University of Groningen

Bachelor Thesis

Two-cover descent on hyperelliptic curves and generalizations

Author:
Wojciech Jerzy Szpytma *(s4760999)*

Supervisors:
prof. Steffen Müller
prof. Cecília Salgado Guimarães da Silva

July 2024

rijksuniversiteit
groningen

Two-cover descent on hyperelliptic curves and generalizations

Abstract

A curve over a field k is a smooth, projective, and absolutely irreducible 1-dimensional k-variety, whereas a hyperelliptic curve is a curve with an affine patch of the form $y^2 = f(x)$, where $f(x)$ is a polynomial of degree≥ 3 without repeated roots, and $\mathrm{char}(k) \neq 2$. According to a theorem by Faltings, for any curve C over $\mathbb{Q}$ of genus ≥ 2 there are at most finitely many rational points satisfying the equation of the curve C; the set of those points is denoted as $C(\mathbb{Q})$. None of the proofs of Faltings' Theorem are *effective*, ie. they do not provide an algorithm that guarantees to find $C(\mathbb{Q})$. In particular, finding $C(\mathbb{Q})$ for a specific hyperelliptic curve happens to be a difficult task in general.

In this Bachelor thesis I present a special case of the two-cover descent, that is an approach which can be used to demonstrate that the set $C(\mathbb{Q})$ is empty if some favorable conditions are met. In further sections I discuss the possibility to generalize the method, so that it can determine whether a curve of the form $y^3 = f(x)$ has no rational points. To do the above mentioned generalization I considered two possible approaches that mimic the two-cover descent in the cubic case; namely a factorization of f into two polynomials, and a factorization into three polynomials.

The text is written so that it should be comprehensible to most bachelor students who have completed some abstract algebra courses, and are familiar with the notion of fields.

Key Words: Two-cover descent, Three-cover descent, 9-cover descent, Descent methods, Hyperelliptic curves, Rational points on curves

Contents

1 Introduction

1.1 Background

Attempts to find rational points on curves can already be traced back to the third century AD, namely to some of the methods developed by Diophantus [8, Page 3]. However, unlike the Greek mathematician who only solved examples of curves of genus 0, this thesis discuses curves of genus at least 2. More precisely in my Bachelor thesis I investigate ways to compute rational points of hyperelliptic curve of the form $C : y^2 = f(x)$, where f is a polynomial of degree ≥ 5. The set of those rational points is denoted as $C(\mathbb{Q})$.

A key result for determining the set of rational points of a curve $C(\mathbb{Q})$, was proven by Faltings, for which he received a Fields Medal in 1986 [8, Page 4]. The theorem by Faltings states that *for a curve of genus* 2 *or more the set* $C(\mathbb{Q})$ *is finite*. Thus, allowing us to conclude that any hyperelliptic curve C has either finitely many points or no points at all. It is however important to set forth that as of today there are no known algorithms for computing $C(\mathbb{Q})$, and no known algorithms for determining if $C(\mathbb{Q})$ is empty [6, Section 7]. The latter is the focus of the descent methods, discussed in this Bachelor thesis, which under some favorable conditions allow one to show that a given curve C has no rational points, and sometimes even compute a non-empty set $C(\mathbb{Q})$ (see Example 3.6.2).

1.2 Outline

The Bachelor thesis is organized as follows:

Prerequisites: In this section I give brief background information about algebraic geometry introducing affine varieties, weighted projective space, weighted projective varieties, unramified n-covers and resultants, along with properties and definitions related to those maps and objects. The notions discussed in the prerequisites are needed to properly define and describe the descent methods.

Two-cover Descent: This section presents a simplified version of the two-cover descent, based on Stoll's article [9]. Unlike Stoll, the considered method only uses the finite fields $\mathbb{F}_p$, and not the p-adic numbers. Towards the end of the section I added python code that can find rational affine points of curves D_d used in the descent method. Also the descent is applied to two examples, one in which the set of rational points $C(\mathbb{Q})$ is shown to be empty, another where the descent is used to compute a non-empty $C(\mathbb{Q})$.

Descent Generalizations: In this section I discuss a possible generalization of the two-cover descent to curves of the from $C\colon y^3 = f(x)$. Two different approaches are considered, one with a factorization of f into two polynomials, and another with a factorization of f into three polynomials.

Further Generalizations: This section presents a more general version of the two-cover descent, so that it can also be used to show that a particular curve C has no rational points even if all of its two-curves D_d have $\mathbb{F}_p$ points for all primes p, and real points. In order to do so I briefly describe the p-adic numbers. Finally I discuss which primes p need to be considered so that to access if a curve D_d has rational points.

Research Suggestions: A list of suggestions of topics related to this thesis that require further research.

2 Prerequisites

This section gives a brief list of definitions that are used throughout the thesis. It is meant to facilitate the reading for mathematics student at a bachelor level, by grouping all potentially new concepts for the reader. It is however not meant to be a complete account, but rather just provide the minimum knowledge that is necessary to understand the two-cover descent discussed in later sections.

2.1 Varieties

Most of this subsection is based on Siksek's paper [6].

A variety is a system of polynomial equations, that can be defined either in affine or projective space.
An affine variety $V \subseteq \mathbb{A}^n$ over a field k is a system of the form:

$$V : \begin{cases} f_1(x_1, ..., x_n) = 0, \\ \vdots \\ f_m(x_1, ..., x_n) = 0 \end{cases} \qquad f_i \in k[x_1, ..., x_n] \text{ where } f_i\text{'a are non-constant}$$

Definition 2.1 (set of l-rational points on a variety)**.** *Let $V \subseteq \mathbb{A}^n$ be a variety over some field k and let l be a field extension of k. Then the set of l-rational points of V is defined as:*

$$V(l) := \{(x_1, ..., x_n) \in V \mid (x_1, ..., x_n) \in l^n\}$$

Remark. This thesis will often consider $V(\mathbb{Q})$, i.e. the $\mathbb{Q}$-rational points of a variety over $\mathbb{Q}$. In that case instead of calling those '$\mathbb{Q}$-rational' points we simply say 'rational' points.

Definition 2.2 (Absolutely irreducible affine variety)**.** *A affine variety is absolutely irreducible if it cannot be written as a union of proper subvarieties over a field extension* [6, Example 4.7].

2.1.1 Dimension and smoothness of varieties

In order to introduce a definition for the dimension of a variety, we need to define the transcendence degree.

Definition 2.3 (Transcendence degree)**.** *Let K be a field, and L/K an extension. We define a transcendence basis S of L/K as a subset of L such that $L/K(S)$ is algebraic and for all subsets $\{\alpha_1, ..., \alpha_n\} \subseteq S$ there are no non-trivial polynomials $f \in K[X_1, ..., X_n]$ for which $f(\alpha_1, ..., \alpha_n) = 0$. We say that the transcendence degree of L over K is equal to $\#S$* [5, Chapter VIII. §1].

Proposition 2.1. *The choice of the set S in* Definition 2.3 *does not affect the transcendence degree of L/K* [5, Thm. 1.1., Chapter VIII. §1].

Then using the above we are able to get the more general definition of dimension of an affine variety:

Definition 2.4 (Function field)**.** *Let V be a absolutely irreducible affine variety over k defined by the equations:*

$$V : \begin{cases} f_1(x_1, ..., x_n) = 0, \\ \vdots \\ f_m(x_1, ..., x_n) = 0 \end{cases} \qquad f_i \in k[x_1, ..., x_n]$$

Then the function field of V, denoted $k(V)$, is defined as the fraction field of $k[x_1, ..., x_n]/(f_1, ..., f_m)$ [6, Section 4.4].

Definition 2.5 (Dimension of affine variety)**.** *An affine variety V defined over a field k has dimension equal to the transcendence degree of $k(V)/k$.*

Example 2.1. *A variety $V \subseteq \mathbb{A}^n$ defined by a single non-constant polynomial $V : f = 0$, has dimension $n-1$.*

Definition 2.6 (Smoothness of affine varieties)**.** *Let $V \subseteq \mathbb{A}^n$ be a variety of dimension d over a field k, and let $\overline{k}$ be an algebraic closure of k. Given a point $P \in V\left(\overline{k}\right)$ we say that V is smooth at P if the Jacobian matrix of V has rank $n-d$ when evaluated at P. Otherwise we say that V is singular at P.*
The variety V is called smooth or non-singular if it is smooth at all the points $P \in V(\overline{k})$ [6, Section 4.2].

2.2 Weighted Projective Space

Let $w_0, w_1, ..., w_n$ be positive integers. The weighted projective space $\mathbb{P}_{(w_0,w_1,...,w_n)}$ is a geometric object whose k-rational points
$(a_0, a_1, ..., a_n) \in k^{n+1} \setminus \{(0,0,...,0)\}$, where k is a field, satisfy the equivalence relation:

$$(a_0, a_1, ..., a_n) \sim (a_0', a_1', ..., a_n') \Leftrightarrow \exists\, \lambda \in k^\times \text{ such that } (\lambda^{w_0} a_0, \lambda^{w_1} a_1, ..., \lambda^{w_n} a_n) = (a_0', a_1', .., a_n').$$

The equivalence class of a point $(a_0, a_1, ..., a_n) \in k^{n+1} \setminus \{(0,0,...,0)\}$ is denoted $(a_0 : a_1 : ... : a_n)$, and the set of k-rational points in $\mathbb{P}_{(w_0,w_1,...,w_n)}$ is written as $\mathbb{P}_{(w_0,w_1,...,w_n)}(k)$ [8].

Remark. The weighted projective space can contain multiple singularities, however those are not a concern in this thesis since the curves that are considered in further sections do not intersect with those singularities in the weighted projective space. An example of such singularity of a weighted projective space, that does not affect hyperelliptic curves is discussed in Stoll's lecture notes [8, page 5].

2.2.1 Varieties in Weighted Projective Space

Before defining varieties in the weighted projective space, one first needs to consider how the notion of a homogeneous polynomial is affected by weights.

Definition 2.7 (Weighted polynomial ring)**.** *A weighted polynomial ring over k with $n+1$ variables is defined as a polynomial ring that assigns a degree (i.e. a weight) to each variable. That is given a weight w_i for each variable x_i, one states that* $\deg(x_i) = w_i$*, or more generally, given non-negative integers c_i one gets:*

$$\deg\left(\prod_{i=0}^{n} x_i^{c_i}\right) = \sum_{i=0}^{n} w_i c_i$$

The weighted polynomial ring, where the weight of each x_i is equal to w_i is denoted as [4, Section 3]:

$$k_{(w_0,w_1,...,w_n)}[x_0, x_1, ..., x_n]$$

Given the above polynomial ring, we say that a polynomial $f \in k_{(w_0,w_1,...,w_n)}[x_0, x_1, ..., x_n]$ is *w-weighted-homogeneous* of degree d if every monomial in f has degree d, that is for $b_i \in k$, and non-negative integers $c_j^{(i)}$, $m \in \mathbb{N}$ one has

$$f = \sum_{i=1}^{m} b_i \left(\prod_{j=0}^{n} x_j^{c_j^{(i)}}\right) \text{ where for all } 0 \leq i \leq n \text{ we get } \sum_{j=0}^{n} w_j c_j^{(i)} = d$$

Remark. Notice that for weights $(w_0, w_1, ..., w_n) = (1, 1, .., 1)$ we obtain the standard definition of a polynomial ring, and a homogeneous polynomial.

With the definitions above we can finally define a weighted projective variety.

Definition 2.8 (Weighted projective variety)**.** *A weighted projective variety $V \subsetneq \mathbb{P}_{(w_0,w_1,...,w_n)}$ is a system of the form*

$$V : \begin{cases} f_1(x_1, ..., x_n) = 0, \\ \vdots \\ f_m(x_1, ..., x_n) = 0 \end{cases} \qquad f_i \in k_{(w_0,w_1,...,w_n)}[x_0, x_1, ..., x_n] \textit{ are } w\textit{-weighted-homogenous of } \deg > 0$$

The relation between affine and weighted projective varieties can be best understood, by considering standard affine patches. Given a weighted projective variety $V \subseteq \mathbb{P}_{(w_0,w_1,...,w_n)}$ over k, of the form

$$V : \begin{cases} f_1(x_1, ..., x_n) = 0, \\ \vdots \\ f_m(x_1, ..., x_n) = 0 \end{cases}$$

A standard affine patch is obtained by setting all of $x_i's$ to 1 for a fixed i, where x_i has weight equal to one. This results in the following affine variety:

$$V' : \begin{cases} f_1(x_1, ..., x_i = 1, ..., x_n) = 0, \\ \vdots \\ f_m(x_1, ..., x_i = 1, ..., x_n) = 0 \end{cases}$$

One can see that the set of all points with $x_i \neq 0$ on V is in bijection with points on V'.

Definition 2.9 (Dimension of weighted projective variety). *The dimension of a weighted projective variety is equal to the dimension of any of its standard affine patches.*

Remark. All of the standard affine patches have the same dimension.

Definition 2.10 (Smoothness of weighted projective varieties). *A weighted projective variety $V \subseteq \mathbb{P}_{(w_0,w_1,...,w_n)}$ is smooth if all of its standard affine patches (i.e. $V \cap \{x_i = 1\}$) are smooth.*

Remark. The above definition can be used for any of the affine patches since their functions fields are isomorphic.

Definition 2.11 (Absolutely irreducible weighted projective variety). *A weighted projective variety is absolutely irreducible if it cannot be written as a union of proper subvarieties over a field extension* [6, Example 4.7].

2.3 Hyperelliptic Curves

Definition 2.12 (Curve). *A curve is a smooth, weighted projective, and absolutely irreducible 1-dimensional variety over a field k* [6].

Definition 2.13 (Hyperelliptic curve). *Let $g \geq 2$. A hyperelliptic curve of genus g over a field k, where $char(k) \neq 2$, is a variety of the weighted projective space $\mathbb{P}_{(1,g+1,1)}$ defined by an equation of the form $Y^2 = F(X, Z)$ where $F \in k[X, Z]$ is a squarefree homogeneous polynomial of degree $2g + 2$. We say that the curve C has genus g* [8].

Remark. We say that F is homogeneous and not w-weighted-homogenous, since the weights of X and Z are equal to one. Moreover, the polynomial that actually needs to be w-weighted-homogeneous for C be a weighted projective variety is $Y^2 - F(X, Z)$, for which it is indeed the case.

Notice that the way we defined the equivalence class on the weighted projective space is related to points on C; namely, given some $(\xi : \eta : \zeta) \in C$ take any $(\lambda\xi, \lambda^{g+1}\eta, \lambda\zeta) \in (\xi : \eta : \zeta)$, and observe:

$$\eta^2 - F(\xi, \zeta) = \left(\lambda^{g+1}\eta\right)^2 - F(\lambda\xi, \lambda\zeta) = \lambda^{2g+2}\eta^2 - \lambda^{2g+2}F(\xi, \zeta) = \lambda^{2g+2}\left(\eta^2 - F(\xi, \zeta)\right)$$

thus

$$\eta^2 = F(\xi, \zeta) \Leftrightarrow \left(\lambda^{g+1}\eta\right)^2 = F(\lambda\xi, \lambda\zeta)$$

Consider a hyperelliptic curve $C \colon Y^2 = F(X, Z)$ defined over $\mathbb{Q}$, with $F \in \mathbb{Z}[X, Z]$. We define the set $C(\mathbb{F}_p)$ as the set of $\mathbb{F}_p$ points on $\overline{C} \colon Y^2 = \overline{F}(X, Z)$, where $\overline{F}$ is obtained by reducing the coefficients of F mod p. One can see that if $C(\mathbb{Q})$ is non empty then $C(\mathbb{F}_p)$ is non empty for all primes p. Namely, using the defined above equivalence relation on points of C, one can see that any point in $C(\mathbb{Q})$ can be represented by $(a : b : c)$ where a, b, c are coprime integers, allowing us to reduce those integers mod p, and therefore showing that whenever C has rational points then $C(\mathbb{F}_p)$ is non-empty for all primes p.

2.3.1 Affine notation of Hyperelliptic Curves

A hyperelliptic curve $C\colon Y^2 = F(X,Z)$ is covered by two standard affine patches: $y^2 = F(x,1)$, and $w^2 = F(1,z)$. Moreover one can see that there exists a bijection between all points in $(\xi : \eta : \zeta) \in C$ with $\zeta \neq 0$ and the affine patch $y^2 = F(x,1)$. The bijection is given by the maps:

$$(\xi : \eta : \zeta) \mapsto \left(\frac{\xi}{\zeta}, \frac{\eta}{\zeta^{g+1}}\right) \text{ and } (\xi, \eta) \mapsto (\xi : \eta : 1)$$

Thus the first standard affine patch (i.e. $y^2 = F(x,1)$) can also be denoted using a one-variable polynomial $y^2 = f(x)$, where $f(x) = F(x,1)$, since all points of the affine patch $y^2 = F(x,1)$ can be bijectivley mapped to the points of $y^2 = f(x)$. This way we can denote hyperelliptic curves C with a single variate polynomial, i.e $C : y^2 = f(x)$. However, even when C is denoted using a single variate polynomial, the curve is still defined on the weighted projective space, that is C is always of the form $Y^2 = F(X,Z)$, but in most cases we only need to consider the simpler equation $y^2 = f(x)$. The only time the notation $y^2 = f(x)$ is insufficient is when checking for points that are only present on $w^2 = F(1,z)$.

Definition 2.14 (Points at infinity)**.** *Let $C : Y^2 = F(X,Z)$ be a hyperelliptic curve. Then $P = (X : Y : Z) \in C$ is a point at infinity if and only if $Z = 0$.*

Notice that the points at infinity are only contained in the $w^2 = F(1,z)$ affine patch, and cannot be found on $y^2 = F(x,1)$ (i.e. cannot be found by only looking for solutions to the simpler equation $y^2 = f(x)$), since for all points in C with $Z \neq 0$ there is a bijection to the affine patch $y^2 = F(x,1)$. That is why when looking for k-rational points of a curve $C : y^2 = f(x)$ we distinguish three possible answers:

$$\begin{aligned}
C(k) &= \{(\xi,\eta) \in k \ : \ \eta^2 = f(\xi)\} \cup \{\infty\} && \text{if } 2 \nmid \deg(f) && (1)\\
C(k) &= \{(\xi,\eta) \in k \ : \ \eta^2 = f(\xi)\} && \text{if } 2 \mid \deg(f) \text{ and } \operatorname{lcf}(f) \neq \square && (2)\\
C(k) &= \{(\xi,\eta) \in k \ : \ \eta^2 = f(\xi)\} \cup \{\infty_s, \infty_{-s}\} && \text{if } 2 \mid \deg(f) \text{ and } \operatorname{lcf}(f) = s^2, s \in k && (3)
\end{aligned}$$

where $\operatorname{lcf}(f)$ is the leading coefficient of f [9, Section 2].

The sets $\{\infty\}$, and $\{\infty_s, \infty_{-s}\}$ in (1) and (3) represent the points at infinity in $C(k)$ (there are no points at infinity in $C(k)$ in case (2)).
In (1), there is only one point at infinity, that is $(1 : 0 : 0)$. Because the degree of f is odd its homogenization is of the form $F(x,z) = 0x^n + a_{n-1}x^{n-1}z + ... + a_1xz^{n-1} + a_0z^n$, thus $F(1,0) = 0$. In cases (2) and (3) the homogenization of f is $F(x,z) = a_nx^n + a_{n-1}x^{n-1}z + ... + a_1xz^{n-1} + a_0z^n$ where $a_n \neq 0$. Therefore the points at infinity are obtained from

$$y^2 = F(1,0) = 1^n a_n + 1^{n-1} \cdot 0a_{n-1} + ... + 1 \cdot 0^{n-1}a_1 + 0^n a_0 = a_n$$

where a_n is also the leading coefficient of f. Hence if a_n is not a square in k there are no points at infinity in $C(k)$ (case (2)), and if a_n is a square in k there are two points at infinity in $C(k)$ i.e. $(1 : \pm\sqrt{a_n} : 0)$, as described by case (3).

2.4 Unramified n-covers

Definition 2.15 (Unramified n-cover)**.** *Let C and D be curves defined over $\mathbb{Q}$ and $\phi : C \to D$ be a rational map, i.e. let ϕ be defined by rational functions. We say that ϕ is an unramified n-cover if all points in $C(\overline{\mathbb{Q}})$ have exactly n elements in their ϕ preimage, i.e. for any $P \in C(\overline{\mathbb{Q}})$ one has $\#\phi^{-1}(P) = n$.*

Remark. What is defined above as a ‘2-cover’ is refereed to as ‘double-cover’ or ‘two-cover’ in other parts of this thesis. Similarly, ‘3-cover’ and ‘three-cover’ are used interchangeably.

2.5 Resultant

The resultant of two single variate polynomials

$$f(x) = f_n x^n + f_{n-1}x^{n-1} + ... + f_1 x + f_0$$
$$g(x) = g_m x^m + g_{m-1}x^{m-1} + ... + g_1 x + g_0$$

is given by the determinant of the following $(n+m) \times (n+m)$ matrix:

$$\operatorname{Res}(f,g) := \begin{vmatrix} f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 \\ 0 & \cdots & 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 \\ 0 & \cdots & 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 \end{vmatrix}$$

Given two homogeneous polynomials

$$F(x,z) = f_n x^n + f_{n-1}x^{n-1}z + ... + f_1 xz^{n-1} + f_0 z^n$$
$$G(x,z) = g_m x^m + g_{m-1}x^{m-1}z + ... + g_1 xz^{m-1} + g_0 z^m$$

we can define their resultant as the determinant of the $(n+m) \times (n+m)$ matrix:

$$\operatorname{Res}(F,G) := \begin{vmatrix} f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 & 0 \\ 0 & \cdots & 0 & f_n & f_{n-1} & \cdots & f_1 & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 \\ 0 & \cdots & 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 \end{vmatrix}$$

Notice that both definitions seem very similar, however it is important to point out that both matrices depend on the degree of the polynomials. Thus, in the single variate case we rely only on the highest power of x, whereas in the multivariate case the size of the matrix depends on the degree of homogenization. That is why when we consider a polynomial $F(x,z) = 0x^n + f_{n-1}x^{n-1}z + ... + f_1 xz^{n-1} + f_0 z^n$, the resultant of its dehomogenization $f(x) = F(x,1)$ will give raise to different result.

It can be shown that the resultant of the homogeneous polynomials has the following properties [9, Section 6.2.]:

1. $\operatorname{Res}(G, F) = (-1)^{\deg F \deg G} \operatorname{Res}(F, G)$
2. $\operatorname{Res}(F, c) = c^{\deg F}$ where c is a contstnt
3. $\operatorname{Res}(F(x, z), -\beta x + az) = F(\alpha, \beta)$
4. $\operatorname{Res}(F, GH) = \operatorname{Res}(F, G) \operatorname{Res}(F, H)$
5. $\operatorname{Res}(F, G) = \operatorname{Res}(F, G + FH)$ if $\deg F + \deg H = \deg G$
6. $\operatorname{Res}(F \circ \gamma, G \circ \gamma) = \det(\gamma)^{\deg F \deg G} \operatorname{Res}(F, G)$ where $\gamma \in GL(2, k)$, and k is the ambient field.

However the two properties that are the most important in this thesis are

Proposition 2.2. *Let F and G be two homogeneous polynomials. Then,*

1. $\operatorname{Res}(F, G) = 0 \Leftrightarrow F$ *and* G *have a common factor*
2. *Let p be a prime, $\overline{F}, \overline{G}$ be the polynomials obtained by reducing the coefficients of $F, G \in \mathbb{Z}[X, Z]$* $\bmod p$*, and* $\overline{\operatorname{Res}(F, G)} := \operatorname{Res}(F, G) \mod p$*. Then,* $\operatorname{Res}(\overline{F}, \overline{G}) = \overline{\operatorname{Res}(F, G)}$*, that is the resultant of the polynomials with coefficients* $\bmod p$*, is equal to the resultant* $\bmod p$*.*

Proof. 1.(⇐:) Assume that F and G have a common factor

$$h(x, z) = a_n x^n + a_{n-1} x^{n-1} z + \cdots + a_1 x z^{n-1} + a_0 z^n.$$

Then we can rewrite the polynomials as $F = hf$ and $G = hg$ for some polynomials f, g. It follows that

$$\begin{aligned} \operatorname{Res}(F, G) &= \operatorname{Res}(F, hg) = \operatorname{Res}(F, h) \operatorname{Res}(F, g) \\ &= (-1)^{\deg F \deg h} \operatorname{Res}(h, hf)(-1)^{\deg F \deg g} \operatorname{Res}(g, hf) \\ &= (-1)^{\deg F (\deg h + \deg g)} \operatorname{Res}(h, hf) \operatorname{Res}(g, hf) \\ &= (-1)^{\deg F \deg G} \operatorname{Res}(h, h) \operatorname{Res}(h, f) \operatorname{Res}(g, hf) \end{aligned}$$

Thus, we can see that $\operatorname{Res}(F, G)$ is a multiple of $\operatorname{Res}(h, h)$. Observe that $\operatorname{Res}(h, h)$ is a $2n \times 2n$ matrix, where the first n rows are the same as the last n rows, allowing us to conclude that the determinant is zero i.e. $\operatorname{Res}(h, h) = 0$. It follows that $\operatorname{Res}(F, G)$ is zero.

1.(⇒): Assume that $\operatorname{Res}(F, G) = 0$.
Let $f(x) := F(x, 1)$, and $g(x) := G(x, 1)$.

Case 1: $\operatorname{Res}(f, g) = 0$:
By observing the determinant of the matrix from which the resultant of f and g is computed we conclude that the following terms are linearly dependent:

$$f, xf.x^2 f, ..., x^{m-1} f, g, xg, x^2 g, ..., x^{n-1} g$$

Thus there must exist some non-zero $\lambda_i \in k$ for which

$$\begin{aligned} 0 &= \lambda_1 f + \lambda_2 x f + ... + \lambda_m x^{m-1} f + \lambda_{m+1} g + \lambda_{m+2} x g + ... + \lambda_{n+m} x^{n-1} g \\ &= \left(\lambda_1 + \lambda_2 x + ... + \lambda_m x^{m-1}\right) f + \left(\lambda_{m+1} + \lambda_{m+2} x + ... + \lambda_{n+m} x^{n-1}\right) g \end{aligned}$$

The above implies that there exist some polynomials in $k[X]$ such that $fh_1 = gh_2$, and notice that $\deg(h_2) \leq \deg(f) - 1$. Thus, there must exist at least one $\alpha \in \overline{k}$ for which $f(\alpha) = 0$, but $h_2(\alpha) \neq 0$. All of the above allows us to conclude that α must also be a root of g, and thus f and g share a common factor.
Since we have shown that there exists some $\alpha \in \overline{k}$ such that $f(\alpha) = g(\alpha) = 0$, it follows that $F(\alpha, 1) = G(\alpha, 1) = 0$, allowing us to conclude that F and G share a common factor.

Case 2: $\mathrm{Res}(f,g) \neq 0$:
Our assumption implies that $\mathrm{Res}(F,G)$ is different from $\mathrm{Res}(f,g)$, thus F or G need to have a zero coefficient next to the term with the highest power of x. Without loss of generality we assume that $F(x,z) = 0x^n + f_{n-1}x^{n-1}z + ... + f_1xz^{n-1} + f_0z^n$. Then using the definition of the resultant and the definition of the determinant we observe:

$$\mathrm{Res}(F,G) = \begin{vmatrix} 0 & f_{n-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & 0 & f_{n-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & 0 & f_{n-1} & \cdots & f_1 & f_0 & 0 \\ 0 & \cdots & 0 & 0 & f_{n-1} & \cdots & f_1 & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 \\ 0 & \cdots & 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 \end{vmatrix}$$

$$= g_m \begin{vmatrix} f_{n-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_{n-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & f_{n-1} & \cdots & f_1 & f_0 & 0 \\ 0 & \cdots & 0 & f_{n-1} & \cdots & f_1 & f_0 \\ g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & g_m & g_{m-1} & \cdots & g_1 & g_0 & 0 \\ 0 & \cdots & g_m & g_{m-1} & \cdots & g_1 & g_0 \end{vmatrix}$$

Notice that we only obtain one matrix, since all others are multiplied by zeros from the first column. Moreover, the remaining matrix is equal to $\mathrm{Res}(f,g)$, namelt it has the correct dimansions and starts with the leading coefficient of f (Note if f would have an even smaller degree we can repeat the process above until obtaining a matrix equal to $\mathrm{Res}(f,g)$). Since by our assumption $\mathrm{Res}(f,g) \neq 0$, the equation above implies that $g_m = 0$. Hence, allowing us to state that the polynomial z is a common factor of both F and G.

Thus, one can observe that $\mathrm{Res}(F,G) = 0$ implies that F and G have a common factor.

2.: Knowing that for any matrix A with coefficients in $\mathbb{Z}$ we have that $\det(\overline{A}) = \overline{\det(A)}$, it follows that $\mathrm{Res}(\overline{F},\overline{G}) = \overline{\mathrm{Res}(F,G)}$. □

A related notion to the resultant is the discriminant.

Definition 2.16 (Discriminant)**.** *Let k be a filed and let $f \in k[X]$, with $deg(f) = n$, leading coefficient a, and let f' be the derivative of f. Then the discriminant of f is defined as:*

$$disc(f) := \frac{(-1)^{n(n-1)/2}}{a}\,\mathrm{Res}(f,f')$$

Lemma 2.3. *A polynomial $f \in k[x]$ has a multiple root if and only if its discriminant is equal to zero.*

Proof. Observe that $\frac{(-1)^{n(n-1)/2}}{a}$ is not equal to zero. It follows that whenever $\mathrm{disc}(f) = 0$, then $\mathrm{Res}(f,f') = 0$. By Proposition 2.2 we know that $\mathrm{Res}(f,f')$ is equal to zero if and only if f and f' share a root, i.e. f has a mutiple root. □

3 Two-cover Descent

This section presents a two-cover descent method based on Stoll's article [9].

3.1 The curves C and D_d

Consider a hyperelliptic curve $C\colon y^2 = F(x,1)$ over $\mathbb{Q}$, of genus g, with $f \in \mathbb{Z}[X]$, such that $f(x) = f_1(x)f_2(x)$ for some $f_1, f_2 \in \mathbb{Z}[X]$ where the degree of f_1 or f_2 is even.

Remark. The exact reason for the degree of at least one of the polynomials being even is discussed in detail in Section 3.1.1.

Assume that $P = (\xi, \eta) \in C(\mathbb{Q})$. It follows that:

$$\eta^2 = f(\xi) = f_1(\xi)f_2(\xi)$$

The above implies that for some $\eta_1, \eta_2 \in \mathbb{Q}$ one has $d\eta_1^2 = f_1(\xi)$, and $d\eta_2^2 = f_2(\xi)$, where d is a unique non-zero squarefree integer; namely, d is the squarefree part of η, so that

$$f(\xi) = f_1(\xi)f_2(\xi) = d\eta_1^2 d\eta_2^2 = (d\eta_1\eta_2)^2 = \eta^2$$

The squarefree integer d will allow us to define curves D_d with which information about $C(\mathbb{Q})$ can be obtained.

3.1.1 The curves D_d

Let $d \in \mathbb{Z}$ be squarefree. We define D_d as the following variety over $\mathbb{Q}$:

$$D_d := \begin{cases} dY_1^2 = F_1(X,Z) \\ dY_2^2 = F_2(X,Z) \end{cases}$$

where $F = F_1F_2$, $f_i(x) = F_i(x,1)$, $\deg(F_i)$ is even, and $F_i \in \mathbb{Z}[X,Z]$ for $i = 1,2$.

Observe that the curve D_d is a weighted projective variety in $\mathbb{P}_{(1,\frac{\deg(F_1)}{2},\frac{\deg(F_2)}{2},1)}$

Moreover, one can see that F_1 and F_2 are:

Homogeneous: F_1 and F_2 are homogenizations of f_1 and f_2 respectively, and can be constructed as follows (taking the example of f_1):
Consider

$$f_1(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \text{ where } n \text{ is a even positive integer.}$$

The polynomial $F_1(x,z)$ is the degree n homogenization of $f_1(x)$ given by:

$$F_1(x,z) = a_nx^n + a_{n-1}x^{n-1}z + ... + a_1xz^{n-1} + a_0z^n \text{ where } n \text{ is a even positive integer.}$$

Remark. n is an even integer, however f_1 can still have an odd degree if $a_n = 0$.

From the definition above one can see that all the terms of F_1 have the same degree allowing us to conclude that F_1 and F_2 are homogeneous.

Squarefree: We know that $C : Y^2 = F(X,Z)$ is a hyperelliptic curve, as defined in Definition 2.13 and thus $F(X,Z)$ is squarefree. Knowing that F is squarefree one cannot have F_1 and F_2 not squarefree, because of the equation $F(X,Z) = F_1(X,Z)F_2(X,Z)$. This way we have shown that F_1 and F_2 are indeed squarefree.

Coprime (i.e. they do not have common factors in $\mathbb{Z}[X,Z]$): First one can see (as shown above) that $F(X,Z) = F_1(X,Z)F_2(X,Z)$ is squarefree. If F_1 and F_2 were to have a common factor G then we could get $G^2 \big| F_1F_2 = F$, hence contradicting the fact that C is a hyperelliptic curve (since F is squarefree). Therefore, we can conclude that F_1 and F_2 are indeed coprime.

Remark. The above shows the reasons why not both $\deg(f_1)$ and $\deg(f_2)$ can be odd. Namely, z would be a common factor of F_1 and F_2, contradicting F being squarefree. That is why for the use of the descent method the assumption that at least one of f_1 or f_2 has an even degree is required.

Note that the curves D_d can also be considered in their affine versions:

$$D_d := \begin{cases} dy_1^2 = f_1(x) \\ dy_2^2 = f_2(x) \end{cases}$$

however, for now we will focus on using the weighted projective notation.

Before discussing the relation of D_d and C we give more explanations as to why D_d is a curve, despite being defined with two equations. To do so we compute the dimension of D_d, that is computing the transcendence degree of $k(D_d)$, over k, where k is the field on which the curve D_d is defined on.
To do the above one starts by observing that $k(x)$ has transcendence degree one over k. Namely, there exists no non-trivial polynomial f in $k[X]$ such that $f(x) = 0$, thus $k(x)/k$ has indeed transcendence degree one.
One can see that $\frac{1}{d}f_1(x), \frac{1}{d}f_2(x) \in k(x)$. Moreover, $y_i^2 = \frac{1}{d}f_i(x)$, thus y_i is a square root of some element in $k(x)$, implying that y_i is algebraic over $k(x)$. Therefore we deduce that $dY^2 - f_i(x)$ is the minimal polynomial of y_i in $k(x)[Y]$, allowing us to conclude: $k(x)[y_1]/(dy_1^2 - f_i(x))$ is an algebraic extension of $k(x)$.
Similarly one can show that $\left(k(x)[y_1]/dy_1^2 - f_1(x)\right)[y_2]/(dy_2^2 - f_2(x))$ is an algebraic extension of $k(x)[y_1]/(dy_1^2 - f_1(x))$. This way we have obtained the following field tower:

$$\begin{tikzcd}
\left(k(x)[y_1]/(dy_1^2 - f_1(x))\right)[y_2]/(dy_2^2 - f_2(x)) \arrow[d, dash, "\text{algebraic extension}"] \\
k(x)[y_1]/(dy_1^2 - f_1(x)) \arrow[d, dash, "\text{algebraic extension}"] \\
k(x) \arrow[d, dash, "\text{transcendence degree 1}"] \\
k
\end{tikzcd}$$

From the above one can see that the extension $k(D_d) = \left(k(x)[y_1]/dy_1^2 - f_1(x)\right)[y_2]/(dy_2^2 - f_2(x))$ over k has transcendence degree one, hence the variety D_d has dimension 1, i.e. D_d is a curve.

The curve D_d can be mapped to C using the unramified double cover π_d:

$$\pi_d : D_d \to C$$
$$(X : Y_1 : Y_2 : Z) \mapsto (X : dY_1Y_2 : Z)$$

The map π_d is indeed well-defined, because given a point $A = (X' : Y_1' : Y_2' : Z') \in D_d$ we get

$$\begin{cases} dY_1'^2 = F_1(X', Z') \\ dY_2'^2 = F_2(X',' Z') \end{cases} \Rightarrow F(X', Z') = F_1(X', Z')F_2(X', Z') = (dY_1'Y_2')^2$$

so indeed $\pi_d(X' : Y_1' : Y_2' : Z') = (X' : dY_1'Y_2' : Z') \in C$, for any $(X' : Y_1' : Y_2' : Z') \in D_d$.

We will now show that π_d is an unramified double-cover.

Take any $(X' : Y' : Z') \in C(\overline{\mathbb{Q}})$, and notice that evaluating F_1 and F_2 at (X', Z') gives a point on D_d, namely $(X' : \sqrt{\frac{F_1(X',Z')}{d}} : \sqrt{\frac{F_2(X',Z')}{d}} : Z')$.

Remark. The numbers $\sqrt{\frac{F_1(X',Z')}{d}}$ and $\sqrt{\frac{F_2(X',Z')}{d}}$ are not necessarily rational since d is squarefree, however the map π_d is not only defined on rational points of the curves, but on all points in $D_d(\overline{\mathbb{Q}})$. In fact if we restrict the map π_d to only rational points on the curves, the restricted version is not necessarily surjective on rational points of C, forcing us to consider all the respective maps for any squarefree d when checking whether $C(\mathbb{Q})$ is empty or not. More explanations are provided in the proof of Proposition 3.2.

One can see that

$$\begin{aligned}\pi_d(X' : \sqrt{\frac{F_1(X',Z')}{d}} : \sqrt{\frac{F_2(X',Z')}{d}} : Z') &= (X' : d\frac{\sqrt{F_1(X',Z')F_2(X',Z')}}{d} : Z') \\ &= (X' : \sqrt{F_1(X',Z')F_2(X',Z')} : Z').\end{aligned}$$

Thus, knowing that $F(X',Z') = F_1(X',Z')F_2(X',Z')$ we get:

$$\left(\sqrt{F_1(X',Z')F_2(X',Z')}\right)^2 = F_1(X',Z')F_2(X',Z') = F(X',Z') = Y'^2$$

This way have shown that any arbitrary point $(X' : Y' : Z') \in C(\overline{\mathbb{Q}})$ has a non-empty pre-image in $\pi_d\left(D_d(\overline{\mathbb{Q}})\right)$, hence the map π_d is surjective.

Assume that for two points $(X' : Y_1' : Y_2' : Z'), (X'' : Y_1'' : Y_2'' : Z'') \in D_d$ one has

$$\pi_d(X' : Y_1' : Y_2' : Z') = \pi_d(X'' : Y_1'' : Y_2'' : Z'').$$

By the definition of π_d we get $X' = X''$ and $Z' = Z''$. Hence,

$$dY_i'^2 = F_i(X',Z') = F_i(X'',Z'') = dY_i''^2 \Rightarrow |Y_i'| = |Y_i''| \text{ for } i = 1,2$$

implying that either $Y_i' = Y_i''$ or $Y_i' = -Y_i''$.
Assume that $Y_1' = Y_1''$, and $Y_2' = -Y_2''$, then

$$\begin{aligned}\pi_d(X' : Y_1' : Y_2' : Z') &= (X' : dY_1'Y_2' : Z') \\ \pi_d(X'' : Y_1'' : Y_2'' : Z'') = \pi_d(X' : Y_1' : -Y_2' : Z') &= (X' : -dY_1'Y_2' : Z') \\ &\Rightarrow \pi_d(X' : Y_1' : Y_2' : Z') \neq \pi_d(X'' : Y_1'' : Y_2'' : Z'')\end{aligned}$$

hence the above contradicts our assumption. A similar reasoning can be made with $Y_1' = -Y_1''$, and $Y_2' = Y_2''$.
Therefore, we conclude that $\pi_d(X' : Y_1' : Y_2' : Z') = \pi_d(X'' : Y_1'' : Y_2'' : Z'')$, if and only if

$$(X' : Y_1' : Y_2' : Z') = (X'' : Y_1'' : Y_2'' : Z''), \text{ or } (X' : Y_1' : Y_2' : Z') = (X'' : -Y_1'' : -Y_2'' : Z'')$$

Thus, all points in $C(\overline{\mathbb{Q}})$ have a double-preimage.

This way we have shown that π_d is indeed an unramified double cover, i.e. a mapping for which any point on C has a preimage with exactly two points.

Remark. The above proof shows that π_d is an unramified double-cover for curves C and D_d defined over a field of characteristic 0, however this property of π_d can be generalized to any field of characteristic not equal to 2.

It is also worth pointing out that the map π_d restricts to the standard affine patches of the curves D_d and C as follows:

$$\begin{aligned}\pi_d : D_d &\to C \\ (x, y_1, y_2) &\mapsto (x, dy_1y_2)\end{aligned}$$

Moreover the map π_d can be used to compute the genus of the curve D_d using the Riemann-Hurwitz formula. This thesis applies the above mentioned formula only to unramified n-covers, and thus only this particular case is stated below.

Theorem 3.1 (Simplified Riemann-Hurwitz formula)**.** *Let C_1 and C_2 be smooth curves defined over a field of characteristic zero, with genus g_1 and g_2 respectively. Let $\pi : C_1 \to C_2$ be an unramified n-cover. Then* [2, Theorem 8.7.3]:

$$2g_1 - 2 = n(2g_2 - 2)$$

3.2 $C(\mathbb{Q})$ as a union

Proposition 3.2. *Given a hyperelliptic curve $C : Y^2 = F(X, Z)$, with $F \in \mathbb{Z}[X, Z]$, such that $F(X, Z) = F_1(X, Z)F_2(X, Z)$ for some $F_1, F_2 \in \mathbb{Z}[X, Z]$, and curves defined the same way as in the previous section for all squarefree integers d $D_d : dY_1^2 = F_1(X, Z), dY_2^2 = F_2(X, Z)$, one has*

$$C(\mathbb{Q}) = \bigsqcup_{d \text{ squarefree}} \pi_d(D_d(\mathbb{Q})),$$

where the union of $\pi_d(D_d(\mathbb{Q}))$'s is disjoint.

Proof. Take any affine point $(\xi, \eta) \in C(\mathbb{Q})$. Then we obtain a curve $D_d : dy_1 = f_1(x), dy_2 = f_2(x)$, where d is the squarefree part of η, and for which $(\xi, \eta) \in \pi_d(D_d(\mathbb{Q}))$. Thus, the union of $\pi_d(D_d(\mathbb{Q}))$ contains all affine points of C. Moreover, given any point at infinity $(1 : \eta : 0) \in C(\mathbb{Q})$, one can also see that there must exist a unique squarefree integer e such that the map $\pi_e(1 : \eta_1 : \eta_2 : 0) = (1 : \eta : 0)$ where $\eta_1, \eta_2 \in \mathbb{Q}$.
Thus,

$$C(\mathbb{Q}) \subseteq \bigcup_{d \text{ sqaurefree}} \pi_d(D_d(\mathbb{Q})) =: U.$$

Take any point $(\xi : \eta : \zeta) \in U$. It follows that there exists at least one squarefree d such that $(\xi : \eta : \zeta) \in \pi_d(D_d(\mathbb{Q}))$, therefore all points of U are in $C(\mathbb{Q})$, that is

$$U \subseteq C(\mathbb{Q}).$$

All of the above proves

$$C(\mathbb{Q}) = U.$$

We only need to show that the union U is disjoint to complete the proof. Remember that when defining the curves D_d, we observed that for any point $P = (\xi : \eta : \zeta) \in C(\mathbb{Q})$ there is a unique squarefree integer d such that $F(\xi, \zeta) = F_1(\xi, \zeta)F_2(\xi, \zeta) = d\eta_1 d\eta_2$, thus the points P can be found in at most one set $\pi_d(D_d(\mathbb{Q}))$. Therefore the intersection of any $\pi_d(D_d(\mathbb{Q}))$ and $\pi_e(D_e(\mathbb{Q}))$ where d and e are distinct squarefree integers is empty. □

3.3 Rational points of D_d

Let p be a prime such that $p|d$, and assume that there exist a point $(\xi : \eta_1 : \eta_2 : \zeta) \in D_d(\mathbb{F}_p)$. Then

$$\overline{F}_1(\xi, \zeta) = d\eta_1 \equiv 0 \mod p, \text{ and } \overline{F}_2(\xi, \zeta) = d\eta_2 \equiv 0 \mod p$$

thus, (ξ, ζ) is a common root of $\overline{F}_1$ and $\overline{F}_2$, which implies that they have a common factor.

Lemma 3.3. *Let p be a prime such that $p|d$, and assume that there exists a point $(\xi : \eta_1 : \eta_2 : \zeta) \in D_d(\mathbb{F}_p)$. Then $\zeta x - \xi z$ is a common factor of $\overline{F}_1$ and $\overline{F}_2$ mod p.*

Proof. Let $F_i(X, Z) = a_n X^n + a_{n-1}X^{n-1}Z + ... + a_1 XZ^{n-1} + a_0 Z$, and $\overline{F}_i$ be the polynomial defined by reducing the coefficients of F_i mod p.

Case 1: $\zeta = 0$
It follows that $\overline{F}_i(\xi, 0) = 0$ for $i = 1, 2$. Thus,

$$\begin{aligned}\overline{F}_i(\xi, 0) = \overline{a}_n \xi^n + \overline{a}_{n-1}\xi^{n-1} \cdot 0 + ... + \overline{a}_1 \xi \cdot 0^{n-1} + 0\overline{a}_0 = 0 \\ \Rightarrow \overline{a}_n \xi^n = 0\end{aligned}$$

Notice that ξ cannot be zero since the point $(0 : 0 : 0)$ is not part of the weighted projective space on which C is defined, as discussed in Section 2.2. Thus we conclude that $\overline{a}_n = 0 \mod p$, implying that $-z\xi = x0 - z\xi = x\zeta - z\xi$ is a common factor of $\overline{F_1}$ and $\overline{F_2}$.

Case 2: $\zeta \neq 0$.
Given the affine polynomials $f_i(x) = F_i(x, 1)$, let $\overline{f}_i$ be the polynomials obtained by reducing the coefficients of f mod p, where $i = 1, 2$. We compute

$$\begin{aligned}
\overline{0} &= \overline{F}_i(\xi, \zeta) \\
\Rightarrow \zeta^{-n}\overline{0} &= \zeta^{-n}\overline{F}_i(\xi, \zeta) \\
&= \zeta^{-n}\left(\overline{a}_n\xi^n + \overline{a}_{n-1}\xi^{n-1}\zeta + ... + \overline{a}_1\xi\zeta^{n-1} + \overline{a}_0\zeta^n\right) \\
&= \overline{a}_n\left(\xi\zeta^{-1}\right)^n + \overline{a}_{n-1}\left(\xi\zeta^{-1}\right)^{n-1} + ... + \overline{a}_1\left(\xi\zeta^{-1}\right) + \overline{a}_0 \\
&= \overline{f}_1(\xi\zeta^{-1})
\end{aligned}$$

Thus $\xi\zeta^{-1}$ is a root of $\overline{f}_i$ implying that $x - \xi\zeta^{-1}\big|\overline{f}_i(x)$. Moreover since we operate withing a field (i.e. in $\mathbb{F}_p$) we can multiply $x - \xi\zeta^{-1}$ by the unit ζ to obtain $\zeta x - \xi\big|\overline{f}_i(x)$. Because $\zeta x - \xi$ is dividing $\overline{f}_i(x)$, there must exist a $g(x) \in \mathbb{F}_p[X]$ for which

$$\overline{f}_i(x) = (\zeta x - \xi)\, g(x) \tag{4}$$

Let $G(x, z)$ be the $\deg(F_i) - 1$ homogenization of $g(x)$. Then by homogenizing both sides of (4) we obtain:

$$\overline{F}_i(x, z) = (\zeta x - \xi z)\, G(x, z) \Rightarrow \zeta x - \xi z\big|\overline{F}_i(x, z)$$

Hence $\zeta x - \xi z$ is indeed a common factor of $\overline{F}_1$ and $\overline{F}_2$. □

The above Lemma tells us what happens when a prime $p|d$ and D_d has $\mathbb{F}_p$ points, using it we can state further:

Theorem 3.4. *Given a curve $D_d : dY_1^2 = F_1(X, Z), dY_2^2 = F_2(X, Z)$, and a prime number p one has:*

$$p|d \textit{ and } D_d(\mathbb{F}_p) \textit{ is non-empty } \Rightarrow p|\ \mathrm{Res}(F_1, F_2).$$

Proof. As shown in Lemma 3.3 we know that whenever $p|d$ and $D_d(\mathbb{F}_p)$ is non empty, then F_1 and F_2 have a common factor mod p, which is equivalent to saying that $\mathrm{Res}(F_1, F_2) \equiv 0 \mod p$ i.e. $p|\ \mathrm{Res}(F_1, F_2)$; thus proving the theorem.

□

3.4 $C(\mathbb{Q})$ as a finite union and condition for $C(\mathbb{Q}) = \emptyset$

So far we have shown that $C(\mathbb{Q})$ can be found using an infinite union of $D_d(\mathbb{Q})$. Such a result might not seem useful for the moment, however going further we show how the infinite union can be reduced to finitely many cases, allowing one to feasibly check whether $C(\mathbb{Q})$ is empty in some cases.

In the previous sections we have shown what happens when there exists a $\mathbb{F}_p$-rational point on the curve D_d. This section focuses on how this criterion can be useful to make the union $\bigsqcup_{\text{squarefree } d} \pi_d(D_d(\mathbb{Q}))$ finite.

As a consequence of Theorem 3.4 we get:

Corollary 3.4.1. *Given a curve $D_d : dY_1^2 = F_1(X, Z), dY_2^2 = F_2(X, Z)$, and a prime number p such that $p|d$, one has:*

$$p \not| \mathrm{Res}(F_1, F_2) \textit{ and } p|d \Rightarrow D_d(\mathbb{F}_p) = \emptyset$$

Proof. Observe that $\mathrm{Res}(F_1, F_2) \in \mathbb{Z} \setminus \{0\}$, namely F_1 and F_2 are coprime hence their resultant is non-zero, moreover they have integer coefficients, so their resultant also needs to be an integer. Using Theorem 3.4 we get:

$$\begin{aligned}
p|d \text{ and } D_d(\mathbb{F}_p) \text{ is non-empty } &\Rightarrow p|\ \mathrm{Res}(F_1, F_2) \\
\text{implying: } p \not| \mathrm{Res}(F_1, F_2) &\Rightarrow p \not| d \text{ or } D_d(\mathbb{F}_p) \text{ is empty} \\
\text{thus we get: } p \not| \mathrm{Res}(F_1, F_2) \text{ and } p \,|\, d &\Rightarrow D_d(\mathbb{F}_p) \text{ is empty}
\end{aligned}$$

□

The above Corollary 3.4.1 allows us to find all curves D_d for which there potentially exists at least one prime p such that $D_d(\mathbb{F}_p)$ is empty.

Another possible approach to check if $D_d(\mathbb{Q})$ is empty consists of verifying if D_d has $\mathbb{R}$ points. Namely, since $\mathbb{Q} \subset \mathbb{R}$, then $D_d(\mathbb{Q}) \subset D_d(\mathbb{R})$, so if $D_d(\mathbb{R})$ is empty, then $D_d(\mathbb{Q})$ must also be empty.

Given the above we can finally restrict our problem to a finite set of squarefree integers d, and we do it as follows:

Theorem 3.5. *Let $C : y^2 = f_1(x)f_2(x)$ be a hyperelliptic curve such that $f_1, f_2 \in \mathbb{Z}[X]$, and the degree of f_1 or f_2 is even. For a squarefree integer d, let $D_d : dY_1^2 = F_1(X,Z), dY_2^2 = F_2(X,Z)$ be the curve, defined in the same way as in the earlier sections. Consider the set*

$$S := \{d \in \mathbb{Z} \ : \ d \text{ squarefree and } \forall \text{ primes } p \text{ one has } p|d \Rightarrow p| \operatorname{Res}(F_1, F_2)\}$$

Then S is finite and

$$C(\mathbb{Q}) = \bigsqcup_{d \in S} \pi_d(D_d(\mathbb{Q})).$$

Moreover if for all $d \in S$ one has the curve D_d has no $\mathbb{R}$ points, or no $\mathbb{F}_p$ points for some prime p then one can conclude that $C(\mathbb{Q})$ is empty

Proof. Any $d \in S$ can only be divisible by the finitely many primes that also divide $\operatorname{Res}(F_1, F_2)$ which is a non-zero integer. Thus, one can see that there are only finitely many primes that can divide d, allowing us to conclude that S must be finite.

For any $d \notin S$ there must exist a prime p such that $p|d$, but $p \not| \operatorname{Res}(F_1, F_2)$. Thus, by Corollary 3.4.1 we get that $D_d(\mathbb{F}_p) = \emptyset$, which implies that D_d has no rational points. The above in combination with Proposition 3.2 implies:

$$C(\mathbb{Q}) = \bigsqcup_{\text{squarefree } d} \pi_d(D_d(\mathbb{Q})) = \bigsqcup_{d \in S} \pi_d(D_d(\mathbb{Q}))$$

Moreover, if one assumes that for all $d \in S$ there exists a prime p such that $D_d(\mathbb{F}_p) = \emptyset$, or $D_d(\mathbb{R}) = \emptyset$ then for all $d \in S$ we get $\pi_d(D_d(\mathbb{Q})) = \emptyset$, implying that $C(\mathbb{Q})$ must also be empty.

□

The above theorem gives us $C(\mathbb{Q})$ as a finite union, and thus provides a method for checking whether C has no rational points. Still, Theorem 3.5 can be further generalised, as discussed in Section 5 of this thesis or in Stoll's article [9].

3.5 Python code

This subsection presents python code that can verify whether a curve D_d has points in $\mathbb{F}_p$ for finitely many primes p on its first standard affine patch. Note that even if one finds a suitable field $\mathbb{F}_p$ for which D_d has no affine points, one still needs to check for points at infinity to conclude $D_d(\mathbb{Q}) = \emptyset$.

Python Code:

```
#Finds all possible elements of F_p of the form dy^2, with y in F_p
def squares_mod_p_times_d(p,d):
  d_square_set = set()
  for i in range(p):
    d_square_i = (d*(i**2)) % p
    d_square_set.add(d_square_i)
  return d_square_set

#Gives all the possible solutions of a one variable polynomial mod p
def sols_mod_p(f,p):
  sol_list = []
  for i in range(p):
    sol_i = f(i) % p
    sol_list.append(sol_i)
  return sol_list

#turns a list into a set
def list_to_set(the_list):
  n = len(the_list)
  the_set = set()
  for i in range(n):
    the_list_elem = the_list[i]
    the_set.add(the_list_elem)
  return the_set

#This function lists all x's at which f yields solution of the form dy^2,
# for y in F_p
def good_sols(sol_list,square_set):
  n = len(sol_list)
  result = []
  for i in range(n):
    current_sol = sol_list[i]
    if current_sol in square_set:
      result.append(i)
  return result

#this function checks if within a list of primes, D_d has F_p-rational points
def Fp_reational_check(function_1,function_2,prime_list,d):
  np = len(prime_list)
  empty = set()
  Dd_empty_primes = []
  for i in range(np):
    #the prime number for which we want to find x's of points in D_d:
    prime = prime_list[i]
    squares = squares_mod_p_times_d(prime,d) #makes a list of all squares mod p
    #get a list of all solutions of f_1(x) mod p, starting from x = 0 to x = p-1:
    solution_list_f1 = sols_mod_p(function_1, prime)
    solution_list_f2 = sols_mod_p(function_2, prime) #same as line above for f_2
    #the line below turns all the solutions into a set,
    inputs_of_sols_set_f1 = list_to_set(good_sols(solution_list_f1,squares))
    inputs_of_sols_set_f2 = list_to_set(good_sols(solution_list_f2,squares))
    #intersect the x's for which f_1 and f_2 have a squared solution:
    x_points_on_Dd = inputs_of_sols_set_f1.intersection(inputs_of_sols_set_f2)
    if x_points_on_Dd == empty:
      Dd_empty_primes.append(prime)
  return Dd_empty_primes

#Example Implementation for the curve
#$D_1: x^2 + 10x - 7 = y_1^2, 3x^4 + 30x^3 - 31x^2 + 2x + 3 = y_2^2$:

def f_1(x):
  solution = x**2 + 10*x - 7
  return solution

def f_2(x):
  solution = 3*(x**4) + 30*(x**3) - 31*(x**2) + 2*x + 3
  return solution

d = 1
first_10_primes = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29]
```

```
empty_primes = Fp_reational_check(f_1,f_2,first_10_primes,d)
#Note: f_1 and f_2 need to be defined in the code
print("primes for which D_d(F_p) is empty "+ str(empty_primes))
#Note: the code only checks for primes in the list
#so here for [2, 3, 5, 7, 11, 13, 17, 19, 23, 29]

#Output:"primes for which D_d(F_p) is empty [5]"
```

3.6 Examples of descent on hyperelliptic curves

3.6.1 $C : y^2 = -3x^6 - 60x^5 - 248x^4 + 518x^3 - 240x^2 - 16x + 21$

We start by observing that the polynomial on the right hand side factors as follows:

$$-3x^6 - 60x^5 - 248x^4 + 518x^3 - 240x^2 - 16x + 21 = \left(x^2 + 10x - 7\right)\left(3x^4 + 30x^3 - 31x^2 + 2x + 3\right)$$

Let $f_1(x) = x^2 + 10x - 7$, and $f_2(x) = 3x^4 + 30x^3 - 31x^2 + 2x + 3$, and let $F_1(X, Z)$ and $F_2(X, Z)$ be their homogenization of degree 2 and 4 respectively.
We compute the resultant as follows:

$$\operatorname{Res}(F_1, F_2) = \begin{vmatrix} 1 & 10 & -7 & 0 & 0 & 0 \\ 0 & 1 & 10 & -7 & 0 & 0 \\ 0 & 0 & 1 & 10 & -7 & 0 \\ 0 & 0 & 0 & 1 & 10 & -7 \\ 3 & 30 & -31 & 2 & 3 & 0 \\ 0 & 3 & 30 & -31 & 2 & 3 \end{vmatrix} = 1$$

The above implies that $S = \{\pm 1\}$, since there are no primes that divide $\operatorname{Res}(F_1, F_2)$, thus the only squarefree integers d that satisfy $\forall\, p$ one has $p|d \Rightarrow p|\operatorname{Res}(F_1, F_2)$ are 1 and -1. This way we obtain the following curves:

$$D_\pm = \begin{cases} \pm y_1^2 & = x^2 + 10x - 7 \\ \pm y_2^2 & = 3x^4 + 30x^3 - 31x^2 + 2x + 3 \end{cases}$$

Using Riemann-Hurwitz formula (Theorem 3.1) we get that $D_\pm$ have both genus 3.

Reducing both curves to $\mathbb{F}_5$ gives us:

$$\overline{D_\pm} = \begin{cases} \pm y_1^2 & = x^2 + 3 \\ \pm y_2^2 & = 3x^4 + 4x^2 + 2x + 3 \end{cases}$$

where one can see that

$$\begin{aligned} \overline{f_1(0)} &= 3 \neq \square \\ \overline{f_2(1)} &= 2 \neq \square \\ \overline{f_1(2)} &= 2 \neq \square \\ \overline{f_1(3)} &= 2 \neq \square \\ \overline{f_2(4)} &= 3 \neq \square \end{aligned}$$

thus $\overline{D}_+$ has no $\mathbb{F}_5$ points on its first affine patch (Note: the same example is used in Section 3.5 with the python code). Moreover, since 3 and 2 are additive inverses mod 5, we can see that for all elements of $\mathbb{F}_5$ there is always at least one of the two polynomials that gives a result which is not of the form $-y^2$, allowing us to conclude that $\overline{D}_-$ has no $\mathbb{F}_5$ points on its first affine patch.
We show that there are no points at infinity as follows:

$$\overline{F_2(1,0)} = 3 \neq \square$$

hence $\overline{D}_\pm$ has no $\mathbb{F}_5$ points at infinity. We conclude that $D_\pm(\mathbb{F}_5) = \emptyset$ implying $D_\pm(\mathbb{Q}) = \emptyset$.

All of the above, along with Thm. 3.5 proves that $C(\mathbb{Q}) = \emptyset$.

A similar example of descent on a curve $C : y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2)$ can be found in Stoll's article [9, Example 6.2].

3.6.2 $C : y^2 = (x^2 + 1)(x^4 + 1)$

So far the reader could get the impression that the two-cover descent only allows to confirm a negative result, namely that $C(\mathbb{Q})$ is empty, however the example below presents a case where a double-cover descent can be used to find all elements of a non-empty set $C(\mathbb{Q})$.

Let $f_1(x) = x^2 + 1$, and $f_2(x) = x^4 + 1$, and let F_1 and F_2 be their respective homogenization. We start by computing the resultant:

$$\operatorname{Res}(F_1, F_2) = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} = 4$$

Thus the set of squarefree integers we need to consider is $S = \{\pm1, \pm2\}$. We directly discard -1 and -2, because the polynomials F_1 and F_2 give non-negative results for all (X, Z), allowing us to conclude that $D_{-1}(\mathbb{R}) = D_{-2}(\mathbb{R}) = \emptyset$. This way we are left with

$$D_1 = \begin{cases} Y_1^2 & = X^2 + Z^2 \\ Y_2^2 & = X^4 + Z^4 \end{cases}, \text{ and } D_2 = \begin{cases} 2Y_1^2 & = X^2 + Z^2 \\ 2Y_2^2 & = X^4 + Z^4 \end{cases}$$

where

$$C(\mathbb{Q}) = \pi_1(D_1(\mathbb{Q})) \cup \pi_2(D_2(\mathbb{Q}))$$

Using Riemann-Hurwitz formula (Theorem 3.1) we get that D_1 and D_2 have both genus 3.

One way to compute $C(\mathbb{Q})$ consists of finding all rational points of the curves $D_2' : 2Y_2^2 = X^4 + Z^4$ and $D_1' : Y_2^2 = X^4 + Z^4$. Namely consider the maps

$$\begin{aligned} \phi_i : D_i &\to D_i' \\ (X : Y_1 : Y_2 : Z) &\mapsto (X : Y_2 : Z) \end{aligned}$$

for $i = 1, 2$. Note that a point in $D_i(\mathbb{Q})$ gives raise to a point in $D_i'(\mathbb{Q})$, thus computing $\phi_i^{-1}(P) \cap D_i(\mathbb{Q})$ for all $P \in D_i'(\mathbb{Q})$ would allow us to find all elements of $D_i(\mathbb{Q})$. The diagram below presents all of the mapping used in this example:

$$\begin{tikzcd}
 & D_1 \arrow[dl, "\phi_1"'] \arrow[dr, "\pi_1"] & & D_2 \arrow[dl, "\pi_2"'] \arrow[dr, "\phi_2"] & \\
D_1' & & C & & D_2'
\end{tikzcd}$$

For $d = 1$: all affine solutions of $y_2^2 = x^4 + 1$, are $(0, \pm1)$. Namely, consider the following coordinate transformation:

$$y \mapsto \frac{u}{2} - \frac{v^2}{4u^2}; \quad x \mapsto \frac{v}{2u}$$

By substituting the above transformation in the equation $y^2 = x^4 + 1$ we get

$$\begin{aligned} y^2 &= x^4 + 1 \\ \Leftrightarrow \left(\frac{u}{2} - \frac{v^2}{4u^2}\right) &= \left(\frac{v}{2u}\right)^4 + 1 \\ \Leftrightarrow \frac{u^2}{4} - \frac{uv^2}{4u^2} + \frac{v^4}{16u^4} &= \frac{v^4}{16u^4} + 1 \\ \Leftrightarrow u^3 - v^2 &= 4u \\ \Leftrightarrow v^2 &= u^3 - 4u \end{aligned}$$

Notice that the above transformations is reversible, by taking

$$u \mapsto 2(y+x^2); \;\; v \mapsto 4x(y+x^2)$$

Moreover both of the transformations presented above are rational, that is they map all rational points of one curve into the other. Using the theory of elliptic curves one can see that the curve $v^2 = u^3 - 4u$ has exactly 4 rational points (for a detailed proof see [7, Chapter III.6, Example 2]). The above implies that D_1' must also have exactly four rational points. In order to find the remaining two we check for points at infinity. Observe that $y_2^2 = F_2(1,0) = 1$ has two solutions: $(\pm 1, 1)$.
Thus there are exactly four rational points on D_1'. Since we know the x coordinate for which solutions to $y^2 = x^4 + 1$ exists, in order to find all rational points of D_1 we need to verify if using the same x in the curve $Y_1^2 = X^2 + Z^2$ also gives raise to a rational point. Notice
that $f_2(0) = (0)^2 + 1 = (\pm 1)^2$, and $F_2(1,0) = (1)^2 + (0)^2 = (\pm 1)^2$; hence the set of rational points on D_1 is given by

$$D_1(\mathbb{Q}) = \{(0:1:\pm 1:1), (0:-1:\pm 1:1), (1:1:\pm 1:0), (1:-1:\pm 1:0)\}$$

For $d = 2$: all affine solutions of $2y_2^2 = x^4 + 1$, are $(\pm 1, \pm 1)$, and $(\pm 1, \mp 1)$. Namely, consider the following coordinate transformations as outlined in [1, Chapter 8]:
We start with $y \mapsto \frac{y}{x^2}$, and $x \mapsto \frac{1}{x} + 1$, which gives us

$$\begin{aligned} 2\left(\frac{y}{x^2}\right)^2 &= \left(\frac{1}{x}+1\right)^4 + 1 \\ \Leftrightarrow 2\frac{y^2}{x^4} &= \frac{1}{x^4} + 4\frac{1}{x^3} + 6\frac{1}{x^2} + 4\frac{1}{x} + 2 \\ \Leftrightarrow y^2 &= \frac{1}{2} + 2x + 3x^2 + 2x^3 + x^4 \end{aligned}$$

Notice that the right hand side of the equation above is equal to $(x^2+x+1)^2 - \frac{1}{2}$, therefore we can transform the equation further to get

$$(y - x^2 - x - 1)(y + x^2 + x + 1) = -\frac{1}{2}$$

Let $t := y + x^2 + x + 1$. It follows that

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

Let $s := xt$, and multiply both sides of the equation above by t^2 to obtain:

$$2s^2 + 2st + 2t^2 = t^3 + \frac{1}{2}t$$

We now map $s \mapsto \frac{1}{4}s$, and $t \mapsto \frac{1}{2}t$ to get:

$$\begin{aligned} \frac{s^2}{8} + \frac{1}{4}ts + \frac{1}{2}t^2 &= \frac{1}{8}t^3 + \frac{1}{4}t \\ \Leftrightarrow s^2 + 2ts + t^2 + 3t^2 &= t^3 + 2t \\ \Leftrightarrow (s+t)^2 &= t^3 - 3t^2 + 2t \end{aligned}$$

then let $v := s + t$, and $u := t - 1$ to obtain

$$\begin{aligned} v^2 &= (u+1)^3 - 3(u+1)^2 + 2(u+1) \\ \Leftrightarrow v^2 &= u^3 - u \end{aligned}$$

All of the above shows that there exists an invertible rational map from $2y^2 = x^4 + 1$ to $v^2 = u^3 - u$. Using the theory of elliptic curves (as described in [7, Chapter III.6, Example 1]) we can see that $v^2 = u^3 - u$ has exactly 4 rational points, implying that $2y_2^2 = x^4 + 1$ has exactly 4 rational points

as well, namely $(\pm 1, \pm 1), (\pm 1, \mp 1)$. Moreover $2Y_2^2 = X^4 + Z^4$ has no points at infinity, because $F_2(1,0) = 1^4 \neq 2Y_2^2$, for any $Y_2 \in \mathbb{Q}$.
By imputing $x = \pm 1$ to the second equation $2y_1^2 = x^2 + 1$ we get:

$$D_2(\mathbb{Q}) = \{(1 : 1 : -1 : \pm 1), (1 : 1 : 1 : \pm 1), (1 : -1 : 1 : \pm 1), (1 : -1 : -1 : \pm 1)\}$$

note that there cannot be any more points in $D_d(\mathbb{Q})$, since the equation $2Y_2^2 = X^4 + Z^4$ has rational solutions only for $X = \pm 1$, and $Z = 1$.

Using the mappings π_1 and π_2 we compute:

$$\pi_1(D_1(\mathbb{Q})) = \{(0 : \pm 1 : 1), (1 : \pm 1 : 0)\}$$
$$\pi_2(D_2(\mathbb{Q})) = \{(1 : \pm 2 : 1), (1 : \pm 2 : -1)\}$$

Thus all of the above along with Theorem 3.5 allows us to prove

$$C(\mathbb{Q}) = \{(0 : \pm 1 : 1), (1 : \pm 1 : 0), (1 : \pm 2 : 1), (1 : \pm 2 : -1)\}$$

4 Descent Generalizations

This section focuses on generalising the double-cover descent to curves of the form $C : Y^3 = F(X, Z)$. In order to do so we begin with restating the problem in terms of the new curve. Then I present two possible approaches: one that requires F be be factored into two polynomials, and another which requires F be factored into three polynomials.

4.1 New weighted projective plane

This section will consider curves defined over a field k where char$k \neq 3$, of the form $C : Y^3 = F(X, Z)$ where $F \in k[X, Z]$ is squarefree, and deg$F = 3n$ where $n \geq 2$ is a integer.

The weighed projective space on which $C : Y^3 = F(X, Z)$ is defined is $\mathbb{P}_{(1,n,1)}$. Similarly to the hyperelliptic curves discussed in Section 3 one can see that, for any $\lambda \in k^\times$ we get

$$(\lambda^n \eta)^3 - F(\lambda\xi, \lambda\zeta) = \lambda^{3n}\eta^3 - \lambda^{3n}F(\xi, \zeta) = \lambda^{3n}\left(\eta - F(\xi, \zeta)\right)$$

hence

$$\eta^3 = F(\xi, \zeta) \Leftrightarrow (\eta\lambda)^3 = F(\lambda\xi, \lambda\zeta) \text{ for all } \lambda \in k^\times$$

It can also be noted that it is not possible for a standard affine patch of C to be defined by a polynomial of degree congruent to $1 \mod 3$. Namely, consider

$$C : Y^3 = F(X, Z) = a_m X^m + a_{m-1}X^{m-1}Z + ... + a_1 X Z^{m-1} + a_0 Z^m$$

and assume that $\deg(f) \equiv 1 \mod 3$, where $f(x) = F(x, 1)$. Since $\deg(F)$ is divisible by 3, we conclude $\deg(f) = \deg(F) - 2 = m - 2$. From the way we defined f we observe

$$F(x, 1) = f(x) = a_m x^m + a_{m-1}x^{m-1} + ... + a_1 x + a_0$$

Since f has degree equal to $m - 2$, it follows $a_m = a_{m_1} = 0$. The above implies

$$F(X, Z) = a_{m-2}X^{m-2}Z^2 + a_{m-3}X^{m-3}Z^3 + ... + a_1 X Z^{m-1} + a_0 Z^m$$

hence $Z^2 | F(X, Z)$, contradicting the assumption that $F(X, Z)$ is squarefree. Therefore it is not possible for the polynomial f to have a degree congruent to $1 \mod 3$.

4.2 Points at infinity

Since we consider a new curve C it will have different possible configurations of points at infinity, analogous to the cases described by the equations (1), (2), and (3). Given the affine equation $y^3 = f(x)$ observe:

$C(k) = \{(\xi, \eta) \in k \ : \ \eta^3 = f(\xi)\} \cup \{\infty\}$ if $\deg(f) \equiv 2 \mod 3$

$C(k) = \{(\xi, \eta) \in k \ : \ \eta^3 = f(\xi)\}$ if $\deg(f) \equiv 0 \mod 3$ and lcf(f) is not a cube in k

$C(k) = \{(\xi, \eta) \in k \ : \ \eta^3 = f(\xi)\} \cup \{\alpha \in k : \alpha^3 = \text{lcf}(f)\}$ if $\deg(f) \equiv 0 \mod 3$ and lcf$(f) = s^3, s \in k$

The reasoning of the result above is also analogous to results (1), (2), and (3) discussed in Section 2.3.1.

4.3 Three-cover descent

4.3.1 The curves C, $D_d^{(1)}$, and $D_d^{(2)}$

Let $y^3 = f(x)$ be the affine equation of a curve $C\colon Y^3 = F(X, Z)$ defined as above, where $\deg(f) \not\equiv 1 \mod 3$, and $\deg(f) \geq 5$, with $f \in \mathbb{Z}[X]$ squarefree, and let f_1, f_2 be two polynomials in $\mathbb{Z}[X]$ such that $f_1(x)f_2(x) = f(x)$, and $\deg(f_1)$ or $\deg(f_2)$ is divisible by 3.

Assume that $P = (\xi, \eta) \in C(\mathbb{Q})$. It follows that there exist some cube free integers s_1 and s_2, and rational numbers η_1 and η_2 such that

$$\eta^3 = f(\xi) = f_1(\xi)f_2(\xi) = s_1\eta_1^3 s_2\eta_2^3.$$

We know that s_1 and s_2 are not cubes in $\mathbb{Q}$, however their product must be a cube. The above implies that there must be a unique non-zero cubefree integer d such that

$$s_1 = d^2, \text{ and } s_2 = d \quad \text{or} \quad s_1 = d, \text{ and } s_2 = d^2.$$

Thus we define the following two curves:

$$D_d^{(1)} := \begin{cases} d^2Y^3 & = F_1(X,Z) \\ dY^3 & = F_2(X,Z) \end{cases} \quad D_d^{(2)} := \begin{cases} dY^3 & = F_1(X,Z) \\ d^2Y^3 & = F_2(X,Z) \end{cases},$$

where $f_i(x) = F_i(x,1)$ for $i = 1,2$.
Note that despite being defined by two equations $D_d^{(1)}$ and $D_d^{(2)}$ are still curves. Showing that they have dimension equal to one can be done similarly to the computations of the dimension of D_d in section 3.1.1.

The polynomials F_1 and F_2 are homogeneous, coprime, squarefree, of degree divisible by 3. Reaching this conclusion can be made in a manner analogous to Section 3.1.1.

Given the curves above one can also define the following unramified three-covers:

$$\begin{aligned} \pi_d^{(1)} &: D_d^{(1)} \to C \\ (x : y_1 : y_2 : z) &\mapsto (x : dy_1y_2 : z) \end{aligned} \qquad \begin{aligned} \pi_d^{(2)} &: D_d^{(2)} \to C \\ (x : y_1 : y_2 : z) &\mapsto (x : dy_1y_2 : z) \end{aligned}$$

Our goal is to show that $\pi_d^{(1)}$, $\pi_d^{(2)}$ are unramified three-covers such that the rational point P satisfies:

$$P \in \pi_d^{(1)}\left(D_d^{(1)}(\mathbb{Q})\right) \cup \pi_d^{(2)}\left(D_d^{(2)}(\mathbb{Q})\right)$$

Since the maps are very similar we will show most of the results only on $\pi_d^{(1)}$.

Well defined: Take any $(\xi : \eta_1 : \eta_2 : \zeta) \in D_d^{(2)}$. Then observe $\pi_d^{(1)}(\xi : \eta_1 : \eta_2 : \zeta) = (\xi : d\eta_1\eta_2 : \zeta)$. Therefore

$$F(\xi,\zeta) = F_1(\xi,\zeta)F_2(\xi,\zeta) = d^2\eta_1^3 d\eta_2^3 = (d\eta_1\eta_2)^3$$

Hence we conclude that for any $(\xi : \eta_1 : \eta_2 : \zeta) \in D_d^{(1)}$ we get $\pi_d^{(1)}(\xi : \eta_1 : \eta_2 : \zeta) \in C$, proving that the map $\pi_d^{(1)}$ is well-defined (the same can be shown for $\pi_d^{(2)}$).

Triple preimage for all points on C: Take any $(\xi : \eta : \zeta) \in C(\overline{\mathbb{Q}})$, and observe that

$$\left(\xi : \sqrt[3]{\frac{F_1(\xi,\zeta)}{d^2}} : \sqrt[3]{\frac{F_2(\xi,\zeta)}{d}} : \zeta\right) \in D_d^{(1)}$$

it follows that

$$\pi_d^{(1)}\left(\xi : \sqrt[3]{\frac{F_1(\xi,\zeta)}{d^2}} : \sqrt[3]{\frac{F_2(\xi,\zeta)}{d}} : \zeta\right) = \left(\xi : d\sqrt[3]{\frac{F_1(\xi,\zeta)F_2(\xi,\zeta)}{d^3}} : \zeta\right) \quad = \left(\xi : \sqrt[3]{F_1(\xi,\zeta)F_2(\xi,\zeta)} : \zeta\right)$$

Thus $\eta^3 = F(\xi,\zeta) = F_1(\xi,\zeta)F_2(\xi,\zeta)$ allowing us to conclude that there exists a $A \in D_d^{(1)}(\overline{\mathbb{Q}})$ such that $\pi_d^{(1)}(A) = (\xi : \eta : \zeta)$ for all $(\xi : \eta : \zeta) \in C(\overline{\mathbb{Q}})$, in other words $\pi_d^{(1)}$ is surjective. A similar proof can be used to show that $\pi_d^{(2)}$ is also surjective.

Take any two $(X' : Y_1' : Y_2' : Z'), (X'' : Y_1'' : Y_2'' : Z'') \in D_d^{(1)}(\overline{\mathbb{Q}})$, such that

$$\pi_d^{(1)}(X' : Y_1' : Y_2' : Z') = \pi_d^{(1)}(X'' : Y_1'' : Y_2'' : Z'')$$

The way $\pi_d^{(1)}$ is defined allows us to deduce that $X' = X''$, and $Z' = Z''$, implying that

$$d^{3-i}(Y_i')^3 = F_i(X',Z') = F_i(X'',Z'') = d^{3-i}(Y_i'')^3 \text{ for } i = 1,2$$

$$\Rightarrow (Y_i')^3 = (Y_i'')^3 \text{ for } i = 1, 2$$

allowing us to conclude that $Y_i'' = \mu^k Y_i'$ where $\mu \in \overline{\mathbb{Q}}$ is a primitive third root of unity, and $k = 1, 2, 3$.
Case 1: $Y_1' = Y_1''$:
We know that $Y_2'' = \mu^k Y_2'$, thus

$$\begin{aligned}(X' : dY_1'Y_2' : Z') = \pi_d^{(1)}(X' : Y_1' : Y_2' : Z') &= \pi_d^{(1)}(X'' : Y_1'' : Y_2'' : Z'') \\ &= \pi_d^{(1)}(X' : Y_1' : \mu^k Y_2' : Z') = (X' : d\mu^k Y_1'Y_2' : Z') \\ &\Rightarrow dY_1'Y_2' = d\mu^k Y_1'Y_2' \Rightarrow 1 = \mu^k \Rightarrow k = 3\end{aligned}$$

Thus we conclude that $Y_2'' = \mu^3 Y_2' = Y_2'$, that is $(X' : Y_1' : Y_2' : Z') = (X'' : Y_1'' : Y_2'' : Z'')$.

Case 2: $Y_1'' = \mu Y_1'$:
We know that $Y_2'' = \mu^k Y_2'$, thus

$$\begin{aligned}(X' : dY_1'Y_2' : Z') = \pi_d^{(1)}(X' : Y_1' : Y_2' : Z') &= \pi_d^{(1)}(X'' : Y_1'' : Y_2'' : Z'') \\ &= \pi_d^{(1)}(X' : \mu Y_1' : \mu^k Y_2' : Z') = (X' : d\mu^{k+1} Y_1'Y_2' : Z') \\ &\Rightarrow dY_1'Y_2' = d\mu^{k+1} Y_1'Y_2' \Rightarrow 1 = \mu^{k+1} \Rightarrow k = 2\end{aligned}$$

Thus we conclude that $Y_2'' = \mu^2 Y_2'$, that is $(X' : \mu Y_1' : \mu^2 Y_2' : Z') = (X'' : Y_1'' : Y_2'' : Z'')$.

Case 3: $Y_1'' = \mu^2 Y_1'$:
We know that $Y_2'' = \mu^k Y_2'$, thus

$$\begin{aligned}(X' : dY_1'Y_2' : Z') = \pi_d^{(1)}(X' : Y_1' : Y_2' : Z') &= \pi_d^{(1)}(X'' : Y_1'' : Y_2'' : Z'') \\ &= \pi_d^{(1)}(X' : \mu^2 Y_1' : \mu^k Y_2' : Z') = (X' : d\mu^{k+2} Y_1'Y_2' : Z') \\ &\Rightarrow dY_1'Y_2' = d\mu^{k+2} Y_1'Y_2' \Rightarrow 1 = \mu^{k+2} \Rightarrow k = 1\end{aligned}$$

Thus we conclude that $Y_2'' = \mu^1 Y_2'$, that is $(X' : \mu^2 Y_1' : \mu Y_2' : Z') = (X'' : Y_1'' : Y_2'' : Z'')$.

All of the cases above exhaustively present all possible preimages of points on $C(\overline{\mathbb{Q}})$, thus allowing us to conclude that all points in $C(\overline{\mathbb{Q}})$ have exactly three elements in their $\pi_d^{(1)}$ preimage i.e. $\pi_d^{(1)}$ is an unramified three-cover. A similar proof can be done for $\pi_d^{(2)}$.

4.3.2 $C(\mathbb{Q})$ as a union

Proposition 4.1. *Let $C : Y^3 = F_1(X, Z)F_2(X, Z)$ be a curve defined as above, and consider the curves $D_d^{(1)} : d^2Y_1^3 = F_1(X, Z), dY^3 = F_2(X, Z)$ and $D_d^{(2)} : dY_1^3 = F_1(X, Z), d^2Y_2^3F_2(X, Z)$ defined as above for any non-zero cubefree integer d, with their respective unramified three covers $\pi_d^{(1)}$ and $\pi_d^{(2)}$. Then,*

$$C(\mathbb{Q}) = \bigsqcup_{d \text{ cubefree}} \left(\pi_d^{(1)}(D_d^{(1)}(\mathbb{Q})) \cup \pi_d^{(2)}(D_d^{(2)}(\mathbb{Q}))\right)$$

Proof. The curves $D_d^{(1)}$ and $D_d^{(2)}$ were defined in such a way that for any $P \in C(\mathbb{Q})$ there exists a unique cubefree d s.t. $P \in \pi_d^{(1)}(D_d^{(1)}(\mathbb{Q})) \cup \pi_d^{(2)}(D_d^{(2)}(\mathbb{Q}))$, hence $C(\mathbb{Q})$ is indeed contained in the union of $\pi_d^{(1)}(D_d^{(1)}(\mathbb{Q})) \cup \pi_d^{(2)}(D_d^{(2)}(\mathbb{Q}))$ over cubefree d's. Also one can see that the three-covers $\pi_d^{(1)}$ and $\pi_d^{(2)}$ can only map rational points to rational points, thus the union of mappings of rational points on curves $D_d^{(1)}$ and $D_d^{(2)}$ is contained in $C(\mathbb{Q})$. Therefore allowing us to conclude:

$$C(\mathbb{Q}) = \bigcup_{d \text{ cubefree}} \left(\pi_d^{(1)}(D_d^{(1)}(\mathbb{Q})) \cup \pi_d^{(2)}(D_d^{(2)}(\mathbb{Q}))\right)$$

Moreover observe that since for any $P \in C(\mathbb{Q})$ the cubefree integer d is unique, thus there exists at most one pair of curves $D_d^{(1)}$ and $D_d^{(2)}$ such that $P \in \pi_d^{(1)}(D_d^{(1)}(\mathbb{Q})) \cup \pi_d^{(2)}(D_d^{(2)}(\mathbb{Q}))$, allowing us to deduce that the union over cubefree integers must be disjoint.

□

Similarly to the two-cover descent we can develop a criterion to reduce the union in Proposition 4.1 to a finite one, moreover the reasoning is almost analogous to the two-cover descent presented previously.

Lemma 4.2. *Let p be a prime, and $D_d^{(1)}$, $D_d^{(2)}$ curves defined as earlier in this section. Then*

$$\operatorname{Res}(F_1, F_2) \in \mathbb{Z} \setminus \{0\}$$

Moreover,

$$p|d, \text{ and } p \nmid \operatorname{Res}(F_1, F_2) \Rightarrow D_d^{(1)}(\mathbb{Q}) \cup D_d^{(2)}(\mathbb{Q}) = \emptyset$$

Proof. We start by showing that $\operatorname{Res}(F_1, F_2) \in \mathbb{Z}\setminus\{0\}$. Since F_1 and F_2 are defined to have integer coefficients, it follows that $\operatorname{Res}(F_1, F_2) \in \mathbb{Z}$. We also know that F_1 and F_2 are coprime, thus by Proposition 2.2 we know $\operatorname{Res}(F_1, F_2) \neq 0$. With the above we conclude that $\operatorname{Res}(F_1, F_2) \in \mathbb{Z} \setminus \{0\}$.

The second statement of the lemma can be proven as follows:
Assume that $p|d$, and that there exists a point $(\xi : \eta_1 : \eta_2 : \zeta) \in D_d^{(1)}(\mathbb{F}_p) \cup D_d^{(2)}(\mathbb{F}_p)$. Then one can observe that in $\mathbb{F}_p$ we get:

$$\overline{F}_1(\xi, \zeta) = \overline{d^{3-i}}\eta_1 = 0, \text{ and } \overline{F}_2(\xi, \zeta) = \overline{d^{3-i}}\eta_2 = 0$$

where $i = 1, 2$ depending on whether the point $(\underline{\xi : \eta_1 : \eta_2 : \zeta})$ is in $D_d^{(1)}$ or $D_d^{(2)}$.
It follows that $\zeta x - \xi z$ is a common factor of $\overline{F_1}$ and $\overline{F_2}$, that is the polynomials obtained by reducing the coefficients of F_1 and F_2 mod p. Therefore, one can conclude:

$$\begin{aligned} p|d, \text{ and } D_d^{(1)}(\mathbb{F}_p) \cup D_d^{(2)}(\mathbb{F}_p) \neq \emptyset &\Rightarrow p| \operatorname{Res}(F_1, F_2) \\ p|d, \text{ and } p \nmid \operatorname{Res}(F_1, F_2) &\Rightarrow D_d^{(1)}(\mathbb{F}_p) \cup D_d^{(2)}(\mathbb{F}_p) = \emptyset \\ &\Rightarrow D_d^{(1)}(\mathbb{Q}) \cup D_d^{(2)}(\mathbb{Q}) = \emptyset \end{aligned}$$

□

Finally with all of the above we can state and prove the descent theorem for the three-cover descent.

Theorem 4.3. *Let C, $D_d^{(1)}$ and $D_d^{(2)}$ be curves defined as earlier in this section, and let*

$$S := \{d \in \mathbb{Z} \ : \ d \textit{ is cubefree, such that for all primes } p \textit{ we get } p|d \Rightarrow p| \operatorname{Res}(F_1, F_2)\}.$$

Then S is a finite set, and

$$C(\mathbb{Q}) = \bigsqcup_{d \in S} \left(\pi_d^{(1)}(D_d^{(1)}(\mathbb{Q})) \cup \pi_d^{(2)}(D_d^{(2)}(\mathbb{Q}))\right)$$

Moreover, if for all $d \in S$ the union $D_d^{(1)}(\mathbb{F}_p) \cup D_d^{(2)}(\mathbb{F}_p) = \emptyset$ for some prime p or $D_d^{(1)}(\mathbb{R}) \cup D_d^{(2)}(\mathbb{R}) = \emptyset$ then $C(\mathbb{Q}) = \emptyset$.

Proof. By Lemma 4.2 we know that $\operatorname{Res}(F_1, F_2) \in \mathbb{Z} \setminus \{0\}$, thus there are finitely many primes that divide $\operatorname{Res}(F_1, F_2)$, allowing us to conclude that S is finite.

Observe that for all cubefree $d \notin S$ there exists at least one prime p that divides d but does not divide $\operatorname{Res}(F_1, F_2)$; hence, by Lemma 4.2 we conclude that for any cubefree $d \notin S$ one has $D_d^{(1)}(\mathbb{Q}) \cup D_d^{(2)}(\mathbb{Q}) = \emptyset$. The above along with Proposition 4.1 allows us to conclude

$$C(\mathbb{Q}) = \bigsqcup_{d \in S} \left(\pi_d^{(1)}(D_d^{(1)}(\mathbb{Q})) \cup \pi_d^{(2)}(D_d^{(2)}(\mathbb{Q}))\right).$$

Now assume that for all $d \in S$ one has that $D_d^{(1)}(\mathbb{F}_p) \cup D_d^{(2)}(\mathbb{F}_p) = \emptyset$ for some prime number p or $D_d^{(1)}(\mathbb{R}) \cup D_d^{(2)}(\mathbb{R}) = \emptyset$. Then it follows that for all $d \in S$ we get $D_d^{(1)}(\mathbb{Q}) \cup D_d^{(2)}(\mathbb{Q}) = \emptyset$. Since $C(\mathbb{Q})$ is equal to a union of empty sets we conclude that $C(\mathbb{Q})$ must be empty itself.

□

As the reader can see all of the above allows us to generalise the two-cover descent to certain curves of the form $C : y^3 = f(x)$. The main difference between the two methods relies on the restrictions on the degree of f, and on the fact that we need to operate on two curves $D_d^{(1)}$ and $D_d^{(2)}$ instead of one. However most of the results along with their proofs are similar to their two-cover equivalents.

4.4 Three polynomial factorization descent method

Another possible approach to imitate the two-cover descent on curves of the form $C : Y^3 = F(X, Z)$, could consist of factoring the polynomial F into three other polynomials. This section does not provide a discussion with as much depth as for the three- and two-cover descents, it is rather meant as an outline of a new method, and discusses what differences need to be taken into account.

4.4.1 9-cover descent

Let $C : y^3 = f(x)$ be a curve, where $\deg(f) \not\equiv 1 \mod 3$, and $\deg(f) \geq 5$, with $f \in \mathbb{Z}[X]$ squarefree, and let f_1, f_2, f_3 be polynomials in $\mathbb{Z}[X]$ such that $f_1(x)f_2(x)f_3(x) = f(x)$, and the degree of at most one of them is not divisible by three.

Assume that there exists a $P = (\xi, \eta) \in C(\mathbb{Q})$. Then there must exist a unique cubefree integer d, and rational numbers η_1, η_2, and η_3 such that

$$f(\xi) = f_1(\xi)f_2(\xi)f_3(\xi) = d\eta_1^3 d\eta_2^3 d\eta_3^3 = (d\eta_1\eta_2\eta_3)^3 = \eta^3$$

Similarly to the previous methods we define a curve D_d as follows:

$$D_d := \begin{cases} dY_1^3 &= F_1(X, Z) \\ dY_2^3 &= F_2(X, Z) \\ dY_3^3 &= F_3(X, Z) \end{cases}$$

where F_1, F_2 and F_3 are homogeneous, coprime and squarefree, and satisfy $F_i(x, 1) = f_i(x)$
for $i = 1, 2, 3$.
Note that D_d is still a curve despite being defined by three equations, since its dimension is equal to one.

We also get a rational map π_d defined as follows:

$$\begin{gathered} \pi_d : D_d \to C \\ (X : Y_1 : Y_2 : Y_3 : Z) \mapsto (X : dY_1Y_2Y_3 : Z) \end{gathered}$$

where π_d turns out to have 9 preimages for any elements of C, thus π_d is an unramified 9-cover. Namely, the following points on D_d are mapped to the same point on C:

$$\begin{array}{ccc} (X : Y_1 : Y_2 : Y_3 : Z) & (X : \mu Y_1 : \mu Y_2 : \mu Y_3 : Z) & (X : \mu^2 Y_1 : \mu^2 Y_2 : \mu^2 Y_3 : Z) \\ (X : \mu Y_1 : \mu^2 Y_2 : Y_3 : Z) & (X : \mu Y_1 : Y_2 : \mu^2 Y_3 : Z) & (X : \mu^2 Y_1 : \mu Y_2 : Y_3 : Z) \\ (X : \mu^2 Y_1 : Y_2 : \mu Y_3 : Z) & (X : Y_1 : \mu Y_2 : \mu^2 Y_3 : Z) & (X : Y_1 : \mu^2 Y_2 : \mu Y_3 : Z) \end{array}$$

where μ is a primitive third root of unity, and all of the above points are distinct.

The main difference when generalizing the descent method to a triple factorization of the polynomial F arises when looking for fields $\mathbb{F}_p$ over which all three polynomials share a common factor. Namely, the definition of the resultant as discussed previously in this thesis in no longer sufficient, as it is foreseeable that F_1, F_2, and F_3 have a zero pairwise resultant, but do not share a common factor between the three of them, for instance consider:

$$\begin{aligned} F_1(X, Z) &= G_1(X, Z)G_2(X, Z) \\ F_2(X, Z) &= G_2(X, Z)G_3(X, Z) \\ F_3(X, Z) &= G_1(X, Z)G_3(X, Z) \end{aligned}$$

Therefore in order to apply a descent using a triple factorization one needs to find a new way to assess whether the polynomials F_1, F_2 and F_3 have a common factor in $\mathbb{F}_p$. A potential way to approach this problem could consist of using the gcd i.e. instead of checking what primes divide the resultants of the polynomials themselves, one should instead consider what primes divide the following gcd:

$$\gcd(\ \mathrm{Res}(F_1, F_2),\ \mathrm{Res}(F_1, F_3),\ \mathrm{Res}(F_2, F_3))$$

Nevertheless the above does not exclude cases where F_1, F_2, and F_3 share common factors only pairwise mod p, and no common factor that would divide all three of them mod p exists. Still the above criterion could be used to obtain a finite set S of cubefree integers d such that

$$C(\mathbb{Q}) = \bigcup_{d \in S} \pi_d(D_d(\mathbb{Q}))$$

However it is conceivable that a more efficient way to define the finite set S exists; namely one could define a resultant for three polynomials, which would allow to prove a theorem where the cases in which F_1, F_2, and F_3 have only pairwise common factors are not considered in the union of $\pi_d(D_d(\mathbb{Q}))$.
Unfortunately due to time restrains while writing my thesis I could not develop a notion of three polynomial resultant, nor rigorously check if the above holds, however if it turns out to be true then generalizing the descent method to the three polynomial factorization case should be feasible.

Nevertheless, it is worth pointing out that one may not need the three polynomial factorization method, for the problem phrased as in this thesis. Any set $C(\mathbb{Q})$ that can be solved using the three factorization method should also be possible to be solved with the method presented in Section 4.3; namely the conditions of the affine equation are the same on both methods, and if F can be factorized into three polynomials of which at most one polynomial has a degree non-divisible by three, then F can also be factorized into two polynomials where at least one has a degree divisible by three. Thus, any curve that satisfies the conditions for a descent with three polynomial factorization, also satisfies all of the conditions for the three-cover descent with two polynomial factorization.

5 Further Generalisations

5.1 p-adic numbers

This subsection is not indented as a complete account of p-adic numbers, but rather a brief explanation so that a bachelor mathematics student can have a sufficient understanding, to read the rest of this thesis. Most of the presented results can be found with more detailed explanations in [3].

5.1.1 p-adic absolute value

Definition 5.1 (p-adic absolute value)**.** *The p-adic absolute value on* $\mathbb{Q}$ *is defined by*

$$|\xi|_p := \begin{cases} 0 & \textit{if } \xi = 0 \\ p^{-n} & \textit{if } \xi = p^n \frac{a}{b} \textit{ with } p \nmid ab \textit{ and } ab \neq 0 \end{cases}$$

The above is indeed an absolute value since:

1. $|\xi|_p \Leftrightarrow \xi = 0$
By definition of $|\cdot|_p$ one has $|0|_p = 0$. For any $\xi \neq 0$ we get that $|\xi|_p = p^{-n}$ for some $n \in \mathbb{Z}$, and since $p \neq 0$ we conclude $|\xi|_p \neq 0$.

2. $|\xi\zeta|_p = |\xi|_p \cdot |\zeta|_p$
Take any $\xi, \zeta \in \mathbb{Q}$ and rewrite them as $\xi = p^n \frac{a}{b}$, and $\zeta = p^m \frac{c}{d}$, where $a, b, c, d, n, m \in \mathbb{Z}$, and $p \nmid abcd$. It follows that

$$|\xi\zeta|_p = p^{-n-m} = p^{-n} \cdot p^{-m} = |\xi|_p \cdot |\zeta|_p$$

3. $|\xi + \zeta|_p \leq \max\{|\xi|_p, |\zeta|_p\}$
Take any $\xi, \zeta \in \mathbb{Q}$ and rewrite them as $\xi = p^n \frac{a}{b}$, and $\zeta = p^m \frac{c}{d}$, where $a, b, c, d, n, m \in \mathbb{Z}$, and $p \nmid abcd$. With out loss of generality assume that $n \geq m$.
Then one can see that

$$\xi + \zeta = p^n \frac{a}{b} + p^m \frac{c}{d} = p^m \left(p^{n-m} \frac{a}{b} + \frac{c}{d} \right)$$

Let $k := p^{n-m} \frac{a}{b} + \frac{c}{d}$, and notice that $p \nmid k$. It follows that

$$|\xi + \zeta|_p = |p^m k|_p = p^{-m} = |\zeta|_p \leq \max\{|\xi|_p, |\zeta|_p\}$$

proving 3.

Remark. We show that $|\xi + \zeta|_p \leq \max\{|\xi|_p, |\zeta|_p\}$ instead of $|\xi + \zeta|_p \leq |\xi|_p + |\zeta|_p$, since the p-adic absolute value is a non-archimedean absolute value, that is an absolute value that satisfies property 3, unlike the standard (archimedean) notion of absolute value.

This way we have shown that $|\cdot|_p$ is indeed a (non-archimedean) absolute value.

5.1.2 $\mathbb{Q}_p$ and $\mathbb{Z}_p$

Theorem 5.1. *(Completion) Let k be a field and $|\cdot|$ an absolute value on k. The completion of k with respect to $|\cdot|$ is a metric space obtained by taking all all possible limits of Cauchy sequences defined over k (Note that the sequences are Cauchy with respect to the above defined absolute value $|\cdot|$).*
The completion of k with respect to $|\cdot|$ is a field that is also a complete metric space (with $d(a, b) = |a - b|$), that contains k as a dense subset [8, Page 12].

Remark. The rational numbers $\mathbb{R}$ are the completion of $\mathbb{Q}$ with respect to the standard absolute value $|\cdot|$. Namely, all $r \in \mathbb{R}$ are limits of Cauchy sequences in $\mathbb{Q}$.

Given the p-adic absolute value we can now define the field of p-adic numbers $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. Still, the p-adic numbers can also be understood as a series

$$\sum_{i=v}^{\infty} a_i p^i$$

where v is a (possibly negative) integer, and $0 \leq a_i < p$ for all i.

With the p-adic numbers one can further define the p-adic ring of integers by

$$\mathbb{Z}_p := \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$$

which intuitively can be phrased as all p-adic numbers that are not divisible by negative powers of p (hence the name of p-adic integers). Similarly to elements of $\mathbb{Q}_p$, the p-adic integers can be represented as a series

$$\sum_{i=0}^{\infty} a_i p^i$$

with $0 \leq a_i < p$ for all i. Notice however that the powers of p in the series cannot be negative due to the condition $|a|_p \leq 1$, otherwise one could get series converging to a p-adic number n_p such that $|n_p|_p > 1$. For example consider a series with $a_i = 0$ for all i's other then -2, and $a_{-2} = 1$, resulting in $|p^{-2}|_p = p^{-(-2)} = p^2$, which is not in $\mathbb{Z}_p$.

Lemma 5.2. *Let p be a prime, and $\mathbb{Z}_p$ the ring of p-adic integers. Then the following holds [3, Corollary 4.2.5]:*

$$\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

Finally, another property of the p-adic numbers that is used further in this thesis is presented below:

Theorem 5.3. *Let p be a prime, and consider any $a \in \mathbb{Q}_p \setminus \{0\}$. There there exist a unique p-adic unit $u \in \mathbb{Z}_p^\times$, and a unique integer n such that* [3, Chapter 4.3]

$$a = p^n u$$

The proofs of the theorems and lemmas above is omitted in this thesis, however the interested reader is invited to find them in [3].

5.2 Everywhere Locally soluble

Before introducing the notion of a curve being everywhere locally soluble we motivate it by Ostrowski's theorem.

Theorem 5.4 (Ostrowski's Theorem)**.** *All non-trivial absolute values that can be defined on $\mathbb{Q}$ are equivalent to either the p-adic absolute value $|\cdot|_p$ for some prime p, or to the usual absolute value $|\cdot|$. That is any non-trivial absolute value defines a topology on $\mathbb{Q}$ that is equal to a topology on $\mathbb{Q}$ defined by either the standard absolute value or a p-adic absolute value for some prime p* [3, Theorem 3.1.4].

Hence, one of the implications of Ostrowski's Theorem is that all completions of $\mathbb{Q}$ are given by $\mathbb{R}$, and $\mathbb{Q}_p$ for all primes p.

Definition 5.2 (ELS)**.** *A curve C is everywhere locally soluble (ELS) if $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p, and $C(\mathbb{R}) \neq \emptyset$.*

Put differently one could say that a curve define over $\mathbb{Q}$ is ELS when it has k-rational points over all completions k of $\mathbb{Q}$.

Notice that for any curves being ELS is a necessary condition for $C(\mathbb{Q}) \neq \emptyset$ [9, Section 3]. Namely as shown in the section in p-adic fields $\mathbb{Q} \subseteq \mathbb{Q}_p$, and thus $C(\mathbb{Q}_p) = \emptyset \Rightarrow C(\mathbb{Q}) = \emptyset$, similarly $C(\mathbb{R}) = \emptyset \Rightarrow C(\mathbb{Q}) = \emptyset$. However it is important to point out that being ELS is not a sufficient condition for $C(\mathbb{Q}) \neq \emptyset$. The rest of this thesis shows a method that can potentially prove whether a ELS hyperelliptic curve has no rational points.

5.3 Two-cover descent with p-adics

Recall the curves C and D_d along with the map $\pi_d : D_d \to C$ from Section 3.1. By Proposition 3.2 we know that

$$C(\mathbb{Q}) = \bigsqcup_{\text{sqaurefree } d} \pi_d(D_d(\mathbb{Q}))$$

The next step consists of defining a stronger criterion of $D_d(\mathbb{Q})$ to be empty, using the p-adic numbers, which can be done as follows:

Theorem 5.5. *Given a curve $D_d : Y_1^2 = F_1(X, Z); Y_2^2 = F_2(X, Z)$, and a prime p one has:*

$$p|d, \text{ and } D_d(\mathbb{Q}_p) \neq \emptyset \Rightarrow p| \operatorname{Res}(F_1, F_2)$$

Proof. Let p be a prime such that $p|d$, and assume that there exists a point $(\xi : \eta_1 : \eta_2 : \zeta) \in D_d(\mathbb{Q}_p)$, and consider its image on the projective line $\mathbb{P}^1 := \mathbb{P}_{(1,1)}$ (the projective line is defined as the weighted projective plane with two coordinates and weights $(1, 1)$). The image is obtained by the morphism:

$$\begin{aligned} \varphi : D_d &\to \mathbb{P}^1 \\ (\xi : \eta_1 : \eta_2 : \zeta) &\mapsto (\xi : \zeta) \end{aligned}$$

Knowing that any p-adic number can be written out as $p^n u$ where $n \in \mathbb{Z}$, and u is a unique p-adic unit (as explained in Theorem 5.3), one can observe that ξ and ζ are coprime p-adic integers, where coprime in this context means *not both divisible by p*. Namely, we get that $(\xi : \zeta) = (p^n u : p^m w)$, for $n, m \in \mathbb{Z}$, and u, w distinct p-adic units. Without loss of generality we assume that $n \leq m$. One can see that:

$$\begin{aligned} (\xi : \zeta) &= (p^n u : p^m w) \\ &= (p^{-n} p^n u : p^{-n} p^m w) \\ &= (u : p^{m-n} w) \end{aligned}$$

Using our assumption:

$$|u|_p = p^0 \leq 1, \text{ and } |p^{m-n} w|_p = p^{-(m-n)} = p^{-m+n} \leq 1$$

implying u and $p^{m-n}w$ are in $\mathbb{Z}_p$. This way we have shown that the image of a $\mathbb{Q}_p$ rational point on D_d can be represented by a point on $\mathbb{P}^1$ with coprime p-adic integers coordinates. It follows that η_1 and η_2 are also p-adic integers, because they are the result of addition and multiplication of other p-adics ($F_1, F_2 \in \mathbb{Z}[X]$, and all integers are also p-adic integers). Since $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$, as discussed in 5.2 we get that $D_d(\mathbb{F}_p) \neq \emptyset$. Therefore by Theorem 3.4 we conclude that $p|\operatorname{Res}(F_1, F_2)$.

□

Finally we can generalise Theorem 3.5 as follows:

Theorem 5.6. *Let $C : y^2 = f_1(x)f_2(x)$ be a hyperelliptic curve such that $f_1, f_2 \in \mathbb{Z}[X]$, and the degree of f_1 or f_2 is even. Let d be a squarefree integer, and $D_d : dY_1^2 = F_1(X, Z), dY_2^2 = F_2(X, Z)$ be a curve, defined the same way as in the earlier sections. Consider the set*

$$S := \{d \in \mathbb{Z} \ : \ d \text{ squarefree and } \forall \text{ primes } p \text{ one has } p|d \Rightarrow p| \operatorname{Res}(F_1, F_2)\}$$

Then S is finite and

$$C(\mathbb{Q}) = \bigsqcup_{d \in S} \pi_d(D_d(\mathbb{Q})).$$

Moreover:

$$\forall\, d \in S \ : \ D_d \text{ is not ELS then } C(\mathbb{Q}) = \emptyset$$

Proof. By Theorem 3.5 we know that S is finite and

$$C(\mathbb{Q}) = \bigsqcup_{d \in S} \pi_d(D_d(\mathbb{Q})).$$

Assume that for all $d \in S$ the curves D_d are not ELS. Then one can see that $D_d(\mathbb{Q}) = \emptyset$, as being ELS is a necessary condition for having rational points. Since in that case $C(\mathbb{Q})$ is equal to the union of mappings from empty sets, we conclude that $C(\mathbb{Q})$ is indeed empty. □

This way we have generalised the two-cover descent to the p-adic numbers, which will allow us to prove in some cases that D_d has no rational points, even though it may have $\mathbb{F}_p$ points for all primes p. The following sections discuss methods that will allow us to verify whether D_d is not ELS, and present a finite list of primes which need to be checked before reaching this conclusion.

5.4 Good and Bad Reduction of C

The idea behind good reduction of a curve C consists of verifying over which field (in the descent context over which $\mathbb{F}_p$) C exhibits non-smooth behaviours. The above happens when the polynomial $y^2 - f(x)$ has a vanishing derivative mod p i.e.:

$$\frac{d}{dy} y^2 \equiv 0 \mod p \equiv \frac{d}{dx} f(x)$$

Notice that the above happens if $\overline{f}$ (i.e. the polynomial obtained by reducing the coefficients of f mod p) has a multiple root, because $f'(x') \equiv 0 \mod p$ and $2y' \equiv 0 \mod p \Rightarrow y' \equiv 0 \mod p$ or $2 \equiv 0 \mod p$. The first observation that can be drawn is that in $\mathbb{F}_2$ deciding whether a curve is singular only depends on the derivative with respect to x, since $\frac{d}{dy} y^2 = 2y \equiv 0 \mod 2$. Therefore C has bad reduction in $\mathbb{F}_2$ if $\frac{d}{dx} f(x) \equiv 0 \mod 2$ for some x.

A more general and rigorous definition of good and bad reduction can be given as follows:

Definition 5.3. *Let p be an odd prime. Given a hyperelliptic curve $C\colon Y^2 = F(X,Z)$ defined over $\mathbb{Q}_p$ such that $F \in \mathbb{Z}_p[X,Z]$, let $\overline{F}$ be the polynomial obtained by reducing the coefficients of F mod p. The curve C has good reduction if the curve $\overline{C} : Y^2 = \overline{F}(X,Z)$ is smooth.*
If $C\colon Y^2 = F(X,Z)$ is defined over $\mathbb{Q}$, with $F \in \mathbb{Z}[X,Z]$, we then say that C has good reduction at p if C has good reduction as a curve over $\mathbb{Q}_p$. If C does not have good reduction (at p) then we say that C has bad reduction (at p) [8, Definition 3.10].

In order to access if C has good reduction at p we prove the following proposition:

Proposition 5.7. *Let $C : Y^2 = F(X,Z)$ be a hyperelliptic curve, and p be an odd prime. Let $f(x) := F(x,1)$, and $h(z) := F(1,z)$. Then C has good reduction at p if and only if $p \nmid disc(f)$ and $p \nmid disc(h)$* [8, page 14].

Proof. Assume that p divides $\mathrm{disc}(f)$ or $\mathrm{disc}(h)$. Then by Lemma 2.3 we can conclude that f or h have a multiple root mod p, thus F is not squarefree over $\mathbb{F}_p$.

If p does not divide $\mathrm{disc}(f)$ or $\mathrm{disc}(h)$, then by Lemma 2.3 f and h do not have any multiple root mod p, therefore C has good reduction at p, as $\overline{F}$ does not have multiple roots over $\mathbb{F}_p$. □

Since a hyperelliptic curve is defined in such a way that $\mathrm{disc}(f)$, $\mathrm{disc}(h) \in \mathbb{Z} \setminus \{0\}$, we conclude that any hyperelliptic curve C has always finitely many primes of bad reduction.

5.5 Bad reduction on D_d

Let D_d be the curve defined as in the two-cover descent. We defined D_d to have good or bad reduction as follows:

Definition 5.4. *Let p be a prime, and consider the curve $D_d(X)\colon dY_1^2 = F_1(X,Z), dY_2^2 = F_2(X,Z)$ defined over $\mathbb{Q}_p$, with $F_1, F_2 \in \mathbb{Z}_p[X,Z]$. Let $\overline{F}_1$ and $\overline{F}_2$ be the polynomials obtained by respectively reducing the coefficients of F_1 and F_2 mod p. Then the curve D_d has good reduction at p if the curve $\overline{D}_d\colon dY_1^2 = \overline{F}_1(X,Z), dY_2^2 = \overline{F}_2(X,Z)$ is smooth.*
Given a curve $D_d(X)\colon dY_1^2 = F_1(X,Z), dY_2^2 = F_2(X,Z)$ defined over $\mathbb{Q}$, we say that D_d has good reduction at p if D_d has good reduction over $\mathbb{Q}_p$. If D_d does not have good reduction (at p), we say that D_d has bad reduction (at p).

The above implies that using the definition of smoothness (Definition 2.6), one can verifying whether the curve has bad reduction is done by computing the rank of the matrices:

$$\begin{pmatrix} f_1'(x) & 2dy_1 & 0 \\ f_2'(x) & 0 & 2dy_2 \end{pmatrix} \mod p, \text{ and } \begin{pmatrix} h_1'(z) & 2dw_1 & 0 \\ h_2'(z) & 0 & 2dw_2 \end{pmatrix} \mod p \tag{5}$$

where $D_d : F_1(X,Z) = dY_1^2, F_2(X,Z) = dY_2^2$, $f_i(x) := F_i(x,1)$, and $h_i(z) := F_i(1,z)$ for $i = 1,2$.

Since D_d has 3 variables (in its weighted projective version) and dimension equal to 1 (see Section 3.1.1), the Jacobians (5) need to have rank $3-1=2$, as explained in the definition of smooth weighted projective varieties 2.10. With the above in mind we state the following theorem:

Theorem 5.8. *Let $C : Y^2 = F(X,Z)$ be a hyperelliptic curve, $D_d : F_1(X,Z) = dY_1^2, F_2(X,Z) = dY_2^2$ be a curve as defined in the two-cover descent, and let p be an odd prime. Then, D_d has bad reduction at p if and only if:*

- *C has bad reduction at p or*
- *$p|d$*

Proof. Assume that C has bad reduction at p, then by Proposition 5.7 we know that p divides disc(f) or disc(h). We assume that p divides disc(f). Because $\overline{f}_1(x)\overline{f}_2(x) = \overline{f}(x)$ it follows that one of the polynomials has a multiple root, or $\overline{f}_1$ and $\overline{f}_2$ share a root.
Case 1: Let $P = (x:0:0:1) \in D_d(\overline{\mathbb{F}}_p)$.
Then the Jacobian (5) evaluated at P gives us:

$$\begin{pmatrix} \overline{f}_1'(x) & 2d\cdot 0 & 0 \\ \overline{f}_2'(x) & 0 & 2d\cdot 0 \end{pmatrix} = \begin{pmatrix} \overline{f}_1'(x) & 0 & 0 \\ \overline{f}_2'(x) & 0 & 0 \end{pmatrix},$$

implying that the Jacobian has rank at most 1, and thus D_d has bad reduction.

Case 2: One of $\overline{f}_1$ and $\overline{f}_2$ has a multiple root.
With out loss of generality assume that $\overline{f}_1$ has a multiple root at x, and let $P = (x:0:y_2:1) \in D_d(\overline{\mathbb{F}}_p)$. Then the Jacobian matrix (5) evauated at P gives us:

$$\begin{pmatrix} \overline{f}_1'(x) & 2d\cdot 0 & 0 \\ \overline{f}_2'(x) & 0 & 2dy_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ \overline{f}_2'(x) & 0 & 2dy_2 \end{pmatrix}$$

Implying that the Jacobian has rank at most 1, and thus D_d has bad reduction.

A similar reasoning can be used when $p|$ disc(h), allowing us to state that whenever C has bad reduction at p, the curve D_d must also have bad reduction at p.

Assume that $p|d$. Then the Jacobian (5) mod p gives us for any point in $D_d(\overline{\mathbb{F}}_p)$:

$$\begin{pmatrix} \overline{f}_1'(x) & 2\cdot 0y_1 & 0 \\ \overline{f}_2'(x) & 0 & 2\cdot 0y_2 \end{pmatrix} = \begin{pmatrix} \overline{f}_1'(x) & 0 & 0 \\ \overline{f}_2'(x) & 0 & 0 \end{pmatrix}$$

Implying again that the Jacobian has rank at most 1, and thus D_d has bad reduction.

Hence so far we have shown that if C has bad reduction at p, or $p|d$ then D_d also has bad reduction at p.

Assume that C has good reduction at p, and $p \nmid d$.
It follows that there is no $(x:y_1:y_2:z) \in D_d(\overline{\mathbb{F}}_p)$ such that both y_1 and y_2 would be equal to

zero mod p, as $p \nmid \text{disc}(f)$, i.e. $\overline{f}$ has no multiple roots. Moreover we know that $2d \not\equiv 0 \mod p$. It follows that it is always the case that either the second or third column is non-zero in the Jacobians (5). Without loss of generality assume that $y_1 = 0 \mod p$. In such a case the Jacobian matrix of the first standard affine patch has a rank less than two only if $\overline{f}'(x) \equiv 0 \mod p$, however because $p \nmid \text{disc}(f)$ it is not possible for $\overline{f}_1$ to have a doubled root. This way we conclude that $f_1'(x) \not\equiv 0 \mod p$. A similar proof can be made using $h(z)$, to show that there are no multiple roots mod p on the second affine patch. This way we have shown that whenever C had good reduction at p, and $p \nmid d$, then the curve D_d has good reduction at p. □

Remark. In the case $p = 2$ any curve D_d has bad reduction, since $2dy_i \equiv 0 \mod p$ making the Jacobian have a rank of one or less.

5.6 Bounds on primes p

So for we have discussed what conditions need to be met to conclude the $D_d(\mathbb{Q}_p)$ is empty, however we did not discuss what primes p need to be checked. Thus, the question that naturally arises is: Is there a bound on the primes one needs check, to decide whether a given curve is ELS? An answer to the above is given by a theorem proved by Helmut Hasse for curves of genus 1, and generalized to curves of any genus by André Weil.

Theorem 5.9 (Hasse-Weil Theorem). *Let C be a smooth absolutely irreducible curve of genus g over a finite field F with q elements. Then* [8, Theorem 3.12]:

$$|\#C(F) - (q+1)| \leq 2g\sqrt{q}$$

The above theorem gives us a finite list of primes p for which it is possible to check if $D_d(\mathbb{F}_p) = \emptyset$. The following corollary generalizes it to p-adic numbers.

Corollary 5.9.1. *Let C be a curve of genus g, and let p be a prime of good reduction for C. Then if $p > 4g^2 - 2$, one has $C(\mathbb{Q}_p) \neq \emptyset$* [8, Corollary 3.13].

In other words in order to verify if a curve of genus g is ELS, one only needs to check whether the curve has $\mathbb{Q}_p$-points for primes $p < 4g^2 - 2$, and primes of bad reduction.

Thus, in order to know how many p-adic fields we need to look at before knowing if a given curve D_d is ELS, we need to know the genus of the curve, which can be obtained from the Riemann-Hurwitz formula 3.1. Since there exists a unramified two-cover π_d between C, and D_d, along with the previous sections allows one to check in finitely many steps if a curve D_d has rational points. Namely, one needs to check if the curves D_d have $\mathbb{R}$ points and have $\mathbb{Q}_p$ points for a finite number of primes (that is all primes less then $4g - 2$ and all primes of bad reduction), to know if D_d is ELS.

5.7 Checking whether D_d is ELS

We have shown that if a certain finite set of curves D_d are not ELS, then C has no rational points. This section focuses on possible approaches to show that D_d is not ELS, when we know that D_d has $\mathbb{F}_p$ points for all primes in the bounds discussed in section 5.6.

One possible approach to verify whether D_d is ELS could consist of finding an isomorphism between D_d and some hyperelliptic curve C'. Since it is always possible to verify whether $C'(\mathbb{Q}_p)$ is empty or not for any hyperelliptic curve [8, Lemma 3.15], thus given a isomorphism $\varphi : D_d \to C'$ it could be possible to find a suitable prime p for which $C'(\mathbb{Q}_p) = \emptyset$ (if such exists), allowing us to conclude that D_d is not ELS. Nevertheless such an isomorphism might not exist for some curves D_d, allowing us to apply the above approach in only in certain cases.

The reason for which C' might have $\mathbb{F}_p$ points but no $\mathbb{Q}_p$-points is partially due to Hensel's Lemma, and bad reduction. Namely, one can see below that Hensel's Lemma requires $\overline{C}'$ to have a smooth $\mathbb{F}_p$ point to be able to lift it to $C'(\mathbb{Q}_p)$. Hensel's Lemma along with a proof is presented below to indicate the key role of good reduction.

Theorem 5.10 (Hensel's Lemma). *Let f be a polynomial in $\mathbb{Z}_p[X]$, and let a be a simple root of $\overline{f} \in \mathbb{F}_p[X]$ (i.e. $\overline{f}(a) \equiv 0 \mod p$ and $\overline{f}'(a) \not\equiv 0 \mod p$), where $\overline{f}$ is obtained by reducing coefficients of f mod p. Then f has a unique root $\alpha \in \mathbb{Z}_p$ such that $\overline{\alpha} = a$ in $\mathbb{F}_p$.*

Proof. We start by showing by induction that for all integer $n \geq 1$ there exists a sequence $(a_n)_{\geq 1}$ in $\mathbb{Z}_p$ such that

$$\begin{aligned} f(a_n) &\equiv 0 \mod p^n, \\ a_n &\equiv a \mod p. \end{aligned}$$

Base case: $a_1 = a$.
We get that $a_1 = a \equiv a \mod p$, and by the assumptions of Hensel's Lemma get that $f(a_1) = f(a) \equiv 0 \mod p$, thus the base case holds.

Induction Hypothesis: $f(a_n) \equiv 0 \mod p^n$ and $a_n \equiv a \mod p$.
The following element of the sequence can be defined as follows : $a_{n+1} := a_n + p^n t_n$, where $t_n \in \mathbb{Z}_p$. This way we get that

$$a_{n+1} = a_n + p^n t_n \equiv a_n \mod p^n \equiv a \mod p$$

To show the other part of the statement (i.e. $f(a_{n+1}) \equiv 0 \mod p^{n+1}$) we need to use the formula:

$$f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2, \text{ where } g \in \mathbb{Z}_p[X,Y]$$

The above expression can be obtained by using the binomial formula as follows

$$\begin{aligned} f(X+Y) &= \sum_{i=0}^{\deg f} c_i \left(X+Y\right)^i = c_0 \sum_{i=1}^{\deg f} c_i \left(X^i + iX^{i-1}Y + g(X,Y)Y^2\right) \\ &= \sum_{i=0}^{\deg f} c_i X^i + Y \sum_{i=1}^{\deg f} ic_i X^{i-1} + Y^2 \sum_{i=1}^{\deg f} c_i g(X,Y) \\ &= f(X) + f'(X)Y + g(X,Y)Y^2 \end{aligned}$$

Note that c_i are the coefficients of f, and $g \in \mathbb{Z}_p[X,Y]$.
Using the above formula on $a_n + p^n t_n$ we get

$$\begin{aligned} f(a_n + p^n t_n) &= f(a_n) + p^n t_n f'(a_n) + g(a_n, p^n t_n) p^{2n} t_{2n} \\ &\equiv f(a_n) + p^n t_n f'(a_n) \mod p^{n+1} \end{aligned}$$

since $2n \geq n+1$.
It follows that

$$f(a_{n+1}) = f(a_n + p^n t_n) \equiv 0 \mod p^{n+1} \Leftrightarrow f'(a_n) t_n \equiv \frac{-f(a_n)}{p^n} \mod p^{n+1}$$

Notice that the above indeed has a solution, since $\frac{-f(a_n)}{p^n} \in \mathbb{Z}_p$, because $f(a_n) \equiv 0 \mod p^n$, as assumed by the induction hypothesis. Moreover there must be a solution t_n in a congruence class mod p, because $f'(a_n) \not\equiv 0 \mod p$.
Given that there exists a t_n, which we can adjust for all n, and by defining $a_{n+1} := a_n + p^n t_n$ we have shown that there is a a_{n+1} such that $f(a_{n+1}) \equiv 0 \mod p^{n+1}$.

All of the above proves that there exists a sequence $(a_n)_{\geq 1}$ in $\mathbb{Z}_p$ for which

$$\begin{aligned} f(a_n) &\equiv 0 \mod p^n, \\ a_n &\equiv a \mod p. \end{aligned}$$

What remains to be shown is that $(a_n)_{\geq 1}$ converges to a limit $\alpha \in \mathbb{Z}_p$, and that $\alpha \equiv a \mod p$.

As shown during the induction, all elements of $(a_n)_{\geq 1}$ satisfy $a_{n+1} \equiv a_n \mod p^n$, hence one can deduce that $a_{n+1} = a_n + bp^n$, where $b \in \{0, 1, ..., p^{n-1}\}$, implying

$$|a_{n+1} - a_n|_p = |a_n + bp^n - a_n|_p = |bp^n|_p = p^{-n}$$

therefore for any $n \geq 1$ we get

$$|a_{n+1} - a_n|_p < p^{1-n}$$

showing that $(a_n)_{\geq 1}$ is Cauchy, hence convergent.
Moreover one could state that the limit is a point in $\mathbb{Z}_p$. Assume that α is the limit of $(a_n)_{\geq 1}$, and that $|\alpha|_p > 1$ i.e. $\alpha \notin \mathbb{Z}_p$. Since all a_n's are p-adic integers we conclude that $|a_n|_p \leq 1$ for all n. Thus

$$\epsilon := \frac{|\alpha|_p - 1}{2} < |\alpha|_p - |a_n|_p \text{ for all } n \in \mathbb{N}$$

contradicting the fact that α is the limit of the sequence $(a_n)_{\geq 1}$. Hence, we conclude that the seuqnce indeed converges to a point in $\mathbb{Z}_p$.

Observe that because $a_{n+1} \equiv a_n \mod p^n$, implying that for all $m > n$ we get $a_m \equiv a_n \mod p^n$, and by taking m to infinity we get $\alpha \equiv a_n \mod p^n$. When $n = 1$ $\alpha \equiv a \mod p$.
Also, the above implies that for any $n \geq 1$ one has

$$f(\alpha) \equiv f(a_n) \equiv 0 \mod p^n \Rightarrow |f(\alpha)|_p \leq p^{-n}$$

Because the above holds for all n, we conclude that $f(\alpha) = 0$.

So far we have shown that if $\overline{f}(a) = 0$, and $\overline{f}'(a) \neq 0$, then there exists an α in $\mathbb{Z}_p$ for which $\overline{\alpha} = a$ mod p, and $f(\alpha) = 0$. The last step of the proof shows that α is unique.
Let $\beta \in \mathbb{Z}_p$ such that $f(\beta) = 0$, and $\beta \equiv a \mod p$. Then

$$\beta \equiv a \mod p \equiv \alpha \mod p$$

Thus $\beta = \alpha + bp$ for some integer $0 \leq b < p$. Using $f(X + Y) = f(X) + f'(X)Y + g(X, Y)Y^2$, we get

$$f(\beta) = f(\alpha + bp) \equiv f(\alpha) + pbf'(\alpha) \mod p^2 \tag{6}$$

given that α and β are roots of f the equation (6) gives us

$$0 \equiv 0 + pbf'(\alpha) \mod p^2$$

Since $f'(\alpha) \not\equiv 0 \mod p$, and $p \not\equiv 0 \mod p^2$, it follows that the equation above can only hold when $b = 0$, implying

$$\beta = \alpha + 0 \cdot p = \alpha$$

proving uniqueness.

All of the above proves Hensel's Lemma. □

Given the proof above the reader can see why the good reduction is essential to apply Hensel's Lemma, namely we need non-vanishing derivatives, to guarantee a possible sequence of $(a_n)_{\geq 1}$ in $\mathbb{Z}_p$, as defined in the proof.

Summing up the procedure to verify of D_d outlined in this thesis is as follows

1. Compute the primes of bad reduction and the genus of D_d to obtain a list of primes p for which D_d may potentially not have $\mathbb{Q}_p$ points, using the bound discussed in section 5.6.
2. Verify if D_d has $\mathbb{F}_p$ points for all primes obtained in the previous step (which can be facilitated using the python code from Section 3.5).
3. If there is a prime p such that $D_d(\mathbb{F}_p)$ is empty conclude that D_d is not ELS.
4. If $D_d(\mathbb{F}_p)$ is non-empty for all primes p find an isomorphism between D_d and some hyperelliptic C', if such a map exists.
5. Verify if C' has no $\mathbb{Q}_p$ points for primes p of bad reduction. If no such prime can be found D_d is ELS.

6 Research Suggestions

A list of suggestions for further research on descent is given below:

- Presenting the 9-cover descent in greater detail, outlining all of the steps, along with a description of an efficient criterion to access if the polynomials F_1, F_2, and F_3 have a common factor mod p.
- Finding and working out examples of the descent on $C : Y^3 = F(X, Z)$.
- Development of the descent methods on $Y^3 = F(X, Z)$ with the same level of generality as Michael Stoll discusses the two-cover descent in [9].
- Generalizing descent methods to curves of the from $Y^n = F(X, Z)$ for $n > 3$.
- Expanding on the code in Section 3.5, so that it also computes points at infinity, and the list of finitely many primes for which $D_d(\mathbb{F}_p)$ can be empty.
- Writing code that can be used in the descent on curves $C : Y^3 = F(X, Z)$.

References

[1] John William Scott Cassels. *Lectures on Elliptic Curves.* Cambridge University Press, 1991.

[2] Steven Galbraith. Mathematics of public key cryptography, version 0.9. 2011. Accessed: 01/07/2024.

[3] Fernando Q Gouvêa. *p-adic Numbers.* Springer, 1997.

[4] Timothy Hosgood. An introduction to varieties in weighted projective space. *arXiv preprint arXiv:1604.02441*, 2016.

[5] Serge Lang. *Algebra.* Springer Science & Business Media, 2002.

[6] Samir Siksek. Chabauty and the mordell-weil sieve. *Advances on superelliptic curves and their applications*, 41:194–224, 2015.

[7] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[8] Michael Stoll. Arithmetic of hyperelliptic curves - lecture notes, 2014.

[9] Michael Stoll. Descent and covering collections. *Advances on Superelliptic Curves and their Applications*, 41:176–193, 2015.