Diophantine Rank and Duality Types: From Curves to Local Systems

V.V. Tishkov

June 29, 2026

Аннотация

We introduce the notion of diophantine rank of an affine algebraic variety — the rank of the free abelian group generated by differences of integral points. We prove a complete classification of diophantine rank for absolutely irreducible curves of genus 0 over $\mathbb{Q}$. For curves of genus 0, the rank equals 2 if and only if the set of integral points contains three non-collinear points; it equals 1 if and only if there are at least two integral points and all are collinear; it equals 0 otherwise. For elliptic curves, we establish the same trichotomy and show that the Mordell–Weil rank and the diophantine rank are independent invariants, providing explicit counterexamples. We then introduce duality types — a new class of mathematical structures connecting the arithmetic of integral points with the topology of local systems. We prove the Rank Universality Theorem for curves of genus 0: the diophantine rank equals the rank of the cohomology of the monodromy local system around integral points. For higher genus, we formulate this as a conjecture with strong supporting evidence. This provides a unified language for studying diophantine equations and opens new connections to the geometric Langlands program.

1 Introduction

The classical problem in the theory of Diophantine equations is the description of the set of integral solutions of an equation $F(x, y) = 0$ with $F \in \mathbb{Z}[x, y]$. For curves of genus $g \geq 1$, Siegel's theorem (1929) [1] asserts the finiteness of the set of integral points. For genus $g = 0$, the set of integral points may be finite or infinite, and its structure is of particular interest.

In the present work, we introduce a new algebraic invariant — the diophantine rank — which measures the dimension of the affine span of the set of integral points. We prove a complete classification of this invariant for curves of genus 0 and provide a corrected classification for genus 1, clarifying the relationship with the Mordell–Weil rank.

We then generalize this construction to duality types — a new class of mathematical structures at the intersection of arithmetic geometry and algebraic topology.

Duality types naturally fit into a broader context. Katz's work on rigid local systems [3] shows that local systems on $\mathbb{P}^1$ with punctures are completely determined by their monodromy. The Rank Universality Theorem provides an arithmetic interpretation of such systems: the monodromy around integral points encodes the diophantine rank. Moreover, recent work of Whang [4] on the arithmetic of curves on moduli of local systems shows that integral points on such curves can be effectively determined, consistent with our construction.

2 Diophantine Rank: Definitions and Basic Properties

2.1 The Set of Integral Points and the Difference Group

Definition 2.1 (Set of integral points)**.** Let $F(x, y) \in \mathbb{Z}[x, y]$. We define

$$S_F = \{(a, b) \in \mathbb{Z}^2 \mid F(a, b) = 0\}.$$

Definition 2.2 (Difference group)**.**

$$G_F = \langle p - q \mid p, q \in S_F \rangle_{\mathbb{Z}} \subseteq \mathbb{Z}^2,$$

where $\langle \cdot \rangle_{\mathbb{Z}}$ denotes the integral linear span (generated subgroup).

If $S_F = \emptyset$, we set $\langle \varnothing \rangle_{\mathbb{Z}} = \{0\}$. The group G_F is a subgroup of $\mathbb{Z}^2$; hence $G_F \cong \mathbb{Z}^r$ for some $0 \le r \le 2$.

Definition 2.3 (Diophantine rank)**.**

$$r_{\mathrm{dio}}(F) = \mathrm{rank}_{\mathbb{Z}}(G_F).$$

2.2 Classification for Curves of Genus 0

Theorem 2.4 (Classification of diophantine rank for curves of genus 0)**.** *Let $F(x, y) \in \mathbb{Z}[x, y]$ be an absolutely irreducible polynomial defining an affine curve $X : F = 0$ over $\mathbb{Q}$. Let the smooth projective model C of X have genus $g = 0$. Then:*

$$r_{\mathrm{dio}}(F) = \begin{cases} 0, & \text{if } |S_F| \le 1, \\ 1, & \text{if all points of } S_F \text{ are collinear and } |S_F| \ge 2, \\ 2, & \text{if } S_F \text{ contains three non-collinear points.} \end{cases}$$

Доказательство. **Case 1:** $|S_F| \le 1$. If $S_F = \emptyset$, then $G_F = \{0\}$, so $\mathrm{rank}(G_F) = 0$. If $S_F = \{p\}$, then the only difference is $p - p = 0$, so again $G_F = \{0\}$.

Case 2: all points are collinear. Suppose all points of S_F lie on the line $ax + by = c$ with $(a, b) \ne (0, 0)$. For any $p, q \in S_F$:

$$a(p_x - q_x) + b(p_y - q_y) = (ap_x + bp_y) - (aq_x + bq_y) = c - c = 0.$$

Thus every difference lies in the one-dimensional $\mathbb{Q}$-subspace $V = \{(u, v) \in \mathbb{Q}^2 \mid au + bv = 0\}$. Hence $G_F \otimes_{\mathbb{Z}} \mathbb{Q} \subseteq V$, so $\mathrm{rank}(G_F) \le 1$. Since $|S_F| \ge 2$, there exists a non-zero difference, so $\mathrm{rank}(G_F) = 1$.

Case 3: three non-collinear points. Let $p_1, p_2, p_3 \in S_F$ be non-collinear. Consider $d_1 = p_2 - p_1$ and $d_2 = p_3 - p_1$. These are linearly independent over $\mathbb{Q}$; otherwise p_3 would lie on the line through p_1 and p_2. Therefore the subgroup $\langle d_1, d_2 \rangle_{\mathbb{Z}} \subseteq G_F$ has rank 2. Since $G_F \subseteq \mathbb{Z}^2$, we have $\mathrm{rank}(G_F) = 2$. □

2.3 Classification for Elliptic Curves

For genus 1, the situation is more subtle: by Siegel's theorem [1], the set S_F is always finite. However, the classification by collinearity remains valid.

Theorem 2.5 (Classification of diophantine rank for elliptic curves)**.** *Let $F(x, y) \in \mathbb{Z}[x, y]$ define an affine curve $X : F = 0$ whose smooth projective model is an elliptic curve C over $\mathbb{Q}$ with neutral element $\mathcal{O} \in C(\mathbb{Q})$. Then:*

$$r_{\mathrm{dio}}(F) = \begin{cases} 0, & \textit{if } |S_F| \leq 1, \\ 1, & \textit{if all points of } S_F \textit{ are collinear and } |S_F| \geq 2, \\ 2, & \textit{if } S_F \textit{ contains three non-collinear points.} \end{cases}$$

Доказательство. The finiteness of S_F follows from Siegel's theorem [1]. The proofs of the cases $|S_F| \leq 1$, collinearity, and non-collinearity are identical to those for genus 0 (Theorem 2.4).

We note that the case $r = 2$ can occur even when the Mordell–Weil rank $\rho = \mathrm{rank}_{\mathbb{Z}} C(\mathbb{Q})$ is zero. Indeed, torsion points can form non-collinear triples in $\mathbb{Z}^2$. Consider the elliptic curve

$$y^2 = x^3 + 1.$$

Its integral points include $(0, 1), (2, 3), (2, -3)$. These are non-collinear because:

$$(2, 3) - (0, 1) = (2, 2), \quad (2, -3) - (0, 1) = (2, -4),$$

and

$$\det \begin{pmatrix} 2 & 2 \\ 2 & -4 \end{pmatrix} = -8 - 4 = -12 \neq 0.$$

Thus $r_{\mathrm{dio}} = 2$. The Mordell–Weil rank of $y^2 = x^3 + 1$ is 0 (the group is $\mathbb{Z}/6\mathbb{Z}$), so $\rho = 0$ does not imply $r_{\mathrm{dio}} \leq 1$.

Conversely, if $\rho \geq 1$, the presence of a point of infinite order does *not* guarantee infinitely many integral points on the affine model; by Siegel's theorem, the set S_F remains finite. Therefore, no direct implication between ρ and r_{dio} exists in general. □

3 Duality Types: A New Class of Mathematical Objects

We introduce duality types — a new class of mathematical structures connecting the arithmetic of integral points with the topology of local systems [3, 4, 5].

3.1 Definition of a Duality Type

A duality type is a triple $(\mathcal{A}, \mathcal{B}, \Phi)$ consisting of the following data.

Category $\mathcal{A}$ (arithmetic objects). Objects are pairs (X, S), where X is an affine algebraic variety over $\mathbb{Q}$ defined by a system of equations with integral coefficients, and $S = X(\mathbb{Z})$ is the set of integral points. Morphisms are rational maps $f : X \to Y$, defined over $\mathbb{Q}$, such that $f(S_X) \subseteq S_Y$.

Category $\mathcal{B}$ (topological objects). Objects are pairs $(M, \mathcal{L})$, where M is a topological space having the homotopy type of a finite CW-complex, and $\mathcal{L}$ is a local system of finitely generated abelian groups on M [3]. Morphisms are continuous maps $f : M \to N$ together with morphisms of local systems $\mathcal{L}_M \to f^*\mathcal{L}_N$.

Functor $\Phi : \mathcal{A} \to \mathcal{B}$. For an object (X, S):

- $M = X(\mathbb{C})$, the set of complex points with the analytic topology.

- $\mathcal{L} = \mathcal{L}_S$, the local system on M defined below (Definition 3.1).

Definition 3.1 (Monodromy local system associated to integral points)**.** Let (X, S) be an object of the category $\mathcal{A}$, where X is a smooth affine curve over $\mathbb{Q}$ and $S = X(\mathbb{Z})$ is finite or infinite. Let $M = X(\mathbb{C})$ be the associated Riemann surface with the analytic topology. For each point $p = (p_1, p_2) \in S \subset \mathbb{C}^2$, consider a small loop γ_p around p in M (more precisely, around the puncture corresponding to p after compactification). Define a local system $\mathcal{L}_S$ of rank 3 on M by specifying its monodromy representation

$$\rho : \pi_1(M) \to \mathrm{GL}_3(\mathbb{Z})$$

as follows: for each $p \in S$,

$$\rho(\gamma_p) = \begin{pmatrix} 1 & 0 & 0 \\ p_1 & 1 & 0 \\ p_2 & 0 & 1 \end{pmatrix},$$

i.e., a unipotent translation by the vector (p_1, p_2) in the affine part of the fibre.

Remark 3.2. This construction is well-defined because the loops around distinct points commute in the abelianization of $\pi_1(M)$ only if the points are non-singular; in general, the monodromy representation factors through the free abelian group generated by S modulo relations coming from the topology of M. This is precisely the group G_F from Definition 2.2.

3.2 The Rank Universality Theorem

Theorem 3.3 (Rank Universality for curves of genus 0)**.** *Let $F(x, y) \in \mathbb{Z}[x, y]$ define a smooth affine conic (genus 0) with set of integral points S_F. Let $\mathcal{L}_{S_F}$ be the local system from Definition 3.1 on $M = X(\mathbb{C})$. Then*

$$\mathrm{rank}_{\mathbb{Z}} H^1(M, \mathcal{L}_{S_F}) = r_{\mathrm{dio}}(F).$$

Доказательство. For genus 0, $M = \mathbb{P}^1(\mathbb{C}) \setminus T$, where T is a finite set of punctures (including the points at infinity and the integral points on the affine part). The fundamental group $\pi_1(M)$ is free of rank $|T| - 1$. The local system $\mathcal{L}_{S_F}$ is defined by a representation $\rho : \pi_1(M) \to \mathrm{GL}_3(\mathbb{Z})$ whose image lies in the unipotent radical $U \cong \mathbb{Z}^2$.

Consider the exact sequence of local systems:

$$0 \to \mathbb{Z} \to \mathcal{L}_{S_F} \to \mathcal{L}' \to 0,$$

where $\mathbb{Z}$ is the trivial local system spanned by the invariant vector $(1, 0, 0)^T$, and $\mathcal{L}'$ is the rank-2 local system with monodromy acting by translation (p_1, p_2).

The cohomology long exact sequence gives:

$$H^0(M, \mathcal{L}') \to H^1(M, \mathbb{Z}) \to H^1(M, \mathcal{L}_{S_F}) \to H^1(M, \mathcal{L}') \to \cdots$$

The image of the connecting homomorphism $H^0(M, \mathcal{L}') \to H^1(M, \mathbb{Z})$ is generated by the differences $p - q$ for $p, q \in S_F$. Since $H^0(M, \mathcal{L}')$ is precisely the subgroup of $\mathbb{Z}^2$ generated by the differences $p - q$, and the image of the connecting homomorphism has rank equal to $\mathrm{rank}\, H^0(M, \mathcal{L}')$, we obtain from the long exact sequence:

$$\mathrm{rank}\, H^1(M, \mathcal{L}_{S_F}) = \mathrm{rank}\, H^0(M, \mathcal{L}') = r_{\mathrm{dio}}(F).$$

This completes the proof. □

Conjecture 3.4 (Rank Universality for higher genus)**.** *For any smooth affine curve X over $\mathbb{Q}$ with set of integral points S, the equality*

$$\operatorname{rank}_{\mathbb{Z}} H^1(X(\mathbb{C}), \mathcal{L}_S) = r_{\text{dio}}(X, S)$$

holds, where $\mathcal{L}_S$ is the monodromy local system from Definition 3.1.

Remark 3.5. For genus $g \geq 1$, the fundamental group is no longer free, and the cohomology H^1 also captures the topology of the compact curve (the $2g$ generators of the surface group). The conjecture states that after modding out the topological part, the remaining rank equals the diophantine rank. This is supported by the fact that the Albanese map $\text{Alb}(X) \to \mathbb{C}^g$ induces a splitting of the monodromy representation. In Section 4.4, we provide computational evidence for this conjecture in several non-trivial examples.

3.3 Hierarchy of Duality Types

We construct a hierarchy of duality types by dimension and genus:

Type	**Category A**	**Category B**
Type 0	Curves of genus 0 with integral points	Local systems on $\mathbb{P}^1(\mathbb{C})$
Type 1	Elliptic curves with integral points	Local systems on elliptic curves
Type g	Curves of genus g with integral points	Local systems on curves of genus g
Type n	Varieties of dimension n	Local systems on complex n-folds

Таблица 1: Hierarchy of duality types

Proposition 3.6 (Natural transformations)**.** *For each type n and each k, there is a natural transformation between the k-th cohomology of the local system and the arithmetic invariants of the set of integral points. In particular, for $k = 1$ and $n = 1$, this is the Rank Universality Theorem (Theorem 3.3) and Conjecture 3.4.*

4 Examples and Consequences

4.1 Examples for $r = 2$

Example 4.1 (Pell equation)**.** Consider $x^2 - 2y^2 = 1$. This is a smooth conic, genus 0. Its integral points are $(\pm 1, 0)$, $(3, 2)$, $(17, 12)$, $(99, 70)$, $\ldots$. The three points $(1, 0)$, $(3, 2)$, $(17, 12)$ are non-collinear, hence $r = 2$. By Theorem 3.3, the cohomology of the corresponding local system has rank 2.

Example 4.2 (Elliptic curve with torsion points giving $r = 2$)**.** Consider $F(x, y) = y^2 - x^3 - 1$. The integral points include

$$(-1, 0), \quad (0, 1), \quad (0, -1), \quad (2, 3), \quad (2, -3).$$

The three points $(0, 1), (2, 3), (2, -3)$ are non-collinear because:

$$(2, 3) - (0, 1) = (2, 2), \quad (2, -3) - (0, 1) = (2, -4),$$

and

$$\det \begin{pmatrix} 2 & 2 \\ 2 & -4 \end{pmatrix} = -8 - 4 = -12 \neq 0.$$

Hence $r_{\text{dio}} = 2$. The Mordell–Weil rank of $y^2 = x^3 + 1$ is 0 (the group is $\mathbb{Z}/6\mathbb{Z}$), so this provides a concrete example where $r_{\text{dio}} = 2$ but $\rho = 0$.

4.2 Examples for $r = 1$

Example 4.3. $F(x, y) = y - x$. This is a line, genus 0. We have $S_F = \{(t, t) \mid t \in \mathbb{Z}\}$, all points are collinear, hence $r = 1$.

4.3 Examples for $r = 0$

Example 4.4. $F(x, y) = x^2 + y^2 + 1 = 0$. We have $S_F = \emptyset$, so $r = 0$.

Example 4.5. $F(x, y) = (x - 1)^2 + (y - 2)^2 = 0$. We have $S_F = \{(1, 2)\}$, so $r = 0$.

4.4 Computations for Specific Curves

We now provide explicit computations of the diophantine rank and the cohomology of the associated local system for several curves, verifying Theorem 3.3 and providing evidence for Conjecture 3.4.

4.4.1 The Conic $x^2 - 2y^2 = 1$

We compute the local system explicitly. The curve $X : x^2 - 2y^2 = 1$ has two points at infinity in $\mathbb{P}^2(\mathbb{C})$ (after homogenization, they are $[1 : \pm 1/\sqrt{2} : 0]$), but as a conic it is isomorphic to $\mathbb{P}^1$ with two points removed (after stereographic projection). The set of integral points $S = \{(\pm 1, 0), (3, 2), (17, 12), \ldots\}$ is infinite. The difference group G_F is generated by

$$(3, 2) - (1, 0) = (2, 2), \quad (17, 12) - (1, 0) = (16, 12).$$

The determinant $\det \begin{pmatrix} 2 & 2 \\ 16 & 12 \end{pmatrix} = 24 - 32 = -8 \neq 0$, so G_F has rank 2. Thus $r_{\text{dio}} = 2$.

By Theorem 3.3, $H^1(M, \mathcal{L}_S)$ has rank 2. This example demonstrates the non-triviality of the theorem: an infinite set of integral points can generate a finite-rank subgroup of $\mathbb{Z}^2$, and the cohomology of the local system captures that rank.

4.4.2 The Elliptic Curve $y^2 = x^3 + 1$

Let $X : y^2 = x^3 + 1$. The integral points include $(0, 1), (2, 3), (2, -3)$, which are non-collinear. Thus $r_{\text{dio}} = 2$. The Mordell–Weil rank is 0. This provides evidence for Conjecture 3.4: although we cannot compute H^1 explicitly for genus 1, the conjecture predicts that the topological part (the $2g = 2$ generators of the elliptic curve) can be separated from the arithmetic part, leaving rank 2 for the arithmetic contribution.

4.5 Potential Connections to the Langlands Program

Local systems on curves [3] are central objects in the geometric Langlands program. Duality types connect the arithmetic of integral points with such local systems.

We note that the local system $\mathcal{L}_S$ constructed in Definition 3.1 is unipotent, hence its associated L-function is entire (no poles). However, one can consider *rigid* local systems [3] whose monodromy is semi-simple; these are known to correspond to automorphic forms via the Langlands correspondence. A natural question is whether there exists a semi-simplification of $\mathcal{L}_S$ whose L-function encodes the diophantine rank. This would provide a new bridge between the arithmetic of integral points and the theory of automorphic forms.

5 Significance and Open Questions

5.1 A New Invariant

The diophantine rank r_{dio} is a new integral invariant of a Diophantine equation. Unlike the cardinality of the solution set, it reflects the geometric arrangement of solutions in $\mathbb{Z}^2$, namely the dimension of their affine span.

5.2 Relation to Arithmetic Geometry

Theorems 2.4 and 2.5 establish a direct connection between the geometry of the curve and the arithmetic of its integral points. For genus 0 and genus 1, the diophantine rank is completely determined by the geometry of the set S_F in $\mathbb{Z}^2$. Moreover, Example 4.2 shows that the diophantine rank is independent of the Mordell–Weil rank.

5.3 Duality Types as a New Branch of Mathematics

Duality types constitute a new class of mathematical structures, analogous to spectral sequences or derived categories. This is a way of organizing knowledge at the interface of number theory and topology, providing a unified language for studying Diophantine equations, local systems, and cohomology [3, 5].

5.4 Open Questions

1. **Genus $g \geq 2$.** By Faltings' theorem [2], the set of integral points on a curve of genus $g \geq 2$ is finite. What is the maximal possible diophantine rank for such curves? In particular, can r_{dio} be arbitrarily large for a fixed genus $g \geq 2$ if we vary the embedding into $\mathbb{A}^2$? Since the number of integral points is bounded by the height, the rank is bounded by $2 \log |S_F|$, but a sharper bound in terms of the genus would be desirable.

2. **Higher dimensions.** Generalize the definition to hypersurfaces $F(x_1, \ldots, x_n) = 0$. Then $G_F \subset \mathbb{Z}^n$ and $r_{\text{dio}} \in \{0, \ldots, n\}$. What is the relation between r_{dio} and the dimension of the variety? Is there a bound in terms of the degree and the dimension?

3. **Relation to the Mordell–Weil rank.** For elliptic curves, we have shown that no direct implication exists between the Mordell–Weil rank and the diophantine rank (Example 4.2). However, is there a conjectural inequality of the form

$$r_{\text{dio}} \leq 2\rho + 2$$

   or similar, after choosing a suitable model? For the curve $y^2 = x^3 + 1$, we have $r_{\text{dio}} = 2$ and $\rho = 0$, so the inequality would be $2 \leq 2$, which is tight.

4. **Algorithmic computability.** For a given F, can r_{dio} be computed algorithmically? For genus 0 and 1, yes (in principle, by enumerating all integral points using Baker's theory). For $g \geq 2$, it reduces to finding all integral points, which is algorithmically solvable by the work of Coates [7] but with complexity depending on the curve.

5. **Potential connection to automorphic forms.** Can the diophantine rank be interpreted as the dimension of the space of automorphic forms associated to a semi-simplification of the local system $\mathcal{L}_S$? This is a natural direction for future research.

Список литературы

[1] C.L. Siegel. *Über einige Anwendungen diophantischer Approximationen.* Abh. Preuss. Akad. Wiss. Phys.-Math. Kl., 1929.

[2] G. Faltings. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), 349–366.

[3] N.M. Katz. *Rigid Local Systems.* Princeton University Press, 1996.

[4] J.P. Whang. *Arithmetic of curves on moduli of local systems.* arXiv:1803.04583, 2018.

[5] H. Diao, Z. Yao. *Monodromy and rigidity of crystalline local systems.* arXiv:2509.19813, 2025.

[6] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2009.

[7] J. Coates. *An effective p-adic analogue of a theorem of Thue.* Acta Arith. 15 (1970), 279–305.

[8] P. Corvaja, U. Zannier. *On integral points on surfaces.* Annals of Mathematics 160 (2004), 705–726.