Panoramas & Synthèses
56, 2021, p. 253–318

SOME ARITHMETIC ASPECTS OF HYPERBOLICITY

by

Pietro Corvaja

Abstract. – We give a survey of the study of integral points and some aspects of Diophantine approximation on algebraic varieties, and we treat arithmetic analogues of the notion of hyperbolicity for algebraic varieties.

According to a conjecture by Lang and Vojta, those (quasi projective) algebraic varieties, defined over number fields, whose complex points form a hyperbolic manifold (in the complex analytic sense) should admit only degenerate sets of integral or rational points.

In dimension one, after the work of Siegel and Faltings, it is known that the analytic and arithmetic notions of hyperbolicity are equivalent. We show, mainly focusing on the two-dimensional case, that many apparently unrelated Diophantine problems can be reduced to questions about the distribution of integral points on certain algebraic surfaces.

Significant examples are the following. The theorem of Darmon and Granville on the generalized Fermat equation $x^p + y^q = z^r$ is proved here in a slightly simplified way and its connection with the hyperbolicity of the triple of exponents (p, q, r) is developed in detail. A conjecture about the denominators of rational points on elliptic curves is linked to Vojta's conjecture, and a weaker version is unconditionally established.

A main tool in the proofs of finiteness or degeneracy results for integral points on varieties is provided by Diophantine approximation. The theory of Diophantine approximation is also linked to questions of hyperbolicity, and in particular a new "gap principle" for rational points on elliptic curves is proved and its formulation is shown to be directly linked to a hyperbolicity condition.

1. Introduction

1.1. Introducing the problems. – Our main concern will be the following problem:

To find geometric properties for an algebraic variety X defined over a number field κ which ensure that for every number field $K \supset \kappa$ the set $X(K)$ of K-rational points of X is not Zariski-dense.

This property can be considered to be the arithmetic analogue of a weak-form of hyperbolicity, namely: *there exists no entire curve* $f : \mathbb{C} \to X(\mathbb{C})$ *with Zariski-dense image.*

An analogue question arises naturally concerning integral points.

The investigation on these problems led to considering two other different issues, namely *Diophantine approximation* and *gap principles.*

Diophantine approximation refers, at first instance, to the theory of approximating algebraic numbers by rationals. More generally, one can fix one or more 'targets' on an algebraic variety in which rational points (over a fixed number field) are dense, in some archimedean or p-adic topology, and look at how fast these targets can be approached by a sequence of rational points. Usually the targets are hypersurfaces on the given algebraic variety, so they are themselves points if the variety is a curve. In any case, they are supposed to be defined over the field of algebraic numbers.

The so called gap principles arise when a sequence of rational points converges 'rapidly' to any point, possibly a transcendental one; we dispose of a gap principle if we can deduce, from the rapidity of its convergence, that the approximating sequence is 'sparse'.

In the case the ambient algebraic variety X is a curve, we have a rather satisfactory solution to all the above issues, due mainly to works of K. Roth, C.-L. Siegel, L. Mordell, A. Weil and G. Faltings.

In each case, a hyperbolicity condition on the variety or on the sequence of approximants implies a finiteness or a sparseness result. More precisely, for a smooth algebraic curve $\mathcal{C}$, of genus g with d points at infinity (in a smooth completion), we define its Euler characteristic χ to be the number

$$\chi = 2g - 2 + d.$$

If $d = 0$, i.e., the curve is projective, then $\chi = 2g - 2$ coincides with the degree of the canonical bundle. We say that a curve is *hyperbolic* if $\chi > 0$, *parabolic* if $\chi = 0$ and *of elliptic type*[1] if $\chi < 0$. Hence the hyperbolicity condition reads

$$\chi := 2g - 2 + d > 0 \qquad \text{(Hyperbolicity).} \tag{1.1}$$

Let us review the mentioned arithmetic results, by starting from the problem of density. Recalling that on an irreducible curve the Zariski-dense sets are just the infinite ones, we are interested in describing those algebraic curves which can contain infinitely many rational or integral points.

In the case of integral points, a theorem proved by Siegel in 1929 (see **[62]** and **[69]**) reads:

***Theorem* (Siegel's Theorem).** – *Let* $X \subset \mathbb{A}^N$ *be an affine irreducible curve, defined over a number field* κ. *If the curve contains infinitely many points with coordinates in the ring of algebraic integers of* κ *then* X *is a rational curve and it has at most two points at infinity.*

[1] By *elliptic curve* we mean something different, namely a parabolic complete curve.

Vice-versa, if a curve is rational (i.e., of genus zero with at least one rational point) and has one or two smooth points at infinity, then a suitable model of it contains infinitely many integral points, as we now show. First, if it has exactly one point at infinity, a normalization of it is isomorphic to the affine line. On a suitable integral model (i.e., after changing coordinates) it will clearly have infinitely many integral points. Note that the coordinate-change is unnecessary if we replace the ring of integers with a suitable ring of S-integers (defined below). If a rational curve has two points at infinity, then after possibly a quadratic field extension a normalization of it becomes isomorphic to the variety $\mathbb{G}_m = \mathbb{A}^1 - \{0\}$ (defined e.g., as a closed subset in the plane by the equation $xy = 1$) and again it has infinitely many integral points, at least after enlarging the ring of integers so to acquire infinitely many units.

In view of these considerations, Siegel's theorem can be considered to be a best-possible result.

For rational points, Faltings theorem, proved in 1983, states that:

***Theorem* (Faltings' Theorem)**. – *Let X be an irreducible algebraic curve defined over a number field κ. If the genus of X is ≥ 2, then its set of κ-rational points is finite.*

As for Siegel's Theorem, the above statement is essentially optimal, since, as we shall see, every algebraic curve of genus ≤ 1 contains infinitely many rational points, after suitably enlarging the ground number field.

Let us now consider briefly the two other issues, starting from Diophantine approximation.

It is well known that every real irrational number α admits infinitely many rational approximations p/q, where p, q are coprime integers, $q > 0$, such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

A proof of this fact is obtained via Dirichlet's box principle (see Chapter I of [**58**]); an explicit sequence of rational approximations is provided by the continued fraction development of α.

The celebrated Theorem of Roth (see §2.3) asserts that for every real number $\delta > 2$ and every real algebraic number α, the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\delta} \tag{1.2}$$

admits only finitely many solutions $p/q \in \mathbb{Q}$ (where p, q are coprime integers, $q > 0$). Note that the approximants $p/q \in \mathbb{Q}$ (and the target α) are points on the line $\mathbb{P}_1$, whose Euler characteristic χ equals -2. Hence the finiteness result of Roth requires

$$\chi + \delta > 0, \tag{1.3}$$

which is the analogue of the hyperbolicity condition (1.1).

We shall see (Theorem 2.21) that when approximating an algebraic point on an elliptic curve with rational ones, the analogue of Roth's theorem holds with any exponent $\delta > 0$; this is in accordance with the fact that the Euler characteristic of an elliptic curve is zero, so the inequality (1.3) holds in that case whenever δ is strictly positive.

If the limit point of the sequence of rational approximations is transcendental, the conclusion of Roth's Theorem does not hold; in fact, for every δ one can construct a real number α such that the inequality (1.2) admits infinitely many rational solutions. However, we dispose in that situation of a gap principle (Theorem 2.27), asserting that if the sequence of approximations $p_1/q_1, p_2/q_2, \ldots$ is ordered by increasing denominators, then

$$\liminf_{n\to\infty} \frac{\log q_{n+1}}{\log q_n} \geq \delta - 1,$$

which is a non-trivial result whenever $\delta > 2$ (i.e., when $\chi + \delta > 0$). The analogue for elliptic curves provides, *mutatis mutandis*, the bound $1 + \delta$ for the above limit, which is non trivial for every $\delta > 0$, i.e., again when $\chi + \delta > 0$.

1.2. Integrality over algebraic varieties. – We shall formulate in a unified way the two problems (and the general results in dimension one) for the integral and for the rational points, by giving a suitable definition of what we mean by an *integral* point.

Definition 1.1. – *Let κ be a number field, S a finite set of places of κ containing the archimedean ones. The ring of S-integers of κ, denoted by $\mathcal{O}_S$, is defined as the set*

$$\mathcal{O}_S = \{x \in \kappa \,:\, |x|_\nu \leq 1 \text{ for all } v \notin S\}.$$

Its group of units, called the group of S-units, is then

$$\mathcal{O}_S^\times = \{x \in \kappa \,:\, |x|_\nu = 1 \text{ for all } v \notin S\}.$$

Definition 1.2. – *Let X be a quasi projective irreducible variety, defined over a number field κ. Let us denote by $\tilde{X}$ a completion of X in a projective space $\mathbb{P}_N$. Then we can write $X = \tilde{X} - D$, where D is a proper closed subvariety of $\tilde{X}$. We say that a rational point $p \in X(\kappa)$ is S-*integral with respect to D *if for no place outside S p reduces to a point of D.*

We note that in the above definition no mention of integral models appears: in fact, we assume that our variety is already embedded in a projective space $\mathbb{P}_N$, which is canonically provided with an integral model; this canonical integral model implicitely appears via the notion of reduction modulo a prime.

We also note that whenever the variety X is affine, and embedded into the affine space $\mathbb{A}^N$, the integral points with respect to the divisor at infinity of X exactly correspond to the points of X having all their coordinates in $\mathcal{O}_S$. If $X = \tilde{X}$ is projective, then $D = \emptyset$ and the set of S-integral points coincides with the full set of κ-rational points.

An alternative definition of integrality, making use of Weil functions, will appear later.

We now give some examples of integrality of rational points on quasi-projective algebraic varieties.

— Let $X = \mathbb{A}^1$ be the affine line, embedded into the projective line $\tilde{X} = \mathbb{P}_1$ by the map $t \mapsto (t : 1)$ so that the complement $\tilde{X} - X$ consists of the single point $D = \{(1 : 0)\}$, also called the point at infinity. Letting $\kappa = \mathbb{Q}$, we can write a rational point on the line as $t = a/b$, where $a, b \in \mathbb{Z}$ are coprime integers, $b \neq 0$. Then t corresponds to the projective point $(a : b)$, which reduces to $(1 : 0)$ modulo the primes dividing b. It is integral if and only if there are no such primes, which amounts to $b = \pm 1$, i.e., $t \in \mathbb{Z}$.

— Let $X = \mathbb{G}_m = \mathbb{P}_1 - \{0, \infty\}$. For the same reason as in the previous example, $X(\mathcal{O}_S) = \mathcal{O}_S^*$.

— Consider the quasi-projective surface $X = \mathbb{A}^2 - \{(0,0)\}$. It can be embedded into $\mathbb{P}_2$ in the usual way: $(x, y) \mapsto (x : y : 1) = (x : y : z)$, so that $X = \mathbb{P}_2 - D$, with D consisting of the line $z = 0$ plus the single point $(0 : 0 : 1)$. The set $X(\mathbb{Z})$ consists of pairs $(x, y) \in \mathbb{Z}^2$ with $\gcd(x, y) = 1$. Note that by changing the compactification $\tilde{X}$, e.g., replacing $\mathbb{P}_2$ by the plane blown up at the point $(0 : 0 : 1)$, we can view X as the complement of a hypersurface in a projective surface.

— Let $\tilde{X} = \mathbb{P}_1 \times \mathbb{P}_1$ be the product of two lines; let D be its diagonal and $X = \mathbb{P}_1^2 - D$. Each $\mathbb{Q}$-rational point of $\mathbb{P}_1 \times \mathbb{P}_1$ can be written as $P = ((a : b), (c : d))$ where a, b (resp. c, d) are coprime integers. The condition of integrality with respect to the diagonal is equivalent to the quantity $ad - bc$ being a unit, i.e., $ad - bc = \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm 1$. Since (a, b) (resp. (c, d)) are defined up to constant, i.e., up to multiplying both of them by -1, we can normalize so that the determinant is positive and the set $X(\mathbb{Z})$ is in natural bijection with $P\mathrm{SL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.

— Let $f(x, y), g(x, y) \in \mathcal{O}_S[x, y]$ be polynomials. Suppose that the affine curves of equations $f(x, y) = 0$ and $g(x, y) = 0$ intersect transversally at every point of intersection. Letting $P_1, \dots, P_k \in \mathbb{A}^2 \subset \mathbb{P}_2$ be the set of the intersection points of the two curves, define $\tilde{X}$ to be the projective plane blown up at these intersection points. Let now D be the union of the pull-back of the line at infinity with the strict transform of the zero divisor of the polynomial $g(x, y)$ and put $X = \tilde{X} - D$. Then $X(\mathcal{O}_S)$ is in natural bijection with the set of pairs $(x, y) \in \mathcal{O}_S^2$ such that $g(x, y)$ divides $f(x, y)$ in the ring $\mathcal{O}_S$. In other words, it represents the set of S-integral solutions to the equation $z \cdot g(x, y) = f(x, y)$.

— This example will be treated in detail in §5. Let $1 < p \leq q \leq r$ be three natural numbers, $\mathcal{S}$ be the quasi-projective surface defined in $\mathbb{A}^3$ by the equation $x^p + y^q = z^r$ *with the origin removed.* The integral points in $\mathcal{S}$ correspond to the integral solutions $(x, y, z) \in \mathbb{Z}^3$ to the defining equation $x^p + y^q = z^r$ such that $(x, y, z) \not\equiv (0, 0, 0) \pmod{p}$ for every prime p, i.e., to the solutions (x, y, z) in coprime integers.