Introduction to Diophantine Geometry

Nicola Dal Cin

Advisor: Prof. Pietro Corvaja

March 2023

Abstract

We present the basic ideas and issues of the theory of Diophantine Geometry, with the main focus on the one–dimensional case. The original problem is to determine whether (a system of) polynomial equations, defined over a number field κ, have infinitely many rational or integer solutions. Such a problem reduces to study $X(K)$, namely the set of K–rational points of an algebraic variety over $K \supset \kappa$; in particular, one is interested in finding geometric properties for X that ensures that $X(K)$ is not Zariski–dense. The aim of this work is to give a brief and intuitive overview of the above topics, focusing on the case of curves for which Siegel's and Faltings' theorems provide a complete description. In particular, in order to study integral points, we will treat some fundamental preliminary results about Diophantine approximation, namely the theory of approximating algebraic numbers by rationals. For some proofs and further remarks and details, we will refer to the bibliography.

1 Introduction

The problem of finding integer solutions to polynomial equations, also known as solving *Diophantine equations*, is among the most antique and fascinating in all mathematics. In fact, the world *"Diophantine"* refers to the Hellenistic Diophantus of Alexandria (III century AD) and suggests how far the first studies in the field date back.

Example 1.1. (Linear equations) The simpler example one can consider is probably finding the integer solutions of the linear equation

$$ax + by = c,$$

where a, b, c are integers. Just a small amount of arithmetic is needed to conclude that the latter has solutions in $\mathbb{Z}$ if and only if the $d := \gcd(a, b)$ divides c, and given a particular solution $(x, y) \in \mathbb{Z}^2$ *all* the *infinite* others are of the form $(x + kv, y + ku)$, with $k \in \mathbb{Z}$ and $u = a/d$, $v = b/d$.

Unluckily — or maybe luckily — it is not always that simple, one could expect that higher degree polynomials provide an higher complexity and, besides there are better indicators for the latter and this is not always the case, it is true that they may involve dealing with algebraic numbers, i.e. field extensions.

Example 1.2. (Pell's equation) For instance, one of the most celebrated examples is *Pell's equation*

$$x^2 - ny^2 = 1, \quad n \in \mathbb{Z}_{>0}.$$

The latter was already known in the IV century AD in India and Greece where it was much investigated thanks to its connection with the square root of two [1]. Only in the XVIII century AD, Lagrange proved that it has infinitely many solutions provided that n is not a perfect square, and in this case the latter can be used to *approximate* $\sqrt{n}$ with the rational fractions x/y. We highlight this fact since, as we shall see later, the problem of approximating irrational numbers by rationals is a crucial technique even in modern approaches. In this case, one can write the continued fraction expansion of $\sqrt{n}$ and check the approximating coefficients p_i/q_i until finds the so called *fundamental solution* that generates all the infinite others. Notice in fact that

$$x^2 - ny^2 = (x + \sqrt{n}y)(x - \sqrt{n}y)$$

is the norm for the ring $\mathbb{Z}[\sqrt{n}]$ and for the quadratic number field $\mathbb{Q}(\sqrt{n})$. Therefore $(x, y) \in \mathbb{Z}^2$ solves Pell's equation if and only if $x + \sqrt{n}y$ is an *unit* in $\mathbb{Z}[\sqrt{n}]$ with norm one. Thus, thanks to Dirichlet's unit theorem, it is possible to generate all the solutions from the fundamental one.

All this to point out that, in contrast with the simplicity of the formulation of such Diophantine problems, the theoretical apparatus that it is employed for their study is far more advanced that what ancient Greeks or eighteenth century people could have even imagined. It is impossible not to mention at this point Fermat's Last Theorem, namely the conjecture that no positive integers a, b, and c satisfy the equation

$$a^n + b^n = c^n,$$

for $n > 2$. Despite the case $n = 2$ was known since Pitagora by centuries, and the conjecture was formulated by Fermat in 1637, the proof of the above "simple" statement was only given in 1995 by A. Wiles employing a fascinating connection between elliptic curves and modular forms [2].

Wiles's theorem is not an isolated case, indeed, modern approaches of the so called "Diophantine geometry" — term that was coined by S. Lang in [3] — involve the study of the underlying geometry of the algebraic variety determined by the polynomial equation (or by the system of equations). In fact, as it is well–understood in case of curves, the latter determines the qualitative arithmetic properties of the variety.

Example 1.3. In the case of Pell's equation, which in Cartesian coordinates represents an hyperbola, the fact that there are infinite integer solutions is linked to the geometric property of having an automorphism group

$$G := \left\{ \begin{pmatrix} a & nb \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R}, \quad a^2 - nb^2 = 1 \right\}$$

that sends the hyperbola into herself, in other words $v \in \mathbb{R}^2$ is a solution if and only if Tv is also a solution, for all $T \in G$.

In fact, above behaviour is an instance of a general *paradigma* which holds for algebraic curves, which can be naively expressed as

$$\text{Hyperbolicity} \quad \Longleftrightarrow \quad \text{finite amount of integeral points}^1.$$

More precisely, recall that a smooth algebraic curve C is topologically characterized by two discrete invariats: its genus g and the number $d = \#(\tilde{C} - C)$ of its points at infinity in a smooth completion $\tilde{C}$. By mean of the above invariant it is defined the *Euler characteristic* of C as

$$\chi = \chi(C) := 2g - 2 + d,$$

and we say that a curve is *hyperbolic* if $\chi > 0$, *parabolic* if $\chi = 0$ and *of elliptic type* if $\chi < 0$. With this notations, the main result concerning integral points for algebraic curves is due to Siegel (here stated in general for a number field κ and $\mathcal{O}_S$, a ring of S–integers, in place of $\mathbb{Q}$ and $\mathbb{Z}$ respectively).

Theorem 1.1. (Siegel 1929) Let C be an affine curve of Euler characteristic χ, defined over a number field κ, and let $\mathcal{O}_S \subset \kappa$ be a ring of S–integers. If the hyperbolicity condition $\chi > 0$ holds, then the set of integral points on the curve $C(\mathcal{O}_S)$ is finite.

Conversely, if a curve has genus zero and has at least a rational point and at most two points at infinity is isomorphic either to the affine line or the multiplicative group — as we shall better see later.

Since, by Riemann–Roch theorem, smooth projective curves of genus zero over κ are isomorphic to plane conic over κ, it follows that the previous ones have an infinite set of integral points (at least after enlarging the ring of integers so to have infinitely many units).

From above results and consideration we can deduce Siegel's theorem is an optimal result, and basically solves the problem of determine whether an affine curve has an infinite set of integral points. What is still an open problem is the task of finding an algorithm to determine such a set, i.e. there is an effective proof of Siegel's result only in particular cases.

[1] In the sense of Definition 3.1.

In this work we will briefly expose some basic results of Diophantine geometry, with focus on the one dimensional case and in particular Siegel's theorem. The main tools we deal with are the theory of *height functions* — which are a better indicator of the complexity of an algebraic object rather than the polynomial degree — and the *Diophantine approximation*, i.e. the theory of approximating algebraic numbers by rationals or, more generally, of studying the convergence speed of a sequence of rational points on a variety to some fixed subset.

2 Diophantine approximation

In this section we recall some classical results about Diophantine approximation, which as already said addresses the problem of approximating an irrational number α by rationals. The notation we will adopt is in part recalled in the appendix, more details and proofs can be found in [4].

2.1 Diophantine approximation on the line

Let us take $\alpha \in \mathbb{R}$, as a consequence of the density of $\mathbb{Q}$ in $\mathbb{R}$, it holds that

$$\inf_{p/q \in \mathbb{Q}} \left| \alpha - \frac{p}{q} \right| = 0,$$

in other words that it is possible to approximate α with arbitrarily high precision. The main concern is to estimate the accuracy in the precision of the latter approximation with respect to the denominator q — since one wishes to have good approximations with relatively small denominators.

More precisely we are interested in determining whether given $\alpha \in \mathbb{R}$ and an exponent $e > 0$ the inequality

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^e}, \tag{1}$$

can have infinitely many solutions in $\mathbb{Q}$.

2.1.1 Basics results

We define the *approximation exponent* for $\alpha \in \mathbb{R}$ to be the smallest number $\tau(\alpha)$ such that the property (1) holds for every exponent $e > \tau(\alpha)$. In 1842, Dirichlet proved that every real number has an approximation exponent at least two; remarkably this is the best possible result for an arbitrary irrational number (i.e. not necessarily algebraic).

Theorem 2.1. (Dirichlet 1842) Let $\alpha \in \mathbb{R} - \mathbb{Q}$ be a real irrational number, there are infinitely many rational numbers $p/q \in \mathbb{Q}$ satisfying

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

In this case, there is also an effective method to determine an approximating subsequence, namely truncating the continued fraction expansion of α.

An upper bound to the approximation exponent of algebraic numbers was found by Liuville two years later: if α is a degree d algebraic number over $\mathbb{Q}$ then $\tau(\alpha) \leq d$.

Theorem 2.2. (Liouville 1844) Let α be an algebraic number of degree d over $\mathbb{Q}$, there exists a positive number $c(\alpha)$ such that for all $p/q \in \mathbb{Q}$ it holds

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{c(\alpha)}{q^d}. \tag{3}$$

Proof. Let $f \in \mathbb{Z}[x]$ be a non–zero irreducible polynomial with root α, and f' its formal derivative. Given p/q, by the mean–value theorem exists $\xi \in \mathbb{R}$ between α and p/q such that $f(\alpha) - f(p/q) = f'(\xi)(\alpha - p/q)$.

Since f is irreducible end of degree d, the rational number $f(p/q)$ is non–zero and has a denominator which is at worse q^d. It follows that $|f(p/q)| \geq 1/q^d$ and

$$|f'(\xi)| \cdot \left| \alpha - \frac{p}{q} \right| = \left| f(\alpha) - f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^d}.$$

Now, notice that since f is irreducible, it has not a double root at α and so $f'(\alpha) \neq 0$. Therefore provided q is large enough, ξ is close to α and also $f'(\xi) \neq 0$; in particular there is a certain positive integer $\bar{q}$ such that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{2/|f'(\alpha)|}{q^d} \quad \text{for all } q \geq \bar{q}.$$

Provided choosing a smaller constant $c(\alpha)$, in place of $2/|f'(\alpha)|$ to make the latter hold for the *finite* set of denominators $1 \leq q < \bar{q}$, the assertion follows. □

Corollary 2.1. A sufficient condition for $\alpha \in \mathbb{R}$ to be a transcendental number is to be "well approximable by rational numbers", in the sense that for all $d \geq 1$ and for every constant $c > 0$ there is a rational number $p/q \in \mathbb{Q}$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^d}. \tag{4}$$

Example 2.1. The real number $\alpha = \sum_{n\geq 1} 2^{-n!}$ is transcendental. We can therefore write

$$\alpha - \underbrace{\sum_{n\leq N} \frac{1}{2^{n!}}}_{p/q \text{ with } q:=2^{N!}} = \sum_{n>N} \frac{1}{2^{n!}} < \frac{2}{2^{(N+1)!}} = \frac{2^{-(N+2)}}{q},$$

and notice that for each $c > 0$ there is an N large enough to make (4) hold for $p/q := \sum_{n\leq N} 2^{-n!}$.

2.1.2 Roth's theorem

A much stronger result — which is optimal considering Dirichlet theorem and is also more difficult to prove — is the theorem due to Roth that guarantees that the approximation exponent for algebraic numbers is $\tau(\alpha) = 2$.

Theorem 2.3. (Roth 1955) For all α algebraic numbers and every $\varepsilon > 0$, the inequality

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\varepsilon}} \tag{5}$$

has only finitely many solutions $p/q \in \mathbb{Q}$.

Equivalently, there exists a constant $c(\alpha, \varepsilon) > 0$ such that for all rationals p/q

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha, \varepsilon)}{q^{2+\varepsilon}}. \tag{6}$$

However, beside being quite complex and articulated, the proof of the previous result is not effective, in other words it does not provide any procedure either to determine the finite set of rationals that do not satisfy (5), or the function $c(\alpha, \varepsilon)$.

As mentioned, Roth's theorem is an optimal result in the case of approximation using rational numbers, because of theorem 2.1. Nonetheless, there are some extensions that use a different number field $\kappa \subset \mathbb{C}$ to approximate α — of course in this case there are Dirichlet analogue results that bound the approximation exponent from below.

2.2 Roth's theorem for algebraic curves

In general one might allow the approximating values to be in a number field κ rather that $\mathbb{Q}$, and may even want to consider other absolute values rather than the only usual one. This can be done choosing a set of places S containing the archimedean as recalled in the appendix. In this general case, Roth's theorem has the following formulation.

Theorem 2.4. (Roth's theorem general version) Let κ be a number field, $S \subset M_\kappa$ a finite set of places on κ, that have been extended in some way to $\bar{\kappa}$. Given $\alpha \in \bar{\kappa}$ and $\varepsilon > 0$, there are only finitely many $\beta \in \kappa$ such that

$$\prod_{v \in S} \min\{\|\beta - \alpha\|_v, 1\} \leq \frac{1}{H_\kappa(\beta)^{2+\varepsilon}} \tag{7}$$

Proof. See Theorem D.2.1 in [4]. □

An application of theorem 2.4, as we will see in the next section, is to prove that the S–unit equation $U + V = 1$ has a finite number of unit solutions in $\mathcal{O}_S^\times$. This result itself is useful to prove that in an affine curve of genus 0 and with at least three points at infinity has a finite number of S–integral points (theorem 3.1).

However, in order to extend above mentioned theorem to curves of greater genus, it is needed another version of Roth's theorem for curves.

Proposition 2.1. If κ is a number field, C/κ a smooth projective curve of genus g defined over κ and $f \in \kappa(C)$ a nonconstant function, let e be the maximum order of the zeros of f. Fixed a constant $\varepsilon > 0$, we choose a function $t \in \kappa(C)$ that is well defined and unramified at all zeros and poles of f. Then there is a positive constant $c := c(f, t, C, \varepsilon, S) > 0$ such that

$$\prod_{v \in S} \min\{\|f(P)\|_v, 1\} \geq \frac{c}{H_\kappa(t(P))^{(2+\varepsilon)\, s \cdot e}} \quad \text{for all } P \in C(\kappa), \tag{8}$$

where $s = \#S$.

Proof. For some effective divisor $E > 0$ we may write the divisor of f as

$$div(f) = e_1(Q_1) + \cdots + e_r(Q_r) - E, \tag{9}$$

with Q_j's distinct zeros of f and $e = \max_{j=1,\ldots,r}\{e_j\}$. If the thesis was false, by contradiction there would be a sequence of points $\{P_i\}_{i \in \mathbb{N}}$ in $C(\kappa)$ such that

$$\lim_{i \to \infty} H_\kappa(t(P_i))^{(2+\varepsilon)\, s \cdot e} \prod_{v \in S} \min\{\|f(P)\|_v, 1\} = 0. \tag{10}$$

Observing that $\prod_{v \in S} \min\{\|f(P)\|_v, 1\} \geq (\min_{v \in S}\{\|f(P_i)\|_v, 1\})^s$, and after substituting and taking the s^{th} roots we have

$$\lim_{i \to \infty} H_\kappa(t(P_i))^{(2+\varepsilon)\, e} \min_{v \in S}\{\|f(P_i)\|_v, 1\} = 0. \tag{11}$$

Recalling that the curve has only finitely many κ–rational points of bounded height, we have that $H_\kappa(t(P_i)) \to \infty$. Thus we can choose a place $w \in S$ and a restrict ourselves to a subsequence of $\{P_i\}_{i \in \mathbb{N}}$ (that we will still indices with i by abuse of notation) such that

$$\lim_{i \to \infty} H_\kappa(t(P_i))^{(2+\varepsilon)\, e} \|f(P_i)\|_w = 0. \tag{12}$$

Since $H_\kappa(t(P_i))$ diverges, it has to be $\|f(P_i)\|_w \to 0$ and so P_i approaches one of the zeros of f in the w–adic topology. By restricting once again to a subsequence we may assume wlog that $\{P_i\}$ approaches some fixed zero Q_j of f, with $j \in \{1, \ldots, r\}$.

Since f vanishes to order e_j at Q_j, the function

$$g := (t - t(Q_j))^{-e_j} f$$

has no zero or pole at Q_j. Therefore g is w–adically bounded in a neighborhood (in the w–adic topology) of Q_j. In other words exist positive constants $c_1, c_2 > 0$ such that definitely

$$c_1 \leq \|(t(P_i) - t(Q_j))^{-e_j} f(P_i)\|_w \leq c_2. \tag{13}$$

Rearranging equations (12) and (13) it follows that

$$\lim_{i \to \infty} H_\kappa(t(P_i))^{(2+\varepsilon)\, e} \|(t(P_i) - t(Q_j))^{e_j}\|_w = 0.$$

Finally, recalling that $e = \max_{j=1,\dots,r}\{e_j\}$, we deduce

$$\lim_{i\to\infty} H_\kappa(t(P_i))^{(2+\varepsilon)}\|t(P_i) - t(Q_j)\|_w = 0.$$

and so that $\|t(P_i) - t(Q_j)\|_w \to 0$. In other words we have that the sequence $\{t(P_i)\} \subset \kappa$ definitely approximates $t(Q_j) \in \bar{\kappa}$ violating Roth's theorem 2.4; hence the statement of the proposition follows by contradiction. □

With a bit more effort and the assumption that C has positive genus, it is possible to show that the exponent $\rho(f) = s \cdot e(f)\,(2+\varepsilon)$ in the above proposition can be replaced by any positive constant.

The idea is to find a covering $\phi : C' \to C$ such that exist rational points $P' \in C'(\kappa)$ lifting the rational points $P \in C(\kappa)$, so to have $\|f(\phi(P'))\|_v = \|f(P)\|_v$. What happens it that for a certain $t' \in \kappa(C')$ we have

$$H_\kappa(t'(P')) \approx H_\kappa(t(P))^{1/\deg\phi}; \tag{14}$$

so if we apply Proposition 2.1 to C', $f \circ \phi$ and t' we find

$$\prod_{v\in S} \min\{\|f\circ\phi(P')\|_v, 1\} \geq \frac{c}{H_\kappa(t'(P'))^{s\cdot e(f\circ\phi)\,(2+\varepsilon)}} \quad \text{for all } P' \in C'(\kappa), \tag{15}$$

and also because of (14)

$$\prod_{v\in S} \min\{\|f(P)\|_v, 1\} \geq \frac{c}{H_\kappa(t(P))^{s\cdot e(f\circ\phi)\,(2+\varepsilon)/\deg\phi}} \quad \text{for all } P \in C(\kappa), \tag{16}$$

in terms of C. Now, by taking ϕ with a very large degree we can intuitively make the approximation exponent arbitrarily small (the detailed proof, which make use of Weil's height machine, can be found below Theorem D.9.4 in [4]).

Theorem 2.5. (Roth's theorem for curves) If κ is a number field, C/κ a smooth projective curve of genus g defined over κ and $f \in \kappa(C)$ a nonconstant function, let e be the maximum order of the zeros of f. If we choose a function $t \in \kappa(C)$ which is defined and unramified at all zeros and poles of f and take $\rho > 0$. Then there is a positive constant $c := c(f, t, C, \rho, S) > 0$ such that

$$\prod_{v\in S} \min\{\|f(P)\|_v, 1\} \geq \frac{c}{H_\kappa(t(P))^\rho} \quad \text{for all } P \in C(\kappa). \tag{17}$$

2.3 The S–unit equation

A remarkable application of Roth's theorem is that the two–variable S–unit equation

$$U + V = 1, \quad U, V \in \mathcal{O}_S^\times \tag{18}$$

has only finitely many solutions. This fact is not very surprising if we notice that we are looking for intersections between the finitely generated group $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$ and the proper subvariety $\{U + V = 1\}$ of $\mathbb{G}_m \times \mathbb{G}_m$.

Theorem 2.6. (Siegel, Malher) Let $\kappa/\mathbb{Q}$ be a number field and let S be a finite set places on κ which includes the archimedean ones. Then the *S–unit equation*

$$U + V = 1$$

has only finitely many solutions in S–units $U, V \in \mathcal{O}_S^\times$.

The idea of the proof is to use the fact $U, V \in \mathcal{O}_S^\times$ and therefore exists an absolute value $w \in S$ for which $|U|_w$ and $|V|_w$ are big. Thus, writing $|UV^{-1} + 1|_w = |V|_w^{-1}$ we find that $-UV^{-1}$ approximates 1. Using the fact that $\mathcal{O}_S^\times$ is finitely generated to write U and V by aX^m and bY^m, and substituting gives

$$\left|\left(\frac{X}{Y}\right)^m - \left(-\frac{b}{a}\right)\right|_w = \left|\frac{1}{aY^m}\right|_w.$$

We deduce that X/Y approximates $\sqrt[n]{-b/a}$ as close as $-U/V$ approximates 1, while the height $H_\kappa(X/Y) \approx H_\kappa(U/V)^{1/m}$, and for large values of m, this fact violates Roth's theorem.

There is also a stronger theorem by Evertse [5], which gives an upper bound for the number of solutions of (18). Moreover, Evertse himself together with van der Poorten and Schlickewei proved the following generalization to the n–variable S–unit equation, which has numerous applications [6].

Theorem 2.7. (Evertse, van der Poorten and Schlinckewei) Consider the n–variable S–unit equation

$$U_1 + \cdots + U_n = 1,$$

which defines an irreducible algebraic subvariety in $\mathbb{G}_m^n$. Then there are only finitely many solutions $(U_1, \ldots, U_n) \in (\mathcal{O}_S^\times)^n$ for which there are no sub–sums of the U_i that vanish.

3 Integral and rational points on curves

In this section we present the main and classical results about integral and rational points on algebraic curves. We will also present the sketch of a proof of Siegel's theorem that applies Roth's approximation result 2.4. Our aim here is simply to give an idea of the main tools and arguments that can be employed in this framework, for any further details the reader can refer to [4] or [7].

We also point out that the following is not the original proof by Siegel — since Roth's theorem is posterior to his result — which only considered the case of algebraic integers over κ. In addition, another proof using a new method based on the subspace theorem was given in 2002 by P. Corvaja and U. Zannier [8].

Before going further we shall give a more detailed and general definition of what we consider an *integral point* of an algebraic variety X defined over a number field κ and the ring of S–integers $\mathcal{O}_S \subset \kappa$ with respect to the finite set of places S containing the archimedean ones — as recalled in the appendix.

Definition 3.1. Let X be a quasi projective irreducibely variety, defined over a number field κ, and assumed embedded in a projective space $\mathbb{P}_N$ (which is canonically provided with an integral model). We denote by $\tilde{X}$ a completion of X in a projective space $\mathbb{P}_N$, and therefore we can write $X = \tilde{X} - D$ where D is a proper closed subvariety of $\tilde{X}$. A point $P \in X(\kappa)$ is *S–integral with respect to D* if P reduces to a point of D for no place outside S.

Point out that if X is an affine variety embedded into the affine space $\mathbb{A}^N$, the integral points with respect to the divisor at infinity of X exactly correspond to what we would intuitively expect to be the integral points, i.e. those whose coordinates are in $\mathcal{O}_S$ (which indeed generalizes the ring of algebraic integers of κ). While, if X is projective $D = \emptyset$ and so the set of S–integral points is the whole $X(\kappa)$.

Example 3.1.

- Considering the affine embedded in the projective line $\mathbb{A}^1 \hookrightarrow \mathbb{P}_1$, gives

  $$D = \tilde{X} - X = \mathbb{P}_1 - \mathbb{A}^1 = \{(1:0)\} = \{\infty\}.$$

  Letting $\kappa = \mathbb{Q}$ one finds that the rational points, those corresponding to the projective points $(a:b)$ with a, b coprime integers, $b \neq 0$, are S–integral with respect to the point at infinity if and only if all p–adic valuations associated to primes that divides b are in S. In particular, in case S does not contain any p–adic valuation, $(a:b)$ does not reduce to $(1:0)$ if and only if $b = \pm 1$, i.e $a/b \in \mathbb{Z}$.

- Another one–dimensional example is the multiplicative group $\mathbb{G}_m$ defined by the hyperbola $xy = 1$ in the affine plane $\mathbb{A}^2$. In this case $D = \{0, \infty\}$ and so $(a:b)$ with $\gcd(a,b) = 1$ does not reduce to either $(0:1)$ or $(1:0)$ and so $X(\mathbb{Z}) = \{(-1:-1:1), (1:1:1)\}$ or in general $X(\mathcal{O}_S) = \mathcal{O}_S^\times$. So if we enlarge the ring of integers to acquire infinitely many units the set of integral points is also infinite.

3.1 Siegel's theorem

Let now κ be a number field, S a finite subset of places, containing the archimedean ones, and $\mathcal{O}_S$ be the relative ring of S–integers of κ.

We study two different cases based on the genus of the curve C in exam. The following result provides conditions in which a function on $\mathbb{P}^1$ can (or can not) assume infinitely many integral values.

Theorem 3.1. (Siegel, case $g = 0$) If κ is a number field, C/κ is a curve of genus zero, and $\phi \in \kappa(C)$ a rational function on C with at least three distinct poles in $C(\bar{\kappa})$. Then, there are only finitely many rational points $T \in C(\kappa)$ such that $\phi(T) \in \mathcal{O}_S$.

Proof. Since in case $C(\kappa) = \emptyset$ the statement is trivial, we can take $C = \mathbb{P}^1$ and write

$$\phi = \frac{f(x,y)}{g(x,y)}, \quad f, g \in \kappa[x,y]$$

where f and g are homogeneus polynomials with the same degree and no roots in $\mathbb{P}^1(\bar{\kappa})$ in common. Taking a finite extension K/κ over which both f and g splits (with abuse of notation we still denote K by κ), and provided adding finitely many primes to S we can assume that

(i) f and g factor completely in κ

$$f = a\,(x - \alpha_1 y)^{d_1} \cdots (x - \alpha_m y)^{d_m}, \quad g = b\,(x - \beta_1 y)^{e_1} \cdots (x - \beta_n y)^{e_n}, \tag{19}$$

where $a, b \in \mathcal{O}_S^\times$ and $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in \mathcal{O}_S$. Moreover, notice that that if ϕ has a zero or a pole at $(1:0)$ then respectively f or respectively g may also have a factor of the form y^d.

(ii) The differences $\alpha_i - \beta_j \in \mathcal{O}_S^\times$ for all $1 \le i \le m$ and $1 \le j \le n$.

(iii) The ring $\mathcal{O}_S$ is a principal ideal domain.

Consider now a point $T \in \mathbb{P}^1(\kappa)$ for which the thesis holds, i.e. $\phi(T) \in \mathcal{O}_S$. Thank to point (iii) above, we can assume it has coprime coordinates that we indicate $T = (X : Y)$ with $\gcd(X, Y) = 1$. For all $1 \le i \le m$ and $1 \le j \le n$ we have the easy reformulations

$$(X - \alpha_i Y) - (X - \beta_j Y) = (\alpha_i - \beta_j)Y \tag{20}$$

and

$$-\beta_j(X - \alpha_i Y) + \alpha_i(X - \beta_j Y) = (\alpha_i - \beta_j)X. \tag{21}$$

Since the differences $\alpha_i - \beta_j$ are units and $\gcd(X, Y) = 1$, we have that $X - \alpha_i Y$ and $X - \beta_j Y$ are coprime for any i and j. By (19) it follows that also $f(X, Y)$ and $g(X, Y)$ are coprime in $\mathcal{O}_S$.

Since $\phi(T) \in \mathcal{O}_S$ by assumption, $g(X, Y)$ divides $f(X, Y)$ and therefore $g(X, Y)$ is a unit, and in particular all the terms $X - \beta_j Y \in \mathcal{O}_S^\times$ for $1 \le j \le n$. By hypothesis ϕ has at least three poles, i.e. $n \ge 3$, and we can consider *Siegel's identity*

$$\frac{\beta_2 - \beta_3}{\beta_2 - \beta_1} \cdot \frac{X - \beta_1 Y}{X - \beta_3 Y} - \frac{\beta_3 - \beta_1}{\beta_2 - \beta_1} \cdot \frac{X - \beta_2 Y}{X - \beta_3 Y} = 1, \tag{22}$$

which, by theorem 2.6, can assume only finitely many values (notice that both terms on the left–hand side are units). Finally we conclude showing that to each fixed value $\gamma := (X - \beta_1 Y)/(X - \beta_3 Y)$ corresponds one single point of coordinates

$$T = (X : Y) = (\beta_1 - \gamma\beta_3 : 1 - \gamma).$$

□

The same result of the latter is true for curves of genus $g \ge 1$, however the proof in this case the proof requires a reformulation of Roth's theorem for curves.

Theorem 3.2. (Siegel, case $g \ge 1$) Let κ be a number field, and C/κ a smooth projective curve of genus $g \ge 1$ over κ. Then, for every nonconstant function $f \in \kappa(C)$, the set

$$\{P \in C(\kappa) \mid f(P) \in \mathcal{O}_S\} \tag{23}$$

is finite.

Proof. In order to apply theorem 2.5, by contradiction assume that the set

$$\{P \in C(\kappa) \mid f(P) \in \mathcal{O}_S\} \tag{24}$$

is infinite. Let us fix a function $t \in \kappa(C)$ that is defined and unramified at all zeros and poles of f, and fix $\rho = \deg f/(2 \deg t)$. First, apply Theorem 2.5 to the function $1/f$ which gives a constant $c_1 > 0$ such that

$$\prod_{v \in S} \min\{\|(1/f)(P)\|_v, 1\} \geq \frac{c_1}{H_\kappa(t(P))^\rho} \quad \text{for all } P \in C(\kappa), \tag{25}$$

which rearranged gives

$$H_\kappa(t(P))^\rho \geq c_1 \prod_{v \in S} \max\{\|f(P)\|_v, 1\} \quad \text{for all } P \in C(\kappa). \tag{26}$$

Now, if $f(P)$ is an S–integral point then by definition $\|f(P)\|_v$ for all $v \notin S$, so its height is

$$H_\kappa(f(P)) = \prod_{v \in M_\kappa} \max\{\|f(P)\|_v, 1\} = \prod_{v \in S} \max\{\|f(P)\|_v, 1\} \tag{27}$$

By (26) and (27) we finally have

$$H_\kappa(t(P))^\rho \geq c_1 H_\kappa(f(P)) \quad \text{for all } P \in C(\kappa) \text{ with } f(P) \in \mathcal{O}_S. \tag{28}$$

We obtain an estimation of logarithmic heights taking logarithms and dividing by $[\kappa : \mathbb{Q}]$ both sides:

$$\rho\, h(t(P)) \geq h(f(P)) - c_2 \quad \text{for all } P \in C(\kappa) \text{ with } f(P) \in \mathcal{O}_S. \tag{29}$$

Dividing by $h(t(P))$, rearranging and using Proposition A.3 gives for all $P \in C(\kappa)$ with $f(P) \in \mathcal{O}_S$

$$\frac{\deg f}{2 \deg t} \geq \frac{h(f(P))}{h(t(P))} - \frac{c_2}{h(t(P))} \xrightarrow{h(t(P)) \to \infty} \frac{\deg f}{\deg t}.$$

Since the above limit is well defined (provided we restrict to the infinite subset (24)), we reach the absurd

$$\frac{\deg f}{2 \deg t} \geq \frac{\deg f}{\deg t}.$$

□

Remark 3.1. The proof of Siegel's theorem we presented is ineffective, actually there are not effective results in the general case, but for many examples Baker's theorem can be used to find a lower bound for linear forms of logarithms and so provides a method to refine above proof and make it effective [9].

Notice that combining theorems 3.1 and 3.2 one gets that: an affine irreducible curve $C \subset \mathbb{A}^n$ defined over κ contains (in a suitable integral model) infinitely many points with coordinates in $\mathcal{O}_S$ if C is a rational curve and has at most two points at infinity, namely Theorem 1.1.

Indeed, let C be an affine curve of genus g and d points at infinity, in other words denoting $\tilde{C}$ a completion of X in $\mathbb{P}_N$, we have $d = \#(\tilde{C} - C)$. Then the above theorems give

$$\overbrace{\chi(C) := 2g - 2 + d > 0}^{\text{Hyperbolicity condition}} \quad \Longrightarrow \quad C(\mathcal{O}_S) \text{ is finite.} \tag{30}$$

Vice–versa if a curve is rational (i.e. of genus zero with at least one rational point) and has exactly one point at infinity it is isomorphic (modulo normalization) to the affine line. On the other hand, if the points at infinity are two, we can normalize it (after possibly taken a quadratic field extension) obtaining a variety isomorphic to the multiplicative group $\mathbb{G}_m = \mathbb{A}^1 - \{0\}$, which has infinitely many integral points too — at least after enlarging the ring of integers to include infinitely many primes.

Remark 3.2.

- Above conclusion (30) is remarkable, indeed, from a topological property we deduce an arithmetic one. Moreover, by the above considerations we can conclude that Siegel's theorem is the best–possible result concerning integral points on curves. It has to be also noticed that for curves of genus $g \geq 2$ Siegel's result is implied by Faltings' theorem, which ensure that the set $C(\kappa)$ of rational points itself is finite.

- Since a curve of genus 1 is an abelian variety of dimension 1, Siegel's theorem states that an affine piece of an abelian variety of dimension 1 has only a finite set of S–integral points. Faltings, using an extension of Vojta's method, proved that this is the case for all abelian varieties of arbitrary dimension [10].

3.2 Hints on Faltings' theorem and generalizations

In this final part, starting by the one–dimensional case, we draw some general considerations about density of integral points in a variety. As anticipated before, the main result concerning κ–rational points on an algebraic curve is due to Faltings, who proved a conjecture formulated by Mordell more that 60 years earlier.

Theorem 3.3. (Faltings 1983) Let C be an irreducible algebraic curve defined over a number field κ. If the genus of C is not less than 2, we have that $C(\kappa)$, its set of κ–rational points, is finite.

As an easy and curious application of this result, we have a weak version of Fermat Last Theorem. By Riemann–Roch theorem descends the formula $g = \frac{1}{2}(n-1)(n-2)$ to compute the arithmetic genus[2] of an irreducible plane curve of degree n. Then if $n \geq 4$, the Fermat curve $x^n + y^n = 1$ has genus ≥ 3 and so $\chi > 0$. Now using Faltings' result we have that $a^n + b^n = c^n$ has at most finitely many primitive integer solutions (i.e. pairwise coprime solutions) if $n \geq 4$.

Combining Theorem 3.3 with Siegel's result one obtains:

Theorem 3.4. (Siegel–Faltings) Let $C = \tilde{C} - D$ be an irreducible (affine or projective) curve over a number field κ, where $D \subset \tilde{C}(\bar{\kappa})$ is the set of its point at infinity in a smooth completion $\tilde{C}$. If $C(\mathcal{O}_S)$ the set of points with coordinates in $\mathcal{O}_S \subset \kappa$ is infinite, then $\chi(C) \leq 0$.

This result is optimal since it holds its converse:

Theorem 3.5. If C/κ is an (affine or projective) curve with $\chi(C) \leq 0$. Than there exists a finite field extension κ'/κ and a ring of S–integers $\mathcal{O}_S \subset \kappa'$ such that $C(\mathcal{O}_S)$ is infinite.

Since the problem of determining geometric conditions that ensure that the set of points with S–integer coordinates is basically solved in the one dimensional case, it is natural to study suitable generalizations of Theorem 3.5 in higher dimensions. In general we are interested in the problem of

determining geometric conditions (analogue to hyperbolicity) that ensure that, in an algebraic variety V/κ, the set of K–rational points of V is not Zariski–dense for every number field extension $K \supset \kappa$.

As expectable, one is led to deal with higher dimensional Diophantine approximation, i.e. with the aim of approximating hyperplanes defined by linear forms with algebraic coefficients by rational points. For instance, the two–dimensional case some results where achieved, using the subspace theorem, in [11].

A good overview of the state of the art, together with some remarks around conjectures in the general case such as the famed Vojta's and Campana's, can be found in [12].

[2] Which coincides with the geometric genus if the curve is non–singular.

A Absolute values and heights

In this appendix we recall some results about absolute values and height functions with the only aim of fix some notations. For further details and proofs we refer to [4] or [7].

A.1 Absolute values

Let κ be a number field.

Definition A.1. An *absolute value* on κ is a real–valued function $|\cdot|_v : \kappa \to [0, \infty)$ such that for all $x, y \in \kappa$ hold

(1) $|x|_v = 0$ if and only if $x = 0$, i.e. it is nondegenerate.

(2) $|xy|_v = |x|_v \cdot |y|_v$, i.e. it is multiplicative.

(3) $|x + y|_v \leq |x|_v + |y|_v$, i.e. satisfies the triangle inequality.

Moreover, if in place of (3) it full–fills the following stronger condition said *ultrametric inequality*:

(3') $|x + y|_v \leq \max\{|x|_v, |y|_v\}$.

the absolute value is said to be *nonarchimedean*.

Example A.1.

- For every κ there is the *trivial valuation*, i.e. the one which is constantly 1 but for $x = 0$, and is clearly nonarchimedean.
- Over $\mathbb{Q}$ we can consider the restriction of the absolute value over $\mathbb{R}$, namely

$$|x| = \max\{x, -x\},$$

  which is an archimedean absolute value on $\mathbb{Q}$.
- For every prime number p is defined a nonarchimedean p–adic absolute value over $\mathbb{Q}$. We denote $ord_p(x)$ the unique integer such that $x \in \mathbb{Q} - \{0\}$ can be written

$$x = p^{ord_p(x)} \cdot \frac{a}{b} \quad \text{with } a, b \in \mathbb{Z} \text{ and } p \nmid ab,$$

  while $ord_p(0) = \infty$ by convention; the homomorphism $ord_p : \mathbb{Q}^\times \to (0, \infty)$ is called p–adic valuation on $\mathbb{Q}$. Finally, the p–adic absolute value of $x \in \mathbb{Q}$ is defined as

$$|x|_p := p^{-ord_p(x)}.$$

An absolute value defines a metric, throughout $d_v(x, y) := |x - y|_v$, and therefore a topology on κ. Two absolute values which induce the same topology are said *dependent, independent* otherwise. It is easy to show that "dependence" is an equivalence relation, and the corresponding equivalence classes of absolute values are called *places*.

Proposition A.1. Let $|\cdot|_a$ and $|\cdot|_b$ be non–trivial absolute values on a field κ.

(i) They are dependent if and only if $|x|_a < 1$ implies $|x|_b < 1$.

(ii) If they are dependent, then there exists a number $\delta > 0$ such that $|x|_a = |x|_b^\delta$ for all $x \in \kappa$.

Proof. Lang, Proposition 1.1, cap. XII. □

Recall that a result by Ostrowski [13] states that every non–trivial absolute value over $\mathbb{Q}$ is either equivalent to the usual absolute value $|\cdot|$ or some p–adic absolute value $|\cdot|_p$.

The set of standard absolute values on $\mathbb{Q}$, i.e. $|\cdot|$ and the p–adic ones, is often denoted as $M_\mathbb{Q}$. More generally M_κ, the set of standard absolute values on κ, consists in those whose restriction to $\mathbb{Q}$ is in $M_\mathbb{Q}$.

Definition A.2. Let κ'/κ be an extension of number fields and $v \in M_\kappa$, $w \in M_{\kappa'}$ two absolute values. We say that w *divides* v (or w *lies over* v) if the restriction of w to κ is v, if this is the case we write $w|v$. The absolute value v is said p–adic if it lies over $|\cdot|_p$ the p–adic absolute value on $\mathbb{Q}$.

From the fact that $\mathbb{Z}$ is an unique factorization ring, follows the product formula for the absolute values over the rational numbers:

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1 \quad \text{for all } x \in \mathbb{Q},\, x \neq 0. \tag{31}$$

By point (ii) of Proposition A.1 to every place of κ correspond absolute values that differ logarithmically by a positive constant. It is now natural to choose a "canonical normalization" which allows to generalize (31).

Definition A.3. Let $v \in M_\kappa$, the *local degree of* v is $n_v := [\kappa_v : \mathbb{Q}_v]$, where κ_v and $\mathbb{Q}_v$ denote the completion of κ and $\mathbb{Q}$ with respect to v (or the restriction of v in the latter case). We define the *normalized absolute value* associated to the absolute value, or better the place, v as

$$\|x\|_v := |x|_v^{n_v}, \quad \text{for all } x \in \kappa.$$

The previous normalization simplifies the notation in the results of Diophantine approximation, such as Roth's theorem, and in the product formula:

Proposition A.2. (Product formula) Let $x \in \kappa - \{0\}$, then $\prod_{v \in M_\kappa} \|x\|_v = 1$.

We conclude this section recalling that is possible to characterize the ring of integers of κ by

$$\mathcal{O}_\kappa = \{x \in \kappa \ : \ |x|_v \leq 1 \ \text{ for all } v \text{ non archimedean absolute value on } \kappa \ \}.$$

This suggests the definition, for each subset S of places of κ containing the archimedean ones, of the *ring of S–integers of κ*

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

Its group of units is

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

and it is called *group of S–units*.

A.2 Height functions

Height functions are an useful tool that aims to quantifies the complexity of algebraic objects. Intuitively, a naive way to determine the size of a rational number p/q could be to take the maximum between the moduli of respectively the numerator and the denominator.

In general it is possible to define the height with respect to an absolute value $|\cdot|_v \in M_\kappa$, and defined for the rational points on an algebraic variety V/κ.

A.2.1 Heights on Projecive Space

A point $P \in \mathbb{P}^n(\mathbb{Q})$ can be written in the (almost unique) form

$$P = (x_0 : x_1 : \cdots : x_n) \quad \text{with } x_0, \ldots, x_n \in \mathbb{Z} \text{ and } \gcd(x_0, \ldots, x_n) = 1.$$

For a given absolute value $|\cdot|$ the *height of* P is defined to be the quantity $H(P) = \max\{|x_0|, \ldots, |x_n|\}$.

Definition A.4. Let $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\kappa)$ be a point with homogeneous coordinates in the number field κ. The *height of P relative to κ* is defined as

$$H_\kappa(P) := \prod_{v \in M_\kappa} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}.$$

It is also useful to define the so called *logarithmic height* $h_\kappa(P) := \log H_\kappa(P)$.

The height of an element $\alpha \in \kappa$ is defined as the height of the associated projective point $(\alpha : 1) \in \mathbb{P}^1(\kappa)$, so that

$$H_\kappa(\alpha) = \prod_{v \in M_\kappa} \max\{\|\alpha\|_v, 1\}.$$

Using the product formula it is possible to show that $H_\kappa(P)$ is well–posed and independent on the choice of homogeneous coordinates for P. It is also clear that by choosing coordinates such that $x_i = 1$ for some i we have $H_\kappa(P) \geq 1$ for every P.

Lemma A.1. If $P \in \mathbb{P}^n(\kappa)$ and let κ' be a finite extension of κ. Then

$$H_{\kappa'}(P) = H_\kappa(P)^{[\kappa':\kappa]}.$$

Proof. Recalling that $n_w = [\kappa' : \mathbb{Q}_w] = [\kappa'_w : \kappa_v]n_v$ we have

$$\begin{aligned} H_{\kappa'}(P) &= \prod_{w\in M_{\kappa'}} \max\{\|x_0\|_w, \dots, \|x_n\|_w\} = \prod_{v\in M_\kappa} \prod_{w\in M_{\kappa'},\, w|v} \max\{\|x_0\|_w, \dots, \|x_n\|_w\} \\ &= \prod_{v\in M_\kappa} \prod_{w\in M_{\kappa'},\, w|v} \max\{|x_0|_v^{n_w}, \dots, |x_n|_v^{n_w}\} = \prod_{v\in M_\kappa} \prod_{w\in M_{\kappa'},\, w|v} \max\{\|x_0\|_v, \dots, \|x_n\|_v\}^{[\kappa'_w:\kappa_v]} \\ &= \prod_{v\in M_\kappa} \max\{\|x_0\|_v, \dots, \|x_n\|_v\}^{[\kappa':\kappa]} = H_\kappa(P)^{[\kappa':\kappa]}, \end{aligned}$$

where in the end we used the degree formula

$$\sum_{w\in M_{\kappa'}, w|v} [\kappa'_w : \kappa_v] = [\kappa' : \kappa].$$

□

The previous lemma suggest the definition of an height function which is independent on the underlying field. We call *absolute height* on $\mathbb{P}^n$ the map $H : \mathbb{P}^n(\bar{\mathbb{Q}}) \to [1, \infty)$ defined as $H(P) = H_\kappa(P)^{1/[\kappa:\mathbb{Q}]}$ with κ any number field with $P \in \mathbb{P}^n(\kappa)$. Similarly the *absolute logarithmic height* on $\mathbb{P}^n$ is defined posing $h(P) = h_\kappa(P)/[\kappa : \mathbb{Q}]$.

We conclude this part stating the following finiteness result, which is of most importance for the application in Diophantine geometry.

Theorem A.1. (Northcott) For any pair of numbers $c \geq 0$, $d \geq 1$ the set

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) \,|\, H(P) \leq c \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

is finite; where $\mathbb{Q}(P)$ denotes the field extension $\mathbb{Q}(x_0/x_j, x_1/x_j, \dots, x_n/x_j)$ with the x's the coordinates of P and $x_j \neq 0$. In particular for any number field κ the set

$$\{P \in \mathbb{P}^n(\kappa) \,|H_\kappa(P) \leq c\}$$

is finite.

A.2.2 Heights on Varieties

We recall now how to extend the definition of height functions to points of an algebraic variety V defined over $\bar{Q}$.

Definition A.5. Let $\phi : V \to \mathbb{P}^n$ be a morphism. The *absolute logarithmic height on V relative to ϕ* is the map

$$h_\phi : V(\bar{\mathbb{Q}}) \to [0, \infty), \quad h_\phi(P) = h(\phi(P)),$$

where $h : \mathbb{P}(\bar{Q}) \to [0, \infty)$ is the height function defined previously. Notice that the definition applies in case V is embedded in $\mathbb{P}^n$.

We state now Weil's construction that associate an height function to every divisor of a smooth projective variety V/κ.

Theorem A.2. (Weil's Height Machine) For every smooth projective variety V over the number field κ there exists a map

$$h_V : Div(V) \longrightarrow \{\text{functions } V(\bar{\kappa}) \to \mathbb{R}\}$$

with the following properties:

(1) (Normalization) Let $H \subset \mathbb{P}^n$ be a hyperplane, then

$$h_{\mathbb{P}^n,H}(P) = h(P) + O(1), \quad \text{for all } P \in \mathbb{P}^n(\bar{\kappa}).$$

(2) (Functoriality) Let $\phi : V \to W$ and $D \in Div(W)$, then

$$h_{V,\phi^* D(P)} = h_{W,D}(\phi(P)) + O(1) \quad \text{for all } P \in V(\bar{\kappa}).$$

(3) (Additivity) Let $D, E \in Div(V)$, then

$$h_{V,D+E}(P) = h_{V,D}(P) + h_{V,E}(P) + O(1), \quad \text{for all } P \in V(\bar{\kappa}).$$

(4) (Linear Equivalence) If $D, E \in Div(V)$ are linearly equivalent then

$$h_{V,D}(P) = h_{V,E}(P) + O(1), \quad \text{for all } P \in V(\bar{\kappa}).$$

(5) (Positivity) If $D \in Div(V)$ is an effective divisor and B the base locus of the linear system $|D|$, then

$$h_{V,D}(P) \geq O(1), \quad \text{for all } P \in (V - B)(\bar{\kappa}).$$

(6) (Algebraic Equivalence) Let $D, E \in Div(V)$ with D ample and E algebraically equivalent to 0. Then

$$\lim_{P \in V(\bar{\kappa})\, h_{V,D}(P) \to \infty} \frac{h_{V,E}(P)}{h_{V,D}(P)} = 0.$$

(7) (Finiteness) Let $D \in Div(V)$ be an ample divisor of V. For every finite field extension κ'/κ and every constant c the set $\{P \in V(\kappa') \,|\, h_{V,D}(P) \leq c\}$ is finite.

(8) (Uniqueness) The height functions $h_{V,D}$ are determined, up to $O(1)$, by normalization (1), functoriality (2) just for embeddings $\phi : V \hookrightarrow \mathbb{P}^n$, and additivity (3).

This correspondence is valid in general, but for our purposes it will be sufficient to consider the case of algebraic curves (which is also easier to prove and deal with). For simplicity, we reformulate here point (6) which will be useful in the proof of Siegel's theorem.

Proposition A.3. Let C/κ be a smooth projective curve[3].

(i) Let $D, E \in Div(C)$ be divisors with $\deg(D) \geq 1$, then for $P \in C(\bar{\kappa})$

$$\lim_{h_D(P) \to \infty} \frac{h_E(P)}{h_D(P)} = \frac{\deg E}{\deg D}.$$

(ii) Let $f, g \in \kappa(C)$ be rational functions of C with f nonconstant. Then for $P \in C(\bar{\kappa})$

$$\lim_{h(f(P)) \to \infty} \frac{h(g(P))}{h(f(P))} = \frac{\deg g}{\deg f}.$$

[3]For notation convenience we drop the first subscript since the reference to the curve is clear by context.

References

[1] W. R. Knorr, "Archimedes and the measurement of the circle: a new interpretation," *Archive for history of exact sciences*, pp. 115–140, 1976.

[2] A. Wiles, "Modular elliptic curves and fermat's last theorem," *Annals of mathematics*, vol. 141, no. 3, pp. 443–551, 1995.

[3] S. Lang, *Diophantine geometry*. No. 11, Interscience publishers, 1962.

[4] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, vol. 201. Springer Science & Business Media, 2013.

[5] J. H. Evertse, "On equations in s-units and the thue-mahler equation," *Inventiones mathematicae*, vol. 75, pp. 561–584, 1984.

[6] J. Evertse, K. György, C. Stewart, and R. Tijdeman, *S-unit equations and their applications*. Rijksuniversiteit Leiden. Mathematisch Instituut, 1987.

[7] W. M. Schmidt, *Diophantine approximations and Diophantine equations*. Springer, 2006.

[8] P. Corvaja and U. Zannier, "A subspace theorem approach to integral points on curves," *Comptes Rendus Mathematique*, vol. 334, no. 4, pp. 267–271, 2002.

[9] A. Baker, *Transcendental number theory*. Cambridge university press, 2022.

[10] G. Faltings, "Diophantine approximation on abelian varieties," *Annals of Mathematics*, vol. 133, no. 3, pp. 549–576, 1991.

[11] P. Corvaja and P. Corvaja, "Integral points on surfaces," *Integral Points on Algebraic Varieties: An Introduction to Diophantine Geometry*, pp. 55–71, 2016.

[12] P. Corvaja, "Some arithmetic aspects of hyperbolicity," *Panoramas & Synthèses*, vol. 56, pp. 253–318, 2021.

[13] K. Conrad, "Ostrowski for number fields," *Expository papers on Algebraic Number Theory*, 2010.