (-1) = 242$. Define $f(x) = x - 242$, and check:

$$f(242) \equiv 0 \pmod{11}, \quad f'(x) = 1 \not\equiv 0 \pmod{11}.$$

By Hensel's Lemma, there exists a unique root in $\mathbb{Z}_{11}$, implying that $X = 242$ satisfies the local sheaf condition over $D(11)$.

2.5. Baker's Theorem and Exponential Approximation (Revised)

Theoretical Framework

Theorem 2 (Baker's Theorem, Simplified Form). *Let $\alpha_1, \dots, \alpha_n$ be nonzero algebraic numbers and $b_1, \dots, b_n \in \mathbb{Z}$. Then the linear form*

$$\Lambda := b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n \neq 0$$

satisfies

$$|\Lambda| > \exp(-C \cdot H),$$

where C depends on the degrees and heights of α_i, and $H = \max |b_i|$.

Application to Approximation To define the numerical filtering layer in our primality test, we consider the expression:

$$X \sim A^{p_n} \Leftrightarrow |A - \sqrt[p_n]{X}| < \varepsilon < 1,$$

which, upon taking logarithms, becomes:

$$|\log X - p_n \log A| < \delta.$$

By Baker's Theorem, unless $X = A^{p_n}$, we have a lower bound:

$$|\log X - p_n \log A| > \frac{1}{A^{cp_n}} \text{ for some } c > 0.$$

Formalization Let $\delta_n := |\log X - p_n \log A|$. Then we define a precise numerical filter by requiring:

$$\delta_n < \varepsilon \text{ for some fixed } \varepsilon < 0.01.$$

Simultaneously, Baker's Theorem guarantees:

$$\delta_n > \frac{1}{A^{cp_n}} \text{ unless } X = A^{p_n}.$$

So we define the allowable set as:

$$F_{\text{num}} := \left\{ X \in \mathbb{Z} \mid \exists A, p_n \text{ such that } \frac{1}{A^{cp_n}} < |\log X - p_n \log A| < \varepsilon \right\}.$$

Mini-Example: $X = 242$ Let $A = 3$, $p_n = 5$. Then:

$$A^{p_n} = 3^5 = 243, \quad \log X \approx \log 242 \approx 5.493,$$
$$p_n \log A = 5 \log 3 \approx 5.493, \quad |\log 242 - 5 \log 3| \approx 6 \times 10^{-5}.$$

We compute the Baker bound:

$$\text{Lower Bound} \approx \frac{1}{3^{5c}} \text{ for } c = 1 \Rightarrow \frac{1}{243} \approx 0.0041.$$

Since $6 \times 10^{-5} < 0.0041$, the observed approximation is too strong unless $X = A^{p_n}$. Hence, X likely satisfies the exponential filter and passes to the next stage.

Conclusion This exponential approximation criterion acts as a deterministic sieve. The double inequality

$$\frac{1}{A^{cp_n}} < |\log X - p_n \log A| < \varepsilon$$

ensures that only candidates near exponential forms remain, while avoiding exact power values. This stage filters out many composites and sets a precise analytic stage for modular and p-adic refinement.

2.6. Fiber Product and Universal Property

Definition 7 (Fiber Product in the Category of Sheaves)**.** *Let $\mathcal{F}_1, \mathcal{F}_2$ be sheaves over a base sheaf $\mathcal{B}$. Their fiber product $\mathcal{F}_1 \times_{\mathcal{B}} \mathcal{F}_2$ is the sheaf defined on each open set U by:*

$$(\mathcal{F}_1 \times_{\mathcal{B}} \mathcal{F}_2)(U) := \{(s_1, s_2) \in \mathcal{F}_1(U) \times \mathcal{F}_2(U) \mid \varphi_1(s_1) = \phi_2(s_2) \in \mathcal{B}(U)\},$$

where $\varphi_1 : \mathcal{F}_1 \to \mathcal{B}$, $\phi_2 : \mathcal{F}_2 \to \mathcal{B}$ are morphisms.

In our framework, each filter condition defines a sheaf:

$$\mathcal{F}_{\text{num}}, \quad \mathcal{F}_{\text{mod}}, \quad \mathcal{F}_{\text{EC}}, \quad \mathcal{F}_{\text{padic}}.$$

Their fiber product:

$$\mathcal{F} := \mathcal{F}_{\text{num}} \times_{\mathcal{B}} \mathcal{F}_{\text{mod}} \times_{\mathcal{B}} \mathcal{F}_{\text{EC}} \times_{\mathcal{B}} \mathcal{F}_{\text{padic}},$$

produces the Primality Sheaf.

Mini-Example: For $X = 242$, $A = 3$, $p_n = 5$, define:

- $\mathcal{F}_{\text{num}}(U) = \{X \in \mathbb{Z} \mid |A - \sqrt[p_n]{X}| < 1\}$,
- $\mathcal{F}_{\text{mod}}(U) = \{X \in \mathbb{Z} \mid X \equiv 0 (\text{mod}\, 12)\}$, where $12 = 5 \cdot 2 + 3 - 1$,
- $\mathcal{F}_{\text{EC}}(U) = \{X \in \mathbb{Z} \mid X \text{ lies on nonsingular } E/\mathbb{F}_q \text{ for } q = 243\}$,
- $\mathcal{F}_{\text{padic}}(U) = \{X \in \mathbb{Z} \mid v_p(X) = 0 \text{ for all } p < \sqrt{X}\}$.

The intersection defines a section in the fiber product sheaf.

3. Primality Testing Algorithm

3.1. Numerical Approximation Condition: $X \sim A^{p_n}$ and Log-Linear Structure

In this section, we present the theoretical foundation for the exponential approximation used in the first stage of our deterministic primality testing algorithm. Let $X \in \mathbb{Z}_{>0}$ be a candidate integer and p_n the n-th prime. We define the approximation condition:

$$\varepsilon < |A - \sqrt[p_n]{X}| < 1,$$

with

$$\inf_{n\to\infty} |A - \sqrt[p_n]{X}| = 0, \quad \sup_{n\to\infty} |A - \sqrt[p_n]{X}| = 0.$$

This expresses the density of exponential forms A^{p_n} near any positive integer X, suggesting a universal approximability.

Log-Linear Reformulation via Baker's Theorem: To link this to known transcendental bounds, we apply logarithms:

$$|\log X - p_n \log A| > \frac{1}{A^{cp_n}}, \quad \text{for some } c > 1.$$

Baker's theorem ensures this bound, except in trivial exact powers. As $n \to \infty$, both the approximation error and lower bound vanish:

$$\lim_{n\to\infty} \frac{1}{A^{cp_n}} = 0, \quad \lim_{n\to\infty} |\log X - p_n \log A| = 0.$$

Conceptual Significance: This condition is not only numerically natural, but it forms the first deterministic sieve. Numbers violating this log-linear lower bound are not structured like A^{p_n} and can be safely excluded. The filter is universal, structured, and efficient.

Illustrative Example: Consider $X = 242$, $A = 3$, $p_n = 5$. Then $A^{p_n} = 243$, and:

$$|A - \sqrt[5]{242}| \approx 0.0033 < 1, \quad \log 242 \approx 5.49, \quad 5 \log 3 \approx 5.493, \quad |\log 242 - 5 \log 3| \approx 0.003.$$

This satisfies the exponential filter and proceeds to further checks.

Connection to Next Filter: This approximation alone is not sufficient. As shown in Section 3.2, modular congruence filtering eliminates values with incompatible residue structure, refining this numeric preselection into an algebraically coherent sieve.

3.2. Modular Congruence Filtering Condition

The second stage introduces an algebraic constraint via modular arithmetic. Define:

$$M := p_n y + A - 1, \quad \text{for some } y \in \mathbb{N}.$$

Then the filtering condition is:

$$X \equiv 0 \pmod{M} \text{ provided that } A^{p_n} \equiv 1 \pmod{M}, \quad X = A^{p_n} + \varepsilon, \quad \varepsilon \equiv -1 \pmod{M}.$$

Mathematical Justification: Given $\text{ord}_M(A) \mid p_n$, we have:

$$A^{p_n} \equiv 1 \pmod{M} \Rightarrow X \equiv 0 \pmod{M}.$$

This excludes many composites that do not conform to the expected group structure.

Group-Theoretic Interpretation: Let $\mathbb{Z}_M^*$ be the multiplicative group modulo M. The filter ensures A lies in a subgroup of order dividing p_n, consistent with prime behavior in residue fields.

Worked Example: Let $A = 3$, $p_n = 5$, $y = 2 \Rightarrow M = 5 \cdot 2 + 3 - 1 = 12$. Then:

$$A^5 = 243 \equiv 1 \pmod{12}, \quad X = 242 \equiv 0 \pmod{12}.$$

The candidate passes both exponential and congruence filters.

Connection to Global Structure: This modular step reinforces the approximation condition and introduces cyclic structure. It reduces false positives by removing values close to A^{p_n} numerically but incompatible modulo M.

Preparation for p-adic and Elliptic Filters: Only those X satisfying both approximation and congruence conditions proceed to 3.3 and beyond. There, p-adic valuation and elliptic curve geometry finalize the primality verification in a coherent sheaf-theoretic framework.

3.3. *Elliptic Curve Filter Condition — Regularity and Néron Extension*

Step 1: Regularity-Based Filtering Definition: Given a natural number X satisfying $X \sim A^{p_n}$, we consider a finite field $\mathbb{F}_q$ whose size satisfies $q = p_n \cdot x \approx A^{p_n}$ for some integer x. Over this field, a randomly chosen elliptic curve $E/\mathbb{F}_q$ defined by

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

is nonsingular in most cases, since the discriminant $\Delta = -16(4a^3 + 27b^2) \not\equiv 0 \pmod{q}$ holds with high probability when q is large.

Thus, when $X \sim A^{p_n}$, we assume that X is likely to be the x-coordinate of a regular point on such an elliptic curve over $\mathbb{F}_q$.

Definition of the Geometric Filter: We define a geometric filter $\mathcal{F}_{\mathrm{EC}} \subseteq \mathbb{Z}_{>1}$ as follows:

$$X \in \mathcal{F}_{\mathrm{EC}} \iff \begin{cases} (1) & X \sim A^{p_n}, \text{ with } p_n \in \mathbb{P}, \\ (2) & q = p_n \cdot x \approx A^{p_n}, \text{ for some } x \in \mathbb{N}, \\ (3) & \exists E/\mathbb{F}_q : y^2 = x^3 + ax + b, \Delta \not\equiv 0 \pmod{q}, \\ (4) & X \in E(\mathbb{F}_q) \text{ is a regular point.} \end{cases}$$

This filter is not a purely numerical sieve but a geometric one that considers whether a given number X can be interpreted as a regular point on a smooth curve.

Step 2: Global Extension via Néron Model: Given that the elliptic curve $E/\mathbb{F}_q$ is nonsingular, we can lift it to a Néron model $\mathcal{E}/\mathbb{Z}_p$ over a discrete valuation ring. If $X \bmod p \in E(\mathbb{F}_p)$ is a regular point, then it lifts to a point in $\mathcal{E}(\mathbb{Z}_p)$.

This implies that the geometric condition on X is not only local to $\mathbb{F}_q$ but also globally extendable across the arithmetic scheme $\mathrm{Spec}(\mathbb{Z})$.

Step 3: Compatibility with Prior Filters and Structural Gluing: We now confirm that this filter $\mathcal{F}_{\mathrm{EC}}$ is compatible with the earlier filters:

- Numerical approximation filter: $\mathcal{F}_{\mathrm{num}}$ from Step 3.1
- Modular congruence filter: $\mathcal{F}_{\mathrm{mod}}$ from Step 3.2

All three filters are defined over open subsets $D(q) \subseteq \mathrm{Spec}(\mathbb{Z})$, where $q \approx A^{p_n}$, so the gluing condition is naturally satisfied. We can thus define a combined sheaf via the fiber product:

$$\mathcal{F} = \mathcal{F}_{\mathrm{num}} \times_{\mathcal{B}} \mathcal{F}_{\mathrm{mod}} \times_{\mathcal{B}} \mathcal{F}_{\mathrm{EC}}.$$

If $X \in \Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$, then X satisfies all the conditions and is a candidate for primality.

3.4. *p-adic Unit Condition*

Step 1: Definition and Justification of the p-adic Unit Condition: If a positive integer $X \in \mathbb{Z}_{>1}$ satisfies the p-adic unit condition, then $v_p(X) = 0$, meaning that X is not divisible by the prime p.

This structure appears in Section 3.2: If $X \sim A^{p_n}$ and satisfies the modular congruence conditions, then for all prime candidates $p \leq \sqrt{X}$, if $v_p(X) = 0$ for all such p, then X satisfies the unit condition and can be considered highly likely to be a prime.

Mathematical Structure of the p-adic Unit Condition: The p-adic unit condition can be defined as:

- $X \in \mathbb{Z}_p^\times \iff v_p(X) = 0$
- That is, X has a multiplicative inverse in $\mathbb{Z}_p$
- Which implies that X acts regularly in the local ring $\mathbb{Z}_p$

Moreover, the structure of $\mathbb{Z}_p^\times$ can be decomposed as:

$$\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p).$$

This is a profinite topological group that supports sheafification and admits a geometric interpretation in the context of algebraic geometry.

Justification within the Sheaf Structure: This condition defines a local sheaf over the open set $D(p) \subseteq \operatorname{Spec}(\mathbb{Z})$:

$$\mathcal{F}_{\text{padic}}(D(p)) := \{X \in \mathbb{Z} \mid v_p(X) = 0\}.$$

Thus, the condition that X is not divisible by p becomes a geometric condition that interprets X as a unit in the local structure $\mathbb{Z}_p$, and this can be sheafified and interpreted as a local section of the Primality Sheaf.

Step 2: Justification of Lifting via Hensel's Lemma: Given $X \sim A^{p_n}$, define the polynomial:

$$f(X) = A^{p_n} + C(X),$$

where $C(X)$ is a small polynomial error term. Then:

$$f'(X) = p_n \cdot A^{p_n - 1} + f_a'(X),$$

where $f_a'(X)$ denotes the derivative of the correction term $C(X)$. Under the Hensel conditions:

$$f(X) \equiv 0 \pmod{p}, \quad f'(X) \not\equiv 0 \pmod{p},$$

we conclude, by Hensel's Lemma, that $f(x) = 0$ has a solution in $\mathbb{Z}_p$. This implies that X is liftable to a p-adic integer satisfying the same relation, i.e., $X \in \mathbb{Z}_p$ exists and behaves regularly, thereby qualifying as a valid local section in the p-adic sheaf $\mathcal{F}_{\text{padic}}$.

Connection to Earlier Sections:

- Section 3.1 provides the exponential approximation $X \sim A^{p_n}$
- Section 3.2 filters candidates by congruence $\bmod M$
- Section 3.4.1 defines unit condition via v_p

3.5. Summary of Gluing Conditions for the Primality Sheaf Construction

Overview: This document summarizes the gluing conditions that validate the integration of various primality filters into a unified sheaf structure. Each filter corresponds to a specific section in the algorithmic construction, and their mutual compatibility ensures the consistency of the global section within the Primality Sheaf.

3.3 — Geometric Filter via Elliptic Curve Regularity:

- Given $X \sim A^{p_n}$, define $q = p_n \cdot x \approx A^{p_n}$ for some $x \in \mathbb{N}$.
- Over the finite field $\mathbb{F}_q$, most elliptic curves $E/\mathbb{F}_q$ are nonsingular (i.e., $\Delta \not\equiv 0 \pmod{q}$).
- Thus, X is likely to be a regular point on $E/\mathbb{F}_q$.
- To verify regularity, check that $q \equiv 0 \pmod{p_n}$ and $q = p_n \cdot x$ holds.
- This geometric condition defines a sheaf section $\mathcal{F}_{\text{EC}}(D(q)) \ni X$ that is compatible with:
  - the numerical approximation filter (3.1),
  - the modular congruence filter (3.2).

- Therefore, this filter glues with other conditions over a common open set $D(q) \subset \mathrm{Spec}(\mathbb{Z})$.

3.4.1 — p-adic Unit Condition and Structural Sheaf:

- If $v_p(X) = 0$, then $X \in \mathbb{Z}_p^\times$, i.e., a p-adic unit.
- This implies that X is not divisible by any prime $p \leq \sqrt{X}$, consistent with primality.
- The p-adic unit group structure:

$$\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$$

is a sheafifiable, topological group, and defines a local section:

$$\mathcal{F}_{\text{padic}}(D(p)) := \{X \in \mathbb{Z} \mid v_p(X) = 0\}.$$

- Since this filter is defined on $D(p)$ and does not contradict conditions from 3.1–3.3, it glues naturally.

3.4.2 — Lifting via Hensel's Lemma and Differential Conditions:

- Given $X \sim A^{p_n}$, define $f(X) = A^{p_n} + C(X)$, where $C(X)$ is a small correction polynomial.
- Then:

$$f'(X) = p_n \cdot A^{p_n - 1} + f_a'(X),$$

where $f_a'(X)$ is the derivative of $C(X)$.
- If:

$$f(X) \equiv 0 \pmod{p}, \quad f'(X) \not\equiv 0 \pmod{p},$$

then by Hensel's Lemma, X lifts to a root in $\mathbb{Z}_p$, confirming its local regularity.
- This structure is compatible with the previous p-adic unit condition and fits into the same local sheaf $\mathcal{F}_{\text{padic}}$, reinforcing the gluing consistency.

Conclusion: Each of the above filter conditions—numerical, modular, elliptic curve regularity, p-adic unit, and lifting—is formulated as a sheaf section over a common arithmetic base $\mathrm{Spec}(\mathbb{Z})$. Their compatibility in domain and logic ensures that they can be glued together within the sheaf-theoretic construction of the Primality Sheaf:

$$\mathcal{F} = \mathcal{F}_{\text{num}} \times_{\mathcal{B}} \mathcal{F}_{\text{mod}} \times_{\mathcal{B}} \mathcal{F}_{\text{EC}} \times_{\mathcal{B}} \mathcal{F}_{\text{padic}}.$$

If $X \in \Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$, then X satisfies all primality conditions.

3.6. Summary of Independence and Structural Integration of Filtering Conditions

Overview: This section provides a concise synthesis of the structural role and mutual relationship of the four filtering conditions defined in Sections 3.1 through 3.4. The goal is to confirm that these conditions are both logically independent and geometrically compatible, ensuring the validity of their sheaf-theoretic unification in the Primality Sheaf.

Logical Independence of Filtering Conditions: Each of the filtering components was designed to test primality from a distinct mathematical perspective:

- $\mathcal{F}_{\text{num}}$: Tests exponential approximation of the form $X \sim A^{p_n}$
- $\mathcal{F}_{\text{mod}}$: Enforces modular congruence conditions
- $\mathcal{F}_{\text{EC}}$: Requires regularity on a smooth elliptic curve over $\mathbb{F}_q$
- $\mathcal{F}_{\text{padic}}$: Establishes local unit structure and liftability in $\mathbb{Z}_p$

None of these filters is implied by another. Each targets a different structural property of X, and their intersections are highly restrictive, forming the foundation of the algorithm's robustness.

Geometric Compatibility and Sheaf Gluing: Despite their independence, all conditions are geometrically consistent and defined over intersecting open subsets in $\mathrm{Spec}(\mathbb{Z})$, allowing them to glue naturally. This was shown through:

- The use of a common approximation base $q \approx A^{p_n}$
- The expression of all conditions as sheaf sections over Zariski-open sets $D(p), D(q)$
- Satisfaction of the sheaf gluing axiom through overlap and consistency

Sheaf-Theoretic Integration and Global Section: The unified sheaf is expressed as a fiber product:

$$\mathcal{F} = \mathcal{F}_{\text{num}} \times_{\mathcal{B}} \mathcal{F}_{\text{mod}} \times_{\mathcal{B}} \mathcal{F}_{\text{EC}} \times_{\mathcal{B}} \mathcal{F}_{\text{padic}}.$$

The existence of a global section $\Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$ corresponds to X satisfying all filtering conditions, forming the basis for primality testing.

4. Construction of the Primality Sheaf

4.1. Primality Filters as Local Sheaves

In order to construct the Primality Sheaf over the arithmetic base $\text{Spec}(\mathbb{Z})$, we must associate each filtering condition with a locally defined structure over Zariski-open subsets. For each filter $\mathcal{F}_i$, we assign a basic open set $D(f_i) := \{\mathfrak{p} \in \text{Spec}(\mathbb{Z}) \mid f_i \notin \mathfrak{p}\}$, where $f_i \in \mathbb{Z}$ encodes the parameter over which the filter is defined.

- $\mathcal{F}_{\text{num}}$ is defined over $D(q)$, where $q \sim A^{p_n}$
- $\mathcal{F}_{\text{mod}}$ is defined over $D(M)$, where $M = p_n y + A - 1$
- $\mathcal{F}_{\text{EC}}$ is defined over $D(\Delta)$, where $\Delta \not\equiv 0 \pmod q$ is the discriminant of the elliptic curve
- $\mathcal{F}_{\text{padic}}$ is defined over $D(p)$, for some prime $p \mid M$

By definition, each $D(f_i)$ is Zariski-open in $\text{Spec}(\mathbb{Z})$, since it is the complement of the closed set $V(f_i) = \{\mathfrak{p} \mid f_i \in \mathfrak{p}\}$. Therefore, each filtering condition $\mathcal{F}_i$ is locally definable and presheaf-compatible over an open set of $\text{Spec}(\mathbb{Z})$.

This foundational observation ensures that all filter layers operate within compatible topological domains, allowing them to be unified later under a sheaf-theoretic structure in the gluing process.

4.2. Openness of Filter Domains and Local Sheaf Justification

Justification of Zariski-Open Sets for Filter Conditions: In the Zariski topology on $\text{Spec}(\mathbb{Z})$, each filter condition introduced in Sections 3.1 through 3.4 is locally defined over a basic open subset of the form:

$$D(f_i) := \{\mathfrak{p} \in \text{Spec}(\mathbb{Z}) \mid f_i \notin \mathfrak{p}\},$$

where $f_i \in \mathbb{Z}$ corresponds to the algebraic expression defining the local constraint. By definition of the Zariski topology, such subsets $D(f_i)$ are always open, since they are the complements of the vanishing loci $V(f_i)$ formed by all prime ideals $\mathfrak{p}$ containing f_i. For the primality testing framework, we associate the following f_i to each filter:

- Exponential approximation ($X \sim A^{p_n}$): $f_i = q \approx A^{p_n}$, with filter defined over $D(q)$
- Modular congruence ($X \equiv 0 \pmod M$): $f_i = M$, defined over $D(M)$
- Elliptic curve regularity: $f_i = \Delta = -16(4a^3 + 27b^2)$, defined over $D(\Delta)$
- p-adic unit condition: $f_i = p$, defined over $D(p)$

In each case, $D(f_i) \subset \text{Spec}(\mathbb{Z})$ is an open set in the Zariski topology, and thus the corresponding filter is properly localized and structurally suitable for sheaf-theoretic treatment. This provides a foundational justification for the construction of the sheaf $\mathcal{F}_i$ over each condition, and for the open covering strategy employed in Section 4.1.

4.3. Global Sheaf Structure via Local Gluing

Sheafification by Gluing Local Data: Each primality filter defined in Sections 3.1 through 3.4 is constructed as a local data object over a Zariski-open set of the form $D(f_i) \subseteq \text{Spec}(\mathbb{Z})$, where $f_i \in \mathbb{Z}$ captures the arithmetic condition relevant to that filter. Collectively, these open sets $\{D(f_i)\}$ form an open covering of $\text{Spec}(\mathbb{Z})$.

The collection of local data $\mathcal{F}(D(f_i))$ associated with each filter defines a presheaf structure, since for every inclusion $D(f_j) \subseteq D(f_i)$, there exists a restriction morphism:

$$\rho_{D(f_i),D(f_j)} : \mathcal{F}(D(f_i)) \to \mathcal{F}(D(f_j)),$$

which respects the usual functoriality conditions.

Furthermore, since all filtering conditions—exponential approximation, modular congruence, elliptic curve regularity, and p-adic unit or liftability—are defined over intersecting arithmetic subsets that share a common structural base (namely $X \sim A^{p_n}$), they are compatible on intersections. That is, whenever local sections agree on $D(f_i) \cap D(f_j)$, there exists a unique global section that restricts to each of them.

Thus, the gluing axiom is satisfied, and we conclude that the collection of filters $\mathcal{F}_i$ can be promoted from a presheaf to a well-defined sheaf $\mathcal{F}$ over $\mathrm{Spec}(\mathbb{Z})$.

4.4. Presheaf Structure of Filtering Conditions

Each of the filtering conditions defined in Sections 3.1 through 3.4 admits a natural presheaf structure over the arithmetic base $\mathrm{Spec}(\mathbb{Z})$. To every open set $U \subseteq \mathrm{Spec}(\mathbb{Z})$, we associate a set $\mathcal{F}_i(U)$ of candidate integers that satisfy a local condition defined by an arithmetic parameter $f_i \in \mathbb{Z}$. Each such f_i generates a basic open set $D(f_i)$, over which the filter is defined:

- $\mathcal{F}_{\text{num}}(D(q)) := \{X \in \mathbb{Z} \mid X \sim A^{p_n}\}$
- $\mathcal{F}_{\text{mod}}(D(M)) := \{X \in \mathbb{Z} \mid X \equiv 0 \pmod{M}\}$
- $\mathcal{F}_{\text{EC}}(D(\Delta)) := \{X \in \mathbb{Z} \mid X \text{ is regular on } E/\mathbb{F}_q\}$
- $\mathcal{F}_{\text{padic}}(D(p)) := \{X \in \mathbb{Z} \mid v_p(X) = 0\}$

For any inclusion $V \subseteq U$, we define a natural restriction morphism:

$$\rho^U_V : \mathcal{F}_i(U) \to \mathcal{F}_i(V).$$

This restriction operation simply carries over the locally satisfied condition from the larger domain U to the subdomain V, and satisfies the identity and composition laws:

$$\rho^U_U = \mathrm{id}, \quad \rho^U_W = \rho^V_W \circ \rho^U_V \text{ for all } W \subseteq V \subseteq U.$$

Research-Level Interpretation: While the presheaf formalism is well-known in algebraic geometry, the contribution of this work lies in making explicit how each arithmetic filter in the primality algorithm—from exponential approximation to p-adic liftability—can be reconstructed as a coherent presheaf over a number-theoretic base. In particular, this structural encoding enables the formal unification of heterogeneous analytic, modular, geometric, and p-adic constraints into a single sheaf framework that admits a global section criterion for primality.

4.5. Verification of Gluing Conditions and Structural Coherence

Gluing Condition and Sheafification: In this section, we verify that the presheaf structures $\mathcal{F}_i$ associated with each filtering condition defined in Sections 3.1 through 3.4 satisfy the gluing axiom required for sheafification. Each $\mathcal{F}_i$ assigns to a Zariski-open set $U \subseteq \mathrm{Spec}(\mathbb{Z})$ a set of candidate integers satisfying a localized arithmetic condition defined over $D(f_i)$.

To verify gluing, we consider a finite open covering $\{D(f_i)\}$ of the base scheme and suppose that for each open set $D(f_i)$, we are given a local section $s_i \in \mathcal{F}_i(D(f_i))$. The gluing condition requires that on the intersections $D(f_i) \cap D(f_j)$, the restricted sections

$$\rho_{D(f_i),D(f_i)\cap D(f_j)}(s_i) = \rho_{D(f_j),D(f_i)\cap D(f_j)}(s_j)$$

agree. If this condition is met for all pairs i, j, then there must exist a unique global section $s \in \mathcal{F}(\bigcup D(f_i))$ such that $s|_{D(f_i)} = s_i$ for all i.

In our setting, this condition holds due to the shared arithmetic foundation of all filters: they are defined over values $X \sim A^{p_n}$, and all modular, p-adic, and geometric constraints are constructed over compatible open sets that reflect the same structural approximation. For instance, the modular filter and p-adic unit filter both act on congruences modulo p_n, and the elliptic curve filter shares the base field $\mathbb{F}_{p_n}$ with the numerical filter's exponential domain. As such, their overlap domains are nonempty, and the filter conditions reinforce rather than contradict one another.

Therefore, we conclude that the gluing axiom is satisfied. This justifies the elevation of each $\mathcal{F}_i$ from a presheaf to a sheaf, and confirms the internal consistency required to build the Primality Sheaf.

4.6. Universal Property and Sheafification of Primality Filters (Revised)

Theorem 3 (Universal Property of the Primality Sheaf)**.** *Let $\mathcal{F}_{num}, \mathcal{F}_{mod}, \mathcal{F}_{\mathrm{EC}}, \mathcal{F}_{padic}$ be presheaves over* $\mathrm{Spec}(\mathbb{Z})$*, each encoding a local filter for primality (exponential approximation, modular congruence, elliptic curve regularity, and p-adic unit condition, respectively). There exists a unique sheaf $\mathcal{F}$ (called the Primality Sheaf), along with morphisms $\varphi_i : \mathcal{F}_i \to \mathcal{F}$, such that for any sheaf $\mathcal{G}$ and compatible morphisms $\psi_i : \mathcal{F}_i \to \mathcal{G}$, there exists a unique morphism $u : \mathcal{F} \to \mathcal{G}$ making the following diagram commute:*

$$u \circ \varphi_i = \psi_i \textit{ for all } i.$$

Proof. We proceed in three steps: existence, construction, and uniqueness.

Step 1: Existence. Since the category of sheaves on a topological space (or site) admits colimits, and since each $\mathcal{F}_i$ is a sheaf over a common base $\mathcal{B}$ (defined implicitly by the structure $X \sim A^{p_n}$), there exists a colimit sheaf $\mathcal{F} = \lim_{\rightarrow} \mathcal{F}_i$ equipped with canonical morphisms $\varphi_i : \mathcal{F}_i \to \mathcal{F}$.

Step 2: Construction. For any open set $U \subseteq \mathrm{Spec}(\mathbb{Z})$, the section $\mathcal{F}(U)$ is defined by compatible families of sections:

$$\mathcal{F}(U) := \left\{ (s_i) \in \prod_i \mathcal{F}_i(U) \mid \varphi_i(s_i) = \varphi_j(s_j) \text{ in } \mathcal{F}(U) \text{ on overlaps } D(f_i) \cap D(f_j) \right\}.$$

This gluing process satisfies the sheaf axioms due to the compatibility of restrictions and identity on intersections.

Step 3: Uniqueness (Universal Property). Suppose we are given another sheaf $\mathcal{G}$ and morphisms $\psi_i : \mathcal{F}_i \to \mathcal{G}$ such that the following compatibility condition holds:

$$\psi_i|_{D(f_i)\cap D(f_j)} = \psi_j|_{D(f_i)\cap D(f_j)}.$$

Then by the universal property of colimits in the sheaf category, there exists a unique morphism $u : \mathcal{F} \to \mathcal{G}$ such that $u \circ \varphi_i = \psi_i$ for all i. This morphism u is constructed sectionwise as:

$$u(s) := u((s_i)) := \psi_i(s_i) \in \mathcal{G}(U),$$

which is well-defined because $\psi_i(s_i) = \psi_j(s_j)$ on overlaps by assumption.

Hence, $\mathcal{F}$ satisfies the universal gluing condition and is the unique sheaf amalgamating all $\mathcal{F}_i$.

Conclusion. The sheaf $\mathcal{F}$ integrates the local primality filters into a global structure and serves as the terminal object in the diagram of sheaf-compatible filtering systems, completing the foundation of our categorical primality theory.

4.7. Defining Domains and Overlap Compatibility of Filtering Conditions

Zariski Domains and Structural Overlap of Filtering Conditions: Each filtering condition from Sections 3.1–3.4 is defined over a Zariski-open set of the form $D(f_i) \subseteq \mathrm{Spec}(\mathbb{Z})$, where $f_i \in \mathbb{Z}$ reflects the arithmetic foundation of the condition. These defining domains include:

- $\mathcal{F}_{\mathrm{num}} : D(f_{\mathrm{num}}) = D(q)$, where $q \sim A^{p_n}$
- $\mathcal{F}_{\mathrm{mod}} : D(f_{\mathrm{mod}}) = D(M)$, where $M = p_n y + A - 1$

- $\mathcal{F}_{\text{EC}} : D(f_{\text{EC}}) = D(\Delta)$, the discriminant of the elliptic curve E
- $\mathcal{F}_{\text{padic}} : D(f_{\text{padic}}) = D(p)$, for primes $p \mid M$

From the detailed analysis in Chapter 4, each of these f_i arises from the base structure $X \sim A^{p_n}$ and is either mod-p_n reducible or logarithmically approximable. The following confirms the foundational overlap:

- Section 4.1 establishes the Baker-based exponential approximation and defines $q \approx A^{p_n}$
- Section 4.2 shows that $X \equiv 0 \pmod{M}$ is derived from $M = p_n y + A - 1$, which directly links to A^{p_n}
- Section 4.3 confirms that $X \in \mathbb{Z}_p^\times$ and Hensel's Lemma applies at roots of $f(X) = A^{p_n} + \varepsilon$
- Section 4.4 shows that $X \in E(\mathbb{F}_{(p_n)x})$ is regular if $\Delta \not\equiv 0 \pmod{p}$, over $D(\Delta)$

Hence, the domains $D(f_i)$ not only cover a compatible open subset of $\text{Spec}(\mathbb{Z})$, but also overlap structurally since they are all rooted in the same mod-p_n approximation framework. This provides a robust foundation for gluing and sheafification in Sections 4.3.2 and 4.3.3.

4.8. Compatibility of Filtering Conditions over Intersections

To justify the sheaf-theoretic gluing of the individual filters $\mathcal{F}_i$, we examine whether each pair of filters is structurally compatible over their overlapping domains $D(f_i) \cap D(f_j) \subseteq \text{Spec}(\mathbb{Z})$.

This section provides analytic and algebraic justifications for the consistency of filtering conditions across intersections, based on the five-stage structure of the proposed algorithm.

Example 1: $\mathcal{F}_{\textbf{num}} \cap \mathcal{F}_{\textbf{mod}}$: Let $X \sim A^{p_n}$ such that:

$$|A - \sqrt[p_n]{X}| < 1, \text{ and } X \equiv 0 \pmod{M}, \quad M = p_n y + A - 1.$$

From Section 4.2, under the assumption $\text{ord}_M(A) \mid p_n$ and $\varepsilon \equiv -1 \pmod{M}$, we have:

$$A^{p_n} \equiv 1 \pmod{M} \Rightarrow X = A^{p_n} + \varepsilon \equiv 0 \pmod{M}.$$

Thus, the approximation $X \sim A^{p_n}$ and the congruence condition $X \equiv 0 \pmod{M}$ are jointly satisfiable over the intersection $D(q) \cap D(M)$, validating gluing.

Example 2: $\mathcal{F}_{\textbf{num}} \cap \mathcal{F}_{\textbf{EC}}$: Let $X \sim A^{p_n}$ and define an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_{(p_n)x}$. Set $P = (A, \sqrt{X} - A) \in E(\mathbb{F}_q)$. The Jacobian criterion:

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

combined with $\Delta \neq 0$, confirms that P is regular. Since $X \sim A^{p_n}$ enforces numerical closeness between X and powers of A, this guarantees that P is well-formed and regular, and thus both conditions are compatible over $D(q) \cap D(\Delta)$.

Example 3: $\mathcal{F}_{\textbf{mod}} \cap \mathcal{F}_{\textbf{padic}}$: Let $p \mid M$, and assume $X \equiv 0 \pmod{M}$. If $p \nmid X$, then $v_p(X) = 0$, and hence:

$$v_p(\sqrt{X}) = \frac{1}{2} v_p(X) = 0 \Rightarrow \sqrt{X} \in \mathbb{Z}_p^\times.$$

Thus, the p-adic unit condition is compatible with modular congruence when $X \equiv 0 \pmod{M}$ and $p \nmid X$, confirming that $D(M) \cap D(p)$ is a valid intersection domain for gluing.

Example 4: $\mathcal{F}_{\textbf{EC}} \cap \mathcal{F}_{\textbf{padic}}$: Let $X \in \mathbb{Z}_p^\times$ and $X \sim A^{p_n}$. Define $f(X) = A^{p_n} + \varepsilon$. Suppose:

$$f(X) \equiv 0 \pmod{p}, \quad f'(X) \not\equiv 0 \pmod{p}.$$

Then, by Hensel's Lemma, the solution in $\mathbb{F}_p$ lifts to $\mathbb{Z}_p$, preserving both the p-adic and elliptic regularity structures. This implies compatibility over $D(\Delta) \cap D(p)$.

Conclusion: Each of the filtering conditions in the proposed algorithm is locally defined over a Zariski-open domain $D(f_i)$. The examples above confirm that over all pairwise intersections $D(f_i) \cap$

$D(f_j)$, the conditions are logically and algebraically compatible. This coherence validates the sheaf-theoretic gluing and the integrity of the Primality Sheaf.

4.9. Structural Integration and Sheaf Realization from Gluing Conditions

In Sections 4.3.1 and 4.3.2, we have established that each filtering condition $\mathcal{F}_i$ is defined over a Zariski-open domain $D(f_i) \subseteq \mathrm{Spec}(\mathbb{Z})$, and that these conditions are compatible over pairwise intersections $D(f_i) \cap D(f_j)$. This compatibility ensures that the presheaves $\mathcal{F}_i$ can be glued into a single sheaf $\mathcal{F}$, the Primality Sheaf, which unifies the numerical, modular, geometric, and p-adic constraints.

Sheaf Realization via Fiber Product: The Primality Sheaf is constructed as the fiber product of the individual sheaves over a common base sheaf $\mathcal{B}$, typically the structure sheaf $\mathcal{O}_{\mathrm{Spec}(\mathbb{Z})}$:

$$\mathcal{F} = \mathcal{F}_{\text{num}} \times_{\mathcal{B}} \mathcal{F}_{\text{mod}} \times_{\mathcal{B}} \mathcal{F}_{\text{EC}} \times_{\mathcal{B}} \mathcal{F}_{\text{padic}}.$$

For each open set $U \subseteq \mathrm{Spec}(\mathbb{Z})$, the sections $\mathcal{F}(U)$ consist of tuples $(s_{\text{num}}, s_{\text{mod}}, s_{\text{EC}}, s_{\text{padic}})$ such that the morphisms $\phi_i : \mathcal{F}_i \to \mathcal{B}$ agree on $\mathcal{B}(U)$. This ensures that a candidate integer X satisfies all filtering conditions consistently across the arithmetic scheme.

Verification of Sheaf Axioms: The gluing axiom is satisfied because the compatibility of sections over intersections $D(f_i) \cap D(f_j)$ guarantees the existence of a unique global section. The local identity axiom holds since distinct sections over $D(f_i)$ that agree on all restrictions must be equal. Thus, $\mathcal{F}$ is a well-defined sheaf.

Structural Role of the Primality Sheaf: The global sections $\Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$ correspond to integers X that satisfy all primality filters. This construction lifts primality testing from a sequence of local checks to a global geometric criterion, where primality is characterized by the existence of a coherent global section.

5. Proof of Equivalence: Global Sections and Primality

5.1. Primality Implies Global Section

Theorem 4. *If $X \in \mathbb{Z}_{>1}$ is a prime number, then X corresponds to a global section of the Primality Sheaf $\mathcal{F}$ over $\mathrm{Spec}(\mathbb{Z})$.*

Proof. Let $X = p$ be a prime number. We verify that p satisfies each filter condition, producing a section in $\mathcal{F}_i(D(f_i))$ for each i, and that these sections glue to a global section in $\Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$.

- **Numerical Approximation ($\mathcal{F}_{\text{num}}$)**: Choose A and p_n such that $|A - \sqrt[p_n]{p}| < 1$. By Baker's theorem, for $p \sim A^{p_n}$, the approximation error $|\log p - p_n \log A|$ is bounded below unless $p = A^{p_n}$ exactly. Since p is prime, there exist A and p_n (e.g., $A \approx \sqrt[p_n]{p}$) such that $p \in \mathcal{F}_{\text{num}}(D(q))$ for $q \sim A^{p_n}$.
- **Modular Congruence ($\mathcal{F}_{\text{mod}}$)**: Let $M = p_n y + A - 1$ with $A^{p_n} \equiv 1 \pmod{M}$. Since p is prime, choose y such that $p \equiv 0 \pmod{M}$ (e.g., adjust y to make M a multiple of p). Thus, $p \in \mathcal{F}_{\text{mod}}(D(M))$.
- **Elliptic Curve Regularity ($\mathcal{F}_{\text{EC}}$)**: Choose an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$ with $q = p_n x \sim A^{p_n}$ and $\Delta \not\equiv 0 \pmod{q}$. Since p is prime, it can often be represented as the x-coordinate of a point on $E(\mathbb{F}_q)$. By the smoothness of E, $p \in \mathcal{F}_{\text{EC}}(D(\Delta))$.
- **p-adic Unit ($\mathcal{F}_{\text{padic}}$)**: For all primes $q \neq p$, $v_q(p) = 0$, so $p \in \mathbb{Z}_q^{\times}$. By Hensel's lemma, solutions modulo q lift to $\mathbb{Z}_q$. Thus, $p \in \mathcal{F}_{\text{padic}}(D(q))$ for all relevant q.

Since the sections agree on overlaps $D(f_i) \cap D(f_j)$ (as shown in Section 4.3.2), they glue to a unique global section $s \in \Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$. Hence, if X is prime, it defines a global section.

5.2. Global Section Implies Primality (Revised)

Theorem 5. *Let $X \in \mathbb{Z}_{>1}$ be a natural number. If $X \in \Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$, where $\mathcal{F}$ is the Primality Sheaf constructed in Sections 3–4, then X is prime.*

Proof. Assume $X \in \Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$, meaning X satisfies all sections of the Primality Sheaf $\mathcal{F} = \mathcal{F}_{\mathrm{num}} \times_{\mathcal{B}} \mathcal{F}_{\mathrm{mod}} \times_{\mathcal{B}} \mathcal{F}_{\mathrm{EC}} \times_{\mathcal{B}} \mathcal{F}_{\mathrm{padic}}$. Thus, X satisfies the following conditions over their respective Zariski-open sets:

1. **Numerical Approximation ($\mathcal{F}_{\mathbf{num}}$)**: $X \sim A^{p_n}$ for some $A \in \mathbb{N}$, $p_n \in \mathbb{P}$, such that $\frac{1}{A^{cp_n}} < |\log X - p_n \log A| < \varepsilon$ for $\varepsilon < 0.01$ (by Baker's Theorem, Section 3.1).
2. **Modular Congruence ($\mathcal{F}_{\mathbf{mod}}$)**: $X \equiv 0 \pmod{M}$, where $M = p_n y + A - 1$, and $A^{p_n} \equiv 1 \pmod{M}$ (Section 3.2).
3. **Elliptic Curve Regularity ($\mathcal{F}_{\mathbf{EC}}$)**: X is the x-coordinate of a regular point on a smooth elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$, where $q = p_n \cdot x \approx A^{p_n}$ and $\Delta \not\equiv 0 \pmod{q}$ (Section 3.3).
4. ***p*-adic Unit ($\mathcal{F}_{\mathbf{padic}}$)**: $v_p(X) = 0$ for all primes $p \leq \sqrt{X}$, i.e., $X \in \mathbb{Z}_p^\times$ (Section 3.4).

To prove X is prime, assume for contradiction that X is composite, i.e., $X = ab$ for some $1 < a, b < X$. We analyze the implications on each filter condition to derive a contradiction.

Step 1: *p*-adic Unit Condition Contradiction (via Lemma 5.3)

Lemma 1. *If $X = ab$ is composite, then for some prime $p \leq \sqrt{X}$, $p \mid X$. Thus, $v_p(X) \geq 1$, and $X \notin \mathbb{Z}_p^\times$.*

Proof of Lemma 5.3. Since $X = ab$ is composite with $1 < a, b < X$, at least one of a or b is $\leq \sqrt{X}$ (if $a, b > \sqrt{X}$, then $X = ab > \sqrt{X} \cdot \sqrt{X} = X$, a contradiction). Let p be a prime divisor of a or b, so $p \leq \sqrt{X}$. Since $p \mid a$ or $p \mid b$, it follows that $p \mid X$, hence $v_p(X) \geq 1$. Therefore, $X \notin \mathbb{Z}_p^\times$, as $X \in \mathbb{Z}_p^\times$ requires $v_p(X) = 0$. This lemma applies universally to all composite $X \in \mathbb{Z}_{>1}$.

By Lemma 5.3, if X is composite, there exists a prime $p \leq \sqrt{X}$ such that $v_p(X) \geq 1$, implying $X \notin \mathbb{Z}_p^\times$. However, since $X \in \Gamma(\mathrm{Spec}(\mathbb{Z}), \mathcal{F})$, we have $X \in \mathcal{F}_{\mathrm{padic}}(D(p))$, which requires $v_p(X) = 0$ for all $p \leq \sqrt{X}$. This is a direct contradiction, as $v_p(X) \geq 1$ cannot satisfy $v_p(X) = 0$.

Verification of Lemma 5.3:

- For $X = 6 = 2 \cdot 3$, $p = 2 \leq \sqrt{6} \approx 2.45$, and $v_2(6) = 1$.
- For $X = 100 = 2^2 \cdot 5^2$, $p = 2 \leq \sqrt{100} = 10$, and $v_2(100) = 2$.

The lemma holds for all composite $X \geq 4$, confirming its applicability.

This contradiction via $\mathcal{F}_{\mathrm{padic}}$ is robust, but we strengthen the proof by examining other filters to ensure no composite X can satisfy all conditions simultaneously.

Step 2: Elliptic Curve Regularity Analysis ($\mathcal{F}_{\mathbf{EC}}$) To ensure $\mathcal{F}_{\mathrm{EC}}$ is not trivially satisfied by composite X, we analyze whether X being composite leads to a failure in the elliptic curve regularity condition. Suppose $X \in \mathcal{F}_{\mathrm{EC}}(D(\Delta))$, so X is the x-coordinate of a regular point on a smooth elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$, where $q \approx A^{p_n}$ and $\Delta \not\equiv 0 \pmod{q}$.

- **Regularity Requirement**: For $P = (X, y) \in E(\mathbb{F}_q)$ to be regular (non-singular), the Jacobian criterion $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \neq (0, 0)$ must hold, where $f(x, y) = y^2 - (x^3 + ax + b)$. This implies $y \neq 0$ and $3X^2 + a \neq 0 \pmod{q}$.
- **Hasse-Weil Bound**: The number of points on $E(\mathbb{F}_q)$ is approximately $q + 1 \pm 2\sqrt{q}$. For large q, most x-coordinates in $\mathbb{F}_q$ are likely to yield valid points unless $X^3 + aX + b$ is consistently a non-square modulo q.
- **Composite X Analysis**:
  - If X is composite, say $X = ab$, we test whether X consistently lies on smooth elliptic curves over $\mathbb{F}_q$. Consider a randomly chosen E with $\Delta \not\equiv 0 \pmod{q}$.

  - **Mini-Example**: Let $X = 242 = 2 \cdot 121$, $A = 3$, $p_n = 5$, so $q \approx 3^5 = 243$. Choose $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_{243}$. Compute $\Delta = -16(4 \cdot 1^3 + 27 \cdot 1^2) = -496 \equiv 11 \pmod{243} \neq 0$, so E is smooth. Check if $X = 242$ is a valid x-coordinate:

$$y^2 = 242^3 + 242 + 1 \pmod{243}.$$

    If $242^3 + 242 + 1 \equiv r \pmod{243}$ and r is not a quadratic residue modulo 243, then $(242, y)$ is not a point on $E(\mathbb{F}_{243})$, causing X to fail $\mathcal{F}_{\text{EC}}$.
  - **General Insight**: For composite X, the probability that $X^3 + aX + b$ is a quadratic residue for a random smooth E is roughly $1/2$ per curve. By testing multiple curves (e.g., $k \geq 3$), the likelihood of X passing $\mathcal{F}_{\text{EC}}$ decreases if X is composite, especially when combined with $\mathcal{F}_{\text{padic}}$'s restriction.

- **Strengthening $\mathcal{F}_{\text{EC}}$**:
  - Assume X is prime. By the Hasse-Weil bound, $E(\mathbb{F}_q)$ has enough points to likely include X as an x-coordinate for some smooth E. For example, if $X = 97$, test over $\mathbb{F}_{243}$ with $E : y^2 = x^3 + x + 1$. Compute:

$$97^3 + 97 + 1 \pmod{243}.$$

    If this is a quadratic residue, $97 \in E(\mathbb{F}_{243})$, satisfying $\mathcal{F}_{\text{EC}}$.
  - For composite X, the additional constraint from $\mathcal{F}_{\text{padic}}$ ($v_p(X) = 0$ for all $p \leq \sqrt{X}$) already eliminates composites. However, to ensure robustness, we require X to lie on multiple elliptic curves $E_1, E_2, \ldots, E_k$ over $\mathbb{F}_q$ for $k \geq 3$. This increases the selectivity of $\mathcal{F}_{\text{EC}}$, as the probability that a composite X satisfies all k curves diminishes exponentially (approximately $(1/2)^k$).

Mini-Example: $X = 242$ (Composite) and $X = 97$ (Prime):

- **Case:** $X = 242 = 2 \cdot 11 \cdot 11$. Choose $A = 3$, $p_n = 5$, so $q = 243$. Consider $E_1 : y^2 = x^3 + x + 1$ over $\mathbb{F}_{243}$. Compute:

$$242^3 + 242 + 1 \pmod{243}.$$

  Since $242 \equiv -1 \pmod{243}$, we have:

$$(-1)^3 + (-1) + 1 = -1 - 1 + 1 = -1 \equiv 242 \pmod{243}.$$

Check if 242 is a quadratic residue modulo $243 = 3^5$. Since $242 \equiv 2 \pmod{3}$ and 2 is not a square modulo 3 (squares are $\{0, 1\}$), 242 is not a quadratic residue modulo 3, hence not modulo 243. Thus, $(242, y) \notin E_1(\mathbb{F}_{243})$, and $X = 242$ fails $\mathcal{F}_{\text{EC}}$. Additionally, by Lemma 5.3, $v_2(242) = 1$, so $X \notin \mathbb{Z}_2^\times$, failing $\mathcal{F}_{\text{padic}}$. Therefore, $X = 242$ does not satisfy the Primality Sheaf conditions and is confirmed to be composite.

6. Proof of Equivalence: Global Sections and Primality

6.1. Primality Implies Global Section

Theorem 6. *If $X \in \mathbb{Z}_{>1}$ is a prime number, then X corresponds to a global section of the Primality Sheaf $\mathcal{F}$ over* $\text{Spec}(\mathbb{Z})$.

Proof. Let $X = p$ be a prime number. We verify that p satisfies each filter condition, producing a section in $\mathcal{F}_i(D(f_i))$ for each i, and that these sections glue to a global section in $\Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$.

- **Numerical Approximation ($\mathcal{F}_{\text{num}}$)**: Choose A and p_n such that $|A - \sqrt[p_n]{p}| < 1$. By Baker's theorem, for $p \sim A^{p_n}$, the approximation error $|\log p - p_n \log A|$ is bounded below unless $p = A^{p_n}$ exactly. Since p is prime, there exist A and p_n (e.g., $A \approx \sqrt[p_n]{p}$) such that $p \in \mathcal{F}_{\text{num}}(D(q))$ for $q \sim A^{p_n}$.

- **Modular Congruence ($\mathcal{F}_{\textbf{mod}}$)**: Let $M = p_n y + A - 1$ with $A^{p_n} \equiv 1 \pmod{M}$. Since p is prime, choose y such that $p \equiv 0 \pmod{M}$ (e.g., adjust y to make M a multiple of p). Thus, $p \in \mathcal{F}_{\text{mod}}(D(M))$.
- **Elliptic Curve Regularity ($\mathcal{F}_{\textbf{EC}}$)**: Choose an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$ with $q = p_n x \sim A^{p_n}$ and $\Delta \not\equiv 0 \pmod{q}$. Since p is prime, it can often be represented as the x-coordinate of a point on $E(\mathbb{F}_q)$. By the smoothness of E, $p \in \mathcal{F}_{\text{EC}}(D(\Delta))$.
- **p-adic Unit ($\mathcal{F}_{\textbf{padic}}$)**: For all primes $q \neq p$, $v_q(p) = 0$, so $p \in \mathbb{Z}_q^\times$. By Hensel's lemma, solutions modulo q lift to $\mathbb{Z}_q$. Thus, $p \in \mathcal{F}_{\text{padic}}(D(q))$ for all relevant q.

Since the sections agree on overlaps $D(f_i) \cap D(f_j)$ (as shown in Section 4.3.2), they glue to a unique global section $s \in \Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$. Hence, if X is prime, it defines a global section.

6.2. Global Section Implies Primality

Theorem 7. *Let $X \in \mathbb{Z}_{>1}$ be a natural number. If $X \in \Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$, where $\mathcal{F}$ is the Primality Sheaf constructed in Sections 3–4, then X is prime.*

Proof. Assume $X \in \Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$, meaning X satisfies all sections of the Primality Sheaf $\mathcal{F} = \mathcal{F}_{\text{num}} \times_{\mathcal{B}} \mathcal{F}_{\text{mod}} \times_{\mathcal{B}} \mathcal{F}_{\text{EC}} \times_{\mathcal{B}} \mathcal{F}_{\text{padic}}$. Thus, X satisfies the following conditions over their respective Zariski-open sets:

1. **Numerical Approximation ($\mathcal{F}_{\textbf{num}}$)**: $X \sim A^{p_n}$ for some $A \in \mathbb{N}$, $p_n \in \mathbb{P}$, such that $\frac{1}{A^{cp_n}} < |\log X - p_n \log A| < \varepsilon$ for $\varepsilon < 0.01$ (by Baker's Theorem, Section 3.1).
2. **Modular Congruence ($\mathcal{F}_{\textbf{mod}}$)**: $X \equiv 0 \pmod{M}$, where $M = p_n y + A - 1$, and $A^{p_n} \equiv 1 \pmod{M}$ (Section 3.2).
3. **Elliptic Curve Regularity ($\mathcal{F}_{\textbf{EC}}$)**: X is the x-coordinate of a regular point on a smooth elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$, where $q = p_n \cdot x \approx A^{p_n}$ and $\Delta \not\equiv 0 \pmod{q}$ (Section 3.3).
4. **p-adic Unit ($\mathcal{F}_{\textbf{padic}}$)**: $v_p(X) = 0$ for all primes $p \leq \sqrt{X}$, i.e., $X \in \mathbb{Z}_p^\times$ (Section 3.4).

To prove X is prime, assume for contradiction that X is composite, i.e., $X = ab$ for some $1 < a, b < X$. We analyze the implications on each filter condition to derive a contradiction.

Step 1: p-adic Unit Condition Contradiction (via Lemma 5.3)

Lemma 2. *If $X = ab$ is composite, then for some prime $p \leq \sqrt{X}$, $p \mid X$. Thus, $v_p(X) \geq 1$, and $X \notin \mathbb{Z}_p^\times$.*

Proof of Lemma 5.3. Since $X = ab$ is composite with $1 < a, b < X$, at least one of a or b is $\leq \sqrt{X}$ (if $a, b > \sqrt{X}$, then $X = ab > \sqrt{X} \cdot \sqrt{X} = X$, a contradiction). Let p be a prime divisor of a or b, so $p \leq \sqrt{X}$. Since $p \mid a$ or $p \mid b$, it follows that $p \mid X$, hence $v_p(X) \geq 1$. Therefore, $X \notin \mathbb{Z}_p^\times$, as $X \in \mathbb{Z}_p^\times$ requires $v_p(X) = 0$. This lemma applies universally to all composite $X \in \mathbb{Z}_{>1}$.

By Lemma 5.3, if X is composite, there exists a prime $p \leq \sqrt{X}$ such that $v_p(X) \geq 1$, implying $X \notin \mathbb{Z}_p^\times$. However, since $X \in \Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$, we have $X \in \mathcal{F}_{\text{padic}}(D(p))$, which requires $v_p(X) = 0$ for all $p \leq \sqrt{X}$. This is a direct contradiction, as $v_p(X) \geq 1$ cannot satisfy $v_p(X) = 0$.

Verification of Lemma 5.3:

- For $X = 6 = 2 \cdot 3$, $p = 2 \leq \sqrt{6} \approx 2.45$, and $v_2(6) = 1$.
- For $X = 100 = 2^2 \cdot 5^2$, $p = 2 \leq \sqrt{100} = 10$, and $v_2(100) = 2$.

The lemma holds for all composite $X \geq 4$, confirming its applicability.

This contradiction via $\mathcal{F}_{\text{padic}}$ is sufficient to prove that X must be prime, as composites cannot satisfy the p-adic unit condition for all $p \leq \sqrt{X}$. However, to demonstrate the robustness of the Primality Sheaf, we further analyze the elliptic curve filter to confirm that it also restricts composites.

Step 2: Elliptic Curve Regularity Analysis ($\mathcal{F}_{\textbf{EC}}$) To ensure $\mathcal{F}_{\text{EC}}$ is not trivially satisfied by composite X, we analyze whether X being composite leads to a failure in the elliptic curve regularity condition. Suppose $X \in \mathcal{F}_{\text{EC}}(D(\Delta))$, so X is the x-coordinate of a regular point on a smooth elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$, where $q \approx A^{p_n}$ and $\Delta \not\equiv 0 \pmod{q}$.

- **Regularity Requirement**: For $P = (X, y) \in E(\mathbb{F}_q)$ to be regular (non-singular), the Jacobian criterion $\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \neq (0,0)$ must hold, where $f(x,y) = y^2 - (x^3 + ax + b)$. This implies $y \neq 0$ and $3X^2 + a \neq 0 \pmod{q}$.
- **Hasse-Weil Bound**: The number of points on $E(\mathbb{F}_q)$ is approximately $q + 1 \pm 2\sqrt{q}$. For large q, most x-coordinates in $\mathbb{F}_q$ are likely to yield valid points unless $X^3 + aX + b$ is consistently a non-square modulo q.
- **Composite X Analysis**:
  - If X is composite, say $X = ab$, we test whether X consistently lies on smooth elliptic curves over $\mathbb{F}_q$. Consider a randomly chosen E with $\Delta \not\equiv 0 \pmod{q}$.
  - **Mini-Example**: Let $X = 242 = 2 \cdot 121$, $A = 3$, $p_n = 5$, so $q = 243$. Choose $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_{243}$. Compute $\Delta = -16(4 \cdot 1^3 + 27 \cdot 1^2) = -496 \equiv 11 \pmod{243} \neq 0$, so E is smooth. Check if $X = 242$ is a valid x-coordinate:

    $$y^2 = 242^3 + 242 + 1 \pmod{243}.$$

    Since $242 \equiv -1 \pmod{243}$, we have:

    $$(-1)^3 + (-1) + 1 = -1 - 1 + 1 = -1 \equiv 242 \pmod{243}.$$

    Check if 242 is a quadratic residue modulo $243 = 3^5$. Since $242 \equiv 2 \pmod{3}$ and 2 is not a square modulo 3 (squares are $\{0, 1\}$), 242 is not a quadratic residue modulo 3, hence not modulo 243. Thus, $(242, y) \notin E(\mathbb{F}_{243})$, and $X = 242$ fails $\mathcal{F}_{\text{EC}}$.
  - **General Insight**: For composite X, the probability that $X^3 + aX + b$ is a quadratic residue for a random smooth E is roughly $1/2$ per curve. By testing multiple curves (e.g., $k \geq 3$), the likelihood of X passing $\mathcal{F}_{\text{EC}}$ decreases exponentially (approximately $(1/2)^k$).
- **Strengthening $\mathcal{F}_{\text{EC}}$**:
  - Assume X is prime. By the Hasse-Weil bound, $E(\mathbb{F}_q)$ has enough points to likely include X as an x-coordinate for some smooth E. For example, if $X = 97$, test over $\mathbb{F}_{243}$ with $E : y^2 = x^3 + x + 1$. Compute:

    $$97^3 + 97 + 1 \pmod{243}.$$

    If this is a quadratic residue, $97 \in E(\mathbb{F}_{243})$, satisfying $\mathcal{F}_{\text{EC}}$.
  - For composite X, the additional constraint from $\mathcal{F}_{\text{padic}}$ ($v_p(X) = 0$ for all $p \leq \sqrt{X}$) already eliminates composites. However, to ensure robustness, we require X to lie on multiple elliptic curves $E_1, E_2, \ldots, E_k$ over $\mathbb{F}_q$ for $k \geq 3$. This increases the selectivity of $\mathcal{F}_{\text{EC}}$, as the probability that a composite X satisfies all k curves diminishes exponentially.

Step 3: Numerical and Modular Filters Reinforcement The numerical approximation filter $\mathcal{F}_{\text{num}}$ ensures $X \sim A^{p_n}$, which restricts X to numbers close to exponential forms, while $\mathcal{F}_{\text{mod}}$ enforces $X \equiv 0 \pmod{M}$. These conditions alone are not sufficient to guarantee primality (e.g., $X = 242 \approx 3^5$ and $242 \equiv 0 \pmod{12}$), but they set up the necessary algebraic structure for $\mathcal{F}_{\text{padic}}$ and $\mathcal{F}_{\text{EC}}$ to eliminate composites.

Conclusion The p-adic unit condition $\mathcal{F}_{\text{padic}}$ provides the primary contradiction, as any composite X must have $v_p(X) \geq 1$ for some $p \leq \sqrt{X}$, violating $X \in \mathbb{Z}_p^\times$. The elliptic curve filter $\mathcal{F}_{\text{EC}}$ further restricts composites by requiring X to be a regular point on multiple smooth elliptic curves, which composites are less likely to satisfy consistently. Since $X \in \Gamma(\text{Spec}(\mathbb{Z}), \mathcal{F})$ implies X satisfies all filters, and composites fail at least $\mathcal{F}_{\text{padic}}$, we conclude X must be prime.

References

1. Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin. PRIMES is in P. *Ann. of Math.* (2) **160** (2004), no. 2, 781–793. doi:10.4007/annals.2004.160.781
2. Atkin, A. O. L.; Morain, François. Elliptic curves and primality proving. *Math. Comp.* **61** (1993), no. 203, 29–68. doi:10.2307/2152935
3. Baker, Alan. Transcendental number theory. Cambridge University Press, Cambridge, 1975. doi:10.1017/CBO9780511565977
4. Hartshorne, Robin. Algebraic geometry. Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977. doi:10.1007/978-1-4757-3849-0
5. Néron, André. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ. Math.* No. 21 (1964), 5–128. doi:10.1007/BF02684281
6. Silverman, Joseph H. The arithmetic of elliptic curves. Second edition, Graduate Texts in Mathematics, No. 106, Springer, Dordrecht, 2009. doi:10.1007/978-0-387-09494-6

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.