Infinite Sets of D-integral Points on Projective Algebraic Varieties

by

Veronika Shelestunova

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2005

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Let $X(K) \subset \mathbf{P}^n(K)$ be a projective algebraic variety over K, and let D be a subset of $\mathbf{P}^n_{\mathcal{O}_K}$ such that the codimension of D with respect to $\overline{X} \subset \mathbf{P}^n_{\mathcal{O}_K}$ is two. We are interested in points P on $X(K)$ with the property that $\overline{P} \cap D = \emptyset$ in $\mathbf{P}^n_{\mathcal{O}_K}$, we call such points D-integral points on $X(K)$. First we prove that certain algebraic varieties have infinitely many D-integral points. Then we find an explicit description of the complete set of D-integral points in $\mathbf{P}^2(\mathbf{Q})$ for several types of D.

Acknowledgments

I want to say a special thank you to my supervisor Professor David McKinnon. This thesis would not be completed without his excellent guidance. I'm grateful to him because he didn't just helped me significantly with the thesis, he also got me interested in this field of mathematics and inspired me to work on the problems.

I want to thank Professors Edlyn Teske and Kevin Hare for their comments and for their time spent on reading this thesis.

Thanks also go to Graduate Secretary Shonn Martin and Technical Secretary Lis D'Alessio for all their help and moral support.

Dedication

This thesis is dedicated to my parents who always believe in me.

Contents

Chapter 1

Introduction

The study of integral (integer) points on algebraic varieties is very old. Pythagoras tried to find integral points on $x^2 + y^2 = z^2$, Fermat tried to prove that there are no non-trivial integral points on $x^n + y^n = z^n$ if $n > 2$, and there are more examples to show that people were always interested in the study of integral points. Unfortunately the number of people who worked on problems dealing with integral points is too big to list them all in this thesis.

There are different ways to look at integral points on algebraic varieties that lead to different definitions of integral points. The idea of defining integral points through schemes (see Section 2.1 of [3] for a precise definition) is relatively new (dated mid 20th century). Even though it might not be obvious, there is a certain connection between that definition and the standard definition of integral points (see Example 1 in Section 2.2).

Brendan Hassett and Yuri Tschinkel were the first who looked at D-integral

points on algebraic varieties X where the codimension of D with respect to X is bigger than one (see [3]). In this thesis we use a simplified version of the above definition (see Definition 2 in Section 2.2) and we look at infinite sets of D-integral points on projective algebraic varieties X where the codimension of D with respect to X is two.

The thesis is organized as follows. In Chapter 2 (Background) we give background which will be essential for understanding and proving main theorems. In particular, we will talk about projective n-space, D-integral points, Zariski dense sets, and elliptic curves. We also include several lemmas that are used in the proofs of the main theorems.

Chapter 3 (Main Theorems) contains eight main theorems, which are divided in two sections.

In the first section of Chapter 3 the goal is to show that given a certain set $D \subset \mathbf{P}^n_{\mathbf{Z}}$ and a certain projective algebraic variety X, such that the codimension of D with respect to $\overline{X} \subseteq \mathbf{P}^n_{\mathbf{Z}}$ is two, there exists a finite field extension $K/\mathbf{Q}$ such that a set of D-integral points on X over K is infinite. In particular, in the first theorem we take $X = \mathbf{P}^1$ and we let D be a finite set of closed points in $\mathbf{P}^1_{\mathbf{Z}}$. In the second theorem we let X be an elliptic curve and we let D be a finite set of closed points in $\mathbf{P}^2_{\mathbf{Z}}$. Next we take a set D that consists of finitely many "lines" in $\mathbf{P}^2_{\mathbf{Z}}$ (i.e. the closures of finitely many points of $\mathbf{P}^n(\mathbf{Q})$ in $\mathbf{P}^2_{\mathbf{Z}}$), say $D = \{\overline{P_1}, \ldots, \overline{P_n}\}$ and we let X be a line in $\mathbf{P}^2$ that does not go through any of the points $P_1, \ldots, P_n$. Since in this case it is possible to find a finite set D' of closed points in $\mathbf{P}^2_{\mathbf{Z}}$, such that $P \in X(K)$ is D-integral if and only if $P \in X(K)$ is D'-integral, the above problem

is equivalent to letting D be a finite set of closed points in $\mathbf{P}^2_{\mathbf{Z}}$ and X a line in $\mathbf{P}^2$. Finally, we show that given a finite set D of "lines" in $\mathbf{P}^2_{\mathbf{Z}}$, we can find a Zariski dense set in $\mathbf{P}^2(K)$ of D-integral points.

In the second section of Chapter 3 we show that for four different types of D, where D is a finite set of "lines" in $\mathbf{P}^2_{\mathbf{Z}}$, we can find an explicit description of the complete set of D-integral points in $\mathbf{P}^2(\mathbf{Q})$. In particular, we start with the case where the set D contains the closure of only one point. Then we take D that contains the closures of two points that are not congruent to each other modulo any prime p. Next we take two points that are congruent modulo p for only finitely many primes p and not congruent modulo p^2 for any prime p, and we let D consist of the closures of the points. We conclude the section by taking the set D consisting of the closures of three points, such that the points are not congruent to each other at the same time modulo any prime p and the matrix, columns of which correspond to the points, has a square-free determinant.

Chapter 4 contains the conclusion of the thesis.

Chapter 2

Background

2.1 Projective n-space

Since throughout the thesis we are working in projective space, we start with defining projective n-space.

Definition 1. *Let K be a field. We define projective n-space over K, denoted by $\mathbf{P}^n$ or $\mathbf{P}^n(K)$, to be the set of equivalence classes of $(n+1)$-tuples $(a_1, \ldots, a_{n+1})$ of elements of K, not all zero, under the equivalence relation given by $(a_1, \ldots, a_{n+1}) \sim (\lambda a_1, \ldots, \lambda a_{n+1})$ for all $\lambda \in K, \lambda \neq 0$ (see Section I.2 of [2]).*

An element of $\mathbf{P}^n(K)$ is called a point in $\mathbf{P}^n(K)$.

Since the introduction of schemes is not necessary for the contents of the thesis, we adjust the definitions of $\mathbf{P}^n_{\mathcal{O}_k}$ (see Section I.2.4 of [1] for the original definition) and integral points (see Section 2.1 of [3] for the original definition) to meet the needs of the thesis.

From now on, K is a number field.

First, let's take $K = \mathbf{Q}$, then the ring of integers of K denoted by $\mathcal{O}_K$ is $\mathbf{Z}$. We define $\mathbf{P}^n_{\mathbf{Z}} = (\coprod_{(p)} \mathbf{P}^n(\mathbf{Z}/p\mathbf{Z})) \coprod \mathbf{P}^n(\mathbf{Q})$, where $\coprod$ denotes a union and (p) runs over all prime ideals of $\mathbf{Z}$. An element of $\mathbf{P}^n_{\mathbf{Z}}$ is called a closed point, if it is in the form $(P \bmod (p))$ denoted by $(P, (p))$, where $P \in \mathbf{P}^n(\mathbf{Q})$ and (p) is a prime ideal of $\mathbf{Z}$. Given a point $P \in \mathbf{P}^n(\mathbf{Q})$, we define the closure of P in $\mathbf{P}^n_{\mathbf{Z}}$ to be $\overline{P} = (\cup_{(p)}\{(P, (p))\}) \cup \{P\}$, where (p) runs over all prime ideals of $\mathbf{Z}$. The following argument shows that $\overline{P}$ is well defined for all $P \in \mathbf{P}^n(\mathbf{Q})$.

Since points $[a_1 : \ldots : a_{n+1}]$ and $[\lambda a_1 : \ldots : \lambda a_{n+1}]$ are the same in $\mathbf{P}^n(K)$ for any non-zero $\lambda \in K$, then in particular when $K = \mathbf{Q}$, we take each point $P \in \mathbf{P}^n(\mathbf{Q})$ and first multiply coordinates of P by the LCM of the denominators, then we divide the new coordinates of P by the GCD of the coordinates and the representation (also called reduced form) that we get for each point in $\mathbf{P}^n(\mathbf{Q})$ is $[a_1 : \ldots : a_{n+1}]$, where $a_1, \ldots, a_{n+1} \in \mathbf{Z}$ and $\gcd(a_1, \ldots, a_{n+1}) = 1$. Thus any point $P \in \mathbf{P}^n(\mathbf{Q})$ is non-zero when we reduce it modulo any prime ideal $(p) \subset \mathbf{Z}$, and the closure of P in $\mathbf{P}^n_{\mathbf{Z}}$ is well defined for each point $P \in \mathbf{P}^n(\mathbf{Q})$.

Note that throughout the thesis when we take a point in $\mathbf{P}^n(\mathbf{Q})$, we assume it is in reduced form.

Similarly, for an arbitrary field K we define $\mathbf{P}^n_{\mathcal{O}_K} = (\coprod_J \mathbf{P}^n(\mathcal{O}_K/J)) \coprod \mathbf{P}^n(K)$, where $\coprod$ denotes a union and J runs over all prime ideals of $\mathcal{O}_K$. An element of $\mathbf{P}^n_{\mathcal{O}_K}$ is called a closed point, if it is in the form $(P \bmod J)$ denoted by (P, J), where $P \in \mathbf{P}^n(K)$ and J is a prime ideal of $\mathcal{O}_K$. Given a point $P \in \mathbf{P}^n(K)$, we define the closure of P in $\mathbf{P}^n_{\mathcal{O}_K}$ to be $\overline{P} = (\cup_J\{(P, J)\}) \cup \{P\}$, where J runs over all prime

ideals of $\mathcal{O}_K$. The following argument shows that $\overline{P}$ is well defined for all points P in $\mathbf{P}^n(K)$.

For a prime ideal $J \subset \mathcal{O}_K$ and $a_i \in K$ let $\mathrm{ord}_J(a_i) = \max\{m \in \mathbf{Z} | a_i \in J^m\}$. For each prime ideal $J \subset \mathcal{O}_K$ there exists a uniformizer $t_J \in \mathcal{O}_K$ with $\mathrm{ord}_J(t_J) = 1$, such that every element of K can be written as $a_i = t_J^{m_i} u_i$, where u_i is a unit (i.e. $\mathrm{ord}_J(u_i) = 0$) and $m_i \in \mathbf{Z}$. Thus every point in $\mathbf{P}^n(K)$ can be written as $P = [u_1 t_J^{m_1} : \ldots : u_{n+1} t_J^{m_{n+1}}]$. Since we work in projective space, P does not change when we divide each coordinate by the smallest power of t_J. Thus at least one coordinate of P is a unit, i.e. non-zero modulo J, and $P \bmod J$ is well defined. Since this is true for each prime ideal $J \subset \mathcal{O}_K$ and each point $P \in \mathbf{P}^n(K)$, the closure of P in $\mathbf{P}^n_{\mathcal{O}_K}$ is well defined for all points P in $\mathbf{P}^n(K)$.

Throughout the thesis when we say $P \in \mathbf{P}^n(K)$ is congruent to $(P_i, J) \in \mathbf{P}^n_{\mathcal{O}_K}$, we mean that $P \equiv P_i \bmod J$.

2.2 D-integral Points on Algebraic Varieties

There are different ways to define integral points on algebraic varieties, the definition of integral points that is used in the thesis is the following:

Definition 2. *Let $X(K) \subseteq \mathbf{P}^n(K)$ be a projective algebraic variety (see Definition 3 in Section 2.3) over a field K, and let D be a subset of $\mathbf{P}^n_{\mathcal{O}_K}$. We say a point $P \in X(K)$ is D-integral if $\overline{P} \bigcap D = \emptyset$ in $\mathbf{P}^n_{\mathcal{O}_K}$.*

Lemma 1. *Let P be a point in $\mathbf{P}^n(\mathbf{Q})$ and Q be a point in $\mathbf{P}^n(K)$ where $K/\mathbf{Q}$ is a finite field extension. Assume that $P \not\equiv Q \bmod (p)$ for some prime p in $\mathbf{Z}$. Then*

for all prime ideals $J \subset \mathcal{O}_K$ lying over (p), $P \not\equiv Q \bmod J$.

Proof: Let L be the Galois closure of $K/\mathbf{Q}$. Each prime ideal $J \subset \mathcal{O}_K$ can be written as $J = I_1 \cdots I_d$ where each I_i is a prime ideal of $\mathcal{O}_L$. Then $(p) = I_1 \cdots I_h$ for prime ideals I_ℓ of $\mathcal{O}_L$. Thus to show that $P \not\equiv Q \bmod J$ for all the prime ideals $J \subset \mathcal{O}_K$ lying over (p), it is enough to show that $P \not\equiv Q \bmod I_\ell$ for any prime ideal $I_\ell \subset \mathcal{O}_L$ lying over (p).

Since $P \not\equiv Q \bmod (p)$, there exists at least one ℓ such that $P \not\equiv Q \bmod I_\ell$. By Proposition I.11 of [4] we know that for any $1 \leq m \leq h$, there exists an automorphism $\sigma \in \mathrm{Gal}(L/Q)$ such that $\sigma(I_\ell) = I_m$. Then

$$P \not\equiv Q \bmod I_\ell \Longrightarrow \sigma(P) \not\equiv \sigma(Q) \bmod \sigma(I_\ell).$$

Since $P \in \mathbf{P}^n(\mathbf{Q})$ and $\mathbf{Q}$ is fixed by σ, then $\sigma(P) = P$. Thus

$$P \not\equiv \sigma(Q) \bmod I_m.$$

If $\sigma(Q) \equiv Q \bmod I_m$, we are done. If $\sigma(Q) \not\equiv Q \bmod I_m$, then Q is not fixed by the action of $\mathrm{Gal}(L/\mathbf{Q})$ on $\mathbf{P}^n(\mathcal{O}_K/I_m)$, but P is fixed, so $P \not\equiv Q \bmod I_m$.

This completes the proof.

Now, in all our theorems, D is a subset of $\mathbf{P}^n_{\mathbf{Z}}$. In particular in the first two theorems D consists of finitely many closed points, i.e. $D = \{(P_1, (p_1)), \ldots, (P_m, (p_m))\}$. Since we are interested in finding D-integral points on X over a finite extension field $K \subset \overline{\mathbf{Q}}/\mathbf{Q}$, we need to check if $\overline{P}$ intersects D in $\mathbf{P}^n_{\mathcal{O}_K}$. Unfortunately, (p)

does not have to be a prime ideal of $\mathcal{O}_K$ and therefore D does not have to be a subset of $\mathbf{P}^n_{\mathcal{O}_K}$, so we need to change the set D, in particular we need to substitute each $(P_i, (p_i))$ with $(P_i, J_{i1}), \ldots, (P_i, J_{ik})$, where the J_{ij} are prime ideals lying over (p_i) in $\mathcal{O}_K$. However, Lemma 1 shows that if $P \not\equiv P_i \bmod p_i$, then $P \not\equiv P_i \bmod J_{ij}$ for all the J_{ij}. Thus to show that $P \in X(K)$ is D-integral, it is enough to show that $P \not\equiv P_i \bmod (p_i)$, for all $1 \leq i \leq m$.

In Theorems 3 and 4, D consists of finitely many "lines" in $\mathbf{P}^n_{\mathbf{Z}}$, i.e. given a finite number of points $P_1, \ldots P_m \in \mathbf{P}^n(\mathbf{Q})$, we take the closure of each of the points in $\mathbf{P}^n_{\mathbf{Z}}$. Since we are interested in finding D-integral points on X over a finite extension field $K \subset \overline{\mathbf{Q}}/\mathbf{Q}$, we want to find points such that $P \not\equiv P_i \bmod J$ for all $1 \leq i \leq m$ and all prime ideals $J \subset \mathcal{O}_K$. Now, each prime ideal J of $\mathcal{O}_K$ lies over some prime ideal (p) in $\mathbf{Z}$ and since each $P_i \in \mathbf{P}^2(\mathbf{Q})$, Lemma 1 proves that if $P \not\equiv P_i \bmod (p)$, where $(p) \subset \mathbf{Z}$, then P is not congruent to P_i modulo all prime ideals of $\mathcal{O}_K$ lying over (p) and in particular $P \not\equiv P_i \bmod J$. Thus if $P \not\equiv P_i \bmod (p)$ for all $1 \leq i \leq m$ and all prime ideals $(p) \subset \mathbf{Z}$, then $P \not\equiv P_i \bmod J$ for all $1 \leq i \leq m$ and all prime ideals $J \subset \mathcal{O}_K$, i.e. P is D-integral.

In Theorems 5, 6, 7 and 8, D consists of finitely many "lines" in $\mathbf{P}^n_{\mathbf{Z}}$, say $D = \{\overline{P_1}, \ldots, \overline{P_m}\}$, and we are interested in finding D-integral points in $\mathbf{P}^n(\mathbf{Q})$. Then $P \in \mathbf{P}^n(\mathbf{Q})$ is D-integral implies that $P \not\equiv P_i \bmod (p)$ for all $1 \leq i \leq m$ and all primes p in $\mathbf{Z}$.

Since saying $P \not\equiv P_i \bmod (p)$, is equivalent to saying $P \not\equiv P_i \bmod p$, for all primes p in $\mathbf{Z}$, we will use the second notation in the second section of Chapter 3. Also throughout the thesis when we say a prime we really mean a prime in $\mathbf{Z}$.

The following example shows a connection between the above definition and the standard definition of integral points.

Example 1 Take a cubic curve $C : y^2 = x^3 + 1$. Then (x, y) is integral on C if $(x, y) \in \mathbf{Z}^2$ satisfies $y^2 = x^3 + 1$.

In projective space C corresponds to homogeneous cubic curve $C_h : y^2z = x^3 + z^3$, and clearly,

$$\begin{gathered}(x, y) \text{ is integral on } C \\ \Longleftrightarrow \\ [x : y : z] \in C_h(\mathbf{Q}) \text{ (in reduced form) and } z = 1 \\ \Longleftrightarrow \\ [x : y : z] \in C_h(\mathbf{Q}) \text{ and } [x : y : z] \not\equiv [a : b : 0] \bmod p \\ \text{for any } a, b \in \mathbf{Z} \text{ and any prime } p \in \mathbf{Z}.\end{gathered}$$

Since there is only one point at infinity on C_h modulo any prime p, the above statement is equivalent to

$$\begin{gathered}(x, y) \text{ is integral on } C \\ \Longleftrightarrow \\ [x : y : z] \in C_h(\mathbf{Q}) \text{ and } [x : y : z] \not\equiv [0 : 1 : 0] \bmod p \text{ for any prime } p.\end{gathered}$$

Thus if we let $D = \{\overline{[0 : 1 : 0]}\}$, then (x, y) is integral on C if and only if $[x : y : z] \in C_h(\mathbf{Q})$ is D-integral.

2.3 Zariski Dense Sets

First we will start with the definition of a Zariski closed subset of $\mathbf{P}^n$.

Definition 3. *A set V is called a Zariski closed subset of $\mathbf{P}^n$ if V is the common zero set of finitely many homogeneous polynomials in $n+1$ variables. V is also called a projective algebraic variety.*

Let S be a subset of $\mathbf{P}^n$. The smallest Zariski closed subset of $\mathbf{P}^n$ that contains S is defined to be the Zariski closure of S, and we denote it by $\overline{S}$.

Now we can define a Zariski dense set.

Definition 4. *Let V be a Zariski closed subset of $\mathbf{P}^n$, and let S be a subset of V. Then the set S is called a Zariski dense set in V if the Zariski closure of S is V.*

We will need the following lemma in the proof of Theorem 4. In this lemma we show one of the conditions when a subset of $\mathbf{P}^2$ is Zariski dense in $\mathbf{P}^2$.

Lemma 2. *Let $S \subset \mathbf{P}^2$ be any subset. Assume that there exists an infinite collection $\mathcal{C}$ of curves such that for all $C \in \mathcal{C}$, $S \cap C$ is infinite. Then S is Zariski dense in $\mathbf{P}^2$.*

Proof: Let $Z = \overline{S}$. Assume that $Z \neq \mathbf{P}^2$; then there exists a finite set of irreducible curves $B_1, B_2, \ldots, B_n$ (i.e. each B_i is defined by the zero set of a single irreducible homogeneous polynomial in $\mathbf{P}^2$) such that $S \subset \bigcup_i B_i$. Choose $C \in \mathcal{C}$ such that $C \neq B_i$ for all i. Then $\bigcup_i (C \cap B_i)$ is finite. This follows from the fact that if B_i is irreducible and $C \neq B_i$ then $C \cap B_i$ is finite. On another hand, $(C \cap S) \subset \bigcup_i (C \cap B_i)$ and we know that $(C \cap S)$ is infinite. This gives us the desired contradiction. Therefore $Z = \mathbf{P}^2$, which implies that the set S is Zariski dense in $\mathbf{P}^2$.

This completes the proof.

2.4 Elliptic Curves

An elliptic curve is a curve of genus 1 with a specified basepoint. By section III.3 of [6] every such curve can be written as a plane cubic, so we can define an elliptic curve in the following way.

Definition 5. *An elliptic curve over a field K, denoted by $E(K)$ is the zero set of a smooth cubic homogeneous polynomial in $\mathbf{P}^2$ with a K-rational point.*

If char(K)$\neq 2, 3$, then every elliptic curve $E(K)$ can be written by a Weierstrass Equation in the form $y^2z = f(x, z)$, where $f(x, z)$ is a cubic homogeneous polynomial with distinct roots (see Section III.1 of [6]). Since throughout the thesis char(K)$= 0$, from now on when we talk about an elliptic curve $E(K)$, we assume it is expressed in the above form.

The Group Law on Elliptic Curves

Let $E(K)$ be an elliptic curve given by a Weierstrass equation. Let $L \subset \mathbf{P}^2$ be a line. Then since $E(K)$ has degree three and L has degree one, using a special case of Bezout's Theorem we can conclude that L intersects $E(K)$ at exactly 3 points P, Q, R (if L is a tangent line to $E(K)$, then P, Q, R may not be distinct). Define a composition law on $E(K)$ by the following rule:

Composition Law (Section III.2 of [6]): Let $E(K)$ be an elliptic curve given by a Weierstrass equation and let I be the point at infinity that satisfies the equation of $E(K)$. Given two points $P, Q \in E(K)$, connect the points with line $L \subset \mathbf{P}^2$ to get a point R which is the third point of intersection of L with $E(K)$. Now, let $L' \in \mathbf{P}^2$

be the line connecting R and I. Then $P+Q$ is the point such that L' intersects $E(K)$ at R, I and $P+Q$.

The composition law makes $E(K)$ into an abelian group with identity element I (see Proposition 2.2 Section III.2 of [6] for the proof).

We will need the next lemma in the proof of Theorem 2.

Lemma 3. *Let K be a number field, $\mathcal{O}_K$ be the ring of integers and $J \subset \mathcal{O}_K$ be a nonzero prime ideal, which implies that J is maximal and $\mathcal{O}_K/J$ is a field, denoted by $k(J)$. Let J be a bad prime ideal of an elliptic curve $E(K)$, i.e. $E(k(J))$ is a singular curve. Then $E(k(J))$ has exactly one singular point S, and $E_J = E(k(J)) - \{S\}$ is a group under the same group law as $E(K)$ restricted modulo J. Formally, we let $E_o(K) = \{P \in E(K) | P \not\equiv S \bmod J\}$. Then $E_o(K)$ is a subgroup of $E(K)$ and*

$$\begin{array}{ccc} E_o(K) \times E_o(K) & \xrightarrow{m} & E_o(K) \\ \downarrow & & \downarrow \\ E_J \times E_J & \xrightarrow{m'} & E_J \end{array}$$

commutes where m and m' are the composition laws defined above.

Proof: First we show that if J is a bad prime ideal of $E(K)$, then $E(k(J))$ has exactly one singular point.

Bezout's Theorem says that if we have two curves with no common factors of degree m and n, then the curves intersect in at most mn points counted with

multiplicities. Thus an elliptic curve and a line can intersect in at most 3 points counted with multiplicities.

Now, if J is a bad prime ideal of $E(K)$, it implies that $E(k(J))$ has at least one singular point. Assume that $E(k(J))$ has two singular points. Then the multiplicities of these points are greater or equal to 2 (as the dimension of $E(k(J))$ is 1). When we join these points with a line, the intersection of the line and the elliptic curve $E(k(J))$ has at least 4 points of intersection counted with multiplicities, which is a contradiction to Bezout's Theorem. Therefore $E(k(J))$ has exactly one singular point.

It is left to show that E_J is a group under the same group law as $E(K)$ restricted mod$J$. The result follows from Proposition III.2.5 of [6].

This completes the proof.

2.5 Important Lemmas

The following lemma is required for the proof of Theorem 5, 6, 7 and 8. We will prove that given a linear change of coordinates T defined by a 3x3 matrix that is invertible modulo prime p, two points are congruent modulo p if and only if their images under T are congruent modulo p.

Lemma 4. *Let M be a 3×3 matrix with coordinates in $\mathbf{Q}$, such that $\det(M) \not\equiv 0 \bmod p$ where p is a prime in $\mathbf{Z}$. Let $T : \mathbf{P}^2(\mathbf{Q}) \longrightarrow \mathbf{P}^2(\mathbf{Q})$ be the linear change of*

coordinates defined by the matrix M. Then

$$[a:b:c] \equiv [x:y:z] \bmod p \Longleftrightarrow T([a:b:c]) \equiv T([x:y:z]) \bmod p.$$

Proof: Since $\det(M) \neq 0$, the linear change of coordinates $T : \mathbf{P}^2(\mathbf{Q}) \longrightarrow \mathbf{P}^2(\mathbf{Q})$ is an isomorphism and since $\det(M) \not\equiv 0 \bmod p$, the linear change of coordinates $T_p : \mathbf{P}^2(\mathbf{Z}/p\mathbf{Z}) \longrightarrow \mathbf{P}^2(\mathbf{Z}/p\mathbf{Z})$ is an isomorphism as well. Then

$$[a:b:c] \equiv [x:y:z] \bmod p \Longleftrightarrow T_p([a:b:c]) \equiv T_p([x:y:z]) \bmod p.$$

It is clear that $T_p([a:b:c]) \equiv T([a:b:c]) \bmod p$, therefore

$$[a:b:c] \equiv [x:y:z] \bmod p \Longleftrightarrow T([a:b:c]) \equiv T([x:y:z]) \bmod p.$$

This completes the proof.

We will use the next lemma in the proof of Theorem 7 and 8. The idea in this lemma is the following. Consider a linear transformation $T : \mathbf{Z}^3 \longrightarrow \mathbf{Z}^3$ defined by a 3x3 matrix M, and a point (x, y, z) with $\gcd(x, y, z) = 1$. Then setting $(a, b, c) = T(x, y, z)$, gives that $\gcd(a, b, c)$ divides the determinant of M.

Lemma 5. *Given a matrix* $M = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$ *with coordinates in* $\mathbf{Z}$, *and integers*

x, y, z *such that* $\gcd(x, y, z) = 1$. *Let*

$$g = \gcd(xa_1 + ya_2 + za_3, xb_1 + yb_2 + zb_3, xc_1 + yc_2 + zc_3).$$

Then g *divides the determinant of* M.

Proof: Let $T : \mathbf{Z}^3 \longrightarrow \mathbf{Z}^3$ be the linear transformation defined by the matrix M. Then $T(x, y, z) = (xa_1 + ya_2 + za_3, xb_1 + yb_2 + zb_3, xc_1 + yc_2 + zc_3) = (gx', gy', gz')$. Then

$$\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} gx' \\ gy' \\ gz' \end{bmatrix}$$

Using Cramer's Rule we get

$$x = \frac{gx'(b_2c_3 - c_2b_3) - gy'(a_2c_3 - c_2a_3) + gz'(a_2b_3 - b_2a_3)}{\det(M)}$$

$$y = \frac{-gx'(b_1c_3 - c_1b_3) + gy'(a_1c_3 - c_1a_3) - gz'(a_1b_3 - b_1a_3)}{\det(M)}$$

$$z = \frac{gx'(b_1c_2 - c_1b_2) - gy'(a_1c_2 - c_1a_2) + gz'(a_1b_2 - b_1a_2)}{\det(M)}$$

$\Longrightarrow$

$$x = \frac{g(x'(b_2c_3 - c_2b_3) - y'(a_2c_3 - c_2a_3) + z'(a_2b_3 - b_2a_3))}{\det(M)}$$

$$y = \frac{g(-x'(b_1c_3 - c_1b_3) + y'(a_1c_3 - c_1a_3) - z'(a_1b_3 - b_1a_3))}{\det(M)}$$

$$z = \frac{g(x'(b_1c_2 - c_1b_2) - y'(a_1c_2 - c_1a_2) + z'(a_1b_2 - b_1a_2))}{\det(M)}.$$

Since $\gcd(x, y, z) = 1$, then g has to divide $\det(M)$.

This completes the proof.

We will need the following lemma in the proof of Theorem 7. In this lemma we prove the following fact. Let D consist of the closures of two points $P_1, P_2 \in \mathbf{P}^2(\mathbf{Q})$ that are only congruent to each other modulo finitely many primes, say $p_1, \ldots, p_n$, and not congruent modulo p^2 for any prime p. Then we can always find a D-integral point $P \in \mathbf{P}^2(\mathbf{Q})$ such that the matrix, whose columns are P_1, P_2 and P has determinant $p_1 \cdots p_n$.

Lemma 6. *Let $P_1 = [a_1 : b_1 : c_1], P_2 = [a_2 : b_2 : c_2] \in \mathbf{P}^2(\mathbf{Q})$ be two points such that $P_1 \equiv P_2 \bmod p_i$ only for finitely many primes, say $p_1, \ldots, p_n$, and $P_1 \not\equiv P_2 \bmod p_i^2$ for all $1 \leq i \leq n$. Let $D = \{\overline{P_1}, \overline{P_2}\}$. It is always possible to find integers A, B, C with $\gcd(A, B, C) = 1$ such that*

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = p_1 \cdots p_n$$

and $[A : B : C]$ *is D-integral in* $\mathbf{P}^2(\mathbf{Q})$.

Proof: Since $[a_1 : b_1 : c_1] \equiv [a_2 : b_2 : c_2] \bmod p_i$ for only $1 \leq i \leq n$ and $[a_1 : b_1 : c_1] \not\equiv [a_2 : b_2 : c_2] \bmod p_i^2$ for $1 \leq i \leq n$, this implies that

$$\gcd(a_1b_2 - b_1a_2, a_1c_2 - c_1a_2, b_1c_2 - c_1b_2) = p_1 \cdots p_n.$$

Thus we can always find integers A, B, C such that

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = p_1 \cdots p_n.$$

Moreover, for all such $[A : B : C]$, we have $\gcd(A, B, C) = 1$. Next we note that

$$p_1 \cdots p_n = A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2)$$

$$= -a_2(b_1C - c_1B) + b_2(a_1C - c_1A) - c_2(a_1B - b_1A)$$

$$= a_1(b_2C - c_2B) - b_1(a_2C - c_2A) + c_1(a_2B - b_2A)$$

$\Longrightarrow$

$$\gcd(b_1C - c_1B, a_1C - c_1A, a_1B - b_1A) | p_1 \cdots p_n$$

$\Longrightarrow$

$$[A : B : C] \equiv [a_1 : b_1 : c_1] \bmod p \text{ is possible only for } p | p_1 \cdots p_n.$$

Similarly,

$$[A : B : C] \equiv [a_2 : b_2 : c_2] \bmod p \text{ is possible only for } p | p_1 \cdots p_n.$$

So we can conclude that all the integer triples A, B, C that satisfy the above equation, have the property that $[A : B : C] \not\equiv [a_1 : b_1 : c_1] \bmod p$ and $[A : B : C] \not\equiv [a_2 : b_2 : c_2] \bmod p$ for all primes p that do not divide $p_1 \cdots p_n$.

Since $P_1 \equiv P_2 \bmod p_i$ for all $1 \leq i \leq n$, we only need to show that we can find $[A : B : C]$ such that $[A : B : C] \not\equiv [a_1 : b_1 : c_1] \bmod p_i$ for all $1 \leq i \leq n$.

First let's fix $i \in \{1, \ldots, n\}$ and look at the case when $P_1 \equiv P_2 \equiv [0 : 1 : 0] \bmod p_i$. This implies that

$$b_1 c_2 - c_1 b_2 = p_i k_1$$

$$a_1 c_2 - c_1 a_2 = p_i^2 k_2$$

$$a_1 b_2 - b_1 a_2 = p_i k_3.$$

Then

$$A(b_1 c_2 - c_1 b_2) - B(a_1 c_2 - c_1 a_2) + C(a_1 b_2 - b_1 a_2) =$$

$$= A p_i k_1 - B p_i^2 k_2 + C p_i k_3 = p_1 \cdots p_n.$$

This implies that p_i^2 does not divide $\gcd(A p_i k_1, C p_i k_3)$ and thus p_i does not divide $\gcd(A, C)$. Therefore, $[A : B : C] \not\equiv [a_1 : b_1 : c_1] \equiv [0 : 1 : 0] \bmod p_i$ for any integer

triple that satisfies

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = p_1 \cdots p_n.$$

We now consider the case when $P_1 \equiv P_2 \not\equiv [0:1:0] \bmod p_i$. If (A, B, C) is a solution to

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = p_1 \cdots p_n$$

then $(A + k\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n}, B + k\frac{b_1c_2 - c_1b_2}{p_1 \cdots p_n} + h\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n}, C + h\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n})$ is also a solution to the equation for any integers k and h.

We compute:

$$[A + k\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n} : B + k\frac{b_1c_2 - c_1b_2}{p_1 \cdots p_n} + h\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n} : C + h\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n}]$$

$$\equiv [a_1 : b_1 : c_1] \bmod p_i$$

$$\Longleftrightarrow$$

$$(A + k\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n})b_1 - (B + k\frac{b_1c_2 - c_1b_2}{p_1 \cdots p_n} + h\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n})a_1 \equiv 0 \bmod p_i$$

$$(A + k\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n})c_1 - (C + h\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n})a_1 \equiv 0 \bmod p_i$$

$$(B + k\frac{b_1c_2 - c_1b_2}{p_1 \cdots p_n} + h\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n})c_1 - (C + h\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n})b_1 \equiv 0 \bmod p_i$$

$$\Longleftrightarrow$$

$$(Ab_1 - Ba_1) + (kc_1 - ha_1)\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n} \equiv 0 \bmod p_i$$

$$(Ac_1 - Ca_1) + (kc_1 - ha_1)\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n} \equiv 0 \bmod p_i$$

$$(Bc_1 - Cb_1) + (kc_1 - ha_1)\frac{b_1c_2 - b_1a_2}{p_1 \cdots p_n} \equiv 0 \bmod p_i.$$

We need to look at two cases:

Case 1: $[A : B : C] \equiv [a_1 : b_1 : c_1] \bmod p_i$.

In this case the above system of congruences implies that

$$(kc_1 - ha_1)\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n} \equiv 0 \bmod p_i$$

$$(kc_1 - ha_1)\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n} \equiv 0 \bmod p_i$$

$$(kc_1 - ha_1)\frac{b_1c_2 - b_1a_2}{p_1 \cdots p_n} \equiv 0 \bmod p_i$$

$\Longrightarrow$

$(kc_1 - ha_1) \equiv 0 \bmod p_i$, since $\gcd(\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n}, \frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n}, \frac{b_1c_2 - b_1a_2}{p_1 \cdots p_n}) = 1.$

Thus, if we can find integers k and h such that $(kc_1 - ha_1) \not\equiv 0 \bmod p_i$, then $[A + k\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n} : B + k\frac{b_1c_2 - c_1b_2}{p_1 \cdots p_n} + h\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n} : C + h\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n}] \not\equiv [a_1 : b_1 : c_1] \bmod p_i$.

This is always possible since $P_1 \not\equiv [0:1:0] \bmod p_i$ which implies that $a_1 \equiv c_i \equiv 0 \bmod p_1$ does not happen.

Case 2: $[A:B:C] \not\equiv [a_1:b_1:c_1] \bmod p_i$.

In this case we can choose integers k and h such that $k \equiv h \equiv 0 \bmod p_i$, then $[A + k\frac{a_1c_2-c_1a_2}{p_1\cdots p_n} : B + k\frac{b_1c_2-c_1b_2}{p_1\cdots p_n} + h\frac{a_1b_2-b_1a_2}{p_1\cdots p_n} : C + h\frac{a_1c_2-c_1a_2}{p_1\cdots p_n}] \not\equiv [a_1:b_1:c_1] \bmod p_i$.

Now, we go back to the beginning and we find $[A:B:C]$ such that

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = p_1 \cdots p_n.$$

Next, we compute $g = \gcd(b_1C - c_1B, a_1C - c_1A, a_1B - b_1A)$. If $g = 1$ then $[A:B:C]$ is D-integral and we are done. If $g \neq 1$, then we divide primes p_i into two sets:

$$V = \{p_i | 1 \leq i \leq n \text{ and } p_i \text{ divides } g\}$$

$$W = \{p_i | 1 \leq i \leq n \text{ and } p_i \text{ does not divide } g\}.$$

Using the Chinese Remainder Theorem (CRT) we can find integers k and h such that

$$(kc_1 - ha_1) \not\equiv 0 \bmod p_i \text{ for all the } p_i \in V$$

and

$$k \equiv h \equiv 0 \bmod p_i \text{ for all the } p_i \in W.$$

Then point $[A + k\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n} : B + k\frac{b_1c_2 - c_1b_2}{p_1 \cdots p_n} + h\frac{a_1b_2 - b_1a_2}{p_1 \cdots p_n} : C + h\frac{a_1c_2 - c_1a_2}{p_1 \cdots p_n}]$ satisfies

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = p_1 \cdots p_n$$

and is D-integral in $\mathbf{P}^2(\mathbf{Q})$.

This completes the proof.

Chapter 3

Main Theorems

3.1 Infinite Sets of D-integral Points on Algebraic Varieties over K

In this section we show that for certain types of $D \subset \mathbf{P}^n_{\mathbf{Z}}$ and projective algebraic varieties $X \subseteq \mathbf{P}^n$, there is a finite field extension $K/\mathbf{Q}$, such that $X(K)$ contains infinitely many D-integral points.

We start the section by showing that given a finite set D of closed points in $\mathbf{P}^1_{\mathbf{Z}}$, there is a finite field extension $K/\mathbf{Q}$ such that there are infinitely many D-integral points on $\mathbf{P}^1(K)$.

Theorem 1. *Let $D \subset \mathbf{P}^1_{\mathbf{Z}}$ be a finite set of closed points; that is $D = \{([a_1 : b_1], (p_1)), ([a_2 : b_2], (p_2)), \ldots, ([a_n : b_n], (p_n))\}$. Then there is a finite field extension $K/\mathbf{Q}$ such that there are infinitely many D-integral points on $\mathbf{P}^1(K)$.*

Proof: It follows from Section 2.2 that to show that $[A : B]$ is D-integral it is enough to show that $[A \ : \ B \ ] \not\equiv [a_i : b_i] \bmod (p_i)$ for all $1 \leq i \leq n$.

A point $[A : B]$ is not congruent to points $([a_i : b_i], (p_i))$ for all $1 \leq i \leq n$ implies that

$$Ab_i - Ba_i \not\equiv 0 \bmod (p_i) \text{ for all } 1 \leq i \leq n.$$

If such point exists, then there are infinitely many points in the form

$$[A + lp_1p_2 \cdots p_n : B + kp_1p_2 \cdots p_n], \text{ where } l, k \in \mathbf{Z}$$

which are not congruent to any points in set D, as

$$(A + lp_1p_2 \cdots p_n)b_i - (B + kp_1p_2 \cdots p_n)a_i \equiv Ab_i - Ba_i \bmod (p_i), 1 \leq i \leq n.$$

Thus, if we can show that there exists at least one point with the above property, we are done.

Let's choose a point $[C : 1]$. Then $[C : 1] \not\equiv [a_i : b_i] \bmod p_i$ if $b_i \equiv 0 \bmod p_i$, so we can remove for now the points $([a_i, b_i], (p_i))$ with $b_i \equiv 0 \bmod p_i$ from the set D. Since b_i^{-1} exists modulo p_i for all the p_i in our new set D, we want to find C such that for all the p_i

$$Cb_i - a_i \not\equiv 0 \bmod p_i$$

$$\Longleftrightarrow$$

$$C \not\equiv a_ib_i^{-1} \bmod p_i.$$

Therefore, if we can find C in some finite field extension $K/\mathbf{Q}$ that is not an element of $\mathbf{Z}/p_i\mathbf{Z}$ for all the p_i, we are done.

For each of the distinct odd p_i we choose $A_i \in \mathbf{Z}/p_i\mathbf{Z}$ such that A_i is not a quadratic residue modulo p_i. We are guaranteed to find such A_i, as there are at most $\frac{m-1}{2}$ quadratic residues, where $m = |\mathbf{Z}/p_i\mathbf{Z}|$. By the CRT there exists $h \in \mathbf{Z}$ such that $h \equiv A_i \bmod (p_i)$ for all the distinct odd p_i and $h \equiv 5 \bmod (8)$. If none of the p_i is equal to 2, we let $C = \sqrt{h}$. If $p_i = 2$ for some i, then let $C = \frac{1+\sqrt{h}}{2}$. Clearly C is not in $\mathbf{Z}/p_i\mathbf{Z}$ for all the odd p_i. The minimal polynomial for $\frac{1+\sqrt{h}}{2}$ is $x^2 - x + 1 - 2d$ (where $h = 5 + 8d, d \in \mathbf{Z}$), which reduces to $x^2 - x + 1$ modulo 2; thus C is congruent to a root of $x^2 - x + 1 = 0$ modulo (2), which is not in $\mathbf{Z}/2\mathbf{Z}$ and, therefore, C is not in $\mathbf{Z}/2\mathbf{Z}$. Then C is defined over $\mathbf{Q}(\sqrt{h})$ and is not defined over $\mathbf{Z}/p_i\mathbf{Z}$ for all the p_i.

Let $K = \mathbf{Q}(\sqrt{h})$. Then $[C : 1] \in \mathbf{P}^1(K)$ is D-integral.

This completes the proof.

In the following theorem we take a set D that consists of finitely many closed points in $\mathbf{P}^2_{\mathbf{Z}}$ and an elliptic curve E. We show that there is a finite field extension $K/\mathbf{Q}$ such that there are infinitely many D-integral points on $E(K)$.

Theorem 2. *Let D be a finite set of closed points in $\mathbf{P}^2_Z$. That is $D = \{([a_1 : b_1 : c_1], (p_1)), ([a_2 : b_2 : c_2]), (p_2)), \ldots, ([a_n : b_n : c_n], (p_n))\}$. Let $E : y^2z = f(x, z)$ be an elliptic curve, where $f(x, z)$ is a cubic homogeneous polynomial with distinct roots. Then there is a finite field extension $K/\mathbf{Q}$ such that there are infinitely many D-integral points on $E(K)$.*

Proof: First we will find a point P on $E(K)$ such that P is D-integral, $P \bmod p_i$ is not singular on $E(k(J_{ij}))$ for all the prime ideals $J_{ij} \subset \mathcal{O}_K$ lying over (p_i) and all the p_i, and P is not a torsion point of $E(K)$, i.e. P has infinite order.

If we add some points to the set D and show that the theorem holds for the enlarged set D, then this will imply that the theorem holds for the original set D.

Proposition VII.5.4(b) of [6] implies that if (p_i) is a prime ideal of $\mathbf{Z}$ and a prime ideal of $\mathcal{O}_K$ lying over (p_i) is a bad prime ideal of $E(K)$, then (p_i) is a bad prime ideal of $E(\mathbf{Q})$. Lemma 3 implies that if (p_i) is a bad prime ideal then there is exactly one singular point on $E(k(p_i))$. Thus for each bad prime ideal (p_i) of $E(\mathbf{Q})$ in our set, we add $(S, (p_i))$ to the set D where S is a singular point of $E(k(p_i))$.

Note that if for some element $([a_i : b_i : c_i], (p_i))$ of D, we have $([a_i : b_i : c_i], J_{ij}) \notin \overline{E(K)} \subset \mathbf{P}^2_{\mathcal{O}_K}$ for all prime ideals $J_{ij} \subset \mathcal{O}_K$ lying over (p_i), then we can remove $([a_i : b_i : c_i], (p_i))$ from the set D.

The new set D contains n' points.

To find a D-integral point on $E(K)$ we need to find a point $[A : B : C] \in E(K)$ such that $[A \ : \ B \ : C] \not\equiv [a_i : b_i : c_i] \bmod (p_i)$ for all $1 \leq i \leq n'$. This follows from Section 2.2.

If a point $[A : B : C]$ is not congruent to a point $([a_i : b_i : c_i], (p_i))$, it implies that

$$Ab_i - Ba_i \not\equiv 0 \bmod (p_i)$$

or

$$Ac_i - Ca_i \not\equiv 0 \bmod (p_i)$$

or

$$Bc_i - Cb_i \not\equiv 0 \bmod (p_i).$$

Thus, if we can find $[A : B] \in \mathbf{P}^1(K)$ such that $Ab_i - Ba_i \not\equiv 0 \bmod (p_i)$, where $1 \leq i \leq n'$ and p_i does not divide $\gcd(a_i, b_i)$, then $[A : B : C]$ is D-integral point for any $C \in K$. Note that since $[A : B]$ is well defined, then $[A : B : C] \not\equiv [0 : 0 : 1] \bmod p_i$ for any p_i.

By Theorem 1, we can find infinitely many points $[A : B] \in \mathbf{P}^1(\mathbf{Q}[\sqrt{h}]/\mathbf{Q})$ for some large $h \in \mathbf{Z}$, such that

$$Ab_i - Ba_i \not\equiv 0 \bmod (p_i) \text{ for all the } p_i \text{ that does not divide } \gcd(a_i, b_i).$$

We pick one of those points $[A : B]$. Now, we plug A, B in the given equation of the elliptic curve to get $C \in K = \mathbf{Q}(\sqrt{h}, \alpha_1, \alpha_2, \alpha_3)/\mathbf{Q}$, where $\alpha_1, \alpha_2, \alpha_3$ are the roots of the equation that we get by substituting x and y with A and B in the equation of the elliptic curve E. The resulting point $P = [A : B : C]$ is not congruent to any point in the original set D and $P \bmod (p_i)$ is not singular on $E(k(J_{ij}))$ for all the prime ideals $J_{ij} \subset \mathcal{O}_K$ lying over (p_i) and for all the p_i.

By the famous theorem of Loic Merel [5] there are finitely many torsion points on $E(K)$ for all finite field extensions $K/\mathbf{Q}$ of degree less than or equal to d. In our case the degree of $K/\mathbf{Q}$ is at most 6 no matter what $[A : B] \in \mathbf{P}^1(\mathbf{Q}[\sqrt{h}]/\mathbf{Q})$ we pick.

Now, we check whether $[A : B : C]$ is a torsion point on $E(K)$. If it is not, then we found a finite field extension $K/\mathbf{Q}$ and a point $[A : B : C]$ on $E(K)$ with the

required properties.

If $[A : B : C]$ is a torsion point, then we pick another $[A : B] \in \mathbf{P}^1(\mathbf{Q}[\sqrt{h}]/\mathbf{Q})$ and follow the above steps to find another D-integral point $[A : B : C] \in E(K)$ for different K. Since there are infinitely many points $[A : B] \in \mathbf{P}^1(\mathbf{Q}[\sqrt{h}]/\mathbf{Q})$ with the required property, then by repeating the above procedure we can find infinitely many points $[A : B : C]$ on $E(K)$ for different field extensions $K/\mathbf{Q}$ with degree at most 6. But there are only finitely many torsion points on $E(K)$ for all finite field extensions with degree less than or equal to 6. Thus, we are guaranteed to find a finite field extension $K/\mathbf{Q}$ and a D-integral point $[A : B : C] \in E(K)$ which is not a torsion point and $[A : B : C] \bmod (p_i)$ is not singular on $E(k(J_{ij}))$ for all the prime ideals $J_{ij} \subset \mathcal{O}_K$ lying over (p_i) and for all the p_i.

Next, if (p_i) is a prime ideal of $\mathcal{O}_K$, then let $(p_i) = J_i$. If (p_i) is not a prime ideal of $\mathcal{O}_K$, then $(p_i) = J_{i1}J_{i2}\dots J_{ir}$, where J_{ij} for $1 \leq j \leq r$ are prime ideals in $\mathcal{O}_K$. The CRT implies that if P is not congruent to $[a_i : b_i : c_i]$ modulo at least one of the J_{ij}, then $P \not\equiv [a_i : b_i : c_i] \bmod (p_i)$. We need to find one prime ideal $J_{ij} = J_i$ such that P is not congruent to $([a_i : b_i : c_i], J_i)$. Moreover, since $[a_i : b_i : c_i]$ is in $\mathbf{P}^2(\mathbf{Q})$, Lemma 1 implies that any of the J_{ij} will satisfy the condition. Now, we substitute the points $([a_i : b_i : c_i], (p_i))$ in the set D with the points $([a_i : b_i : c_i], J_i)$.

Let E_{J_i} denote $E(k(J_i))$ if J_i is not a bad prime ideal, and $E(k(J_i)) - \{S\}$ (where S is the singular point) if J_i is a bad prime ideal. Then $P \bmod J_i \in E_{J_i}$ for all $1 \leq i \leq n'$. Lemma 3 proves that E_{J_i} is a group with the same group law as

$E(K)$. Let $s_i = |E_{J_i}|$. The following statement is true for all $\ell \in \mathbf{Z}$:

$$(\ell s_i + 1)P \equiv P \bmod J_i.$$

Let $m =$LCM$(s_1, \ldots, s_{n'})$. Thus, for all $1 \leq i \leq n'$ and $\ell \in \mathbf{Z}$

$$(\ell m + 1)P \equiv P \bmod J_i.$$

Since P is not a torsion point on $E(K)$, i.e. P has infinite order, the points $(\ell m + 1)P$ are all different in $E(K)$ for different ℓ. Therefore, there are infinitely many D-integral points on $E(K)$.

This completes the proof.

Next, we take a set D that consists of finitely many "lines" in $\mathbf{P}^2_{\mathbf{Z}}$, say $D = \{\overline{P_1}, \ldots, \overline{P_n}\}$ and let L be a line that does not go through any of the points $P_1, \ldots, P_n$. We show that there is a finite field extension $K/\mathbf{Q}$ such that there are infinitely many D-integral points on $L(K)$. Since $L(\mathbf{Q})$ does not contain any of the points $P_1, \ldots, P_n$, it is possible to find a finite set D' of close points in $\mathbf{P}^2_{\mathbf{Z}}$, such that P is D-integral on L if and only if P is D'-integral on L. Then the original problem reduces to the problem of finding a finite field extension $K/\mathbf{Q}$ such that a set of D'-integral points on $L(K)$ is infinite.

Theorem 3. *Let* $P_1 = [a_1 : b_1 : c_1], \ldots, P_n = [a_n : b_n : c_n] \in \mathbf{P}^2(\mathbf{Q})$ *and let* $D = \{\overline{P_1}, \ldots, \overline{P_n}\} \subset \mathbf{P}^2_{\mathbf{Z}}$. *Let* $L : Ax + By + Cz = 0$ *(with* $A, B, C \in \mathbf{Z}$ *and* $\gcd(A, B, C) = 1$*) be a line such that* L *does not go through any of the points* $P_1, \ldots, P_n$. *Then there is a finite field extension* $K/\mathbf{Q}$ *such that there are infinitely*

many D-integral points on $L(K)$.

Proof: In Section 2.2 we showed that $[X : Y : Z]$ is D-integral if $[X : Y : Z] \not\equiv [a_i : b_i : c_i] \bmod (p)$ for all $1 \leq i \leq n$ and all prime ideals $(p) \subset \mathbf{Z}$.

Let $[X : Y : Z] \in L$ and assume that $[X : Y : Z] \equiv [a_i : b_i : c_i] \bmod (p)$. Then

$$\begin{cases} a_iY - b_iX \equiv 0 \bmod (p) \\ a_iZ - c_iX \equiv 0 \bmod (p) \\ b_iZ - c_iY \equiv 0 \bmod (p) \\ AX + BY + CZ \equiv 0 \bmod (p). \end{cases}$$

We know that at least one of a_i, b_i, c_i is not zero, and since the above system of congruences is symmetric with respect to a_i, b_i, c_i, without loss of generality we assume that $a_i \neq 0$. There are finitely many primes that divide a_i.

First, let's look at the primes that do not divide a_i. For each such prime p we have $a_i \not\equiv 0 \bmod (p)$ and there exists an inverse a_i^{-1} of a_i. Thus, the following must be true

$$Y \equiv a_i^{-1}b_iX \bmod (p)$$

$$Z \equiv a_i^{-1}c_iX \bmod (p)$$

$$\implies AX + Ba_i^{-1}b_iX + Ca_i^{-1}c_iX \equiv 0 \bmod (p)$$

$$\implies a_i^{-1}X(Aa_i + Bb_i + Cc_i) \equiv 0 \bmod (p).$$

We have that $a_i^{-1} \not\equiv 0 \bmod (p)$ and if $X \equiv 0 \bmod (p)$, then $Y \equiv Z \equiv 0 \bmod (p)$,

which is impossible. Therefore,

$$(Aa_i + Bb_i + Cc_i) \equiv 0 \bmod (p).$$

Since $[a_i : b_i : c_i] \notin L$, we have $Aa_i + Bb_i + Cc_i \neq 0$, and this implies that the above congruence is possible only for finitely many primes, namely the primes that divide $Aa_i + Bb_i + Cc_i$.

We are left to check the primes that divide a_i. For each such prime p, we have $a_i \equiv 0 \bmod (p)$. As $\gcd(a_i, b_i, c_i) = 1$, at least one of b_i, c_i is not congruent to zero modulo (p), and at least one of b_i, c_i has an inverse. Using the same argument as above, at least one of following congruences must be true.

$$b_i^{-1}Y(Aa_i + Bb_i + Cc_i) \equiv 0 \bmod (p)$$

$$c_i^{-1}Z(Aa_i + Bb_i + Cc_i) \equiv 0 \bmod (p).$$

This implies that p has to divide $Aa_i + Bb_i + Cc_i$.

Therefore, a point $[X : Y : Z] \in L$ can be congruent to $[a_i : b_i : c_i]$ modulo (p) only for primes p that divide $Aa_i + Bb_i + Cc_i$.

Let $Aa_i + Bb_i + Cc_i = p_1 p_2 \cdots p_m$; then to find a point on L that is not congruent to $[a_i : b_i : c_i]$ modulo any prime, we need to find a point which is not congruent to any point in the set $\{([a_i : b_i : c_i], (p_1)), ([a_i : b_i : c_i], (p_2)), \ldots, ([a_i : b_i : c_i], (p_m))\}$.

Following the same procedure for each point $P_1, \ldots, P_n$, we get a finite set $D' = \{(P_1, (p_1)), (P_2, (p_2)), \ldots, (P_{n'}, (p_{n'}))\}$. Now the original problem reduces to

the problem of finding a finite field extension $K/\mathbf{Q}$ such that there are infinitely many points on $L(K)$ that are not congruent to any of the points in set D'.

By Theorem 1 we can find a finite field extension $K/\mathbf{Q}$ with X and Y in K, such that $[X : Y] \not\equiv [a_i : b_i] \bmod (p_i)$ for all $1 \leq i \leq n'$ and p_i does not divide $\gcd(a_i, b_i)$. Note that since $[X : Y]$ is well defined, then $[X : Y : Z] \not\equiv [0 : 0 : 1] \bmod p_i$ for any p_i. Then $[X : Y : \frac{-AX-BY}{C}] \not\equiv [a_i : b_i : c_i] \bmod (p_i)$ for all $1 \leq i \leq n'$, and $[X : Y : Z] = [X : Y : \frac{-AX-BY}{C}] \in L(K)$. Let $N = LCM_{1 \leq i \leq n'}(Aa_i + Bb_i + Cc_i)$. Then clearly points in the form $[X + CkN : Y + ChN : Z - (Ak + Bh)N]$ for $k, h \in \mathbf{Z}$, are in $L(K)$ and are not congruent to any of the points in D'. Therefore, there are infinitely many points in $L(K)$ which are not congruent to any point in the set D', and thus there are infinitely many D-integral points on $L(K)$.

This completes the proof.

We conclude the section by showing that given a set D of finitely many "lines" in $\mathbf{P}^2_{\mathbf{Z}}$, we can find a Zariski dense set in $\mathbf{P}^2(K)$ of D-integral points for some finite field extension $K/\mathbf{Q}$.

Theorem 4. *Let $P_1 = [a_1 : b_1 : c_1], \ldots, P_n = [a_n : b_n : c_n] \in \mathbf{P}^2(\mathbf{Q})$ and let $D = \{\overline{P_1}, \ldots, \overline{P_n}\} \subset \mathbf{P}^2_{\mathbf{Z}}$. There is a Zariski dense set S in $\mathbf{P}^2(K)$ for some finite field extension $K/\mathbf{Q}$ such that $[X : Y : Z] \in S$ implies that $[X : Y : Z]$ is D-integral.*

Proof: First we find a line $L : Ax + By + Cz = 0$ (with $A, B, C \in \mathbf{Z}$ and $\gcd(A, B, C) = 1$) that does not go through any of the points $P_1, \ldots, P_n$. We are guaranteed to find such a line since there are infinitely many lines with this property. By Theorem 3 we know that we can find a finite field extension $K/\mathbf{Q}$ with $[X :$

$Y : Z] \in L(K)$ being D-integral. Moreover, since $[X : Y : Z] \in L(K)$ is D-integral, then points of the form $[X + CkN : Y + ChN : Z - (Ak + Bh)N]$, where $N = LCM_{1 \leq i \leq n}(Aa_i + Bb_i + Cc_i)$, are also D-integral on $L(K)$ for any integers k and h.

Next, a general equation for the lines over K that go through the point $[X : Y : Z]$ can be written in the form $L_{\alpha\beta} : (\alpha Z)x + (\beta Z)y - (\alpha X + \beta Y)z = 0$ for $\alpha, \beta \in K$. There are at most n lines that go through the point $[X : Y : Z]$ and at least one of the points $[a_1 : b_1 : c_1], [a_2 : b_2 : c_2], \ldots, [a_n : b_n : c_n]$. In particular, there are infinitely many distinct lines $L_{\alpha,\beta}$ which do not go through any $[a_i : b_i : c_i]$.

Let G be the set of all the lines over K that go through $[X : Y : Z]$ and at least one of the points $[a_1 : b_1 : c_1], [a_2 : b_2 : c_2], \ldots, [a_n : b_n : c_n]$.

After clearing the denominators and renaming the coefficients we get

$$L_{\alpha\beta} : A_{\alpha\beta}x + B_{\alpha\beta}y + C_{\alpha\beta}z = 0,$$

where $A_{\alpha\beta}, B_{\alpha\beta}, C_{\alpha\beta} \in \mathcal{O}_K$.

Now, for each pair (α, β) such that the line $L_{\alpha\beta} \notin G$, we use the following argument. Since $L_{\alpha\beta}$ does not go through P_i, then using the idea from Theorem 3 we can say that for $[a : b : c] \in L_{\alpha\beta}$ and a prime ideal $J \subset \mathcal{O}_K$

$$[a : b : c] \equiv [a_i : b_i : c_i] \bmod J$$

$\Longrightarrow$

$$A_{\alpha\beta}a_i + B_{\alpha\beta}b_i + C_{\alpha\beta}c_i \equiv 0 \bmod J$$

$\Longrightarrow$

$$A_{\alpha\beta}a_i + B_{\alpha\beta}b_i + C_{\alpha\beta}c_i \in J.$$

Now, $\mathcal{O}_K$ is a Dedekind domain, i.e. every ideal of $\mathcal{O}_K$ can be written uniquely (up to order) as a product of prime ideals of $\mathcal{O}_K$. Thus,

$$(A_{\alpha\beta}a_i + B_{\alpha\beta}b_i + C_{\alpha\beta}c_i) = J_{i1} \cdots J_{ir}$$

for a unique set of prime ideals $J_{i1}, \ldots, J_{ir} \subset \mathcal{O}_K$. Therefore, a point $[a : b : c] \in L_{\alpha\beta}(K)$ can be congruent to P_i modulo only finitely many prime ideals $J_{i1}, \ldots, J_{ir} \subset \mathcal{O}_K$.

Now, each J_{ij} $(1 \leq j \leq r)$ lies over some prime ideal $(p_{ij}) \subset \mathbf{Z}$ and since each $P_i \in \mathbf{P}^2(\mathbf{Q})$, Lemma 1 proves that if $[a : b : c] \not\equiv P_i \bmod (p_{ij})$, where $(p_{ij}) \subset \mathbf{Z}$, then $[a : b : c]$ is not congruent to P_i modulo all prime ideals of $\mathcal{O}_K$ lying over (p_{ij}) and in particular $P \not\equiv P_i \bmod J_{ij}$.

Thus, a point $[a : b : c] \in L_{\alpha\beta}(K)$ is not congruent to P_i modulo any prime ideal of $\mathcal{O}_K$ if and only if $[a : b : c] \in L_{\alpha\beta}(K)$ is not congruent to any of the points in the set $\{(P_i, p_{i1}), \ldots, (P_i, p_{ir})\}$.

Using the same procedure for each of the P_i we can construct a set $D_{\alpha\beta}$ of finitely many closed points such that $[a : b : c] \in L_{\alpha\beta}(K)$ is D-integral if and only if $[a : b : c] \in L_{\alpha\beta}(K)$ is $D_{\alpha\beta}$-integral.

Now, let $N_{\alpha\beta}$ be the product of all the p_{ij} described above. Then

$$[X + C_{\alpha\beta}kN_{\alpha\beta} : Y + C_{\alpha\beta}hN_{\alpha\beta} : Z - (A_{\alpha\beta}k + B_{\alpha\beta}h)N_{\alpha\beta}] \equiv [X : Y : Z] \bmod (p_{ij})$$

for all the p_{ij} and all $k, h \in \mathbf{Z}$.

Therefore, since $[X : Y : Z]$ is D-integral and the above argument is true for every $L_{\alpha\beta} \notin G$, then the points in the form

$$[X + C_{\alpha\beta}kN_{\alpha\beta} : Y + C_{\alpha\beta}hN_{\alpha\beta} : Z - (A_{\alpha\beta}k + B_{\alpha\beta}h)N_{\alpha\beta}],$$

$$k, h \in \mathbf{Z}; \alpha, \beta \in K, L_{\alpha,\beta} \notin G$$

will form a set S of D-integral points.

Now, we are left to show that the set S is Zariski dense in $\mathbf{P}^2$. There are infinitely many curves $L_{\alpha\beta} : A_{\alpha\beta}x + B_{\alpha\beta}y + C_{\alpha\beta}z = 0$ (where $L_{\alpha,\beta} \notin G$) with infinitely many points from set S on each of them. Thus, by Lemma 2, the set S is Zariski dense in $\mathbf{P}^2(K)$.

This completes the proof.

3.2 Complete Descriptions of D-integral points in $\mathbf{P}^2(\mathbf{Q})$

In this section we show that for four different types of D, where D is a set of "lines" in $\mathbf{P}^2_{\mathbf{Z}}$, we can find an explicit description of the complete set of D-integral points in $\mathbf{P}^2(\mathbf{Q})$.

We start with the simplest case, i.e. the set D contains the closure of only one point P. We will show that there exists a linear change of coordinates T such that

the complete set S of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$ is

$$S = \{T([x : y : z])| \gcd(y, z) = 1\}.$$

Moreover, this T can be explicitly determined by P.

Theorem 5. *Given a point $P = [a : b : c] \in \mathbf{P}^2(\mathbf{Q})$. Let $D = \{\overline{P}\} \subset \mathbf{P}^2_{\mathbf{Z}}$. Then there is an explicit description of the complete set S of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$ (see Description 1).*

Proof: If $[a : b : c] = [1 : 0 : 0]$, then $[x : y : z] \equiv [1 : 0 : 0] \bmod p$ if and only if $y \equiv 0 \bmod p$ and $z \equiv 0 \bmod p$. Thus $[x : y : z] \not\equiv [a : b : c] \bmod p$ for all primes p if and only if $\gcd(y, z) = 1$. Then the complete set S of all D integral points in $\mathbf{P}^2(\mathbf{Q})$ consists of $[x : y : z]$ such that $\gcd(y, z) = 1$. Similarly if $[a : b : c] = [0 : 1 : 0]$ or $[0 : 0 : 1]$, then the complete set S of all D integral points in $\mathbf{P}^2(\mathbf{Q})$ consists of $[x : y : z]$ such that $\gcd(x, z) = 1$ or $\gcd(x, y) = 1$ respectively.

Now, let's look at the problem in general.

First, we want to show that we can always find a D-integral point $[A : B : C]$ in $\mathbf{P}^2(\mathbf{Q})$. If $[a : b : c] = [1 : 0 : 0]$ or $[0 : 1 : 0]$ or $[0 : 0 : 1]$, we take any $[A : B : C]$ with $\gcd(B, C) = 1$ or $\gcd(A, C) = 1$ or $\gcd(A, B) = 1$ respectively. In all other cases we choose a pair $(a, b), (a, c)$ or (b, c) such that the pair has non-zero elements. Due to the symmetry, without loss of generality we take (a, b). Then there are integers A, B with $\gcd(A, B) = 1$ such that $Ab - Ba = \gcd(a, b)$.

For all primes p_i that do not divide $\gcd(a, b)$,

$$Ab - Ba \not\equiv 0 \bmod p_i.$$

$\Longrightarrow$

$$[A : B : 1] \not\equiv [a : b : c] \bmod p_i.$$

For all primes p_i that do divide $\gcd(a, b)$, we have $a \equiv b \equiv 0 \bmod p_i$ and $c \not\equiv 0 \bmod p_i$. Since $\gcd(A, B) = 1$, then at least one of A or B is non-zero modulo p_i. Thus,

$$Ac - Ca \equiv Ac \not\equiv 0 \bmod p_i$$

or

$$Bc - Cb \equiv Bc \not\equiv 0 \bmod p_i$$

$\Longrightarrow$

$$[A : B : 1] \not\equiv [a : b : c] \bmod p_i.$$

Therefore,

$$[A : B : 1] \not\equiv [a : b : c] \bmod p, \text{ for all primes } p.$$

Thus, $[A : B : 1]$ is D-integral in $\mathbf{P}^2(\mathbf{Q})$.

Using the above argument we can easily find a D-integral point $[A_1 : B_1 : C_1]$ in $\mathbf{P}^2(\mathbf{Q})$. This implies that

$$aB_1 - bA_1 \not\equiv 0 \bmod p$$

or

$$aC_1 - cA_1 \not\equiv 0 \bmod p$$

or

$$bC_1 - cB_1 \not\equiv 0 \bmod p$$

for all primes p. Thus, we have $\gcd(aB_1 - bA_1, aC_1 - cA_1, bC_1 - cB_1) = 1$. Therefore, we can find integers A_2, B_2, C_2 such that

$$A_2(bC_1 - cB_1) - B_2(aC_1 - cA_1) + C_2(aB_1 - bA_1) = 1.$$

Let $M = \begin{bmatrix} a & A_1 & A_2 \\ b & B_1 & B_2 \\ c & C_1 & C_2 \end{bmatrix}$. The determinant of M is equal to 1, which implies that $\det(M)$ is non-zero modulo any prime p. Let $T : \mathbf{P}^2(\mathbf{Q}) \longrightarrow \mathbf{P}^2(\mathbf{Q})$ be the linear change of coordinates defined by the matrix M. Then using Lemma 4 we conclude that for all primes p

$$[x : y : z] \not\equiv [a' : b' : c'] \bmod p \Longleftrightarrow T([x : y : z]) \not\equiv T([a' : b' : c']) \bmod p.$$

Now, consider the point $[1 : 0 : 0]$. Then $[x : y : z] \not\equiv [1 : 0 : 0] \bmod p$ for all primes p if and only if $\gcd(y, z) = 1$. We have $T([1 : 0 : 0]) = [a : b : c]$. Thus,

$$T([x : y : z]) \not\equiv [a : b : c] \bmod p \text{ for all primes } p \Longleftrightarrow \gcd(y, z) = 1.$$

Description 1 Define

$$S = \{T([x : y : z]) | \gcd(y, z) = 1\}.$$

Then S forms a complete set of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$.

This completes the proof.

In the following theorem we let D contain the closures of two points P_1, P_2 that are not congruent to each other modulo any prime p. We will show that there exists a linear change of coordinates T such that the complete set S of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$ is

$$S = \{T([x : y : z]) | \gcd(y, z) = 1, \gcd(x, z) = 1\}.$$

Moreover, this T can be explicitly determined by P_1 and P_2.

Theorem 6. *Let $P_1 = [a_1 : b_1 : c_1], P_2 = [a_2 : b_2 : c_2] \in \mathbf{P}^2(\mathbf{Q})$ be two points such that $P_1 \not\equiv P_2 \bmod p$ for all primes p. Let $D = \{\overline{P_1}, \overline{P_2}\} \subset \mathbf{P}^2_{\mathbf{Z}}$. Then there is an explicit description of the complete set S of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$ (see Description 2).*

Proof: Since $[a_1 : b_1 : c_1] \not\equiv [a_2 : b_2 : c_2] \bmod p$ for all primes p, this implies that

$$a_1 b_2 - b_1 a_2 \not\equiv 0 \bmod p$$

or

$$a_1 c_2 - c_1 a_2 \not\equiv 0 \bmod p$$

or

$$b_1c_2 - c_1b_2 \not\equiv 0 \bmod p$$

for all primes p. Thus, we have $\gcd(a_1b_2-b_1a_2, a_1c_2-c_1a_2, b_1c_2-c_1b_2) = 1$. Therefore, we can find integers A, B, C such that

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = 1.$$

Let $M = \begin{bmatrix} a_1 & a_2 & A \\ b_1 & b_2 & B \\ c_1 & c_2 & C \end{bmatrix}$. The determinant of M is equal to 1, which implies that $\det(M)$ is non-zero modulo any prime p. Let $T : \mathbf{P}^2(\mathbf{Q}) \longrightarrow \mathbf{P}^2(\mathbf{Q})$ be the linear change of coordinates defined by the matrix M. Then using Lemma 4 we conclude that for all primes p

$$[x : y : z] \not\equiv [a' : b' : c'] \bmod p \Longleftrightarrow T([x : y : z]) \not\equiv T([a' : b' : c']) \bmod p.$$

Now, consider the points $[1 : 0 : 0]$ and $[0 : 1 : 0]$. Then $[x : y : z] \not\equiv [1 : 0 : 0] \bmod p$ for all primes p if and only if $\gcd(y, z) = 1$, and $[x : y : z] \not\equiv [0 : 1 : 0] \bmod p$ for all primes p if and only if $\gcd(x, z) = 1$. We have $T([1 : 0 : 0]) = [a_1 : b_1 : c_1]$ and $T([0 : 1 : 0]) = [a_2 : b_2 : c_2]$. Thus,

$$T([x : y : z]) \not\equiv [a_1 : b_1 : c_1] \bmod p \text{ for all primes } p \Longleftrightarrow \gcd(y, z) = 1$$

and

$$T([x:y:z]) \not\equiv [a_2:b_2:c_2] \bmod p \text{ for all primes } p \Longleftrightarrow \gcd(x,z)=1.$$

Description 2 Define

$$S = \{T([x:y:z]) | \gcd(y,z)=1 \text{ and } \gcd(x,z)=1\}.$$

Then S forms a complete set of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$.

This completes the proof.

Next, we take two points P_1, P_2 that are congruent modulo p_i for only finitely many primes $p_1, \ldots p_n$, but not congruent modulo p_i^2 for all the p_i. We let D consist of the closures of the two points. We will show that there exists a linear change of coordinates T such that the complete set S of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$ is

$$\begin{aligned} S = \{T([x:y:z]) | \gcd(y,z)=1, \gcd(x,z)=1, \\ [x:y:z] \notin E_{p_i} \text{ for all } 1 \le i \le n\}. \end{aligned}$$

Moreover, this T and the sets E_{p_i} can be explicitly determined by P_1 and P_2.

Theorem 7. *Let $P_1 = [a_1:b_1:c_1], P_2 = [a_2:b_2:c_2] \in \mathbf{P}^2(\mathbf{Q})$ be two points such that $P_1 \equiv P_2 \bmod p_i$ for only finitely many primes $p_1, \ldots, p_n$, and $P_1 \not\equiv P_2 \bmod p_i^2$ for $1 \le i \le n$. Let $D = \{\overline{P_1}, \overline{P_2}\} \subset \mathbf{P}^2_{\mathbf{Z}}$. Then there is an explicit description of the complete set S of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$ (see Description 3).*

Proof: Since $[a_1:b_1:c_1] \equiv [a_2:b_2:c_2] \bmod p_i$ for only $1 \le i \le n$ and

$[a_1 : b_1 : c_1] \not\equiv [a_2 : b_2 : c_2] \bmod p_i$ for $1 \leq i \leq n$, this implies that

$$\gcd(a_1b_2 - b_1a_2, a_1c_2 - c_1a_2, b_1c_2 - c_1b_2) = p_1 \cdots p_n.$$

Using Lemma 6 we can find integers A, B, C such that

$$A(b_1c_2 - c_1b_2) - B(a_1c_2 - c_1a_2) + C(a_1b_2 - b_1a_2) = p_1 \cdots p_n$$

and $[A : B : C]$ is D-integral.

Let $M = \begin{bmatrix} a_1 & a_2 & A \\ b_1 & b_2 & B \\ c_1 & c_2 & C \end{bmatrix}$. The determinant of M is equal to $p_1 \cdots p_n$ and it is square-free. Let $T : \mathbf{P}^2(\mathbf{Q}) \longrightarrow \mathbf{P}^2(\mathbf{Q})$ be the linear change of coordinates defined by the matrix M. We construct the set

$$S' = \{T([x : y : z]) | \gcd(y, z) = 1 \text{ and } \gcd(x, z) = 1\}.$$

For all primes p except $p_1, \ldots, p_n$, the determinant of M is non-zero modulo p, thus using Lemma 4 and the ideas from Theorem 5 we can conclude that the set S' contains all the points in $\mathbf{P}^2(\mathbf{Q})$, which are not congruent to points P_1 and P_2 modulo all primes except maybe $p_1, \ldots, p_n$. So, let's check the points in the set S' modulo p_i for $1 \leq i \leq n$.

For each prime p_i we have to check two cases:

Case 1: p_i divides g_{xyz} where $g_{xyz} = \gcd(xa_1 + ya_2 + zA, xb_1 + yb_2 + zB, xc_1 + yc_2 + zC)$. If

$$T([x:y:z]) \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$\Longrightarrow$

$$\left[\frac{xa_1 + ya_2 + zA}{g_{xyz}} : \frac{xb_1 + yb_2 + zB}{g_{xyz}} : \frac{xc_1 + yc_2 + zC}{g_{xyz}}\right] \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$\Longrightarrow$

$$\left(\frac{xa_1 + ya_2 + zA}{g_{xyz}} - \alpha a_1, \frac{xb_1 + yb_2 + zB}{g_{xyz}} - \alpha b_1, \frac{xc_1 + yc_2 + zC}{g_{xyz}} - \alpha c_1\right)$$

$$\equiv (0,0,0) \bmod p_i \text{ for some } \alpha \not\equiv 0 \bmod p_i$$

$\Longrightarrow$

$$\left(\frac{(x - \alpha g_{xyz})a_1 + ya_2 + zA}{g_{xyz}}, \frac{(x - \alpha g_{xyz})b_1 + yb_2 + zB}{g_{xyz}}, \frac{(x - \alpha g_{xyz})c_1 + yc_2 + zC}{g_{xyz}}\right)$$

$$\equiv (0,0,0) \bmod p_i$$

$\Longrightarrow$

$$((x - \alpha g_{xyz})a_1 + ya_2 + zA, (x - \alpha g_{xyz})b_1 + yb_2 + zB, (x - \alpha g_{xyz})c_1 + yc_2 + zC)$$

$$\equiv (0,0,0) \bmod p_i^2$$

$\Longrightarrow$

$$p_i^2 | \gcd((x-\alpha g_{xyz})a_1 + ya_2 + zA, (x-\alpha g_{xyz})b_1 + yb_2 + zB, (x-\alpha g_{xyz})c_1 + yc_2 + zC)$$

$$= g_{(x-\alpha g_{xyz})yz}.$$

Since $\gcd(y,z) = 1$, it follows that $\gcd((x-\alpha g_{xyz}), y, z) = 1$. Thus, we can use Lemma 5 to see that $g_{(x-\alpha g_{xyz})yz} | \det(M)$. This implies that $p_i^2 | \det(M)$, which is a contradiction as $\det(M)$ is square-free. Therefore, if $p_i | g_{xyz}$, then $T([x:y:z]) \not\equiv P_1 \bmod p_i$ and $T([x:y:z]) \not\equiv P_2 \bmod p_i$.

Case 2: p_i does not divides g_{xyz}.

$$T([x:y:z]) \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$$\Longleftrightarrow$$

$$[xa_1 + ya_2 + zA : xb_1 + yb_2 + zB : xc_1 + yc_2 + zC] \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$$\Longleftrightarrow$$

$$((x-\alpha)a_1 + ya_2 + zA, (x-\alpha)b_1 + yb_2 + zB, (x-\alpha)c_1 + yc_2 + zC)$$

$$\equiv (0,0,0) \bmod p_i \text{ for some } \alpha \not\equiv 0 \bmod p_i$$

$$\Longleftrightarrow$$

$$(x-\alpha)(a_1,b_1,c_1)+y(a_2,b_2,c_2)+z(A,B,C)\equiv(0,0,0) \bmod p_i.$$

Since $[a_1:b_1:c_1],[a_2:b_2:c_2]$ and $[A:B:C]$ are not congruent to each other at the same time modulo p_i, there exist a unique triple of integers U,V,W up to scalars such that

$$U(a_1,b_1,c_1)+V(a_2,b_2,c_2)+W(A,B,C)\equiv(0,0,0) \bmod p_i.$$

Moreover, since $[a_1:b_1:c_1]\equiv[a_2:b_2:c_2] \bmod p_i$, we know that

$$[U:V:W]\equiv[1:-1:0] \bmod p_i.$$

Thus, we can see that

$$T([x:y:z])\equiv[a_1:b_1:c_1] \bmod p_i$$

$$\Longleftrightarrow$$

$$[x-\alpha:y:z]\equiv[1:-1:0] \bmod p_i \text{ for some } \alpha\not\equiv 0 \bmod p_i.$$

Let $E_{p_i}=\{[x:y:z]|[x:y:z]\not\equiv[1:-1:0] \bmod p_i \text{ and } z\equiv 0 \bmod p_i\}$.

Then

$$T([x:y:z])\equiv[a_1:b_1:c_1]\equiv[a_2:b_2:c_2] \bmod p_i \Longleftrightarrow [x:y:z]\in E_{p_i}.$$

Description 3 Define

$$S = \{T([x : y : z]) | \gcd(y, z) = 1, \gcd(x, z) = 1, \\ [x : y : z] \notin E_{p_i} \text{ for all } 1 \leq i \leq n\}.$$

Then S is the complete set of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$.

This completes the proof.

Finally, we take a set D that consists of the closures of three points P_1, P_2 and P_3 such that P_1, P_2 and P_3 are not congruent to each other at the same time modulo any prime p, and the matrix M, whose columns are P_1, P_2 and P_3, has a square-free determinant. There exists a linear change of coordinates T such that the complete set S of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$ is

$$S = \{T([x : y : z]) | \gcd(y, z) = 1, \gcd(x, z) = 1, \gcd(x, z) = 1, \\ [x : y : z] \notin E_p \text{ for all the } p | \det(M)\}.$$

Moreover, this T and the sets E_p can be explicitly determined by P_1, P_2 and P_3.

Theorem 8. *Let* $P_1 = [a_1 : b_1 : c_1], P_2 = [a_2 : b_2 : c_2], P_3 = [a_3 : b_3 : c_3] \in \mathbf{P}^2(\mathbf{Q})$ *be three points such that* P_1, P_2, P_3 *are not congruent to each other at the same time modulo any prime. Let* $D = \{\overline{P_1}, \overline{P_2}, \overline{P_3}\} \subset \mathbf{P}^2_{\mathbf{Z}}$. *Let* $M = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$ *with the property that the determinant of* M *is square-free, say* $\det(M) = p_1 \cdots p_n$. *Then there is an explicit description of the complete set* S *of all* D*-integral points in* $\mathbf{P}^2(\mathbf{Q})$ *(see Description 4).*

Proof: Let $T : \mathbf{P}^2(\mathbf{Q}) \longrightarrow \mathbf{P}^2(\mathbf{Q})$ be the linear change of coordinates defined by

the matrix M. We construct the set

$$S' = \{T([x:y:z]) | \gcd(y,z) = 1, \gcd(x,z) = 1 \text{ and } \gcd(z,y) = 1\}.$$

For all primes p except $p_1, \ldots, p_n$, we have $\det(M)$ is non-zero modulo p, so using Lemma 4 and the ideas from Theorem 5, we can conclude that the set S' contains all the points in $\mathbf{P}^2(\mathbf{Q})$, which are not congruent to points P_1, P_2 and P_3 modulo all primes except maybe $p_1, \ldots, p_n$. So, let's check the points in the set S' modulo p_i for $1 \leq i \leq n$.

For each prime p_i we have to check two cases:

Case 1: p_i divides g_{xyz} where $g_{xyz} = \gcd(xa_1 + ya_2 + za_3, xb_1 + yb_2 + zb_3, xc_1 + yc_2 + zc_3)$. If

$$T([x:y:z]) \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$\Longrightarrow$

$$\left[\frac{xa_1 + ya_2 + za_3}{g_{xyz}} : \frac{xb_1 + yb_2 + zb_3}{g_{xyz}} : \frac{xc_1 + yc_2 + zc_3}{g_{xyz}}\right] \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$\Longrightarrow$

$$\left(\frac{xa_1 + ya_2 + za_3}{g_{xyz}} - \alpha a_1, \frac{xb_1 + yb_2 + zb_3}{g_{xyz}} - \alpha b_1, \frac{xc_1 + yc_2 + zc_3}{g_{xyz}} - \alpha c_1\right)$$

$$\equiv (0,0,0) \bmod p_i \text{ for some } \alpha \not\equiv 0 \bmod p_i$$

$$\Longrightarrow$$

$$\left(\frac{(x-\alpha g_{xyz})a_1 + ya_2 + za_3}{g_{xyz}}, \frac{(x-\alpha g_{xyz})b_1 + yb_2 + zb_3}{g_{xyz}}, \frac{(x-\alpha g_{xyz})c_1 + yc_2 + zc_3}{g_{xyz}}\right)$$

$$\equiv (0,0,0) \bmod p_i$$

$$\Longrightarrow$$

$$((x-\alpha g_{xyz})a_1 + ya_2 + za_3, (x-\alpha g_{xyz})b_1 + yb_2 + zb_3, (x-\alpha g_{xyz})c_1 + yc_2 + zc_3)$$

$$\equiv (0,0,0) \bmod p_i^2$$

$$\Longrightarrow$$

$$p_i^2 | \gcd((x-\alpha g_{xyz})a_1 + ya_2 + za_3, (x-\alpha g_{xyz})b_1 + yb_2 + zb_3, (x-\alpha g_{xyz})c_1 + yc_2 + zc_3)$$

$$= g_{(x-\alpha g_{xyz})yz}.$$

Since $\gcd(y,z) = 1$, it follows that $\gcd((x-\alpha g_{xyz}), y, z) = 1$. Thus, we can use Lemma 5 to see that $g_{(x-\alpha g_{xyz})yz} | \det(M)$. This implies that $p_i^2 | \det(M)$, which is a contradiction as $\det(M)$ is square-free. Therefore, if $p_i | g_{xyz}$, then $T([x:y:z]) \not\equiv$

$P_1 \bmod p_i$. Similarly, we can show that if $p_i | g_{xyz}$, then $T([x:y:z]) \not\equiv P_2 \bmod p_i$ and $T([x:y:z]) \not\equiv P_3 \bmod p_i$.

Case 2: p_i does not divides g_{xyz}.

$$T([x:y:z]) \equiv [a_1:b_1:c_1] \bmod p_i$$

$$\Longleftrightarrow$$

$$[xa_1+ya_2+za_3 : xb_1+yb_2+zb_3 : xc_1+yc_2+zc_3] \equiv [a_1:b_1:c_1] \bmod p_i$$

$$\Longleftrightarrow$$

$$((x-\alpha)a_1+ya_2+za_3, (x-\alpha)b_1+yb_2+zb_3, (x-\alpha)c_1+yc_2+zc_3)$$

$$\equiv (0,0,0) \bmod p_i \text{ for some } \alpha \not\equiv 0 \bmod p_i$$

$$\Longleftrightarrow$$

$$(x-\alpha)(a_1,b_1,c_1)+y(a_2,b_2,c_2)+z(a_3,b_3,c_3) \equiv (0,0,0) \bmod p_i.$$

Since $[a_1:b_1:c_1], [a_2:b_2:c_2]$ and $[a_3:b_3:c_3]$ are not congruent to each other at the same time modulo p_i, there exists a unique triple of integers U, V, W up to scalars such that

$$U(a_1,b_1,c_1)+V(a_2,b_2,c_2)+W(a_3,b_3,c_3) \equiv (0,0,0) \bmod p_i.$$

Thus, we can see that

$$T([x:y:z]) \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$$\iff$$

$$[x - \alpha : y : z] \equiv [U : V : W] \bmod p_i \text{ for some } \alpha \not\equiv 0 \bmod p_i.$$

Therefore,

$$T([x:y:z]) \equiv [a_1 : b_1 : c_1] \bmod p_i$$

$$\iff$$

$$[x:y:z] \not\equiv [U:V:W] \text{ and } yW \equiv Vz \bmod p_i.$$

Similarly, we can show that

$$T([x:y:z]) \equiv [a_2 : b_2 : c_2] \bmod p_i$$

$$\iff$$

$$[x:y:z] \not\equiv [U:V:W] \text{ and } xW \equiv Uz \bmod p_i$$

and

$$T([x:y:z]) \equiv [a_3 : b_3 : c_3] \bmod p_i$$

$$\iff$$

$$[x : y : z] \not\equiv [U : V : W] \text{ and } xV \equiv Uy \bmod p_i.$$

Let

$$E_{p_i} = \{[x : y : z] | [x : y : z] \not\equiv [U : V : W] \bmod p_i \text{ and}$$

$$(yW - Vz)(xW - Uz)(xV - Uy) \equiv 0 \bmod p_i\}.$$

Then $T([x : y : z])$ is congruent to at least one of the points P_1, P_2 or P_3 modulo p_i if and only if $[x : y : z] \in E_{p_i}$.

Description 4 Define

$$S = \{T([x : y : z]) | \gcd(y, z) = 1, \gcd(x, z) = 1, \gcd(x, z) = 1,$$
$$[x : y : z] \notin E_{p_i} \text{ for all } 1 \leq i \leq n\}.$$

Then S is the complete set of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$.

This completes the proof.

It is a logical place to stop at three points, since we work in $\mathbf{P}^2$ and the linear change of coordinates T is defined by a 3x3 matrix.

Chapter 4

Conclusion

In the thesis we looked at two types of problems.

First, we showed that for four different types of $D \subset \mathbf{P}^n_{\mathbf{Z}}$ and projective algebraic varieties $X \subseteq \mathbf{P}^n$, where the codimension of D with respect to X is two, we can find a finite field extension $K/\mathbf{Q}$ such that there are infinitely many D-integral points on $X(K)$. In the future, we plan to discover more properties of D-integral points on algebraic varieties X, perhaps, taking X and D with higher codimension of D with respect to X.

Secondly, we showed that if $D \subset \mathbf{P}^2_{\mathbf{Z}}$ consists of the closure of one, two or three points of $\mathbf{P}^2(\mathbf{Q})$ (with certain restrictions), we can find an explicit description of the complete set of all D-integral points in $\mathbf{P}^2(\mathbf{Q})$. In the future, we want to look at sets $D \subset \mathbf{P}^n_{\mathbf{Z}}$ that consist of the closure of more than three points of $\mathbf{P}^n(\mathbf{Q})$, and see if we can find an explicit description of all D-integral points in $\mathbf{P}^n(\mathbf{Q})$.

Bibliography

[1] D. Eisenbud, and J. Harris. *The Geometry of Schemes.* Graduate Texts in Mathematics, 197, Springer-Verlag, New York, 2000.

[2] R. Hartshorne. *Algebraic Geometry.* Graduate Texts in Mathematics, 52, Springer-Verlag, New York, 1977.

[3] B. Hassett, and Yu. Tschinkel "Density of integral points on algebraic varieties." Rational points on algebraic varieties, 169–197, Progr. Math., 199, Birkhäuser, Basel, 2001.

[4] S. Lang. *Algebraic Numbers.* Addison-Wesley Pub. Co., Reading, Mass., 1964

[5] L. Merel. "Bornes pour la torsion des courbes elliptiques sur les corps de nombres." Invent. Math. 124 (1996) no.1-3, 437-444.

[6] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.