UNIVERSITÀ DEGLI STUDI DI PADOVA
DIPARTIMENTO DI MATEMATICA
CORSO DI LAUREA MAGISTRALE IN MATEMATICA

MASTER THESIS

FINDING INTEGRAL POINTS ON ALGEBRAIC VARIETIES

Candidate:
Daniele Di Tullio
1130706

Supervisor University of Udine:
Prof. Pietro Corvaja
Internal Supervisor:
Prof. Bruno Chiarellotto

October 13, 2017

Academic Year 2016/2017

Abstract

The Vojta's conjecture establishes geometrical conditions on the degeneracy of the set of S-integral points for an algebraic variety. The goal of the thesis is to prove that for certain algebraic varieties for which such conditions are not verified the set of S-integral points is Zariski-dense. Some effective methods in this respect has been developed by Beukers in his paper "Ternary form Equations" , in which he proved the density of integral solutions of some homogeneous diophantine equations. Following such ideas, the work of the thesis consists of finding the density of S-integral points on some varieties for which it is not known at the moment, imposing the needed arithmetical and geometrical conditions.

Contents

1 Introduction **1**
- 1.1 Historical notes . . . 1
- 1.2 Goals and structure of the thesis. . . . 3

2 Pell equation and related equations **5**
- 2.1 Diophantine Approximation . . . 5
- 2.2 Solutions to Pell and Pell-type equations . . . 6
- 2.3 The general case of degree 2 . . . 9

3 S-integral points on algebraic varieties **11**
- 3.1 Some facts from valuation theory . . . 11
- 3.2 Definition and various characterizations . . . 12
- 3.3 Basic examples . . . 16
- 3.4 S-integral points for embedded varieties . . . 16
- 3.5 Integral points on linear subvarieties of the projective space . . . 17

4 Constructing integral points on surfaces **22**
- 4.1 Integral points on lines and conics . . . 22
- 4.2 Ternary homogeneous equations . . . 30

5 Higher dimensional results **43**
- 5.1 Integral points on quadric surfaces of $\mathbb{P}^3$ . . . 43
- 5.2 Quaternary homogeneous equations of degree≤ 3 . . . 46
- 5.3 Quaternary homogeneous equations of degree 4 . . . 52

Chapter 1

Introduction

1.1 Historical notes

The study of the diophantine equations, namely of the set of integral or rational solutions to an equation of the form

$$f(x_1, ..., x_n) = 0, \;\; f \in \mathbb{Z}[x_1, ..., x_n]$$

has fascinated many mathematicians since ancient times. One of the most famous problem is the Fermat's last theorem on the non-existence of solutions in integers to the diophantine equation

$$x^n + y^n = z^n$$

for $n \geq 3$. Fermat himself proved the conjecture in the case $n = 4$, successively Euler proved it for $n = 3$, Legendre for $n = 5$ and Kummer for n a regular prime. Nevertheless the general case was an open problem in Number Theory from 1637, when it was conjectured by Pierre de Fermat, to 1995 when it was definitively solved by Andrew Wiles, who used modern techniques from Algebraic Geometry and Algebraic Number Theory.

The research area of this thesis is Diophantine Geometry, the branch of Mathematics which studies diophantine equations using methods from Algebraic Geometry. Roughly speaking the idea of the subject is the following: suppose to have a diophantine equation

$$f(x_1, .., x_n) = 0, \;\; f \in \mathbb{Z}[x_1, ..., x_n].$$

Its zero locus in $\mathbb{C}$ is a complex algebraic variety $V(f)$ and we want to study how its geometric properties determine the distribution of integral or rational solutions of our equation.

In the case of the plane curves (when $n = 2$) the theorems of Siegel and Faltings give geometrical conditions for the finiteness of the set of the integral and rational points on an algebraic plane curve:

Theorem 1.1.1 (Siegel's Theorem)**.** *Let $\mathcal{C} \subseteq \mathbb{A}^2$ be an affine plane curve defined over $\mathbb{Q}$, let $\tilde{\mathcal{C}}$ be its projective closure. If $|\mathcal{C}(\mathbb{Z})| = \infty$ then $g(\mathcal{C}) = 0$ (so $\mathcal{C}$ is a rational curve) and $|\tilde{\mathcal{C}} \setminus \mathcal{C}| \leq 2$.*

Theorem 1.1.2 (Faltings' Theorem)**.** *Let $\tilde{\mathcal{C}}$ be a projective plane curve defined over $\mathbb{Q}$. If $|\tilde{\mathcal{C}}(\mathbb{Q})| = \infty$ then $g(\tilde{\mathcal{C}}) \in \{0, 1\}$.*

The previous results actually hold in a more general context: substituting any number field κ for $\mathbb{Q}$ and any ring of S-integers $\mathcal{O}_S$ for $\mathbb{Z}$ (for the definition of $\mathcal{O}_S$ see chapter 3). Observe that Faltings' theorem implies a weak version of Fermat's last theorem

Corollary 1.1.3. *The diophantine equation*

$$x^n + y^n = z^n$$

has only a finite number of primitive integral solutions if $n \geq 4$.

Proof. Primitive integral solutions correspond to $\mathbb{Q}$-rational points on

$$\tilde{\mathcal{C}} : X^n + Y^n = Z^n.$$

Since $\tilde{\mathcal{C}}$ is smooth, from the genus formula we have that

$$g(\mathcal{C}) = \frac{(n-1)(n-2)}{2}$$

then $g(\mathcal{C}) > 1$ for $n \geq 4$, by Faltings' theorem there is only a finite number of solutions in $\mathbb{Z}$. □

We see some example in which the set of rational point is infinite.

Example 1.1.4. It is known that the Fermat's equation for $n = 2$ has infinitely many primitive solutions, i.e. that the circumference

$$\tilde{\mathcal{C}} : X^2 + Y^2 = Z^2$$

has infinitely many $\mathbb{Q}$-rational points. Since for $Z = 0$ there is no solution in $\mathbb{Q}$, all the possible solutions are in the affine part

$$\mathcal{C} : x^2 + y^2 = 1$$

Note that there is a point with rational coordinates: $P = (1, 0)$, all the lines throw P except the vertical one are of those of equation

$$y = tx - t.$$

Note that there is a bijection between $t \in \mathbb{Q}$ and points with rational coordinates different from $(1, 0)$: in fact any line with slope $t \in \mathbb{Q}$ intersects $\mathcal{C}$ in a $\mathbb{Q}$-defined point and for any $Q \in \mathcal{C}$ κ-rational point the line L_{PQ} is defined over κ. So all the rational points of $\mathcal{C}$ are solutions of a system

$$\begin{cases} y & = t(x-1) \\ x^2 + y^2 & = 1 \end{cases}$$

It follows that all the primitive integral pythagorean triples are

$$\{(t^2 - s^2, -2ts, t^2 + s^2), \text{ where } t, s \in \mathbb{Z}, \ \gcd(t, s) = 1\}$$

Example 1.1.5. Consider the elliptic curve defined over $\mathbb{Q}$ whose affine equation is

$$E : y^2 = x^3 + ax + b$$

where $4a^3 + 27b^2 \neq 0$. Suppose that there is a point P which is $\mathbb{Q}$-rational and not a torsion point. Then there are infinitely many $\mathbb{Q}$-rational points on $\mathcal{C}$: in fact the summation formulas are defined over $\mathbb{Q}$, so

$$Q \mapsto Q \oplus P$$

is an infinite order automorphism defined over $\mathbb{Q}$ which preserves rational points. The idea of constructing infinitely many automorphisms which fix integral or rational points is widely used to prove the non-degeneracy of the set of S-integral points.

Faltings and Vojta gave deep generalizations of the Siegel's theorem in their papers [Fa], [V1] and [V2]. The idea of their work is to embed the varieties in their generalized Jacobian and to use the Roth theorem and the theory of the heights in the Jacobians. Corvaja and Zannier gave another proof of Siegel's theorem based on Schmidt Subspace Theorem, avoiding thus the use of the embedding in the jacobian. See for example [Co, Ch.3] for a proof. This approach has both the advantages to simplify the argument and to be generalizable to higher dimension.

Though many results has been discovered in higher dimension, it does not exist a result like Siegel and Faltings theorems for curve. Vojta formulated a conjecture, still unproven, which establishes conditions under which the integral points on an algebraic variety of arbitrary dimension is not Zariski-dense.

Conjecture 1.1.6 (Vojta's Conjecture)**.** Let $\tilde{X} \subseteq \mathbb{P}^n$ be a smooth complex projective variety defined over κ. Let D be a κ-defined divisor with only normal crossing singularities. Let K be a canonical divisor of $\tilde{X}$ and suppose that $K + D$ is big. Let S be any finite set of valuations containing the archimedean ones, then the set of the S-integral points on $\tilde{X} \setminus D$ is not Zariski-dense.

For the definition of S-integral point with respect to a divisor D the reader is referred to chapter 3. Recall that a divisor D on a projective variety $\tilde{X}$ is said to be big if

$$h^0(\tilde{X}, nD) \approx n^{\dim(\tilde{X})} \text{ for } n \to \infty.$$

1.2 Goals and structure of the thesis.

As we have seen in the previous section, many important results in literature concern the degeneracy of the set of integral points on algebraic varieties and of course Vojta's conjecture is one of the most important open problem in Diophantine Geometry. Nevertheless the goal of this thesis is in some sense the opposite: finding methods to prove the existence of a Zariski-dense set of integral points for algebraic varieties (obviously not satisfying the hypothesis of the Vojta conjecture). We will mainly follow the ideas developed by Beukers in his paper [Beu]. A standard method to construct integral points is to construct a large family of automorphisms of the variety fixing them. Anyway constructing such automorphisms is in general a difficult problem. The strategy ideated by Beukers

consists of finding a sufficiently large number of subvarieties on which it is known the density of integral points.

Chapter 2 contains standard results about the Pell equation and related equations. Though the content is very elementary, the method used to prove the infiniteness of the solutions in integers of a Pell-Type equation (if there is at least one of them) can be geometrically interpreted as the construction of an infinite order automorphism. It is a first example of the which we will use later.

In Chapter 3 we give the definition of S-integral point, which depends on a number field κ, on a finite set of primes of κ, on projective variety defined over κ, on a divisor of the variety defined over κ. We will see various characterizations and examples. This chapter belongs to the compilation part of the thesis, nevertheless some characterization of the notion of S-integral point is not usual in literature and the section about integral points on linear spaces is a generalization of a result proved by Beukers in [Beu] and other mathematicians before him

Chapter 4 belongs to the compilation part of the work: we describe the method developed by Beukers in his paper [Beu] used to prove existence of a Zariski-dense set of integral points on algebraic surfaces of the type $\mathbb{P}^2 \setminus D$, $\deg(D) \leq 3$. It is related to find solutions to ternary homogeneous equations of low degree, particularly interesting is the case when the degree is 3. The original contribution in this chapter consists of some interesting examples and some results of density (theorems 4.2.8 and 4.2.12) concerning higher degree divisors with not normal crossing singularities.

Chapter 5 is the original one of the thesis. We generalize the ideas of Chapter 4 to prove the non-degeneracy of the set of the integral points on 3-dimensional algebraic varieties of the type $\mathbb{P}^3 \setminus D$. Analogously to what happens in chapter 4, it is related to the solutions of some quaternary homogeneous equations. Particularly interesting is the case when $\deg(D) = 4$. The author was able to prove the density only under some particular hypothesis on the geometry of D.

Chapter 2

Pell equation and related equations

One of the most famous diophantine equations is the so-called Pell equation:

$$x^2 - dy^2 = 1$$

where d is a square-free integer. As we will prove in this section, this equation has an infinity of solutions in integers. A complete treatment can be found in [Za, Ch. 1, Sec 4] or in [Mo, Ch. 8]. A strictly related problem is the following:

$$x^2 - dy^2 = m \text{ where } m \in \mathbb{Z}$$

This kind of diophantine equation is called Pell type equation. Not always this equation has solutions. But if there is a solution, then the equation has infinity solutions.

2.1 Diophantine Approximation

The first step in proving the existence of infinite solutions of a Pell equation is to discuss about Diophantine approximation. Informally the subject is to find a "good" rational approximation of a real number α. The idea is that a rational approximation $\frac{p}{q}$ $(p, q \in \mathbb{Z})$ with $\gcd(p, q) = 1$ is good whenever we are able to obtain a small value of $\left|\frac{p}{q} - \alpha\right|$ using small coprime integers p, q. So for example we want to consider $\left|\sqrt{2} - \frac{99}{70}\right| \simeq 7.2 \cdot 10^{-5}$ a better approximation than $\left|\sqrt{2} - \frac{1414213}{1000000}\right| \simeq 5.6 \cdot 10^{-6}$, though the last is more accurate considering only the absolute value of the difference. More formally:

Definition 2.1.1. A rational approximation is good if $\left|\frac{p}{q} - \alpha\right| < q^{-2}$

In fact, there are infinitely many good approximations of an $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ as stated by the following proposition.

Proposition 2.1.2. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then there are infinitely many $p, q \in \mathbb{Z}$ such that* $\gcd(p, q) = 1$ *and*

$$|q\alpha - p| < q^{-1}$$

For the proof we need the following lemma:

Lemma 2.1.3. (Dirichlet) *Let $n \in \mathbb{Z}^+$, $\alpha \in \mathbb{R}$. Then it is possible to find $p, q \in \mathbb{Z}$ such that $0 < q \leq n$ and*

$$|q\alpha - p| < \frac{1}{n+1}$$

Proof. (of the lemma) The problem is clearly solved if we find $q \in \{0, 1, \dots n\}$ such that

$$|\{q\alpha\}| < \frac{1}{n+1} \text{ (We take } p = \lfloor q\alpha \rfloor)$$

So consider the set $\{0, \{\alpha\}, \dots, \{n\alpha\}\}$ and the partition of the interval $[0, 1)$:

$$[0,1) = \left[0, \frac{1}{n+1}\right) \cup \dots \cup \left[\frac{n}{n+1}, 1\right)$$

Two situations may occur:

(1) There is a $q \in \{0, ..., n\}$ such that $\{q\alpha\} \in \left[0, \frac{1}{n+1}\right)$. In this case it is plain that we are done.

(2) There is no $q \in \{0, ..., n\}$ such that $\{q\alpha\} \in \left[0, \frac{1}{n+1}\right)$. The set $\{0, \{\alpha\}, \dots, \{n\alpha\}\}$ has $n+1$ elements so by the box's principle there are distinct $r, s \in \{0, ..., n\}$ such that $\{r\alpha\}, \{s\alpha\} \in \left[\frac{m}{n+1}, \frac{m+1}{n+1}\right)$. So $|\{r\alpha\} - \{s\alpha\}| < \frac{1}{n+1}$ and the conclusion follows from the fact that if $r > s$ then $|\{(r-s)\alpha\}| = |\{(r)\alpha\} - \{(s)\alpha\}|$

It can happen that p and q are not coprime, but we can simplify the factors by $\gcd(p, q)$ and the inequality holds a fortiori. □

Proof. (of the proposition) The fact that it exists a couple (p, q) such that $\gcd(p, q) = 1$ and $|q\alpha - p| < q^{-1}$ is trivial: we can choose $q = 1$ and $p = \lfloor \alpha \rfloor$. Suppose now that there are only finitely many couples $(p_i, q_i) \in \mathbb{Z} \times \mathbb{Z}$ such that $|q_i\alpha - p_i| < q_i^{-1}$. Let $\epsilon := \min |q_i\alpha - p_i|$, so $\epsilon > 0$ (here we use the fact that $\alpha \in \mathbb{R} \setminus \mathbb{Q}$) and we choose $n >> 0$ such that $\epsilon < \frac{1}{n}$. Apply the previous lemma: we can find p and q such that

$$|q\alpha - p| < \frac{1}{n} < \epsilon$$

which is a contradiction. □

2.2 Solutions to Pell and Pell-type equations

As anticipated before, the diophantine approximation problem is related to Pell equations. Suppose to have a solution (x, y) of $x^2 - dy^2 = 1$. We can assume that $x, y > 0$. So

$x = \sqrt{1+dy^2}$, so $|x - y\sqrt{d}| = \sqrt{1+dy^2} - y\sqrt{d}$. Recall that in general $\sqrt{1+x} \leq 1 + \frac{1}{2}x$ for $x \geq 0$. So we have the following inequality:

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2\sqrt{d}y^2}$$

in other words a solution of the equation gives a good rational approximation of $\sqrt{d}$. We will see in the proof of the next theorem how we can perform the other direction, so how to prove the existence of solutions of a Pell Equation, starting from the diophantine approximation.

Theorem 2.2.1. *There are infinitely many solutions to the Pell equation*

$$x^2 - dy^2 = 1$$

Proof. The proof consists of two steps:

STEP 1 In this first step we prove that for a suitable choice of an integer $k \in \mathbb{Z}$ the equation

$$x^2 - dy^2 = k$$

has infinitely many solutions. We know by diophantine approximation that the inequality

$$|x - y\sqrt{d}| < \frac{1}{|y|}$$

has infinitely many integral solutions with $\gcd(x, y) = 1$.
Note that from the inequality $|x - y\sqrt{d}| \leq |y^{-1}| \leq 1$ we get that $x \leq 1 + y\sqrt{d}$. This implies the following chain of inequalities

$$|x^2 - dy^2| = |x \leq 1 + y\sqrt{d}||x \leq 1 - y\sqrt{d}| \leq \frac{2|y|\sqrt{d}}{|y|} \leq 2\sqrt{d} + 1$$

So actually all the infinitely many solutions (x, y) of the good-approximation problem are such that the quantity $x^2 - dy^2 \in (-1 - 2\sqrt{d}, 1 + 2\sqrt{d}) \cap \mathbb{Z}$, which is a finite set. So there must be a $k \in (-1 - 2\sqrt{d}, 1 + 2\sqrt{d}) \cap \mathbb{Z}$ such that the diophantine equation

$$x^2 - dy^2 = k$$

has infinitely many solutions.

STEP 2 The idea is the following: two solutions $(x_1, y_1), (x_2, y_2)$ of the equation of STEP 1 correspond to factorizazions in the ring $\mathbb{Z}[\sqrt{d}]$:

$$\begin{aligned}(x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d}) &= k \\ (x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) &= k\end{aligned} \tag{2.1}$$

The idea is to divide the two equations, obtaining in this way a factorizazion of the form

$$\alpha\beta = 1, \quad \alpha, \beta \in \mathbb{Q}[\sqrt{d}]$$

We are interested to the case in which $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$. It happens when we have "non-trivially" equivalent factorizations, i.e. when

$$\begin{aligned}(x_1 + y_1\sqrt{d}) &= u(x_2 + y_2\sqrt{d}) \\ (x_1 - y_1\sqrt{d}) &= u^{-1}(x_2 - y_2\sqrt{d})\end{aligned} \tag{2.2}$$

$u \in \mathbb{Z}[\sqrt{d}]^* \setminus \{\pm 1\}$ (And in fact we want to prove that $\mathbb{Z}[\sqrt{d}] \neq \{\pm 1\}$)
Consider the fraction $\dfrac{x_1 + y_1\sqrt{d}}{x_2 + y_2\sqrt{d}} = \dfrac{1}{k}[(x_1x_2 - dy_1y_2) + \sqrt{d}(-x_1y_2 + x_2y_1)]$
it is an element of $\mathbb{Z}[\sqrt{d}]$ if

$$\begin{cases} x_1 \equiv x_2 \mod k \\ y_1 \equiv y_2 \mod k \end{cases}$$

We have infinitely many solution $(x, y) \in \mathbb{Z}^2$ to the equation $x^2 - dy^2 = k$, so there are infinitely many of them congruent $\mod k$ and so equivalent, consequently there are infinitely many non-trivially equivalent (i.e. $u \neq \pm 1$). And so we are able to find a non-trivial solution (ξ, η) of this Pell equation (i.e. with $\eta \neq 0$). Having a non trivial solution allows us to construct infinitely many distinct solutions simply taking power. □

Remark 2.2.2. Whenever $d \neq 1 \mod 4$ the ring $\mathbb{Z}[\sqrt{d}]$ is exactly the ring of integers O_κ of the number field $\kappa = \mathbb{Q}[\sqrt{d}]$. Remember the Dirichlet Unit Theorem (See for example [Ma, Ch.5] or [Mi1, Ch. 5])

$$O_\kappa^* \cong U \times \mathbb{Z}^{r_1 + r_2 - 1}$$

where U is the group of roots of unity in O_κ, r_1 is the number of the real embeddings of κ and r_2 is the number of complex non-coniugate embeddings. In the case $\kappa = \mathbb{Q}[\sqrt{d}]$ $r_1 + r_2 - 1 = 1$, $U = \{\pm 1\}$.
One can prove, following essentially the same method of the proof of Dirichlet Unit Theorem, that also in the case $d \equiv 1 \mod 4$ the structure of $\mathbb{Z}[\sqrt{d}]^*$ is of this kind. See for example [Za, Ch.1, Sec. 4].

Remark 2.2.3. We have seen during the proof of the above theorem that if there is a non-trivial solution we can construct infinitely many of them. There is also a geometric interpretation of this fact: the orthogonal group over $\mathbb{Z}$ of the quadratic form $x^2 - dy^2$ is composed by elements of the shape $M = \begin{pmatrix} x & \pm dy \\ y & \pm x \end{pmatrix}$ where $x, y \in \mathbb{Z}$ and $x^2 - dy^2 = 1$. This group fixes the hyperbola $x^2 - dy^2 = 1$ and preserve points with coordinates in $\mathbb{Z}$.

In general the diophantine equation, called Pell type equation,

$$x^2 - dy^2 = m$$

with $m \neq \pm 1$ not necessarily has solutions in integers for example

$$x^2 - 3y^2 = 2$$

has no solution as it can be shown by an easy argument: If $(x, y) \in \mathbb{Z}^2$ would be a solution, then necessarily $x \equiv y \equiv 1 \bmod 2$ and so $x^2 \equiv y^2 \equiv 1 \bmod 8$. It follows that

$$x^2 - 3y^2 \equiv -2 \mod 8$$

which is a contradiction.
Anyway applying the idea of the remark it is possible to show that the existence of one solution to Pell type equation implies that they are infinitely many.

Proposition 2.2.4. *Let d be a squarefree positive integer. Suppose that there is $(x, y) \in \mathbb{Z}^2$ such that*

$$x^2 - dy^2 = m$$

Then there are infinitely many solutions to such diophantine equation.

Proof. Suppose that $(a, b) \in \mathbb{Z}^2$ is a solution of the Pell equation

$$a^2 - db^2 = 1$$

then by remark 2.2.3 there is an element of the orthogonal group over $\mathbb{Z}$ of the quadratic form $X^2 - dY^2$, namely

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}$$

which fixes the hyperbola $x^2 - dy^2 = m$ and preserves integral points. □

2.3 The general case of degree 2

Now we want to understand when an irreducible conic $\mathcal{C}$ of equation

$$Q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0 \text{ where } a, b, c, d, e, f \in \mathbb{Z} \tag{2.3}$$

has infinitely many integral points. Recall the classification of the real affine plane conics:

(i) It is an hyperbola whenever it has two real points at infinity, i.e. whenever $ax^2 + bxy + cy^2$ split into two linear form over $\mathbb{R}[x, y]$

(ii) It is a parabola whenever it has one real points at infinity, i.e. whenever $ax^2 + bxy + cy^2$ is the square of a linear form over $\mathbb{R}[x, y]$

(iii) It is an ellipse whenever it has two complex conjugated points at infinity i.e whenever $ax^2 + bxy + cy^2$ is irreducible over $\mathbb{R}[x, y]$.

In the case (iii) it is plain that it has only a finite number of integral points, in fact $\mathbb{Z}^2$is a lattice in $\mathbb{R}^2$ and an ellipse is a compact subset.

The case (i) generalizes that of Pell-type equations. And actually it is possible to reduce the problem to Pell equation. In fact let $ax^2 + bxy + cy^2 + dx + ey + f = 0$ be the equation of the hyperbola. We can do the following change of variables:

$$\begin{cases} t = 2ax + by + d \\ u = (b^2 - 4ac)y + bd - 2ae \end{cases}$$

We got that the equation of the hyperbola is a Pell-type equation

$$u^2 - \Delta t^2 = \alpha^2 + \Delta\beta \tag{2.4}$$

where

$$\Delta = b^2 + 4ac, \quad \alpha = bd - 2ae \quad \beta = 4af - d^2$$

One can verify that the integral solutions (x, y) of (1.3) correspond to integral solutions (u, v) of (1.4) which further satisfy the following congruences:

$$\begin{cases} u \equiv \alpha \mod \Delta \\ \Delta t \equiv b(u - \alpha) + \Delta d \mod 2a\Delta \end{cases}$$

If Δ is a square it is trivial that there are only finitely many solutions. If it is not a square we can consider μ a non trivial element of $\mathbb{Z}[\sqrt{\Delta}]^*$. Because of the fact that $\mathbb{Z}[\sqrt{\Delta}]/(2a\Delta)$ is a finite set, there exists an integer $m \in \mathbb{N}$ such that $\mu^m \equiv 1 \mod 2a\Delta$. If (u, t) is a solution of (1.4) satisfying the congruences, also (u', t') given by $u' + t'\sqrt{\Delta} = (u + t\sqrt{\Delta})\mu^k$ it is. Consequently we have found an infinite family of solutions of the starting problem.

Consider now the case (ii). We have that $ax^2 + bxy + cy^2 = A(rx + sy)^2$, where $A, r, s \in \mathbb{Z}$ and $\gcd(r, s) = 1$. There exists a Bezout relation:

$$ru - sv = 1, \quad u, v \in \mathbb{Z}$$

so we can do the following change of coordinates:

$$\begin{cases} X = rx + sy \\ Y = vx + uy \end{cases}$$

Since $\det \left(\begin{smallmatrix} r & s \\ v & u \end{smallmatrix} \right) = 1$, the linear isomorphism induced by this matrix preserves integral points. We have thus shown that we can assume without loss of generality that the equation of the parabola is

$$dy = ax^2 + bx + c$$

This is a congruence problem, in fact it is equivalent to solve

$$ax^2 + bx + c \equiv 0 \mod d$$

and it is clear that if there is a solution, there are infinitely many.

Chapter 3

S-integral points on algebraic varieties

In this section we will give a notion which generalizes that of integral points on an affine variety. For an affine variety a point is integral if all their coordinates are. This kind of notion cannot be immediately generalized to arbitrary quasi-projective varieties. Consider for example the case of the projective space $\mathbb{P}^n(\mathbb{C})$. We know that a point $P = [p_0 : ... : p_n]$ is said to be $\mathbb{Q}$-rational if it is possible to find a suitable choice of the homogeneous coordinates such that $p_0, ..., p_n \in \mathbb{Q}$. But then we can also find a choice such that $p_0, ..., p_n \in \mathbb{Z}$, so every $\mathbb{Q}$-rational point is also integral, which does not agree with what we expect in the case of affine spaces. Identifying $\mathbb{A}^n$ with $\mathbb{P}^n \setminus D$ with $D = \{X_0 = 0\}$ the integral points of $\mathbb{A}^n$ correspond to $\{[1 : a_1, ..., a_n] : a_1, ..., a_n \in \mathbb{Z}\}$. Note that in general for every $P \in \mathbb{P}^n(\mathbb{Q})$ is possible to choose the coordinates in such a way that $p_0, \dots p_n \in \mathbb{Z}$ and $\gcd(p_0, ..., p_n) = 1$. The integral points on $\mathbb{P}^2 \setminus D$ are those which do not "reduce to D" modulo every prime p, making that particular choice of the homogeneous coordinates. The idea is that the notion of integrality depends on the divisor we are removing from $\mathbb{P}^n$.

3.1 Some facts from valuation theory

Recall some results about the theory of the absolute values which we will need later, see for example [Mi1, Ch.7,8].

Definition 3.1.1. Let K be a field. An absolute value on K is a a function $|| : K \to \mathbb{R}$ such that

1) $|a| \geq 0$, $|a| = 0 \iff a = 0$

2) $|ab| = |a||b|$

3) $|a + b| \leq |a| + |b|$

An absolute value is called non-archimedean if $|a + b| \leq \max(|a|, |b|)\ \forall a, b \in K$, archimedean otherwise.

Example 3.1.2. Let $\mathbb{Q}$ be the field of the rational numbers. There is the standard euclidean absolute value $|\cdot|$ which is archimedean. There are also non-archimedean absolute values

corresponding to the prime integers p:

$$|x|_p := \left(\frac{1}{p}\right)^{v_p(x)}$$

where v_p is the p-adic valuation.

In some sense these are the only absolute values on $\mathbb{Q}$.

Definition 3.1.3. Let K be a field. Two absolute values are equivalent if they induce the same topology on K.

Proposition 3.1.4. *$|\cdot|_v$ and $|\cdot|_w$ are equivalent if and only if $\exists \alpha > 0$ such that*

$$|\cdot|_v = |\cdot|_w^\alpha$$

Definition 3.1.5. A place on a field κ is an equivalence class of absolute values.

Theorem 3.1.6. *Let κ be a number field, the "infinite" (archimedean) places of κ correspond to the non-conjugate inclusions $\sigma : \kappa \hookrightarrow \mathbb{C}$: in fact all the non-equivalent archimedean valuations are those of the form*

$$\{|\cdot| \circ \sigma, \ \ \sigma \in Emb(\kappa/\mathbb{Q})\}$$

The "finite" (non-archimedean) non-equivalent absolute values correspond to $\mathfrak{p}$-adic valuations, where $\mathfrak{p} \in Spec(\mathcal{O}_\kappa)$.

As for the standard euclidean absolute value, there exist analogue notions of Cauchy sequence and completion of a valuation field (κ, v), denoted by κ_v.

3.2 Definition and various characterizations

Definition 3.2.1. Let κ be a number field, let S be a finite set of valuations of κ containing the archimedean ones. The ring of S-integers of κ is

$$\mathcal{O}_S := \bigcap_{v \notin S} \mathcal{O}_v = \{x \in \kappa \text{ such that } |x|_v \leq 1 \ \ \forall v \notin S\}$$

Remark 3.2.2. Note that $\mathcal{O}_S \supseteq \mathcal{O}_\kappa$. If $S = \{\infty\}$ then $\mathcal{O}_S = \mathcal{O}_\kappa$.

Example 3.2.3. Let $\kappa = \mathbb{Q}$, $S = \{\infty, p_1, ..., p_t\}$, then $\mathcal{O}_S = \left\{ \dfrac{m}{p_1^{e_1} \cdot ... \cdot p_t^{e_t}} \right\}$

Note that, since $\mathcal{O}_v$ is a PID, we can define a reduction map in a very similar way to what we did at the beginning of this section in the case of $\mathbb{Z}$:

$$\begin{array}{rccc} \rho_{\kappa,v} : & \mathbb{P}^n(\kappa) & \to & \mathbb{P}^n(\kappa(v)) \\ & [p_0 : ..., p_n] & \mapsto & [p_0 \mod v : ... : p_n \mod v] \end{array}$$

by choosing coordinates $[p_0 : \cdots : p_n]$ such that $p_0, ..., p_n \in \mathcal{O}_v$ and $\gcd(p_0, ..., p_n) = 1$ in $\mathcal{O}_v$.

Definition 3.2.4. Let κ be a number field. Let v be a non-archimedean valuation of κ. Let $P, Q \in \mathbb{P}^n(\bar{\mathbb{Q}})$. Let κ'/κ be a number field on which both P and Q are defined. Let V' be the set of the valuations of κ' extending v. We say that P does not coincide with $Q \bmod v$ or that P does not reduce to $Q \bmod v$ if

$$\rho_{\kappa',v'}(P) \neq \rho_{\kappa',v'}(Q), \ \forall v \in V'$$

Remark 3.2.5. The previous definition is independent from the choice of the extension κ'/κ in which both P and Q are defined. In fact if there is $\kappa'' \supset \kappa'$ then for every v'' extending a fixed valuation v' of κ'

$$Q \equiv P \mod v' \iff Q \equiv P \mod v''$$

Definition 3.2.6. Let κ be a number field, let S be a finite set of valuations containing the archimedean ones. Let X be an irreducible smooth projective variety defined over κ. Let D be an effective divisor defined over κ. Let $P \in X \setminus D$ be a κ-rational point. We say that P is an S-integral point on $X \setminus D$ if P does not coincide with $Q \bmod v$, $\forall Q \in D(\bar{\mathbb{Q}})$, $\forall v \notin S$.

Remark 3.2.7. Let κ be a number field, let S be a finite set of valuations containing the archimedean ones. Let $P = [p_0 : \cdots : p_n]$, $Q = [p_0 : \cdots : p_n] \in \mathbb{P}^n(\kappa)$, the condition that P and Q do not coincide mod v for any $v \notin S$ can be described "globally":

$$(\{p_i q_j - p_j q_i : 0 \leq i < j \leq n\}) = (p_0, ..., p_n)(q_0, ..., q_n)$$

where the equality holds in $\mathrm{Spec}(\mathcal{O}_S)$. Obviously the only non trivial inclusion is "$\supseteq$".

In the case when the variety is the projective space there is a nicer characterization.

Lemma 3.2.8. *Let κ a number field. Let $\mathfrak{p} \in Spec(\mathcal{O}_\kappa)$. Let $f \in \mathcal{O}_\mathfrak{p}[x]$ be a polynomial with coprime coefficients in $\mathcal{O}_\mathfrak{p}$. Suppose that $x_0 \bmod \mathfrak{p}$ is a solution of the congruence*

$$f(x) \equiv 0 \mod \mathfrak{p}$$

Then it is possible to find a number field extension ℓ/κ, a prime $\mathcal{P} \in Spec(\mathcal{O}_\ell)$ lying over $\mathfrak{p}$ and $x_1 \in \mathcal{O}_\mathcal{P}$ such that

1. $f(x_1) = 0$
2. $x_1 \equiv x_0 \bmod \mathcal{P}$

Proof. Let ℓ be the splitting field of $f(x)$. Let $\mathcal{P}$ be a prime lying over $\mathfrak{p}$. Then there is a factorization of $f(x)$ in $\mathcal{O}_\mathcal{P}[x]$

$$f(x) = (a_1 x + b_1)(a_2 x + b_2) \cdots (a_n x + b_n)$$

where $\gcd(a_i, b_i) = 1$ in $\mathcal{O}_\mathcal{P}$. Note that it is not possible that $\mathcal{P} \mid a_i$ for all $i = 1, ..., n$. Otherwise $f(x) \bmod \mathcal{P}$ would have no solution, contradicting our assumptions. Suppose that $a_1, ..., a_m$ are all the a_i not divided by $\mathcal{P}$, then $f(x) \bmod \mathcal{P}$ has degree m (and so $f(x) \bmod \mathfrak{p}$), and so all its roots are classes $\bmod \mathcal{P}$ of some $-\dfrac{b_i}{a_i}$ for $i = 1, ..., m$, in particular $x_0 \bmod \mathfrak{p}$. □

Proposition 3.2.9. *Let κ be a number field, let v be a non-archimedean valuation of κ. Let D be a κ-defined divisor of $\mathbb{P}^n$ defined by the equation*

$$F(X_0, ..., X_n) = 0,\ F \in \kappa[X_0, \dots, X_n]$$

Then:

$$P \text{ does not coincide with } Q \mod v\ \forall Q \in D(\bar{\kappa}) \iff F(P) \in \mathcal{O}_v^*$$

whenever we choose coprime coefficients for F in $\mathcal{O}_v$ and coprime coordinates for P in $\mathcal{O}_v$.

Proof. The implication "$\Leftarrow$" is easy: if P reduces to a point $Q \in D \mod v$, then, denoting κ'/κ a finite extension on which Q is defined, there is a valuation v' of κ' extending v such that $P \mod v' = Q \mod v'$, then $F(P) \equiv 0 \mod v'$, so $F(P) \equiv 0 \mod v$.

Consider now the implication "$\Rightarrow$". Assume that $F \in \mathcal{O}_v[X_0, ..., X_n]$ with coprime coefficients and $P = [x_0 : \cdots : x_n]$ where $x_0, ..., x_n \in \mathcal{O}_v$ and $\gcd(x_0, ..., x_n) = 1$. Suppose that $F(x_0, ..., x_n) \equiv 0 \mod v$, we want to find $Q \in D$ coinciding with $P \mod v$. There is $i \in \{1, ..., n\}$ such that $v(x_i) = 0$. We can assume without loss of generality that $i = 0$ and that $x_0 = 1$. Let $f(x_1, ..., x_n) := F(1, x_1, ..., x_n)$, we are reduced to the problem of lifting $(x_1, ..., x_n) \mod v$ solution of

$$f(x_1, ..., x_n) \equiv 0 \mod v$$

to a a point $(x_1', ..., x_n')$ such that $f(x_1', ..., x_n') = 0$. This can be done simply fixing $n-1$ variables and considering the problem in t

$$f(t, x_2, ..., x_n) \equiv 0$$

Then by lemma 3.2.8 there is an extension field κ'/κ, a valuation v' extending v such that $x_1' \equiv x_1 \mod v$ and $f(x_1', x_2, ..., x_n) = 0$. □

Corollary 3.2.10. *Let κ be a number field, $D \subset \mathbb{P}^n$ a κ-defined divisor. Let S be a finite set places containing the archimedean ones. Then*

$$P \in \mathbb{P}^n(\kappa) \setminus D \text{ is an } S\text{-integral point}$$
$$\iff$$
$$v(F(P)) = 0 \text{ for all } v \notin S, \text{ choosing coprime coefficients for } F \text{ in } \mathcal{O}_v \text{ and coprime coordinates for } P \text{ in } \mathcal{O}_v.$$

Proof. Immediate from the previous proposition. □

This notion of S-integral point generalizes the usual notion, as shown by the following proposition.

Proposition 3.2.11. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Consider $X = \mathbb{P}^n$ and let $D = \{X_0 = 0\}$. Then the set of S-integral points on $\mathbb{A}^n = \mathbb{P}^n \setminus D$ is*

$$\mathbb{A}^n(\mathcal{O}_S) = \mathcal{O}_S^n = \{[1 : a_1 : ... : a_n] : a_1, ..., a_n \in \mathcal{O}_S\}$$

Proof. It is clear that every point $[1 : a_1 : ... : a_n]$ with $a_1, ..., a_m \in \mathcal{O}_S$ is an S-integral point on $\mathbb{P}^n \setminus D$. Consider now the converse inclusion:
Assume that $a_0, ..., a_n \in \mathcal{O}_S$. If $[a_0 : ... : a_n]$ is S-integral, let $\mathfrak{a} = \gcd(a_0, ..., a_n)$, it can be factorized

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$$

Let $v \notin S$ be a place of κ, let $\mathfrak{p}_v$ be the corresponding prime ideal. Suppose that $\mathfrak{p}_v \notin \{\mathfrak{p}_1, ..., \mathfrak{p}_t\}$, then in $\mathcal{O}_v$ we have that $\gcd(a_0, ..., a_n) = 1$ and so the fact that the point $[a_0 : ... : a_n]$ does not reduce to D means that $\mathfrak{p}_v \nmid a_0$, i.e. $|a_0|_v = 1$, and then in particular $|a_0|_v \geq \max(|a_1|_v, ..., |a_n|_v)$.
Suppose now that $\mathfrak{p}_v = \mathfrak{p}_1$, choose $b \in \mathfrak{p}_1^{e_1} \setminus \mathfrak{p}_1^{e_1+1}$. Then

$$\left[\frac{a_0}{b} : ... : \frac{a_n}{b}\right] = [a_0 : ... : a_n]$$

and $\frac{a_0}{b}, ..., \frac{a_n}{b} \in \mathcal{O}_v, \gcd\left(\frac{a_0}{b}, ..., \frac{a_n}{b}\right) = 1$ in $\mathcal{O}_v$. The fact that the point does not reduce to D implies that $\mathfrak{p}_v \nmid \frac{a_0}{b}$, it follows also in this case that $|a_0|_v \geq \max(|a_1|_v, ..., |a_n|_v)$. This means that $\frac{a_1}{a_0}, ..., \frac{a_n}{a_0} \in \mathcal{O}_S$. □

There is also a more global characterization of S-integral points when $X = \mathbb{P}^n$:

Proposition 3.2.12. *Let $A \in \mathbb{P}^n(\kappa)$, let $D = \{F(X_0, ..., X_n) = 0\}$ be a κ-defined divisor, $d = \deg(F)$. Let $\mathcal{A}$ be the (fractional) ideal generated by the homogeneous coordinates of A, let $\mathcal{F}$ be the ideal generated by the coefficients of F. Then*

$$A \text{ is } S\text{-integral} \iff (F(A)) = \mathcal{F} \cdot \mathcal{A}^d$$

Remark 3.2.13. This is independent from the choice of homogeneous coordinates for and coefficients for F. And it is equivalent to the fact that $F(A) \in \mathcal{O}_S^*$ whenever $\mathcal{O}_S$ is a UFD, choosing F and A with coprime coefficients.

Proof. Note that in general $F(A) \in \mathcal{F} \cdot \mathcal{A}^d \iff (F(A)) \subseteq \mathcal{F} \cdot \mathcal{A}^d$.
Suppose that A is S-integral. Let $v \notin S$ a valuation of κ, the fact that A does not reduce to $D \mod v$ means that if we choose $a, f \in \mathcal{O}_v$ such that $(a) = \mathcal{A}, (f) = \mathcal{F}$ then

$$\frac{1}{f} F\left(\frac{1}{a} A\right) = (1) \iff (F(A)) = \mathcal{F} \cdot \mathcal{A}^n, \text{ in } \mathcal{O}_v$$

this is equivalent to the fact that $|F(A)|_v = |\mathcal{F} \cdot \mathcal{A}^n|_v, \ \forall v \notin S \iff (F(A)) = \mathcal{F} \cdot \mathcal{A}^n$

□

Remark 3.2.14. Note that, if $\mathcal{O}_S$ is a PID, for every $P = [p_0 : ....p_n] \in \mathbb{P}^n(\kappa)$ we can choose representatives in such a way that $p_0, ..., p_n \in \mathcal{O}_S$, $\gcd(p_0, ..., p_n) = 1$. In this case let $F(X_0, ..., X_n) = 0$ be the equation of D, where $F(X_0, ..., X_n) \in \mathcal{O}_S[X_0, ..., X_n]$ is an homogeneous polynomial with coprime coefficients, then P is an S-integral point if and only if $F(p_0, ..., p_n) \in \mathcal{O}_S^*$

Remark 3.2.15. In the case $\kappa = \mathbb{Q}$ and $S = \{\infty\}$, if $F \in \mathbb{Z}[X_0, \ldots, X_n]$ is a homogeneous polynomial with coprime coefficients, then if $D := V(F)$ then integral points on $\mathbb{P}^n \setminus D$ correspond to solutions in $\mathbb{Z}$ of the diophantine equation

$$F(X_0, \ldots, X_n) = \pm 1$$

3.3 Basic examples

Example 3.3.1. Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{[1:0],[0:1]\}$, $\kappa = \mathbb{Q}$, $S = \{\infty\}$. Let $[x_0 : x_1] \in \mathbb{G}_m$, where $x_0, x_1 \in \mathbb{Z}$ and $\gcd(x_0, x_1) = 1$. $[x_0 : x_1]$ is an integral point if

$$p \nmid x_0, x_1 \forall p \text{ prime} \iff [x_0 : x_1] = [1 : \pm 1]$$

So in this case there are only finitely many S-integral points.

Example 3.3.2. Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{[1:0],[0:1]\}$, $\kappa = \mathbb{Q}$, $S = \{\infty, p_1, ..., p_t\}$. In this case the S-integral points are those of the form $\pm p_1^{e_1} \cdot ... \cdot p_t^{e_t}$, $e_1, ..., e_t \in \mathbb{Z}$, of course they are infinitely many if $t > 0$.

Example 3.3.3. Consider $\kappa = \mathbb{Q}$, $S = \{\infty\}$, $X = \mathbb{P}^1$, $D = \{[1 : \pm i]\}$, then D has equation $X^2 + Y^2 = 0$, so $[x : y]$ with $x, y \in \mathbb{Z}, \gcd(x, y) = 1$ is integral if $x^2 + y^2 \in \{\pm 1\}$, so there are only finitely many solutions.

The next example, though similar, has a completely different behaviour.

Example 3.3.4. Consider $\kappa = \mathbb{Q}$, where $d \in \mathbb{N}$ is square-free. $S = \{\text{archimedeans}\}$. Let $D = \{[\pm\sqrt{d} : 1]\}$. The equation of D is $X^2 - dY^2 = 0$, so it is $\mathbb{Q}$-defined. A point $[x : y] \in \mathbb{P}^1 \setminus D$ (with $\gcd(x, y) = 1$) is integral if and only if $x^2 - dy^2 \in \mathcal{O}_S^* = \mathbb{Z}^* = \{\pm 1\}$. It follows from the discussion about the Pell equation that they are infinitely many.

Example 3.3.5. Let $X = \mathbb{P}^1$, lκ a number field, S any finite set of places containing the archimedean ones, $D = \{[1 : 0], [0 : 1], [1 : 1]\}$. Then there are only finitely many S-integral points on $\mathbb{P}^1 \setminus D$. In fact if $[X_0 : X_1]$ is S-integral on $\mathbb{P}^1 \setminus D$ if and only if

$$X_0, X_1, X_0 - X_1 \in \mathcal{O}_S^*$$

there are only finitely many possibilities by S-unit equation:

Theorem 3.3.6 (S-unit equation)**.** *Let κ be a number field, S a finite set of places containing the archimedean ones. The set of the solutions to the diophantine equation*

$$u + v = 1, \text{ where } u, v \in \mathcal{O}_S^*$$

is finite.

3.4 S-integral points for embedded varieties

Let $X \subset \mathbb{P}^n$ be a smooth irreducible variety defined over a number field κ. Let S be a finite set of valuations containing the archimedean ones. Let D be a κ-defined divisor, we investigate the relation between S-integral points on $\mathbb{P}^n \setminus D$ and S-integral points on $X \setminus (X \cap D)$ An inclusion is trivial:

$$\{S\text{-integral points on } X \setminus (X \cap D)\} \supseteq \{S\text{-integral points on } \mathbb{P}^n \setminus (D)\} \cap X$$

in fact if a point on X does not coincide with any point of $D \mod v$ for any $v \notin S$, then a fortiori it does not coincide with a point on $X \cap D$. The converse is not true, as shown by this example.

Example 3.4.1. Let $\kappa = \mathbb{Q}$, $S = \{\infty\}$, let $L : 2X_1 + 2X_2 = X_0$ and $D : X_0 = 0$. By proposition 3.2.11 the set of S-integral points on $L \setminus D$ is given by the solutions in integers of the equation $2x + 2y = 1$ which is plainly the empty set. Nevertheless there are infinitely many S-integral points on $X \setminus [1 : -1 : 0]$, this is true in general (see 3.5.3). For example there is the point $[2 : -1 : 2]$.

Note that in the previous example the lines L and D coincide mod 2. This is in fact the cause for which the two notions of integrality are not equivalent: if X mod v has no component contained in D mod v for any $v \notin S$, then

$$\{S\text{-integral points on } X \setminus (X \cap D)\} = \{S\text{-integral points on } \mathbb{P}^n \setminus D\} \cap X$$

3.5 Integral points on linear subvarieties of the projective space

In this section we study the density of integral Spoints on varieties of the type $V \setminus W$, where $V \subseteq \mathbb{P}^n$ is a linear subspace and $W \subseteq V$ is a codimension-1 linear subspace of V. The easiest case is $\mathbb{P}^1 \setminus \{P\}$. The proof of the next proposition follows that of [Beu, Thm 2.1].

Proposition 3.5.1. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $P \in \mathbb{P}^1(\kappa)$ be a κ-defined point. Then there are infinitely many S-integral points on $\mathbb{P}^1 \setminus \{P\}$.*

Proof. Let $P = [a : b]$. Let $X = [x : y]$ be a κ-rational point, then X is S-integral on $\mathbb{P}^1 \setminus \{P\}$ if and only if

$$(ay - bx) \supseteq (a, b)(x, y)$$

Substituting $x = ta, y = 1 + tb$ we have that $ay - bx = a$, and so the condition of S-integrality becomes

$$(ta, 1 + tb)(a, b) \subseteq (a) \iff ta^2, a + tab, tab, b + tb^2 \in a\mathcal{O}_S.$$

So we have to find $t \in \kappa$ such that

1. $t \in a^{-1}\mathcal{O}_S \cap b^{-1}\mathcal{O}_S$
2. $b + tb^2 \in a\mathcal{O}_S$, so $b + tb^2 = am$, for some $m \in \mathcal{O}_S$.

Now $t = \dfrac{am - b}{b^2}$ so $\dfrac{am - b}{b^2} \in a^{-1}\mathcal{O}_S \cap b^{-1}\mathcal{O}_S$. It is possible to find such t and m if and only if $b \in a\mathcal{O}_S + \left(\dfrac{b^2}{a} \cap b\mathcal{O}_S\right)$. In other terms if and only if

$$\begin{aligned} v(b) &\geq \min(v(a), \max(2v(b) - v(a), v(b)) \\ &= \min(v(a), v(b) + \max(v(b) - v(a), 0)) \end{aligned}$$

which is true in both the cases $v(b) \geq v(a)$ or $v(b) \leq v(a)$. This proves the existence of an S-integral point.
To see that they are infinitely many note that if $[x : y]$ is integral on $\mathbb{P}^1 \setminus \{[a : b]\}$, then

$$(x, y)(a, b) \subseteq (ay - bx)$$

If we choose $t \in a^{-1}(x, y) \cap b^{-1}(x, y)$ we have that

$$(x + ta, y + tb)(a, b) \subseteq (x, y)(a, b) \subseteq (ay - bx) = (a(y + tb) - b(x + ta))$$

so $[x + ta : y + tb]$ is also integral. Since we have infinitely many choices for t, the set of S-integral points on $\mathbb{P}^1 \setminus \{[a : b]\}$ is Zariski-dense. □

The previous result can be generalized to any line $L \subset \mathbb{P}^n$ defined over κ and any κ-rational point $P \in L$.

Lemma 3.5.2. *Let κ be a number field, S a finite set of places containing the archimedean ones. Let $\mathbb{P}^n$ be the projective space with homogeneous coordinates $[X_0, ..., X_n]$. Let P be a κ-defined point. Denote $H := \{X_0 = 0\}$. Then the set of S-integral points on $\mathbb{P}^n \setminus H$ which do not coincide with $P \mod v$ for any $v \notin S$ is Zariski-dense.*

Proof. Let $P = [p_0 : ... : p_n]$. Let $Q = [1 : q_1 : ... : q_n]$ be an S-integral point on $\mathbb{P}^3 \setminus H$. Then Q does not coincide with $P \mod v$ if and only if

$$(p_0q_1 - p_1, ..., p_0q_n - p_n) = (p_0, ..., p_n) =: I$$

In other words we want to find $q_1, ..., q_n \in \mathcal{O}_S$ such that for every prime $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_S)$ we have that

$$v_\mathfrak{p}(p_0q_1 - p_1, ..., p_0q_n - p_n) = v_\mathfrak{p}(I).$$

Let $\mathfrak{p} \mid I$, let $e := v_\mathfrak{p}(I)$. If $v_\mathfrak{p}(p_0) \geq e + 1$ then there exists $i \in \{1, ..., n\}$ such that $v_\mathfrak{p}(p_i) = e$ and so $v_\mathfrak{p}(p_0q_i - p_i) = e$ and so $v_\mathfrak{p}(p_0q_1 - p_1, ..., p_0q_n - p_n) = e$: in this case we do not need to impose conditions on the q_j.
Suppose conversely that $v_\mathfrak{p}(p_0) = e$, we impose that

$$q_1 \equiv 1 + \frac{p_1}{p_0} \mod \mathfrak{p}$$

By Chinese Remainder Theorem it is possible to find $q_1 \in \mathcal{O}_S$ which satisfies all these congruences.
Let $\mathfrak{q} \mid (p_0q_1 - p_1)$ be a prime such that $\mathfrak{q} \nmid I$. If $v_\mathfrak{q}(p_0) > 0$ then there exists p_i such that $\mathfrak{q} \nmid p_i$, so $v_\mathfrak{q}(p_0q_i - p_i) = 0$ and so $v_\mathfrak{q}(p_0q_1 - p_1, ..., p_0q_n - p_n) = 0$. If $\mathfrak{q} \nmid p_0$ then we impose that

$$q_2 \equiv 1 + \frac{p_2}{p_0} \mod \mathfrak{q}$$

By Chinese Remainder Theorem it is possible to find q_2 satisfying these congruences. It follows that

$$(p_0q_1 - p_1, p_0q_2 - p_2) = (p_0, ..., p_n)$$

and so a fortiori for every choice of $q_3, ..., q_n$. Since we have infinitely many choices for q_1 and infinitely many choices for q_2 fixed q_1, the set of $(q_1, ..., q_n) \in \mathcal{O}_S^n$ satisfying all the conditions is Zariski-dense. □

Proposition 3.5.3. *Let κ be a number field, let S be a finite set of valuations of κ containing the archimedean ones. Let $L \subset \mathbb{P}^n$ be a straight line defined over κ. Let $P \in L$. Then there are infinitely many S-integral points on $L \setminus \{P\}$*

Proof. We proceed by induction on n. The case $n = 1$ has been already proved. Suppose that $n > 1$. We can assume without loss of generality that L is not contained in $H : X_0 = 0$. Let Q be an S-integral point on $\mathbb{P}^n \setminus H$, not belonging to L and not coinciding with P mod v for any $v \notin S$: we have proved its existence in the previous lemma. Consider the projection from Q to H: it restricts to an isomorphism

$$\pi : L \to L'$$

Let $L' := \pi(L)$, $P' := \pi(P)$. By inductive hypothesis there is a Zariski-dense set of S-integral points on $L' \setminus \{P'\}$ Let R' be an S-integral point on $L' \setminus \{P'\}$. Then $R := \pi^{-1}(R')$ is S-integral on $L \setminus \{P\}$. We distinguish two cases:

1. If $Q \bmod v \notin L \bmod v$ then $R \bmod v \neq P \bmod v$ otherwise

   $$P' \bmod v = L_{Q \bmod v, P \bmod v} \cap H \bmod v = L_{Q \bmod v, R' \bmod v} \cap H \bmod v = R' \bmod v$$

   which contradicts what we are assuming.

2. If $Q \bmod v \in L \bmod v$ then

   $$R \bmod v = L_{Q \bmod v, R' \bmod v} \cap L \bmod v = Q \bmod v$$

   since Q does not coincide with $P \bmod v$ then the same is true for R.

Since by inductive hypothesis there are infinitely many S-integral points on $H \setminus L$, the assertion follows. □

Remark 3.5.4. Note that in the proof, if we assume that Q coincides with no point of L mod v for any $v \notin S$, the projection π restricts to a bijection between S-integral points on $L \setminus \{P\}$ and S-integral points on $L' \setminus \{P'\}$.
If it is not the case, an S-integral point on $L \setminus \{P\}$ can be sent to a point not S-integral on $L' \setminus \{P'\}$. Suppose that $P \bmod v \in L \bmod v$ and that it does not coincide with a certain point R, which is S-integral on $L \setminus \{P\}$, then $R' = \pi(R)$ is not S-integral on $L' \setminus \{P'\}$. In fact

$$P' \bmod v = L_{R \bmod v, Q \bmod v} \cap H \bmod v = L_{R \bmod v, Q \bmod v} \cap H \bmod v = R' \bmod v$$

The method of the previous propositions gives an effective way to compute integral points on lines.

Example 3.5.5. Let $\kappa = \mathbb{Q}$, $S = \infty$. Let $L \subset \mathbb{P}^2$ be a line defined by the equation

$$L : 15X + 10Y + 6Z = 0.$$

Compute all the S-integral points on $L \setminus \{P\}$, where

$$P := [2 : -3 : 0]$$

In this case $P' = P = [2 : -3 : 0]$. Note that there exists $Q = [1 : -1 : 1]$ an S-integral point on $\mathbb{P}^2 \setminus D$. The integral points on $\mathbb{P}^1 \setminus \{[2 : -3]\}$ correspond to the solutions of the Bezout's relation

$$3x + 2y = 1$$

The set of all the solutions is $\{(1 + 2n, -1 - 3n) : \ n \in \mathbb{Z}\}$. Intersecting the line through $[1 : -1 : 1]$ and $[1 + 2n : -1 - 3n : 0]$ with L we get the set of points

$$\{[16 + 22n : -16 - 33n : 5]\}$$

Example 3.5.6. Let $\kappa = \mathbb{Q}$, $S = \infty$. Let L be the line

$$5X + 10Y + 2Z = 0$$

and $P = [2 : -1 : 0]$ the point we are removing. Note that the diophantine equations

$$(5x + 10y + 2z)z = \pm 1$$

have no solution in $\mathbb{Z}$, so the set of S-integral points on $\mathbb{P}^2 \setminus D$, where

$$D := \{(5X + 10Y + 2Z)Z = 0\}$$

is empty. The set of S-integral points on $\mathbb{P}^1 \setminus \{[2 : -1]\}$ correspond to the solutions of the Bezout's relation

$$x + 2y = 1$$

and so it is the set $\{[-1 + 2n : 1 - n] : \ n \in \mathbb{Z}\}$.
Consider the point $P = [0 : 0 : -1]$. Then, using the projection from P of the proof of the theorem, we get an infinite family of integral points on $L \setminus \{P\}$.

$$\{[-2 + 4n : 2 - 2n : 5] : \ n \in \mathbb{Z}\}$$

If we project from the point $P' := [1 : 0 : -1]$ we find the family

$$\{[2 + 6n : 3 - 3n : 5] : \ n \in \mathbb{Z}\}$$

Note that the two families are disjoint since the linear system

$$\begin{cases} 4n - 2 & = 6m + 2 \\ -2n + 2 & = -3m + 3 \end{cases}$$

has no solution.

Proposition 3.5.3 is actually a particular case of a more general result.

Theorem 3.5.7. *Let κ be a number field, S a finite set of valuations of κ containing the archimedean ones. Let $V \subseteq \mathbb{P}^n$ be an m-dimensional projective linear subspace defined over κ. Let $W \subset V$ be an $(m-1)$-dimensional projective linear subspace defined over κ. Then the set of S-integral points on $V \setminus W$ is Zariski-dense.*

Proof. We proceed by induction on m. The case $m = 1$ is precisely the proposition 3.5.3. Suppose now $m > 1$. Let $X \subset W$ be a codimension 1 linear subspace defined over κ. Consider the set

$$\{W' \leq V \ : W' \supseteq X, \ \dim(W') = m - 1\}$$

It is parametrized by a line in $\mathbb{P}(\bigwedge^{n-m+1}\bar{\mathbb{Q}}^{n+1})$. So by theorem 3.5.3 there are infinitely many W' defined over κ, passing through X and not coinciding with $W \mod v$ for any $v \notin S$. By inductive hypothesis there is a Zariski-dense set of S-integral points on $W' \setminus X = W' \setminus (W' \cap W)$. Since W' does not coincide with $W \mod v$ for any $v \notin S$, they are also S-integral on $V \setminus W$. □

Corollary 3.5.8. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $H \subseteq \mathbb{P}^n$ be an hyperplane defined over κ. Then set of S-integral points on $\mathbb{P}^n \setminus H$ is Zariski-dense.*

Remark 3.5.9. Note that the corollary is trivial if we assume that $\mathcal{O}_S$ is a UFD. In fact if

$$a_0X_0 + ... + a_nX_n = 0$$

is the equation of H, where $\gcd(a_0, ..., a_n) = 1$ in $\mathcal{O}_S$, then obviously there exist $\xi_0, ..., \xi_n \in \mathcal{O}_S$ such that

$$a_0\xi_0 + ... + a_n\xi_n = 1$$

So $[\xi_0 : ... : \xi_n]$ is an S-integral point.

Chapter 4

Constructing integral points on surfaces

In this chapter we shall see the methods to prove the existence of a Zariski-dense set of S-integral points on certain surfaces developed by Beukers in [Beu]. The main ideas are the following ones:

1. Find a sufficiently large number of automorphisms preserving integral points.
2. Find infinitely many curves contained in the surface for which it is known the existence of infinitely many integral points.

4.1 Integral points on lines and conics

This section contains technical results needed later.

Proposition 4.1.1. *Let κ be a number field, S a finite set of valuations of κ containing the archimedean ones. Let $\mathcal{C} \subseteq \mathbb{P}^2$ be a geometrically irreducible conic defined over κ. Let $P \in \mathcal{C}$ be a κ-rational point. Suppose that $\mathcal{C}$ has good reduction outside S, i.e. $\mathcal{C}$ is irreducible for every $v \notin s$. Then there are infinitely many S-integral points on $\mathcal{C} \setminus \{P\}$.*

Proof. Let L_0 be the tangent line to $\mathcal{C}$ in P. Consider the pencil $\mathcal{P} \subseteq \mathbb{P}^{2*}$ of all the straight lines through P. By proposition 3.5.3 there are infinitely many lines L S-integral on $\mathcal{P} \setminus L_0$, so they do not coincide with $L_0 \mod v$ for any $v \notin S$. Each of these L intersects the conic in P and in another point Q. This point is integral on $\mathcal{C} \setminus P$: In fact it is the other point of intersection of $L \mod v$ with $\mathcal{C} \mod v$. □

Remark 4.1.2. Note that all the S-integral points arise in this way: if Q is S-integral on $\mathcal{C} \setminus P$ then the line through P and Q does not coincide with the tangent mod v, for any $v \notin S$.

Example 4.1.3. Consider the parabola given by the equation

$$x + y = (x - y)^2.$$

We find all the solutions in $\mathbb{Z}$ using the method of the previous corollary. Using projective coordinates X, Y, Z the point is $P = [1 : 1 : 0]$, the tangent in P is $Z = 0$. The integral lines on $\mathcal{P} \setminus \{Z = 0\}$ are

$$X - Y = nZ, \text{where } n \in \mathbb{Z}$$

so all integral points are solutions of the systems

$$\begin{cases} x+y &= (x-y)^2 \\ x-y &= n \end{cases}$$

So $(x,y) = \left(\frac{n(n+1)}{2}, \frac{n(n-1)}{2}\right)$

Proposition 4.1.4. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $\mathcal{C}$ be a singular cuspidal cubic defined over κ with good reduction outside S, i.e. $\mathcal{C} \bmod v$ is a geometrically irreducible cuspidal cubic $\bmod v$ for every $v \notin S$. Then there are infinitely many S-integral points on $\mathcal{C} \setminus \{P\}$.*

Proof. Similarly to the proof of corollary 4.1.1 we choose the cuspidal tangent L_0 in P, we consider the pencil $\mathcal{P}$ of all the lines through P. We have that the integral points on $\mathcal{C} \setminus \{P\}$ correspond to integral lines on $\mathcal{P} \setminus \{L_0\}$. □

Example 4.1.5. We find all the solutions in $\mathbb{Z}$ of the diophantine equation

$$y = (x+y)^3$$

Note that it has a cusp $P = [1 : -1 : 0]$, which is the intersection of $\mathcal{C}$ with the line at infinity $Z = 0$, which is of course the tangent L_0. The lines through P are that of the form

$$aX + aY + cZ = 0.$$

The integral lines on $\mathcal{P} \setminus L_0$ are those with $a \in \{\pm 1\}$, $c \in \mathbb{Z}$, so in the affine part that of the form $x + y = n$. So all the integral points are solutions of the systems

$$\begin{cases} y = (x+y)^3 \\ x+y = n \end{cases}$$

$(x,y) = \left(n - n^3, n^3\right)$.

As we have seen (proposition 3.5.3), for every κ-defined straight line, for every κ-defined point $P \in L$, the set of S-integral points on $L \setminus P$ is Zariski-dense.
We now consider the case when we remove a κ-defined divisor on L given by two points. The next examples show that there can be different behaviours

Example 4.1.6. Let $\kappa = \mathbb{Q}$, $L = \mathbb{P}^1$, $S = \{\infty\}$.
$\{P_1, P_2\} = \{[a : \pm bi]\}$, where $a, b \in \mathbb{Z}$ $\gcd(a,b) = 1$: in this case there are only finitely many S-integral points on $\mathbb{P}^1 \setminus \{P_1, P_2\}$, corresponding to the solutions in integers of

$$a^2y^2 + b^2x^2 = 1$$

Example 4.1.7. Let $\kappa = \mathbb{Q}$, $L : \mathbb{P}^1$, $S = \{\infty\}$, $D = \{[\pm\sqrt{d} : 1]\}$. Then the set of S-integral points on $\mathbb{P}^1 \setminus D$ corresponds to the solutions of the equations

$$x^2 - dy^2 = \pm 1$$

which are infinitely many.

The solutions of a Pell Equation can be interpreted also as integral points on a projective conic minus two points.

Example 4.1.8. Let $\kappa = \mathbb{Q}$, Let $\mathcal{C} : X^2 - dY^2 = Z^2$, where $d \in \mathbb{Z}$ is squarefree,

$$D = \{[\pm\sqrt{d} : 1 : 0]\} = \mathcal{C} \cap \{Z = 0\}$$

Since $\mathcal{C}$ has no component coinciding with $\{Z = 0\} \bmod v$ for every $v \notin S$, the set of S-integral points corresponds also in this case to solutions in $\mathbb{Z}$ of the diophantine equations

$$x^2 - dy^2 = \pm 1$$

Recall that we remarked (2.2.3) that the existence of infinitely many solutions of the Pell equation was geometrically interpreted as existence of infinitely automorphisms of the hyperbola fixing the set of S-integral points. The idea for the general case is the same: constructing automorphisms fixing integral points. We start from a technical result.

Lemma 4.1.9. *Let κ be a number field, S a finite set of valuations of κ containing the archimedean ones. Let $A, B, C \in \mathbb{P}^2$ such that $A + B + C$ is a 0-cycle defined over κ. Suppose that they are not contained in the same straight line. Denote $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ the corresponding ideals generated by their coordinates. Let $I = \det(A|B|C)\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{c}^{-1}$ (I is independent from the choice of the homogeneous coordinates).*

(1) Suppose that $A, B, C \in \mathbb{P}^2(\kappa)$. Let

$$U := \{x \in \mathcal{O}_S^* : x \equiv 1 \mod I\}$$

then for every choice of $\alpha, \beta, \gamma \in U$, there exists $T \in GL_3(\mathcal{O}_S)$ such that T has eigenvectors A, B, C (thinking them as column vectors), and α, β, γ are the corresponding eigenvalues:

$$T \cdot A = \alpha A, \ T \cdot B = \beta B, \ T \cdot C = \gamma C$$

(2) Suppose that $A \in \mathbb{P}^2(\kappa)$, B and C are conjugate points defined over a quadratic extension κ'/κ of κ, let S' be the set of valuations of κ' extending those of S, let

$$U' = \{x \in \mathcal{O}_{S'}^* : x \equiv 1 \mod (I)\},$$

then for every $\alpha \in U, \beta \in U'$ we can find $T \in GL_3(\mathcal{O}_S)$ such that

$$T \cdot A = \alpha A, \ T \cdot B = \beta B, \ T \cdot C = \bar{\beta} \cdot C$$

(3) Suppose that κ''/κ is a cubic extension and A, B, C are conjugate points defined over κ'', let S'' be the set of valuations of κ'' extending those of S, let

$$U'' = \{x \in \mathcal{O}_S''^* : x \equiv 1 \mod (I)\}$$

Then for every $\alpha \in U''$ we can find $T \in GL_3(\mathcal{O}_S)$ such that

$$T \cdot A = \alpha A \ T \cdot B = \bar{\alpha} B, \ T \cdot C = \bar{\bar{\alpha}} \cdot C$$

Proof.

(1) Consider

$$M := (A|B|C),\ L = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$$

Then $T = MLM^{-1}$ satisfies the request. One has to check that for every choice of $\alpha, \beta, \gamma \in U$ all the entries of T are in $\mathcal{O}_S$, i.e. that:

$$M \cdot L \cdot \mathrm{adj}(M) \equiv 0 \mod \det(M),$$

or equivalently that they are in $\mathcal{O}_v$ for every $v \notin S$. We can assume that A, B, C have coprime coordinates in $\mathcal{O}_v$ (it is a UFD) , case $I\mathcal{O}_v = \det(M)\mathcal{O}_v$, then

$$M \cdot L \cdot \mathrm{adj}(M) \equiv MI_3\mathrm{adj}(M) \equiv 0 \mod \det(A|B|C).$$

Then T has entries in $\mathcal{O}_v$ for every $v \notin S$, then it has entries in $\mathcal{O}_S$.

(2), (3) Similar to (1), consider $L = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \bar{\beta} \end{pmatrix}$ for (2) and $L = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \bar{\alpha} & 0 \\ 0 & 0 & \bar{\bar{\alpha}} \end{pmatrix}$ for (3).

□

Theorem 4.1.10. *Let κ be a number field, S a finite set of valuations of κ containing the archimedean ones. Let $L \subseteq \mathbb{P}^2$ be a κ-defined projective line. Let $A, B \in \mathbb{P}^2(\bar{\kappa})$ such that $D = \{A, B\}$ is a κ-defined divisor.*

(1) Suppose that $A, B \in L(\kappa)$. If $|\mathcal{O}_S^*| = \infty$ then the set of S-integral points on $L \setminus \{A, B\}$ is either empty or infinite.

(2) Suppose that $|\mathcal{O}_S^*| < \infty$ and one of the following hypothesis holds:

- *$A, B \in L(\kappa)$;*
- *$A, B \in L(\kappa')$, where κ'/κ is a quadratic extension such that no archimedean valuation of κ splits in κ'.*

Then there are only finitely many S-integral points on $\mathcal{C} \setminus \{A, B\}$.

(3) Suppose that $A, B \in \mathbb{P}^2(\kappa')$ where κ'/κ is a quadratic extension such that at least one valuation of κ splits in κ'. Then the set of S-integral points on $L \setminus \{A, B\}$ is either empty or infinite.

Proof.

(1) Suppose that $|\mathcal{O}_S^*| = \infty$. Let $x \in L \setminus \{A, B\}$ be an S-integral point. Then, for every $v \notin S$, choosing coprime coordinates for A and for x

$$\mathrm{rk}((A|x) \mod v) = 2$$

Let $C \in \mathbb{P}^2 \setminus L$ be a κ-rational point. Choose $\alpha, \beta, \gamma \in U$ as in 4.1.9 and $T \in GL_3(\mathcal{O}_S)$ such that

$$T(A) = \alpha A, \quad T(B) = \beta B, \quad T(C) = \gamma C$$

Then T fixes the line L, in fact the equation for L is

$$\det(A|B|x) = 0$$

and $\det(A|B|Tx) = \dfrac{\det(T)\det(A|B|x)}{\alpha\beta}$. Further T preserves integral points on $L \setminus \{A, B\}$. The fact that x is S-integral means that for every $v \notin s$ if we choose coprime homogeneous coordinates for A and for x

$$\mathrm{rk}((A|x) \mod v) = 2$$

Note that

$$\begin{aligned} \mathrm{rk}((A|Tx) \mod v) &= \mathrm{rk}((\alpha A|Tx) \mod v) \\ &= \mathrm{rk}((TA|Tx) \mod v) \\ &= \mathrm{rk}(T \cdot (A|x) \mod v) \\ &= \mathrm{rk}((A|x) \mod v) \text{ since } \det(T) \in \mathcal{O}_S^* \end{aligned} \tag{4.1}$$

So Tx is an S-integral point. We want to prove that they are infinitely many. Note that the function

$$f(x) := \frac{\det(A|C|x)}{\det(B|C|x)}$$

is such that $f(Tx) = \dfrac{\beta}{\alpha} f(x)$ So in particular

$$f(Tx) \neq f(x) \Rightarrow Tx \neq x$$

Since we can choose infinitely many different values for $\dfrac{\beta}{\alpha}$ it follows that the set of S-integral points on $L \setminus \{P\}$ is infinite.

(2) We prove only the case when $A, B \in L(\kappa)$ and $|\mathcal{O}_S^*| < \infty$. Suppose to have chosen C an S-integral point on $\mathbb{P}^2 \setminus L$ (it exists by theorem 3.5.7). Then it follows that for an S-integral point x on $L \setminus \{P\}$ we have that.

$$\det(A|C|x) = \mathfrak{a}\mathfrak{c}\mathfrak{x}, \quad \det(B|C|x) = \mathfrak{b}\mathfrak{c}\mathfrak{x}$$

where $\mathfrak{a}, \mathfrak{b}, \mathfrak{x}$ are the ideals respectively generated by the coordinates of A, B, x. It follows that

$$(f(x)) = \frac{\mathfrak{a}}{\mathfrak{b}}$$

Since $|\mathcal{O}_S^*| < \infty$ there are only finitely many choices for $f(x)$, so all the S-integral points are contained in a finite number of lines

$$\det(A|C|x) = a \det(B|C|x), \text{ where } (a) = \frac{\mathfrak{a}}{\mathfrak{b}}$$

so they are finitely many.

(3) We choose $\alpha \in U'$ as in lemma 4.1.9 and $T \in GL_3(\mathcal{O}_S)$ such that

$$T(A) = \alpha A, \;\; T(B) = \bar{\alpha} B, \;\; T(C) = \gamma C$$

Given an S-integral point x, we can find infinitely many S-integral points considering $T(x)$, since there are infinitely many choices for $\frac{\bar{\alpha}}{\alpha}$. □

Remark 4.1.11. The previous proof can be generalized to a line $L \subset \mathbb{P}^n$ for $n \in \mathbb{N}^+$. In fact we can choose auxiliary points C_1, C_{n-1} such that C_i does not reduce to $Span(C_{i-1}, ..., C_1, A, B)$ mod v for any $v \notin S$ and consider the fibration

$$f(x) := \frac{\det(A|C_1|...|C_{n-1}|x)}{\det(B|C_1|...|C_{n-1}|x)}$$

The proof in the cases of a geometrically irreducible conic is very similar.

Theorem 4.1.12. *Let κ be a number field, S a finite set of valuations of κ containing the archimedean ones. Let $\mathcal{C} \subset \mathbb{P}^2$ be a κ-defined projective and geometrically irreducible conic. Let $A, B \in \mathbb{P}^2(\bar{\kappa})$ such that $D = \{A, B\}$ is a κ-defined divisor of $\mathcal{C}$.*

(1) Suppose that $A, B \in \mathcal{C}(\kappa)$ and that $|\mathcal{O}_S^*| = \infty$, then the set of S-integral points on $\mathcal{C} \setminus \{A, B\}$ is either empty or infinite.

(2) Suppose that $|\mathcal{O}_S^*| < \infty$ and that one of the following is true

- *A and B are defined over κ;*
- *A and B are defined over a quadratic extension κ'/κ such that no archimedean valuation of κ splits in κ'.*

Then there are only finitely many S-integral points on $\mathcal{C} \setminus \{A, B\}$.

(3) Suppose that A, B are defined over a quadratic extension κ'/κ such that there is at least one archimedean valuation of κ which splits in κ'. Then there are infinitely many S-integral points on $L \setminus \{A, B\}$.

Proof.

(1) Let C be the intersection point of the two tangents to $\mathcal{C}$ in A and B. Note that $\mathcal{C}$ is a member of the pencil

$$a \det(A|C|x) \det(B|C|x) + b \det(A|B|x)^2 = 0, \;\; [a : b] \in \mathbb{P}^1(\bar{\kappa})$$

in fact $\mathcal{C}$ belong to the pencil of all conics passing through A and B and having two specified lines intersecting it with multiplicity 2 in those points, which is in fact the pencil defined above. Choose $\alpha, \beta\, \gamma \in U$, where U is the set defined in lemma 4.1.9. Suppose that

$$\gamma^2 = \alpha\beta$$

We construct the automorphism T as in lemma 4.1.9 such that

$$T(A) = \alpha A, \;\; T(B) = \beta B, \;\; T(C) = \gamma C$$

Then T fixes any conic of the pencil, in particular $\mathcal{C}$ and preserves integral points. The function

$$f(x) := \frac{\det(A|C|x)\det(B|C|x)}{\det(A|B|x)^2}$$

is such that

$$f(Tx) = \frac{\det(A|P|Tx)}{\det(B|P|Tx)} = \frac{\beta}{\alpha} f(x)$$

Since there are infinitely many choices for $\frac{\beta}{\alpha}$, we are able to construct infinitely many S-integral points.

(2) We consider the case when A, B are defined over κ. We want to show that there are only finitely many S-integral points. This part is trickier than the case of the line, since we cannot assume that C is S-integral. Write

$$x = aA + bB + cC$$

The fact that x is S-integral means that it does not reduce to A or B mod v for any $v \notin S$, which is equivalent to the fact that:

$$|a\mathfrak{a}|_v \leq \max(|b\mathfrak{b}|_v, |c\mathfrak{c}|_v)$$
$$|b\mathfrak{b}|_v \leq \max(|a\mathfrak{a}|_v, |c\mathfrak{c}|_v)$$

This implies that for every $v \notin S$

$$|c\mathfrak{c}|_v \leq \max(|b\mathfrak{b}|_v, |a\mathfrak{a}|_v)$$

$\mathcal{C}$ has an equation of the form

$$\det(A|C|x)\det(B|C|x) = d\det(A|B|x)^2$$

which implies $d = \frac{ab}{c^2}$.

$|c\mathfrak{c}|_v^2 \geq \max(|a|_v^2|\mathfrak{a}|_v^2, |b|_v^2|\mathfrak{b}|_v^2)$

$\frac{|ab|_v|\mathfrak{c}|_v}{|d|_v} \geq \max(|a|_v^2|\mathfrak{a}|_v^2, |b|_v^2|\mathfrak{b}|_v^2)$

$\frac{|\mathfrak{c}|_v^2}{|d|_v} \geq \max\left(\left|\frac{b}{a}\right|_v |\mathfrak{b}|_v, \left|\frac{a}{b}\right|_v |\mathfrak{a}|_v\right)$

So we have a system of inequalities:

$$\begin{cases} \left|\frac{b}{a}\right|_v |\mathfrak{b}|_v^2 \leq \frac{|\mathfrak{c}|_v^2}{|d|_v} \\ \left|\frac{a}{b}\right|_v |\mathfrak{a}|_v^2 \leq \frac{|\mathfrak{c}|_v^2}{|d|_v} \end{cases} \iff \frac{|d|_v|\mathfrak{a}|_v}{|\mathfrak{c}|_v^2} \leq \left|\frac{b}{a}\right|_v \leq \frac{|\mathfrak{c}|_v^2}{|d|_v|\mathfrak{b}|_v}$$

this implies that $(f(x)) = \left(\frac{b}{a}\right)$ belongs to a finite set of ideals, and since $|\mathcal{O}_S^*| < \infty$ there are only finitely many values for $f(x)$, and so only finitely many integral points.

(3) Very similar to (1).

□

Remark 4.1.13. Also in this case it is possible to extend the previous theorem to a κ-defined conic $\mathcal{C}$ contained in a κ-defined plane $H \subset \mathbb{P}^n$, considering auxiliary points $C_1, ..., C_{n-2}$ and a fibration

$$f(x) = \frac{\det(C_1|...|C_{n-2}|A|C|x)\det(C_1|...|C_{n-2}|B|C|x)}{\det(C_1|...|C_{n-2}|A|B|x)^2}$$

Example 4.1.14. Consider $\mathcal{C} : X^2 - dY^2 = mZ^2$, $\kappa = \mathbb{Q}$, $S = \{\infty\}$, $\{A, B\} = \{[\pm\sqrt{d} : 1 : 0]\}$. In this case $\ell = \mathbb{Q}(\sqrt{d})$. This is the classical Pell-type equation. We follow the way of PART 1 to find the automorphisms T fixing integral points. Consider $\alpha = +b\sqrt{d} \in \mathcal{O}_{S'}^* = \mathcal{O}_\ell^*$, such that $a^2 - db^2 = 1$, so $\beta = a - b\sqrt{d}$ and $\gamma = 1$. Consider $T \in GL_3(\mathbb{Z})$ the matrix with eigenvectors $\begin{pmatrix} 1 \\ \pm\sqrt{d} \\ 0 \end{pmatrix}$ and corresponding eigenvalues α and β. It is

$$\begin{pmatrix} a & bd & 0 \\ b & a & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which acts on the affine part as the matrix $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$ which is an element of the orthogonal group over $\mathbb{Z}$ of the quadratic form $x^2 - dy^2$.

Example 4.1.15. Consider the hyperbola $x^2 - 2xy - y^2 + x + y = 0$. It has two conjugates points at infinity, namely $\{A, B\} = \{[1 \pm \sqrt{2} : 1 : 0]\}$, it contains (1,1), then it has infinitely many integral points, let's compute a non-trivial automorphisms T. First we find the point P. The two tangents in A and B (i.e. the two asymptotes) and their point of intersection are:

$$2x - (2 + 2\sqrt{2})y + 1 + \sqrt{2} = 0$$
$$2x - (2 - 2\sqrt{2})y + 1 - \sqrt{2} = 0$$
$$P = \left(\frac{1}{2}, 0\right)$$

We have that $P = \left(0, \frac{1}{2}\right) = [0 : 1 : 2]$ Consider $\alpha = 3 + 2\sqrt{2}, \beta = 3 - 2\sqrt{2}, \gamma = 1$. Then we are searching for T such that:

$$T \cdot \begin{pmatrix} 1+\sqrt{2} & 1-\sqrt{2} & 0 \\ 1 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 7+5\sqrt{2} & 7-5\sqrt{2} & 0 \\ 3+2\sqrt{2} & 3+2\sqrt{2} & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

A solution is $T = \begin{pmatrix} 5 & 2 & -1 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. In affine coordinates it is the affine map

$$T(x, y) = (-1, 0) + (5x + 2y, 2x + y)$$

Corollary 4.1.16. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $\mathcal{C}$ be a nodal singular cubic, which is irreducible* mod *v for every $v \notin S$. Suppose that the node P is κ-defined. Let L_1 and L_2 be the two distinct tangent lines in P.*

(1) If $\mathcal{O}_S^*$ is infinite or the lines are defined over a quadratic extension in which at least one archimedean place of κ splits, then the set of the integral points on $\mathcal{C} \setminus \{P\}$ is either empty or infinite.

(2) If $\mathcal{O}_S^*$ is finite and the lines are either defined over κ or over a non-split quadratic extension, then there are only finitely many S-integral points.

Proof. Consider the pencil of all the lines of $\mathbb{P}^2$ through P. A point $Q \in \mathcal{C} \setminus \{P\}$ is integral if and only if $L := L_{PQ}$ is S-integral on $\mathcal{P} \setminus \{L_1, L_2\}$, where $\mathcal{P}$ is the pencil of lines spanned by L_1 and L_2. So the theorem follows immediately from 4.1.10. □

4.2 Ternary homogeneous equations

In this section we consider the problem of finding solution to the equation

$$F(x, y, z) \in \mathcal{O}_S^* \text{ where } F(X, Y, Z) \text{ is a form with coprime coefficients}$$

Particularly interesting is the case when $\mathcal{O}_S = \mathbb{Z}$: we are searching for solutions of the diophantine equation

$$F(X, Y, Z) = \pm 1.$$

The problem is equivalent to find S-integral points on the algebraic surface $\mathbb{P}^2 \setminus \{F(X, Y, Z) = 0\}$. Note that the canonical class of $\mathbb{P}^2$ is $K = [-3\mathrm{div}(H)]$, where $\mathrm{div}(H)$ is a line divisor. If $\deg(F) \leq 3$ we have that

$$K + D = [(\deg(F) - 3)H]$$

is not a big divisor. So the hypothesis of the Vojta's conjecture are not satisfied and it is possible that the set of S-integral points on $\mathbb{P}^2 \setminus D$ is Zariski-dense. The next theorem considers the case when $\deg(F) = 2$.

Theorem 4.2.1. *Let κ be a number field, S a finite set of valuations of κ containing the archimedean ones. Let $\mathcal{C}$ be a geometrically irreducible conic defined over κ. Let κ_v be the completion with respect to the valuation v.*

(1) Suppose that $\mathcal{C}(\kappa_v) = \emptyset$ for every $v \in S$. Then there exist only finitely many S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$.

(2) If $\kappa \supsetneq \mathbb{Q}$ or $|\mathcal{O}_S^*| = \infty$ then the set of S-integral point on $\mathbb{P}^2 \setminus \mathcal{C}$ is either empty or Zariski dense.

(3) If $\kappa = \mathbb{Q}$, $S = \{\infty\}$ and $\mathcal{C}(\mathbb{R}) \neq \emptyset$, then the set of S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ is either empty or Zariski-dense.

Proof.

(1) The idea is to prove that the height of S-integral points is bounded. Consider now $\mathcal{C} : F(X,Y,Z) = 0$, where F is a ternary quadratic form. There is a well defined continuous function:

$$\begin{array}{ccc} \mathbb{P}^2(\kappa_v) & \to & \mathbb{R}^+ \\ [X:Y:Z] & \mapsto & \dfrac{|F(X,Y,Z)|_v}{\max(|X|_v^2, |Y|_v^2, |Z|_v^2)} \end{array}$$

Since $\mathbb{P}^2(\kappa_v)$ is compact in the v-adic topology, the function has a minimum $m_v > 0$ since $\mathcal{C}(\kappa_v) = \emptyset$. Let $[X:Y:Z]$ be an S-integral point in $\mathbb{P}^2 \setminus \mathcal{C}$ we have by global characterization of integrality that:

$$F(X,Y,Z) = \mathcal{F} \cdot (X,Y,Z)^2$$

where $\mathcal{F}$ denotes the ideal generated by the coefficients of F. So for every $v \notin S$

$$|F(X,Y,Z)|_v = |\mathcal{F}|_v \max(|X|^2, |Y|^2, |Z|^2)$$

Using the product formula for the valuations we have that

$$\begin{aligned} 1 = \prod_v |F(X,Y,Z)|_v &\geq \prod_{v\in S} m_v \prod_{v\notin S} |\mathcal{F}|_v \prod_{v\in S} \max(|X|_v, |Y|_v, |Z|_v)^2 \\ &= \prod_{v\in S} m_v \prod_{v\notin S} |\mathcal{F}|_v H(X,Y,Z)^2 \end{aligned} \tag{4.2}$$

So the height is bounded on integral points, so they are finitely many.

(2) Let P be a fixed S-integral point.

(2.1) If $|\mathcal{O}_S^*| = \infty$, then, for any κ-defined straight line L, passing through P, there are infinitely many S-integral points on $L \setminus (L \cap \mathcal{C})$ by proposition 4.1.10, which are S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$. It follows that the set of S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ is Zariski-dense.

(2.2) If $|\mathcal{O}_S^*| < \infty$, $\kappa \supsetneq \mathbb{Q}$ the assertion follows also in this case if there are infinitely many lines through P intersecting $\mathcal{C}$ in two conjugate points. Note that this is in fact a consequence of Hilbert Irreducibility Theorem.

Theorem 4.2.2 (Hilbert Irreducibility Theorem)**.** *Let κ be a number field, $d \in \mathbb{Z}^+$, $F(X_1,...,X_d,Y) \in \kappa[X_1,...,X_d,Y]$ an irreducible polynomial of degree ≥ 1 in Y. Then for a Zariski-dense set of $(a_1,...,a_d) \in \kappa^d$ the polynomial $F(a_1,...,a_d,Y) \in \kappa[Y]$ is irreducible.*

For a proof see for example [Co]. In our case if we assume that the affine equation of the conic is $f(x,y) \neq 0$ and $P = [0:1:0]$, then the lines through P are exactly those of the form $x = a$.

(3) Suppose that $\mathcal{C}(\mathbb{R}) \neq \emptyset$, let $P \in \mathcal{C}(\mathbb{R})$, let Q be an S-integral point on $\mathbb{P}^2 \setminus \mathcal{C}$. Also in this case the idea is to apply 4.1.10, but we need to prove the existence of infinitely many lines for which the two intersection points are conjugate over a real quadratic

extension of $\mathbb{Q}$.
Denote by X the pencil of lines through P and consider it as a real manifold. Let L_0 be the line through P and Q. There is a neighbourhood of L_0 (in the euclidean real topology) $U \subset X$ such that $L \cap \mathcal{C} \subset \mathbb{P}^2(\mathbb{R})$, for all $L \in U$. The set of $\mathbb{Q}$-rational points of U is euclidean-dense in U, so a fortiori they are infinitely many, i.e. there are infinitely many lines through P, defined over $\mathbb{Q}$ and intersecting $\mathcal{C}$ in real points. From the proof of Hilbert Irreducibility Theorem it can be deduced that actually if $F(X_1, ..., X_d, Y) \in \mathbb{Q}[X_1, ..., X_d, Y]$ is an irreducible polynomial then the set of $(x_1, ..., x_d) \in \mathbb{Q}^d$, such that $F(x_1, .., x_d, Y) \in \mathbb{Q}[Y]$ is irreducible, is dense in the euclidean topology. It follows that there are infinitely many straight lines through P which are $\mathbb{Q}$-defined and which intersect $\mathcal{C}$ in two points conjugate defined over a real quadratic extension of $\mathbb{Q}$.

□

The case when $\mathcal{C}$ is a reducible conic is also simpler.

Proposition 4.2.3. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Suppose that $\mathcal{C} = L_1 + L_2$ is a reducible plane conic defined over κ.*

(1) Suppose that $|\mathcal{O}_S^*| = \infty$ and L_1, L_2 are defined over κ, or that they are defined over a quadratic extension κ'/κ and $|\mathcal{O}_{S'}^*| = \infty$, where S' denotes the set of valuations of κ' extending those of κ. Then the set of S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ is either empty or Zariski-dense.

(2) If $|\mathcal{O}_S^*| < \infty$ and L_1, L_2 are lines which are either κ-defined or defined over a non-split quadratic extension, then the S-integral points are contained in a finite number of lines through $P = L_1 \cap L_2$.

Proof. Let $\mathcal{P}$ be the pencil of all lines through P. It is a line in $\mathbb{P}^{2*}$. If $\exists Q \in \mathbb{P}^2 \setminus \mathcal{C}$ integral then the line $L := P \vee Q$ does not coincide with L_1 or $L_2 \mod v$ for any $v \notin S$. So it is an S-integral point on $\mathcal{P} \setminus \{L_1, L_2\}$

(1) By proposition 4.1.10 there are infinitely many lines through P not coinciding with L_1 and $L_2 \mod v$ for any $v \notin S$. For each of these lines M there are by 3.5.3 infinitely many S-integral points on $M \setminus P$ so S-integral in $\mathbb{P}^2 \setminus L_1 + L_2$.

(2) By proposition 4.1.10 in this case there are finitely many L S-integral on $\mathcal{P} \setminus \{L_1, L_2\}$, and any S-integral point Q must lies on one of these lines.

□

Now we study the solutions of ternary homogeneous equations of degree 3. We start from the case of a geometrically irreducible cubic. The following the theorem is the main of result of the paper [Beu].

Theorem 4.2.4 (Beukers)**.** *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $\mathcal{C}$ be a geometrically irreducible cubic curve defined over κ with a κ-rational flex F. Denote by M the inflectional tangent to the curve in F. Assume that $L \mod v$ is not a component of $\mathcal{C} \mod v$ for any $v \notin S$. Then the set of S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ is Zariski-dense.*

Proof. The idea is to find infinitely many conics which intersect $\mathcal{C}$ in 2 points (with multiplicity 3) having no common component with $\mathcal{C} \mod v$ for every $v \notin S$ and containing at least one integral point. Let

$$T(X, Y, Z) = 0$$

be the equation for $\mathcal{C}$. By an abuse of notation we call $L(X, Y, Z)$ the linear form defining L. By proposition 3.5.3 there are infinitely many S-integral points on $L \setminus \{F\}$, which are S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ since $L \bmod v$ is not a component of $\mathcal{C} \bmod v$ for any $v \notin S$. Let R be one of these points. Fix a κ-defined straight line M throw F, which does not coincide with $L \bmod v$ for any $v \notin S$ (it exists by proposition 3.5.3). Also in this case, by an abuse of notation, we call $M(X, Y, Z)$ the linear form defining M. Let $a = \dfrac{T(R)}{M(R)^3}$, then the cubic curve

$$\mathcal{C}_0 : T(X, Y, Z) - aM(X, Y, Z) = 0$$

contains the line L since $\deg(\mathcal{C}_0) = 3$, but $(L.\mathcal{C}_0)_F \geq 3$ and $(L.\mathcal{C}_0)_R \geq 1$. Then

$$T(X, Y, Z) - aM(X, Y, Z) = L(X, Y, Z)Q(X, Y, Z)$$

where $Q(X, Y, Z)$ is a quadratic form defined over κ. For any $t \in \kappa$ call $M_t = M + tL$, then the cubic

$$\mathcal{C}_t : T(X, Y, Z) - aM_t(X, Y, Z)^3 = 0$$

contains the line L

$$T(X, Y, Z) - aM_t(X, Y, Z)^3 = L \cdot Q_t$$

where $Q_t = Q - 3tM^2 - 3t^2LM - t^3L^2$ is a quadratic form. For all but finitely many $t \in \kappa$ the zero locus of Q_t is a geometrically irreducible conic. Note that

$$Q_t \cap \mathcal{C} = M_t \cap \mathcal{C} =: \{A_t, B_t\}$$

and clearly $(Q_t.\mathcal{C})_{A_t} = (Q_t.\mathcal{C})_{B_t} = 3$. Remember by global characterization of S-integral points that

$$T(R) = \mathfrak{t}\mathfrak{r}^3, \quad M(R) = \mathfrak{m}\mathfrak{r}$$

where $\mathfrak{t}, \mathfrak{m}, \mathfrak{r}$ denote the ideals generated respectively by the coefficients of T, M and the coordinates of R. It follows that

$$(a) = \frac{\mathfrak{t}}{\mathfrak{m}^3}.$$

We can assume without loss of generality that $a = 1$ and so $\mathfrak{t} = \mathfrak{m}^3$. Recall (3.5.1) that, given an S-integral point R on $L \setminus \{F\}$, it is possible to construct infinitely many of them taking $R_s := R + sF$, where $s \in \mathfrak{r} \cdot \mathfrak{f}^{-1}$ ($\mathfrak{f}$ denotes the ideal generated by the coefficients of F). The condition that $R_s \in Q_t$ can be written

$$Q(R_s) - 3tM(R_s)^2 - 3t^2L(R_s)M(R_s) - t^3L(R_s)^2 = 0 \iff t = \frac{Q(R + sF)}{3M(R)^2}$$

In particular the conic Q_t is κ-defined and it contains the S-integral point R_s. Note that if $|\mathcal{O}_S^*| = \infty$ it contains infinitely many S-integral points. It follows that the set of S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ is Zariski-dense. In the remaining part of the proof we suppose that

$|\mathcal{O}_S^*| < \infty$. First we show that for infinitely many $t \in \kappa$, the line M_t intersects the cubic $\mathcal{C}$ in F and two points which are conjugate defined over a quadratic extension of κ. To see this, assume (without loss of generality) that $L : Z = 0$, $M : X = 0$ and $F = [0 : 1 : 0]$. Then the equation of the cubic is

$$X^3 + ZG(X, Y, Z) = 0$$

The κ-defined lines through F are those of equation

$$M_t : X = -tZ,\ t \in \kappa.$$

The intersection $M_t \cap \mathcal{C}$ is given by the system of equations

$$\begin{cases} X & = -tZ \\ -t^3Z^2 + Q(-tZ, Y, Z) & = 0 \end{cases}$$

and for $t \neq 0$ a solution $[X : Y : Z]$ is such that $Z \neq 0$. Since $t^3 + g(t, y, 1) \in \kappa[t, y]$ is an irreducible polynomial, we have that, by Hilbert Irreducibility Theorem, for infinitely many $t \in \kappa$ the solutions of the previous system are not defined over κ.
Note that if $\kappa \supsetneq \mathbb{Q}$ then it implies that the set of S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ is Zariski-dense.
To end the proof we consider the case $\kappa = \mathbb{Q}$. We show that for $s >> 0$ the two points of intersection are defined over $\mathbb{R}$. We have the study the sign of the discriminant of the equation

$$-t^3Z^2 + Q(-tZ, Y, Z) = 0$$

Write explicitly $Q(X, Y, Z) = a_{11}X^2 + a_{22}Y^2 + a_{33}Z^2 + 2a_{12}XY + 2a_{13}XZ + 2a_{23}YZ$. Then

$$-t^3Z^2 + Q(-tZ, Y, Z) = a_{22}Y^2 + (-ta_{12} + a_{23})YZ + (-t^3 + t^2a_{11} - ta_{13} + a_{33})Z^2$$

Note that $a_{22} = Q(0 : 1 : 0)$ and that $t(s) = Q(1 : s : 0)$. $Q(1 : s : 0)$ and $Q(0 : 1 : 0)$ have the same sign for $s >> 0$, so it is clear that the discriminant of the previous equation is positive for $s >> 0$.

□

Example 4.2.5. Consider the case when $\mathcal{C}$ is an elliptic curve defined over $\mathbb{Q}$, $S = \{\infty\}$.

$$Y^2Z = X^3 + pXZ^2 + qZ^3,\ \ p, q \in \mathbb{Q}$$

In this case

$$F = [0 : 1 : 0],\ \ L = Z,\ \ M = X,\ \ T = X^3 + pXZ^2 + qZ^3 - Y^2Z$$

We have that $M_t(X, Y, Z) = X + tZ$ so

$$Q_t(X, Y, Z) = pXZ + qZ^2 - Y^2 - 3tX^2 - 3t^2XZ - t^3Z^2$$

An integral point on $L \setminus \{F\}$ in this case is $[1 : 0 : 0]$, and actually the family of all S-integral points is $\{[1 : n : 0]\}$. For every n the condition to impose on t if we want that Q_t contain $[1 : n : 0]$ is

$$t = \frac{Q(1 : n : 0)}{M(1 : 0 : 0)} = -\frac{n^2}{3}$$

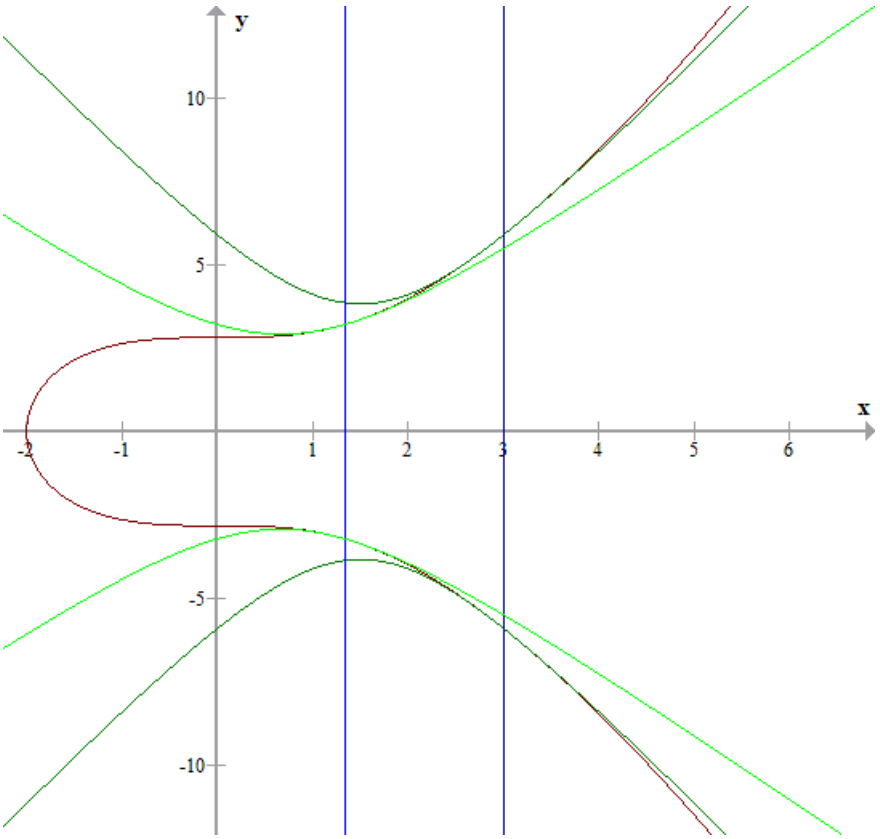

Figure 4.1: An example of the previous construction for the elliptic curve $y^2 = x^3 + 8$

It follows that we get hyperbolas $y^2 = px + q + n^2x^2 - \frac{n^4x}{3} + \frac{n^6x}{27}$
In the figure we picture the case of the curve $y^2 = x^3 + 8$. When $n = 2, 3$ the vertical lines are respectively $x = \frac{4}{3}$ and $x = 3$. The corresponding conics are

$$y^2 = 9x^2 - 27x + 35, \;\; y^2 = 4x^2 - \frac{16}{3}x + \frac{280}{27}$$

Example 4.2.6. Consider the diophantine equation $x^3 + y^3 + z^3 = 1$. Searching solutions in integer corresponds to find integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ where $\mathcal{C}$ is the projective smooth cubic given by $T(X, Y, Z) = X^3 + Y^3 + Z^3$.
We can apply the method of the previous theorem: Consider the $\mathbb{Q}$-rational flex $F = [1 : -1 : 0]$. The tangent line to $\mathcal{C}$ in F is $L(X, Y, Z) = X + Y$. We choose a line

$$M(X, Y, Z) = Z$$

not coinciding with $L \bmod v$ for any $v \notin S$. An integral point on $L \setminus \{F\}$ is $R = [0 : 0 : 1]$. Actually the set of S-integral points on $L \setminus \{F\}$ is $\{[n : -n : 1],\ n \in \mathbb{Z}\}$. We have that

$$Q(X, Y, Z) = X^2 - XY + Y^2$$

$$Q_t(X, Y, Z) = X^2 - XY + Y^2 - 3t(X + Y)^2 - 3t^2Z(X + Y) - t^3Z^2$$

Choosing $R = [0 : 0 : 1]$ we have that

$$t(n) = \frac{Q(n : -n : 1)}{3M(0 : 0 : 1)^2} = n^2.$$

If we consider the system

$$\begin{cases} Z & = -t(X+Y) \\ X^3+Y^3+Z^3 & = 0 \\ X+Y & \neq 0 \end{cases} \iff \begin{cases} Z & = -t(X+Y) \\ X^2-XY+Y^2-t^3(X+Y)^2 & = 0 \end{cases}$$

Substituting $t = n^2$ the last equation is equivalent to

$$(n^6-1)x^2 + (2n^6+1)XY + (n^6-1)Y = 0$$

which has real solutions if and only if $\Delta = 3(4n^6-1) > 0$, so for all $n \neq 0$.

Remark 4.2.7. The problem of finding a Zariski-dense set of solutions in $\mathbb{Z}$ to the previous diophantine equation was very studied by the number theorists in the past. It was solved by D.H. Lehmer in 1956, see [Le], to which the interested reader is referred. He started from a set of known parametric solutions.

$$x_0(t) = 9t^4,\ y_0(t) = -9t^4+3t,\ z_0(t) = -9t^3+1$$

He noted that for any t, (x_0, y_0, z_0) verifies an equation of the second degree:

$$x^2 - xy + y^2 = 21t^6(x+y)^2 - 27t^4(x+y) + 9t^2$$

whose solutions can be obtained from those of the Pell equation

$$a^2 - db^2 = 1$$

where $d = 324t^6 - 3$ is the discriminant of the equation above. For each $t \in \mathbb{Z}$ he considered the family of solutions of such an equation, which allowed him to produce a sequence of curves on the surface containing infinitely many integral points.

Suppose now that the cubic is singular either cuspidal or nodal, then we see that considering a divisor D containing the cubic and the tangents in the singularity (so its degree is 4 or 5 depending on the case the singularity is a node or a cusp) the set of S-integral points on $\mathbb{P}^2 \setminus D$ is Zariski-dense. Note that in this case $K + D$ is big, but it is not normal crossing, so the assumptions of the Vojta's Conjecture are not satisfied.

Theorem 4.2.8. *Let κ be a number field, let S be a finite set of valuations containing the archimedean ones such that $|\mathcal{O}_S^*| = \infty$. Let $\mathcal{C}$ be a cuspidal cubic defined over κ. Let P be the cusp and let L_0 be the principal tangent in P.*

(1) If $|\mathcal{O}_S^*| < \infty$ then the set of S-integral points on $\mathbb{P}^3 \setminus (\mathcal{C} + L_0)$ is not Zariski-dense.

(2) Suppose that $\mathcal{C} \bmod v$ is irreducible for every $v \notin S$. Suppose that there exists another cuspidal cubic $\mathcal{C}'$ irreducible $\bmod v$ for every $v \notin S$ having a cusp in P and tangent L_0. Suppose also that it is distinct from $\mathcal{C} \bmod v$, $\forall v \notin S$ and that $\mathcal{C} \cap \mathcal{C}' = \{P\}$. Then the set of S-integral points on $\mathbb{P}^2 \setminus (\mathcal{C} + L_0)$ is Zariski-dense.

Proof.

(1) Let $F(x) = 0$ be the equation for $\mathcal{C}$. Consider the fibration

$$f(x) := \frac{F(x)}{L_0(x)^3}$$

If x is S-integral on $\mathbb{P}^3 \setminus (\mathcal{C} + L_0)$ then

$$(f(x)) = \frac{\mathcal{F}}{\mathcal{L}_0^3}$$

where $\mathcal{F}, \mathcal{L}_0'$ are the ideal generated respectively by the coefficients of F and L_0. So all the S-integral points are contained in a finite number of cubic curves of the pencil

$$\left\{ (f(x)) = aL(x)^3, \text{ where } (a) = \frac{\mathcal{F}}{\mathcal{L}_0^3} \right\}$$

(2) Consider the pencil $\mathcal{P}$ of the lines through P. Let L be an S-integral points on $\mathcal{P} \setminus \{L_0\}$. We have that $L \cap \mathcal{C} = \{P, Q\}$, $L \cap \mathcal{C}' = \{P, Q'\}$. By corollary 4.1.4 Q' is integral on $\mathcal{C}' \setminus \{P\}$. Then by our hypothesis it is integral on $\mathbb{P}^2 \setminus (\mathcal{C} + L_0)$. Then it is also integral on $L \setminus \{P, Q\}$. By proposition 4.1.10 there are infinitely many S-integral points on $L \setminus \{P, Q\}$ and these points are also integral on $\mathbb{P}^2 \setminus (\mathcal{C} + L_0)$, since by assumptions $L \bmod v$ is not a component of $\mathcal{C} + L_0 \bmod v$, $\forall v \notin S$. Since there are infinitely many integral lines L, the set of S-integral points on $\mathbb{P}^3 \setminus (\mathcal{C} + L_0)$ is Zariski-dense.

□

Remark 4.2.9. There is an easier way to show potential density for this variety. Note that there is an obvious fibration

$$\mathbb{P}^2 \setminus D \to \Lambda \setminus L_0 \cong \mathbb{G}_a$$

where Λ is the pencil of lines through the cusp P. This fibration is a principal $\mathbb{G}_m$-bundle. The existence of another cusp as in the hypothesis ensures that there is a regular section of the bundle and so

$$\mathbb{P}^2 \setminus D \cong \mathbb{G}_m \times \mathbb{G}_a$$

So it is geometrically isomorphic to an homogeneous space. The idea of the proof is the same as in [Co, Thm 5.3.1].

Example 4.2.10. Let $\kappa = \mathbb{Q}[\sqrt{2}]$, $S = \{\infty\}$. Let

$$\mathcal{C} : y^2 + x^3 = 0.$$

In this case $P = (0, 0)$ and $L_0 : y = 0$. This cubic satisfies all the assumptions of the theorem. Since there is the cubic

$$\mathcal{C}' : y^2 + x^3 + y^3 = 0$$

which verifies all the needed hypothesis we conclude that the diophantine equation

$$y(y^2 z + x^3) = (1 + \sqrt{2})^e$$

has a Zariski-dense set of solutions where $x, y, z \in \mathbb{Z}[\sqrt{2}]$ are coprime. $e \in \mathbb{Z}$.

Example 4.2.11. Let $\kappa = \mathbb{Q}$, $S = \{\infty, v_p\}$. Let, as in the previous example

$$\mathcal{C} : y^2 + x^3 = 0,\ \mathcal{C}' : y^2 + x^3 + y^3 = 0$$

it follows that the diophantine equation

$$y(y^2z + x^3) = p^e$$

has a Zariski-dense set of solutions where $x, y, z \in \mathbb{Z}$ are coprime, $e \in \mathbb{Z}$. Note that with this method we can compute all the solutions to this equation: note that they are contained in the family of cubics

$$Y^2Z + X^3 - uY^3 = 0, \text{ where } u \in \mathcal{O}_S^* = \mathbb{Z}[p^{-1}]^*$$

All these cubics verify the hypothesis of $\mathcal{C}'$ in the theorem, so all S-integral points on them are given by intersections with lines L which are S-integral on $\mathcal{P} \setminus L_0$. They lines of equation $X + tY = 0$ where $t \in \mathbb{Z}\left[\frac{1}{p}\right]$.

$$\begin{cases} X & = -tY \\ Y^2Z + X^3 - uY^3 & = 0 \end{cases}$$

It follows that $Z = (t + u)Y$. Then all S-integral points are

$$\left\{ [-t : 1 : t^3 + u] :\ t \in \mathbb{Z}\left[\frac{1}{p}\right], u \in \mathbb{Z}\left[\frac{1}{p}\right]^* \right\}$$

More explicitly

$$\left\{ [-n \cdot p^{2a} : p^{3a} : n^3 \pm p^b] :\ \ n, a, b \in \mathbb{Z},\ \ p \nmid n \right\}$$

Theorem 4.2.12. *Let κ be a number field, let S be a finite set of valuations containing the archimedean ones. Let $\mathcal{C}$ be a geometrically irreducible nodal cubic defined over κ. Let $P \in \mathcal{C}$ be the node, let L_1 and L_2 be the two principal tangents in P.*

(1) Suppose that $|\mathcal{O}_S^*| < \infty$. Then the set of S-integral points on $\mathbb{P}^2 \setminus (\mathcal{C} + L_1 + L_2)$ is not Zariski-dense.

(2) Suppose that $\mathcal{C} \bmod v$ is irreducible for every $v \notin S$. Assume that there is an integral point on $\mathbb{P}^2 \setminus (\mathcal{C} + L_1 + L_2)$ and that there exists another nodal cubic $\mathcal{C}'$ irreducible $\bmod v$ for every $v \notin S$ having a node in P and principal tangents L_1 and L_2. Suppose also that it is distinct from $\mathcal{C} \bmod v$, $\forall v \notin S$ and that $\mathcal{C} \cap \mathcal{C}' = \{P\}$.
Then there are infinitely many integral points on $\mathbb{P}^2 \setminus \mathcal{C} + L_1 + L_2$.

Proof.

(1) Suppose that $F(x) = 0$ is the equation for $\mathcal{C}$.

$$f(x) := \frac{F(x)^2}{L_1(x)^3 L_2(x)^3}$$

If x is an S-integral point we have that

$$(f(x)) = \frac{\mathcal{F}^2}{\mathcal{L}_1^3 \mathcal{L}_2^3}$$

Since $|\mathcal{O}_S^*| < \infty$ there are only finitely many possible values for $f(x)$ and so x is contained in the finite set of sextic curves

$$F(x)^2 = aL_1(x)^3 L_2(x)^3, \quad \text{where } (a) = \frac{\mathcal{F}^2}{\mathcal{L}_1^3 \mathcal{L}_2^3}$$

(2) Consider the pencil $\mathcal{P}$ of lines through P. Let L be an S-integral point on $\mathcal{P} \setminus \{L_1, L_2\}$ (it exists since we are assuming that there exists at least one integral point on $\mathbb{P}^2 \setminus L_1 + L_2$). We have that $L \cap \mathcal{C} = \{P, Q\}$, $L \cap \mathcal{C}' = \{P, Q'\}$. By corollary 4.1.16 Q' is integral on $\mathcal{C}' \setminus \{P\}$. then by hypothesis it is S-integral on $\mathbb{P}^2 \setminus \mathcal{C} + L_1 + L_2$. Then it is also integral on $L \setminus \{P, Q\}$. By theorem 4.1.10 there are infinitely many S-integral points on $L \setminus \{P, Q\}$ and these points are also S-integral on $\mathbb{P}^2 \setminus \mathcal{C} + L_1 + L_2$, since by assumptions L is not a component of $\mathcal{C} + L_1 + L_2$ mod v for any $v \notin S$. Since there are infinitely many integral lines L, the set of Sintegral points is Zariski-dense. □

Remark 4.2.13. Similarly to the case of theorem 4.2.8, it can be proved that this variety is geometrically isomorphic to $\mathbb{G}_m \times \mathbb{G}_m$, which is an homogeneous space for the action of an algebraic group. See for example [Co, Thm 5.3.1].

Consider now the case when the cubic is reducible.

Theorem 4.2.14. *Let κ be a number field, S a finite set of places containing the archimedean ones. Let $L_1 + L_2 + L_3$ be a κ-defined cubic given by three lines.*

(1) If $L_1 \cap L_2 \cap L_3 = \{P\}$ then all the S-integral points on $\mathbb{P}^2 \setminus (L_1 \cup L_2 \cup L_3)$ are contained in finitely many lines through P.

For the next cases we assume that L_1, L_2, L_3 are in general position.

(2) Suppose that $|\mathcal{O}_S^*| < \infty$ and that at least one of the lines is defined over κ. Then the set of S-integral points is not Zariski-dense: more precisely, assuming L_3 is κ-defined, it is possible to find a finite set of conics passing through $A := L_1 \cap L_3$ and $B := L_2 \cap L_3$ tangent to L_1 and L_2 containing all integral points.

(3) Suppose that the three lines are conjugate defined over a cubic extension of κ, then the set of S-integral points on $\mathbb{P}^2 \setminus (L_1 \cup L_2 \cup L_3)$ is either empty or infinite.

(4) Suppose that $|\mathcal{O}_S^*| = \infty$, then the set of S-integral points on $\mathbb{P}^2 \setminus (L_1 \cup L_2 \cup L_3)$ is either empty or infinite.

Proof.

(1) In this case the set of S-integral points is not potentially dense, i.e. is not dense for every enlargement of κ and S. In fact all the S-integral points on $\mathbb{P}^2 \setminus (L_1 \cup L_2 \cup L_3)$ are contained in a a finite set of lines through P. In fact if Q is an S-integral point, then L_{PQ} is a line which is not a component of $(L_1 \cup L_2 \cup L_3)$ mod v for any $v \notin S$. The conclusion follows from the fact that there are only finitely many S-integral points $\mathcal{P} \setminus \{L_1, L_2, L_3\}$, where $\mathcal{P}$ is the pencil of lines through P.

(2) Suppose that x is an integral point on $\mathbb{P}^2 \setminus L_1 + L_2 + L_3$. Let $C := L_1 \cap L_2$. C is a κ-defined point since L_1 and L_2 are either κ-defined or conjugate. The points $A = L_1 \cap L_3$ and $B = L_2 \cap L_3$ are conjugate if L_1 and L_2 are. It follows that the rational function

$$f(x) = \frac{\det(A|C|x)\det(B|C|x)}{\det(A|B|x)^2}$$

is κ-defined. Since x is an integral point we have that, denoting by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{X}$ the ideals generated by the coordinates of A, B, C, x;

$$(\det(A|B|x)) = \mathcal{A}\mathcal{B}\mathcal{X},\ ,(\det(A|C|x)) = \mathcal{A}\mathcal{C}\mathcal{X},\ (\det(B|C|x)) = \mathcal{B}\mathcal{C}\mathcal{X}$$

where, if L_1 and L_2 are conjugate, the equalities hold in $O_{S'}$, where S' is set of valuations of κ' extending those in S. Anyway we get that

$$(f(x)) = \frac{\mathcal{C}^2}{\mathcal{A}\mathcal{B}}$$

as ideals in $\mathcal{O}_S$. So in particular $(f(x))$ does not depend on the chosen integral point x, then $f(y) = uf(x)$ with $u \in \mathcal{O}_S^*$ for any other y integral. Then all integral points y satisfies an equation

$$\det(A|C|y)\det(B|C|y) = \alpha \det(A|B|y)^2$$

where $\alpha \in f(x) \cdot \mathcal{O}_S^*$.

(3) Suppose that κ'' is a cubic extension. We can construct a function

$$f(x) = \frac{\det(A|C|x)\det(B|C|x)}{\det(A|B|x)^2}$$

Under our assumption we can construct automorphisms T from any $\lambda \in U''$ as in lemma 4.1.9 such that $T \in GL_3(\mathcal{O}_S)$ and

$$T(A) = \lambda A, T(B) = \lambda B, T(C) = \bar{\bar{\lambda}} \text{ if the degree is 3}$$

Note that T preserves the property that a point $P \in \mathbb{P}^2(\kappa'')$ does not coincide with a point of $\mathcal{C}(\overline{\mathbb{Q}})$ mod v'' for any $v'' \notin S''$, where S'' is the set of the valuations of κ'' extending those of S. It follows that T preserves S-integral points. Suppose that

$$x = \alpha A + \beta B + \gamma C$$

then

$$T(x) = \lambda\alpha A + \bar{\lambda}\beta B + \bar{\bar{\lambda}}\gamma C$$

and since $\alpha, \beta, \gamma \neq 0$, the density of S-integral points follows from the density in $\mathbb{P}^2$ of the set

$$\{[\lambda : \bar{\lambda} : \bar{\bar{\lambda}}],\ \lambda \in U''\}$$

(4) Similar to part (3).

□

The last is the case when the cubic is a union of a line and of a geometrically irreducible conic.

Theorem 4.2.15. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $\mathcal{C} = L + Q$ be a κ-defined cubic, whose components are a line and a geometrically irreducible conic (necessarily defined over κ).*

(1) If $|\mathcal{O}_S^*| < \infty$ then the set of S-integral points is not Zariski-dense.

(2) If $|\mathcal{O}_S^*| = \infty$ and $L \cap Q \subseteq \mathbb{P}^2(\kappa)$, then the set of the S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$ is either empty or Zariski-dense.

(3) If $|\mathcal{O}_S^*| = \infty$ and there exists at least an integral point P such that the tangent to $\mathbb{Q}$ through P is κ-defined, then the set of S-integral points is Zariski-dense.

Proof.

(1) Let $L = 0$ and $Q = 0$ be the equations for the line and the conic. We consider the fibration

$$f(x) = \frac{Q(x)}{L(x)^2}$$

Note that if x is integral then we have that

$$(f(x)) = \frac{\mathcal{Q}}{\mathcal{L}^2}$$

so there are only finitely many possibilities for $f(x)$ if $\mathcal{O}_S^*$ is finite, so there is a finite number of conics in the pencil spanned by Q and L^2 containing all the integral points.

(2) Suppose that P is an integral point.

(2.1) If $\{A, B\} = L \cap Q$ we consider the lines L_{AP} and L_{BP}. By integrality of P they do not reduce to components of $\mathcal{C}$ mod v for any $v \notin S$. By theorem 4.1.10 there are infinitely many integral points R on $L_{AP} \setminus \{A, P\}$, which are also integral on $\mathbb{P}^2 \setminus \mathcal{C}$. For each R we can consider the lines L_{BR}: by the same argument they contain infinitely many S-integral points on $\mathbb{P}^2 \setminus \mathcal{C}$. Since we have infinitely many choices for R we have that the set of S-integral points is Zariski-dense.

(2.2) Suppose that L is tangent to Q, i.e. $L \cap Q = \{A\}$. Consider the pencil of conics

$$\alpha L(x)^2 = \beta Q(x), \text{ where } [\alpha : \beta] \in \mathbb{P}^1$$

All of them have L as tangent line in A. We need to add the assumption that L is not a component of $Q \mod v$ for any $v \notin S$. So all conics

$$L(x)^2 = uQ(x),\ u \in \mathcal{O}_S^*$$

have no common component with $L + Q \mod v$ for any $v \notin S$. And by corollary 4.1.1 they have infinitely many integral points.

(3) Consider the κ-defined tangent L_P: it intersects the cubic in two κ-defined points. By proposition 4.1.10 there are infinitely many integral points R on $L_P \setminus L_P \cap L + L_P \cap Q$. For each R we consider a line L_R through R, tangent to Q and distinct from L_P: it is κ-defined and contains an integral point, so it contains infinitely many of them. Since we have infinitely many choices for R the set of S-integral points is Zariski-dense.

□

Chapter 5

Higher dimensional results

In this section we consider the case when the variety has dimension 3. We consider the case $X = \mathbb{P}^3$, the canonical class is $K = [-4\mathrm{div}(H)]$, where $\mathrm{div}(H)$ is a plane divisor. For a divisor D such that $\deg(D) \leq 4$ we have that $K + D$ is not big, so we can hope that the set of S-integral points on $\mathbb{P}^3 \setminus D$ is Zariski-dense.

5.1 Integral points on quadric surfaces of $\mathbb{P}^3$

Now we study the density of integral points on smooth quadric surfaces of $\mathbb{P}^3$. Recall that in general every smooth quadric is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. It can be proved using the Segre's embedding:

$$\begin{array}{rccc} \sigma : & \mathbb{P}^1 \times \mathbb{P}^1 & \to & \mathbb{P}^3 \\ & ([X_0 : X_1], [Y_0 : Y_1]) & \mapsto & [X_0Y_0 : X_0Y_1 : X_1Y_0 : X_1Y_1] \end{array}$$

Potential density of the set of S-integral points on $\mathbb{P}^1 \times \mathbb{P}^1 \setminus D$, where D is a smooth divisor of type $(2, 2)$, was already proved by Hasset and Tschinkel under some geometrical and arithmetical conditions. It is actually a consequence of a more general theorem:

Theorem 5.1.1. *Let X be a smooth Del Pezzo surface and D a smooth anticanonical divisor. Then the set of integral points on $X \setminus D$ is potentially dense.*

Proof. see [HS, Th. 7.2]. □

We will see that actually we do not need to require D to be smooth.

Lemma 5.1.2. *Let κ be a number field. Let X be a smooth quadric surface defined over κ. Suppose that there exists a straight line $L_0 \subset X$ defined over κ. Then for every κ-rational point $P \in X$, the two lines contained in X and passing through P are κ-defined.*

Proof. Let $P \in L_0$ be a κ-rational point. Let $M_P \subset X$ be the other line through P. Then M_P is necessarily κ-defined: otherwise we would have three distinct lines $L, M_P, \overline{M_P}$ contained in X and containing P: contradiction.
Suppose now that P_0, P_1 are two distinct κ-rational points in L_0. Let M_0 and M_1 be the two lines of the other ruling passing respectively through P_0 and P_1. Let $P_2 \in M_0$ be a

κ-defined point $P_2 \neq P_0$. Let L_1 be the line of the other ruling passing through P_2. Then there exists a fourth κ-defined point $P_3 := L_1 \cap M_1$. Let H_0, H_1, H_2, H_3 be the κ-defined tangent planes to the quadric surface respectively in P_0, P_1, P_2, P_3. The set of all quadric surfaces containing the lines L_0, L_1, M_0, M_1 is a pencil spanned by H_0H_3 and H_1H_2, then the equation of the quadric is

$$H_0H_3 = aH_1H_2$$

where necessarily $a \in \kappa$ since, by hypothesis, X is κ-defined. The four planes are in general position, so there is a κ-defined isomorphism between X and the quadric

$$X_0X_3 = X_1X_2$$

for which the assertion is plainly true. □

Proposition 5.1.3. *Let κ be a number field and S a finite set of valuations containing the archimedean ones such that $|\mathcal{O}_S^*| = \infty$. Suppose that $\mathcal{Q}$ is a smooth quadric surface defined over κ and $D = \mathcal{Q} \cap \mathcal{Q}'$ a $(2,2)$-divisor defined over κ, where $\mathcal{Q}'$ is a κ-defined quadric surface such that $\mathcal{Q}'$ mod v has no common component with $\mathcal{Q}$ mod v for any $v \notin S$. Suppose further that*

1. *$\exists L_0 \subset X$ a κ-defined straight line*
2. *$\exists P \in X \setminus D$ an S-integral point.*

Then the set of S-integral points on $\mathcal{Q} \setminus D$ is Zariski-dense.

Proof. By the previous lemma the two lines contained in $\mathcal{Q}$ through P are κ-defined. Let L be one of them. By proposition 4.1.10 there are infinitely many S-integral points Q on $L \setminus L \cap D$. Since L mod v is not a component of $\mathcal{Q}'$ mod v for any $v \notin S$, they are also S-integral on $\mathbb{P}^3 \setminus \mathcal{Q}'$ and so a fortiori on $\mathcal{Q} \setminus D$. For each Q we can choose the line $M_Q \subset \mathcal{Q}$ containing Q. This line is necessarily κ-defined and so it contains infinitely many S-integral points of $\mathcal{Q} \setminus D$. So the set of S-integral points is Zariski-dense. □

To end the section we consider the easier case when D is a conic (a plane section). In this case we do not need any assumptions on existence of κ-defined lines contained in the quadric.

Lemma 5.1.4. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $H \subset \mathbb{P}^n$ be a κ-defined plane. Let $\mathcal{C} \subset H$ be a κ-defined conic. Assume that $\exists P \in \mathcal{C}(\kappa)$ such that P mod v is a smooth point of $\mathcal{C}$ mod v for every $v \notin S$. Then there are infinitely many straight lines contained in H and defined over κ which do not coincide with a component of $\mathcal{C}$ mod v for any $v \notin S$.*

Proof. Let L_0 be the tangent in P to $\mathcal{C}$ and $\mathcal{P}$ the pencil of all the lines contained in H passing through P. By proposition 3.5.3 there are infinitely many S-integral points on $\mathcal{P} \setminus \{L_0\}$, so there are infinitely many κ-defined lines through P not coinciding with L_0 mod v for any $v \notin S$. We show that L mod v is not a component of $\mathcal{C}$ mod v for any $v \notin S$. We distinguish two cases:

- $\mathcal{C}$ mod v is irreducible. In this case the assertion is tautological.

- $\mathcal{C} \bmod v$ is reducible, given by two distinct lines. One of them is $L_0 \bmod v$ and by construction

$$L_0 \bmod v \neq L \bmod v$$

on the other side $L \bmod v$ cannot be the other component, otherwise $P \bmod v$ would be a singular point of $\mathcal{C} \bmod v$.

□

Proposition 5.1.5. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $\mathcal{Q}$ be a quadric surface of $\mathbb{P}^3$ defined over κ, $H \subset \mathbb{P}^3$ a plane defined over κ. Let $\mathcal{C} := H \cap \mathcal{Q}$. Suppose that there is a κ-defined point $P \in \mathcal{Q}$ which is S-integral on $\mathcal{Q} \setminus (\mathcal{Q} \cap H)$.*

(1) Suppose that P is an S-integral on $\mathbb{P}^3 \setminus H$, that $|\mathcal{O}_S^*| = \infty$ and that there is a point $Q \in \mathcal{C}$ not belonging to one of the two lines through P contained in $\mathcal{Q}$, defined over κ and such that $Q \bmod v$ is a smooth point for $\mathcal{Q} \bmod v$ for every $v \notin S$. Then the set of S-integral points on $\mathcal{Q} \setminus (\mathcal{Q} \cap H)$ is Zariski-dense.

(2) Suppose that $|\mathcal{O}_S^*| = \infty$ and that $\mathcal{C} \bmod v$ is irreducible for any $v \notin S$. Then the set of S-integral points on $\mathcal{Q} \setminus (\mathcal{Q} \cap H)$ is Zariski-dense.

(3) Suppose that $\kappa = \mathbb{Q}$, P is an S-integral point on $\mathbb{P}^3 \setminus H$, that $\mathcal{C}$ is geometrically irreducible with good reduction outside S, i.e. $\mathcal{C} \bmod v$ is irreducible for any $v \notin S$ and that $\mathcal{C}(\mathbb{R}) \neq \emptyset$. Then the set of S-integral points on $\mathcal{Q} \setminus (\mathcal{Q} \cap H)$ is Zariski-dense.

Proof.

(1) By the previous lemma there are infinitely many κ-defined straight lines $L \subset H$ such that $L \bmod v$ is not a component of $\mathcal{C} \bmod v$. For each such L denote by Π be the plane generated by L and P. Then $\Pi \bmod v$ contains no component of $\mathcal{C} \bmod v$ for any $v \notin S$. The family of the planes Π through P and Q is a pencil not equal to one of the two pencils of planes containing a line of $\mathcal{Q}$ through P (in fact otherwise P, Q would belong to both the lines contained in $\mathcal{Q}$). So, for all but finitely many planes Π through P and Q, we have that $\Pi \cap \mathcal{Q}$ is a conic $\mathcal{C}'$ which intersects $\mathcal{C}$ in two points. By proposition 4.1.12 the set of S-integral points on $\mathcal{C} \setminus (\mathcal{C} \cap \mathcal{C}')$ is Zariski-dense and they are also S-integral on $\mathcal{Q} \setminus \mathcal{C}$. In fact suppose that $P' \in \mathcal{C}'$ reduces mod v to a point of $\mathcal{C}$, so in particular

$$P' \bmod v \in H \bmod v \cap \Pi \bmod v$$

But by construction the line $H \bmod v \cap \Pi \bmod v$ is not a component of $\mathcal{C} \bmod v$ so

$$P' \bmod v \in (\Pi \cap \mathcal{C}) \bmod v$$

(2) The set of the κ-defined planes passing through P which do not coincide with $H \bmod v$ for any $v \notin S$ is Zariski-dense on the linear system of all the planes through P.
Let Π be one of these planes, we can assume that it is not a plane through one of the lines of $\mathcal{Q}$ passing through P (in fact the planes through one of these two lines

form a 1-dimensional family), then $\mathcal{C}' := \Pi \cap \mathcal{Q}$ is an irreducible κ-defined conic, by proposition 4.1.12 the set of S-integral points on $\mathcal{C}' \setminus (\mathcal{C}' \cap H)$ is Zariski dense. Now we show that they are also S-integral on $\mathcal{Q} \setminus \mathcal{C}$. Let $v \notin S$ be a valuation of κ, let $R \in \mathcal{Q} \setminus \mathcal{C}(\kappa)$ such that $R \bmod v \in \mathcal{C} \bmod v$, then

$$R \mod v \in \mathcal{C} \mod v \cap \Pi \mod v$$

which is given by two points (counting multiplicities) since by assumptions $\mathcal{C} \bmod v$ is irreducible and it cannot have a component contained in $\Pi \bmod v$. So R coincides with a point of $\mathcal{C} \cap \Pi \bmod v \; \forall v \notin S$.

(3) Since there are infinitely many couples of points of $\mathcal{C}$ defined over a real quadratic extension of $\mathbb{Q}$, there are infinitely many $\mathbb{Q}$-defined planes Π through P intersecting $\mathcal{C}$ in a couple of conjugate points defined over a real quadratic extension. Since $\mathcal{C} \bmod v$ is not contained in $\Pi \bmod v$, the result follows like part (1).

□

Example 5.1.6. The set of the solutions in $\mathbb{Z}$ of the equation

$$xy + xz + yz + x + y + z = 0$$

is Zariski-dense in the affine surface defined by that equation. In fact we are in the case when $\kappa = \mathbb{Q}$, $S = \{\infty\}$, the quadric surface is

$$\mathcal{Q} : XY + XZ + YZ + XW + YW + ZW = 0$$

and the plane is

$$H : W = 0$$

Note that $H \bmod p$ is not a component of $\mathcal{Q} \bmod p$ for any prime number p, the plane conic

$$XY + XZ + YZ = 0$$

is irreducible $\bmod p$ for every prime number p and it contains real points, so it contains points belonging to a real quadratic extension of $\mathbb{Q}$. There is an integral point $P = [1 : -1 : 1 : 1]$ on $\mathbb{P}^3 \setminus H$.
So the set of S-integral points on $\mathcal{Q} \setminus (\mathcal{Q} \cap H)$ is Zariski-dense. Since $H \bmod v$ is not a component of $\mathcal{Q} \bmod v$ for any $v \notin S$, they are also integral on $\mathbb{P}^3 \setminus H$.

5.2 Quaternary homogeneous equations of degree≤ 3

In this section we study the density of S-integral points on $\mathbb{P}^3 \setminus D$, where D is a κ-defined divisor and $\deg(D) \leq 3$. The case of degree 1 was considered in a more general context in theorem 3.5.7. We start with the case when $\deg(D) = 2$, the idea of the proof is very to similar to 4.2.1.

Theorem 5.2.1. *Let κ be a number field, S be a finite set of valuations containing the archimedean ones. Let $\mathcal{Q}$ be a smooth quadric surface defined over κ.*

(1) If $\kappa \supsetneq \mathbb{Q}$ or $|\mathcal{O}_S^*| = \infty$, then the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{Q}$ is either empty or Zariski-dense.

(2) If $\kappa = \mathbb{Q}$ and $\mathcal{Q}(\mathbb{R}) \neq \emptyset$, then the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{Q}$ is either empty or Zariski-dense.

(3) If $\mathcal{Q}(\kappa_v) = \emptyset$ for every $v \in S$, then there are only finitely many S-integral points on $\mathbb{P}^3 \setminus \mathcal{Q}$.

Proof.

(1) The idea is to apply proposition 4.1.10.

- Suppose that $|\mathcal{O}_S^*| = \infty$ and that there exists a point P, which is S-integral on $\mathbb{P}^3 \setminus \mathcal{Q}$. Then, for every κ-defined straight line L through P, L contains infinitely many S-integral points by 4.1.10.
- Suppose that $\kappa \supsetneq \mathbb{Q}$, let P an S-integral point on $\mathbb{P}^3 \setminus \mathcal{Q}$. Denote by X the 2-dimensional linear system of the lines through P. Then the set

$$\{L \in X \text{ such that } L \text{ is } \kappa\text{-defined and } L \cap \mathcal{Q} \subset \mathbb{P}^3(\kappa)\}$$

  is not Zariski-dense by Hilbert's Irreducibility Theorem. So the set of the lines of X which are κ-defined and intersect the quadric surface in two points not defined over κ is Zariski-dense on X. On each of these lines there are infinitely many S-integral points. It follows that the set of S-integral points is Zariski-dense.

(2) Let P be an S-integral point on $\mathbb{P}^3 \setminus D$. Since $\mathcal{Q}(\mathbb{R}) \neq \emptyset$, there is an $\mathbb{R}$-defined straight line, denoted by L_0 such that $L \cap \mathcal{Q}(\mathbb{R}) \neq \emptyset$. Denote by X the 2-dimensional linear system of the straight lines through P, considered as a real manifold with the euclidean topology. There is an open neighbourhood U of $L_0 \in X$ such that $L \cap \mathcal{Q}(\mathbb{R}) \neq \emptyset, \forall L \in U$. The set of $\mathbb{Q}$-rational points of U is euclidean-dense on U. Then it is Zariski-dense on X. We are also able, as in the proof of 4.2.1 to find an euclidean-dense subset of U composed by $\mathbb{Q}$-defined straight lines which intersect $\mathcal{Q}$ in two points which are conjugate defined over a quadratic extension of $\mathbb{Q}$. It follows that the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{Q}$ is Zariski-dense.

(3) Suppose that $\mathcal{Q}(\kappa_v) = \emptyset$ for any $v \notin S$, the idea is the same of 4.2.1. We consider a function

$$F(X, Y, Z, W) = 0$$

the equation for $\mathcal{Q}$. Consider for any $v \in S$ the map

$$\begin{array}{rccc} \pi: & \mathbb{P}^3(\kappa_v) & \to & \mathbb{R}_0^+ \\ & [X:Y:Z:W] & \mapsto & \dfrac{|F(X,Y,Z,W)|_v}{\max(|X|_v, |Y|_v, |Z|_v, |W|_v)^2} \end{array}$$

This is clearly well defined and independent from the choice of homogeneous coordinates. Since $\mathbb{P}^3(\kappa_v)$ is compact in the v-adic topology, we have that π has a minimum value $m_v > 0$ and proceeding like in 4.2.1 we prove that the height of integral points is bounded, so they are only finitely many.

□

Example 5.2.2. The solutions $[x : y : z : w]$ of the diophantine equation

$$x^2 + y^2 - z^2 - w^2 = 1$$

form a Zariski-dense subset of $\mathbb{P}^3$. In fact we are in the case (2) of the previous theorem when

$$\mathcal{Q} : X^2 + Y^2 - Z^2 - W^2 = 0$$

there is a point

$$Q = [1 : 0 : 1 : 0] \in \mathcal{Q}(\mathbb{R})$$

and a point $P = [1 : 0 : 0 : 0]$ S-integral. So the set of solutions $[x : y : z : w]$ in integers to

$$x^2 + y^2 - z^2 - w^2 = \pm 1$$

is Zariski-dense. Since

$$F(X, Y, Z, W) = -F(Z, W, X, Y)$$

it follows that

$$x^2 + y^2 - z^2 - z^2 = 1$$

has a Zariski-dense set of solutions in $\mathbb{Z}$.

Now we consider the case when $\mathcal{S}$ is an irreducible cubic surface.

Theorem 5.2.3. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $\mathcal{S}$ be an irreducible cubic surface defined over κ.*

(1) Suppose that $\mathcal{S}$ has only a finite number of singularities. Suppose that there is a κ-rational smooth point F and a κ-defined straight line L containing F such that:

- $(L.\mathcal{S})_F$=3;
- $L \bmod v$ *is not a sub-variety of* $\mathcal{S} \bmod v$ *for any* $v \notin S$;
- *it exists a plane $H_0 \supset L$ such that $H_0 \cap \mathcal{S}$ is a smooth plane cubic curve.*

Then the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense.

(2) Suppose that $\mathcal{S}$ is singular, but not a cone and that $|\mathcal{O}_S^*| = \infty$. Assume that there are $L, M \subset \mathbb{P}^3$ κ-defined lines such that:

- *L and M are skew lines;*
- *$L \subset \mathcal{S}$ and it contains a κ-rational singular point of $\mathcal{S}$;*
- *there exists $P \in M$ such that P is S-integral on $\mathbb{P}^3 \setminus \mathcal{S}$;*
- *M is either tangent to $\mathcal{S}$ in a κ-defined point or it intersects $\mathcal{S}$ in a κ-defined point.*

Then the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense.

Proof.

(1) Let $\mathcal{P}$ be the pencil of all the planes containing L. If there is $H_0 \in L$ sucht that $H \cap \mathcal{S}$ is smooth, then the set of all the planes $H \in \mathcal{P}$ intersecting $\mathcal{S}$ in a smooth curve is a dense open set of $\mathcal{P}$. So in particular there are infinitely many such that H is κ-defined and $H \cap \mathcal{Q}$ is a smooth plane cubic. For each such H let $\mathcal{C} := H \cap \mathcal{S}$, then all assumptions of Beukers' theorem 4.2.4 are verified:

- $\mathcal{C}$ is a smooth cubic by construction, hence irreducible;
- F is a κ-rational flex of $\mathcal{C}$ whose inflexional tangent is L;
- L is not a component of $\mathcal{C}$ mod v for any valuation $v \notin S$: this follows a fortiori from the fact that L mod v is not a subvariety of $\mathcal{S}$ mod v.

Then the set of S-integral points on $H \setminus \mathcal{C}$ is Zariski-dense. Since H is not a component of $\mathcal{S}$ mod v for any $v \notin S$, they are S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$. Since we have infinitely many choices for H. Since there are infinitely many choices for H, it follows that the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense.

(2) By proposition 4.1.10 M contains infinitely many S-integral points R. For each such R we consider the plane H containing R and L. Note that, since L and M are skew lines, all these planes are distinct one from the other. Let $Q \in L$ be a κ-defined singular point of $\mathcal{S}$. Note that Q is a singular point of $H \cap \mathcal{S} = \mathcal{C} + L$, so, if $\mathcal{C}$ is an irreducible conic (it happens except for a finite number of planes), it follows that $Q \in L \cap \mathcal{C}$. So by theorem 4.2.15 the set of S-integral points contained in H is Zariski-dense in H. So the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense.

□

Example 5.2.4. The diophantine equation

$$x^3 + y^3 + z^3 + w^3 = 1$$

has a Zariski-dense set of solutions in integers. In this case $\kappa = \mathbb{Q}$, $S = \{\infty\}$ and the cubic is the Fermat cubic surface:

$$\mathcal{S} : X^3 + Y^3 + Z^3 + W^3 = 0.$$

We are in the case (1) of the previous theorem, there is a κ-defined triple tangent to $\mathcal{S}$ which is not a component of $\mathcal{S}$ mod p for any prime integer p, namely

$$M : \begin{cases} X + Y & = 0 \\ Z & = 0 \end{cases}$$

in the point $F = [1 : -1 : 0 : 0]$. If we choose $H_0 : Z = 0$, we have that $H_0 \cap \mathcal{S}$ is a smooth cubic curve, so the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense.

Example 5.2.5. Let $\kappa = \mathbb{Q}$, $S = \{\infty, p\}$, where p is a prime number, let $\mathcal{S}$ be the Cayley's nodal cubic surface

$$XYZ + YZW + ZWX + WXY = 0$$

Then the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense, i.e the diophantine equation

$$xyz + yzw + zwx + wxy = p^e$$

has a Zariski-dense set of solutions in $\mathbb{Z}\left[\frac{1}{p}\right]$. The singular points of $\mathcal{S}$ are $[1:0:0:0]$ and its permutations. Note that there is a line $L \subset \mathcal{S}$ containing a κ-defined singular point

$$L : \begin{cases} X = 0 \\ Y = 0 \end{cases}$$

$[0:0:0:1] \in L$ and there is another κ-defined line

$$M := \begin{cases} Z = 0 \\ X = W \end{cases}$$

which is skew to L and contains the S-integral point

$$[1:1:0:1]$$

Note that the general plane containing L has an equation

$$X = tY$$

and its intersection with $\mathcal{S}$ is

$$\begin{cases} X & = tY \\ Y(tYZ + ZW + tZW + tYW) & = 0 \end{cases}$$

the other component is an irreducible conic for $t \neq 0, -1$. The two points of intersection between L and $\mathcal{C}$ are given by the system

$$\begin{cases} X & = 0 \\ Y & = 0 \\ ZW(1+t) & = 0 \end{cases}$$

and they are $[0:0:1:0]$ and $[0:0:0:1]$.

We end this section considering the case when the cubic is reducible

Theorem 5.2.6. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $\mathcal{S} = \mathcal{Q} + H$ be a cubic surfaces given by a smooth quadric $\mathcal{Q}$ and a plane H both defined over κ.*

(1) If $|\mathcal{O}_S^*| < \infty$ then the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is not Zariski-dense.

(2) Assume either that $H \cap \mathcal{Q}$ is a couple of κ-defined lines or $H \cap \mathcal{Q} = \mathcal{C}$ is an irreducible conic and it contains a point A such that $A \bmod v$ is a smooth point for $\mathcal{C} \bmod v$ for any $v \notin S$. Suppose that there is a point P which is S-integral on $\mathbb{P}^3 \setminus \mathcal{S}$ and a κ-defined line M containing P. Suppose that M verifies one of the following assumptions:

- *M is tangent to $\mathcal{Q}$ in a point not in $H \cap \mathcal{Q}$*
- *M intersects $\mathcal{Q}$ in a point of $\mathcal{Q} \cap H$ and it is not contained in any quadric of the pencil spanned by $\mathcal{Q}$ and H^2.*

Then the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense.

Remark 5.2.7. Note that if M would be tangent to $\mathcal{Q}$ in a point Q of $H \cap \mathcal{Q}$, then it would be tangent in Q to any quadric of the pencil spanned by $\mathcal{Q}$ and H^2, consequently we could find a quadric of the pencil containing it.

Proof.

(1) Consider the fibration

$$f(x) = \frac{\mathcal{Q}(x)}{H(x)^2}$$

Then if x is an S-integral point on $\mathbb{P}^3 \setminus \mathcal{S}$, then

$$(\mathcal{Q}(x)) = \mathfrak{q} \cdot \mathfrak{x}^2, \ \ (H(x)) = \mathfrak{h} \cdot \mathfrak{x}$$

where $\mathfrak{q}, \mathfrak{h}, \mathfrak{x}$ are the ideals generated by the coefficients of $\mathcal{Q}, H$ and the coordinates of x. Then all the S-integral points belong to a finite number of quadric surfaces

$$aH(x)^2 = \mathcal{Q}(x), \text{ where } (a) = \frac{\mathfrak{q}}{\mathfrak{h}^2}.$$

(2) By construction the line M intersects $\mathcal{S}$ in at most two points which are either κ-defined or conjugate defined over a quadratic extension. Then by proposition 4.1.10 the set of S-integral points on $M \setminus (M \cap \mathcal{S})$ is Zariski-dense and, since $M \bmod v$ is not a subvariety of $\mathcal{S} \bmod v$ for any $v \notin S$, they are S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$. For both the possible behaviours of M we can find infinitely many quadric surfaces of the pencil containing at least one integral point:

- If M is tangent to $\mathcal{Q}$ in $Q \notin H$ then no quadric of the pencil contains M: if it would exist such a quadric then it would intersect $\mathcal{Q}$ in $\mathcal{Q} \cap H$ and so it would follow that $Q \in H$: contradiction. In this case we can construct recursively a sequence of distinct quadrics containing at least one integral point: we start from an S-integral point $R_1 \in M$, we define $\mathcal{Q}_1$ a quadric of the pencil and R_1' the other point of intersection between M and $\mathcal{Q}$ and for any $n \geq 2$:
  - We choose an S-integral point $R_n \in M \setminus \{R_i, R_i', \ i = 1, ..., n-1\}$;
  - We define $\mathcal{Q}_n$ the quadric of the pencil through R_n.

  By construction $\mathcal{Q}_{n_1} \neq \mathcal{Q}_{n_2}$ if $n_1 \neq n_2$.
- M intersect $\mathcal{Q}$ in two distinct points Q and Q' and necessarily $Q' \notin H$, so like in the previous case M cannot be contained in some quadric of the pencil (since it would imply that $Q' \in H$). Let R, R' be two distinct S-integral points on M, let $\mathcal{Q}_R, \mathcal{Q}_{R'}$ be the corresponding quadric surfaces of the pencil through them. If $\mathcal{Q}_R = \mathcal{Q}_{R'}$ then $R = R'$ otherwise $\mathcal{Q}_R \supset M$ contradicting our assumptions.

If $H \cap \mathcal{Q}$ is a couple of κ-defined lines then any κ-defined quadric of the pencil has the rulings defined over κ, using an argument analogous to 5.1.3 each quadric containing at least an integral point contains a Zariski-dense set of integral points. In the other case the assertion follows from 5.1.5.

Example 5.2.8. The set of the solutions [X:Y:Z:W] in integers of the diophantine equation

$$(X+Y+Z+W)(XY+XZ+XW+YZ+YW+ZW) = 2^e \text{ for some } e \in \mathbb{N}$$

is Zariski-dense. In this case $\kappa = \mathbb{Q}$, $S = \{\infty, 2\}$

$$\mathcal{S} : (X+Y+Z+W)(XY+XZ+XW+YZ+YW+ZW) = 0$$

We have that
$(X+Y+Z+W, XY+XZ+XW+YZ+YW+ZW) =$
$(X+Y+Z+W, Y^2+YZ+YW+Z^2+ZW+W^2)$
So the intersection is an irreducible conic. Note that there exists an S-integral point $P = [1:2:0:-1]$. Let $M = V(X+W, Y+Z+2W)$, then $M \ni P$ and it is tangent to $\mathcal{Q}$ in $[1:1:1:-1]$ which is not a point of H. So by previous theorem the set of S-integral points on $\mathbb{P}^3 \setminus \mathcal{S}$ is Zariski-dense. Since the change of variables

$$X \mapsto -X, \;\; Y \mapsto -Y, \;\; Z \mapsto -Z, \;\; W \mapsto -W$$

inverts the sign of the form $\mathcal{S}$, then the set of the solutions in $\mathbb{Z}$ of the diophantine equation

$$(X+Y+Z+W)(XY+XZ+XW+YZ+YW+ZW) = 2^e, \text{ for some } e \in \mathbb{N}$$

is Zariski-dense.

□

5.3 Quaternary homogeneous equations of degree 4

In this section we study the problem of finding a Zariski-dense set of S-integral points on $\mathbb{P}^3 \setminus D$, where D is a reducible κ-defined divisor such that

$$D = H_1 + H_2 + H_3 + H_4 \text{ or } D = \mathcal{Q}_1 + \mathcal{Q}_2$$

where H_1, H_2, H_3, H_4 are distinct planes, $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are smooth quadric surfaces defined over κ, whose intersection is reducible. Unfortunately the author was not able to prove (or disprove) the density in the interesting cases when $\mathcal{Q}_1$ or $\mathcal{Q}_2$ intersect transversally or in a couple of distinct conics. The case when D is irreducible looks to be very hard.

Theorem 5.3.1. *Let κ be a number field. Let S be a finite set of valuations containing the archimedean ones. Let $D = H_1 + H_2 + H_3 + H_4$ be a κ-defined quartic surface, where $H_1, H_2, H_3, H_4 \subset \mathbb{P}^3$ are 4 planes in general position (so $H_1 \cap H_2 \cap H_3 \cap H_4 = \emptyset$).*

(1) If $|\mathcal{O}_S^*|$ is finite and that there is a sub-divisor $D' \subset D$ defined over κ. Then the set of S-integral points on $\mathbb{P}^3 \setminus D$ is not Zariski-dense. In the case when all the H_i are defined over κ, there is only a finite number of S-integral points.

(2) Suppose that $|\mathcal{O}_S^*| = \infty$ and that there is a sub-divisor $D' \subset D$ defined over κ. Then the set of S-integral points on $\mathbb{P}^3 \setminus D$ is either empty or Zariski-dense.

Proof. (1) We distinguish three possible cases

(1.1) H_1, H_2, H_3, H_4 are defined over κ. In this case we can choose various fibrations over $\mathbb{G}_m$:

$$f_1(x) = \frac{H_1(x)H_2(x)}{H_3(x)H_4(x)}$$
$$f_2(x) = \frac{H_1(x)H_3(x)}{H_2(x)H_4(x)}$$
$$f_3(x) = \frac{H_1(x)H_4(x)}{H_2(x)H_3(x)}$$

If x is integral we have that

$$(H_i(x)) = \mathcal{H}_i \cdot \mathcal{X}$$

where $\mathcal{H}_i$ and $\mathcal{X}$ are the ideal generated respectively by the coefficients of H_i and the coordinates of x. Then we have that

$$(f_1(x)) = \frac{\mathcal{H}_1\mathcal{H}_2}{\mathcal{H}_3\mathcal{H}_4},\ (f_2(x)) = \frac{\mathcal{H}_1\mathcal{H}_3}{\mathcal{H}_2\mathcal{H}_4},\ (f_3(x)) = \frac{\mathcal{H}_1\mathcal{H}_4}{\mathcal{H}_2\mathcal{H}_3}.$$

Let ξ be a fixed S-integral point on $\mathbb{P}^3 \setminus D$. Consider the three family of quadric surfaces:

$$\mathcal{F}_1 := \{H_1(x)H_2(x) = aH_3(x)H_4(x),\ a \in f_1(\xi)\mathcal{O}_S^*\}$$
$$\mathcal{F}_2 := \{H_1(x)H_3(x) = aH_2(x)H_4(x),\ a \in f_2(\xi)\mathcal{O}_S^*\}$$
$$\mathcal{F}_3 := \{H_1(x)H_4(x) = aH_2(x)H_3(x),\ a \in f_3(\xi)\mathcal{O}_S^*\}$$

For each i all the S-integral points are contained in $\bigcup_{Q \in \mathcal{F}_i} Q$. So all integral points are contained in the finite set

$$\bigcup_{Q_1 \in \mathcal{F}_1, Q_2 \in \mathcal{F}_2, Q_3 \in \mathcal{F}_3} Q_1 \cap Q_2 \cap Q_3$$

(1.2) Suppose that $H_1 + H_2$ is defined over κ. Then $H_3 + H_4$ is also κ-defined. So there is a κ-defined fibration

$$f(x) := \frac{H_1(x)H_2(x)}{H_3(x)H_4(x)}.$$

If ξ is a fixed integral point then all integral points are contained in the finite family of quadrics

$$H_1(x)H_2(x) = aH_3(x)H_4(x),\ a \in f(\xi)\mathcal{O}_S^*$$

(1.3) Suppose that $H_1 + H_2 + H_3$ is defined over κ. Then H_4 is κ-defined and we can construct a κ-defined fibration

$$f(x) = \frac{H_1(x)H_2(x)H_3(x)}{H_4(x)^3}.$$

By the same argument we can prove that if ξ is a fixed integral point then all integral points are contained in the finite set of cubic surfaces

$$H_1(x)H_2(x)H_3(x) = aH_4(x)^3,\ a \in f(\xi)\mathcal{O}_S^*$$

(2) Consider the points

$$P_1 := H_2 \cap H_3 \cap H_4,\ P_2 := H_1 \cap H_3 \cap H_4,\ P_3 := H_1 \cap H_2 \cap H_4,\ P_4 := H_1 \cap H_2 \cap H_3$$

We have that

$$\begin{aligned} H_1(x) &= \det(x|P_2|P_3|P_4) \\ H_2(x) &= \det(P_1|x|P_3|P_4) \\ H_3(x) &= \det(P_1|P_2|x|P_4) \\ H_4(x) &= \det(P_1|P_2|P_3|x) \end{aligned}$$

Let ξ be an S-integral point on $\mathbb{P}^3 \setminus D$. We distinguish three cases:

(2.1) H_1, H_2, H_3, H_4 are defined over κ. Consider the following group of automorphisms

$$\mathcal{T} := \{T \in GL_4(\mathcal{O}_S)\ :\ T(P_i) = \lambda_i P_i \text{ where } \lambda_i \in \mathcal{O}_S^*\}.$$

It' $T(\xi)$ is integral for any $T \in \mathcal{T}$. Further the set $\{T(\xi) : T \in \mathcal{T}\}$ is Zariski-dense in $\mathbb{P}^3$ since $\xi \notin H_1 + H_2 + H_3 + H_4$ and the set

$$\{[\lambda_1 : \lambda_2 : \lambda_3 : \lambda_4]\}$$

is Zariski-dense in $\mathbb{P}^3$.

(2.2) Suppose that $H_1 + H_2$ and $H_3 + H_4$ are defined over κ, then also the subvarieties $\{P_1, P_2\}$ and $\{P_3, P_4\}$ are defined over κ. Similarly to (2.1) we consider set of automorphisms

$$\mathcal{T} := \{T \in GL_4(\mathcal{O}_S)\ :\ T(P_i) = \lambda_i P_i \text{ where } \lambda_i \in \mathcal{O}_S^*,\ \lambda_2 = \bar{\lambda}_1,\ \lambda_4 = \bar{\lambda}_3\}.$$

Also in this case the density of the set of S-integral points follows from the density in $\mathbb{P}^3$ of the set

$$\{[\lambda_1 : \bar{\lambda}_1 : \lambda_3 : \bar{\lambda}_3]\}$$

(2.3) Suppose that $H_1 + H_2 + H_3$ is defined over κ and that H_1, H_2, H_3 are conjugate over a cubic extension. Let

$$f(x) = \frac{\det(x|P_2|P_3|P_4)\det(P_1|x|P_3|P_4)\det(P_1|P_2|x|P_4)}{\det(P_1|P_2|P_3|x)^3}.$$

All integral points verify an equation

$$\det(x|P_2|P_3|P_4)\det(P_1|x|P_3|P_4)\det(P_1|P_2|x|P_4) = f(\xi)\det(P_1|P_2|P_3|x)^3$$

and the set of automorphisms

$$\mathcal{T} := \{T \in GL_4(\mathcal{O}_S) \ : \ T(P_i) = \lambda_i P_i \text{ where } \lambda_2 = \bar{\lambda}_1,\ \lambda_3 = \bar{\bar{\lambda}}_1\}$$

preserve S-integral points. In this case the density of integral points follows from the density in $\mathbb{P}^3$ of the set

$$\{[\lambda_1 : \bar{\lambda}_1 : \bar{\bar{\lambda}}_1 : \lambda_4]\}$$

□

Theorem 5.3.2. *Let κ be a number field, S a finite set of valuations containing the archimedean ones. Let $D = \mathcal{Q}_1 + \mathcal{Q}_2$ be a κ-defined divisor, where $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are smooth quadric surfaces. Suppose that $\mathcal{Q}_1 \bmod v$ and $\mathcal{Q}_2 \bmod v$ have no common component for any $v \notin S$.*

(1) Suppose that $|\mathcal{O}_S^*| < \infty$ and that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are either defined over κ or they are conjugate over a quadratic extension κ'/κ such that $|\mathcal{O}_{S'}^*| < \infty$, where S' denotes the set of the valuations of κ' extending those of κ. Then the set of S-integral points on $\mathbb{P}^3 \setminus D$ is not Zariski-dense: they are contained in a finite set of quadric surfaces of the pencil spanned by $\mathcal{Q}_1$ and $\mathcal{Q}_2$.

(2) Suppose that $|\mathcal{O}_S^*| = \infty$. Assume that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are κ-defined and that $\mathcal{Q}_1 \cap \mathcal{Q}_2$ contains at least one straight line defined over κ. Suppose further:

- *There is an S-integral point P on $\mathbb{P}^3 \setminus D$;*
- *There is a straight line $M \subset \mathbb{P}^3$ defined over κ, not contained in any quadric of the pencil spanned by $\mathcal{Q}_1$ and $\mathcal{Q}_2$, such that $P \in M$ and that one of the following is true:*
  - $\exists Q \in \mathcal{Q}_1 \cap \mathcal{Q}_2 \cap M$ such that M is tangent to $\mathcal{Q}_1$ in Q, but not to $\mathcal{Q}_2$.
  - M is tangent both to $\mathcal{Q}_1$ and to $\mathcal{Q}_2$ and $\mathcal{Q}_1 \cap \mathcal{Q}_2 \cap M = \emptyset$.

Then the set of S-integral points on $\mathbb{P}^3 \setminus D$ is Zariski-dense.

(3) Suppose that $|\mathcal{O}_S^*| = \infty$. Assume that $\mathcal{Q}_1 \cap \mathcal{Q}_2 = 2\mathcal{C}$, where $\mathcal{C}$ is a smooth conic irreducible mod v for any $v \notin S$. Suppose further:

- *$\exists P$ an S-integral point on $\mathbb{P}^3 \setminus (\mathcal{Q}_1 + \mathcal{Q}_2)$;*
- *$\exists M$ a κ-defined bitangent line to $(\mathcal{Q}_1 + \mathcal{Q}_2)$ not intersecting $\mathcal{C}$ and not contained in $\mathcal{Q}_1 + \mathcal{Q}_2$ such that $P \in M$;*
- *M is not contained in any quadric of the pencil spanned by $\mathcal{Q}_1$ and $\mathcal{Q}_2$;*

Then the set of S-integral points on $\mathbb{P}^3 \setminus (\mathcal{Q}_1 + \mathcal{Q}_2)$ is Zariski-dense.

Proof.

(1) Consider the fibration $f : \mathbb{P}^3 \setminus D \to \mathbb{G}_m$ given by

$$f(x) = \frac{\mathcal{Q}_1(x)}{\mathcal{Q}_2(x)}.$$

Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be the corresponding ideals of $\mathcal{O}_S$ generated by their coefficients. If x is an integral point on $\mathbb{P}^3 \setminus D$ then

$$(f(x)) = \frac{\mathfrak{q}_1}{\mathfrak{q}_2}$$

so there are only finitely many possibilities.

(2) Suppose to be in the case when $\exists Q \in \mathcal{Q}_1 \cap \mathcal{Q}_2 \cap M$ such that M is tangent to $\mathcal{Q}_1$ in Q, but not to $\mathcal{Q}_2$. The other case is very similar.
We have that $M \cap \mathcal{Q}_1 = \{Q\}$, $M \cap \mathcal{Q}_2 = \{Q, Q'\}$, where $Q \neq Q'$. By proposition 4.1.10 the set of S-integral points on $M \setminus \{Q, Q'\}$ is infinite. Since $M \bmod v$ is not contained in $\mathcal{Q}_1 + \mathcal{Q}_2 \bmod v$ for any $v \notin S$, we have that they are S-integral points on $\mathbb{P}^3 \setminus D$. For each R S-integral point on $M \setminus \{Q, Q'\}$ there exists one and only one quadric of the pencil, denoted by $\mathcal{Q}_R$, containing it. Note that

$$R \neq R' \Rightarrow \mathcal{Q}_R \neq \mathcal{Q}_{R'}$$

in fact otherwise there would be a quadric of the pencil containing three distinct points of M (Q, R and R') so it would contain M, contradicting our assumptions. So we have found infinitely many quadric surfaces of the pencil containing at least one integral point. By proposition 5.1.3 the set of S-integral points on $\mathcal{Q}_R \setminus (\mathcal{Q}_1 \cap \mathcal{Q}_2)$ is Zariski-dense for any R as before. Since $\mathcal{Q}_R \bmod v$ has no common component with $(\mathcal{Q}_1 \cup \mathcal{Q}_2) \bmod v$ for any $v \notin S$, they are S-integral points on $\mathbb{P}^3 \setminus D$. It follows that the set of S-integral points on $\mathbb{P}^3 \setminus D$ is Zariski-dense.

(3) By proposition 4.1.10 the set of S-integral points on $M \setminus M \cap (\mathcal{Q}_1 \cup \mathcal{Q}_2)$ is Zariski-dense and they are also S-integral on $\mathbb{P}^3 \setminus (\mathcal{Q}_1 \cup \mathcal{Q}_2)$. Since M is not contained in any quadric of the pencil spanned by $\mathcal{Q}_1$ and $\mathcal{Q}_2$ there are infinitely many quadric surfaces $\mathcal{Q}$ of the pencil containing at least one integral point. Applying proposition 5.1.5 for each $\mathcal{Q}$ the set of S-integral points on $\mathcal{Q} \setminus \mathcal{C}$ is Zariski-dense and since $\mathcal{Q} \bmod v$ has no common component with $\mathcal{Q}_1 \bmod v$ and $\mathcal{Q}_2 \bmod v$ for any $v \notin S$ they are S-integral points on $\mathbb{P}^3 \setminus (\mathcal{Q}_1 + \mathcal{Q}_2)$. □

Example 5.3.3. The diophantine equation

$$(XW - YZ)(XY - ZW) = 2^e \text{ for some}$$

has a Zariski-dense set of solutions in $\mathbb{Z}\left[\frac{1}{p}\right]$. This is the case of the previous theorem part (2) whenever

$$\kappa = \mathbb{Q},\ S = \{\infty, 2\}\ \mathcal{Q}_1 = XW - YZ,\ \mathcal{Q}_2 = XY - ZW.$$

Consider the point $P = [1 : 1 : 0 : 2]$: it is an S-integral point on $\mathbb{P}^3 \setminus (\mathcal{Q}_1 + \mathcal{Q}_2)$, consider the κ-defined straight line

$$M := \begin{cases} X - Y & = 0 \\ 2Y - Z - W = 0 \end{cases}$$

then $P \in M$ and M is tangent to $\mathcal{Q}_2$ in $[1:1:1:1] \in \mathcal{Q}_1 \cap \mathcal{Q}_2$ and it is not contained in any quadric of the pencil spanned by $\mathcal{Q}_1$ and $\mathcal{Q}_2$: in fact: $M \cap \mathcal{Q}_1 = \{[1:1:1:1], [0:0:1:-1]\}$ and $[0:0:1:-1] \notin \mathcal{Q}_2$. So the set of solutions in integers to the diophantine equation

$$(XY - ZW)(XW - YZ) = \pm 2^e \text{ for some } e \in \mathbb{N}$$

is Zariski-dense. Since the change of variables

$$X \mapsto Z, \;\; Y \mapsto W, \;\; Z \mapsto X, \;\; W \mapsto Y$$

invert the sign of the form

$$F(X, Y, Z, W) = (XY - ZW)(XW - YZ),$$

it follows that the set of solutions in integers to the diophantine equation

$$(XY - ZW)(XW - YZ) = 2^e \text{ for some } e \in \mathbb{N}$$

is Zariski-dense.

Example 5.3.4. Let p be a prime number. The set of solutions in integers to the diophantine equation

$$(X^2 + Y^2 + Z^2 - W^2)(XY - ZW) = p^e$$

is Zariski-dense.
We have that

$$V(X^2 + Y^2 + Z^2 - W^2) \cap V(XY - ZW) = V(Y - W, X - Z) \cup V(Y + W, X + Z) \\ \cup V(Y - Z, X - W) \cup V(Y + Z, X + W)$$

We are in the case (2) of the theorem when $\kappa = \mathbb{Q}$ and $S = \{\infty, p\}$, the two quadrics have plainly no common component $\bmod v$ for any v, we need only to find the line M of the statement. Consider the points

$$Q = [1:0:0:1] \in \mathcal{Q}_1 \cap \mathcal{Q}_2, \;\; P := [1:1:0:1]$$

Then P is S-integral on $\mathbb{P}^3 \setminus D$ and the line through P and Q is

$$M := \begin{cases} X = W \\ Z = 0 \end{cases}$$

which is tangent to Q. Note also that M is not contained in any quadric of the pencil spanned by $\mathcal{Q}_1$ and $\mathcal{Q}_2$

$$\mathcal{Q}_t : X^2 + tXY + Y^2 + Z^2 - tZW - W^2$$

So the result follows from part (2).

Example 5.3.5. The set of the solutions in integers of the diophantine equation

$$(XY + XZ + YW)(XW + YZ + YW) = \pm 2^e$$

is Zariski-dense. We are in the case (2) of the theorem, whenever $\kappa = \mathbb{Q}$ and $S = \{\infty, 2\}$, $\mathcal{Q}_1 = V(XY + XZ + YW)$, $\mathcal{Q}_2 = V(XW + YZ + YW)$.

$$V(XY + XZ + YW) \cap V(XW + YZ + YW)$$

$$=$$

$$V(Z^2 - XW + ZW - W^2, YZ + XW + YW, XY + XZ + YW) \cup V(Y, X)$$

where the first component is irreducible of degree 3. Let $Q = [1 : 0 : 0 : 0]$, $P = [1 : 0 : 1 : 1]$. Then P is an S-integral point on $\mathbb{P}^3 \setminus D$ and the line joining them is

$$M := V(Y, X - W)$$

which is tangent to $\mathcal{Q}_2$ in Q. Note that M is not contained in any quadric of the pencil, then the result follows from part (2).

Bibliography

[Beu] Beukers F. (1995), *Ternary forms equations*, J. Number Theory 54, no. 1, 113133.

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

[Co] Corvaja P.(2016), *Integral Points on Algebraic Varieties*, IMSc Lecture Notes in Mathematics, Springer Singapore, ISBN 978-981-10-2648-5.

[Fa] G. Faltings (1983), *Endlichkeitssatzes fur Abelsche Varietaten uber Zahlkorpern*, Inv. Math. 73, 349-366.

[Ha] R. Hartshorne (1977), *Algebraic Geometry*, GTM 52, Springer-Verlag.

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

[Le] D.H. Lehmer (1956), *On the diophantine equation* $x^3 + y^3 + z^3 = 1$, London Mathematical Society **31**, 275-280.

[Ma] Marcus D. (1977) *Number Fields*, Springer-Verlag, New York. ISBN 0-387-90279-1

[Mi1] Milne J.S. (1997-2016), *Algebraic Number Theory*

[Mo] Mordell L.J. (1969) *Diophantine Equations*, Volume 30 in PURE AND APPLIED MATHEMATICS, Columbia University, New York

[V1] P. Vojta (1987), *Diophantine approximation and value distribution theory*, L.N.M. 1239, Springer-Verlag.

[V2] P. Vojta (1996), *Integral points on subvarieties of semi-abelian varieties*, Inv. Math. 126, 133-181.

[Za] Zannier U. (2014), *Lecture Notes on Diophantine Analysis*, Scuola Normale Superiore di Pisa, ISBN 978-88-7642-341-3.