# A Complete Deterministic Prime Sieve Based on Integer Descartes Triples

Norman-Hendrik Michels

November 2025

## Contents

# 1 Foreword

This work presents a deterministic procedure which, starting from an arbitrary prime $p_1 > 3$, produces another prime number of the form

$$z = p_1^2 - 12\,n^2, \qquad z \equiv 1 \pmod{12}.$$

The method does not rely on factorization, primality testing, or probabilistic arguments. Instead, it combines algebraic constraints of the quadratic form $u^2 - 12v^2$, geometric properties of integer Descartes configurations, and structural conditions arising in the Eisenstein integer lattice.

A central result of this work is the soundness of the construction: every value $z$ admitted by all derived conditions is necessarily prime. This is established through a finite sequence of algebraic and modular filters, each of which excludes an explicitly characterized family of composite integers. Together, these filters eliminate all non-prime possibilities, so that the final output of the sieve consists solely of primes.

The derivation imposes no congruence assumptions on the input $p_1$; its primality is the only requirement. The evidence suggests that the only prerequisite for p is that it is not divisible by 2 or 3. In this paper, however, primality is assumed for the time being. For each such $p_1$, the sieve selects integer parameters $n$ arising from acceptable Descartes triples, resulting in candidates of the form $z = p_1^2 - 12n^2$. We compare these values with the full set of primes representable by the quadratic form, defined as

$$P_{\text{quad}}(p_1) := \big\{(v, z) \,\big|\, z = p_1^2 - 12v^2 \text{ is prime}\big\}.$$

Likewise, the Descartes-based construction yields the set

$$P_{\text{Desc}}(p_1) := \big\{(n, z) \,\big|\, (k_1, k_2, k_3) \text{ is a valid Descartes triple, } z = p_1^2 - 12n^2\big\}.$$

[Soundness Theorem] For every prime $p_1 > 3$,

$$P_{\text{Desc}}(p_1) \subseteq P_{\text{quad}}(p_1).$$

Extensive computations (up to $p_1 \leq 10^8$) indicate that this inclusion is, in fact, an equality:

$$|P_{\text{Desc}}(p_1)| = |P_{\text{quad}}(p_1)|$$

for all tested $p_1$, including all multiplicities arising from distinct representations of the same prime.

In the final part of the paper we analyze the inverse direction. Fixing a prime $z \equiv 1 \pmod{12}$, the solutions $(p_1, n)$ of

$$z = p_1^2 - 12n^2$$

lie on a Pell-type hyperbola in the real quadratic field $\mathbb{Q}(\sqrt{3})$. These inverse families admit a complete algebraic parametrization. Numerical experiments confirm that applying a set of filters in reverse recovers exactly those $(p_1, n)$ that the forward sieve accepts, providing further structural support for the framework developed here.

This publication develops the sieve systematically, provides rigorous proofs of its correctness, and illustrates its behaviour through examples and numerical experiments. The results should be viewed as a contribution to the structural understanding of primes arising from specific quadratic and geometric configurations.

## 2 Introduction

Prime numbers are fundamental objects in number theory, and understanding their structural properties has been a central mathematical goal for centuries. Classical sieves, such as the Sieve of Eratosthenes or the Atkin–Bernstein sieve, operate by systematically eliminating composite numbers. While effective, these methods rely purely on arithmetic exclusion rather than providing a structural description of primes.

This work presents a deterministic, geometrically motivated prime sieve that takes a fundamentally different perspective. The method begins with the observation that primes in the congruence class

$$p \equiv 1 \pmod{12}$$

exhibit special algebraic behaviour. Among all rational primes, those with

$$p \equiv 1 \pmod{3}$$

split in the Eisenstein integer ring $\mathbb{Z}[\omega]$. In this work we focus on the subfamily

$$p \equiv 1 \pmod{12},$$

for which these splitting properties interact with additional congruence conditions in a particularly rigid way. Such primes admit simultaneous representations

$$p = a^2 + b^2, \qquad p = d^2 - de + e^2,$$

linking them both to classical quadratic forms and to the geometry of the Eisenstein lattice.

The central idea of this project is to connect these representations with the Descartes equation

$$k_1^2 + k_2^2 + k_3^2 + k_4^2 = \frac{1}{2}(k_1 + k_2 + k_3 + k_4)^2,$$

which governs the curvatures of four mutually tangent circles. Under suitable modular side conditions, integer Descartes triples can be transformed into pairs $(u, v)$ giving rise to the associated quantity

$$z = u^2 - 12v^2.$$

Elementary algebra shows that this expression satisfies

$$z \equiv 1 \pmod{12}$$

whenever the underlying Descartes data are admissible.

A central outcome of the analysis is that every admissible value $z$ produced by this structure enjoys a remarkably constrained arithmetic profile:

1. $z$ is odd and coprime to 2 and 3;

2. $z$ has no prime divisors 5 or 7;

3. all remaining possible prime divisors must lie in the classes

$$p \equiv 1 \pmod{12} \quad \text{or} \quad p \equiv 11 \pmod{12};$$

4. should $z$ fail to be prime, then any admissible prime divisor may only occur with an odd exponent

$$k \in \{1, 3, 5, 7, \dots\}.$$

At this point, the geometric structure of Descartes triples becomes decisive. Every admissible value $z$ is associated with at least one canonical integer Descartes triple $(k_1, k_2, k_3)$, and—as shown later in this work—the number of such triples is controlled by the factorisation of $z$ in $\mathbb{Z}[\omega]$. A key structural fact is that squarefree integers $z$ with more than one rational prime factor $p \equiv 1 \pmod 3$ necessarily admit more than one canonical Descartes triple, whereas rational primes yield exactly one. This leads to a *triple filter* that eliminates precisely those candidates with multiple canonical Descartes triples. Crucially, this mechanism removes all composite candidates within the congruence class 1 mod 12 without any use of integer factorisation.

A second structural mechanism arises from the Eisenstein lattice itself. For an Eisenstein integer $d + e\omega$ with norm

$$z = N(d + e\omega) = d^2 - de + e^2,$$

any rational prime $q$ dividing $\gcd(d, e)$ appears in $z$ with exponent at least 2, because

$$d = qd', \quad e = qe' \quad \Longrightarrow \quad z = q^2 N(d' + e'\omega).$$

This applies to all primes

$$q \equiv 2 \pmod 3 \quad \Longleftrightarrow \quad q \equiv 11 \pmod{12}.$$

Imposing the lattice condition $\gcd(d, e) = 1$ removes such primes immediately, giving rise to a simple but powerful gcd-based lattice filter. Together, the triple filter and the gcd filter remove *all* composite values compatible with the modular constraints described above.

The resulting sieve is therefore *complete*: every surviving candidate is a genuine prime, and no explicit factorisation is ever required. Its construction relies solely on algebraic identities, modular reductions, and geometric properties of Descartes configurations.

This introduction sets the stage for the subsequent sections, where we develop:

- the algebraic structure of the form $z = u^2 - 12v^2$,
- the role of quadratic representations,

- modular analysis modulo 12,
- the geometric embedding via Descartes triples,
- and the full mathematical justification of the sieve.

The project thus yields a deterministic, geometrically and algebraically grounded method that isolates a structured subset of the primes in the class $1 \pmod{12}$. This subset forms the core of a complete prime sieve whose surviving elements are precisely the prime numbers themselves.

# 3 The Quadratic Form $z = u^2 - 12v^2$

The quadratic form

$$z = u^2 - 12v^2$$

is an indefinite rational form of discriminant 48. It is closely connected to the arithmetic of the real quadratic number field

$$\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(2\sqrt{3}),$$

and constitutes the natural algebraic starting point of our construction. Since

$$12 = 4 \cdot 3,$$

the form may be viewed as a scaled Pell-type form,

$$z = u^2 - (2\sqrt{3}\, v)^2.$$

The transformation group associated with this form is infinite cyclic and, for any starting point, generates an infinite orbit $(u_n, v_n)$ with values of $z$ of increasing absolute size. This dynamical structure explains the existence of infinitely many representations of both signs.

## 3.1 Residue Class Structure

A fundamental arithmetic feature arises from the quadratic residues modulo 12. For all integers $u, v$, we have

$$u^2 \equiv 0, 1 \pmod{12}, \qquad 12v^2 \equiv 0 \pmod{12},$$

thus

$$z = u^2 - 12v^2 \equiv 0 \text{ or } 1 \pmod{12}.$$

Therefore, values of this form that are candidates for primality can only occur in the residue class

$$z \equiv 1 \pmod{12}.$$

This observation ties the form directly to classical representations as sums of two squares and to norm forms in the Gaussian and Eisenstein integers.

## 3.2 Connection to Norm Representations

Prime numbers of the form $12k + 1$ admit the simultaneous representations

$$z = a^2 + b^2 \qquad \text{(Gaussian norm)},$$

$$z = d^2 - de + e^2 \qquad \text{(Eisenstein norm)}.$$

These two formulations are equivalent via a linear basis transformation between $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$. The quadratic form

$$u^2 - 12v^2$$

can be transformed into either representation through suitable linear mappings, thereby serving as an algebraic link between $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, and the Descartes triples introduced later.

## 3.3 Geometric Structure and Candidate Restriction

The quadratic form $z = u^2 - 12v^2$ defines a family of thin hyperbolic curves in the $(u, v)$-plane. For fixed $u$ or $v$, these curves restrict the admissible values of $z$ to a sparse and highly structured set. This geometric thinning does not explain primality by itself, but it dramatically reduces the ambient search space compared with unrestricted arithmetic progressions.

The relevance of this geometric structure is that it aligns naturally with the modular constraints that arise from Descartes triples and with the algebraic identities in $\mathbb{Z}[\omega]$. When these ingredients are combined in later sections — including residue conditions, gcd-filters, and the structure of canonical Descartes triples — the resulting sieve is able to isolate the remaining admissible values in a fully deterministic manner, without relying on probabilistic heuristics or density arguments.

## 3.4 Role of the Form in the Overall Framework

The form

$$z = u^2 - 12v^2$$

constitutes the arithmetic core of a broader geometric–algebraic framework. It connects:

- linear relations of the type $p_2 = p_1 + 4n$,
- the quadratic identity $z = p_1^2 - 12n^2$,
- norm representations $z = a^2 + b^2 = d^2 - de + e^2$,
- and the structure of Descartes triples.

Because of this central role, the form provides a unified perspective on the interaction between modular arithmetic, algebraic number fields, and geometric structures. It serves as the natural point of departure for deriving the prime-generating sieve developed in the subsequent chapters. In fact, at least in the range of numbers examined, the algorithm selects exactly all Pell-prime numbers in every possible combination. However, based on current knowledge, it cannot be said that this is always the case.

# 4 Modular structure of numbers congruent to $1 \pmod{12}$

We consider the quadratic form

$$z = u^2 - 12v^2, \qquad u, v \in \mathbb{Z}.$$

The behaviour of squares modulo 12 immediately restricts the residue classes of possible values of $z$. Since

$$u^2 \equiv 0, 1, 4, 9 \pmod{12}$$

for all integers $u$, and

$$12v^2 \equiv 0 \pmod{12},$$

every value of the form

$$z = u^2 - 12v^2$$

must satisfy

$$z \equiv u^2 \equiv 0, 1, 4, 9 \pmod{12}.$$

Only the residue classes

$$z \equiv 0, 1, 4, 9 \pmod{12}$$

are admissible at this purely quadratic level.

In the construction developed later in this work, we are interested in those values of $z$ which may be prime (or close to prime) and which satisfy additional compatibility conditions arising from geometric and algebraic structures introduced in subsequent sections. These constraints will ultimately force the restriction

$$z \equiv 1 \pmod{12}.$$

The other admissible residue classes $0, 4, 9 \pmod{12}$ are excluded step by step by further arithmetic and geometric conditions that do not belong to the quadratic form itself.

There is also an arithmetic perspective behind the distinguished role of the class $1 \pmod{12}$ at the level of prime factors. Consider the real quadratic field

$$\mathbb{Q}(\sqrt{3}),$$

whose discriminant is 12. For any odd prime $p \neq 3$, the splitting behaviour in this field is determined by its residue class modulo 12:

- $p$ splits in $\mathbb{Q}(\sqrt{3})$ if and only if $p \equiv 1$ or $11 \pmod{12}$,
- $p$ is inert if and only if $p \equiv 5$ or $7 \pmod{12}$,
- $p = 3$ is ramified.

From this point of view, primes in the classes 1 and 11 (mod 12) are precisely those that split in $\mathbb{Q}(\sqrt{3})$ and can therefore appear in norm factorizations associated with the quadratic form.

### 4.1 Excluded prime divisors under the condition $z \equiv 1 \pmod{12}$

Let $z \in \mathbb{Z}$ satisfy

$$z \equiv 1 \pmod{12}.$$

Then the only primes that cannot divide $z$ are

$$\boxed{2 \quad \text{and} \quad 3}.$$

In particular, every prime divisor $p$ of $z$ fulfills

$$p \geq 5 \qquad \text{and} \qquad \gcd(p, 12) = 1,$$

and no further prime classes are excluded by the congruence condition $z \equiv 1 \pmod{12}$.

## 5 Representation of $z$ as a sum of two squares

A central structural property of the values

$$z = u^2 - 12v^2$$

arising in this work is that all candidates which survive the full filtering process must be representable as a sum of two squares. This section collects the classical arithmetic conditions governing such representations and explains their relevance for the present construction.

### 5.1 Basic criterion

A positive integer $z$ admits a representation

$$z = a^2 + b^2, \qquad a, b \in \mathbb{Z},$$

if and only if every prime $p \equiv 3 \pmod{4}$ appears with even exponent in the prime factorisation of $z$. This is the classical theorem of Fermat–Euler on sums of two squares.

In particular, if $z$ is prime, then

$$z = a^2 + b^2 \qquad \Longleftrightarrow \qquad z \equiv 1 \pmod{4}.$$

## 5.2 Consequences for the values of $z$

From Section 4 we know that the quadratic form $u^2 - 12v^2$ can only take residue classes

$$z \equiv 0, 1, 4, 9 \pmod{12}.$$

Each of these corresponds to a residue class modulo 4, namely

$$0 \mapsto 0, \quad 1 \mapsto 1, \quad 4 \mapsto 0, \quad 9 \mapsto 1 \pmod{4}.$$

Thus every admissible value of the form $u^2 - 12v^2$ automatically satisfies

$$z \equiv 0 \text{ or } 1 \pmod{4}.$$

For primality candidates, only the class

$$z \equiv 1 \pmod{4}$$

is relevant, because primes congruent to 3 (mod 4) cannot be written as sums of two squares.

## 5.3 Compatibility with the later representation $z = d^2 - de + e^2$

A second representation,

$$z = d^2 - de + e^2,$$

appears later in this paper as a consequence of transformations derived from Descartes triples. The expression $d^2 - de + e^2$ is the norm form of the quadratic extension

$$\mathbb{Q}\left(e^{2\pi i/3}\right),$$

and it satisfies the classical identity

$$d^2 - de + e^2 = a^2 + b^2 \quad \text{if and only if} \quad d + e \equiv a + b \pmod{2}.$$

In particular, whenever $z$ is representable in the Eisenstein form $d^2 - de + e^2$ and is odd, it automatically satisfies

$$z \equiv 1 \pmod{4},$$

hence it is eligible to be written as a sum of two squares.

## 5.4 Summary of this section

For the values $z = u^2 - 12v^2$ relevant to this work:

- they lie only in the residue classes $0, 1, 4, 9 \pmod{12}$;
- the only residue class compatible with primality and a sum-of-two-squares representation is

$$z \equiv 1 \pmod{4};$$

- every prime divisor $p \equiv 3 \pmod 4$ is excluded by the classical Fermat–Euler theorem;
- the later Eisenstein representation $z = d^2 - de + e^2$ is fully compatible with this restriction.

Thus, the ability of a candidate $z$ to be expressed as a sum of two squares is not an optional feature but an intrinsic structural requirement for all values that survive the sieve developed in the subsequent chapters.

# 6 The Descartes equation

The Descartes equation describes the relationship between four pairwise tangent oriented circles. If

$$k_1,\ k_2,\ k_3,\ k_4$$

denote their curvatures (with signs encoding orientation), then they satisfy the classical algebraic constraint

$$(k_1 + k_2 + k_3 + k_4)^2 = 2\big(k_1^2 + k_2^2 + k_3^2 + k_4^2\big). \tag{1}$$

## 6.1 Solutions for the fourth curvature

For a fixed triple $(k_1, k_2, k_3)$, equation (1) is quadratic in $k_4$ and yields two solutions. The larger of the two,

$$k_4 = k_1 + k_2 + k_3 + 2\sqrt{k_1k_2 + k_1k_3 + k_2k_3}, \tag{2}$$

corresponds to the inner circle enclosed by the three others. It is convenient to introduce the symmetric quantity

$$\Delta(k_1, k_2, k_3) := k_1k_2 + k_1k_3 + k_2k_3. \tag{3}$$

In the setting of this work we restrict attention to those Descartes triples for which $\Delta(k_1, k_2, k_3)$ is a perfect square of the form

$$\Delta(k_1, k_2, k_3) = (2n)^2 \qquad \text{with } n \in \mathbb{Z}. \tag{4}$$

Equivalently,

$$\sqrt{\Delta(k_1, k_2, k_3)} = 2n.$$

With this convention we write

$$p_1 := k_1 + k_2 + k_3, \qquad p_2 := k_4,$$

so that the Descartes relation for the fourth curvature becomes

$$p_2 = p_1 + 2\sqrt{\Delta} = p_1 + 4n. \tag{5}$$

This is the form used later in the construction of the prime-generating sieve.

## 6.2 A second invariant: the symmetric quadratic form

Besides the term $\Delta$, the triple possesses a second symmetric invariant:

$$z = \frac{1}{2}\Big[(k_1 - k_2)^2 + (k_1 - k_3)^2 + (k_2 - k_3)^2\Big], \tag{6}$$

a quadratic form in the three parameters. Expanding the squares gives

$$(k_1 - k_2)^2 + (k_1 - k_3)^2 + (k_2 - k_3)^2 = 2\big(k_1^2 + k_2^2 + k_3^2 - k_1k_2 - k_1k_3 - k_2k_3\big), \tag{7}$$

and hence

$$z = k_1^2 + k_2^2 + k_3^2 - \Delta(k_1, k_2, k_3). \tag{8}$$

Introducing

$$p_1 := k_1 + k_2 + k_3, \qquad \Delta := \Delta(k_1, k_2, k_3),$$

we note that

$$p_1^2 = k_1^2 + k_2^2 + k_3^2 + 2\Delta,$$

so that

$$z = p_1^2 - 3\Delta. \tag{9}$$

Under the restriction $\Delta = (2n)^2 = 4n^2$ this becomes

$$z = p_1^2 - 3 \cdot 4n^2 = p_1^2 - 12n^2. \tag{10}$$

## 6.3 The algebraic structure $z = p_1^2 - 12n^2$

In summary, for every admissible Descartes triple $(k_1, k_2, k_3)$ with $\Delta(k_1, k_2, k_3) = 4n^2$ and

$$p_1 = k_1 + k_2 + k_3, \qquad p_2 = p_1 + 4n,$$

the associated symmetric invariant $z$ can be written in the Pell-type form

$$z = p_1^2 - 12n^2. \tag{11}$$

This identity is the precise bridge between the Descartes configuration and the quadratic form $u^2 - 12v^2$ used in the subsequent analysis: the variables $(p_1, n)$ play the role of $(u, v)$.

## 6.4 Conclusion

Thus, for every admissible Descartes triple considered in this work, the associated invariant $z$, constructed purely from the geometry of tangent circles, can be written in the form

$$z = u^2 - 12v^2,$$

a real binary quadratic form of discriminant 48. This identity provides a direct deterministic bridge between the geometry of Descartes triples and the arithmetic of the quadratic form $u^2 - 12v^2$. In subsequent sections we exploit this shared quadratic structure and its symmetries to analyse the arithmetic properties of $z$ and of its prime divisors.

## 6.5 Modular restrictions on integer Descartes triples

In this section we determine the admissible residue classes of integer Descartes triples

$$(k_1, k_2, k_3)$$

under the sole assumption that

$$p = k_1 + k_2 + k_3$$

is an odd prime, the result is remarkably restrictive: only two residue class types modulo 4 can occur.

## 6.6 Parity structure

Since $p$ is an odd prime, exactly two of the curvatures $k_i$ must be even and one must be odd. Modulo 4 this means

$$k_i \in \{0, 2\} \pmod 4, \qquad k_j \in \{1, 3\} \pmod 4.$$

This is the only possible parity pattern for integer Descartes triples in the present setting.

## 6.7 The modulo-4 constraint

Writing

$$k_i \equiv a_i \pmod 4, \qquad a_i \in \{0, 1, 2, 3\},$$

the Descartes configuration forces a finite system of congruences between the $a_i$. A short case analysis, using only the relation "exactly two $a_i$ even, one $a_i$ odd" together with the Descartes equation for the quadruple, shows that (up to permutation of indices) the only solutions modulo 4 are

$$(k_1, k_2, k_3) \equiv (0, 0, 1) \quad \text{or} \quad (k_1, k_2, k_3) \equiv (2, 2, 3) \pmod 4. \tag{12}$$

In particular, the residue class of $p = k_1 + k_2 + k_3 \pmod 4$ uniquely determines which of the two patterns occurs:

$$p \equiv 1 \pmod 4 \implies (k_1, k_2, k_3) \equiv (0, 0, 1) \pmod 4,$$
$$p \equiv 3 \pmod 4 \implies (k_1, k_2, k_3) \equiv (2, 2, 3) \pmod 4.$$

## 6.8 Mod-4 analysis of admissible Descartes triples

### Lemma

Let $(k_1, k_2, k_3)$ be an admissible integer Descartes triple of one of the two types

$$(k_1, k_2, k_3) \equiv (0, 0, 1) \quad \text{or} \quad (k_1, k_2, k_3) \equiv (2, 2, 3) \pmod 4,$$

and put

$$S = k_1k_2 + k_1k_3 + k_2k_3.$$

If $S$ is a perfect square, then

$$p_2 = p_1 + 2\sqrt{S} \quad \implies \quad p_2 \equiv p_1 \pmod 4.$$

### Proof

In both admissible residue classes one has $S \equiv 0 \pmod 4$. Since squares modulo 4 are 0 or 1, the assumption $\sqrt{S} \in \mathbb{N}$ forces $\sqrt{S} \equiv 0 \pmod 2$. Hence $\sqrt{S} = 2m$ for some integer $m$, and therefore

$$p_2 = p_1 + 2\sqrt{S} = p_1 + 4m \equiv p_1 \pmod 4.$$

□

The obstruction is purely arithmetic: for those $n$ with $4n^2 \notin R$, the quadratic form

$$Q(k_1, k_2, k_3) = k_1k_2 + k_1k_3 + k_2k_3$$

cannot represent $4n^2$ under the Descartes-enforced residue class restrictions (**??**), and hence no compatible curvature triple can exist.

## 7 Eisenstein Integers and the Norm Representation

The Eisenstein integers form the ring

$$\mathbb{Z}[\omega] = \{\, d + e\omega \mid d, e \in \mathbb{Z} \,\},$$

where

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$

is a primitive third root of unity satisfying $\omega^2 + \omega + 1 = 0$. The ring $\mathbb{Z}[\omega]$ is a Euclidean domain, and its arithmetic is governed by the multiplicative norm

$$N(d + e\omega) = d^2 - de + e^2,$$

a positive definite quadratic form that induces a lattice of hexagonal symmetry. Because the norm is multiplicative and never negative, it provides a natural generalization of the Gaussian norm $a^2 + b^2$ to the cubic extension $\mathbb{Q}(\omega)$.

A crucial observation for our context is the residue behaviour of Eisenstein norms. For all integers $d, e$ with not both even, the value

$$d^2 - de + e^2$$

lies in the residue class 1 (mod 12). Thus every nontrivial Eisenstein norm is automatically constrained to the same modular structure that governs the values of the quadratic form $u^2 - 12v^2$.

## 7.1 Connection to the quadratic form $z = u^2 - 12v^2$

The expression

$$z = u^2 - 12v^2$$

is directly equivalent to the Eisenstein norm via the substitution

$$u = d - \frac{e}{2}, \qquad v = \frac{e}{2}.$$

A short computation shows that this yields the exact identity

$$u^2 - 12v^2 = d^2 - de + e^2 = N(d + e\omega).$$

Thus every value produced by the real quadratic form is the norm of an Eisenstein integer, and conversely every Eisenstein norm can be written as a value of $u^2 - 12v^2$.

This identity embeds the real quadratic structure into the complex multiplication framework of $\mathbb{Q}(\omega)$. It also allows arithmetic statements over $\mathbb{Z}[\omega]$ — including gcd-conditions, prime decompositions, and residue constraints — to be transferred into statements about the real form $u^2 - 12v^2$.

## 7.2 Connection to Descartes triples

**Key identity.** For every integer Descartes triple $(k_1, k_2, k_3)$, introduce

$$d = k_1 - k_2, \qquad e = k_1 - k_3.$$

A direct computation shows

$$(k_1 - k_2)^2 + (k_1 - k_3)^2 + (k_2 - k_3)^2 = 2(d^2 - de + e^2),$$

and therefore

$$\boxed{z = d^2 - de + e^2.}$$

Thus the Descartes invariant $z$ admits two independent algebraic representations:

$$\boxed{z = d^2 - de + e^2} \qquad \text{and} \qquad \boxed{z = u^2 - 12v^2.}$$

Both arise directly and canonically from the same curvature triple $(k_1, k_2, k_3)$, but through different algebraic projections of the Descartes configuration. The key insight is that the geometry of integer Descartes triples simultaneously encodes:

$$\begin{array}{ccccc} \text{Descartes triple} & \longrightarrow & (d, e) & \longrightarrow & d^2 - de + e^2 \\ \Uparrow & & & & \Downarrow \\ \text{Descartes triple} & \longrightarrow & (u, v) & \longrightarrow & u^2 - 12v^2. \end{array}$$

### 7.3 Structural implications

Because Descartes triples, Eisenstein norms, and the quadratic form $u^2 - 12v^2$ all reduce to the same expression modulo 12, they necessarily occupy the same residue classes. This coincidence explains why numerical invariants derived from Descartes configurations obey the same modular laws as Eisenstein norms and why both structures appear jointly in the formulas that underpin our sieve.

Furthermore, the identification $z = N(d + e\omega)$ provides the foundation for the gcd-based filters in $\mathbb{Z}[\omega]$, the uniqueness criteria for Descartes triples, and the algebraic pruning rules that ultimately yield a *complete prime sieve*, that is, a sieve whose surviving elements are *exclusively* prime numbers.

## 8 Structural constraints on possible prime divisors

In the previous sections we derived the fundamental algebraic relations

$$p = k_1 + k_2 + k_3, \qquad S = k_1k_2 + k_1k_3 + k_2k_3 = 4n^2,$$

together with the induced expression

$$z = p^2 - 12n^2,$$

arising from any admissible integral Descartes triple. Before introducing additional layers of arithmetic filtering, it is natural to ask a more primitive question:

> *Which prime divisors can appear in the integers $z$ generated by the system itself, even before any external sieving is applied?*

This chapter answers this question in full generality. We show that several classes of prime divisors are already ruled out purely by the intrinsic structure of the Descartes–Pell relation. The exclusions proved here arise without any use of gcd-filters, uniqueness assumptions, or geometric normalisations—they are unavoidable consequences of the equations themselves.

For clarity of exposition we treat the cases in increasing subtlety.

### 8.1 Fundamental congruence constraints

We begin with the most elementary congruence restrictions.

**Parity.** Since $p = k_1 + k_2 + k_3$ is an odd prime $> 3$, we have

$$p^2 \equiv 1 \pmod 4.$$

As $12n^2 \equiv 0 \pmod 4$, it follows that

$$z = p^2 - 12n^2 \equiv 1 \pmod 4.$$

Thus $z$ is automatically odd, in particular

$$2 \nmid z.$$

**Modulo 3.** Because every prime $p > 3$ satisfies $p^2 \equiv 1 \pmod 3$, and since $12n^2 \equiv 0 \pmod 3$, we obtain

$$z \equiv 1 \pmod 3,$$

hence

$$3 \nmid z.$$

Both conclusions rely only on the Pell-type identity and hold for all admissible triples.

## 8.2 A deeper obstruction: the case of modulus 5

Assume for contradiction that $5 \mid z$. From

$$z = p^2 - 12n^2 \equiv 0 \pmod 5$$

we obtain

$$p^2 \equiv 12n^2 \equiv 2n^2 \pmod 5.$$

We distinguish two cases.

**Case 1: $5 \nmid n$.** Then $n$ is invertible modulo 5 and

$$\left(\frac{p}{n}\right)^2 \equiv 2 \pmod 5.$$

The quadratic residues modulo 5 are $\{0, 1, 4\}$, hence 2 is not a square. This case is impossible.

**Case 2: $5 \mid n$.** Write $n = 5n'$. Then from $5 \mid z$ we obtain $p^2 \equiv 0 \pmod 5$, hence $p = 5$.

Thus $p = k_1 + k_2 + k_3 = 5$. Using the identity

$$(k_1 + k_2 + k_3)^2 = k_1^2 + k_2^2 + k_3^2 + 2S,$$

we may express $S$ for fixed $p$ as

$$S = \frac{p^2 - \left(k_1^2 + k_2^2 + k_3^2\right)}{2}.$$

To bound $S$ from above for fixed $p$, it is convenient to eliminate $k_3$ via

$$k_3 = p - k_1 - k_2$$

and regard $S$ as a quadratic form in $k_1, k_2$. A straightforward computation yields

$$S(k_1, k_2) = -k_1^2 - k_1 k_2 - k_2^2 + p(k_1 + k_2).$$

The quadratic part $-k_1^2 - k_1k_2 - k_2^2$ is negative definite, hence $S(k_1, k_2)$ is a strictly concave quadratic function in $(k_1, k_2)$. Its unique real maximum is attained at

$$k_1 = k_2 = \frac{p}{3}, \qquad k_3 = \frac{p}{3},$$

with maximal value

$$S_{\max,\mathbb{R}} = \frac{p^2}{3}.$$

For $p = 5$ this gives

$$S \leq \left\lfloor \frac{5^2}{3} \right\rfloor = \left\lfloor \frac{25}{3} \right\rfloor = 8.$$

Since $S = 4n^2$, we have

$$4n^2 \leq 8 \quad \Rightarrow \quad n^2 \leq 2 \quad \Rightarrow \quad n \in \{-1, 0, 1\}.$$

Combined with $5 \mid n$, the only possible value is $n = 0$, which forces $S = 0$, the trivial (degenerate) case excluded in our construction (we assume $S = 4n^2 > 0$).

Hence the assumption $5 \mid z$ leads to a contradiction, and we obtain

$$5 \nmid z.$$

## 8.3 Another structural obstruction: modulus 7

Similarly, assume that $7 \mid z$. Then

$$p^2 - 12n^2 \equiv 0 \pmod 7 \quad \Rightarrow \quad p^2 \equiv 5n^2 \pmod 7,$$

since $12 \equiv 5 \pmod 7$.

**Case 1: $7 \nmid n$.** Then $n$ is invertible modulo 7 and

$$\left(\frac{p}{n}\right)^2 \equiv 5 \pmod 7.$$

The quadratic residues modulo 7 are $\{0, 1, 2, 4\}$; 5 is not among them. This case is impossible.

**Case 2: $7 \mid n$.** Set $n = 7n'$. Then $7 \mid z$ forces $p^2 \equiv 0 \pmod 7$, hence $p = 7$.

Thus $p = k_1 + k_2 + k_3 = 7$. As above, we express

$$S(k_1, k_2) = -k_1^2 - k_1k_2 - k_2^2 + p(k_1 + k_2),$$

with $k_3 = p - k_1 - k_2$. This concave quadratic form attains its real maximum at

$$k_1 = k_2 = \frac{p}{3}, \qquad k_3 = \frac{p}{3},$$

with value

$$S_{\max,\mathbb{R}} = \frac{p^2}{3}.$$

For $p = 7$ this yields

$$S \leq \left\lfloor \frac{7^2}{3} \right\rfloor = \left\lfloor \frac{49}{3} \right\rfloor = 16.$$

Since $S = 4n^2$, we obtain

$$4n^2 \leq 16 \quad \Rightarrow \quad n^2 \leq 4 \quad \Rightarrow \quad n \in \{-2, -1, 0, 1, 2\}.$$

Together with $7 \mid n$, we again obtain $n = 0$ and hence $S = 0$, the degenerate case.

Therefore

$$7 \nmid z.$$

## 8.4 Consolidated structural exclusion

Collecting the results of the previous sections, we obtain the following intrinsic restriction on the arithmetic of the system.

$$2 \nmid z, \qquad 3 \nmid z, \qquad 5 \nmid z, \qquad 7 \nmid z.$$

These exclusions arise purely from the combined relations

$$p = k_1 + k_2 + k_3 > 3, \qquad S = 4n^2 > 0, \qquad z = p^2 - 12n^2,$$

and therefore hold for every integer $z$ generated by an admissible Descartes configuration with $S = 4n^2$. No additional sieving or external assumptions are required.

## 8.5 Exclusion of residue classes for all divisors of $z$

In the previous subsections we established that every admissible integer

$$z = p^2 - 12n^2, \qquad p = k_1 + k_2 + k_3 > 3 \text{ prime}, \qquad S = k_1k_2 + k_1k_3 + k_2k_3 = 4n^2 > 0,$$

satisfies the intrinsic congruence restrictions

$$2 \nmid z, \qquad 3 \nmid z, \qquad 5 \nmid z, \qquad 7 \nmid z.$$

In this section we lift these statements from the level of *prime divisors* to the level of *all divisors* of $z$. The result is considerably stronger: not only are certain primes excluded as factors, but entire residue classes modulo 12 are impossible for any divisor of $z$.

**Prime factor restrictions.** Let $q$ be any prime divisor of $z$. From the results of the previous subsections, every such $q$ satisfies

$$q \geq 11, \qquad q \not\equiv 5 \pmod{12}, \qquad q \not\equiv 7 \pmod{12}.$$

Since every odd prime $q > 3$ belongs to one of the residue classes

$$q \equiv 1, 5, 7, 11 \pmod{12},$$

the only remaining possibilities are

$$q \equiv 1 \pmod{12} \qquad \text{or} \qquad q \equiv 11 \pmod{12}.$$

**Products of admissible prime factors.** Let $t \mid z$ be any positive divisor, and let

$$t = \prod_{i=1}^{r} q_i^{e_i}$$

be its prime factorisation. Since each prime $q_i$ lies in the set $\{1, 11\} \pmod{12}$, we analyse the modulo-12 behaviour of products of these residue classes.

We have the multiplication rules

$$1{\cdot}1 \equiv 1 \pmod{12}, \qquad 1{\cdot}11 \equiv 11 \pmod{12}, \qquad 11{\cdot}11 \equiv 121 \equiv 1 \pmod{12}.$$

By induction on the number of factors it follows that any product of elements of $\{1, 11\} \pmod{12}$ again lies in $\{1, 11\} \pmod{12}$. Therefore every divisor $t$ of $z$ satisfies

$$t \equiv 1 \pmod{12} \qquad \text{or} \qquad t \equiv 11 \pmod{12}.$$

**Conclusion.** No divisor of $z$ can lie in any of the residue classes

$$2, 3, 5, 7 \pmod{12}.$$

This restriction is inherited directly from the prime factor structure of $z$; no additional filtering or descent arguments are required.

| Every divisor $t \mid z$ satisfies $t \equiv 1 \pmod{12}$ or $t \equiv 11 \pmod{12}$. |
|---|

| In particular, no divisor of $z$ lies in $\{2, 3, 5, 7\} \pmod{12}$. |
|---|

# 9 The emergence of genuine arithmetic filters

In the preceding sections we have identified the intrinsic structural constraints imposed by the Descartes–Pell system. Most notably, we established that every admissible value

$$z = p^2 - 12n^2$$

generated under the conditions

$$p = k_1 + k_2 + k_3 > 3 \text{ prime}, \qquad S = 4n^2 > 0,$$

admits only divisors in the two residue classes

$$t \equiv 1 \pmod{12} \qquad \text{or} \qquad t \equiv 11 \pmod{12},$$

while the classes $2, 3, 5, 7 \pmod{12}$ are completely excluded by the intrinsic algebraic structure.

This leaves exactly two families of possible prime divisors of $z$:

$$\boxed{q \equiv 1 \pmod{12}} \qquad \text{and} \qquad \boxed{q \equiv 11 \pmod{12}}.$$

Up to this point, all restrictions followed directly from the intrinsic algebraic structure of the Descartes–Pell system: the parity pattern of admissible curvature triples, the quadratic identity

$$S = k_1k_2 + k_1k_3 + k_2k_3 = 4n^2,$$

and the Eisenstein representation

$$z = d^2 - de + e^2.$$

These constraints arise internally and require no additional sieving.

We now introduce explicit structural filters. They operate on the prime factorisation of the Eisenstein norm

$$z = N(a + b\omega),$$

and determine which integers $z$ correspond to genuine Descartes–Eisenstein solutions.

Two mechanisms are fundamental:

- the **triplet filter**, which counts the primitive Eisenstein norm representations of $z$ and removes all integers admitting more than one canonical Descartes triple,
- the **gcd filter** in $\mathbb{Z}[\omega]$, which eliminates all Eisenstein integers whose coordinates share a nontrivial divisor.

Together these filters isolate exactly those values of $z$ that remain compatible with both the Descartes geometry and the Eisenstein arithmetic structure.

## 9.1 The triplet filter and the distinction between split and inert primes

Let

$$z = \frac{(k_1 - k_2)^2 + (k_1 - k_3)^2 + (k_2 - k_3)^2}{2} = N(a + b\omega)$$

be an admissible candidate arising from a canonical Descartes configuration, and let

$$z = \prod_{i=1}^{r} p_i^{e_i} \prod_{j=1}^{s} q_j^{2f_j}$$

be its rational prime factorisation, where:

- each $p_i \equiv 1 \pmod 3$ is a split prime in $\mathbb{Z}[\omega]$, satisfying $(p_i) = \pi_i \overline{\pi_i}$;
- each $q_j \equiv 2 \pmod 3$ (equivalently $q_j \equiv 11 \pmod{12}$) is inert in $\mathbb{Z}[\omega]$, with $N(q_j) = q_j^2$.

Primitive Eisenstein norm representations correspond bijectively to canonical Descartes triples, so we determine their number.

**1. Split versus inert primes**

A primitive representation of $z$ has the form

$$\alpha = u \prod_{i=1}^{r} \pi_i^{\varepsilon_i} \, \overline{\pi_i}^{\,1-\varepsilon_i} \prod_{j=1}^{s} q_j^{f_j}, \qquad \varepsilon_i \in \{0,1\},$$

with $u$ a unit in $\mathbb{Z}[\omega]$. Thus:

- each split prime $p_i$ contributes one binary choice $\varepsilon_i \in \{0,1\}$;
- inert primes $q_j$ contribute no choices.

Conjugation sends $\varepsilon_i \mapsto 1 - \varepsilon_i$, pairing opposite choices. Hence the number of inequivalent primitive norm representations is

$$\#\{\text{primitive Eisenstein representations of } z\} = 2^{\,r_{\text{split}}-1}, \qquad r_{\text{split}} = \#\{p_i : p_i \equiv 1 \pmod 3\}.$$

Inert primes do not affect this number.

**2. Consequence for canonical Descartes triples**

Since primitive Eisenstein representations correspond to canonical Descartes triples,

$$\boxed{\#\{\text{canonical triples for } z\} = 2^{\,r_{\text{split}}-1}.}$$

Thus:

- if $r_{\text{split}} = 1$, exactly one canonical Descartes triple exists;
- if $r_{\text{split}} \geq 2$, at least two exist.

The triplet filter therefore retains exactly those integers with

$$r_{\text{split}} = 1.$$

**3. What the triplet filter actually removes**

The triplet filter removes precisely those integers $z$ containing two or more distinct split primes:

$$z = p_1^{e_1} p_2^{e_2} \cdots, \qquad p_i \equiv 1 \pmod 3,\ r_{\text{split}} \geq 2.$$

Inert primes do not influence the number of canonical triples. For example:

- $z = 13 \cdot 37$: two split primes; removed;
- $z = 11^2 \cdot 13$: one split prime and one inert prime; survives.

## The gcd filter in $\mathbb{Z}[\omega]$

Let $\omega^2 + \omega + 1 = 0$, and let

$$N(d + e\omega) = d^2 - de + e^2$$

be the Eisenstein norm. Each candidate arises as $z = d + e\omega$.

**1. The gcd filter**

The gcd filter removes all Eisenstein integers

$$z = d + e\omega \qquad \text{with} \qquad \gcd(d, e) > 1.$$

Only primitive pairs $(d, e)$ survive.

**2. Composite norms from a common divisor**

If $\gcd(d, e) > 1$, then $N(d + e\omega)$ is composite.

**Proof.** Write $d = gd'$, $e = ge'$ with $\gcd(d', e') = 1$. Then

$$d + e\omega = g(d' + e'\omega), \qquad N(d + e\omega) = g^2 N(d' + e'\omega).$$

Thus $N(d + e\omega)$ contains the rational square factor $g^2$ and is composite. □

**3. Inert primes necessarily force** $\gcd(d, e) > 1$

Let $q \equiv 2 \pmod 3$ be inert and suppose $q \mid N(d + e\omega)$. Then

$$d^2 - de + e^2 \equiv 0 \pmod q.$$

Over the field $\mathbb{F}_q$, the quadratic form

$$F(d, e) = d^2 - de + e^2$$

is anisotropic for all inert primes $q \equiv 2 \pmod 3$. Hence the only solution of $F(d, e) \equiv 0 \pmod q$ is

$$d \equiv 0, \qquad e \equiv 0 \pmod q.$$

Thus:

$$q \mid N(d + e\omega) \implies q \mid d \text{ and } q \mid e, \implies \gcd(d, e) \geq q > 1.$$

*Every inert prime dividing $N(z)$ forces a nontrivial common divisor of $d$ and $e$. Therefore, no inert prime can survive the gcd filter.*

**Conclusion**

After applying:

- the **triplet filter**, which removes all integers containing two or more split primes $p \equiv 1 \pmod 3$;
- the **gcd filter**, which removes every candidate with $\gcd(d, e) > 1$, and therefore eliminates all inert prime factors;

every surviving norm has the form

$$\boxed{N(z) = p^k, \qquad p \equiv 1 \pmod{12}, \;\; k \geq 1.}$$

Thus the combined filters reduce the entire search space to pure powers of a single split prime.

After the triplet and gcd filters, every surviving candidate has the form $N(z) = p^k$ with $p \equiv 1 \pmod{12}$ and $p \geq 13$. A perfect square test removes all even exponents, leaving only the odd powers $p^{2m+1}$. To eliminate the remaining composite exponents, one applies a general $n$-th–root test: since $p^k$ can only be an $n$-th power if $n \mid k$, and since $p \geq 13$ implies $k \leq \lfloor \ln(z)/\ln(13) \rfloor$, only finitely many odd values $n \leq k$ must be checked. This removes all higher perfect powers and leaves precisely the genuine odd prime powers $p^3, p^5, p^7, \ldots$.

**Exclusion of the unit value $z = 1$.** Although the expression $z = p_1^2 - 12n^2$ may take the value $z = 1$ for certain admissible pairs $(p_1, n)$, this case does not represent a prime. In the Eisenstein integer ring $\mathbb{Z}[\omega]$, the value 1 is the norm of the units $\{\pm 1, \pm\omega, \pm\omega^2\}$ and therefore corresponds to no non-trivial factorisation. Since all prime candidates in this work must satisfy $z > 1$, the unit case is excluded explicitly. All further filtering mechanisms apply only to $z \geq 13$, the smallest admissible value congruent to 1 (mod 12).

# 10 Global structure of the sieve as a two–dimensional surface

The preceding sections established the internal algebraic and geometric constraints of the Descartes–Pell system and showed that, after applying the triplet filter and the gcd filter in Z[] together with the perfect power tests, every surviving candidate is a genuine prime of the form

$$z = p^2 - 12n^2, \qquad p \equiv 1 \pmod{12}.$$

In this section we collect these results into a global structural picture. The prime sieve can be interpreted as operating on a two–dimensional algebraic surface in the integer lattice, with the primes appearing as the surviving points after all constraints are imposed.

## 10.1 Forward families for fixed seed primes

Throughout, let $p_1 > 3$ be an arbitrary rational prime. Recall from the foreword the sets

$$P_{\text{quad}}(p_1) := \big\{(v, z) \in \mathbb{N} \times \mathbb{N} : z = p_1^2 - 12v^2 \text{ and } z \text{ is prime}\big\},$$

and

$$P_{\text{Desc}}(p_1) := \big\{(n, z) \in \mathbb{N}\times\mathbb{N} : (k_1, k_2, k_3) \text{ is an admissible integer Descartes triple associated with } p_1,$$
$$S = k_1k_2+k_1k_3+k_2k_3 = 4n^2,\ z = p_1^2-12n^2 \text{ is prime}\big\}.$$

The soundness result proved earlier can be summarised as

$$P_{\text{Desc}}(p_1) \subseteq P_{\text{quad}}(p_1) \qquad \text{for every prime } p_1 > 3.$$

In words: for a fixed seed prime $p_1$, every pair $(n, z)$ produced by an admissible Descartes triple yields a prime $z$ lying on the quadratic curve

$$z_{p_1}(n) = p_1^2 - 12n^2, \qquad n \in \mathbb{N}.$$

Numerical experiments strongly support the conjectural reverse inclusion

$$P_{\text{Desc}}(p_1) = P_{\text{quad}}(p_1) \qquad \text{for all primes } p_1 > 3,$$

including all multiple representations of the same prime $z$. Under this completeness conjecture for fixed $p_1$, the sieve is exhaustively capturing all prime values of the form $p_1^2 - 12n^2$: no prime on the forward quadratic curve is missed.

For each prime $p_1 > 3$ we may therefore view the construction as acting on the discrete quadratic family

$$\Gamma_{p_1} := \big\{(n, z) \in \mathbb{N}^2 : z = p_1^2 - 12n^2\big\},$$

and the sieve selects exactly those lattice points on $\Gamma_{p_1}$ that satisfy all geometric and algebraic admissibility conditions and are prime.

## 10.2 Reverse families for fixed primes $z$

The same quadratic identity can be read in reverse. Fix a prime $z$ and consider integer solutions $(p_1, n)$ of

$$z = p_1^2 - 12n^2.$$

Whenever such a solution exists, the seed prime $p_1$ is recovered from

$$p_1(n) = \sqrt{z + 12n^2}.$$

Thus, for fixed $z$, the Diophantine relation defines a discrete family

$$\Lambda_z := \big\{(p_1, n) \in \mathbb{N}^2 : p_1 > 3 \text{ prime},\ z = p_1^2 - 12n^2\big\},$$

which can be viewed as a "reverse" curve in the $(p_1, n)$–plane. Each integral point on $\Lambda_z$ represents a seed prime $p_1$ that could generate $z$ through the quadratic form.

By construction, every prime $z$ that is produced by the sieve arises from at least one admissible pair $(p_1, n)$, hence lies on at least one such reverse family $\Lambda_z$. Multiple Descartes configurations associated with the same $z$ give rise to multiple points on $\Lambda_z$, reflecting the multiplicity structure discussed in the factorisation of $z$ in Z[].

## 10.3 The global $(p_1, n, z)$ surface

It is convenient to combine all forward and reverse families into a single global object. Define

$$\mathcal{F} := \big\{(p_1, n, z) \in \mathbb{N}^3 : p_1 > 3 \text{ prime},\ z = p_1^2 - 12n^2 \text{ is prime},$$
$$(k_1, k_2, k_3) \text{ is an admissible Descartes triple with } S = 4n^2\big\}.$$

Each fixed $p_1$ gives rise to a one–dimensional fibre

$$\mathcal{F}_{p_1} := \{(n, z) : (p_1, n, z) \in \mathcal{F}\} \subseteq \Gamma_{p_1},$$

and each fixed $z$ determines a fibre

$$\mathcal{F}^z := \{(p_1, n) : (p_1, n, z) \in \mathcal{F}\} \subseteq \Lambda_z.$$

From the soundness results it follows that every point of $\mathcal{F}$ encodes a genuine prime $z$ produced by the sieve from a seed prime $p_1$. Projecting onto the $z$–coordinate yields the set of all primes generated by the method,

$$\pi_z(\mathcal{F}) = \{z : \exists\, p_1, n \text{ with } (p_1, n, z) \in \mathcal{F}\},$$

while projection onto the $p_1$–coordinate simply returns the set of all seed primes used as input,

$$\pi_{p_1}(\mathcal{F}) = \{p_1 > 3 : p_1 \text{ prime}\}.$$

The set $\mathcal{F}$ may be viewed as a thin, arithmetically constrained subset of the quadratic surface

$$\Sigma := \{(p_1, n, z) \in \mathbb{Z}^3 : z = p_1^2 - 12n^2\},$$

with the Descartes, Eisenstein, and modular conditions cutting out precisely those lattice points corresponding to primes that survive all filters of the sieve.

## 10.4 Interpretation and conjectural completeness

The picture that emerges is the following.

- For each fixed seed prime $p_1 > 3$, the sieve explores the discrete quadratic family $z = p_1^2 - 12n^2$ and, under the completeness conjecture for $P_{\mathrm{Desc}}(p_1)$, selects exactly all prime values on this curve that are compatible with the Descartes configuration.
- For each prime $z$ produced by the method, the reverse relation $z = p_1^2 - 12n^2$ describes a family of potential seed primes $p_1$ lying on the reverse curves $\Lambda_z$. Each admissible solution corresponds to an underlying Descartes triple and an Eisenstein norm representation.
- The full sieve can thus be interpreted as operating on a two–dimensional family of curves in the $(p_1, n)$–plane, with the primes realised as the values of $z$ along these curves that survive all structural filters.

If, in addition to the completeness conjecture for fixed $p_1$, one assumes that every prime in the relevant residue classes admits at least one representation $z = p_1^2 - 12n^2$ compatible with an admissible Descartes triple, then the set $\mathcal{F}$ would provide a genuine two–dimensional parametrisation of the entire output of the sieve in terms of integer pairs $(p_1, n)$.

Even without this global completeness assumption, the description above shows that the sieve is not merely an exclusion process. It is naturally organised along a structured two–dimensional quadratic surface, on which the combined Descartes, Eisenstein, and modular constraints carve out a highly rigid subset whose projection to the $z$–axis consists exclusively of prime numbers.

## 10.5 Geometric consequences of the reverse parametrisation

The numerical analysis of the reverse families $\Lambda_z$ reveals a further global structural feature of the sieve. For every prime

$$z \equiv 1 \pmod{12},$$

the Diophantine relation

$$z = p_1^2 - 12n^2$$

forces any admissible seed prime $p_1$ to lie strictly above the square-root threshold

$$p_1 > \sqrt{z}.$$

Indeed, from $p_1^2 = z + 12n^2$ and $n \geq 1$ one obtains the sharp lower bound

$$p_1 \geq \sqrt{z+12},$$

with equality precisely in the extremal case $12n^2 = 12$. Thus every integral point on the reverse curve $\Lambda_z$ lies inside the open half-strip

$$\{(p_1, n) \in \mathbb{R}^2 : p_1 > \sqrt{z}\}.$$

Geometrically, each $\Lambda_z$ is therefore a discrete branch of a Pell-type hyperbola contained entirely above the barrier $p_1 = \sqrt{z}$. This has two notable consequences.

**(1) Visibility of small primes in the reverse fibres.** Although each reverse curve $\Lambda_z$ starts strictly above $\sqrt{z}$, the projection of all reverse fibres onto the $p_1$–axis,

$$\pi_{p_1}(\mathcal{F}) = \{p_1 > 3 : \exists\, n, z \text{ with } (p_1, n, z) \in \mathcal{F}\},$$

contains *all* rational primes $p_1 > 3$. This follows from the explicit solutions

$$z = p_1^2 - 12n^2$$

for small prime values of $z$. Already the initial sample

$$z \in \{13, 37, 61, 73, 97, 109, 157\}$$

produces seed primes

$$p_1 \in \{5, 7, 11, 13, 17, 19, 23, \dots\},$$

showing that the reverse curves naturally recover all smaller primes despite the global restriction $p_1 > \sqrt{z}$. In other words, the reverse parametrisation distributes the small primes across the family of curves $\{\Lambda_z\}$ in a manner entirely consistent with the quadratic identity.

**(2) Duality of forward and reverse fibres.** The forward fibres $\mathcal{F}_{p_1}$ lie on the downward–opening quadratic curves $\Gamma_{p_1}$, whereas the reverse fibres $\mathcal{F}^z$ lie on the hyperbolic curves $\Lambda_z$, confined to the region $p_1 > \sqrt{z}$. The global set $\mathcal{F}$ may thus be seen as the intersection pattern of two transverse one–parameter families of curves on the surface

$$\Sigma = \{(p_1, n, z) \in \mathbb{Z}^3 : z = p_1^2 - 12n^2\}.$$

The sieve selects exactly those intersection points of the two families that satisfy the Descartes and Eisenstein admissibility constraints and are prime in the $z$–coordinate.

Taken together, these observations show that the sieve operates not merely on a collection of quadratic sequences, but on a *geometrically rigid* two–dimensional web formed by the curves $\Gamma_{p_1}$ and $\Lambda_z$, whose intersection pattern is arithmetically sparse yet sufficiently rich to recover all seed primes $p_1 > 3$ and all output primes $z$ produced by the method.

**Theorem 1** (Geometric representation under the completeness assumption)
*Assume that the sieve is* complete *in the following sense:*

1. *For every rational prime $p_1 > 3$ there exists at least one integer $n \geq 1$ such that*
$$z = p_1^2 - 12n^2$$
*is prime and satisfies $z \equiv 1 \pmod{12}$.*

2. *Every prime $z \equiv 1 \pmod{12}$ that is representable in the form*
$$z = p^2 - 12n^2$$
*for some integers $(p, n)$ is realised by at least one forward fibre $\mathcal{F}_{p_1}$ of the sieve.*

*Then the following geometric description of the sieve holds.*

*[(i)]*

1. *The quadratic surface*
$$\Sigma = \{(p_1, n, z) \in \mathbb{Z}^3 : z = p_1^2 - 12n^2\}$$
*carries two transverse one–parameter families of curves:*

   - *the forward curves*
$$\Gamma_{p_1} = \{(p_1, n, z) : z = p_1^2 - 12n^2\},$$
*which project to downward–opening parabolas in the $(n, z)$–plane;*
   - *the reverse curves*
$$\Lambda_z = \{(p_1, n, z) : p_1^2 - 12n^2 = z\},$$
*which project to Pell-type hyperbolas in the $(p_1, n)$–plane and lie entirely in the half-strip $p_1 > \sqrt{z}$.*

2. *The global fibre set*

$$\mathcal{F} = \{(p_1, n, z) \in \Sigma : p_1 > 3,\ z \equiv 1 \pmod{12},\ z \in \mathbb{P}, \}$$

*(and all admissibility constraints are satisfied) is exactly the set of integral intersection points*

$$\mathcal{F} = \left( \bigcup_{p_1 > 3} \Gamma_{p_1} \right) \cap \left( \bigcup_{z \equiv 1 (12)} \Lambda_z \right).$$

3. *The projections of $\mathcal{F}$ onto the coordinate axes recover both sets of primes occurring in the sieve:*

$$\pi_{p_1}(\mathcal{F}) = \{\, p_1 > 3 : p_1 \text{ prime} \,\},$$

$$\pi_z(\mathcal{F}) = \{\, z \equiv 1 \pmod{12} : z \text{ prime and representable} \,\}.$$

*In particular, every prime $p_1 > 3$ occurs as the $p_1$–coordinate of some intersection point, and every admissible output prime $z$ occurs as the $z$–coordinate of such a point.*

*Hence, under the completeness assumption, the sieve operates on a two–dimensional arithmetic web whose nodes are precisely the integral intersection points of the families $\Gamma_{p_1}$ and $\Lambda_z$ on the surface $\Sigma$.*

# 11 The quadratic number field underlying the sieve

The central geometric relation of the sieve,

$$z = p^2 - 12n^2,$$

admits a natural interpretation as a norm equation in a quadratic number field. In this section we construct this field explicitly and show how its arithmetic explains the structural behaviour of the curves and surfaces introduced earlier.

## 11.1 The natural number field

Consider the quadratic extension

$$K = \mathbb{Q}(\sqrt{3}),$$

whose ring of integers is

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{3}].$$

Every element of $\mathcal{O}_K$ has the form

$$a + b\sqrt{3}, \qquad a, b \in \mathbb{Z}.$$

The field norm of an element $\alpha = a + b\sqrt{3}$ is

$$N(\alpha) = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2.$$

Setting $a = p$ and $b = 2n$ yields

$$N(p + 2n\sqrt{3}) = p^2 - 12n^2 = z.$$

Thus the defining surface

$$\mathcal{Q} = \{(p, n, z) \in \mathbb{R}^3 : z = p^2 - 12n^2\}$$

is exactly the norm surface associated with the one-parameter family of algebraic integers $\alpha_{p,n} = p + 2n\sqrt{3}$.

$$\boxed{z = p^2 - 12n^2 \quad \Longleftrightarrow \quad z = N_{K/\mathbb{Q}}(p + 2n\sqrt{3}).}$$

## 11.2 Prime decomposition in $\mathbb{Q}(\sqrt{3})$

Let $q$ be a rational prime. Its decomposition behaviour in $K$ is completely determined by the residue class of $q$ modulo 3:

- $q = 3$ is ramified,
$$(3) = \mathfrak{p}^2.$$
- $q \equiv 2 \pmod 3$ is inert in $K$: the ideal $(q)$ remains prime.
- $q \equiv 1 \pmod 3$ splits,
$$(q) = \mathfrak{p}\,\mathfrak{p}^{\sigma}.$$

All primes produced by the sieve satisfy $z \equiv 1 \pmod{12}$, hence

$$z \equiv 1 \pmod 3,$$

and therefore fall into the splitting case.

$$\boxed{\text{Every prime } z \equiv 1 \pmod{12} \text{ splits in } \mathbb{Q}(\sqrt{3}).}$$

This explains the observed multiplicity of representations of $z$ by the form $p^2 - 12n^2$: every split rational prime admits infinitely many algebraic factorizations in $K$.

## 11.3 Units and infinite families of representations

The unit group of $\mathcal{O}_K$ is

$$\mathcal{O}_K^\times = \{\pm(2+\sqrt{3})^k : k \in \mathbb{Z}\},$$

generated by the fundamental unit

$$\varepsilon = 2+\sqrt{3}, \qquad N(\varepsilon) = 1.$$

Thus

$$N(\alpha) = N(\alpha\varepsilon^k) \qquad \text{for all } k \in \mathbb{Z}.$$

Consequently, any prime $z$ which has one representation

$$z = p_0^2 - 12n_0^2 = N(p_0 + 2n_0\sqrt{3})$$

automatically has infinitely many representations

$$z = N\big((p_0 + 2n_0\sqrt{3})\varepsilon^k\big).$$

This is the algebraic explanation of the hyperbolic curves $C_z$ on the surface $\mathcal{Q}$ and of the multiple intersections observed in numerical experiments.

## 11.4 Geometric interpretation

Fixing $p$ corresponds to restricting the norm equation to the one-dimensional slice

$$\Gamma_p = \{(p,n,z) \in \mathcal{Q} : p = \text{constant}\},$$

which projects to the downward-opening parabola

$$z = p^2 - 12n^2$$

in the $(n,z)$-plane.

Fixing $z$ yields the curve

$$C_z = \{(p,n,z) \in \mathcal{Q} : z = \text{constant}\},$$

which projects to the Pell-type hyperbola

$$p^2 - 12n^2 = z$$

in the $(p,n)$-plane.

The set of "prime points" of the sieve is therefore

$$\mathcal{P} = \{(p,n,z) \in \mathcal{Q} : p \in \mathbb{P},\ z \in \mathbb{P},\ z \equiv 1 \pmod{12}\},$$

and consists precisely of the integer intersection points of the two orthogonal families $\{\Gamma_p\}$ and $\{C_z\}$.

### 11.5 Summary

The number field $K = \mathbb{Q}(\sqrt{3})$ provides a complete algebraic framework for the sieve:

- the surface $z = p^2 - 12n^2$ is the norm surface of $K$;
- primes $z \equiv 1 \pmod{12}$ split in $K$ and therefore admit infinitely many norm representations;
- the unit group of $K$ generates infinite orbits of such representations;
- the parabolic and hyperbolic curve families of the sieve are geometric shadows of ideal factorisations in $\mathcal{O}_K$.

This connection explains all structural features observed in the numerical analysis of the sieve and places the construction into a classical algebraic number theoretic context.

## 12 An inverse sieve on the hyperbolic curves $C_z$

In the previous sections we analysed the forward parametrisation

$$z = p^2 - 12n^2, \qquad p > 3 \text{ prime},$$

and established (numerically, and subject to explicit filtering conditions) a completeness property for the sieve acting along the parabolic families

$$\Gamma_p = \{(p, n, z) \in \mathcal{Q} : z = p^2 - 12n^2\}.$$

In this section we investigate the *inverse direction*: for a fixed prime

$$z \equiv 1 \pmod{12},$$

we study the structure of the hyperbolic curve

$$C_z := \{(p, n) \in \mathbb{Z}^2 : p^2 - 12n^2 = z\}$$

and show that, under the same completeness assumption used previously, the geometry of $C_z$ admits a natural two–stage sieve structure: a *local norm sieve* restricting integer points to two thin lattice strips, and a *global unit–orbit sieve* governing all integer solutions and their arithmetic periodicities.

### 12.1 Hyperbolic structure and reduction modulo $z$

Since $z \equiv 1 \pmod{12}$, in particular $z \equiv 1 \pmod{3}$. Hence the Legendre symbol $\left(\frac{3}{z}\right) = 1$, and there exists an integer $t$ satisfying

$$t^2 \equiv 3 \pmod{z}.$$

Via the norm identity in the quadratic field $\mathbb{Q}(\sqrt{3})$,

$$z = N(p + 2n\sqrt{3}) = p^2 - 12n^2,$$

and reduction modulo $z$, we obtain

$$p^2 \equiv 3(2n)^2 \pmod{z}.$$

The degenerate case $z \mid 2n$ cannot occur: inserting $2n = zk$ into the norm equation forces $p^2 = z(1+3zk^2)$, implying $z \mid p$, which contradicts $p > 3$ (prime) and $z \neq p$. Thus $2n$ is invertible modulo $z$, and the above congruence yields

$$\frac{p}{2n} \equiv \pm t \pmod{z} \qquad \Longleftrightarrow \qquad p \equiv \pm 2tn \pmod{z}.$$

Thus every integer point on the hyperbola $C_z$ with $p > 3$ prime must lie on one of the two arithmetic progressions

$$p \equiv 2tn \pmod{z}, \qquad p \equiv -2tn \pmod{z}.$$

These congruences act as a local sieve on $C_z$, restricting admissible integer points to two thin lattice strips of total density $2/z$.

## 12.2 Unit orbits and cyclic structure in $\mathbb{Q}(\sqrt{3})$

Let $\varepsilon = 2 + \sqrt{3}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{3})$, satisfying $N(\varepsilon) = 1$. If

$$z = p_0^2 - 12n_0^2 = N(p_0 + 2n_0\sqrt{3}),$$

then for every integer $k$ the elements

$$\alpha_k := (p_0 + 2n_0\sqrt{3})\,\varepsilon^k = p_k + 2n_k\sqrt{3}$$

again satisfy

$$N(\alpha_k) = z, \qquad p_k^2 - 12\,n_k^2 = z.$$

Writing

$$v_k = \begin{pmatrix} p_k \\ 2n_k \end{pmatrix}, \qquad M := \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix},$$

the identity $(p_{k+1}, 2n_{k+1}) = (2p_k + 6n_k,\, p_k + 2n_k)$ translates to

$$v_{k+1} = Mv_k, \qquad v_k = M^k v_0.$$

For any rational prime $q$, reduction modulo $q$ yields a linear dynamical system in the finite vector space $(\mathbb{F}_q)^2$,

$$\overline{v}_{k+1} = \overline{M}\,\overline{v}_k,$$

and therefore the sequence $\{\overline{v}_k\}$ is periodic. A prime $q$ divides $p_k$ if and only if $\overline{v}_k$ lies in the subspace $\{(0, y) : y \in \mathbb{F}_q\}$, and thus the indices $k$ at which

$q \mid p_k$ form a finite union of arithmetic progressions modulo the order of $\overline{M}$ in $\mathrm{GL}_2(\mathbb{F}_q)$.

Consequently every "disturbance prime" $q$ appearing in composite values of $p_k$ occurs in *predictable periodic cycles*, determined solely by the residue class of $v_0$ and the order of $\overline{\varepsilon}$ in the finite ring $\mathcal{O}_K/\mathfrak{q}$.

**Theorem 2** (Inverse sieve on the hyperbolic curves)
*Assume the empirical completeness property that every prime* $z \equiv 1 \pmod{12}$ *admits at least one representation*

$$z = p^2 - 12n^2, \qquad p > 3 \text{ prime},$$

*and that all integer solutions of this equation are detected by the unit–orbit structure in* $\mathbb{Q}(\sqrt{3})$. *Then the following statements hold.*

1. ***Local norm sieve.*** *Every integer point* $(p, n) \in C_z$ *with* $p > 3$ *prime satisfies*

$$p \equiv 2tn \pmod{z} \quad \text{or} \quad p \equiv -2tn \pmod{z},$$

*where* $t^2 \equiv 3 \pmod{z}$. *Thus all admissible points lie on two lattice strips of density* $2/z$.

2. ***Global unit–orbit sieve.*** *If* $(p_0, n_0)$ *is one solution of* $p^2 - 12n^2 = z$, *then all integer solutions are given by*

$$p_k + 2n_k\sqrt{3} = (p_0 + 2n_0\sqrt{3})\,\varepsilon^k, \qquad k \in \mathbb{Z}.$$

*Reduction modulo any prime* $q$ *yields a periodic linear orbit in*

*Proof.* We work in the quadratic number field

$$K = \mathbb{Q}(\sqrt{3}), \qquad \mathcal{O}_K = \mathbb{Z}[\sqrt{3}],$$

with norm

$$N(a + b\sqrt{3}) = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2.$$

For integers $p, n$ we have

$$N(p + 2n\sqrt{3}) = p^2 - 12n^2.$$

Throughout, let $z$ be a rational prime with $z \equiv 1 \pmod{12}$, and let

$$C_z = \{(p, n) \in \mathbb{Z}^2 : p^2 - 12n^2 = z\}$$

denote the corresponding Pell-type curve.

*(1) Local norm sieve.* Let $(p, n) \in C_z$ with $p > 3$ prime. Then

$$p^2 - 12n^2 = z \quad \Longrightarrow \quad p^2 - 3(2n)^2 \equiv 0 \pmod{z}.$$

Write $y = 2n$. Then

$$p^2 \equiv 3y^2 \pmod{z}.$$

First we exclude the degenerate case $z \mid y$. Suppose $z \mid y$, so $y = zk$ for some $k \in \mathbb{Z}$. Then

$$z = p^2 - 3y^2 = p^2 - 3z^2k^2 = z\big(1 + 3zk^2\big),$$

hence

$$p^2 = z\big(1 + 3zk^2\big).$$

Since $z$ is prime, this forces $z \mid p$, say $p = zm$. Then

$$z^2m^2 = z\big(1 + 3zk^2\big) \quad \Longrightarrow \quad zm^2 = 1 + 3zk^2.$$

Reducing modulo $z$ gives $0 \equiv 1 \pmod{z}$, a contradiction. Thus $z \nmid y$, so $y$ is invertible in $\mathbb{F}_z = \mathbb{Z}/z\mathbb{Z}$.

Because $z \equiv 1 \pmod{12}$, in particular $z \equiv 1 \pmod{3}$, so 3 is a quadratic residue modulo $z$: there exists $t \in \mathbb{Z}$ such that

$$t^2 \equiv 3 \pmod{z}.$$

Now in $\mathbb{F}_z$ we have

$$\left(\frac{p}{y}\right)^2 \equiv \frac{p^2}{y^2} \equiv 3 \equiv t^2 \pmod{z}.$$

Hence

$$\frac{p}{y} \equiv \pm t \pmod{z},$$

and therefore

$$p \equiv \pm ty \equiv \pm 2tn \pmod{z}.$$

This proves the asserted congruence

$$p \equiv 2tn \pmod{z} \quad \text{or} \quad p \equiv -2tn \pmod{z}.$$

For each fixed $n$, the residue class of $p$ modulo $z$ is thus constrained to one of two values. Since there are $z$ possible residue classes in total, the admissible points lie on two lattice strips of relative density $2/z$ in $\mathbb{Z}^2$.

*(2) Global unit–orbit sieve.* Let $(p_0, n_0) \in C_z$ be any fixed integer solution, and set

$$\alpha_0 = p_0 + 2n_0\sqrt{3} \in \mathcal{O}_K.$$

Then by construction

$$N(\alpha_0) = p_0^2 - 12n_0^2 = z.$$

Let $(p, n) \in C_z$ be any other integer solution and define

$$\alpha = p + 2n\sqrt{3} \in \mathcal{O}_K.$$

Again $N(\alpha) = z$, hence

$$N\left(\frac{\alpha}{\alpha_0}\right) = \frac{N(\alpha)}{N(\alpha_0)} = 1.$$

On the ideal-theoretic level, both $(\alpha)$ and $(\alpha_0)$ are prime ideals lying above the rational prime $z$ (or their conjugates), since $N(\alpha) = N(\alpha_0) = z$ is prime in $\mathbb{Z}$. It follows that $(\alpha) = (\alpha_0)$ as ideals, and hence $\alpha/\alpha_0 \in \mathcal{O}_K^\times$. Thus

$$\beta := \frac{\alpha}{\alpha_0} \in \mathcal{O}_K^\times \quad \text{with} \quad N(\beta) = 1.$$

The unit group of the real quadratic field $K = \mathbb{Q}(\sqrt{3})$ is well known to be of the form

$$\mathcal{O}_K^\times = \{\pm\varepsilon^k : k \in \mathbb{Z}\},$$

where $\varepsilon = 2 + \sqrt{3}$ is a fundamental unit satisfying $N(\varepsilon) = 1$. Thus there exists an integer $k$ and a sign $\delta \in \{\pm 1\}$ such that

$$\beta = \delta\, \varepsilon^k.$$

Consequently

$$\alpha = \alpha_0\, \beta = \delta\, \alpha_0\, \varepsilon^k.$$

Writing

$$\varepsilon^k = u_k + v_k\sqrt{3}, \qquad u_k, v_k \in \mathbb{Z},$$

we obtain

$$\alpha_0\varepsilon^k = (p_0 + 2n_0\sqrt{3})(u_k + v_k\sqrt{3}) = (p_0u_k + 6n_0v_k) + (p_0v_k + 2n_0u_k)\sqrt{3}.$$

Hence every solution $(p, n) \in C_z$ is of the form

$$p + 2n\sqrt{3} = \delta\,(p_0 + 2n_0\sqrt{3})\,\varepsilon^k \qquad \text{for some } \delta \in \{\pm 1\},\ k \in \mathbb{Z}.$$

Absorbing the sign into the exponent (or into the choice of initial solution) gives the stated representation

$$p_k + 2n_k\sqrt{3} = (p_0 + 2n_0\sqrt{3})\,\varepsilon^k, \qquad k \in \mathbb{Z}.$$

Finally, consider reduction modulo a rational prime $q$. The image of $\mathcal{O}_K$ in the quotient ring $\mathcal{O}_K/q\mathcal{O}_K$ is finite; in particular, the unit group $(\mathcal{O}_K/q\mathcal{O}_K)^\times$ is finite. Let $\overline{\varepsilon}$ and $\overline{\alpha}_0$ denote the images of $\varepsilon$ and $\alpha_0$ modulo $q$. Then

$$\overline{\alpha}_k := \overline{\alpha}_0\, \overline{\varepsilon}^{\,k}$$

is a sequence in a finite set, so the orbit $\{\overline{\alpha}_k : k \in \mathbb{Z}\}$ is periodic in $k$. Writing $\overline{\alpha}_k = \overline{p}_k + 2\overline{n}_k\sqrt{3}$, this yields a periodic linear orbit for the pairs $(\overline{p}_k, \overline{n}_k)$ in the corresponding finite $\mathbb{F}_q$-vector space (equivalently, via the matrix representation, in $(\mathbb{Z}/q\mathbb{Z})^2$). This is the claimed global unit–orbit sieve structure modulo $q$. $\square$

## 12.3 Disturbance primes and local admissibility

For a fixed prime $z \equiv 1 \pmod{12}$ and the associated hyperbola

$$C_z = \{(p, n) \in \mathbb{Z}^2 : p^2 - 12n^2 = z\},$$

we call a rational prime $q \neq 2, 3, z$ a *disturbance prime* for $z$ if there exists an integer solution $(p, n) \in C_z$ such that $q \mid p$. The following lemma characterises disturbance primes by a purely local quadratic–residue condition.

[Local admissibility of disturbance primes] Let $z \equiv 1 \pmod{12}$ be prime and $q \neq 2, 3, z$ a rational prime. If there exists an integer solution

$$p^2 - 12n^2 = z$$

with $q \mid p$, then the congruence

$$n^2 \equiv -z \cdot 12^{-1} \pmod{q}$$

is solvable, and in particular

$$\left(\frac{-3z}{q}\right) = 1.$$

Conversely, if

$$\left(\frac{-3z}{q}\right) = -1,$$

then no integer solution $(p, n)$ of $p^2 - 12n^2 = z$ can satisfy $q \mid p$; in this case $q$ is locally excluded as a disturbance prime.

*Proof.* Suppose first that $p^2 - 12n^2 = z$ with $q \mid p$. Reducing modulo $q$ yields

$$0 - 12n^2 \equiv z \pmod{q} \qquad \Longrightarrow \qquad n^2 \equiv -z \cdot 12^{-1} \pmod{q},$$

where $12^{-1}$ denotes the multiplicative inverse of 12 modulo $q$, which exists since $q \neq 2, 3$. Thus $-z \cdot 12^{-1}$ is a quadratic residue modulo $q$. Because $12 = 4 \cdot 3$ and 4 is a square modulo $q$, this is equivalent to

$$\left(\frac{-3z}{q}\right) = 1.$$

Conversely, if $\left(\frac{-3z}{q}\right) = -1$, then $-z \cdot 12^{-1}$ is not a quadratic residue modulo $q$, so the congruence $n^2 \equiv -z \cdot 12^{-1} \pmod{q}$ has no solution. In particular, there can be no integers $n$ and $p$ with $q \mid p$ and $p^2 - 12n^2 = z$. □

Lemma 12.3 provides a necessary local condition for a prime $q$ to divide some $p$ on the hyperbola $C_z$. In our numerical experiments, for fixed $z$ all disturbance primes observed in composite values of $p$ satisfy $\left(\frac{-3z}{q}\right) = 1$, and no prime with $\left(\frac{-3z}{q}\right) = -1$ appears as a divisor of any $p$ on $C_z$.

Combining this local admissibility with the unit–orbit structure from the previous subsection yields a cyclicity statement for disturbance primes.

[Cyclic occurrence of disturbance primes] Let $z \equiv 1 \pmod{12}$ be prime and assume the orbit description

$$p_k + 2n_k\sqrt{3} = (p_0 + 2n_0\sqrt{3})\,\varepsilon^k, \qquad k \in \mathbb{Z},$$

with $\varepsilon = 2 + \sqrt{3}$ as above. Let $q \neq 2, 3, z$ be a rational prime such that $\left(\frac{-3z}{q}\right) = 1$. Then the sequence of residue classes $p_k \pmod{q}$ is periodic, and the set of indices

$$S_q := \{\, k \in \mathbb{Z} : q \mid p_k \,\}$$

is a finite union of arithmetic progressions

$$S_q = \bigcup_j \{\, k \equiv k_j \pmod{T_q} \,\},$$

where $T_q$ is the order of the matrix $M = \left(\begin{smallmatrix} 2 & 3 \\ 1 & 2 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{F}_q)$. Thus every locally admissible disturbance prime $q$ appears, if at all, in predictable periodic cycles along the unit orbit.

*Proof.* By the discussion in the previous subsection we have

$$v_k = \begin{pmatrix} p_k \\ 2n_k \end{pmatrix} = M^k v_0, \qquad M = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}.$$

Reducing modulo $q$ gives a linear recurrence in the finite vector space $(\mathbb{F}_q)^2$,

$$\overline{v}_{k+1} = \overline{M}\,\overline{v}_k,$$

so the sequence $\{\overline{v}_k\}$ is periodic with some period $T_q$, equal to the order of $\overline{M}$ in $\mathrm{GL}_2(\mathbb{F}_q)$. The condition $q \mid p_k$ is equivalent to $\overline{v}_k$ lying in the one–dimensional subspace $\{(0, y) : y \in \mathbb{F}_q\} \subset (\mathbb{F}_q)^2$. Since $\{\overline{v}_k\}$ is periodic, the set of indices for which this happens is a finite union of residue classes modulo $T_q$, as claimed. □

**Example 1** (Example: Disturbance primes for the case $z = 157$)
*We illustrate Lemma 12.3 and Corollary 12.3 in the concrete case*

$$z = 157 \equiv 1 \pmod{12}.$$

*The norm equation*

$$p^2 - 12n^2 = 157$$

*admits the integer solutions*

$$(p, n) \in \left\{ \begin{matrix} (13, 1),\ (67, 19),\ (115, 33),\ (925, 267),\ (1597, 461), \\ (12883, 3719),\ (22243, 6421),\ (179437, 51799), \\ (309805, 89433),\ (2499235, 721467) \end{matrix} \right\}.$$

*Among these, the values*

$$13,\ 67,\ 1597,\ 179437$$

*are prime, while the composite solutions factor as*

$$115 = 5 \cdot 23, \quad 925 = 5^2 \cdot 37, \quad 12883 = 13 \cdot 991, \quad 22243 = 13 \cdot 29 \cdot 59,$$

$$309805 = 5 \cdot 61961, \quad 2499235 = 5 \cdot 191 \cdot 2617.$$

*Thus every composite $p$ on $C_{157}$ is divisible by*

$$q \in \{5, 13\}.$$

*We now verify that both $q = 5$ and $q = 13$ are locally admissible disturbance primes in the sense of Lemma 12.3. Since*

$$-3z = -3 \cdot 157 = -471,$$

*we have*

$$-471 \equiv 4 \pmod 5, \qquad \left(\frac{4}{5}\right) = 1,$$

*and*

$$-471 \equiv -3 \equiv 10 \pmod{13}, \qquad 10 \equiv 3^2 \pmod{13}, \qquad \left(\frac{10}{13}\right) = 1.$$

*Therefore*

$$\left(\frac{-3 \cdot 157}{5}\right) = 1, \qquad \left(\frac{-3 \cdot 157}{13}\right) = 1,$$

*so both 5 and 13 pass the local quadratic–residue test and are not excluded as disturbance primes for $z = 157$.*

*Conversely, for many other small primes $q$ one checks that $\left(\frac{-3 \cdot 157}{q}\right) = -1$, so these $q$ are locally forbidden and indeed do not occur as divisors of any $p$ on $C_{157}$ in the above solution set.*

*Finally, once a disturbance prime $q$ occurs in one solution, the unit orbit*

$$p_k + 2n_k\sqrt{3} = (p_0 + 2n_0\sqrt{3})\,\varepsilon^k, \qquad \varepsilon = 2 + \sqrt{3},$$

*together with Corollary 12.3 implies that $q \mid p_k$ recurs in predictable arithmetic progressions of the index $k$, reflecting the cyclic behaviour of the matrix $M$ modulo $q$. This explains observed phenomenon that, for $z = 157$, the primes 5 and 13 appear repeatedly as "genetic" disturbance factors in composite values of $p_k$.*

## 12.4 Forward and inverse completeness

The structural theory requires the following two completeness properties. The first concerns the *forward direction*: starting from a prime $p$, one acts by the quadratic form $p^2-12n^2$ and obtains a prime $z$. The second concerns the *inverse direction*: starting from a prime $z$, one must be able to recover at least one pair $(p, n)$ that satisfies the same quadratic relation.

**Theorem 3** (Bidirectional completeness of the sieve)
*Consider the quadratic relation*

$$z = p^2 - 12n^2, \qquad p > 3,$$

*where* $z \equiv 1 \pmod{12}$ *is prime and where* $n$ *is constrained to arise from a valid Descartes triple* $(k_1, k_2, k_3)$ *via*

$$n = \sqrt{k_1k_2 + k_1k_3 + k_2k_3}.$$

*Assume that the modulo-4 and curvature restrictions for Descartes triples hold as established earlier.*

*The sieve is said to be* bidirectionally complete *if the following conditions are satisfied:*

- ***Forward completeness****: For every prime* $p \equiv 1 \pmod{12}$ *there exists an admissible Descartes value* $n \neq 0$ *such that* $z = p^2 - 12n^2$ *is prime.*
- ***Inverse completeness****: For every prime* $z \equiv 1 \pmod{12}$ *there exists at least one integer solution* $(p, n)$ *of* $p^2 - 12n^2 = z$ *with* $p > 3$ *and* $n$ *admissible.*
- ***Orbit uniqueness****: Every integer solution* $(p, n)$ *of* $p^2 - 12n^2 = z$ *with admissible* $n$ *belongs to exactly one inverse orbit generated by multiplication with the unit*

$$\varepsilon = 2 + \sqrt{3}.$$

***Conclusion.*** *Under these assumptions, forward and inverse completeness coincide, and the entire prime set in the residue class* $p \equiv 1 \pmod{12}$ *is represented bijectively by the integer points of the inverse orbits. Moreover, along each orbit the eigenvector alignment*

$$\frac{p_k}{n_k} \longrightarrow 2\sqrt{3}$$

*holds, and for sufficiently large primes the parameter* $n$ *is uniquely determined by the projection*

$$n = \operatorname{round}\left(\frac{p}{2\sqrt{3}}\right).$$

### 12.5 Consequences for the global sieve structure

Combining forward completeness, inverse completeness, and the eigenvector alignment yields a fully bidirectional prime correspondence:

$$p \longleftrightarrow (p, n) \longleftrightarrow z.$$

Every prime $p \equiv 1 \pmod{12}$ generates at least one prime $z$, every such $z$ admits at least one preimage $(p, n)$, and every solution belongs to a unique orbit governed by $\varepsilon$. Hence the entire prime set in this residue class is captured within a single geometric framework.

## Software implementation and reproducibility

All algorithms developed in this work were implemented in C# and are publicly available in three dedicated repositories. The code is intentionally minimalistic, reflecting the algebraic structure of the sieve rather than relying on external number–theoretic libraries. Each repository corresponds to one conceptual component of the theory:

- **Inverse Hyperbolic Sieve** (https://github.com/nhmichelsPrimes/inverse-hyberbolic-sieve) implements the inverse mapping $(p, n) \mapsto z = p^2 - 12n^2$ and the local norm sieve $p \equiv \pm 2tn \pmod{z}$, together with the disturbance–prime filtration. It generates the global surface $\mathcal{F}$, on which the completeness conjectures are formulated.
- **Descartes Prime Sieve** (https://github.com/nhmichelsPrimes/Descartes-Prime-Sieve) implements the forward direction $p_1 \mapsto z$ via integer Descartes triples, Eisenstein norm conditions and the perfect–power exclusion in $\mathbb{Z}[\omega]$. This module provides the geometric reduction that isolates all candidates $z \equiv 1 \pmod{12}$ compatible with the Descartes constraints.

Together, these three modules provide a fully reproducible computational framework for all numerical claims made in this paper. They also offer a reference implementation for further exploration of the Descartes–based prime sieve presented here.

## 13 Concluding Remarks

The starting point of this work was an observation that appeared, at first sight, purely numerical. For a given prime $p_1$, the admissible Descartes triples $(k_1, k_2, k_3)$ define a finite domain of feasible values, and at the upper boundary of this domain one frequently encounters another prime number. This value, denoted $p_2$, satisfies the relation

$$p_2 = p_1 + 4n,$$

where $n$ is determined by the curvature term $n = \sqrt{k_1k_2 + k_1k_3 + k_2k_3}$. Empirically, the ratio $p_2/p_1$ was observed to cluster around the value

$$1 + \frac{2}{\sqrt{3}},$$

and to converge towards this quantity as $p_1$ increases.

At that stage, the significance of this phenomenon was unclear. The value $p_2$ seemed to stand out among the admissible candidates, yet no direct structural interpretation was available. Only the later analysis revealed that this behaviour is a consequence of a deeper geometric framework linking Descartes triples, Eisenstein norms, and the quadratic form

$$z = p_1^2 - 12n^2.$$

Within this framework, the quantity $p_2$ turns out not to play a central role. It represents the point where the linear boundary of the admissible Descartes region meets the quadratic curve defined by $z = p_1^2 - 12n^2$. Its frequent primality and its apparent regularity stem from the fact that the pairs $(p_1, n)$ associated with primes $z$ lie asymptotically on the universal direction

$$(p, n) \parallel (2\sqrt{3}, 1),$$

which governs the orbits of the transformation induced by the unit $\varepsilon^2 = 7+4\sqrt{3}$ in the underlying Pell-type equation. The value of $p_2$ is therefore a visible trace of this alignment: it arises exactly at the intersection of the Descartes boundary with the geometric direction that all admissible pairs $(p, n)$ acquire in the limit.

For the overall theory, the quantity $p_2$ has no independent significance. However, its behaviour served as a first indication of an underlying structural rigidity, eventually leading to the full formulation of the sieve and to the universal linear asymptotics of the inverse parametrisation.

---

**Author contact:** `mail@nhmichels.de`