Some arithmetic aspects of hyperbolicity

Pietro Corvaja

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 $X(K)$ 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 [59] and [70]) 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.*

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

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

[1] by elliptic cuve we mean something different, namely a parabolic complete curve.

A proof of this fact is obtained via Dirichlet's box principle (see Chapter I of [57]); 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 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 2.26), 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 $1 + \delta$, 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* is 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 coincide 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 if 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 $\mathbb{A}^2 - \{(0, 0)\}$. It can be embedded into $\mathbb{P}_2$ in the ususal way: $(x, y) \mapsto (x : y : 1) = (x : y : z)$, so that $X = \tilde{X} - D$ consists 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 $ad - bc = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$. 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 $P_1, \ldots, P_k \in \mathbb{A}^2 \subset \mathbb{P}_2$ 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.

1.3 Density in the 1-dimensional case

As anticipated, we now state the main theorem concerning curves, obtained by combining results of Siegel's (1929) and Faltings (1983).

We first need a definition. A smooth algebraic curve $\mathcal{C}$ defined over the complex number field is topologically characterised by two discrete invariants: its genus g and the number $d = \sharp(\tilde{\mathcal{C}} - \mathcal{C})$ of its points at infinity in a smooth completion $\tilde{\mathcal{C}}$ (so d equals zero if $\mathcal{C}$ is projective). We define the *Euler characteristic* of $\mathcal{C}$ to be the number

$$\chi = \chi(\mathcal{C}) = 2g - 2 + d.$$

It is a homotopy invariant.

The mentioned combination for Siegel's and Falting's theorem reads as follows:

Theorem 1.4 (Siegel-Faltings Theorem)**.** *Let $\mathcal{C} = \tilde{\mathcal{C}} - D$ be an irreducible (affine or projective) curve over a number field κ, where $D \subset \tilde{\mathcal{C}}(\bar{\kappa})$ is the set of its points at infinity. Let $\mathcal{O}_S \subset \kappa$ be a ring of S-integers. If the set $\mathcal{C}(\mathcal{O}_S)$ is infinite, then $\chi \leq 0$.*

This result is best-possible, in view of the following theorem:

Theorem 1.5. *Let $\mathcal{C}$ be a (affine or projective) curve with $\chi(\mathcal{C}) \leq 0$, defined over a number field κ. There exists a finite field extension κ' of κ and a ring of S-integers $\mathcal{O}_S \subset \kappa'$ such that $\mathcal{C}(\mathcal{O}_S)$ is infinite.*

We say that the integral points are potentially dense, if the conclusion of the above theorem holds.

The proof of Theorem 1.5 consists in analyzing one by one all the possible cases of curves with $\chi \leq 0$. We start with the projective ones, where, we recall, integral points coincide with rational ones. In the projective case, the Euler characteristic, if ≤ 0, can only be -2 and 0.

The first case $\chi = -2$ corresponds to a curve of genus 0; after performing a suitable quadratic extension of κ, such a curve becomes isomorphic to the line $\mathbb{P}_1$, which posses infinitely many rational points.

The case $\chi = 0$ corresponds to a genus 1 curve; after enlarging if necessary the number field κ, we can suppose that there exists a rational point, hence we obtain the structure of an elliptic curve. If we find an algebraic point of infinite order on this elliptic curve, we can then choose a number field κ' so that the elliptic curve (including its origin) and the given point of infinite order are defined over κ'. Hence, over κ' the curve in question will have infinitely many rational points. Now, to prove that not all algebraic points have infinite order, we dispose of several methods, none of which is completely obivious. First, we can prove that the absolute height of torsion points is bounded, so any point of sufficiently high height is necessarily of infinite order. Alternatively, one can argue p-adically, proving that a point sufficiently closed to the origin in the p-adic sense cannot be torsion, unless it coincides with the origin; again, this property provides algebraic points of infinite order.

Concerning open curves, the inequality $\chi \leq 0$ holds for the affine line $\mathbb{A}^1 = \mathbb{P}_1 - \{\infty\}$, for which $\chi = -1$, and for the complement of two points on $\mathbb{P}_1$, for which $\chi = 0$.

In the first case, over a suitable ring of S-integers (or after changing the integral model), we have infinitely many integral points.

In the second case, after possibly a quadratic extension we can achieve the rationality of the points at infinity, so the curve will become $\mathbb{P}_1 - \{0, \infty\} \simeq \mathbb{G}_m$ and again, after a suitable enlargment of $\mathcal{O}_S$ if necessary (so that the group $\mathcal{O}_S^*$ becomes infinite) we obtain infinitely many integral points.

It is worthwile to notice some alternative formulations of the inequality $\chi \leq 0$, as well as some coincidences with hyperbolicity results in the sense of Picard's theorem. Namely, we can restate Theorem 1.4 (together with its converse, Theorem 1.5) as follows:

For an (affine or projective) smooth algebraic curve $\mathcal{C}$ the following properties are equivalent:

(i) $\mathcal{C}(\mathcal{O}_S)$ is Zariski-dense, for a suitable ring of S-integers $\mathcal{O}_S$;

(ii) $\mathcal{C}$ is a homogeneous space for an algebraic group;

(iii) the fundamental group of the topological space $\mathcal{C}(\mathbb{C})$ is abelian;

(iv) there exists a non-constant holomorphic map $\mathbb{C} \to \mathcal{C}(\mathbb{C})$;

(v) the degree of the divisor $(D + K_{\tilde{\mathcal{C}}})$, where D is the divisor at infinity and $K_{\tilde{\mathcal{C}}}$ is a canonical divisor of the complete curve $\tilde{\mathcal{C}}$, is ≤ 0.

In other words, the negation of any of the properties (ii),...,(v) implies that for every ring of S-integers $\mathcal{O}_S$ the set $\mathcal{C}(\mathcal{O}_S)$ is finite.

1.4 The higher dimensional case

In higher dimensions, it is natural to try to figure out which of the above properties (ii),...(v) (after suitable reformulation of (v)) implies the potential density of integral points, and which ones are incompatible with that density. Let us analyze the possibility of such implications.

It is rather easy to see (although not completely obvious) that on every homogenous space the set of integral points is potentially dense; for instance, in the case of principle homogeneous spaces, this fact amounts to saying that the integral points on an algebraic group are potentially dense. The crucial fact consists in proving that not all algebraic points on an algebraic group (of positive dimension) are torsion.

However, in dimension ≤ 2 the implication $(i) \Rightarrow (ii)$ does not hold; for instance, the rational points on a elliptic surface can be Zariski-dense, and in general there are no non-trivial algebraic group actions on such surfaces.

An alternative to asking that the variety be acted on by a single algebraic group is that it is covered by images of non-constant maps from algebraic groups (which can then be chosen to be commutative). It was asked (e.g. by Vojta) whether *the Zariski closure of the set of integral points on a variety X is the union of a finite set and the images of non-constant maps $G \to X$, where G is a commutative algebraic group).* The above assertion might be viewed as a substitute to the implication (i)⇒(ii).

Concerning relations between (iii) and (i), neither implication holds. It is rather easy to construct examples both of (smooth) algebraic varieties with non-abelian fundamental group and a Zariski-dense set of integral points as well as varieties with abelian fundamental group and degenerate integral points. Some examples of the first class are represented by hyperelliptic surfaces [2]; for examples in the other direction, one can take the complement of four or more lines in general position on the plane: its fundamental group is abelian by a theorem of Zariski, while its integral points are degenerate by the S-unit equation Theorem (see §6). Hence property (iii) neither implies nor is implied by the potential density of integral points.

The relations between conditions (i) and (iv) in higher dimensions have been intensively investigated.

Concerning (v), we need to reformulate the condition on the positivity of the degree of divisor; a possibility is the notion of bigness: a divisor D on a (smooth complete) variety $\tilde{X}$ is said to be big if $h^0(\tilde{X}, nD) \gg n^{\dim \tilde{X}}$. This condition amounts to a positive multiple of D being linearly equivalent to the sum of an ample and an effective divisor.

One of the most important problems in this field, raised by Vojta after combining previous formulations suggested by Bombieri and Lang, aims at providing a substitution for the implication $(i) \Rightarrow (v)$ and reads as follows:

Vojta's Conjecture. *Let $\tilde{X}$ be a smooth projective variety defined over a number field κ. Let $D \subset \tilde{X}$ be a possibly reducible hypersurface, defined over κ, with normal crossing*

[2]Here is an exemple: given an elliptic curve E and a torsion point $T \in E(\kappa)$ of order 2, consider the automorphism of order four $E^2 \to E^2$ sending $(P, Q) \to (Q, P + T)$. The fundamental group of the quotient variety is a non-trivial extension of $\{\pm 1\}$ by $\mathbb{Z}^4$, hence it is non-abelian. For a discussion of hyper-elliptic varieties and their fundamental groups, see [11].

singularities (if any) and put $X = \tilde{X} - D$. *Letting* $K_{\tilde{X}}$ *be a canonical divisor for* $\tilde{X}$, *suppose that the sum* $D + K_{\tilde{X}}$ *is a big divisor. Then* $X(\mathcal{O}_S)$ *is not Zariski-dense.*

The complete varieties whose canonical bundle is big are said to be of *general type*. The smooth open varieties of the form $X = \tilde{X} - D$, where D has normal crossing singularities and $K_{\tilde{X}} + D$ is big are called varieties of *log-general type*. The condition for an open variety X of being of log-general type depends only on X, not on its compactification $\tilde{X}$.

It is easy to check that Theorem 1.4 implies the positive solution of Vojta's Conjecture in the one-dimensional case. On the other hand, Theorem 1.5 asserts that whenever the divisor $D + K$ on a curve $\tilde{X}$ is not big, the integral points on $X = \tilde{X} - D$ are potentially dense.

We now present some consequences of Vojta's conjecture.

(i) Let A be an abelian variety, $D \subset A$ an hypersurface which is an ample divisor[3]. Put $X := A - D$. Since $K_A = 0$, $K_A + D = D$ which is ample by assumption, Vojta's Conjecture predicts the degeneracy of the integral points of X. Actually a stronger result was proved by Faltings [32], namely the finiteness of such points.

(ii) Let A be an abelian variety, $X \subset A$ be a closed proper algebraic subvariety, not a translate of a sub-abelian variety. It is then known (and easy to prove) that X is of general type. This case of Vojta's conjecture, already formulated by Weil, was again proved by Faltings in [32], whose result implies that the Zariski closure of the set of rational points is a finite union of translates of algebraic subgroups contained in X. In particular, if A is simple, the set of rational points on any proper closed subvariety is finite.

(iii) Consider now an irreducible closed algebraic subvariety X of a torus $\mathbb{G}_m^r$. If X is not a translate of an algebraic subgroup of $\mathbb{G}_m^r$, then X is of log-general type. The degeneracy of its integral points, which follows from the S-unit equation theorem, was proved before Vojta's Conjecture was formulated. These three examples, together with some applications, will be discussed in detail in §6.

(iv) Consider a smooth algebraic surface $\tilde{X} \subset \mathbb{P}_3$. It is of log-general type if and only if its degree is ≥ 5. We dispose of no example of any such surface for which the degeneracy of rational points is proved. Note that the smooth hypersurfaces in $\mathbb{P}_3$ are simply connected, so they cannot be embedded into an abelian variety (more generally, any rational from such surfaces to an abelian variety is constant). Hence Faltings' theorem discussed above cannot be applied. When the degree of the surface $\tilde{X}$ is ≤ 3, it is known that the set of rational points is potentially dense. This follows from the fact that $\tilde{X}$ becomes rational after an extension of the scalars. However, the case of degree four is still open. Examples are known of smooth quadric surfaces with a Zariski-dense set of rational points (for instance when they admit an elliptic fibrations, see e.g. Swinnerton-Dyer's paper on the quartic Fermat surface [60]) and it is widely believed that the rational points are always potentially dense.

[3]It is always the case if A is simple

(v) Consider an affine surface obtained from the projective plane by removing a (possibly reducible) curve with normal crossing singularities. We obtain a surface of log-general type whenever the degree of this curve is ≥ 4. The degeneracy of the corresponding integral points is proved only when such a boundary curve has at least four components. In that case, it admits non trivial maps to $\mathbb{G}_m^3$, hence the S-unit equation theorem can be applied (see §6). The first open case arises for a curve consisting of a conic and two lines in general position. It implies for instance the following (still unknown) assertion: the pairs of S-units $(u, v) \in \mathcal{O}_S^* \times \mathcal{O}_S^*$ such that $1 + u + v$ is a perfect square are not Zariski dense in the plane.

(vi) Consider again a smooth irreducible hypersurface of $\tilde{X}$ of degree $d \leq 4$. When the degree is 4, the canonical divisor of $\tilde{X}$ is equivalent to zero, and so the complement of a hyperplane section (with normal corissing singularities) is of log-general type. The same is true for the complement of two hyperplane sections in a cubic surface, and of three hyperplane sections on a quadric. In general, the degeneracy of the integral points in these situations is still unproven, but partial results (especially in the cubic case) are provided in [22] and will be discussed in §7.

(vii) Let A be an abelian surface, with origin O. A rational point $P \in A(\kappa)$ is S-integral with respect to O if for no valutaion (outside S) it reduces to O. It can be conjectured that whenever $A(\kappa)$ is Zariski-dense, the subset of integral points with respect to O is also Zariski-dense. This example can also be reduced to an instance of integrality with respect to a divisor, after blowing-up the origin O on A and removing the resulting exceptional divisor. The sum of the canonical divisor plus the divisor at infinity turns out to be twice that divisor, which is not big.

2 Heights, Diophantine approximation

2.1 Valuations and heights

We recall the standard vocabulary and fix the notation that will be used throughout.

Let κ be a number field. For every place ν of κ, the corresponding absolute values differ logarithmically by a positive constant: namely, if $|\cdot|_\nu$ and $\|\cdot\|_\nu$ are two equivalent absolute values of κ there exists a positive real number δ such that for every $x \in \kappa$, $|x|_\nu = \|x\|_\nu^\delta$. We are looking for a canonical normalization, which will simplify the notation in the formulation of results from Diophantine approximation. One natural choice would be simply to choose the ν-adic absolute values extending the natural ones already defined in the rational number field $\mathbb{Q}$. However, there is another possibility, which is less canonical since it depends on the number field κ, but has the advantage that by adopting this new convention, the generalization and extensions of Roth's theorem will be easier to state. We proceed to define this second normalization.

For each place ν (i.e. equivalence class of absolute values of κ) we normalize the corresponding absolute value $|\cdot|_\nu$ of κ in the following way: if ν is ultrametric, lying

above the prime p of $\mathbb{Z}$, we set for every $\alpha \in \mathbb{Q}$,

$$|\alpha|_\nu = |\alpha|^{\frac{[\kappa_\nu:\mathbb{Q}_p]}{[\kappa:\mathbb{Q}]}},$$

where $|\cdot|_p$ denotes the ususal p-adic absolute value of $\mathbb{Q}$. If ν is archimedean, corresponding to an embedding $\kappa \hookrightarrow \mathbb{C}$, we put

$$|\alpha|_\nu = |\alpha|^{\frac{[\kappa_\nu:\mathbb{R}]}{[\kappa:\mathbb{Q}]}},$$

where $|\cdot|$ denotes the usual complex absolute value.

With these normalizations, the Weil height of an algebraic number α can be expressed as

$$H(\alpha) = \prod_\nu \max(1, |\alpha|_\nu),$$

or in logarithmic form

$$h(\alpha) = \sum_\nu \log^+ |\alpha|_\nu.$$

Here the sum (and the product in the previous formula) runs over the places of any number field containing α, and the result turns out to be independent of such a number field. Hence the height can be defined as a function $h : \bar{\mathbb{Q}} \to \mathbb{R}^+$. (Here $\mathbb{R}^+$ denotes the semigroup of non-negative real numbers).

The fundamental property of Weil height is represented by the following finiteness statement

Theorem 2.1 (Northcott Theorem)**.** *For each pair of numbers $d \geq 1, c \geq 0$, the set of algebraic numbers $\alpha \in \bar{\mathbb{Q}}$ such that*

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d, \qquad h(\alpha) < c$$

is finite.

The height satisfies the following properties: for every $\alpha \in \bar{\mathbb{Q}} - \{0\}$,

$$\begin{aligned} h(\alpha^n) &= |n| \cdot h(\alpha), \qquad \forall n \in \mathbb{Z}, \\ h(\alpha) = 0 \qquad &\Leftrightarrow \quad \alpha \quad \text{is a root of unity.} \end{aligned}$$

These properties can be restated by saying that the Weil height is a normalized height on the multiplicative group $\mathbb{G}_m$. It defines a norm on the quotient group $\bar{\mathbb{Q}}^*/\mathrm{Tors}(\mathbb{Q}^*)$ (*see* [8], Chap. V).

Another class of one-dimensional algebraic groups we shall be interested in is provided by elliptic curves.

Given an elliptic curve E over a number field κ, its set of rational points $E(\kappa)$ has the structure of an abelian group. Letting $x \in \kappa(E)$ being a non-constant function

(for instance the x-coordinate in a Weierstrass model), one can define the "naive" height associated to the rational function x by letting

$$h(P) = h_x(P) := h(x(P)), \qquad \forall P \in E(\bar{\kappa}),$$

where the last height is the one already defined in $\mathbb{P}_1(\bar{\kappa})$. The crucial point in the construction of the Néron-Tate height is the following proposition

Proposition 2.2. *Let E be an elliptic curve defined over the field of algebraic numbers $\bar{\mathbb{Q}}$. Then the function $E(\bar{\mathbb{Q}}) \to \mathbb{R}$*

$$P \mapsto |h(2P) - 4h(P)|$$

is bounded.

It follows that the sequence $n \mapsto h(2^n P)/4^n$ converges. Letting $\hat{h}_E(P)$ be its limit, we obtain the so-called Néron-Tate height on E, i.e. a function $E(\bar{\mathbb{Q}}) \to [0, +\infty)$ with the following properties

(i) $\hat{h}(P) \geq 0 \quad \forall P \in E(\bar{\mathbb{Q}})$ and $\hat{h}(P) = 0$ if and only if P is a torsion point.

(ii) $\hat{h}(nP) = n^2 \hat{h}(P)$ for all $P \in E(\bar{\mathbb{Q}})$ and all integers n.

(iii) The function $(P, Q) \mapsto \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$ is a non-degenerate bilinear form on the real vector space $E(\bar{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{R}$.

(iv) $\hat{h}(P) = h_x(P) + O(1)$

(v) For each $A \in E(\bar{\mathbb{Q}})$, there exists a bounded function denoted $O_A(1)$ such that for all $P \in E(\bar{\mathbb{Q}})$, $\hat{h}(P + A) = \hat{h}(P) + O_A(1)$.

Note that from (iv) it easily follows the finiteness of points of bounded height which are defined over a fixed number field.

2.2 The Chevalley-Weil and Mordell-Weil theorems

Let X, Y be algebraic varieties defined over a number field κ, and let $F : X \to Y$ be a morphism, also defined over κ. Then each κ-rational point $p \in X(\kappa)$ will be sent to a κ-rational point $F(p) \in Y(\kappa)$.

If the morphism F is (generically) finite of degree d, the pre-image of a rational point in Y is (generically) formed by d algebraic points; one expects that in fact these points have degree d and consequently form a unique orbit for the Galois action of $\mathcal{G}al(\bar{\kappa}/\kappa)$. [4] However, there are cases of morphisms $F : X \to Y$ of degree > 1 between irreducible varieties, with $Y(\kappa)$ Zariski-dense, when the pre-images of rational points will automatically be rational, or at least they will be all together defined on a finite degree extension of κ.

[4] The so called Hilbert Irreducibility Theorem asserts precisely that for a κ-rational variety Y and a generically finite morphism $F : X \to Y$ there always exists a Zariski-dense set of rational points of Y whose pre-images consist of a single Galois orbit. See [14], Ch. 4 or [23], Ch. III.

This happens when the morphism is unramified, and is the content of the Chevalley-Weil theorem below.

Since we are interested only on varieties in characteristic zero, we give a topological definition of unramified morphism. We say that a morphism $F : X \to Y$ between smooth quasi-projective varieties over a field $\kappa \subset \mathbb{C}$ is unramified if the corresponding continuous map $X(\mathbb{C}) \to Y)\mathbb{C})$ is a covering in the topological sense. In particular, each point $p \in Y(\mathbb{C})$ admits exactly $\deg F$ pre-images.

The mentioned theorem of Chevalley and Weil (which can be found in this formulation e.g. in [14], Ch. 5 or [23], Chap. III, §2) , reads:

Theorem 2.3 (Chevalley-Weil). *Let $F : X \to Y$ be un unramified morphisim between smooth quasi-projective varieties over a number field κ. Then*

- *there exists a number field κ' such that for each point $p \in X(\bar{\kappa})$ with $F(p) \in Y(\kappa)$, p lies in $X(\kappa')$.*
- *there exist finitely many κ-varieties $X^{(i)}$, $i = 1, \ldots, n$, and morphisms $F_i : X_i \to X$ defined over κ such that: (a) for each $i = 1, \ldots, n$ there exists an isomorphism $G_i : X^{(i)} \to X$, defined over $\bar{\kappa}$, with $F \circ G_i = F_i$ and (b)*

$$Y(\kappa) = \bigcup_{i=1}^{n} F_i(Y(\kappa)).$$

A typical example is provided by isogenies between algebraic groups; other examples in the compact case, which necessarily concern higher dimensions, are provided in [23], Ch. III, §8.

In the affine case, a crucial instance is provided by isogenies of linear tori. Take for instance the squaring map $\mathbb{G}_m \to \mathbb{G}_m$ sending $x \mapsto x^2$. The variety $\mathbb{G}_m = \mathbb{P}_1 - \{0, \infty\}$ is affine and its integral points, over a ring of S-units $\mathcal{O}_S$, form the group of units $\mathcal{O}_S^*$. As a consequence of Dirichlet's unit theorem, this group is finitely generated, hence its subgroup of squares has finite index. It follows that there exist units $\epsilon_1, \ldots, \epsilon_k \in \mathcal{O}_S^* = \mathbb{G}_m(\mathcal{O}_S)$ such that each element of $\mathbb{G}_m(\mathcal{O}_S)$ is of the form $\epsilon_i u^2$ for some $u \in \mathbb{G}_m(\mathcal{O}_S)$. Then the two conclusions of Theorem 2.3 easily follow: the first one by putting $\kappa' = \kappa(\sqrt{\epsilon_1}, \ldots, \sqrt{\epsilon_k})$; the second one by taking $X_i = \mathbb{G}_m$ for each $i = 1, \ldots, k$ and $F_i : X_i \to \mathbb{G}_m$ being the morphism $F_i(x) = \epsilon_i x^2$.

An example of this kind in the compact case is provided by elliptic curves. Start with the Legendre model of an elliptic curve E

$$y^2 = x(x-1)(x-\lambda),$$

where $\lambda \in \kappa - \{0, 1\}$, κ being a number field. Let us choose a finite set of places S so large that it contains the archimedean places and λ and $1 - \lambda$ are both units. Then for each rational point $(a, b) \in E(\kappa)$ and each valuation ν outside S the ν-adic valuation of a and of $a - 1$ is even. Then the square roots of a and of $a - 1$ generate an extension of κ which is unramified at ν. Since, by Minkowski's theorem, there are only finitely extensions of fixed degree and unramified outside a given finite set, all the square roots of a and $a - 1$ lie in a number field κ'.

The Chevalley-Weil Theorem is the first tool in the proof of the finite generation of the group of rational points on an elliptic curve (Mordell-Weil theorem). The second tool is the theory of heights on elliptic curves (Néron-Tate height).

We can now prove the Mordell-Weil Theorem. Fix an elliptic curve E over a number field κ. Consider the multiplication-by-2 map $E \to E$; being an unramified cover of E, we can apply the Chevalley-Weil theorem deducing the existence of finitely many κ-twists of this morphism such that each rational point on E lifts to at least one of them. In concrete terms, there exist finitely many points $A_1, \ldots, A_k \in E(\kappa)$ such that each rational point $P \in E(\kappa)$ is of the form $P = A_i + 2Q_i$, for some rational point $Q \in E(\kappa)$.

From properties (ii) and (v) of the canonical height it follows that there exists a number H such that whenever $\hat{h}(P) > H$ and $P = 2Q + A$, $\hat{h}(Q) < \hat{h}(A)$. Let now $\Gamma \subset E(\kappa)$ be the subgroup generated by $A_1, \ldots, A_k$ and all rational points of height $\leq H$. We claim that this group coincides with $E(\kappa)$. Actually, suppose not and let P be the rational point of smallest height outside Γ. Then $\hat{h}(P) > H$ and so P can be written as $P = 2Q + A$ with $A \in \Gamma$ and $\hat{h}(Q) < \hat{h}(P)$, so that, by minimality of P, also Q must belong to Γ. Then P too belongs to Γ, and this contradiction concludes the proof.

2.3 Diohantine approximation on the line

In this section, we present without proof classical material about Diophantine approximation, mainly following [14]. More details and complete proofs can be found for instance in [57], [58], [8], [12].

We are primarly interested in the rational approximation to algebraic numbers; more precisely, we are interested in estimating the accuracy in the approximation to such numbers with respect to the denominator of the approximant. The following theorem gives the best possible result for an arbitrary irrational number.

Theorem 2.4 (Dirichlet). *Let $\alpha \in \mathbb{R} - \mathbb{Q}$ be a real irrational number. There exist infinitely many rational numbers a/b (a, b coprime integers, $b > 0$) such that*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

For instance, one can take for a/b the truncated continued fraction expansion of α.

Some irrational numbers can be approximated to a higher degree; for instance, Liouville's number $\alpha := \sum_{n=1}^{\infty} 10^{-n!}$ has the property that for every positive μ there exist infinitely many rationals a/b (a, b coprime integers, $b > 0$) such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^\mu}.$$

Such numbers are never algebraic; actually, a theorem of Liouville, admitting an elementary proof, states that:

Theorem 2.5 (Liouville). *Let α be a real irrational algebraic number of degree d over $\mathbb{Q}$. There exists a positive number $c(\alpha)$ such that for all rational numbers a/b*

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{c(\alpha)}{b^d}.$$

A theorem due to Roth (1955) [54], which is much harder to prove, improves on Liouville's exponent d:

Theorem 2.6 (Roth's Theorem)**.** *Let α be a real algebraic number, $\epsilon > 0$. For all but finitely many rational numbers a/b, the following inequality holds:*

$$\left|\alpha - \frac{a}{b}\right| > \frac{1}{b^{2+\epsilon}}. \tag{2.7}$$

In an other formulation: if α is algebraic irrational, there exists a positive real number $c(\alpha, \epsilon)$ such that *for all* rational numbers a/b,

$$\left|\alpha - \frac{a}{b}\right| > \frac{c(\alpha, \epsilon)}{b^{2+\epsilon}}. \tag{2.8}$$

Roth's proof is ineffective, in the sense that it does not provide any means of finding the finitely many rational numbers a/b which violate the inequality (2.7). Looking at its second formulation, by the ineffective nature of Roth's proof it is not possible to calculate the function $c(\alpha, \epsilon)$.

Roth's theorem is best possible as far as the exponent is concerned in view of the mentioned result of Dirichlet (Theorem 2.4). However, one can try to improve on Roth's exponent after restricting the approximations to suitable classes of rational numbers. For instance, one can consider the set of rational numbers which, once written in base ten, have only finitely many digits. These numbers form the ring of S-integers $\mathbb{Z}[\frac{1}{10}] = \mathbb{Z}[\frac{1}{2}, \frac{1}{5}]$.

For these approximations, Ridout [50] improved Roth's bound by proving that: for every irrational algebraic number α and every positive real $\epsilon > 0$, there are only finitely many pairs of integers $(a, n) \in \mathbb{Z} \times \mathbb{N}$ such that $|\alpha - \frac{a}{10^n}| < 10^{-(1+\epsilon)n}$.

A similar result holds whenever the numerators of the approximations are supposed to be of special type, e.g. products of powers of primes from a fixed finite set. When both numerators and denominators are subject to lie in a finitely generated multiplicative semi-group, then the exponent can be lowered to "ϵ" (see Corollary 2.13).

In another direction, one can try to replace the rational number field $\mathbb{Q}$ by an arbitrary number field $\kappa \subset \mathbb{C}$. Of course, the expected exponent should change; for instance, if $\kappa \subset \mathbb{R}$ and has degree $d = [\kappa : \mathbb{Q}]$ over the rational, a variation of Dirichlet's theorem asserts that each real number $\alpha \in \mathbb{R} - \kappa$ can be approximated to a degree $-2d$ with respect to the "height" of the approximant (see below for the precise definition of height).

However, our care in chosing the normalization of absolute values and heights assure that, with respect to our choice, the exponent in Roth's theorem remains the same, as in the following statement:

Theorem 2.9. *Let κ be a number field, ν be a place of κ and $\alpha \in \kappa_\nu$ be an element of the topological closure of κ, algebraic over κ but not lying in κ. Let $\|\cdot\|_\nu$ denote the absolute value normalized with respect to κ and extended to κ_ν. Then for every positive real number $\epsilon > 0$ there exists a number $c(\alpha, \nu, \epsilon)$ such that for all $\beta \in \kappa$*

$$|\alpha - \beta|_\nu > c(\alpha, \nu, \epsilon) \cdot H(\beta)^{-2-\epsilon}.$$

Let us consider the particular case where ν is archimedean and $\kappa \subset \kappa_\nu = \mathbb{R}$. While generic real numbers can be approximated by a sequence of rationals with an error bounded by Dirchlet's Theorem, we expect that using as approximants elements of κ instead of only rational numbers the degree of approximability of any real number will increase. Since κ is a vector space of

dimension $[\kappa : \mathbb{Q}]$ over $\mathbb{Q}$, it should be possible to make the error in the approximation as little as the height of the approximant to the power $-2[\kappa : \mathbb{Q}]$. Actually this is true, and can be proved via the classical pigeon-hole principle. However, in Theorem 2.9 above the usual exponent 2 appears; taking into consideration our normalization, the same inequality written with respect to the usual real absolute value would show precisely the exponent $-2[\kappa : \mathbb{Q}]$; so Theorem 2.9 states that for algebraic numbers no improvement on Dirichlet's exponent can be obtained.

The most general version of Roth's Theorem, encompassing both Ridout's theorem and the above Theorem 2.9, was formulated by Lang in [44]:

Theorem 2.10. *Let κ be a number field; let S be a finite set of places of κ. Let, for every $\nu \in S$, $|\cdot|_\nu$ be the extension of the ν-adic absolute value to κ_ν, normalized with respect to κ and let $\alpha_\nu \in \kappa_\nu$ be an algebraic number. For every $\epsilon > 0$ there exists a number $c = c(S, (\alpha_\nu)_{\nu \in S}, \epsilon)$ such that for all $\beta \in \kappa$ with $\beta \neq \alpha_\nu$ for every $\nu \in S$,*

$$\prod_{\nu \in S} |\alpha_\nu - \beta|_\nu > c \cdot H(\beta)^{-2-\epsilon}.$$

Notice that interesting cases arise when some, or even all, the α_ν lie in κ. Indeed, another equivalent formulation of the general Roth's Theorem 2.10 involves only κ-rational points. It appears e.g. in [12] and reads as follows:

Theorem 2.11. *Let κ be a number field, $d \geq 1$ an integer, $\alpha_1, \ldots, \alpha_d$ be pairwise distinct elements of κ. Let $S_1, \ldots, S_d$ be pairwise disjoint finite sets of absolute values. Finally, let $\epsilon > 0$ be a positive real number. Then for all but finitely many elements $\beta \in \kappa$,*

$$\prod_{h=1}^{d} \prod_{\nu \in S_h} |\alpha_h - \beta|_\nu > H(\beta)^{-2-\epsilon}. \tag{2.12}$$

(

The above theorem can be further generalized, by allowing also points at infinity as target of the approximation. This will be useful in order to deduce the mentioned theorem of Ridout. Precisely, for $\alpha = \infty$ and any absolute value ν, let us define the ν-adic distance from α to $\beta \in \kappa$, provided $\beta \neq 0$, by putting

$$|\alpha - \beta|_\nu = |\infty - \beta|_\nu := |\beta|_\nu^{-1}.$$

Then the condition that a rational number $\beta \in \mathbb{Q}$ be of the form $\beta = a/b$ where b is a product of primes from a fixed set T can be expressed by the inequality $\prod_{\nu \in T} |\beta - \infty|_\nu \leq |b|^{-1}$; if $|\beta| \leq 1$ we also have $H(\beta) = |b|$ so the arithmetic condition that β lies in a fixed ring of S integers is equivalent to the inequality

$$\prod_{\nu \in T} \min(1, |\beta - \infty|_\nu) \leq H(\beta)^{-1},$$

where $T \subset S$ is the set of ultrametric places in S.

Actually, the generalization of Theorem 2.11 with one point α allowed to be at infinity follows formally from the present version of Theorem 2.11 itself: observe that applying projective transformations $\Phi : \mathbb{P}_1 \to \mathbb{P}_1$ of the form

$$\Phi(x) = \frac{ax + b}{cx + d},$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\kappa)$ one can send the given set of target points $\{\alpha_\nu\}_{\nu \in S} \subset \mathbb{P}_1(\kappa) = \kappa \cup \{\infty\}$ to a subset of $\kappa = \mathbb{P}_1(\kappa) - \{\infty\}$.

For instance, in the special case in which the set of $\{\alpha_\nu, \nu \in S\}$ consists of the three rational points $0, 1, \infty \in \mathbb{P}_1(\kappa)$, the above Theorem 2.11 implies:

Corollary 2.13. *Let $\Gamma \subset \kappa^*$ be a finitely generated multiplicative group. Let T be a finite set of places of κ and $\epsilon > 0$ a positive real number. Then for all but finitely many $\gamma \in \Gamma$*

$$\prod_{\nu \in T} |\gamma - 1|_\nu > H(\gamma)^{-\epsilon}. \tag{2.14}$$

The proof of the deduction from Theorem 2.11 can be found e.g. in [14], Ch. II.

In the rational case, we state the following further corollaries:

Corollary 2.15 (Theorem of Ridout)**.** *Let $\{p_1, \ldots, p_l\}, \{q_1, \ldots, q_m\}$ be two set of prime numbers; let λ, μ be real numbers in the closed interval $[0, 1]$. Let us consider the set $\mathcal{B}$ of rational numbers β of the form $\beta = p/q$ where*

$$\begin{aligned} p &= p_1^{a_1} \cdots p_l^{a_l} \cdot p^* \\ q &= q_1^{b_1} \cdots q_m^{b_m} \cdot q^* \end{aligned}$$

where $a_1, \ldots, a_l, b_1, \ldots, b_m$ are integers with $a_i \geq 0, b_j \geq 0$ and p^*, q^* satisfy

$$\begin{aligned} p^* &\leq p^{1-\lambda} \\ q^* &\leq q^{1-\mu} \end{aligned}$$

Let $\alpha \in \mathbb{R}$ be a real algebraic number and let $\epsilon > 0$ be a positive real number. Then for all but finitely many $\beta \in \mathcal{B}$,

$$|\alpha - \beta| > H(\beta)^{-2+\lambda+\mu-\epsilon}.$$

Corollary 2.16. *Let p be a prime number, $\alpha \in \mathbb{Z}_p$ a p-adic algebraic integer. For every $\epsilon > 0$ there exist only finitely many integers $n \in \mathbb{Z}$ such that*

$$|n - \alpha|_p < |n|^{-1-\epsilon}.$$

We end this section by providing yet another version of Roth's theorem; we shall present it as a lower bound for *homogeneous* linear form.

Theorem 2.17 (Homogeneous Roth's Theorem)**.** *Let κ be a number field, S be a finite set of absolute values of κ. For each $\nu \in S$, let $L_{1,\nu}(X, Y), L_{2,\nu}(X, Y)$ be linearly independent linear forms with coefficients in κ. Finally, let $\epsilon > 0$ be a positive real number. For all but finitely many $(x : y) \in \mathbb{P}_1(\kappa)$ the following inequality holds:*

$$\prod_{\nu \in S} \frac{|L_{1,\nu}(x, y)|_\nu}{\max(|x|_\nu, |y|_\nu)} \cdot \frac{|L_{2,\nu}(x, y)|_\nu}{\max(|x|_\nu, |y|_\nu)} > H(x/y)^{-\epsilon}. \tag{2.18}$$

Note that, due to the appearance of the denominator $\max(|x|_\nu, |y|_\nu)$, the left hand-side term is invariant by multiplication of x and y by a non-zero constant, so it only depends on the projective class $(x : y)$ of (x, y). This is consistent with the right-hand side term, which only depends on the ratio x/y.

The left-hand side term in the inequality of Theorem 2.17 can be viewed as the product of distances from the approximating points $(x : y) \in \mathbb{P}_1(\kappa)$ to the points defined by the vanishing of the linear forms $L_{1,\nu}, L_{2,\nu}$.

If $Q = (a : b) \in \mathbb{P}_1(\kappa)$ is a point and $L(x, y) = bx - ay$ is a linear form vanishing on $(a : b)$, we can define the distance between a point $P := (x : y) \in \mathbb{P}_1$ and the point Q to be

$$\mathrm{dist}_\nu(P, Q) = \frac{|L(x, y)|_\nu}{\max(|x|_\nu, |y|_\nu)}. \tag{2.19}$$

Of course this quantity depends on the chosen equation for Q, but this choice affects the outcome just by a multiplicative constant independent of P.

Coming back to Theorem 2.17, where for each place ν two ν-adic linear forms are involved, let us remark that by the triangle's inequality, only one of the linear forms can be "small" at one single point $(x : y)$. If Q_1, Q_2 are the zeros of $L_1(X, Y), L_2(X, Y)$ respectively, and the sequence $(x : y)$ converges to Q_1, then asymptotically $\frac{|L_2(x,y)|_\nu}{\max(|x|_\nu,|y|_\nu)} \to \mathrm{dist}_\nu(Q_1, Q_2) > 0$.

Hence Theorem 2.17 can be rephrased by saying that given rational points Q_ν for $\nu \in S$, for all $\epsilon > 0$ the lower bound

$$\prod_{\nu \in S} \mathrm{dist}_\nu(P, Q_\nu) > H(P)^{-2-\epsilon}$$

holds for all but finitely many rational points $P \in \mathbb{P}_1(\kappa)$.

2.4 Diophantine approximation on elliptic curves

Given an elliptic curve E over a number field κ, and a place ν of κ, one can define a distance on the compact topological $E(\kappa_\nu)$. Several possibilities are available, all being equivalent for our purposes: one can for instance define a metric in the projective plane $\mathbb{P}_2(\kappa_\nu)$ and take the induced one on $E(\kappa_\nu)$. Alternatively, if the place ν is archimedean, and corresponds to an embedding $\kappa \hookrightarrow \mathbb{C}$ of κ into the complex number field $\mathbb{C}$, one can view $E(\mathbb{C})$ as a quotient $\mathbb{C}/\Lambda$ of the complex plane $\mathbb{C}$ by a lattice Λ and define locally the metric as the one induced from the archimedean metric in $\mathbb{C}$. In any case, given a sequence $\{P_n\}_{n\in\mathbb{N}}$ in E, converging ν-adically to a point $Q \in E(\kappa_\nu)$, a distance will be fixed in a neighborhood of Q in such a way that for a local parameter t at Q,

$$|t(P_n)|_\nu \ll \mathrm{dist}(P_n, Q) \ll |t(P_n)|_\nu.$$

Now, the standard Roth's theorem on the line, e.g. in the version of Theorem 2.6, immediately provides a lower bound of the form

$$\mathrm{dist}(P_n, Q) \gg H(P_n)^{-2-\epsilon} \tag{2.20}$$

for every sequence P_n converging (in an archimedean place, say) to an algebraic target.

Since the Euler characteristic of an elliptic curve is 0, while for the projective line $\mathbb{P}_1$ it is -2, it is natural that the exponent $-2 - \epsilon$ of Roth's Theorem is replaced in the elliptic case by a $-\epsilon$ exponent.

This refined inequality can in fact be proved, by combining the Mordell-Weil Theorem with Roth's Theorem:

Theorem 2.21. *Let E be an elliptic curve over a number field κ, ν a valuation of κ and $Q \in E(\kappa_\nu)$ be an algebraic point. For every $\epsilon > 0$ there exists a real number $c > 0$ such that for every point $P \in E(\kappa)$, $P \neq Q$,*

$$\mathrm{dist}_\nu(P, Q) \geq c \cdot H(P)^{-\epsilon}. \tag{2.22}$$

Proof. Let $\epsilon > 0$ be given. Suppose by contradiction that (2.22) does not hold for any real number $c > 0$. Then in particular there would exist infinitely many rational points $P \in E(\kappa)$ such that

$$\mathrm{dist}_\nu(P, Q) < H(P)^{-\epsilon}. \tag{2.23}$$

Choose an integer $m > 0$ such that

$$\frac{3}{m^2} < \epsilon. \tag{2.24}$$

Since the quotient group $E(\kappa)/mE(\kappa)$ is finite, we can find a point $F \in E(\kappa)$ and infinitely many solutions P to (2.23) of the form $P = F + mP'$, for some $P' \in E(\kappa)$. By compactness of the topological group $E(\kappa_\nu)$, there exists a number $c_1 > 1$ such that

$$c_1^{-1}\mathrm{dist}_\nu(mP', Q - F) < \mathrm{dist}_\nu(F + mP', Q) < c_1\mathrm{dist}_\nu(mP', Q - F),$$

so that the solutions to (2.23) with $P = F + mP'$ give rise to solutions to the equation

$$\mathrm{dist}_\nu(mP', Q - F) < c_1 H(P)^{-\epsilon}.$$

Let now $Q_1, \ldots, Q_{m^2} \in E(\bar{\kappa})$ be the solutions X to the equation $mX = Q - F$; if a sequence of points of the form mP' converges to $Q - F$, then the corresponding sequence of the points P' admits a subsequence converging to one of the points $Q_1, \ldots, Q_{m^2}$ (after suitably extending the valuation ν to $\bar{\kappa}$). Choose one such point $Q' \in \{Q_1, \ldots, Q_{m^2}\} \cap E(\kappa_\nu)$. Since the map $E(\kappa_\nu) \ni X \mapsto mX \in E(\kappa_\nu)$ is unramified, we have (using again the compactness of $E(\kappa_\nu)$) that for some number $c_2 > 1$

$$c_2^{-1}\mathrm{dist}_\nu(P', Q') \leq \mathrm{dist}_\nu(mP', Q - F) \leq c_2\mathrm{dist}_\nu(P', Q').$$

Then the solutions to (2.23) give rise to infinitely many solutions to the equation

$$\mathrm{dist}_\nu(P', Q') \leq c_3 H(P)^{-\epsilon} = c_3 H(mP' + F)^{-\epsilon},$$

for some real number c_3. But we now from the properties of the Néron-Tate height, there exist a number $c_4 = c_4(F)$, independent of P', such that

$$c_4^{-1}H(P')^{m^2} \leq H(mP' + F) \leq c_4 H(P')^{m^2}.$$

From the above inequalities and (2.24) it follows that $H(P)^\epsilon = H(mP' + F)^\epsilon > c_4^{-1}H(P')^3$, so from the infinitude of the set of solutions to (2.23) we obtain infinitely many solutions to the inequality $\mathrm{dist}_\nu(P', Q') < c_5 H(P')^{-3}$, for some fixed number c_5, contradicting (2.20). □

The above proof carries out also on the multiplicative group, giving rise to an alternative proof of Theorem 2.13, which can be formally deduced from Roth's Theorem 2.6 (making use of the finite generation of the group of S-units). Also, a weeker version of Roth's Theorem would be sufficient; actually, the first proof of 2.13 is due to Gelfond [36], who already in 1952 proved the inequality (2.14), using an approximation result of his own in place of the yet unavailable Roth's Theorem.

Once again, the exponent $-\epsilon$ appearing in (2.14) instead of $-2 - \epsilon$ is justified by the fact that the Euler characteristic of $\mathbb{G}_m$ is 0.

2.5 The gap principle on the line and on elliptic curves

The so-called gap principle in Diophantine approximation is the elementary but crucial fact that the ratio of the heights of two "very good" rational approximations to a single real number can be bounded from below (see inequality (2.25)). An important theorem of Mumford, which constitutes a first step toward the Vojta-Bombieri proof of Mordell's conjecture (see e.g. [8]), provides a compact analogue to that inequality.

Suppose we have two rational numbers p_1/q_1, p_2/q_2, where p_1, q_1 (resp. p_2, q_2) are coprime integers, with $0 < q_1 < q_2$ and suppose that $\alpha \in \mathbb{R}$ is a real number. If for some exponent $\mu > 0$ the two inequalities

$$\left|\alpha - \frac{p_1}{q_1}\right| < \frac{1}{q_1^\mu}, \qquad \left|\alpha - \frac{p_2}{q_2}\right| < \frac{1}{q_2^\mu}$$

then by the triangle's inequality

$$\left|\frac{p_1}{q_1} - \frac{p_2}{q_2}\right| < \frac{1}{q_1^\mu} + \frac{1}{q_2^\mu} \leq \frac{2}{q_1^\mu}.$$

Writing the left-hand side above with a common denominator, one obtains

$$\frac{|p_1 q_2 - p_2 q_1|}{q_1 q_2} < \frac{2}{q_1^\mu}.$$

On the other hand, the determinant at the numerator is non-zero, due to the fact that the approximations $p_1/q_1, p_2/q_2$ are distinct, so its absolute value is at least 1. We deduce

$$q_2 > \frac{1}{2} \cdot q_1^{\mu-1}. \tag{2.25}$$

Now, *if the exponent μ satisfies $\mu > 2$* the inequality is non-trivial and leads to the following:

Theorem 2.26 (Gap Principle)**.** *Let $\alpha \in \mathbb{R}$ be any real number. Let $\mu > 2$ be a real number and $p_1/q_1, p_2/q_2, \ldots$ a sequence of rational numbers with $0 < q_1 < q_2 < \ldots$, satisfying for all $n = 1, 2, \ldots$*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^\mu}.$$

Then

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

We remark at once that we do not suppose that the target α is algebraic. Also, the result remains true, but trivial, if $\mu \leq 2$, whenever when $\mu > 2$ it says that the sequence of the approximations grows at least exponentially with n. Note that we are considering approximations by rational numbers, i.e. by points on $\mathbb{P}_1$, and that $\chi(\mathbb{P}_a) = -2$; this is the reason why the result requires $\mu > 2$ to be non-trivial.

The p-adic versions of Roth's theorem also admit corresponding gap principles. Take a prime number p; Theorem 2.9 states that for every algebraic p-adic number $\alpha \in \mathbb{Q}_p$ and every $\epsilon > 0$, there are only finitely many rational solutions a/b, $a, b \in \mathbb{Z}$, $b \neq 0$, to the inequality

$$\left|\alpha - \frac{a}{b}\right|_p < \max(|a|, |b|)^{-2-\epsilon}$$

Take now an arbitray p-adic number α, possibly transcendental. Then the above inequality can admit infnitely many solutions. However, given two solutions $a_1/b_1, a_2/b_2$ with $\max(|a_1|, |b_1|) < \max(|a_2|, |b_2|)$ to the above inequality, we obtain that

$$|a_2 b_1 - a_1 b_2|_p < \max(|a_1|, |b_1|)^{-2-\epsilon}$$

while clearly $|a_2 b_1 - a_1 b_2| \leq 2\max(|a_1|, |b_1|) \cdot \max(|a_2|, |b_2|)$. It follows from the product formula (i.e. from the fact that no power of p cannot divide any non-zero number which is smaller than that power) that

$$\max(|a_1|, |b_1|)^{-2-\epsilon} \cdot 2\max(|a_1|, |b_1|) \cdot \max(|a_2|, |b_2|) \geq 1$$

i.e. $\max(|a_2|, |b_2|) > \frac{1}{2}\max(|a_1|, |b_1|)^{1+\epsilon}$. This is the sought gap inequality.

If, on the other hand, we are interested in approximating a p-adic integer $\alpha \in \mathbb{Z}_p$ by rational integers, as it was the case in Corollary 2.16 to Ridout's theorem, we shall consider an inequality of the type

$$|\alpha - m|_p < |m|^{-1-\epsilon}, \tag{2.27}$$

to be solved in integers. Suppose $0 < m < n$ are two solutions. From the (ultra-metric) triangle's inequality we obtain

$$|n - m| \leq m^{-1-\epsilon}.$$

On the other hand, the maximal power of p dividing the non-zero integer $n - m$ cannot exceed $n - m$. We then obtain

$$n - m > m^{1+\epsilon},$$

so in particular $n > m^{1+\epsilon}$.

The difference between the two last situations is that the approximating numbers in the second case are integers, so they are automatically close to infinity in the infinite place of $\mathbb{Q}$.

From another view point, we are doing approximation on the affine line, which has Euler characteristic -1, hence the gap principle only requires inequality (2.27) to give a non-trivial conclusion.

A generalization, involving several places and arbitrary number fiels, reads as follows:

Theorem 2.28. *Let κ be a number field, S a finite set of places of k. For each place $\nu \in S$, let α_ν be a point in $\kappa_\nu$and μ_ν a positive real number. Suppose that*

$$\sum_{\nu \in S} \mu_\nu = 2 + \epsilon > 2.$$

Let $\beta_1, \beta_2 \in \kappa$ be two solutions of the system of inequalities

$$|\alpha_n u - \beta|_\nu < \max(1, |2|_\nu)^{-1} \cdot H(\beta)^{-\mu_\nu} \tag{2.29}$$

with $0 < h(\beta_1) \leq h(\beta_2)$. If $\beta_1 \neq \beta_2$ then $h(\beta_1) < h(\beta_2)$ and

$$\frac{h(\beta_2)}{h(\beta_1)} \geq 1 + \epsilon.$$

The proof mimics the three particular cases already analyzed. From this result, one can deduce a gap principle for the solutions to the slightly different inequality of the form appearing in Theorem 2.10. Namely one can prove the following

Corollary 2.30. *Let κ, S be as above, and for each $\nu \in S$, α_ν be as before a point in the completion κ_ν. Let $\epsilon > 0$ be a real number. Let $\beta_1, \beta_2, \ldots$ be a sequence of rational points in κ with $h(\beta_1) \leq h(\beta_2) \leq \ldots$ satisfying*

$$\prod_{\nu \in S} |\alpha_\nu - \beta|_\nu < H(\beta)^{-2-\epsilon}. \tag{2.31}$$

Then there exists a real number $\delta > 0$ and an integer $N = N(|S|, \epsilon, \delta)$ such that for all large integers n

$$\frac{h(\beta_{n+N})}{h(\beta_n)} > 1 + \delta.$$

The idea for deducing Corollary 2.30 from Theorem 2.28 is that the inequality (2.31) implies one of the finitely many systems of inequalities like (2.29), up to "shrinking ϵ". The details, in quantitative form, appear e.g. in §3.4 of [12]. Clearly, doubling N one can replace δ by $2\delta + \delta^2 = (1+\delta)^2 - 1$, so the conclusion of the Corollary holds for every δ.

As mentioned in the introduction and just explained above, the reason for the exponent -2 in equation (2.31) is that the approximation takes place on the projective line, whose Euler characteristic is precisely -2.

It is then natural to expect that on elliptic curve the exponent can be lowered to "$0 + \epsilon$"; actually, given a reasonable notion of distance on elliptic curves (see after the statement of the theorem for a precise definition) one expects the following theorem to hold:

Theorem 2.32. *Let E be an elliptic curve over a number field κ. Let ν be a place of κ and $A \in E(\kappa_\nu)$ be a point defined over the corresponding completion κ_ν. Let $\epsilon > 0$ be a positive real number and let $P_1, P_2, \ldots \in E(\kappa)$ be a sequence of κ-rational points of E satisfying $h(P_1) < h(P_2) < \ldots$ and*

$$\mathrm{dist}_\nu(A, P_n) < H(P_n)^{-\epsilon} \tag{2.33}$$

for all $n = 1, 2, \ldots$. Then there exist an integer $N \geq 1$ and a real $\delta > 0$ such that for all n

$$\frac{h(P_{n+N})}{h(P_n)} > 1 + \delta.$$

As for Corollary 2.30, the conclusion could be rephrased by saying that *for every positive number C there exists an integer N such that for all solutions $P_1, P_2, \ldots$ to the inequality* (2.33) *(ordered by increasing height), $h(P_{n+N}) > C \cdot h(P_n)$.*

We provide a detail proof of Theorem 2.32, since we cannot locate this statement, nor its proof, anywhere in the literature.

We start by proving the following Proposition, from which Theorem 2.32 will follow rather formally:

Proposition 2.34. *Let E be an elliptic curve over a number field κ, ν a valuation of κ and $A \in E(\kappa_\nu)$ and $m \geq 2$ an integer number. Let $\epsilon > 0$ be a positive real number, $m > 0$ a positive*

integer. There exists a number $c = c(E, \nu, m, \epsilon)$ such that for all rational points $P, Q \in E(\kappa)$ with $\mathrm{dist}_\nu(A, P) < H(P)^{-\epsilon}$, $\mathrm{dist}_\nu(A, Q) < H(Q)^{-\epsilon}$ and $\hat{h}(P) < \hat{h}(Q)$, $P - Q \in mE(\kappa)$, then

$$\frac{\hat{h}(Q)}{\hat{h}(P)} \geq \epsilon m^2 - 1 + \frac{c}{\hat{h}(P)}.$$

The result is non-trivial whenever $\epsilon m^2 > 2$, i.e. for all sufficiently large values of m.

Proof. By assumption, there exists a rational point $B \in E(\kappa)$ such that P, Q can be written in the form

$$P = B + mP', \qquad Q = B + mQ',$$

for rational points $P', Q' \in E(\kappa)$. In the sequel of the proof, we let $C_1, C_2, \ldots$ denote numbers ('multiplicative constants') depending only on E, m and ν (as well as, of course, on the notion of ν-adic distance). By the properties of distances and of heights, we have

$$\mathrm{dist}_\nu(A, mP' + B) < H(mP' + B)^{-\epsilon} \Rightarrow \mathrm{dist}_\nu(A - B, mP') < C_1 \cdot H(mP' + B)^{-\epsilon} < C_2 H(mP'),$$

and analogously for Q, so we have also $\mathrm{dist}_\nu(A - B, mQ') < C_2 H(mQ')^{-\epsilon}$. By the triangle's inequality, the fact that $\hat{h}(P) < \hat{h}(Q)$ and the fact that the naive and canonical height differ by a bounded function, we obtain

$$\mathrm{dist}_\nu(mP', mQ') < C_3 \cdot \exp(\hat{h}(P))^{-\epsilon} \tag{2.35}$$

Now, since the multiplication-by-m map is unramified, we have $\mathrm{dist}_\nu(mP', mQ') \geq \mathrm{dist}_\nu(P', Q')$. Also, by the Liouville's inequality, $\mathrm{dist}_\nu(P, Q) \geq C_4 (H(P')H(Q'))^{-1} \geq H(Q)^{-2}$. Taking logarithms, and replacing again the naive with the canonical height, we obtain

$$-\log(\mathrm{dist}_\nu(P, Q)) \leq (\hat{h}(P') + \hat{h}(Q')) + \log C_5 = \frac{\hat{h}(P) + \hat{h}(Q)}{m^2} + \frac{\log C_5}{m^2}.$$

Comparing with 2.35, we get

$$\epsilon \hat{h}(P) \leq \frac{\hat{h}(P) + \hat{h}(Q)}{m^2} + c,$$

with $c = (\log C_5)/m^2 - \log C_3$. Dividing by $\hat{h}(P)$ we obtain the conclusion. □

Proof of Theorem 2.32. We can now finish the proof of the elliptic Gap Principle (Theorem 2.32). Let $m > 1$ be an integer such that $m^2 \epsilon > 2$. We let $\{A_1, \ldots, A_h\}$ be a set of representatives of $E(\kappa)$ modulo $mE(\kappa)$. Set $N = h$; then in every finite sequence $P_n, P_{n+1}, \ldots, P_{n+N}$ of rational points in $E(\kappa)$ there are two points $P_i =: P$ and $P_j =: Q$, with $n \leq i < j \leq n + N$ such that $P - Q$ is divisible by m in $E(\kappa)$. Any lower bound for the ratio $\hat{h}(Q)/\hat{h}(P)$ applies *a fortior* to the ratio $\hat{h}(P_{n+N})/\hat{h}(P_n)$. Now, fix a number δ with $0 < \delta < \epsilon m^2 - 2$. Proposition 2.34 provides the lower bound $\hat{h}(Q)/\hat{h}(P) \geq \epsilon m^2 - 1 + \frac{c}{\hat{h}(P)}$ which implies, for large values of $h(P)$, that $\hat{h}(Q)/\hat{h}(P) > (1 + \delta)$, concluding the proof.

3 Higher dimensional Diophantine approximation

In higher dimensions, we shall be interested in approximating hyperplanes defined by linear forms with algebraic coefficients by rational points. We shall adopt the language and notation of projective geometry for simplicity, as in the homogeneous version of Roth's Theorem given in Theorem 2.17.

The main result of this section is the so-called Subspace Theorem, first proved, in a particular case, by W. M. Schmidt in the seventies. Here we formulate the generalization provided by H.-P. Schlickewei, which is the natural extension of Roth's theorem to higher dimension.

We need an extension to higher dimension of the notion of height, already introduced for algebraic numbers.

Let κ be a number field, $\mathbf{x} = (x_0, \ldots, x_N) \in \kappa^{N+1} - \{0\}$ a non-zero vector. For every place ν of κ, its ν-adic norm $\|\mathbf{x}\|_\nu$ is defined to be

$$\|\mathbf{x}\|_\nu = \max(|x_0|_\nu, \ldots, |x_N|_\nu).$$

Let us define the height of the associated projective point, still denoted by $\mathbf{x} = (x_0 : \ldots : x_N) \in \mathbb{P}_N(\kappa)$, to be

$$H(\mathbf{x}) = \prod_\nu \|\mathbf{x}\|_\nu,$$

where the product runs over all the valuations of κ.

With these conventions, Schmidt's Subspace Theorem reads:

Theorem 3.1 (Subspace Theorem)**.** *Let $N \geq 1$ be a positive integer, κ be a number field and S a finite set of places of κ. Let, for every $\nu \in S$, $L_{0,\nu}(X_0, \ldots, X_N), \ldots, L_{N,\nu}(X_0, \ldots, X_N)$ be linearly independent linear forms with algebraic coefficients in κ_ν. Then for each $\epsilon > 0$ the solutions $\mathbf{x} = (x_0 : \ldots : x_N) \in \mathbb{P}_N(\kappa)$ to the inequality*

$$\prod_{\nu \in S} \prod_{i=0}^{N} \frac{|L_{i,\nu}(\mathbf{x})|_\nu}{\|\mathbf{x}\|_\nu} < H(\mathbf{x})^{-N-1-\epsilon} \tag{3.2}$$

lie in the union of finitely many hyperplanes of $\mathbb{P}_N$, defined over κ.

For $N = 1$, the conclusion provides the finiteness of the solutions to the inequality (3.2); so we recover Roth's Theorem. In higher dimension, however, the finiteness conclusion does not hold: for instance, when the point $\mathbf{x}$ lies in the hyperplane defined by the vanishing of one linear form, the left-hand side term in (3.2) vanishes, so the inequality is satisfied. It is worth noticing, however, that the exceptional hyperplanes containing the infinite families of solutions are not necessarily the zero sets of the involved linear forms, as the following example shows:

`Example`. Let α be a real irrational algebraic number, with $0 < \alpha < 1$; consider a "good" rational approximation $p/q \in \mathbb{Q}$ to α. By this we mean that p, q are coprime integers, $q > 0$, and

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

we know from Dirichlet's Theorem that there exist infinitely many of them. Since $\alpha < 1$, for infinitely many good approximations p/q one has $\max(|p|, |q|) = |q|$, so we can write the above inequality as

$$\left|\alpha - \frac{p}{q}\right| < \max(|p|, |q|)^{-2}.$$

For each such pair (p, q) we have the upper bound

$$\frac{|q\alpha - p|}{\max(|p|, |q|)} \leq \frac{|q\alpha - p|}{|q|} < \max(|p|, |q|)^{-2}. \tag{3.3}$$

Now take $N = 2$, $\kappa = \mathbb{Q}$ and S consisting of the archimedean absolute value of $\mathbb{Q}$ and define the three linear forms $L_i(X_0, X_1, X_2)$ $(i = 0, 1, 2)$ as follows:

$$L_0(X_0, X_1, X_2) = X_0 - \alpha X_2, \quad L_1(X_0, X_1, X_2) = X_1 - \alpha X_2, \quad L_2(X_0, X_1, X_2) = X_2.$$

Now, with each good approximation p/q to the number α as above we associate the point $(x_0 : x_1 : x_2) = (p : p : q)$. Then the double product in (3.2) becomes

$$\prod_{\nu \in S} \prod_{i=0}^{N} \frac{|L_{i,\nu}(\mathbf{x})|_\nu}{\|\mathbf{x}\|_\nu} = \left(\frac{|p - q\alpha|}{\max(|p|, |q|)} \right)^2 \cdot \frac{|q|}{\max(|p|, |q|)}.$$

By the above inequality (3.3) and the trivial estimate $|q| \leq \max(|p|, |q|)$, we have the upper bound

$$\prod_{\nu \in S} \prod_{i=0}^{N} \frac{|L_{i,\nu}(\mathbf{x})|_\nu}{\|\mathbf{x}\|_\nu} < \max(|p|, |q|)^{-4},$$

which means that inequality (3.2), with e.g. $\epsilon = 1/2$, admits infinitely many solutions $(x_0 : x_1 : x_2) = (p : p : q)$ on the projective line of equation $X_0 = X_1$. So, the degeneracy conclusion of Theorem 3.1 cannot be replaced by a finiteness one, even after assuming $L_{i,\nu}(\mathbf{x}) \neq 0$.

It will prove useful to have an 'affine version' of the Subspace Theorem, of which Theorem 3.1 represents the projective, or homogeneous, version. Here is such affine version, which can be formally deduced from Theorem 3.1:

Theorem 3.4. *Let κ be a number field, S a finite set of places containing the archimedean ones, $N \geq 2$ an integer. Let, for each $\nu \in S$, $L_{\nu,1}(X_1, \ldots, X_N), \ldots, L_{\nu,N}(X_1, \ldots, X_N)$ be linearly independent linear forms with algebraic coefficients in κ_ν. Then the solutions $(x_1, \ldots, x_N) \in \mathcal{O}_S^N$ to the inequality*

$$\prod_{\nu \in S} \prod_{i=1}^{N} |L_{\nu,i}(\mathbf{x})|_\nu < H(\mathbf{x})^{-\epsilon}$$

lie in the union of finitely many proper linear subspaces of κ^N.

The Subspace Theorem, like Roth's theorem, is ineffective; however, the number of the higher dimensional components of the Zariski-closure of the set of solutions to (3.2) can be bounded (see [30]).

An interesting issue on higher dimensional Diophantine approximation concerns approximation to non-linear hypersurfaces.

Given a hypersurface $D \subset \mathbb{P}_n$, defined by a homogenous equation $F(x_0, \ldots, x_n) = 0$, and a place ν of a field, we can define the distance from a point $P = (p_0 : \ldots, p_n)$ to the hypersurface D relatively to the place ν as

$$\mathrm{dist}_\nu(P, D) = \frac{|F(p_0, \ldots, p_n)|_\nu}{\|(p_0, \ldots, p_n)\|_\nu^{\deg F}};$$

changing the equation for D affects the distance function by a multiplicative constant.

In this context, Vojta's Main Conjecture (see [63]) predicts the following:

Conjecture [Vojta's Main Conjecture]. Let S be a finite set of places of a number field κ; for each $\nu \in S$, let D_ν be a hypersurface of $\mathbb{P}_n$ (possibly reducible) with normal crossing singularities, defined over κ. Let $\epsilon > 0$ be a positive real number. There exists a proper closed subvariety $Z \subset \mathbb{P}_n$ and a number $c > 0$ such that for all rational points $P \in (\mathbb{P}_n - Z)(\kappa)$

$$\prod_\nu \operatorname{dist}_\nu(P, D_\nu) > c \cdot H(P)^{-n-1-\epsilon} \tag{3.5}$$

This is a reformulation of a particular case of Conjecture 3.4.3 from [63] (the Main Conjecture in [63]) or Conjecture 15.5 from [64]). The original Vojta's conjecture applies to hypersurfaces of any smooth projective variety; in that case the right-hand side takes into consideration the canonical bundle of the variety.

The following theorem has been proved independently by Evertse-Ferretti in [28] and by Corvaja-Zannier in [19]:

Theorem 3.6. *Let S be a finite set of places of a number field κ, and for each place $\nu \in S$, $F_\nu(x_0, \dots, x_n) \in \kappa[x_0, \dots, x_n]$ be a homogeneous form. Let $\epsilon > 0$ be a positive real number. Then for all rational points $P = (x_0 : \dots : x_n)$ outside a proper Zariski closed subset the inequality*

$$\prod_{\nu \in S} \left(\frac{|F_\nu(x_0, \dots, x_n)|_\nu}{\|(x_0, \dots, x_n)\|_\nu} \right)^{1/\deg F_\nu} > H(P)^{-n-1-\epsilon}$$

holds.

In the case of polynomials of degree 1 the result is best-possible, and is a particular case of the Subspace theorem. As for the subspace theorem, one can consider approximating several hypersurfaces with respect to a same valuation. Also, one can try to improve on the exponent on the right-hand side working with approximants on a fixed algebraic subvariety. The most general result obtained so far is the following theorem of Evertse and Ferretti from [28]:

Theorem 3.7. *Let $X \subset \mathbb{P}_n$ be a projective variety over a number field κ. Let S be a finite set of places of κ. Let $F_1, \dots, F_q \in\in \kappa[x_0, \dots, x_n]$ be homogeneous forms with coefficient in κ such that the hypersurfaces of X defined by the vanishing of $F_1, \dots, F_q$ are in general position. Let $\epsilon > 0$ be a positive real number. Then for all rational points $P = (x_0 : \dots : x_n) \in X(\kappa)$ outside a proper Zariski closed subset of X the following inequality holds:*

$$\prod_{\nu \in S} \prod_{i=1}^{q} \min \left(1, \frac{|F_\nu(x_0, \dots, x_n)|_\nu}{\|(x_0, \dots, x_n)\|_\nu} \right)^{1/\deg F_\nu} > H(P)^{-\dim X - 1 - \epsilon}$$

It is easy to deduce from the above statement analogues lower bounds for non-homogeneous polynomials and integral points. For instance, the following result appears in [19]

Theorem 3.8. *Let $X \subset \mathbb{A}^n$ be an affine algebraic variety defined over a number field κ. For each place ν in a finite set of places S, containing the archimedean ones, let $f_\nu \in \kappa[x_1, \dots, x_n]$ be a polynomial of degree $d > 0$. For each $\epsilon > 0$ there are only finitely many integral points $\mathbf{x} \in X(_S)$ such that*

$$0 < \prod_{\nu \in S} |f_\nu(\mathbf{x})|_\nu < H(\mathbf{x})^{-d(\dim X - 1 - \epsilon)}.$$

In the above statement, the (affine) height $H(\mathbf{x})$ of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{A}^n$ coincides with the projective height of the point $(1 : x_1 : \ldots : x_n) \in \mathbb{P}_n$.

By known argument involving Galois conjugates of polynomials and places, one can deduce from the above the following

Corollary 3.9. *Let $X \subset \mathbb{A}^n$ be an affine algebraic variety defined over $\mathbb{Q}$. Let $f(x_1, \ldots, x_n) \in \bar{\mathbb{Q}}[x_1, \ldots, x_n]$ be a polynomial with algebraic coefficients. The set of integral points $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n \cap X(\mathbb{Q})$ such that*

$$0 < |f(\mathbf{x})| < H(\mathbf{x})^{-d(\dim X - 1) - \epsilon}.$$

We strees that in the above formula, although the polynomial f has algbebraic irrational coefficients, the absolute value must be normalized with respect to $\mathbb{Q}$, i.e. it must be the ordinary real or complex absolute value. Liouville bound would give $|f(\mathbf{x})| \gg H(\mathbf{x})^{-d[\kappa:\mathbb{Q}]}$, where κ is the field generated by the coefficients of f. Hence the result is non-trivial whenever $[\kappa : \mathbb{Q}] > \dim X - 1$.

In the same way, Theorem 3.6 implies the following generalization of Thue's inequality:

Theorem 3.10. *Let $F(x_0, \ldots, x_n) \in \mathbb{Q}[x_0, \ldots, x_n]$ be an irreducible homogeneous polynomial, which splits over $\bar{\mathbb{Q}}$ in the product of m factors of degree d. Let $X \subset \mathbb{P}_n$ be an algebraic variety, defined over $\mathbb{Q}$, not contained in the zero set of F. Let $\epsilon > 0$ be a positive real number. Then for each rational point $P = (x_0 : \ldots : x_n) \in X(\mathbb{Q})$ outside a proper closed Zariski subset of X, the following holds:*

$$\frac{|F(x_0, \ldots, x_n)|}{\|x\|^{\deg F}} > H(P)^{-d(\dim X + 1) - \epsilon}.$$

Note that for $n = 1$ each polynomial splits into linear factors. Hence, putting $X = \mathbb{P}_1$ we reobtain Thue-Roth's inequality, from which Thue's theorem on the finiteness of solutions to the equation $F(x_0, x_1) = 1$ follows immediately. If $n > 1$, however, the homogeneous polynomial F can remain irreducible in the ring $\bar{\mathbb{Q}}[x_0, \ldots, x_n]$. In that case, the above inequality is trivial (d being the degree of F, taking integral coprime coordinates for P, the inequality boils down to $|F(x_0, \ldots, x_n)| > \max(|x_0|, \ldots |x_n|)^{-d \dim X - \epsilon}$ which is weaker then Liouville's. In particular, one cannot prove the analogue of Thue's theorem, namely the finiteness (or the degeneracy) of the solutions to $F(x_0, \ldots, x_n) = 1$ in integers $(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$.

Recent developments on these topics have been carried out by Min Ru [51] (see also the preprint by P. Vojta and M. Ru [52]).

A very different problem consists in studying the approximation of points by (sequences of) points in higher dimensional algebraic varieties. This topic has been investigated by D. Mc Kinnon and M. Roth (see [46]).

4 A proof of Siegel's theorem for integral points on curves

In this section we prove Siegel's Theorem using the approach developed in [17], which is based on the Subspace Theorem.

We recall the statement of Siegel's theorem, in the generalized version for rings of S-integers, whose original proof is due also to the contribution by Mahler [45]. The most general version, equivalent to the one below, appears probably for the first time in a paper of Lang [43].

Theorem 4.1 (Siegel's Theorem). *Let $\mathcal{C}$ be an affine curve of Euler characteristic χ, defined over a number field κ. Let $\mathcal{O}_S \subset \kappa$ be a ring of S-integers. If $\chi > 0$ then $\mathcal{C}(\mathcal{O}_S)$ is finite.*

The above theorem encompasses, in particular, Thue's 1909 finiteness result on the equations of the type

$$F(x, y) = c, \tag{4.2}$$

where $F(X, Y) \in \mathbb{Z}[X, Y]$ is a homogeneous form of degree $d \geq 3$, with no repeated factors, and $c \in \mathbb{Z} - \{0\}$ a non-zero constant.

Note that the affine curve defined by an equation as above has genus $(d-1)(d-2)/2$ and has d points at infinity, so its Euler characteristic is $\chi = d^2 - 2d$ and is positive precisely whenever $d \geq 3$.

We shall prove, using the Subspace Theorem treated in the previous section, the particular case below of Siegel's theorem. The full Siegel's Theorem will follow by reducing the general case to the special one via the Chevalley-Weil theorem.

Theorem 4.3. *Let κ be a number field, $\mathcal{O}_S \subset \kappa$ a ring of S-integers. Let $\mathcal{C}$ be an affine algebraic curve over κ with at least three points at infinity. Then $\mathcal{C}(\mathcal{O}_S)$ is finite.*

Some remarks are in order: (1) the number of points at ininifty depends on a compactification of $\mathcal{C}$, i.e. on embeddings $\mathcal{C} \hookrightarrow \mathbb{A}^n \hookrightarrow \mathbb{P}_n$; the statement means that if in some embedding this number is ≥ 3, then the conclusion follows. The maximal number of points at infinity occurs for a compactification for which the points at infinity are all smooth. (2) We did not suppose that the affine curve $\mathcal{C}$ is smooth, either in Theorem 4.1 nor in Theorem 4.3; however, by taking a normalization $\mathcal{C}' \to \mathcal{C}$, the finiteness of $\mathcal{C}'(\mathcal{O}_S)$ would imply the same conclusion for $\mathcal{C}(\mathcal{O}_S)$. Hence one can reduce to the case when $\mathcal{C}$ is smooth. (3) No general finiteness result can hold for all curves with just one or two points at infinity, as shown by the case of smooth rational ones (resp. $\mathbb{A}^1$ and $\mathbb{G}_m$).

Before proving Theorem 4.3, let us show how to use the Chevalley-Weil theorem to deduce Theorem 4.1 from Theorem 4.3.

We have already remarked that we can reduce to the smooth case. If a (smooth) curve $\mathcal{C}$ has positive Euler characteristic but only one or two points at infinity, then its genus must be positive. Then its smooth completion $\tilde{\mathcal{C}}$ is not simply connected; more precisely, it admits connected unramified covers of any degree. Consider an unramified cover $\tilde{\mathcal{C}}' \to \tilde{\mathcal{C}}$ of degree ≥ 3. Then the pre-image in $\tilde{\mathcal{C}}'$ of the set $\tilde{\mathcal{C}} - \mathcal{C}$ consisting of the points at infinity has cardinality ≥ 3, hence Theorem 4.3 applies to $\mathcal{C}'$. The finiteness of any set of S-integer points on $\mathcal{C}'$ implies, via the Chevalley-Weil Theorem, the same assertion for $\mathcal{C}$.

We first look at the example of the Thue's equation, which we can write in the form

$$F(x, y) = m \cdot \prod_{i=1}^{d} (x - \alpha_i y) = c \tag{4.4}$$

where $\alpha_1, \ldots, \alpha_d \in \bar{\mathbb{Q}}^*$ are conjugate algebraic numbers and $c, m \in \mathbb{Z} - \{0\}$ are non-zero rational integers.

Suppose that $d \geq 3$ and, by contradiction, there is an infinite set of integral solutions to (4.4).

We write $\mathcal{C} \subset \mathbb{A}^2$ for the algebraic curve defined by equation (4.4) and embed $\mathcal{C} \hookrightarrow \tilde{\mathcal{C}} \subset \mathbb{P}_2$, where $\tilde{\mathcal{C}}(\bar{\mathbb{Q}})$ contains the d points at infinity $Q_i := (\alpha_i : 1 : 0)$, $i = 1, \dots, d$.

Bu the compactness of the topological space $\tilde{\mathcal{C}}(\mathbb{R})$, from any infinite sequence of solutions $(x_n, y_n) \in \mathbb{Z}^2$ we can extract a sequence convergent to one of the points at infinity, say $Q_1 = (\alpha_1 : 1 : 0)$.

Consider the rational function $\varphi := x - \alpha_1 y \in \kappa(\mathcal{C})$, where $\kappa = \mathbb{Q}(\alpha_1)$. We can view φ also as a morphism $\tilde{\mathcal{C}} \to \mathbb{P}_1$, of degree d, sending $(\alpha_1 : 1 : 0)$ to 0 (with multiplicity d). Clearly, for every solution $(u, v) \in \mathbb{Z}^2$ of (4.4) we have

$$|u - \alpha_1 v| = \frac{|c|}{|m|} \cdot \frac{1}{|u - \alpha_2 v| \cdots |u - \alpha_d v|}.$$

Now, for all but finitely many solutions of the sequence of solutions converging to Q_1, we have the lower bound

$$|u - \alpha_i v| > \frac{\min(|\alpha_1 - \alpha_i|, |\alpha_1^{-1} - \alpha_i^{-1}|)}{2} \cdot \max(|u|, |v|),$$

valid for every $i = 2, \dots, d$. By the two above inequalities there exists a positive real number C such that for all but finitely many solutions in our sequence

$$|\varphi(u, v)| = |u - \alpha_1 v| \leq C \cdot \max(|u|, |v|)^{-d+1} \leq C \cdot \max(|u|, |v|)^{-2}.$$

This inequality contradicts Roth's theorem.

Little modification is needed to recover the full Thue-Mahler theorem, where S-integer solutions to a general equation of the form (4.4) are considered.

Let us now come to the general case of Theorem 4.3: $\mathcal{C}$ is an arbitrary affine algebraic curve; let us embed it into an affine space $\mathbb{A}^n$ so that its completion $\tilde{\mathcal{C}}$ in $\mathbb{P}_n$ is smooth at infinity. Let $d \geq 3$ be the number of points at infinity, which are labelled $Q_1, \dots, Q_d$.

Suppose by contradiction that $\mathcal{C}(\mathcal{O}_S)$ is infinite. Let κ be a number field containing a field of definition for the curve and for the points at infinity. We denote again by $\mathcal{O}_S$ a ring of S-integers of κ containing the given ring (appearing in Theorem 4.3).

By compactness of the topological space $\prod_{\nu \in S} \tilde{\mathcal{C}}(\kappa_\nu)$ we can extract an infinite sequence of integral points $P_1, P_2, \dots$ converging with respect to the places of S. Let, for each place $\nu \in S$, $R_\nu \in \tilde{\mathcal{C}}(\kappa_\nu)$ be the ν-adic limit of the sequence $P_1, P_2, \dots$.

Since the height of P_n tends to infinity, and the points P_n are S-integers, some of the limit points R_ν must lie at infinity. Let $S' \subset S$ be the set such of places.

The idea is to replace the morphism $\varphi : \tilde{\mathcal{C}} \to \mathbb{P}_1$ used in the proof of Thue's theorem by a morphism $\Phi : \tilde{\mathcal{C}} \to \mathbb{P}_M$ for some (large) dimension M.

We give the details, following closely the original paper [17] and the book [14].

For a large integer N, put

$$V_N = \mathrm{H}^0(\tilde{\mathcal{C}}, N(Q_1 + \ldots + Q_d)) = \{f \in \bar{\kappa}[\mathcal{C}] \,:\, (f) \geq -N(Q_1 + \ldots + Q_r)\}.$$

Let $f_0, \dots, f_M$, where $M + 1 = h^0(N(Q_1 + \ldots + Q_d)) = dN + O(1)$, be a basis of V_N. Since the divisor $Q_1 + \ldots + Q_d$ is defined over κ, we can choose $f_0, \dots, f_M$ defined over κ, i.e. with $f_i \in V_N \cap \kappa[\mathcal{C}]$ for $i = 0, \dots, M$.

After multiplying the f_j by a suitable constant, we can suppose that $f_j(P_n) \in \mathcal{O}_S$ for all j, n.

For every $\nu \in S$, consider the filtration $V = W_{\nu,1} \supset W_{\nu,2} \supset \dots$ defined as

$$W_j = W_{\nu,j} = \{f \in V_N \,:\, \mathrm{ord}_{R_\nu} f \geq j - 1 - N\}.$$

We have $\dim(W_j/W_{j+1}) \leq 1$ for each j; in particular $\dim W_j \geq d-j+1$.

Now, for each $\nu \in S'$, choose a basis of V_N containing a basis of each subspace $W_{\nu,j}$ (for each j such that $W_{\nu,j} \neq \{0\}$). These functions can be expressed as linear combinations of the basis $(f_0, \ldots, f_M)$, i.e. as values of linear forms $L_{\nu,j}(f_0, \ldots, f_M)$, where $L_{\mu,j}(X_1, \ldots, X_d)$ has its coefficients in $\bar{\kappa}$. Clearly

$$\mathrm{ord}_{R_\nu} L_{\nu,j}(f_0, \ldots, f_M) \geq j - N + 1.$$

For $\nu \in S - S'$ we just put $L_{\nu,j}(f_0, \ldots, f_M) = f_j$.

For each $\nu \in S'$ choose a local parameter $t_\nu \in \kappa(\mathcal{C})$ at R_ν. The above displayed inequality implies that

$$|L_{\nu,j}(f_0(P_n), \ldots, f_M(P_n))|_\nu \ll |t_\nu(P_n)|_\nu^{j+N}.$$

Now, observe that we dispose of $M+1 = dN+O(1)$ rational functions $L_{\nu,j}(f_0, \ldots, f_M)$, of which at most N have poles and approximately $(r-1)N$ have zeros at R_ν. Estimating the order of the product $\prod_j L_{\nu,j}(f_0, \ldots, f_M)$ we have that this order is positive, and actually $> (d-2)N + O(1)$ for large N (a stronger asymptotic estimates in fact holds, but we do not need it).

Put $\mathbf{x} = (f_0(P_n), \ldots, f_M(P_n)) \in \mathcal{O}_S^{M+1}$ and let as before $\|\mathbf{x}\|_\nu$ be its sup-norm in the ν-adic absolute value. Observing that for $\nu \notin S'$ the absolute values of $f_j(P_n)$ are uniformly bounded, we can deduce that

$$\prod_{\nu \in S} \prod_{j=0}^{M} \frac{|L_{\nu,j}(\mathbf{x})|_\nu}{\|\mathbf{x}\|_\nu} \ll \prod_{\nu \in S'} \left(|t_\nu(P_n)|\right)^{(d-2)N+O(1)}.$$

On the other hand, the height is easily estimated by $H(\mathbf{x}) \ll \prod_{\nu \in S'} \left(|t_\nu(P_n)|\right)^N$. Finally we obtain, dividing the exponents by N,

$$\prod_{\nu \in S} \prod_{j=0}^{M} \frac{|L_{\nu,j}(\mathbf{x})|_\nu}{|\mathbf{x}|_\nu} \ll H(\mathbf{x})^{2-d+\delta+O(1/N)}.$$

The Subspace Theorem then implies that infinitely many vectors $\mathbf{x}$ lie on a hyperplane; this is impossible, since the functions $f_0, \ldots, f_M$ are linearly independent, so every non-trivial linear combination of $f_0, \ldots, f_M$ can have only finitely many zeros.

Historical note. The original proof of Siegel's theorem appeared in [59], and treated only the case in which the ring of S-integers coincides with the ring of algebraic integers of κ. An English translation accompanied by the original German version is reproduced in [70]. For a discussion on this proof, see the papers by S. Lang [43], C. Fuchs and U. Zannier [70] and by Zannier [69]. A different proof, in the spirit of Dyson's proof of his Diophantine approximation theorem [26], is due to C. Gasbarri [35]. Still another approach, using the language of non-standard analysis, appears in work of Robinson and Roquette [53].

5 The generalized Fermat equation and triangle groups

In this section, we show yet another example of a situation in which a hyperbolicity condition implies a finiteness result for a Diophantine equation. The main results are due to H. Darmon and A. Granville [25].

Let p, q, r be a triple of natural numbers with

$$1 \leq p \leq q \leq r.$$

The aim of this section is the study of the Diophantine equation

$$x^p + y^q = z^r \tag{5.1}$$

to be solved in coprime integers $x, y, z \in \mathbb{Z}$. More generally, we shall treat the equations $ax^p + by^q = cz^r$, where the coefficients a, b, c are non-zero integers. We shall also consider the corresponding equations in a ring of S-integers.

It will turn out once again that the results (finiteness or density according to the cases) will heavily depend on the sign of a kind of Euler characteristic which we now define.

Given the triple (p, q, r), the Euler characteristic χ of the triple will be the rational number

$$\chi = \chi(p, q, r) := 1 - \frac{1}{p} - \frac{1}{q} - \frac{1}{q}.$$

In accordance to this position, we say that the triple is hyperbolic, elliptic or euclidean (alternatively: parabolic) according to the sign of the difference $1 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r}$, so:

$$\begin{array}{lcll} \frac{1}{p} + \frac{1}{q} + \frac{1}{r} & > & 1 & \text{elliptic} \\ \frac{1}{p} + \frac{1}{q} + \frac{1}{r} & = & 1 & \text{euclidean} \\ \frac{1}{p} + \frac{1}{q} + \frac{1}{r} & < & 1 & \text{hyperbolic.} \end{array} \tag{5.2}$$

The motiviation for this trichotomy comes from the theory of triangle groups, which we recall here.

Given three positive integers p, q, r as before, one can define the abstract group $T(p, q, r)$ by generators and relations as

$$T(p, q, r) :=< a, b \,|\, a^p = b^q = (ab)^r = 1 > .$$

For instance, the group $T(2, 2, n)$, for $n \geq 1$, is the dihedral group $\mathcal{D}_n$ of order $2n$. These groups are named *triangle groups*, because of their geometric realizations, shown below, which differ according to the above mentioned trichotomy (5.2). We first classify all the possible groups with $\chi = 1 - \frac{1}{p} - \frac{1}{q} - \frac{1}{q} < 0$ (elliptic case).

We have already mentioned infinite family $(2, 2, n)$, giving rise to the dihedral groups; these groups can be realized as (finite) subgroups of the orthogonal group SO(3), so they act on the sphere. More precisely, they correspond to the symmetric group of a tiling of the sphere with $2n$ triangles of angles $\pi/2, \pi/2, \pi/n$. The three other possible triples are: $(2, 3, 3)$, defining the abstract group A_4, the alternating group on four points, of order 24; $(2, 3, 4)$, corresponding to the symmetric group S_4 (of order 24) and finally the triple $(2, 3, 5)$, corresponding to the alternating group A_5, of order 60. Note that the first 'sporadic group' A_4 can be realized as the group of orientation preserving isometries (rotations) of a tetrahedron, while the group S_4 is the symmetric group of a cube (or its dual, the octahedron) and A_5 the group of the icosahedron (and its dual, the dodecahedron). In each case, these triangle groups can be viewed as the symmetry group of a (finite) tassellation of the sphere in geodesic triangles. They are said to be of elliptic type, since the sphere has positive curvature (if endowed with its natural metric, invariant by the action of the group SO(3)).

In the euclidean (or parabolic) case only three triples are possible: $(2, 3, 6)$, $(2, 4, 4)$ and $(3, 3, 3)$. The corresponding groups are infinite, and are associated to tilings of the euclidean plane by triangles with angles $(\pi/2, \pi/3, \pi/6)$, $(\pi/2, \pi/4, \pi/4)$ and $(\pi/3, \pi/3, \pi/3)$ respectively.

The hyperbolic case is the richest one: we have infinitely many triangle groups, each being an infinite group. They can be constructed as follows: take a triple (p,q,r) with $\chi(p,q,r)>0$, and construct a geodesic triangle in the hyperbolic plane with angles $(\pi/p, \pi/q, \pi/r)$ (this is possible precisely because $\chi > 0$; by Lambert's theorem on hyperbolic triangles, its area will be $\pi\chi$). The reflections with respect to the sides of the triangles generate an infinite discrete group of hyperbolic isometries; the index-two subgroup of orientation preserving isometries turns out to be isomorphic to the abstract triangle group $T(p,q,r)$.

The main arithmetic result is the following theorem due to Darmon and Granville [25]:

Theorem 5.3. *Let (p,q,r) be a hyperbolic triple. Then for every non-negative integers a,b,c there exist only finitely many solutions $(x,y,z)\in\mathbb{Z}^3$ with $\gcd(x,y,z)=1$ to the equation*

$$ax^p + by^q = cz^r. \tag{5.4}$$

On the contrary, for euclidean or elliptic triples, we have

Theorem 5.5. *Let (p,q,r) be a triple with $\chi(p,q,r)\leq 0$. Then there exist non-zero integers a,b,c such that the solutions $(x,y,z)\in\mathbb{Z}^3$ in coprime integers to the equation (5.4) are Zariski-dense in the surface defined by the above equation.*

Our approach constitutes a simplification of the original one, and makes essential use of the Chevalley-Weil theorem.

Before starting the proofs of the above statements, we pause for a remark on the condition of coprimality of x,y,z. Since equations (5.1), (5.4) are not homogeneous, there is no way in general to pass from a solution (x,y,z) to one with coprime coordinates. For instance, the solution $(8,4,2)$ to the equation

$$x^2 + y^3 = z^7 \tag{5.6}$$

does not produce, at least in any obvious way, any solution with coprime coordinates.

We dispose of a geometric formulation of the coprimality condition: let us denote by $\mathcal{S}$ the quasi projective surface in $\mathbb{A}^3$ defined by the system of equation and inequality

$$\begin{cases} ax^p + by^q &= cz^r \\ (x,y,z) &\neq (0,0,0) \end{cases} \tag{5.7}$$

Then the integral points on $\mathcal{S}$ are precisely the integral solutions to (5.4) with coprime coefficients.

Yet in other words: let $\bar{\mathcal{S}}$ be the projective closure in $\mathbb{P}_3$ of the quasi-projective surface $\mathcal{S}$ defined by (5.7); blowing-up the origin of $\mathbb{A}^3\subset\mathbb{P}_3$ we obtain a new surface $\hat{\mathcal{S}}$ in the projective 3-space blowun-up at one point. Let D be the curve obtained by intersecting $\hat{\mathcal{S}}$ with the union of the pull-back of the plane at infinity and the exceptional divisor. The rational points on $\hat{\mathcal{S}}$ which are integral with respect to D correspond to the solutions to (5.4) with coprime coordinates.

We have seen that the coprimality condition is not a trivial one, and the existence of a solution to (5.1) does not lead automatically to a new one with coprime coordinates. However, every solution $(x,y,z)\in\mathbb{Z}^3$ to equation (5.1) (or to the equation (5.4)) gives rise to infinitely many of them, whose coordinates are not coprime. These are obtained in the following way: let $(u,v,w)\in\mathbb{N}^3$ be a generator of the one-dimensional lattice in $\mathbb{Z}^3$ formed of the vectors

$(l,m,n) \in \mathbb{Z}^3$ with $pl = qm = rn$ (if p,q,r are coprime, then $(u,v,w) = (qr, rp, pq)$). Then the group $\mathbb{G}_m$ acts on the surface defined by (5.4) via

$$\mathbb{G}_m \times \mathcal{S} \ni (\lambda, (x,y,z)) \mapsto (\lambda^u x, \lambda^v y, \lambda^r z) \in \mathcal{S}. \tag{5.8}$$

It follows that for each integral solution $(x,y,z) \in \mathbb{Z}^3$ to (5.4) one can produce infinitely many solutions by taking integral values of λ in (5.8) above.

The above considerations lead to the following versions of Theorems 5.3 and 5.5 for rings of S-integers

Theorem 5.9. *Let (p,q,r) be a triple of positive integers. The following are equivalent:*

(i) *There exists a ring of S-integers $\mathcal{O}_S$ such that the set of integral points on the surface of equation (5.7) is Zariski-dense;*

(ii) $\chi(p,q,r) \leq 0.$

Let us start with the proof of Darmon-Granville's finiteness theorem (Theorem 5.3). Let $\mathcal{S} \subset \mathbb{A}^3 - \{(0,0,0)\}$ be the surface defined by the equation (5.7) and let $\beta : \mathcal{S} \to \mathbb{P}_1$ be the morphism

$$\mathcal{S} \ni (x,y,z) \mapsto \frac{ax^p}{cz^r}.$$

Note that if $\gcd(p,q,r) = 1$ then the fibers of β are all isomorphic to $\mathbb{G}_m$ and are precisely the orbits for the $\mathbb{G}_m$-action described in (5.8). However, the projection $\beta : \mathcal{S} \to \mathbb{P}_1$ does not define a bundle over $\mathbb{P}_1$; one does obtain a (principal) $\mathbb{G}_m$-bundle over $\mathbb{P}_1 - \{0,1,\infty\}$ aftery removing from $\mathcal{S}$ the pre-images of $0,1,\infty$, which are the multiple fibers for β.

Let us now consider a Galois cover $\mathcal{C} \to \mathbb{P}_1$ of the projective line ramified over $\{0,\infty,1\}$ of order (p,q,r); if $\gcd(p,q,r) = 1$, these covers are obtained from any non-trivial finite quotient of the triangle group $T(p,q,r)$: take a finite index normal subgroup $\Delta \lhd T(p,q,r)$ distinct from the triangle group itself; then define the compact Riemann surface $\mathcal{C}$ to be the quotient of the hyperbolic plane $\mathcal{H}$ by the action of Δ; Δ is necessarily free and so acts freely on $\mathcal{H}$, and the quotiemt map $\mathcal{H} \to \mathcal{C}$ turns out to be the universal cover of $\mathcal{C}$. Recall that the quotient $\mathcal{H}/T(p,q,r)$ of the hyperbolic plane by the action of the full triangle group is the projective line $\mathbb{P}_1$. The corresponding map $\pi : \mathcal{C} \to \mathbb{P}_1$, induced from the surjective map $\mathcal{H} \to \mathbb{P}_1$, ramifies precisely over three points, which correspond to the vertices of the triangles composing the tiling of $\mathcal{H}$. The ramifications indeces are precisely p,q and r.

If the integers p,q,r fail to be coprime, the construction is similar up to the provisio that we must avoid that the quotient $T(p,q,r) \to (T(p,q,r)/\Delta)$ factors through another triangle group of the form $T(p/m, q/m, r/m)$, for any common divisor $m > 1$ of p,q,r.

The Riemann surface defined analytically in the above way turns out to be an algebraic curve defined over the field of algebraic numbers; also the map $\pi : \mathcal{C} \to \mathbb{P}_1$ can be defined over the field of algebraic numbers.

The crucial point in the proof of Theorem 5.3 is the following

Lemma 5.10. *In the above setting, let $\mathcal{F} = \mathcal{C} \times_{\mathbb{P}_1} \mathcal{S}$ be the normalization of the fiber product of $\pi : \mathcal{C} \to \mathbb{P}_1$ and $\beta : \mathcal{S} \to \mathbb{P}_1$. Then the natural morphism $\bar{\pi} : \mathcal{F} \to \mathcal{S}$ is unramified.*

This lemma permits to apply the Chevalley-Weil theorem.

Proof. The statement is local, so we shall argue locally in the complex topology. Let us denote by $\bar{\beta} : \mathcal{F} \to \mathcal{C}$ the projection to $\mathcal{C}$; it satisfies $\pi \circ \bar{\beta} = \beta \circ \bar{\pi}$.

Let $s \in \mathcal{S}$ be any point; if $\beta(s) \notin \{0, \infty, 1\}$ then there exists a neighborhood U of $\beta(s)$ in $\mathbb{P}_1(\mathbb{C})$ such that $\pi : \pi^{-1}(U) \to U$ is a topological cover. In that case, the surface $\mathcal{F}$ can be locally defined as the fiber product $\beta^{-1}(U) \times_U \pi^{-1}(U)$, which is a smooth complex space, so $\bar{\pi} : (\pi \circ \bar{\beta})^{-1}(U) \to \beta^{-1}(U)$ is a topological cover (the pull-back via $\beta : \beta^{-1}(U) \to U$ of the topological cover $\pi : \pi^{-1}(U) \to U$).

The problem arises when $\beta(s) \in \{0, 1, \infty\}$. In these cases we exploit the multiplicity of the fibers of $\beta : \mathcal{S} \to \mathbb{P}_1$ to kill the ramification of the map $\pi : \mathcal{C} \to \mathbb{P}_1$.

Note that in that case the (set-theoretic) fiber product of $\mathcal{S} \to \mathbb{P}_1$ and $\mathcal{C} \to \mathbb{P}_1$ is singular above $\beta(s)$, as we now show (but the normalization that we called $\mathcal{F}$ is smooth).

Suppose for instance that s lies over the point 0 on the line, so that the coordinate x vanishes (the argument is symmetric if $\beta(s) = \infty$ or $\beta(s) = 1$). Local parameter at s on the smooth surface $\mathcal{S}$ are for instance the regular functions $x, z - z(s)$, while the y function can be expressed in term of x, z as

$$y = \left(\frac{cz^r - ax^p}{b} \right)^{1/q}, \tag{5.11}$$

where the q-th root is a well-defined function in a neighborhood of s and the choise of the branch is the one compatible with the y-coordinate at s.

Take a point f in the pre-image $\bar{\pi}^{-1}(s)$. Since the point 0 is ramified of order p under the Galois cover $\pi : \mathcal{C} \to \mathbb{P}_1$, there is a local parameter t on $\mathcal{C}$ (in the analytic sense) at the point $\bar{\beta}(f) =: \gamma \in \mathcal{C}$ which is a p-th root of the function $\pi^*(\beta)$. The ramified cover $\mathcal{C} \to \mathbb{P}_1$ will be locally defined by $t \mapsto t^p = \beta$. Now locally at f the surface $\mathcal{F}$ is birationally defined by adding the function t to the local parameter $x, z - z(s)$ and to the function y defined in (5.11); the algebraic relation satisfied by t is

$$t^p = \beta = \frac{ax^p}{cz^r}.$$

Note that the above equation defines a singular, and non-normal, variety; the local ring at f of $\mathcal{F}$, which is integrally closed, is generated over the local ring of $\mathcal{S}$ at s by an element which we shall denote again by t, of the form

$$t = \frac{x}{(cz^r/a)^{1/p}},$$

where again the p-th root is well-defined and the choice of its branch depends on the choice of the point $f \in \mathcal{F}$ lying over s. Note that there are p choices of points $f \in \mathcal{F}$ corresponding to the point $(s, \gamma) \in \mathcal{S} \times \mathcal{C}$, while in the set-theoretic fiber product $\mathcal{S} \times_{\mathbb{P}_1} \mathcal{C}$ there would be just one; these p points correspond to the p possible branches of the p-th root of the function appearing in the denominator in the above formula.

Clearly t and $\bar{\pi}^*(z - z(s)) =: w$ are local parameter at f and the map $\bar{\pi}$ can be defined by sending

$$(t, w) \mapsto (x, y, z)$$

where $x = t(cz^r/a)^{1/p}$, y is defined by (5.11) and $z = w + z(s)$. Hence it is a local biholomorphism, which implies that the cover is unramified at f. □

We note (although this fact will not be used) that the projection $\bar{\beta} : \mathcal{F} \to \mathcal{C}$ defines a principal $\mathbb{G}_m$-bundle on the curve $\mathcal{C}$.

We can now conclude the *proof of Theorem 5.3*: we have already remarked that the integral solutions (x, y, z) with coprime coordinates to the equation (5.4) correspond to the integral points on the surface $\mathcal{S}$ defined in (5.7). By the Chevalley-Weil theorem, these integral points lift to integral points of $\mathcal{F}$, defined over a fixed ring of S-integers. But now, the rational points on $\mathcal{F}$, in particular the integral ones, project via $\bar{\beta}$ to rational points on $\mathcal{C}$, which is a curve of genus ≥ 2. By Faltings theorem, $\mathcal{C}$ contains only finitely many rational points, which implies that the rational points on $\mathcal{F}$ accumulate on finitely many fibers of $\bar{\beta}$. This last fact, in turn, implies that the integral points on $\mathcal{S}$ accumulate on finitely many fibers for β; but a fiber of β can contain only finitely many points with integral coprime coordinates, which ends the proof. □

We remark that the coprimality assumption appearing in Theorem 5.3 is used only in the application of the Chevalley-Weil theorem. It is an open problem to decide whether, for a hyperbolic triple (p, q, r), the integral solutions to (5.4) are contained in finitely many $\mathbb{G}_m$-orbit for the action (5.8). A conjecture of F. Campana predicts this finiteness.

We have just seen that hyperbolic triples always lead to finitely many solutions (with coprime coordinates). We now turn to the inverse direction: if the triple is not hyperbolic, can we have infinitely many coprime solutions to equation (5.4), at least for one choice of the non-zero coefficients a, b, c?

The answer turns out to be affirmative, as claimed in Theorem 5.5.

We divide the proof of Theorem 5.5 into two parts, one for the elliptic and one for the parabolic case.

Elliptic case. The elliptic case is divided into four sub-cases, the first cooresponding to the dihedral groups, the following ones to the three groups associated to the regular solids.

• Dihedral case. Suppose first the triple is $(2, 2, n)$, for some $n \geq 2$. Then the equation (with the choice $(a, b, c) = (1, 1, 1)$) becomes $x^2 + y^2 = z^n$. It can be written as

$$(x + iy)(x - iy) = |x + iy|^2 = z^n.$$

It then boils down to finding infinitely many Gaussian integers $\alpha \in \mathbb{Z}[i]$ which are n-th powers in $\mathbb{Z}[i]$ and whose real and imaginary parts are coprime. For instance, writing

$$(1 + ki)^n = p_n(k) + iq_n(k)$$

where $p_n(T), q_n(T) \in \mathbb{Z}[T]$ are polynomials, one observes that $(p_n(0), q_n(0)) = (1, 0)$ so $p_n(k), q_n(k)$ take coprime values for infinitely many integers k. The above solutions correspond to integral points on the rational curve

$$\mathbb{A}^1 \ni t \mapsto (x, y, z) = (p_n(t), q_n(t), 1 + t^2)$$

lying on the surface of equation $x^2 + y^2 = z^n$. To produce a Zarski-dense set of integral solutions just use to parameters, replacing $1 + ki$ by $h + ki$.

• Tetrahedral case. Consider now the triple $(2, 3, 3)$ (associated to the Tetrahedron). We shall prove that the equation

$$x^2 + y^3 = z^3 \tag{5.12}$$

admits infinitely many solutions $(x, y, z) \in \mathbb{Z}^3$ with coprime coordinates, and that these triples are indeed Zariki-dense in the surface defined by the above equation. Note that equation (5.12) is equivalent to the equation

$$(z - y)(z^2 + zy + y^2) = x^2,$$

and that the latter is certainly solved in coprime integers whenever we find coprime integers z, y such that both $z - y$ and $z^2 + zy + y * 2$ are perfect squares. The condition that $z^2 + zy + y^2$ be a perfect square can be expressed by the following equation

$$z^2 + zy + y^2 = v^2$$

which represents a smooth projective conic with at least one rational point (e.g. the point $(v : y : z) = (1 : 1 : 0)$). We then obtain a rational parametrization

$$(v : y : z) = (t^2 - ts + s^2 : t^2 - s^2 : 2ts - t^2). \tag{5.13}$$

Whenever t, s are coprime integers, we obtain coprime values of y, z unless $t \equiv -s \pmod 3$ in which case the $\gcd(y, z) = 3$. Now, the condition that $y - z$ be also a square leads to the equation

$$s^2 + 2ts - 2t^2 = u^2 \tag{5.14}$$

which again represents a smooth projective conic with a rational point (e.g. the point $(s : t : u) = (1 : 0 : 1)$). We then obtain infinitely many other rational points, via the parametrization

$$(s : t : u) = (2\lambda^2 + \mu^2 : 2\lambda^2 + 2\lambda\mu : 2\lambda^2 - 2\lambda\mu - \mu^2). \tag{5.15}$$

By letting λ, μ vary among the integers we obtain integer values of s, t, u satisfying (5.14). If we choose coprime integers λ, μ with $(\lambda, \mu) \equiv (0, 1) \pmod 3$ we obtain $(s, t) \equiv (1, 0) \pmod 3$, hence coprime values for z, y as wanted.

This concludes the proof for the triple $(2, 3, 3)$. We note that the bulk of this proof was the geometric fact that the surface $\mathcal{S}$ admits a degree 2 (unramified) cover $\mathcal{S}' \to \mathcal{S}$ with $\mathcal{S}' \simeq \mathbb{P}_1 \times \mathbb{G}_m$ (over the complex number field). Since this last surface admits a Zariski dense set of integral points, the same will be true of the surface $\mathcal{S}$.

• Ocatahedral case. We now consider the triple $(2, 3, 4)$, associated to the octahedron (or the cube). We sall prove that the equation

$$x^2 + y^3 = z^4 \tag{5.16}$$

admits infinitely many integral solutions with coprime coordinates. Again, the equation is tranformed into $(z^2 - x)(z^2 + x) = y^3$ whose solutions can be obtaiend from the solutions to the system

$$\begin{cases} z^2 - x &= u^3 \\ z^2 + x &= v^3 \end{cases}$$

which is equivalent to the single equation

$$v^3 + u^3 = 2z^2 \tag{5.17}$$

(any solution (u, v, z) of (5.17) gives rise to the solution $(v^3 - z^2, u, v, z)$ to the system above). The equation (5.17) is of Fermat-type with an elliptic exponent vector $(2, 3, 3)$, as the one considered before. Certainly it will admit infinitely many integral solutions with coprime coordinates in a suitable ring of S-integers, since the surface it defines is isomorphic over the complex number field to the ome defined by equation (5.12). However, we can easily see that the above equation admits infinitely many integral solutions with coprime coordinates already over the ring $\mathbb{Z}$.

Again, we can factor the left-hand side in (5.17) as $(v+u)(v^2-uv+v^2)$ and reduce to finding u, v such that for some integers ξ, η

$$\begin{cases} u^2 - uv + v^2 &= \xi^2 \\ u + v &= 2\eta^2 \end{cases}$$

This system is treated as before. The first equation defines the same smooth conic with one rational point as in the previous case, so admits a parametrization with quadratic polynomials (e.g. $(u, v, \xi) = (t^2-s^2, t^2-2ts : t^2-ts+s^2$). The second equation becomes then $2t^2-2ts-s^2 = 2\eta^2$ which again represents a smooth conic with a rational point (e.g. $(s : t : \eta) = (0 : 1 : 1)$) so it admits infinitely many rational points, parametrized by values of quadratic polynomials in new variables. Again, suitable specializations of the variables give rise to copirme soultions (x, y, z) to the original equation.

This completes the proof in the octahedral case. The link between the octahedral and the tetrahedral cases admits the following geometric interpretation: letting $\mathcal{S}_{(2,3,3)}$ and $\mathcal{S}_{(2,3,4)}$ be the surfaces associated to the tetrahedral and the octahedral equations respectively, the above calculations provide a degree 3 unramified cover $\mathcal{S}_{(2,3,3)} \to \mathcal{S}_{(2,3,4)}$.

• Icosahedral case. As expected, the icosahedral triple $(2, 3, 5)$ leads to the most difficult case. The corresponding equation was implicitely solved by Klein in his famous book on the icosahedron [40]. He considered the degree sixty Galois cover $\mathbb{P}_1 \to \mathbb{P}_1$ given by

$$z \mapsto \frac{(-z^{20} + 228z^{15} - 494z10 - 228z^5 - 1)^3}{1728z^5(z^{10} + 11z5 - 1)^5}$$

which admits a Galois group isomorphic to the triangle group $T(2, 3, 5) \equiv A_5$. He found three fundamental invariants x, y, z, of respective degrees $30, 20, 12$ (the number of edges,faces and vertices of an icosahedron),which in homogenous coordinates u, v (where $z = u/v$) can be written as

$$\begin{aligned} x &= 12^6(u^30 + v^30 + 522(u^{25}v^5 - u^5v^{25}) - 10005(u^{20}v^{10} + u^{10}v^{20})) \\ y &= 12^4(-u^{20} - v^{20} + 228(u^{15}v^5 - u^5v^{15}) - 494u^{10}v^{10} \\ z &= 12^3uv(u^{10} + 11u^5v^5 - v^{10}) \end{aligned}$$

These three fundamental invariants satisfy the Fermat-type icosahedral equation $x^2 + y^3 = z^5$; the integral coprime specializations of (u, v) give rise, after clearing out the twelfth power of twelve, an integral solution to the equation

$$x^2 + y^3 = 1728 \cdot z^5,$$

which then turns out to admit infinitely many integral solutions (x, y, z) with coprime coordinates.

Parabolic case. We must now consider the three parabolic triples $(2, 4, 4), (3, 3, 3)$ and $(2, 3, 6)$. Not surprisingly, to produce infinitely many integral solutions one is led to producing infinitely many rational points on elliptic curves (recall that the elliptic curves are complete curves of parabolic type).

• Let us start from the triple $(2, 4, 4)$. The Diophantine equation $x^4+y^4 = z^2$ has no coprime integral solutions outside those with one vanishing term, as proved already by Fermat via his infinite descent method, introduced precisely for solving that equation. However, as we now show, the equation admits infinitely many integral solutions over suitable number fields, and suitable twisted forms of it admit infinitely many integral solutions already in $\mathbb{Z}$.

We interpret the coordinates $(x, y$ as homogeneous coordinates in $\mathbb{P}_1$. Let $\tilde{\mathcal{C}}$ be a complete curve which covers the line with a degree two morphism ramified over the zero set of the binary quartic form $x^4 + y^4$, i.e. over the points $(1 : \xi)$, $(1 : i\xi), (1 : -\xi)$ and $(1 : -i\xi)$, where $\xi^4 = -1$. Then encessarily $\tilde{\mathcal{C}}$ has genus one, and can be defined in an affine model by the equation $u^2 = 1 + v^4$. It will have infinitely many rational points over some number field κ. Writing $u = z/\delta$ with x, δ coprime S-integers on a suitable principal ring of S-integers of κ, we see that δ must be a square; writing $\delta = x^2$ we have $z^2 = x^4 + (\delta v)^4$, so that $\delta v =: y$ is an S-integer. We have then solved the original equation.

If one wants the solutions already in the ring $\mathbb{Z}$ of rational integers, it suffices to change the coefficients for the monomials. For instance, the Diophantine equation

$$15z^2 = x^4 - y^4$$

admits infinitely many solutions in coprime integers.

• The triple $(3, 3, 3)$ already defines an elliptic curve, if we interpret the coordinates in the projective sense.

Also in this case, the $\mathbb{Q}$-rank is zero, as proved by Euler, but putting as coefficient for z the famous 'taxi-cab number' 1729 leads to the elliptic curve

$$x^3 + y^3 = 1729z^3,$$

admitting, in addition to the trivial solution $(1 : -1 : 0)$, the two non-trivial solutions $(1, 12, 1)$ and $(9, 10, 1)$, which provide infinitely many rational points.

• Finally, let us study the case of the $(2, 3, 6)$: the Diophantine equation $x^2 + y^3 = z^6$ is equivalent to the system

$$\begin{cases} x^2 + y^3 &= z^3 \\ z &= w^2 \end{cases}$$

Recall that the first equation is of tetrahedral type, and was solved via the parametrizations (5.13) and (5.15), from which it follows that z can be expressed as a quartic form in two parameters. We then reduce to the triple $(2, 4, 4)$ already considered.

We end this paragraph by noting that all our calculations could be expressed in the language of weighted projective space, which might be considered simpler by some readers.

6 Algebraic groups and the S-unit equation theorem

Throughout this chapter, κ is a fixed number field and S a finite set of absolute values of κ, containing the archimedean ones. Unless otherwise stated, all algebraic varieties are defined over the number field κ.

6.1 The S-units equation

In this section we will be interested in the Diophantine equation

$$u_1 + \ldots + u_n = 1 \tag{6.1}$$

to be solved in S-units $u_1, \ldots, u_n \in \mathcal{O}_S^*$. The above equation defines an irreducible algebraic subvariety $V \subset \mathbb{G}_m^n$, not a translate of a subgroup. Its set $V(\mathcal{O}_S)$ of S-integral points corresponds to

the set of solutions in S-units to the equation (6.1). Since V is a variety of log-general type, after Vojta's conjecture it is expected that its set of integral points is not Zariski-dense. This assertion is in fact a theorem, proved by Evertse, van der Poorten and Schlickewei, after preliminary work by Dubois and Rhin, actually in the stronger form given here

Theorem 6.2. *Equation* (6.1) *admits only finitely many solutions* $(u_1, \dots, u_n) \in (\mathcal{O}_S^*)^n$ *for which no sub-sum of the* u_i *vanishes.*

Of course, if $n = 2$ then no-subsum can vanish, so we obtain unconditional finiteness (and, by the way, this was the Siegel-Mahler theorem for integral points on $\mathbb{P}_1 - \{0, 1, \infty\}$).

If, on the contrary, $n \geq 3$, then there are certainly infinite families of solutions; for instance, for $n = 3$ the family $(u, -u, 1)$, where $u \in \mathbb{G}_m$. These families correspond to sub-tori contained in V.

The three-dimensional case ($n = 3$ in the above theorem) corresponds to the complement of four lines in general position on the projective plane, as we now explain. Using suitable projective coordinates X, Y, Z for $\mathbb{P}_2$, we can suppose that the four lines, labeled $L_1, \dots, L_4$, are defined by the equations $X = 0, Y = 0, Z = 0$ and $X + Y = Z$. The complement of the union of the first three lines is isomorphic to $\mathbb{G}_m^2$; actually, putting $u = X/Z$ and $v = Y/Z$, we see that the integral points on this complement correspond to the S-unit values of u and v. The condition that the point $(X : Y : Z)$ does not reduce to the line $X + Y = Z$ modulo any prime amounts to saying that $u + v \not\equiv 1$ modulo any prime. This means precisely that $w =: 1 - u - v$ is a unit, and this leads to the linear equation $u + v + w = 1$, to be solved in S-units. The mentioned infinite families (there are three of them in this case) correspond to the three lines in $\mathbb{P}_2$ intersecting the union of the four lines $L_1, \dots, L_4$ in only two points. These lines are images of non-constant morphisms $\mathbb{G}_m \to \mathbb{P}_2 - (L_1 \cup \dots \cup L_4)$. It is easy to see that there are no other curves in the affine surface $\mathbb{P}_2 - (L_1 \cup \dots \cup L_4)$ of Euler characteristic ≤ 0, hence no other infinite family of solutions.

Proof. The theorem can be restated as follows: for every infinite sequence of solutions to (6.1), there is a sub-sum vanishing infinitely often. Also, the theorem is equivalent ot the following statement: *for every infinite set of solutions, some ratio* u_h/u_k *takes infinitely often the same value.* We shall prove the theorem under this formulation.

We follow the pattern given in Chapter II of [67] and Chapter II of [23].

We argue by induction on n, the case $n = 1$ being obvious.

Let $P_1 = (u_1^{(1)}, \dots, u_n^{(1)}), P_2 = (u_1^{(2)}, \dots, u_n^{(2)}), \dots$ be an infinite sequence of solutions to (6.1). For each place $\nu \in S$ and each index $j = 1, 2 \dots$, let i_ν^j be such that $|u_{i_\nu^j}^{(j)}| = \max_i\{|u_i^{(j)}|_\nu\}$. Up to extracting a subsequence, we can suppose that the index $i_\nu^j \in \{1, \dots, n\}$ does not depend on j. Hence we denote it by i_ν. Let us define linear forms $L_{\nu,i}$, for $i = 1, \dots, n$, $\nu \in S$, put putting

$$L_{\nu,i}(X_1 \dots, X_n) = X_i, \qquad i \neq i_\nu$$

and

$$L_{\nu,i_\nu}(X_1, \dots, X_n) = X_1 + \dots + X_n.$$

Let us estimate the double product

$$\prod_{i=1}^{n} \prod_{\nu \in S} |L_{\nu,i}(P_j)|_\nu = \left(\prod_{i=1}^{n} \prod_{\nu \in S} |u_i^{(j)}|_\nu \right) \cdot \prod_{\nu \in S} \frac{|u_1^{(j)} + \dots + u_n^{(j)}|_\nu}{\|P_j\|_\nu}.$$

Due to the fact that the $u_i^{(j)}$ are S-units, the first factor equals 1; also, due to the equation (6.1), the second factor equals $\prod_{\nu\in S}\|P_j\|_\nu^{-1} = H(P_j)^{-1}$. An application of the Subspace Theorem in the form of Theorem 3.4 provides the existence of a linear equation of the form

$$a_1u_1^{(j)} + \ldots a_nu_n^{(j)} = 0,$$

valid for infinitely many indices j. Let us consider from now on only these indeces j. Dividing out by u_n and putting $b_i = -a_i/a_n$ for $i = 1, \ldots, n-1$, we obtain another S-unit equation

$$b_1v_1 + \ldots + b_{n-1}v_{n-1} = 1$$

satisfied by $(v_1, \ldots, v_n) = (u_1u_n^{-1}, \ldots, u_{n-1}u_n^{-1})$ for infinitely many solutions $(u_1, \ldots, u_n)$ of (6.1). Up to enlarging the set S, we can suppose that all the non-vanishing coefficients b_i are S-units, so also the addends b_iv_i in the above equation are S-units. By the inductive hypothesis, a single value for some ratio b_iv_i/b_jv_j is attained infinitely often. Then the same is true for the ratio u_i/u_j, finishing the proof. □

A generalization of the S-unit equation theorem, obtained via a similar proof, reads as follows:

Theorem 6.3. *Let $V \subset \mathbb{G}_m^n$ be an algebraic sub-variety of a torus. Then the Zariski-closure of the set $V(\mathcal{O}_S)$ of integral points of V is a finite union of translates of algebraic sub-groups of $\mathbb{G}_m^n$ contained in V.*

For the proof, see [67] or [23]. □

6.2 Applications of the S-unit equation theorem

The S-unit equations appear in different contexts, so that Theorem 6.2 (and Theorem 6.3) admits numerous applications. For a survey on some of these applications, the reader is addressed to [29].

We want just to explain here the geometric pattern inherent to *any* application of the S-unit equation theorem.

Suppose we are studying the integral points on a quasi-projective variety V, and that on V one can find a regular never vanishing function f. Then (after possibly multiplying f by a fixed non-zero constant), for every S-integral point $P \in V(\mathcal{O}_S)$, the value $f(P)$ of f at P is a unit.

Suppose now that we dispose of several such functions $f_1, \ldots, f_n$, with $n > \dim V$, and that these functions are multiplicative independent modulo constants. Certainly $f_1, \ldots, f_n$ are algebraically dependent, and they satisfy at least $n - \dim V$ independent algebraic relations $P_i(f_1, \ldots, f_n) = 0$, for $i = 1, \ldots, n - \dim V$, where $P_1, \ldots, P_{n-\dim V}$ are polynomials in n variables. These equations define a proper closed sub-variety W of $\mathbb{G}_m^n$, which is not a translate of an algebraic subgroup. Moreover, the dominant map $F = (f_1, \ldots, f_n) : V \to W'$ (where W' is a component of W, image of V) sends integral points of V to integral points of W'. An application of Theorem 6.3 (with W' replacing the variety V appearing in the Theorem) enables to conclude that the integral points on V are not Zariski-dense.

We can conclude by saying that the S-unit equation theorem applies to varieties V admiting dominant maps to a sub-variety of a torus, not (isomorphic to) a torus itself.

Actually, the use of the Chevalley-Weil Theorem permits sometimes to apply the S-unit theorem in a more general situation: namely, suppose that an algebraic variety V admits an étale cover $V' \to V$ with a variety V' admitting such a map to a sub-variety of a torus. Then

one can prove via the S-unit theorem the degeneracy of integral points on V', and deduce via Chevalley-Weil the same conclusion for V.

In the case of curves, the above described technique has been used for the first time by X [65] to prove the finiteness of the integral solutions to the hyper-elliptic equation

$$y^2 = f(x) \tag{6.4}$$

where $f(x) \in \kappa[x]$ is a polynomial without quadratic factors of degree ≥ 3. The affine curve $\mathcal{C}$ defined by the above equation admits in general no morphism to $\mathbb{G}_m$, and in any case any morphism $\mathcal{C} \to \mathbb{G}_m^n$ factors through a morphism $\mathcal{C} \to \mathbb{G}_m$. Hence the S-unit equation theorem cannot be applied directly. However, there always exist an étale cover $\mathcal{C}' \to \mathcal{C}$ such that the curve $\mathcal{C}'$ admits a map $\mathcal{C}' \to \mathbb{G}_m^n$, for some $n \geq 2$, such that the image curve has positive Euler characteristic.

Here are the details: let us factor the polynomial $f(X)$ in $\bar{\mathbb{Q}}[X]$ as

$$f(X) = c \cdot \prod_{i=1}^{d} (X - \alpha_i),$$

where $d \geq 3$ is the degree of $f(X)$ and $\alpha_1, \ldots, \alpha_d$ are pairwise distinct algebraic number. Put $\kappa' = \kappa(\alpha_1, \ldots, \alpha_d)$. The function field of the affine curve $\mathcal{C}$ defined by (6.4) over κ' is $\kappa'(x)(\sqrt[d]{f(x)})$. Since the rational functions $(x - \alpha_1), \ldots, (x - \alpha_d)$ have no common zeroes on $\mathcal{C}$ and their product is a perfect d-th power, each factor is a d-th power in $\mathbb{C}[\mathcal{C}]$. Hence the field extension $\kappa'(\mathcal{C})(\sqrt[d]{x - \alpha_1}, \ldots, \sqrt[d]{x - \alpha_d})$ is unramified over the affine curve $\mathcal{C}$. Hence by Chevalley-Weil the S-integral points of $\mathcal{C}$ lifts to solutions over a fixed number field of the system of equations

$$\begin{cases} x - \alpha_1 &= y_1^d \\ x - \alpha_2 &= y_2^d \\ x - \alpha_3 &= y_3^d \end{cases} \tag{6.5}$$

(here we used just the intermediate extension $\kappa'(\mathcal{C})(\sqrt[d]{x - \alpha_1}, \sqrt[d]{x - \alpha_2}, \sqrt[d]{x - \alpha_3})/\kappa'(\mathcal{C})$, omitting the other d-th roots). From the above system of equations it follows that

$$\begin{cases} \alpha_1 - \alpha_2 &= y_2^d - y_1^d &= (y_2 - y_1) \cdot (y_2^{d-1} + \ldots + y_1^{d-1}) \\ \alpha_2 - \alpha_3 &= y_3^d - y_2^d &= (y_3 - y_2) \cdot (y_3^{d-1} + \ldots + y_2^{d-1}) \\ \alpha_3 - \alpha_1 &= y_1^d - y_3^d &= (y_1 - y_3) \cdot (y_1^{d-1} + \ldots + y_3^{d-1}) \end{cases}$$

Enlarging S so that $\alpha_i - \alpha_j$ becomes an S-units for $1 \leq i < j \leq 3$ we obtain that the three S-integers $u_1 := y_3 - y_2, u_2 := y_1 - y_3$ and $u_3 := y_2 - y_1$ are S-units. Since their sum vanishes, we apply the S-unit equation theorem and conclude easily the finiteness of the S-integral solutions to equation (6.4). The appearance of the S-units u_1, u_2, u_3 is due to the fact that the affine curve $\mathcal{C}'$ defined by the system (6.5) (endowed with an unramified map $\mathcal{C}' \to \mathcal{C}$) admits a morphism $\mathcal{C}' \to \mathbb{G}_m^2$.

A simpler application of the S-unit equation in two variables appear already with Thue's equation (4.2), as follows: letting $\mathcal{C}$ be the affine curve defined by Thue's equation (4.2), which we can re-write as

$$\prod_{i=1}^{d} (x - \alpha_i y) = c,$$

for $\alpha_1, \dots, \alpha_d$ pairwise distinct algebraic numbers, consider the map

$$\mathcal{C} \to \mathbb{P}_1 - \{(\alpha_1 : 1), \dots, (\alpha_d : 1)\} \hookrightarrow \mathbb{P}_1 - \{(\alpha_1 : 1), (\alpha_2 : 1), (\alpha_3 : 1)\} \hookrightarrow \mathbb{G}_m^2$$

sending

$$(x, y) \mapsto (x : y).$$

Then apply the S-unit equation theorem to the image into $\mathbb{G}_m^2$.

6.3 Semi-abelian varieties and quasi-Albanese maps

In this section, we partially follow Chap. III, §5.1 of [23].

Recall that a semi-abelian variety is an extension of an abelian variety by a torus, i.e. an irreducible algebraic group A sitting in an exact sequence

$$\{0\} \to \mathbb{G}_m^r \to A \to A_0 \to \{0\}.$$

Automatically, A is commutative.

If A is defined over a number field κ and $_S$ is ring of S-integers of κ, the group of integral points $A(_S)$ is finitely generated; this fact follows formally by the combination of Mordell-Weil Theorem, applied to the abelian variety A_0, and Dirichlet's Unit Theorem, applied to the torus $\mathbb{G}_m^r$ (recalling that the set of S-integral points on a torus $\mathbb{G}_m$ coincides with the group of S-units).

The mentioned theorem of Vojta, generalizing a previous one by Faltings, states the following:

Theorem 6.6. *Let A be a semi-abelian variety defined over a number field κ, $X \subset A$ an algebraic subvariety. Then the set $X(_S) = X \cap A(_S)$ is a finite union of translate of subgroups.*

It then follows formally that each of these translate is actually the set of integral points of a translate of an algebraic group entirely contained in X. In particular, if X contains no translate of algebraic subgroups of positive dimension, then $X(_S)$ is finite.

Theorem 6.6 can be restated without mentioning integrality nor rationality: simply, *the intersection $\Gamma \cap X$ between a finitely generated subgroup $\Gamma \subset A(\mathbb{C})$ and an algebraic variety $X \subset A$ is a finite union of cosets of Γ.*

We pause to discuss the applicability of the above theorem.

Let us consider first the compact case. An abelian variety A of dimension g admits g linearly independent invariant 1-forms, trivializing the sheaf Ω_A^1. Whenever a (compact) variety X can be embedded into A, the restriction to X of these 1-forms are regular 1-form on X; they remain linearly independent unless X is contained in a translate of an algebraic subgroup of A (corresponding to the linear subspace of the Lie algebra of A determined by the linear relations on the restrictions of the g forms).

More generally, whenever a variety X admits a morphism $X \to A$, whose image is not contained in a translate of an algebriac subgroup, then $H^0(X, \Omega_X^1) =: q(X) \geq g$.

Vice-versa, one can produce an abelian variety and a morphism $X \to A$ starting from the holomorphic 1-forms on X: letting $\omega_1, \dots, \omega_g$, where $g = q(X)$, be a basis of $H^0(X, \Omega_X^1)$, and $P \in X$ a point of X, the integration map

$$X \ni Q \mapsto \left(\int_P^Q \omega_1, \dots, \int_P^Q \omega_g \right) \pmod{\Lambda}, \tag{6.7}$$

where $\Lambda \subset \mathbb{C}^g$ is the $\mathbb{Z}$-module of the periods, i.e. the integrals over the loops on $X(\mathbb{C})$. The quotient $\mathbb{C}^g/\Lambda$ turns out to be an abelian variety, defined over the same field of definition for X and P. This abelian variety is called the Albanese variety of X, denoted by $\mathrm{Alb}(X)$; it has the universal property that every map from X to an abelian variety B (actually to any algebraic group) factors through the Albanese of X via a group homomorphism $\mathrm{Alb}(X) \to B$ (possibly composed with a translation). In the case of curves, one obtains Abel's construction of the jacobian variety.

Hence the 'maximal' abelian variety A such that X admits a morphism to A whose image is not contained in an proper algebraic translate is the Albanese $\mathrm{Alb}(X)$, which has dimension $q(X) = h^0(X, \Omega^1_X)$; this number is also called the irregularity of X. When $q(X) > \dim X$, one can apply Falting's Theorem (Theorem 6.6 in the compact case) which implies the degeneracy of the integral points on the image of X in $\mathrm{Alb}(X)$, hence also the degeneracy of the rational points on X.

If, on the contrary, $q(X) \leq \dim X$ then the canonical map to its Albanese is surjective, and Theorem 6.6 does not apply.

For non complete algebraic varieties, a parallel theory is possible. We address the interested reader to Chapter 5 of the book by Noguchi-Winkelmann [49]. Here we just sketch the main idea.

Every smooth quasi-projective (complex) algebraic variety X can be realized as the complement $\tilde{X} - D$ for a smooth complete variety $\tilde{X}$ and a normal crossing divisor $D \subset \tilde{X}$.

We say that a regular 1-form ω on X has logarithmic singularities on $\tilde{X}$ along D (or that ω is a logarithmic 1-form) if locally at any point p of D where D admits an equation $f_1 \cdots f_h = 0$, for $(f_1, \ldots, f_h)$ a subset of a coordinate system at p, ω can be written as

$$\omega = a_1 \frac{\mathrm{d}f_i}{f_1} + \ldots + a_h \frac{\mathrm{d}f_h}{f_h} + \text{regular form},$$

where $a_1, \ldots, a_p$ are holomorphic functions in a neighborhood of the point p. It is well known that the logarithmic 1-forms are closed (see e.g. [47]). Also, they always form a finite -dimensional vector space.

Hence one can repeat the construction performed in the compact case, by integrating a basis of logarithmic 1-forms, obtaining a map of the form (6.7) to a complex Lie group, which turns out to be a semi-abelian variety, called the quasi Albanese (or generalized Albanese) of X. It is an extension of the Albanese of $\tilde{X}$ with a torus of dimension equal to the dimension of the quotient $\{\log 1 - \text{forms}\}/\{\text{regular } 1 - \text{forms}\}$.

Let us analyze some cases. Suppose D_1, D_2 are linearly equivalent divisors on $\tilde{X}$. Then $X = \tilde{X} - (D_1 + D_2)$ admits a morphism $F : X \to \mathbb{G}_m$, where f is a function with all its poles on D_1 and all its zeros on D_2. The corresponding logarithmic 1-form is $\mathrm{d}f/f$; in that case the quasi Albanese variety of X is simply the product of the Albanese variety of $\tilde{X}$ by $\mathbb{G}_m$.

However, it is not always the case that the quasi-Albanese is a trivial extension of the Albanese. Already in the case of curves, the extension in general does not split.

Consider a non-rational complete (smooth) curve $\tilde{\mathcal{C}}$. Let $P \in \tilde{\mathcal{C}}$ be a point on $\tilde{\mathcal{C}}$. Every 1-form which is regular on $\mathcal{C} = \tilde{\mathcal{C}} - \{P\}$ having a pole of order ≤ 1 on P is in fact regular everywhere; this follows by considering the sum of the residues, which must vanish. (Alternatively, one can compare the abelianized fundamental groups of $\mathcal{C}$ and $\tilde{\mathcal{C}}$: if g is the genus of $\tilde{\mathcal{C}}$, then the fundamental group is generated by $2g$ element subject to one commutation relation; eliminating from $\tilde{\mathcal{C}}$ a single point P the commutation relation disappears, and the fundamental group of

the complement $\mathcal{C}$ of P turns out to be freely generated by $2g$ generators. Hence the inclusion $\mathcal{C} \hookrightarrow \tilde{\mathcal{C}}$ induces an isomorphism between the abelianized fundamental groups, showing that the abelian covers of the two curves correspond bijectively in a natural manner. In particular $H^1(\mathcal{C}(\mathbb{C}), \mathbb{R}) \simeq H^1(\tilde{\mathcal{C}}(\mathbb{C}), \mathbb{R}) \simeq \mathbb{R}^{2g})$.

Consider now the complement of two point P_1, P_2 on $\tilde{\mathcal{C}}$. Now, by Riemann-Roch it follows that $h^0(\tilde{\mathcal{C}}, \Omega^1_{\tilde{\mathcal{C}}}(P+Q)) = g+1 > h^0(\tilde{\mathcal{C}}, \Omega^1_{\tilde{\mathcal{C}}})$, hence we obtain an extra logarithmic 1-form which is not a regular one.

Whenever the class of $[P_1] - [P_2]$ in the jacobian of $\tilde{\mathcal{C}}$ (identified with $\mathrm{Pic}^0(\tilde{\mathcal{C}})$ is torsion, one can find a function f having all its zeros on P_1 and its poles on P_2, thus providing a morphism $\mathcal{C} = \tilde{\mathcal{C}} - \{P_1, P_2\} \to \mathbb{G}_m$. If, however, $[P_1] - [P_2]$ is not torsion on the jacobian, such a morphism does not exist, although the logarithmic 1-form with poles at P_1, P_2 still exists.

Note that the two points P_1, P_2 on $\tilde{\mathcal{C}}$ are in any case algebraically equivalent, and this fact suffices o produce the logarithmic 1-form.

This principle has been exploit by Vojta and Noguchi-Winkelmann to produce maps to a semi-abelian variety from an algebraic varieties with sufficiently many components at infinity compared with the rank of the Néron-Severi group. See for instance the main theorem in [48].

We now exploit this same principle to a curious Diophantine problem, also considered in [23].

We first introduce some notation: let an elliptic curve over $\mathbb{Q}$ be defined by a Weierstrass equation

$$y^2 = x^3 + ax + b, \tag{6.8}$$

where $a, b \in \mathbb{Z}$ are integers with $4a^3 - 27b^2 \neq 0$. For a rational solution $P = (x, y) \in \mathbb{Q}^2$ of the above equation, one can write the rational numbers x, y in a unique way as

$$x = \frac{u}{d^2}, \quad y = \frac{v}{d^3},$$

for integers u, v, d without common factor, $d > 0$. Denote by $d(P)$ the positive number d appearing in the above formulae. The primes dividing $d(P)$ are precisely the primes modulo which the point reduces to the (unique) point at infinity of the completion of the curve defined by the above equation.

We propose the following conjecture, inspired by a result in complex analysis (see the main theorem in [16]), which would follows from Vojta's Conjecture, as we shall explain in a moment:

Conjecture. *Let E_1, E_2 be two elliptic curves defined over the rational integers by a Weierstrass equation. If there exist infinitely many pairs $(P_1, P_2) \in E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$ with*

$$d(P_1) = d(P_2) \tag{6.9}$$

then E_1 is isomorphic to E_2 over the rationals and for all but finitely many such pairs $P_1 = \pm P_2$.

(In the above equation the symbol $d(P_1)$ denotes the denominator-function attached to E_1 while $d(P_2)$ denotes the denominator-function attached to E_1).

Note that this statement, already in the particular case $E_1 = E_2$, constitues a strong generalization of Siegel's finiteness theorem for integral points on curves. In fact, Siegel's theorem is equivalent to saying that $d(P)$ can be 1 only finitely many times. It is easy to derive from Siegel's theorem that each value of $d(P)$ can be attained only finitely often. The proposed conjecture

implies that only finitely many values of $d(P)$ can be attained more than two times (i.e. for other points then $\pm P$).

Let us show how to reduce to a question on integral points on a quasi-projective variety, to which Vojta's Conjecture can be applied.

For this purpose, we first note that the condition $d(P_2) = d(P_2)$ can be restated by saying that P_1 reduces to the origin $O_1 \in E_1$ modulo some prime only if P_2 reduces to the origin $O_2 \in E_2$ modulo the same prime, with the same multiplicity. So the pair $(P_1, P_2) \in E_1 \times E_2$ does not reduce, modulo any prime, to the divisor $\{O_1\} \times E_2 + E_1 \times \{O_2\}$ unless it reduces to the single point (O_1, O_2).

Let then $\tilde{X}$ be the surface obtained by blowing-up the origin (O_1, O_2) in $E_1 \times E_2$. Let $D_1 \subset \tilde{X}$ be the strict transform of the divisor $\{O_1\} \times E_2$ and D_2 the strict transform of the divisor $E_1 \times \{O_2\}$. Then the solutions to equation (6.9) correspond to the integral points on $X := \tilde{X} - (D_1 + D_2)$.

Letting L be the exceptional divisor of the blow-up $\tilde{X} \to E_1 \times E_2$, the canonical divisor of $\tilde{X}$ turns out to be (linearly equivalent to) L. Then the sum of the divisor at infinity of X plus the canonical divisor is $D_1 + D_2 + L$. Note that $2(D_1 + D_2 + L) = (D_1 + D_2) + (D_1 + D_2 + 2L)$ and that the second addend is the pull-back of the ample divisor $\{O_1\} \times E_2 + E_1 \times \{O_2\}$; hence $(D_1 + D_2 + 2L)$ is a big divisor, and so is the sum $2(D_1 + D_2 + L)$ and $D_1 + D_2 + L$. Hence Vojta's Conjecture applies, and provides (conjecturally) the degeneracy of the integral points on X. To deduce the strong conclusion of our Conjecture, we need to classify the possible infinite families of solutions, corresponding to curves integral points on curves on X. By Siegel's theorem, such curves must be non-hyperbolic; we conclude via the following

Lemma 6.10. *In the above notation, if the elliptic curve E_1 is not isomorphic to E_2, the only non-hyperbolic curve on X is the intersection with X of the exceptional divisor L of the blow-up $\tilde{X} \to E_1 \times E_2$. If E_1 is isomorphic to E_2 (over $\mathbb{C}$) the quasi-projective variety contains complete non-hyperbolic curves, which are all obtained as pre-image in X of algebraic subgroups in $E_1 \times E_2$ of the form $\{(P, Q) \in E_1 \times E_2 \,|\, Q = \Phi(P)\}$ for some isomorphism $\Phi : E_1 \to E_2$. If $E_1 = E_2$ has no complex multiplication, the only such subgroups are defined by equations of the form $P = \pm Q$.*

The proof is rather easy; we address to Ch. 4, §5.1 of the book [23] for the details. Note that the extra non-hyperbolic curves arising in case of complex multiplication are irrelevant for our problem, since the $\mathbb{Q}$-rational points on such curves cannot be Zariski-dense.

Unfortunately, we cannot prove the degeneracy of the integral points on that surface X, so our conjecture is still an open problem. However we can prove, using Theorem 6.6, the following weaker result:

Theorem 6.11. *Let E_1, E_2 be two elliptic curves in Weierstrass equation, with origins O_1, O_2 respectively. Let $A_1 \neq O_1$ (resp. $A_2 \neq O_2$) be a rational point on E_1 (resp. E_2). Suppose there are infinitely many pairs $(P_1, P_2) \in E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$ such that*

$$d(P_1) = d(P_2) \qquad \text{and} \qquad d(P_1 - A_1) = d(P_2 - A_2). \tag{6.12}$$

Then E_1 is isomorphic to E_2 over $\mathbb{Q}$ and after identifying $E_1 \simeq E_2$ we have $A_1 = A_2$ and, unless $2A_1 = O$, for all but finitely solutions of (6.12), $P_1 = P_2$. If $A_1 = A_2$ has order two, then for all but finitely many solutions $P_1 = \pm P_2$.

Proof. Let us denote by O_i, $i = 1, 2$, the point at infinity of the curve E_i, which we take as neutral element for the group law.

We start by noting that for $(P_1, P_2) \in (E_1 \times E_2)(\mathbb{Q})$, the condition (6.12) means that "*for every integer m, P_1 reduces to 0_1 modulo m if and only if P_2 reduces to O_2 modulo m and it reduces to A_1 modulo m if and only if P_2 also to A_2 modulo m*".

In geometric terms, the point (P_1, P_2) reduces to the divisor $\{O_1\} \times E_2 + E_1 \times \{O_2\}$ only when (P_1, P_2) reduces to the point (O_1, O_2) and it reduces to the divisor $\{A_1\} \times E_2 + E_1 \times \{O_2\}$ only if it reduces to the point (A_1, A_2).

More precisely, define $\tilde{Y} \to E_1 \times E_2$ to be the blow-up of the abelian surface $E_1 \times E_2$ over the two points (O_1, O_2), (A_1, A_2).

Let D_1 (resp. D_2) be the strict transform of $\{O_1\} \times E_2$ (resp. $E_1 \times \{O_2\}$) and C_1 (resp. C_2) the strict transforms of the divisor $\{A_1\} \times E_2$ (resp. $E_1 \times \{A_2\}$).

Then a rational point $R \in \tilde{X}(\mathbb{Q})$, not belonging to the exceptional divisors, lying over a point $(P_1, P_2) \in (E_1 \times E_2)(\mathbb{Q})$ is integral with respect to $D_1 + D_2 + C_1 + C_2$ if and only if (P_1, P_2) is a solution to equation (6.12). Hence the solutions to our equation (6.12) correspond to the integral points on the quasi-projective surface $Y := \tilde{Y} - (D_1 + D_2 + C_1 + C_2)$.

Note the natural morphism $Y \to X$, sending integral points on Y to integral points on X. A generic integral point on X, however, might lift to a rational non-integral point on Y.

We would like to apply Theorem 6.6 to the quasi projective variety Y. The presence of a dominant map $Y \to E_1 \times E_2$ guarantees that the logarithmic irregularity of Y is at least $2 = \dim Y$. Moreover, the complete variety $\tilde{Y}$ has irregularity exactly 2, being birational to an abelian surface. Our aim is to exploit the divisors that we removed to produce a 1-form with logarithmic singularities along the removed divisors, thus producing a map to an semi-abelian variety of dimension 3.

As we remarked, on the first elliptic curve E_1 one can construct a meromorphic 1-form ω_1 with simple poles at O_1 and A_1; automatically, the residues will be the opposite one of the other; we can suppose that the residue at O_1 is $2\pi i$, while at A_1 is $-2\pi i$. We can do the same on the second elliptic curve E_2, producing a meromorphic 1-form ω_2 with simple poles at O_2, A_2 and corresponding residues $2\pi i, -2\pi i$.

Denoting by $\pi_i : \tilde{Y} \to E_i$ the canonical projections, let us compute the pole divisor of the 1-form on $\tilde{Y}$

$$\omega := \pi_1^* \omega_1 - \pi_2^* \omega_2.$$

Certainly, it has simple poles at D_1, D_2, C_1, C_2 and is regular at any point not sent to $A_1, O_1, A_2 O_2$ by the two projections. It only remains to check what happens over the exceptional divisors of the blow-up. We claim that these divisors are not poles of ω. Let us make the explicit calculation in local coordinates. Let t be a local parameter at O_1 in E_1 and s a local parameter at O_2 in E_2. Up to a regular term, the forms ω_1, ω_2 are expressed loally as

$$\omega_1 = \frac{\mathrm{d}t}{t}, \qquad \omega_2 = \frac{\mathrm{d}s}{s}.$$

The blow-up of the point (O_1, O_2) on the surface $E_1 \times E_2$ can be locally described by the equation

$$t\eta = s\xi, \qquad (t, s) \in \mathbb{C}^2, (\xi : \eta) \in \mathbb{P}_1,$$

and the exceptional divisor lies over $(t, s) = (0, 0)$.

Over the opens set $(\xi : \eta) \neq (1 : 0)$, we can put $\eta = 1$ and use the coordinates s, ξ, while

$$t = s \cdot \xi.$$

Then the 1-form ω can be written as

$$\omega = \frac{\mathrm{d}t}{t} - \frac{\mathrm{d}s}{s} = \frac{s\mathrm{d}\xi}{s\xi} + \frac{\xi \mathrm{d}s}{s\xi} - \frac{\mathrm{d}s}{s} = \frac{\mathrm{d}\xi}{\xi},$$

which is regular. Hence ω is regular on Y, with logarithmic poles at infinity. It follows that the generalized Albanese variety of Y is three-dimensional, being an extension of $E_1 \times E_2$ by $\mathbb{G}_m$.

Then Vojta's Theorem 6.6 applies and implies the degeneracy of the integral points on Y.

Now, the possible infinite families of solutions, corresponding to curves on Y, also provide infinite families on X, and these have beeen already classified in Lemma 6.10. We obtain that if such infinite families do exist, $E_1$and E_2 are isomorphic and after identifying E_1 with E_2 the pairs (P_1, P_2) satisy $P_1 = \pm P_2$. But the curve defined by $P_1 = P_2$ gives rise to a complete curve on Y (hence non-hyperbolic) only if $A_1 = A_2$; so if such infinite family of solutions exist, we must have $A_1 = A_2$. Otherwise, the only infinite family must be that of the form $P_12 = -P_2$, which again can exist only if $A_1 = -A_2$. In that case, after applying applying to E_2 the automorphism $P \mapsto -P$, we obtain another identification between E_1 and E_2 under which A_1 coincides with A_2. If $A_1 = A_2$ is of order 2, then both infinite families are present. □

We end the discussion on Theroem 6.11 by making the parallel with a classical arithmetical problem of Erdös and Woods.

For a natural number $n \in \mathbb{N}$, denote by $\mathcal{P}(n)$ its set of its prime divisors: suppose that two natural numbers m, n satisfy the two equalities of sets:

$$\begin{array}{rcl} \mathcal{P}(m) & = & \mathcal{P}(n) \\ \mathcal{P}(m+1) & = & \mathcal{P}(n+1). \end{array}$$

Can one derive the equality $m = n$? The answer is known to be negative, as shown by the infinite family of pairs

$$m = 2(2^h - 1), \qquad n = 2^{h+2}(2^h - 1)$$

so that $m + 1 = 2^{h+1} - 1$ and $n + 1 = 2^{2h+2} - 2^{h+2} + 10(m + 1)^2$. However, no infinite families of pairs $m < n$ with

$$\begin{array}{rcl} \mathcal{P}(m) & = & \mathcal{P}(n) \\ \mathcal{P}(m+1) & = & \mathcal{P}(n+1) \\ \mathcal{P}(m+2) & = & \mathcal{P}(n+2) \end{array}$$

are known. Erdös and Woods conjectured that there exists an integer k such that, given two natural numbers m, n, the equalities $\mathrm{P}(m+i) = \mathrm{P}(n+i)$ for $i = 0, \ldots, k-1$ implies the equality $x = y$.

Of course, in the equality of sets $\mathcal{P}(m) = \mathcal{P}(n)$ one does not take into account the multiplicities with which the primes appear in the factorizations of m and n. If one wants to take into account these multiplicities, it is necessary to disregard a finite set of primes, in order to avoid trivialities.

Then a natural analogue with multiplicity of the Erdös-Woods problem might be asking whether several consecutive ratios x/y, $(x+1)/(y+1)$,..., $(x+k)/(y+k)$ can consist of S-units.

In this respect, we can prove the following

Theorem 6.13. *Let $\mathcal{O}_S \subset \mathbb{Q}$ be a finitely generated ring. If the group of units $\mathcal{O}_S^*$ is infinite, there exist infinitely many pairs of distinct natural numbers $m < n$ such that*

$$\begin{cases} \frac{n}{m} & \in \mathcal{O}_S^* \\ \frac{n+1}{m+1} & \in \mathcal{O}_S^*. \end{cases}$$

For every finitely generated ring $\mathcal{O}_S \subset \mathbb{Q}$, the system

$$\begin{cases} \frac{n}{m} & \in \mathcal{O}_S^* \\ \frac{n+1}{m+1} & \in \mathcal{O}_S^* \\ \frac{n+2}{m+2} & \in \mathcal{O}_S^* \end{cases}$$

has only finitely many solutions.

The first part of the Theorem can be interpreted as a density result for the integral points on a certain surface, and will be discussed in the last section.

The finiteness statement can be easily deduced from the S-units equation theorem in three variables, i.e. once again can be interpreted as a result on integral points on surfaces, the topic of next section.

7 Integral points on surfaces

We shall consider now several further problems reducing to integral or rational points on surfaces. We partially follow the presentation in [14].

We first consider the problem of rational points. In that case we can consider surfaces up to birational isomorphism.

The birational classification of (complex) algebraic surfaces was carried out by the Italian school at the end of the 19th century, and let to the following list

- Rational surfaces. These are the surfaces birationally isomorphic to the plane; it is the case of all smooth hypersurfaces of degree ≤ 3 in projective 3-space.
- Ruled surfaces, i.e. surfaces birationally isomorphic to a product $\tilde{\mathcal{C}} \times \mathbb{P}_1$, where $\mathcal{C}$ is a curve (if $\mathcal{C}$ is the line, then the resulting surface will be rational).
- Elliptic surfaces. They can be thought of as elliptic curves over a 1-dimensional function field; in other words they are surfaces admitting a dominant map $\tilde{X} \dashrightarrow \tilde{\mathcal{C}}$ whose generic fibre has genus one. They can belong to other families (e.g. they can be rational).
- Abelian surfaces, i.e. abelian varieties of dimension two.
- K3 surfaces. These are (smooth projective) surfaces which are simply connected and whose canonical bundle is trivial. Being simply connected, they admit no non-zero regular 1-forms, so their cotangent bundle is certainly not trivial, unlike what happens for abelian surfaces. They might admit a fibration to $\mathbb{P}_1$, with elliptic generic fiber, so they can be elliptic in our sense. All smooth quartics in $\mathbb{P}_3$ are K3 surfaces, as well as the smooth hypersurfaces of multi-degree $(2,2,2)$ in $\mathbb{P}_1^3$.
- Kummer, bielliptic (or hyper-elliptic) and Enriques surfaces. They are obtained as quotients of abelian surfaces. For instance a Kummer surface is the normalization of the quotient of the form $A/\pm \mathrm{Id}$, where A is an abelian surface and $-\mathrm{Id}$ is the involution of A sending $P \mapsto -P$.

- Surfaces of general type: all the remaining ones. They are characterised by having a canonical divisor which is big. It is the case for all smooth hypersurfaces of $\mathbb{P}_3$ of degree ≥ 5, as well as those with irregularity ≥ 2 which are not abelian varieties.

According to Bombieri's Conjecture (Lang-Vojta's Conjecture in the case of compact surfaces) the set of reational points on surfaces of general should be degenerate.

Let us then analyze the other classes of surfaces.

The rational points on rational surfaces are clearly potentially dense. The same is true of the ruled surfaces with elliptic base.

Elliptic surfaces with rational base can have a Zariski-dense set of rational points, e.g. whenever they admit a section of infinite order (with respect to the group law on the fibers).

Abelian varieties over admit algebraic points which generate a Zariski dense group: hence the rational points are potentially dense.

Little is known in general on K3 surfaces, but in several cases (e.g. when they admit elliptic fibrations) one can show the potential density of rational points, which is believed to hold in general.

Kummer and bielliptic surface always satisfy potential density of rational points, since they are dominated by abelian varieties.

Finally the Enriques surfaces, which always admit elliptic fibrations, are known to satisfy potential density of rational points (see [9]).

We shall concentrate from now on on integral points on surfaces. We have already remarked, while discussing Vojta's Conjecture at §1.4, that the complement in $\mathbb{P}_2$ of a curve of degree ≥ 4, with normal crossing singularities, is conjectured to have degenerate sets of integral points. We said that this question is open, the only general result being proved when the curve has at least four components. We add that in some cases the degeneracy of integral points has been proved on the complement of an irreducible curve (see [33], [68], [41]) ; however the method of proof, consisting on increasing the number of components at infinity after taking an unramified cover, only works for highly singular curves, never for curves with normal crossing singularities.

The degeneracy on the complement of a four component curve on $\mathbb{P}_2$ is proved by mapping $\mathbb{P}_2 - D$, where D is a curve with $r \geq 4$ components, to $\mathbb{G}_m^{r-1}$. This map is constructed from functions having zeros and poles in the support of D, and there exist $r-1$ multiplicative independent functions of that type, since any two divisors on $\mathbb{P}_2$ are linearly dependent in the Picard group. The same strategy holds if one removes four (or more) divisors on any algebraic surface whenever they define a rank-1 subgroup in the Picard group.

This number four can be compared with the number three in Siegel's Theorem 4.3: recall that a basically equivalent formulation of Siegel's Theorem on curves states that on every affine curve with at least three points at infinity, the set of integral points is finite.

However, in higher dimensions, one cannot expect to prove any degeneracy result valid for all surfaces with four divisors removed; actually, for every number n one can easily construct an affine surface whose set of integral points is Zariski dense and whose divisor at infinity consists of n components: simply starting from the affine plane $\mathbb{A}^2$, viewed as a complement of a line in the projective plane; after blowing-up $n-1$ points at infinity, the same affine plane becomes the complement in a projective surface of a set of $n-1$ curves (and the full divisor at infinity admits normal crossing singularities).

The aim of the next section is to provide a criterion involving the intersection matrix of the divisor at infinity.

7.1 A Subspace Theorem approach

Most of the results and proofs in this section are based on the paper [18].

Here is the announced general statement on integral points on curves:

Theorem 7.1. *Let $\tilde{X}$ be a smooth projective surface, $D_1, \ldots, D_r$ be irreducible curves, no three of them intersecting. Assume there exist positive integers $p_1, \ldots, p_r$ such that*

- *the divisor $D = p_1 D_1 + \ldots + p_r D_r$ is big and numerically effective;*
- *for each $i = 1, \ldots, r$, letting ξ be the minimal (real) solution to the equation*

$$D_i^2 \xi^2 - 2(D.D_i)\xi + D^2 = 0,$$

(which, by Hodge index theorem, admits real solutions, since D is big and nef) the inequality

$$2\xi D^2 > (D.D_i)\xi^2 + 3p_i D^2 \tag{7.2}$$

holds.

Then there exists a (possibly reducible) curve $Y \subset X := \tilde{X} - |D|$ such that for every ring of S-integers $\mathcal{O}_S$, the set $X(\mathcal{O}_S) - Y(\mathcal{O}_S)$ of the S-integral points on X not lying on Y is finite.

In particular, the set $X(\mathcal{O}_S)$ is not Zariski-dense, but the conclusion of the theorem is stronger, since it implies that the 1-dimensional part of the Zariski-closure of the set of integral points is independent of $\mathcal{O}_S$ (for a sufficiently large ring $\mathcal{O}_S$).

The idea of the proof is the same as the one for Siegel's theorem: consider a finite dimensional vector space of regular functions on $X = \tilde{X} - |D|$.

Seppose we dispose of an infinite sequence $P_1, P_2, \ldots$ of S-integral points of X.

Letting $f_1, \ldots, f_d$ be a basis for this vector space; after possibly multiplying each function by a non-zero integer, we obtain that $f_1, \ldots, f_d$ take S-integral values at the S-integral points of X.

Since $\tilde{X}(\kappa_\nu)$ is compact for every valuation, in particular for every valuation in S, from any sequence of integral points one can extract a sequence of points converging in each valuation of S. Since the values of the function f_i at S-integral points are bounded by 1 in each valuation outside S, the height of $f_i(P)$, for P an S-integral point, must be given by some absolute values in S. This means that the sequence converges to some point at infinity $Q_\nu \in |D|(\kappa_\nu)$ in at least one valuation ν of S.

Let us find a new basis $g_1, \ldots, g_d$ of the κ-vector space generated by $f_1, \ldots, f_d$, such that the product $g_1(P) \cdots g_d(P)$ is as small as possible at the place ν. Recall that the f_i might have poles at the divisor at infinity; however, by making suitable linear combinations of them, we can hope to find functions $g_1, \ldots, g_d$ whose products has more zeros than poles at each component at infinity containing Q_ν. Expressing the $g_i = g_{i\,nu}$ as linear combination, $g_{i,\nu} = L_{i,\nu}(f_1, \ldots, f_d)$, where $L_i(T_1, \ldots, T_d)$ is a linear form with rational coefficients, we obtain "small" values, with respect to the place ν, of the form $L_i(f_1(P), \ldots, f_d(P))$, for each S-integral point P of the selected infinite sequence.

If this procedure can be performed at every valuation of S, then the double product

$$\prod_{\nu \in S} \prod_{i=1}^{d} \frac{|L_{i,\nu}(f_1(P), \ldots, f_d(P))|_\nu}{\max(|f_j(P)|_\nu)}$$

will be smaller than a suitable negative power of the height of the point $(f_1(P), \dots, f_d(P))$. An application of the Subspace Theorem will permit to conclude that some fixed non-zero linear form in $f_1, \dots, f_d$ vanishes for infinitely many point of the sequence.

Since this must hold for every subsequence of the given sequence, the degeneracy follows easily.

The main difference between dimension one and higher dimension lies in the fact that the irreducible component of a divisor on a curve are single points, while on a surface they are curves. Now, given a vector space of regular functions (say) on a neighborhood of a point P on a curve, the subspace of those having at that point a zero of order k has codimension $\leq k$ on the whole space.

Replacing the point P on a curve with a curve C on a surface, things change dramatically. The subspace of the functions vanishing on C is no more a hyperplane on the whole space. Its codimension depends on the geometry of the curve C relatively to the vector space of rational functions.

In the case of our concern, when the vector space of functions is the full linear system attached to a divisor, the codimension of those functions vanishing on C can be estimated via the following lemma:

Lemma 7.3. *Let $\tilde{X}$ be a smooth complete surface. Let D be a divisor on $\tilde{X}$ and C an irreducible curve on D. Then*

$$\dim(H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D))/H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D-C)) \leq \max(0, 1 + D \cdot C).$$

In the above formula, the symbol $D \cdot C$ denotes the intersection product of D and C.

The lemma can be applied also when C is a component of D; it then give an estimate of the codimension of the subspace of $H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D))$ formed by those functions having a pole on C of lesser order than the generic one of $H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D))$.

The proof follows by taking the cohomology of the short exact sequenc

$$0 \to \mathcal{O}_{\tilde{X}}(D-C) \to \mathcal{O}_{\tilde{X}}(D) \to \mathcal{O}_{\tilde{X}}(D)_{|C} \to 0.$$

The first steps of the long cohomology sequence

$$0 \to H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D-C)) \to H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D)) \to H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D)_{|C}) \to \dots$$

provides an embedding

$$H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D))/H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D-C)) \hookrightarrow H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D)_{|C}) = H^0(C, \mathcal{O}_{\tilde{X}}(D)_{|C}).$$

The last term is the space of global sections of a line bundle of degree $D \cdot C$ on an irreducible curve. Hence its dimension is bounded by $1 + D \cdot C$ and the lemma follows.

The above estimates are responsible for the apparence of the intersection products on the statement of Theorem 7.1.

The details of the proof can be found in [18], [14], [23] or in Bilu's Bourbaki lecture [6].

Let us comment on the condition expressed by the inequalities (7.2). Whenever the divisors $D_1 \, ldots, D_r$ are algebraically equivalent (or more general algebraically equivalent up to multiplicative constant), it turns out that one can find some weights $p_1, \dots, p_r$ verifying (7.2) for all $i = 1, \dots, r$ if and only if $r \geq 4$. This fact is in accordance with the fact that removing three lines on the plane one still obtain a surface with potentially dense integral points.

On the other hand, A. Levin and P. Autissier (see [41] or [6]) proved that whenever the D_i are ample divisors, the hypothesis of Theorem 7.1 again reduces to $r \geq 4$. As observed by Levin in his paper [41], for every smooth projective algebraic surface $\tilde{X}$, the complement of four ample divisors is of log-general type (while, once again, the example of $\mathbb{P}_2$ – (three lines) shows that the number 4 cannot be lowered to 3.

Another interesting case to which Theorem 7.1 can be applied is shown in the next statement, proved in [20].

Corollary 7.4. *Let D_1, D_2, D_3 be three ample algebraically equivalent divisors on a smooth complete surface $\tilde{X}$. Let D_4 be any divisor with $D_4 \cdot D_1 > 0$. Then the integral points on $X = \tilde{X} - (D_1 \cup \ldots \cup D_4)$ are not Zariski-dense.*

The method introduced in [18] has been much developed in higher dimensions by Levin and Autissier (see [41], [1], [2], [6]).

7.2 Integral points on certain rational surfaces

In view of the fact that the set of rational points on a rational surface is potentially dense, and in some sense denser than on any other kind of surfaces (at least according to Manin's conjecture) it is tempting to investigate the behaviour of integral points on affine (or quasi-projective) rational surfaces.

We have already discussed in some detail the case of the complement of a curve in the projective plane.

After the projective plane, the first natural example of a rational surface is constituted by (smooth) quadric surfaces on $\mathbb{P}_3$. These surfaces can be identified with $\mathbb{P}_1 \times \mathbb{P}_1$ and the divisors on it are identified modulo linear equivalence by their bi-degree. The canonical divisors have bi-digree $(-2, -2)$, hence it is conjecture that the removal of a divisor of bidegree (a, b) with $a \geq 3$, $b \geq 3$ (and normal corssing singularities) produces an affine surface with degenerate sets of integral points.

Again, this is not settled in general, but can be proved whenever the divisor at infinity has at least four components. However, one case of a divisor with three components was provided in [20]:

Theorem 7.5. *Let $\tilde{Q} \subset \mathbb{P}_3$ be a smooth quadric surface, H_1, H_2, H_3 irreducible hyperplane sections sharing a common point where they intersect transversally. Then the integral points on $\tilde{Q} - (H_1 \cup H_2 \cup H_3)$ are not Zariski-dense.*

The proof consists on reducing to the situation of Corollary 7.4 after blowing up the point of intersection of H_1, H_2, H_3. Letting $\tilde{X}$ denote the new surface, D_i, for $i = 1, 2, 3$, the strict transform of H_i and D_4 the exceptional divisor, we can apply the corollary. Since the integral points on $\tilde{X} - (D_1 \cup D_2 \cup D_3 \cup D_4)$ correspond bijectively to the integral points on $\tilde{Q} - (H_1 \cup H_2 \cup H_3)$ the conclusion of Corollary 7.4 implies the conclusion of the theorem.

The integral points on the surface $\tilde{Q} - (H_1 \cup H_2 \cup H_3)$ can be viewed as the solution to a divisibility problem, as we now explain, following [20], §4.

Suppose that $\tilde{Q}$ is given in $\mathbb{P}_3$ by the homogeneous equation

$$X_0(X_1 + X_2 + X_3) = Q(X_1, X_2, X_3),$$

for a quadratic form Q in three variables (chosen so that the above equation defines a smooth surface). Take for H_i the hyperplane section defined by $x_i = 0$, for $i = 1, 2, 3$. The three curves H_1, H_2, H_3 meet at the point $(1 : 0 : 0 : 0)$. A rational point $(x_0 : x_1 : x_2 : x_3) \in \mathbb{P}_3(\kappa)$ is integral with respect to these three divisors if coordinates can be chose such that $y := x_0$ is an S-integer, while $u := x_1, v := x_2, w := x_3$ are S-units. We then obtain the Diophantine equation

$$y(u + v + w) = Q(u, v, w),$$

which is equivalent to the integrality condition

$$\frac{Q(u, v, w)}{u + v + w} \in \mathcal{O}_S.$$

Several other problems on integral points on rational surfaces can be reduced to divisibility problems. Even in dimension one, Siegel's finiteness result, in the case of rational curves, can be expressed in terms of divisibility: *given two coprime polynomials $f(X), g(X) \in \mathcal{O}_S[X]$, if for infinitely many S-integers $x \in \mathcal{O}_S$ $f(x)$ divides $g(x)$ in the ring $\mathcal{O}_S$, then f has at most one complex root.*

Considering polynomials in two variables, some extensions of the above statement are possible. The S-unit equation theorem for three variables is an example. Solvin the equation $u + v + w = 1$ in S-units amounts to finding two S-integers $x, y \in \mathcal{O}_S$ such that

$$x \,|\, 1, \qquad y \,|\, 1, \qquad (1 - x - y) \,|\, 1,$$

so the values of three polynomials, namely $X, Y, 1 - X - Y$, divide the values of three more polynomials, in this case all taken to be the constant 1 polynomial.

By applying once again Theorem 7.1, it was proved in [22] the following

Theorem 7.6. *Let, for $i = 1, 2, 3$, $(f_i(X, Y), g_i(X, Y))$ three pairs of non-zero polynomials satisfying $\deg f_i \geq deg g_i$. Suppose they satisfy the general position assumptions below. Then the set of pairs of S-integers $(x, y) \in \mathcal{O}_S^2$ such that*

$$f_i(x, y) \,|\, g_i(x, y)$$

for $i = 1, 2, 3$, are not Zariski-dense in the plane.

The general position assumptions:

- for each $1 \leq i < j \leq 3$ the curves of equation $f_i = 0$ and $f_j = 0$ do not meet at infinity (under the canonical embedding $\mathbb{A}^2 \hookrightarrow \mathbb{P}_2$).
- there exist no common zero to the three polynomials f_1, f_2, f_3
- for each i such that the polynomial g_i is not constant, the two affine curves $f_i = 0$ and $g_i = 0$ intersect transversely.
- for $1 \leq i < j$ and $h \in \{i, j\}$, the three curves $f_i = 0$, $f_j = 0$ and $g_h = 0$ have no points in common.

As mentioned, the S-unit equation theorem is the case $\deg f_i = 1$ and $\deg g_i = 0$ for each $i = 1, 2, 3$.

Already the case in which $deg f_i = \deg g_i = 1$ for $i = 1, 2, 3$ escapes from any attempt based on the S-unit equation theorem, and leads to the following result.

Theorem 7.7. *Let $L_1, \dots, L_4$ be four lines in general position on the projective plane. Let $P_i \in L_i$, for $i = 1, 2, 3$, be a point of L_i, not belonging to other lines on the configuration. Let $\tilde{X}$ be the surface obtained by blowing-up the three points P_1, P_2, P_3 and let D_i be the strict transform of L_i, for $i = 1, 2, 3, 4$. Then the integral points on $X = \tilde{X} - (D_1 \cup D_2 \cup D_3 \cup D_4)$ are not Zariski-dense.*

Let us show the link between the above statement and divisibility problems; this example will show how to connect in general divisibility questions to problems on integral points on varieties.

Suppose L_4 is the line at infinity, so that the integral points with respect to L_4 are the pairs of S-integers $(x, y) \in \mathbb{A}^2(\mathcal{O}_S)$.

If $f_i = 0$ is the equation of L_i, for $i = 1, 2, 3$, the points P_i can be defined by a system of equations $f_i = g_i = 0$.

Now the condition that $g_i(x, y)/f_i(x, y)$ be an integer, amounts to saying that no prime divides $f_i(x, y)$ unless it divides also $g_i(x, y)$, and in that case it must divide $g_i(x, y)$ with at least the same multiplicity. Geometrically, this means that after blowing-up the point P_i, the corresponding point induced by (x, y) on the blowun-up surface does not reduce to the strict transform of the line $f_i = 0$.

An interesting feature of the surface appearing in Theorem 7.7 is that *the surface X in Theorem 7.7 is simply connected.* As we explained in the discussion following Theorem 6.6, when a smooth (projective or quasi-projective) variety is simply connected, no method based on S-unit equations or on abelian varieties can be applied, since the log-irregularity vanishes.

We have discussed surfaces of degree 1 and 2 in the three-space. The next step is represented by the cubic surfaces, which are still rational.

Recall that a smooth cubic surface can be realized from blowing-up the plane over six points, not all on a conic and no three of them on a line. The immersion is provided by the linear system of cubic curves passing through the six given points.

7.3 Around Vojta's Conjectures

In this last section, we present some remarks around Vojta's conjecture.

We shall show with a simple example that the normal crossing condition in Vojtas' conjecture cannot be removed.

Consider the case of a conic and two non-tangent lines intersecting on the conic. After a coordinate change we can suppose that the lines are defined by $ZX = 0$ and the conic by $XY + YZ = Z^2$, so the three components meet at the point $(0 : 1 : 0)$. The integral points on the complement of the pair of lines correspond to pairs (u, y) with $u \in \mathcal{O}_S^*$ and $y \in \mathcal{O}_S$.

The further integrality requirement, due to the removal of the conic, amounts to imposing that $uy - y + 1$ be an S-unit. We then obtain the equation

$$v = uy - y + 1,$$

which can be written in the form of a divisibility problem

$$\frac{v - 1}{u - 1} \in \mathcal{O}_S. \tag{7.8}$$

Clearly, over a sufficiently large ring of S-integers, the solutions are Zariski dense (in the plane). For instance, there exist infinitely many pairs of natural numbers (m, n) such that

$$\frac{3^m - 1}{2^n - 1} \in \mathbb{Z}.$$

It suffices to chose an odd number n, so that $2^n - 1$ i coprime with 3, and to set m to be the order of 3 modulo $2^n - 1$.

The first part of Theorem 6.13 is reduced to the density of the solution of a divisibility relation like (7.8).

As a second remark, we point out a curious coincidence; consider a smooth irreducible curve $D \subset \mathbb{P}_2$ in the plane. As we said, Vojta's Conjecture predicts the degeneracy of the integral points on the complement $\mathbb{P}_2 \setminus D$ when $\deg D \geq 4$.

Also, the same conjecture, referred to lower dimension and to the compact case, which is Falting's theorem, predicts the degeneracy of the rational points on D precisely whenever $\deg D \geq 4$.

When D is reducible, say the union of two smooth curves D_1, D_2 intersecting transversally, the condition of Vojta's conjecture becomes $\deg D_1 + \deg D_2 \geq 4$. In that case, one should compare with the condition on Vojta's conjecture for *integral* points on D_1 relative to the divisor $D_1 \cap D_2$ and on D_2 relative to the divisor $D_1 \cap D_2$. It turns out that the two affine curves $D_1 - (D_1 \cap D_2)$ and $D_2 - (D_1 \cap D_2)$ satisfy simultaneously the hypothesis of Siegel's theorem, so that their set of integral points is finite, if and only if the pair $(\mathbb{P}_2, D)$ satisfies the hypothesis of Vojta's conjecture on surfaces, predicting the degeneracy of the integral points on $\mathbb{P}_2$ with respect to D. For example, if D_1, D_2 are conic intersecting on four points, then the affine curves $D_i - (D_1 \cap D_2)$ are isomorphic to the complement of four points on the line. If, on the other hand, D_1 is a cubic and D_2 a line, then $D_1 - (D_1 \cap D_2)$ is a genus one curve deprived of three points while $D_2 - (D_1 \cap D_2) \simeq \mathbb{P}_1 - \{0, 1, \infty\}$.

The same happen in arbitrary dimension with any number of components (e.g. with hyperplanes in general position in $\mathbb{P}_n$).

Vojta's conjecture has been revisited by F. Campana in a series of paper (see e.g. [10]). We present here a (very) simplified version of a conjecture proposed by Campana.

Define a point $p \in \tilde{X}(\kappa)$ to be *half-integral* with respect to a divisor $D \subset \tilde{X}$ if $p \notin D$ and for every prime ideal $P \subset \mathcal{O}_S$, if p reduces modulo P to some point of D, then p reduces modulo P^2 to a point of D.

The mentioned simplified version of Campana's conjecture is the following:

Conjecture. Let then $\tilde{X}$ be a smooth projective variety over a number field κ, $\mathcal{O}_S \subset \kappa$ a ring of S-integers. Let $D = D' + D''$ be a reduced effective normal crossing divisor on $\tilde{X}$. Let $K_{\tilde{X}}$ be a canonical divisor for $\tilde{X}$. If the $\mathbb{Q}$-divisor

$$K_{\tilde{X}} + D' + \frac{1}{2} D''$$

is big, then the set of rational points of $\tilde{X} - D$ which are S-integral with respect to D' and helf-S-integral with respect to D'' is not Zariski-dense.

For example, given a square-free polynomial $f(X) \in \mathbb{Z}[X]$, the integers $x \in \mathbb{Z}$ such that $f(x)$ is a 'powerfull number' (all its prime factors appear with multiplicity ≥ 2), then x is half-integral with respect to the zero set of $f(X)$. According to Campana's conjecture, there should be only finitely many such numbers, whenever the degree of $f(X)$ is at least three. This would be also a consequence of the *abc* conjecture.

Note that the condition that an integer number n is powerfull can be expressed in term of the solvability of the Diophantine equation

$$n = x^2 y^3.$$

Some cases of Campana's conjecture can be proved over function fields: for instance, the Stother-Mason *abc* inequality for polynomials is an example in dimension 1. In dimension two, some cases are settled in [21], and a very general result has been proved by Yamanoi [66] for compact varieties $\tilde{X}$ of arbitrary dimension n with $q(\tilde{X}) \geq n$.

However, in the arithmetic context, little is known, due to the well-known difficulty of exploiting the ramification term in the Diophantine inequalities.

References

[1] P. Autissier, Géométrie, points entiers et courbes entières, *Annales Sci. E.N.S.* **42** (2009), 221-239.

[2] P. Autissier, Sur la non-densité des points entiers, *Duke Math. Journal*, **158** (2011), 13-27.

[3] A. Baker (editor), New Advances in Transcendence Theory, Cambridge Univ. Press 1988.

[4] A. Beauville, Surfaces algébriques complexes, *Astérisque* **54** (1978).

[5] F. Beukers, Ternary Form Equations, *J. Numb. Theory* **54** (1995), 113-133.

[6] Yu. Bilu, The Many Faces of the Subspace Theorem (after Adamczewski, Bugeaud, Corvaja, Zannier). Séminaire Bourbaki, exposé 967 Novembre 2006, *Astérisque* **317** (2007), 1-38.

[7] Yu. Bilu, M. Strambi, A. Surroca, Quantitative Chevalley-Weil Theorem for Curves, to appear in *Monatshefte f. Math.*

[8] E. Bombieri, W. Gubler, Heights in Diophantine Geometry, Cambridge University Press, 2006

[9] F. Bogomolov, Yu. Tschinkel, Density of rational points on Enriques surfaces, *Math. Res. Letters* **5** (1998), 623-628.

[10] F. Campana, Orbifolds, special varieties and classification theory, *Annales de l'institut Fourier*, **54** (2004) no. 3 , p. 499-630.

[11] F. Catanese, Topological methods in moduli theory, *Bull. Math. Sci* **5** (2915), no. 3, 287-449.

[12] P. Corvaja, Autour du Théorème de Roth. *Monatshefte f. Math.* **124** (1997), 147-175.

[13] P. Corvaja, Problems and results on integral points on rational surfaces. Diophantine Geometry, U. Zannier ed., 123-141, CRM Series, 4, Ed. Norm., Pisa, (2007).

[14] P. Corvaja, Integral Points on Algebraic Varieties: an introduction to Diophantine Geometry, Hindustan Book Agency, 2016.

[15] P. Corvaja, A. Levin, U. Zannier, Integral points on threefolds and other varieties, *Tohoku Math. Journal* **(2) 61** (2009), 589-601.

[16] P. Corvaja, J. Noguchi, A new unicity theorem and Erdös problem for polarized semi-abelian varieties, *Math. Annalen* **353** (2012), 439-464.

[17] P. Corvaja, U. Zannier, A subspace theorem approach to integral points on curves. *C. R. Math. Acad. Sci. Paris* **334** (2002), no. 4, 267-271.

[18] P. Corvaja, U. Zannier, On integral points on surfaces. *Ann. of Math.* (2) **160** (2004), no. 2, 705-726.

[19] P. Corvaja, U. Zannier, On a general Thue's equation. *Amer. J. Math.* **126** (2004), no. 5, 1033-1055, *Addendum* ibidem **128** (2006), no 4, 1057-1066.

[20] P. Corvaja, U. Zannier, On the integral points on certain surfaces. *Int. Math. Res. Not.* **2006**, 20 pp. (2006).

[21] P. Corvaja, U. Zannier, Some cases of Vojta's conjecture for integral points over function fields. *J. Alg. Geom.* **17** n.2 (2008), 295-333.

[22] P. Corvaja, U. Zannier, Integral points, divisibility between values of polynomials and entire curves on surfaces, *Advances in Math.* **225** (2010), 1095-1118.

[23] P. Corvaja, U. Zannier, Applications of Diophantine Approximation to Integral Points and Transcendence, Cambridge University Press (to appear).

[24] O. Debarre, Higher Dimensional Algebraic Geometry, Springer Verlag 2001.

[25] H. Darmon, A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London. Math. Soc.*, **27** (1995), 513-543.

[26] F. Dyson, The approximation to algebraic numbers by rationals, *Acta Math.* **79** (1947), 225-240.

[27] J.-H. Evertse, R. G. Ferretti, Diophantine inequalities on projective varieties, *Int. Math. Res. Notes* **2002**, 1295-1330.

[28] J.-H. Evertse, R. G. Ferretti, A generalization of the Subspace Theorem with polynomials of higher degree, in *Diophantine Approximation*, Developments in Mathematics **16**, Springer Verlag 2008.

[29] J.-H. Evertse, K. Gyory, C. Stuart, R. Tijdeman, S-unit equation and their applications, in [3]

[30] J.-H. Evertse, H.P. Schlickewei, A quantitative version of the absolute subspace theorem. J. Reine Angew. Math. 548 (2002), 21-127.

[31] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), no. 3, 349-366.

[32] G. Faltings, Diophantine approximation on abelian varieties, *Ann. Math.* **133** (1991), 549-576.

[33] G. Faltings, A new application of diophantine approximation, in A panorama of number theory, or the view from Baker's garden (ed. G. Wüstholz), pp. 231-246, Cambridge University Press, 2002.

[34] C. Fuchs and U. Zannier, Integral points on curves: Siegel's theorem after Siegel's proof, published in [70].

[35] C. Gasbarri, Dyson's theorem for curves, *J. Number Theory*, **129** (2009), 36-58.

[36] A.O. Gelfond, Transcendental and Algebraic Numbers, Dover Publications, 1960 and 2015 (Translation of the 1952 Russian edition).

[37] B. Hassett, Y. Tschinkel, Density of integral points on algebraic varieties, in: Rational points on algebraic varieties, 169-197, Progress in Math. **199**, Birkhäuser, 2001.

[38] Gordon Heier and Min Ru. On essentially large divisors, *Asian Journal of Mathematics*, **16** (2012), 387-407.

[39] M. Hindry, J. Silverman, Diophantine Geometry: an introduction, Graduate Texts in Mathematics 201, Springer Verlag, 2000.

[40] F. Klein, Lectures on the icosahedron and the solution to the equations of the fifth degree.

[41] A. Levin, Generalizations of Siegel's and Picard's theorems *Annals of Math.* **70** (2009), 609-655.

[42] A. Levin, One-parameter families of unit equations, *Math. Res. Letters* **13** (2006), 935-945

[43] S. Lang, On Integral Points on Curves. *Publications Mathématiques I.H.E.S.* **6** (1960), 27-43.

[44] S. Lang, Fundamentals of Diophantine Geometry, Springer Verlag 1983.

[45] K. Mahler, Ueber die rationalen Punkte auf Kurven vom Geschlecht Eins. (German) *J. Reine Angew. Math.* **170** (1934), 168-178

[46] D. Mc Kinnon, M. Roth, Seshadri constants, diophantine approximation and Roth's theorem for arbitrary varieties, *Inventiones Math.* **200** (2015), 513-583.

[47] J. Noguchi, A short analytic proof of closedness of logarithmic forms, *Kodai Math. Journal* **18** (1995), 295-299.

[48] J. Noguchi, J. Winkelmann, Holomorphic curves and integral points off divisors, *Math. Z.* **239** (2002), 593-610.

[49] J. Noguchi, J. Winkelmann, Nevanlinna Theory in Several Comples Variables and Diophantine Approximation, Grundlehren der Math. Wiss. **350**, Springer 2014.

[50] D. Ridout, The p-adic generalization of the Thue-Siegel-Roth theorem, *Mathematika* **5** (1958), 40-48.

[51] Min Ru, A general Diophantine inequality, Funct. Approx. Comment. Math. (2017).

[52] P. Vojta, Min Ru, A birational Nevanlinna constant and its consequences, `preprint` availabel at: https://arxiv.org/abs/1608.05382 (2016).

[53] A. Robinson, P. Roquette, On the finiteness theorem of Siegel and Mahler concerning Diophantine equations, *J. Number Theory* **7** (1975), 121-176.

[54] K. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 1-10.

[55] J.-P. Serre, Lectures on the Mordell-Weil Theorem, Aspects of Mathematics E 15, Viehweg Verlag, 1989.

[56] W. M. Schmidt, Approximation to Algebraic Numbers, *Monographie de L'Enseignement Amthématiques* **19**, Genève 1972.

[57] W. M. Schmidt, Diophantine Approximation, Lecture Notes in Mathematics **785**, Springer Verlag 1980.

[58] W. M. Schmidt, Diophantine Approximations and Diophantine Equations, Lecture Notes in Mathematics **1467**, Springer Verlag 1991.

[59] C. L. Siegel, Ueber einige Anwendungen diophantischer Approximationen, *Abh. Pr. Akad. Wiss.* **1** (1929) (Ges. Abh., I, 209-266). English translation in [70].

[60] H.P.F. Swinnerton-Dyer, $A^4 + B^4 = C^4 + D^4$ Revisited, *J. London Math. Soc.*, **43** (1968), 149-151.

[61] A. Thue, Ueber Annäherungswerte algebraischer Zahlen, *J. reine ang. Math.* **135** (1909), 284-305.

[62] P. Vojta, Diophantine Approximations and Value Distribution Theory, Lecture Notes in Mathematics **1239**, Springer Verlag, 1987.

[63] P. Vojta, Integral points on subvarieties of semiabelian varieties, I, II, *Invent. Math.* **126** (1996), 133-181.

[64] P. Vojta, Diophantine Approximation and Nevanlinna Theory, in Arithmetic Geometry, P. Corvaja and C. Gasbarri eds, Cetraro, Italy 2007, Lecture Notes in Mathematics **2009**, 2011.

[65] X. The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$, *J. London Math. Soc.* **1** (1926), 66-68.

[66] K. Yamanoi, Holomorphic curves in algebraic varieties of maximal Albanese dimension, *Forum Math.* (2015).

[67] U. Zannier, Some Applications of Diophantine Approximation to Diophantine Equations (with special emphasis on Schmidt's Subspace theorem), Forum Editrice, Udine 2003

[68] U. Zannier, On the integral points on the complement of ramification-divisors. *J. Inst. Math. Jussieu* **4** (2005), no. 2, 317-330.

[69] U. Zannier, Roth theorem, integral points and certain ramified covers of $\mathbb{P}_1$. In *Analytic Number Theory - Essays in honor of Klaus Roth*, Cambridge University Press 2008.

[70] U. Zannier (ed.) On Some Applications of Diophantine Approximations. A translation of Carl Ludwig Siegel's *Über einige Anwendungen Diophantischer Approximationen* by C. Fuchs.

Pietro Corvaja
Dipartimento di Scienze Matematiche, Fisiche e Informatiche
Università di Udine
Via delle Scienze, 206
33100 Udine (Italy)