THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

The density of rational points and invariants of genus one curves

MANH HUNG TRAN

CHALMERS

Division of Algebra and Geometry
Department of Mathematical Sciences
CHALMERS UNIVERSITY OF TECHNOLOGY
AND UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden, 2019

The density of rational points and invariants of genus one curves

MANH HUNG TRAN

ISBN 978-91-7905-204-1

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 4671
ISSN 0346-718X

Department of Mathematical Sciences
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg, Sweden
Phone: +46 (0)31 772 4997
Author e-mail: manhh@chalmers.se

Typeset with LaTeX
Department of Mathematical Sciences
Printed in Gothenburg, Sweden 2019

The density of rational points and invariants of genus one curves

Manh Hung Tran

Department of Mathematical Sciences
Chalmers University of Technology and University of Gothenburg

ABSTRACT

The present thesis contains three papers dealing with two arithmetic problems on curves of genus one, which are closely related to elliptic curves.

The first problem is to study the density of rational points presented in Papers I and II. We give uniform upper bounds for the number of rational points of bounded height on smooth curves of genus one given by ternary cubics or complete intersections of two quadratic surfaces. The main tools used in these two papers are descent on elliptic curves and determinant methods. While working with the rational points counting problem, one need to deal with the smoothness of geometric objects and the bad reduction of polynomials. To characterize these properties, there is a classical object called the discriminant which naturally appears.

The above discriminant gives an inspiration to the study of the next problem in the thesis concerning invariants of models of genus one curves presented in Paper III. Here an invariant of a genus one curve is a polynomial in the coefficients of the model defining the curve that is stable under certain linear transformations. The discriminant is a classical example of an invariant. Besides that, there are two more important invariants which generate the ring of invariants of genus one models over a field. Fisher considered these invariants over the field of rational numbers and normalized them such that they are moreover defined over the integers. We provide an alternative way to express these normalized invariants using a natural connection to modular forms. In the case of the discriminant of ternary cubics over the complex numbers, we also present another approach using determinantal representations. This latter approach produces a natural connection to theta functions.

The common idea in the thesis is to link a smooth genus one curve to a Weierstrass form, which is a more well-understood object.

Keywords: Elliptic curve, genus one, rational point, height, descent, determinant method, discriminant, invariant, modular form, determinantal representation, theta function.

List of appended papers

The following papers are included in this thesis:

Paper I. Manh Hung Tran. *Counting rational points on smooth cubic curves*, Journal of Number Theory **189**, 2018, 138-146.

Paper II. Manh Hung Tran. *Uniform bounds for rational points on complete intersections of two quadric surfaces*, Acta Arithmetica **186**, No. 4, 2018, 301-318.

Paper III. Manh Hung Tran. *Invariants of models of genus one curves via and modular forms and determinantal representations*, Submitted, arXiv:1911.01350.

Acknowledgments

First of all, I would like to thank my supervisor Dennis Eriksson for his guidance during the last five years in every aspect of my studies: introducing research topics, suggesting ideas and materials, providing corrections and comments, explaining theories, supporting me in many ways. I really appreciate his patience when I was slow or made mistakes. Thank you, Dennis, for always being kind to me.

I am grateful to my co-supervisor Martin Raum for many of his useful discussions, feedback as well as his explanation to important theories and materials. I would like to thank Per Salberger for his crucial help in writing my first two articles.

I am very thankful to the Department of Mathematical Sciences for providing me a wonderful working environment. Especially, I would like to thank Håkan Samuelsson for his great support in many situations.

During my last five years, I have been talking to excellent members of the algebraic geometry and number theory research group. I wish to thank them, especially Julia Brandes and Anders Södergren, for their fruitful discussions.

I would like to thank all of my friends, doctoral students at the department for giving me such a special experience of an academic life. Among all of you, I wish to specially thank my closest friends, Medet and Valentina, for being together with me, encouraging me and sharing with me all the stressful and fun moments during the last five years. Thank both of you for making my time at the department more colourful and memorable.

Finally, I want to thank my beloved wife and my little son for their invaluable support and encouragement in any of my difficult periods. Thank you for coming into my life.

Contents

Chapter 1

Introduction

In this thesis, we study algebraic equations of the form

$$y^2 = x^3 + ax + b \tag{1.1}$$

and its various generalizations. Here a, b are elements in a field. The equation (1.1) is called a Weierstrass equation. The solution set of (1.1) defines a curve which is called an elliptic curve if it is smooth. This type of curve appears in many important problems in number theory. The most famous one among them is probably the Birch-Swinnerton-Dyer conjecture, which is one of the seven Millennium Prize Problems.

Elliptic curves are central objects in many other areas of mathematics such as algebraic geometry, complex analysis, representation theory, etc. Outside of mathematics, elliptic curves also have applications in physics, cryptography, banking security and computer science.

Geometric objects can be studied through algebraic equations. This is one of the fundamental ways to think of algebraic geometry. In this thesis, we study problems in number theory with tools coming from algebraic geometry. The solution set of a system of polynomial equations defines an object called an algebraic variety. We are interested in the case of algebraic curves, which are algebraic varieties of dimension one. Furthermore, we focus on genus one curves, which are defined by natural generalized equations of (1.1). The concept genus one will be discussed later in this chapter.

The present thesis discusses two arithmetic problems on curves of genus one. The first problem arises from Diophantine geometry in which we study the density of integral solutions of Diophantine equations, i.e., equations given by polynomials with integer coefficients. The second problem concerns invariants, which are stable algebraic forms under certain transformations.

1.1 Density of rational points on curves of genus one

The set of integral solutions of an equation might be empty, finite or infinite. To quantify the infinite case, it is interesting to estimate the number of solutions inside a large box and study the density of solutions when the box size goes to infinity. To measure the boxes, we introduce a height function which characterizes the size of integral solutions of algebraic equations, which can be understood as integral points on algebraic varieties. More concretely, the naive height function H is defined as

$$H(P) = \max\{|x_1|, |x_2|, ..., |x_n|\}$$

for an integral point $P = (x_1, x_2, ..., x_n) \in \mathbb{Z}^n$.

Let us start with a simple example of a planar line which is defined by the equation $x + y = z$. This line contains infinitely many integral points. It can be proven that in the box $I_B = \{P \in \mathbb{Z}^3 : H(P) \leq B\}$ for some $B > 0$, this line approximately contains $4B$ integral points. This should be compared with the number $\sharp I_B \approx (2B)^3$ of integral points in that box to get an intuition about the density of integral points on this line.

We are interested in equations defined by homogeneous polynomials. If x is an integral solution of a homogeneous polynomial F, then so is λx for any $\lambda \in \mathbb{Q}$. It is then natural to consider primitive integral solutions of $\{F = 0\}$ which correspond, up to sign, to rational points on the variety defined by F. We then study the density of rational points. Equations defined by homogeneous polynomials of degree 1 or 2 are well-understood. The first non-trivial case is a plane curve defined by a cubic form $F(x, y, z)$. It is hard to describe its set of rational points.

Heath-Brown [19] proved that inside the box $\{P \in \mathbb{Z}^3_{\text{primitive}} : H(P) \leq B\}$, the number of rational points on a plane curve defined by an irreducible cubic form $F(x, y, z)$ is bounded, up to some constant, by $B^{2/3}$. Furthermore, he constructed an example (see (3.7)) showing that the bound $B^{2/3}$ is essentially optimal for cubic curves having infinitely many rational points. Thus, the set of rational points on a line is more dense than a cubic curve.

If the cubic form F defines a smooth curve then this curve is of genus one, which is a natural generalization of the elliptic curve defined by (1.1). The name genus one comes from the fact that if we consider this type of curve over the complex numbers, then it looks like an one-hole torus as in Figure 1.1.

In Papers I and II, we study the density of rational points of bounded height on smooth curves of genus one given in two typical forms:

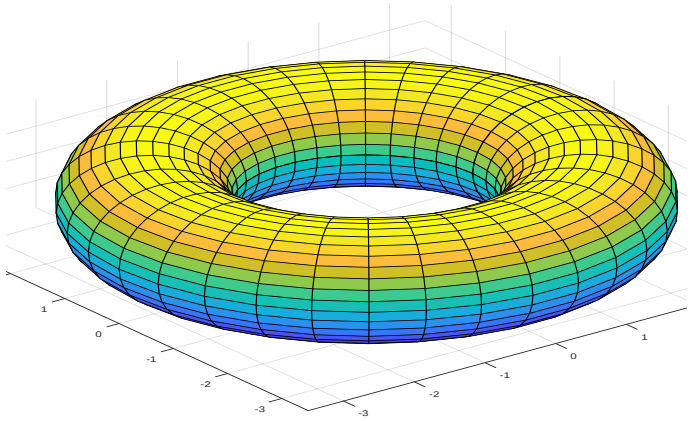

Figure 1.1: A curve of genus one over $\mathbb{C}$

- Ternary cubics:

$$ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2x + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz. \quad (1.2)$$

- Complete intersections of two quadratic surfaces:

$$\begin{cases} a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_0x_1 + a_5x_0x_2 + ... + a_9x_2x_3 = 0. \\ b_0x_0^2 + b_1x_1^2 + b_2x_2^2 + b_3x_3^2 + b_4x_0x_1 + b_5x_0x_2 + ... + b_9x_2x_3 = 0. \end{cases} \quad (1.3)$$

The main tools to study this problem are descent and the determinant method. The former tool is based on the fact that one can partition the group of rational points on a genus one curve into a finite number of subsets of points of smaller heights. The latter tool is a strong method for counting points on varieties of low dimensions, especially for curves.

1.2 Invariants of genus one curves

When considering working with heights of rational points on a genus one curve, there is a classical invariant which naturally appears and is called the discriminant. Its vanishing corresponds to the smoothness of the curve. For instance, the discriminant

of the curve defined by (1.1) is

$$\Delta = -16(4a^3 + 27b^2).$$

One can think about an invariant of an algebraic variety as a polynomial in the coefficients of the polynomials defining that variety, that remains unchanged under certain linear transformations of the coordinates. These transformations preserve the solutions of the polynomials. For example, the linear transformation which preserves the solutions of (1.1) is of the form (see [13, Section 3.1])

$$x = u^2x' + r,\ y = u^3y' + u^2sx' + t \text{ for any } u \neq 0. \tag{1.4}$$

The discriminant Δ of (1.1) and Δ' of the one obtained by the transformation (1.4) are related by $\Delta' = u^{12}\Delta$, where the extra power of u comes from the determinant of this transformation. This discriminant inspired the author to work on the second problem in this thesis which concerns invariants of models of genus one curves. These models are different ways of representing a curve of genus one.

Ternary cubics and intersections of two quadrics given in (1.2) and (1.3) are two typical models of genus one, which are models of degrees 3 and 4 respectively. The definition of the degree of a genus one model of degree n is presented in Section 2.3. In Paper III, we systematically study models of genus one of degrees $n \leq 5$ and their invariants. Besides the discriminant, there are also two important invariants which can be used to describe all the other invariants of models of genus one of degree $n \leq 5$ in characteristics not 2 or 3 as confirmed in Fisher [13, Theorem 4.4]. In that paper, he also gives a normalization of these invariants for models of degrees $n = 2, 3, 4$ such that they are primitive polynomials with integer coefficients.

By relating invariants to modular forms, we produce an alternative way to express these normalized invariants. Here a modular form is a function on the upper half plane $\mathbb{H} := \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$, which transforms in a certain way related to some type of Möbius transformation (see (4.3)). Classical examples of modular forms are theta functions, for instance, the function $\theta(\tau) = \theta(0, \tau)$. Here θ is the Jacobi theta function defined on $\mathbb{C} \times \mathbb{H}$ as

$$\theta(z, \tau) = \sum_{n=-\infty}^{\infty} \exp(\pi i n^2 + 2\pi i n z).$$

Over the complex numbers, we present another approach to study invariants of ternary cubics using determinantal representations. More concretely, one can represent a homogeneous polynomial of certain types as the determinant of a matrix whose elements

are linear forms. The study of the polynomial is then reduced to the study of the corresponding matrix. We will see in Section 4.4 that in the case of Weierstrass forms, determinantal representations naturally give us theta functions.

This approach is motivated by the classical expression of the discriminant of Weierstrass forms in terms of theta functions (see (1.6)). More precisely, let C be a smooth genus one curve defined by the Weierstrass equation

$$y^2 = 4x^3 - g_2x - g_3. \tag{1.5}$$

As explain in Section 2.2, there exists a natural Weierstrass parametrization which provides a lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with some complex numbers ω_1, ω_2 such that $\mathrm{Im}(\omega_2/\omega_1) > 0$ and $C(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Let $\tau := \omega_2/\omega_1$, the discriminant of the Weierstrass form corresponding to (1.5) satisfies the following identity

$$\Delta = 16\left(\frac{\pi}{\omega_1}\right)^{12}(\theta(0,\tau)\theta(\tau/2,\tau)\theta(1/2,\tau))^8. \tag{1.6}$$

One can ask if we also have this phenomena for general cubics or not. This provides a natural connection between algebraic (discriminants) and analytic (theta functions) objects.

We will see in both of these two arithmetic problems an important step is that we can link a smooth curve of genus one to a Weierstrass equation, which is a better understood object. Together with the group structure of elliptic curves as described in the next section, this is one of the most important properties of genus one curves.

1.3 Organization of the thesis

The structure of the thesis is as follows: we introduce the theory of elliptic curves and genus one models in Chapter 2. The first problem in the thesis concerning the density of rational points will be presented in Chapter 3. Then in Chapter 4, we discuss the second problem in the thesis about invariants as well as the theory of modular forms and determinantal representations. All three papers are then summarized in Chapter 5.

Chapter 2

Elliptic curves and genus one models

The theory of elliptic curves has been studied for centuries. It is a rich area where many different branches of mathematics come together. Elliptic curves also make an important role in the present thesis as mentioned in Chapter 1. In this chapter, we first provide the definition of elliptic curves as well as their crucial properties. Many of these properties are related to Weierstrass forms, which are the first examples of genus one models. We will also introduce other models of genus one curves systematically.

2.1 Geometry of elliptic curves

Definition. *An elliptic curve over a field K is a pair $(E, \mathcal{O})$ of a smooth projective curve E of genus one over K with a specified base point $\mathcal{O} \in K$.*

This curve can be given by a (long) Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

Here the base point $\mathcal{O}$, which is called the point at infinity, is understood as the extra point $[0 : 1 : 0]$ on the projective curve defined by the homogeneous form associated to (2.1). This equation can be written in one of the following (short) forms if $\mathrm{char}(K) \neq 2, 3$:

$$y^2 = x^3 + ax + b \tag{2.2}$$

or

$$y^2 = 4x^3 - g_2x - g_3. \tag{2.3}$$

When char$(K) \neq 2$, one can transform (2.2) to (2.3) and vice versa. The equation (2.3) is useful when for instance working over $K = \mathbb{C}$, since it is connected to the natural differential equation associated to Weierstrass $\mathcal{P}$-functions (see (2.4)).

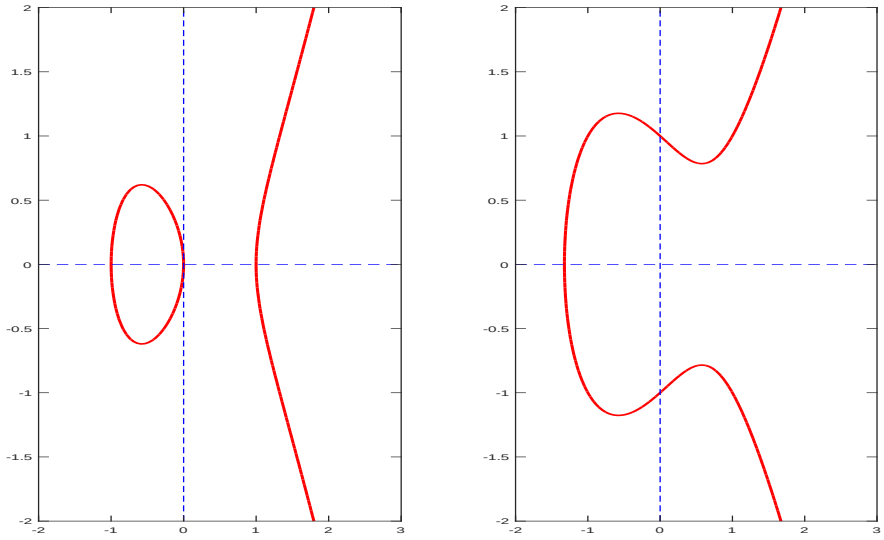

Figure 2.1: Two main shapes of elliptic curves over $\mathbb{R}$

Typically, elliptic curves look like Figure 2.1. The smooth condition in the definition of an elliptic curve means that the curve has no singular point. If we consider the curve given by (2.2) for instance, this condition is equivalent to the fact that the discriminant $\Delta = -16(4a^3 + 27b^2)$ is non-zero as mentioned in Chapter 1.

One of the important properties of elliptic curves concerns the group structure of the points. More precisely, let $(E, \mathcal{O})$ be an elliptic curve over a field K, then the set $E(K)$ of points over K on E forms an abelian group with neutral element $\mathcal{O}$. Let us geometrically describe the addition law of this group. For simplicity, we suppose that the elliptic curve E is given in the form (2.2). The following addition law is described as in Figure 2.2:

Let P, Q be two points on the elliptic curve E and $l = \overline{PQ}$ be the line joining them. For simplicity we suppose that $P \neq Q$. If l is not a vertical line, then l intersects E at a third point R. Since E is symmetric about the x-axis, the point obtained by reflecting R about the x-axis also lies on E and it is defined to be the point $P + Q$. If l is a vertical line, it intersects E at infinity. Therefore, in this case we can define $P + Q = \mathcal{O}$. If at least one of two points P or Q is the point at infinity, say $Q = \mathcal{O}$, then the line passing P and Q is a vertical line. This line meets E at the point whose

reflection about the x-axis is again P. Hence, we can define $P + \mathcal{O} = P$.

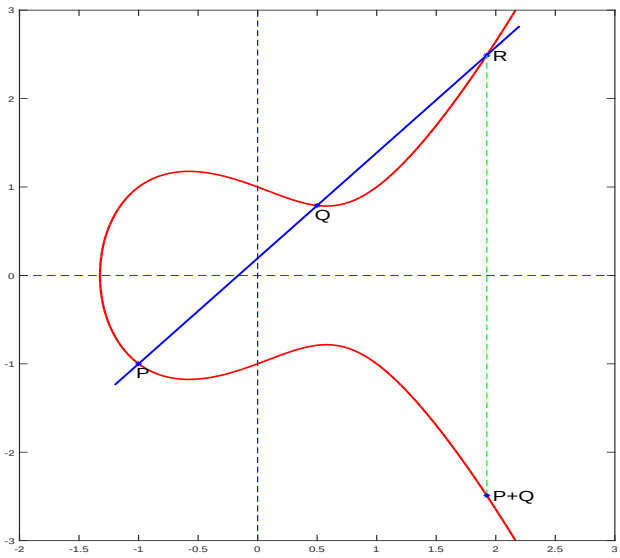

Figure 2.2: The addition law

Given a smooth curve C of genus one, we can associate to C the Jacobian $\mathrm{Jac}(C)$. This Jacobian is an elliptic curve and can be given by a Weierstrass equation. Reducing the study of a genus one curve to a Weierstrass form plays a crucial role in the thesis, since we then work with a more well-understood object. More details about elliptic curves will discussed in the next section.

2.2 The structure of points on elliptic curves over specific fields

In this section, we give more details about elliptic curves over specific fields such as the field of complex numbers, number fields and finite fields, which are the main focuses of the thesis.

Over $\mathbb{C}$

An elliptic curve E over the complex numbers can be illustrated as a torus. It can be written as a quotient $\mathbb{C}/\Lambda$ of the complex plane $\mathbb{C}$ by a lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ for some complex numbers ω_1, ω_2 satisfying $\mathrm{Im}(\omega_1/\omega_2) > 0$. To be precise, we consider the

Weierstrass $\mathcal{P}$-function associated to the lattice Λ defined for all $s \notin \Lambda$ as

$$\mathcal{P}(s) = \mathcal{P}(s; \omega_1, \omega_2) = \frac{1}{s^2} + \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \left(\frac{1}{(s + m\omega_1 + n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2} \right).$$

It satisfies the differential equation

$$\mathcal{P}'(s)^2 = 4\mathcal{P}(s)^3 - g_2\mathcal{P}(s) - g_3, \tag{2.4}$$

where

$$g_2 = 60 \sum_{(m,n)\neq(0,0)} (m\omega_1 + n\omega_2)^{-4},$$

$$g_3 = 140 \sum_{(m,n)\neq(0,0)} (m\omega_1 + n\omega_2)^{-6}.$$

We have the group isomorphism $\mathbb{C}/\Lambda \to E(\mathbb{C})$ sending $s \notin \Lambda \to (\mathcal{P}(s), \mathcal{P}'(s))$ and $0 \to \mathcal{O}$. Elliptic curves over the complex numbers have a crucial role in Paper III.

Over number fields

When K is a number field ($K = \mathbb{Q}$ for instance), the group $E(K)$ of K-points on an elliptic curve E is finitely generated by the Mordell-Weil theorem. In Chapter 3, we will provide a proof for this theorem in the case $K = \mathbb{Q}$. One of the main ingredients of the proof is descent method, which is one of the important tools used in Papers I and II working over the rational numbers.

Over finite fields

Let p is a prime number, let n be a positive integer and let $K = \mathbb{F}_q$ be the finite field with $q = p^n$ elements. In this case, one can estimate the number of K-points on an elliptic curve E by Hasse's theorem as follows:

$$|\sharp E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

Elliptic curves over finite fields are important in this thesis. On the one hand, it is critical in Papers I and II when using the p-adic determinant method to estimate the number of rational points. On the other hand, it is also discussed in Paper III when working over fields of positive characteristics.

2.3 Models of genus one

Elliptic curves in Weierstrass forms are the first examples of genus one models. This type of curve can also be presented in many other ways. Let C be a smooth curve of genus one over a field K and D be a K-rational divisor on C of degree n. Generally, the complete linear system associated to D naturally provides a map from C to $\mathbb{P}^{n-1}$. The pair (C, D) gives us the natural definition of models of genus one of degrees $n \leq 5$ formulated by the authors in [1, Section 2] and [13, Section 3]. More precisely:

Models of degree $n = 1$

In this case, C has a point over K and thus it can be given by a Weierstrass equation (2.1). Therefore, we define a genus one model to be a Weierstrass form.

Models of degree $n = 2$

The map $C \to \mathbb{P}^1$ is now a double cover. The curve C can be determined by an equation of the form

$$y^2 + (\alpha_0 x^2 + \alpha_1 xz + \alpha_2 z^2)y = ax^4 + bx^3 z + cx^2 z^2 + dxz^3 + ez^4. \tag{2.5}$$

A genus one model is defined to be a pair of a binary quadratic and a binary quartic.

When $n \geq 3$, the map $C \to \mathbb{P}^{n-1}$ is an embedding. Therefore, we can identify the curve C with its image in $\mathbb{P}^{n-1}$. More precisely:

Models of degree $n = 3$

In this case, a genus one model ϕ is a ternary cubic as in (1.2).

Models of degree $n = 4$

The model ϕ is given by a pair of quadrics in four variables as in (1.3).

Models of degree $n = 5$

The model is a 5×5 alternating matrix of linear forms in five variables and the equations defined by this model are the 4×4 Pfaffians of the matrix. The definition of Pfaffians

can be found in [13, Section 5.2] and [15]. To be precise, if the model ϕ is the matrix

$$\begin{pmatrix} 0 & a_1 & a_2 & a_3 & a_4 \\ -a_1 & 0 & b_1 & b_2 & b_3 \\ -a_2 & -b_1 & 0 & c_1 & c_2 \\ -a_3 & -b_2 & -c_1 & 0 & d_1 \\ -a_4 & -b_3 & -c_2 & -d_1 & 0 \end{pmatrix},$$

then the 5 corresponding Pfaffians are $p_i = \mathrm{pf}(\phi^i)$ $(i = 1, ..., 5)$ with ϕ^i being the principal sub-matrix of ϕ which is obtained by removing its i-th row and i-column. The Pfaffians of an 4×4 alternating matrix is computed as follows:

$$\mathrm{pf} \begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{pmatrix} = af - be + cd.$$

Chapter 3

Rational points of bounded heights and the counting problem

This chapter discusses the first problem in the thesis about counting rational points on smooth curves defined by models of genus one of degree $n = 3$ and 4. We first give an overview to the topic and then discuss the methods as well as known results in this field.

3.1 Rational points counting

Diophantine equations is one of the oldest areas in mathematics and one of the classical problems in this area is to study the density of solutions of such equations, i.e., the integral solutions of the equations of the form $F(x_0, x_1, ..., x_n) = 0$, where F is a polynomial in $\mathbb{Z}[x_0, x_1, ..., x_n]$. One of the most famous examples is the equation related to Fermat's Last Theorem:

$$x^n + y^n = z^n, \tag{3.1}$$

where n is a positive integer. Fermat conjectured in 1637 that if $n \geq 3$, (3.1) has no non-trivial integral solution and this was proved by Andrew Wiles in 1995.

This problem can be viewed more geometrically since the equation $F = 0$ defines a hypersurface in the affine space $\mathbb{A}^{n+1}$. It means that integral solutions to Diophantine equations can be viewed as integral points on algebraic varieties. Moreover, if F is homogeneous, it defines a hypersurface in the projective space $\mathbb{P}^n$ and the non-zero primitive integer solutions of $F = 0$ correspond (up to sign) to rational points on this hypersurface. We are thus then interested in rational points on projective varieties.

Let us start with the cases in which F is a homogeneous polynomial in $\mathbb{Z}[x_0, x_1, x_2]$ defining a plane curve C in $\mathbb{P}^2$. The theory of plane curves has been studied for a

long time by many mathematicians such as Fermat, Euler, Mordell and there are still many interesting open questions. In the case deg $F = 1$, i.e., $F = a_0x_0 + a_1x_1 + a_2x_2$ for some integers a_0, a_1, a_2, then C is just a line in the plane. If say $a_2 \neq 0$, then its rational points can be represented by pairs of rational numbers $(x_0, x_1) \neq (0, 0)$ as $x_2 = -(a_0x_0+a_1x_1)/a_2$. In case deg $F = 2$, the solutions to $F = 0$ can also be described by one parameter. For example, if $F = x_0^2 + x_1^2 - x_2^2$, then the rational solutions are of the form

$$(x_0, x_1, x_2) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}, 1\right),$$

where t is an arbitrary rational number.

The first non-trivial case is thus when deg $F = 3$. Then C is of genus one if it is non-singular. The solutions to $F = 0$ can thus not be parametrized in the same way as before as C is no longer rational. In general, it is hard to know whether there are finitely or infinitely many rational points on C. It depends on the particular nature of the equation. But we will in this thesis focus on results which hold for general classes of curves. We shall therefore count the number of points inside large boxes and give upper bounds for the number

$$N(C, B) = \sharp\{P \in C(\mathbb{Q}) : \ H(P) \leq B\}$$

of rational points of height at most B on C. Here H is the naive height function $H(P) = \max\{|x_0|, |x_1|, |x_2|\}$ for $P = (x_0, x_1, x_2)$ with coprime integer values of x_0, x_1, x_2. The aim is to establish uniform estimates for $N(C, B)$ which do not depend on the polynomial F defining C.

The first important uniform upper bound for irreducible plane cubic curves was obtained by Heath-Brown [19] in 2002 as a special case of a more general result. He showed that for any $\varepsilon > 0$:

$$N(C, B) \ll_\varepsilon B^{2/3+\varepsilon}. \tag{3.2}$$

Here our notation $f \ll g$ means $f = O(g)$, i.e., there exists a positive constant M such that $|f| \leq M|g|$. The implicit constant in (3.2) depends solely on ε.

The proof of (3.2) was based on his p-adic determinant method which is one of the few tools available for counting problems on varieties of low dimensions. We will in the next section give a description of the basic idea of this method by providing a sketch of the proof of (3.2).

Although the thesis is only devoted to curves of genus one, it is illuminating to give an overview of the density of rational points on an arbitrary non-singular curve C of genus g in $\mathbb{P}^n$. We will here use the notation $N(C, B)$ for the number of

points $P \in C(\mathbb{Q})$ with $H(P) \leq B$, where the height function H is then defined by $H(P) = \max\{|x_0|, ..., |x_n|\}$ for $P = (x_0, ..., x_n)$ with coprime integer values of $x_0, ..., x_n$. There are three cases:

- If $g(C) = 0$: either C has no rational point or $C \cong \mathbb{P}^1$. In the latter case, C is called a rational curve and that $N(C, B) \sim_C B^{2/d}$, where d is the degree of C. Thus the best possible result is $N(C, B) \ll_d B^{2/d}$ shown by Walsh [33].

- If $g(C) = 1$: either C has no rational point or C is an elliptic curve and its rational points form a finitely generated abelian group by Mordell-Weil theorem. Then by Néron, $N(C, B) \sim_C (\log B)^{r/2}$, where r is the rank of the Jacobian $\mathrm{Jac}(C)$.

- If $g(C) \geq 2$: according to Mordell's conjecture, now Faltings's Theorem, C has only a finite number of rational points, i.e., $N(C, B) = O_C(1)$. The best known uniform bound is due to Ellenberg-Venkatesh [12]. They showed that $N(C, B) \ll_d B^{2/d-\delta}$, where δ is a small constant depending only on d, which they do not specify.

The asymptotic behaviour is similar over any number field if we normalize the heights correctly. Here the genus 0 case is easy. So the first non-trivial case is when $g(C) = 1$. In this thesis, we focus on two important classes of genus one curves: smooth plane cubic curves and non-singular complete intersections of two quadrics in $\mathbb{P}^3$.

3.2 Determinant methods

We first describe Heath-Brown's p-adic method by giving a proof to (3.2). We divide all rational points of height at most B on C into congruence classes modulo some prime number p and then count points in each class. By the Hasse-Weil bound, there are $p + O_d(\sqrt{p})$ $\mathbb{F}_p$-points on an irreducible plane curve of degree d. Since an irreducible cubic curve can have at most one singular point, we will only count non-singular points on $C(\mathbb{Q})$. Moreover, by a version of Siegel's lemma (see Theorem 4 of [19]), we can always assume that $||F|| \ll B^{30}$ and then any non-singular point on $C(\mathbb{Q})$ will be non-singular modulo p except for a small number of primes p. Here $||F||$ is the maximum modulus of the coefficients of $F(x_0, x_1, x_2) \in \mathbb{Z}[x_0, x_1, x_2]$.

For a given degree d, we first fix $3d$ monomials $\{F_j\}$, $1 \leq j \leq 3d$ of degree d, which are linearly independent on C. Our goal is now to prove that $\det(M) = 0$ for any $3d \times 3d$-matrix $M = (F_j(P_i))_{i,j}$, where $\{P_i\}$, $1 \leq i \leq 3d$ are rational points on C of height at most B, which reduce to the same non-singular $\mathbb{F}_p$-point for a prime p. The

vanishing of $\det(M)$ for all such sets $\{P_i\}$ will guarantee the existence of a homogeneous polynomial G of degree d which does not vanish everywhere on C. However, G vanishes at all $P \in C(\mathbb{Q})$ of height $H(P) \leq B$, which reduce to the given non-singular $\mathbb{F}_p$-point on the curve defined by $F(x_0, x_1, x_2) = 0 \pmod{p}$. By the theorem of Bézout, there are then at most $3d$ such points in $C(\mathbb{Q})$.

To show that $\det(M) = 0$, we first give an upper bound and then a factor of the integer $\det(M)$ which exceeds the bound. Since all the points are of height at most B, we get the following upper bound by using Hadamard's inequality:

$$|\det(M)| \leq (3d)^{\frac{3d}{2}} B^{3d^2}.$$

But we can also prove that $\det(M)$ is divisible by $p^{3d(3d-1)/2}$ by using the p-adic implicit function theorem and the fact that all $\{P_i\}$ reduce to the same non-singular $\mathbb{F}_p$-point. Hence as long as we only consider integral points which are non-singular (mod p) for a prime p with $p^{3d(3d-1)/2} > (3d)^{\frac{3d}{2}} B^{3d^2}$, then we get at most $3d$ points in each congruence class. We then obtain (3.2) by summing over all $O(p)$ congruence classes for such p.

In this thesis we use the global version of this p-adic determinant method developed by Salberger [24] in which he considers congruences modulo all primes p where C is irreducible over $\mathbb{F}_p$.

3.3 Descent on elliptic curves

We are interested in the case when the curve C is non-singular of genus one. If we fix a rational point $\mathcal{O}$ on C, then we get a bijection between $C(\mathbb{Q})$ and $E(\mathbb{Q})$ for the Jacobian E of C, where P is sent to $P - \mathcal{O}$ in the group $E(\mathbb{Q})$. As E is an elliptic curve over $\mathbb{Q}$, we get by the Mordell-Weil theorem that $E(\mathbb{Q})$ is a finitely generated abelian group as mentioned in Chapter 2. More precisely,

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r, \tag{3.3}$$

where T is the group of all elements of finite order of $E(\mathbb{Q})$ and r is called the rank of E.

We will make essential use of the fact that the Jacobian $E = \text{Jac}(C)$ of a genus one curve C is given by a Weierstrass equation. This makes it possible to use descent with unramified covers to study rational points on cubic curves. It can be proven that any rational point on the original cubic curve may be lifted to a rational point on one of these new cubic curves, we can apply the determinant method to the new curves

instead. This leads to sharper estimates which are not possible to obtain if we only use the determinant method. This is why we only consider non-singular cubic curves.

The main tools for counting rational points in this thesis are the determinant method and descent. We have already discussed the determinant method. It thus remains to discuss descent theory which plays an important role in the thesis. This theory was first developed to prove the Mordell-Weil theorem. We will therefore now provide a sketch of the proof of (3.3).

The theorem holds for general abelian varieties over number fields. But in this section we will only discuss the special case of elliptic curves over the rationals. We follow closely the discussion in Serre [27]. The proof has two parts. The first part is the so called weak Mordell-Weil theorem which says that if E is an elliptic curve, then $E(\mathbb{Q})/mE(\mathbb{Q})$ is a finite abelian group for any positive integer m. To show this one uses Galois cohomology to find an injection of $E(\mathbb{Q})/mE(\mathbb{Q})$ into a Selmer group which is known to be finite. This corresponds to a partition

$$E(\mathbb{Q}) = \bigcup_{\alpha} p_\alpha(C_\alpha(\mathbb{Q})) \tag{3.4}$$

for a finite set of unramified covers $p_\alpha : C_\alpha \to E$ of degree m^2.

The second part of the descent is to use the height function defined in Section 3.1. It can be seen that if a finite set A of elements of $E(\mathbb{Q})$ can be found, such that they generate the group $E(\mathbb{Q})/mE(\mathbb{Q})$, then the finite set $A \cup B$ will generate $E(\mathbb{Q})$, where $B \subset E(\mathbb{Q})$ is the finite set of elements of a given bounded height. Hence, $E(\mathbb{Q})$ is finitely generated. The method is called descent since it can be viewed as a modern more general version of Fermat's method of infinite descent.

A basic feature of the descent process is that for any rational point P and positive integer m, we have that $H(mP) \approx m^2 H(P)$. From (3.4), we thus get that the study of $N(E, B)$ essentially reduces to the study of $\sum_\alpha N(C_\alpha, B/m)$ for a finite set of unramified covers $p_\alpha : C_\alpha \to E$ of degree m^2. This leads to better estimates since we are now working with points of smaller height. This method was first used by Ellenberg and Venkatesh [12] and by Heath-Brown and Testa [20].

3.4 A survey of results

In case of cubic curves, after Heath-Brown's estimate (3.2), Salberger [24] proved a slightly better result

$$N(C, B) \ll B^{2/3} \log B, \tag{3.5}$$

by using his global version of Heath-Brown's p-adic determinant method. He then considered congruences modulo all primes p where C is irreducible over $\mathbb{F}_p$.

The best known uniform bound for irreducible plane cubic curves was given by Walsh [33] using the global determinant method in [24]

$$N(C, B) \ll B^{2/3}. \tag{3.6}$$

We also observe that if $F(x_0, x_1, x_2) = x_0^3 - x_1^2 x_2$, then the solutions $(m^2 n, m^3, n^3)$ show that

$$N(C, B) \gg B^{2/3}. \tag{3.7}$$

But as this curve is singular, it may still be possible to find a sharper bound than (3.6) for non-singular plane cubic curves.

Remark 3.4.1. *All the bounds* (3.2), (3.5) *and* (3.6) *are special cases of more general results for irreducible curves of arbitrary degree d in a fixed projective space. In that case the main term $B^{2/3}$ will then be replaced by $B^{2/d}$.*

Then Ellenberg and Venkatesh [12] proved the following bound for smooth plane cubic curves

$$N(C, B) \ll_\varepsilon B^{2/3 - 1/450 + \varepsilon}$$

by combining the p-adic determinant method with descent theory. Their method was then refined by Heath-Brown and Testa [20] by a clever use of the p-adic determinant method for biprojective curves. They got in this way the sharper estimate

$$N(C, B) \ll_\varepsilon B^{2/3 - 1/110 + \varepsilon}. \tag{3.8}$$

The proof of (3.8) is divided into three steps. The first step is to partition $C(\mathbb{Q})$ into equivalence classes by means of descent where each class is of the form $p_\alpha(C_\alpha(\mathbb{Q}))$ for some unramified cover $p_\alpha : C_\alpha \to C$. The second step is to embed each C_α in $\mathbb{P}^2 \times \mathbb{P}^2$ and reduce to the counting problem for a biprojective curve in $\mathbb{P}^2 \times \mathbb{P}^2$ in order to avoid the comparisons with canonical heights on $\mathrm{Jac}(C)$ used in [12]. The last step is to apply the p-adic determinant method for this biprojective curve. This is more complicated than for the projective plane curves. But the fundamental idea is the same.

The best known result is the following proved by Salberger in his unpublished work

$$N(C, B) \ll_\varepsilon B^{2/3 - 1/84 + \varepsilon}.$$

A striking feature of [20] is that Heath-Brown and Testa also proved the following

bound for any positive integer m

$$N(C,B) \ll m^{r+2}\left(B^{\frac{2}{3m^2}} + \log B\right)\log B,$$

with an implied constant independent of m, where r is the rank of $\mathrm{Jac}(C)$. Taking $m = 1 + [\sqrt{\log B}]$ they obtain that

$$N(C,B) \ll (\log B)^{3+r/2}.$$

For curves of arbitrary degree we also have similar discussion. In [19], Heath-Brown proved that

$$N(C,B) \ll_{\varepsilon} B^{2/d+\varepsilon}$$

for arbitrary irreducible space curves over $\mathbb{Q}$ of degree d by means of his p-adic determinant method. Salberger [24] showed a slightly better uniform bound by using his global determinant method

$$N(C,B) \ll B^{2/d}\log B,$$

which was then improved by Walsh [33] to $N(C,B) \ll B^{2/d}$.

Chapter 4

Invariants of genus one curves

We discuss in this chapter the second problem in the thesis concerning invariants of genus one curves. Besides the structure of points, the structure of invariants is also an interesting and important aspect in order to deeply understand this class of curves. We start with an overview of invariant theory. After that, we discuss the classical invariants of models of genus one as well as the Jacobians of smooth models. Relating a smooth curve of genus one to its Jacobian given by a Weierstrass equation makes an important role in this thesis. We then describe our two main approaches to study this problem with modular forms and determinantal representations.

4.1 Overview on invariants

Invariant theory is the study of algebraic forms, which are invariant under certain linear transformations. The origin of invariant theory was opened by Boole via his works in the 1840s, but this field of study was only systematically developed after that by Cayley and then Sylvester. The modern view of invariant theory was then introduced by Mumford in 1965, where he used the language of algebraic geometry to study invariants. This opened a new subject called geometric invariant theory.

To develop an intuition for invariant theory, let us start with quadratic forms. Let n be any positive integer, we want to determine polynomials in the coefficients of the quadratic form

$$Q = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$$

that is invariant under the action of $SL_n(K)$. One can write $Q = x^T A x$ for $A = (a_{ij})_{i,j}$ and $x = (x_1, x_2, ..., x_n)^T$. We define the discriminant $\Delta(Q)$ of Q to be $\det(A)$. For any

$M \in SL_n$, we have

$$Q \circ M = (Mx)^T A(Mx) = x^T (M^T AM)x.$$

Therefore $\Delta(Q \circ M) = \det(M^T AM) = \det(A)$ since $M \in SL_2$. Thus $\Delta(Q \circ M) = \Delta(Q)$ for any $M \in SL_2$ or Δ is an invariant of Q.

In the case Q is a binary quadratic form $ax^2 + 2bxy + cy^2$, we recover the classical discriminant $\Delta = ac - b^2$. The invariant property of the discriminant of binary quadratic forms with integer coefficients was mentioned in 1801 by Gauss in his *Disquititiones Arithmeticae*, where he studied the class numbers of quadratic fields. We can define invariants of any homogeneous polynomial as below:

Definition 4.1.1. *Let $K[x_1, ...x_n]_d$ be the space of homogeneous polynomials of degree d over a field K. An invariant I of $K[x_1, ...x_n]_d$ is a universal polynomial in the coefficients of elements in $K[x_1, ...x_n]_d$ satisfying $I(f \circ M) = I(f)$ for all $M \in SL_n(\overline{K})$ and $f \in K[x_1, ...x_n]_d$. The degree of I is the degree of I as a polynomial in the coefficients of f.*

Moreover, I is called an invariant of weight $k \in \mathbb{Z}$ if $I(f \circ M) = (\det M)^k I(f)$ for all $M \in GL_n(\overline{K})$ and $f \in K[x_1, ...x_n]_d$.

The fundamental problem in this field, raised by Cayley, is to formulate the invariants and to determine the set of generators, i.e., the set of invariants which can be used to describe all the others in the invariant ring. It was known by Salmon [26] that a ternary cubic over the complex numbers has two invariants, which generate the ring of invariants. The situation in the quartic case is more complicated. The ring of invariants of ternary quartics is generated by 13 elements called Dixmier-Ohno invariants (see [11] and [26]).

For more general cases, Gordan [17] proved that the ring of invariants of any system of binary forms is finitely generated. This famous result is called the finiteness theorem for binary forms. A more general version of this was proposed by Hilbert, which became his fourteenth problem, where he aimed to extend the result to any system of forms in arbitrary number of variables. Hilbert himself established this finiteness property in some special cases. Unfortunately, this property was proved to be false in general. However, it is true in many interesting cases and invariant theorists still pay attention to the Hilbert's fourteenth problem.

In this thesis, we focus on models of genus one which were defined in Section 2.3. Starting with a curve C given by the Weierstrass equation (2.1). There are two classical

invariants defined for instance in [28, p. 42] as

$$c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \tag{4.1}$$

where $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$. The above invariants c_4 and c_6 define the discriminant $\Delta = (c_4^3 - c_6^2)/1728$ so that its non-vanishing is equivalent to the non-singularity of the curve. In this case the curve C is of genus one. Moreover, these c_4 and c_6 generate the ring of invariants of Weierstrass forms associated to (2.1) over fields of characteristics not 2 or 3.

Our goal is to expand this problem to other models of genus one curve of degree $n \leq 5$ defined in Section 2.3. It was first discovered by Weil [35] that in the case $n = 2$, there are two invariants which can be used to write an equation for the Jacobian of a smooth curve of genus one over fields of characteristics not 2 or 3. It shows in this case that the Jacobian of a smooth genus one curve can be defined over the same field as the curve. The classical invariants of genus one models of degree $n = 2, 3, 4$ are summarized in the next section.

4.2 Invariants of genus one models

This section studies the invariants of the affine space X_n of all genus one models of degree n. Since not all genus one models are defined by a single homogeneous polynomial as in Definition 4.1.1, we do not use the linear group GL_n. Fisher [13, Section 3] defined the natural linear algebraic groups $\mathcal{G}_n$ acting on X_n ($n \leq 5$) so that it preserves the solutions of the models. For instance, $\mathcal{G}_1$ is the linear group of the transformations of the form (1.4). We denote by $K[X_n]$ the coordinate ring of X_n and G_n the commutator subgroups of $\mathcal{G}_n$.

Definition 4.2.1. *The ring of invariants of X_n ($n \leq 5$) over K is*

$$K[X_n]^{G_n} := \{I \in K[X_n] : I \circ g = I \text{ for all } g \in G_n(\overline{K})\}.$$

The vector space of invariants of weight k of X_n over K is defined as

$$K[X_n]_k^{G_n} := \{I \in K[X_n] : I \circ g = (\det g)^k I \text{ for all } g \in \mathcal{G}_n(\overline{K})\}.$$

The character det on $\mathcal{G}_n$ is explicitly described as in [13], which provides appropriate weights for the invariants in the above definition. Furthermore, it (see [13, Lemma 4.3])

equips the ring of invariants with the grading structure

$$K[X_n]^{G_n} = \bigoplus_{k \geq 0} K[X_n]_k^{G_n}.$$

The following facts about invariants of genus one models of degrees $n \leq 4$ are classical and summarized in [1]. The case $n = 5$ has recently been treated by Fisher [14] in characteristic zero. The two invariants introduced in each degree below generate the ring of invariants and determine the Jacobians of smooth models in characteristic not 2 or 3. These generalize Weil's result in the case $n = 2$.

Models of degree $n = 1$

The invariants c_4, c_6 of a Weierstrass form corresponding to (2.1) are defined as in (4.1).

Models of degree $n = 2$

If $\mathrm{char}(K) \neq 2$, we can rewrite (2.5) in the short form $y^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$. This short model ϕ has two classical invariants (see [1, Section 3.1])

$$i = (12ae - 3bd + c^2)/12,$$

$$j = (72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3)/432$$

and a corresponding Weierstrass equation $y^2 = 4x^3 - ix - j$. The invariants of the generalized model (2.5) can be found in [6, p. 766] by completing the square.

Models of degree $n = 3$

The two classical invariants S, T of the ternary cubic (1.2) are defined in [1, p. 309-310] and a corresponding Weierstrass equation of this cubic is $y^2 = 4x^3 + 108Sx - 27T$.

Models of degree $n = 4$

The model ϕ is given by a pair of quadrics $q_1, q_2 \in K[x_0, x_1, x_2, x_3]$, we write $q_1 = \overline{x}A\overline{x}^T$ and $q_2 = \overline{x}B\overline{x}^T$ for the two symmetric 4×4 matrices A, B with $\overline{x} = (x_0, x_1, x_2, x_3)$. The invariants of the model (q_1, q_2) are then defined by the invariants of the quartic

$$\det(xA + zB) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 \tag{4.2}$$

as in the case $n = 2$. A corresponding Weierstrass equation of (q_1, q_2) is thus given by the corresponding ones of the model (4.2).

Invariants in characteristic 2 and 3

We have seen that there are two invariants of weights 4 and 6 generating the ring of invariants of models of genus one and provide for smooth models their Jacobians in characteristic not 2 or 3. The situation in characteristic 2 and 3 is more complicated, since the above invariants are no longer enough to generate the ring of invariants of genus one models. This problem was studied by Fisher [13], where he prove that the ring of invariants of genus one models of degree $n \leq 5$ is also generated by two elements in characteristic 2 and 3.

To put things all together, we recall the following structure result from [13, Theorems 4.4, 10.2, Lemma 10.1]. Here c_4, c_6 are the usual invariants defined in the previous page and a_1, b_2 are the invariants of weight 1,2 respectively defined as in [13, Theorem 10.2].

Proposition 4.2.2. *The ring of invariants $K[X_n]^{G_n}$ of X_n $(n \leq 5)$ over a field K is*

$$\begin{cases} K[c_4, c_6], & \text{if } char(K) \neq 2, 3; \\ K[a_1, \Delta], & \text{if } char(K) = 2; \\ K[b_2, \Delta], & \text{if } char(K) = 3. \end{cases}$$

Normalized invariants

Multiplying with a non-zero scaler preserves the weight of an invariant of weight k of a genus one model. One can ask the question: what is a nice normalization of an invariant? Fisher [13] gave an answer to this question. More precisely, he normalized the invariants c_4, c_6 of X_n $(n = 2, 3, 4)$ such that they are primitive polynomials defined over the integers. Furthermore, these invariants produce the appropriate discriminant $\Delta = (c_4^3 - c_6^2)/1728$ which characterizes the singularity of genus one models over any field K as for X_1. Note that in the case $n = 3$, these invariants was normalized before in [2].

One can compare these normalized invariants with the classical ones mentioned in the previous section as follows:

$$\begin{cases} c_4 = 2^6 3i, \ c_6 = 2^9 3^3 j, & n = 2; \\ c_4 = -2^4 3^4 S, \ c_6 = 2^3 3^6 T, & n = 3; \\ c_4 = 2^{10} 3i, \ c_6 = 2^{15} 3^3 j, & n = 4. \end{cases}$$

In this thesis, by relating invariants to modular forms, we provide a different way to express these normalized invariants. The details are presented in Paper III. The next section discusses modular forms and their natural connection to invariants.

4.3 Modular forms and invariants

Modular forms is a broad subject. This field of study plays important roles in different fields of mathematics and physics. There is a link between modular forms and elliptic curves via the modularity theorem, also known as the Taniyama-Shimura-Weil conjecture, which is an important result in number theory. In this thesis, we want to study the natural connection between modular forms and invariant theory. We first recall some basic knowledge to this topic.

Classical modular forms

Generally speaking, a modular form is a function on the upper half-plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}\tau > 0\}$ which satisfies a certain transformation property. We will give formal definitions of some types of modular forms, which have important role in the thesis.

A holomorphic modular form F of weight $k \in \mathbb{Z}$ is a holomorphic function on $\mathbb{H}$, which satisfies the following properties:

a)

$$F\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k F(\tau) \text{ for any } \tau \in \mathbb{H}\ ,\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}). \qquad (4.3)$$

b) F is holomorphic at ∞.

The latter condition means that F has an absolutely convergent Fourier expansion

$$F(\tau) = \sum_{n=0}^{\infty} a_n q^n,\ q = e^{2\pi i\tau}$$

in $\{|q| < 1\}$. If we replace this condition by that F is meromorphic at ∞, then F is called a weakly holomorphic modular form.

Denote by $M_k(\mathbb{C})$ (resp. $M_k^!(\mathbb{C})$) the space of holomorphic modular forms (resp. weakly holomorphic modular forms) of weight k and $M(\mathbb{C})$ (resp. $M^!(\mathbb{C})$) the graded algebra

$$M(\mathbb{C}) = \bigoplus_{k\in\mathbb{Z}} M_k(\mathbb{C}) \text{ (resp. } M^!(\mathbb{C}) = \bigoplus_{k\geq 0} M_k^!(\mathbb{C})).$$

Among all the others, for us, the Eisenstein series G_{2k} ($k \in \mathbb{Z}_{\geq 2}$) is an important example of holomorphic modular forms. The function G_{2k} is a holomorphic modular

form of weight $2k$ defined by

$$G_{2k}(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m+n\tau)^{2k}}, \tag{4.4}$$

which has the following normalized form

$$E_{2k}(\tau) = \frac{G_{2k}(\tau)}{2\zeta(2k)} = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{+\infty} \sigma_{2k-1}(n) q^n, \tag{4.5}$$

where $\zeta(s), B_{2k}$ and σ_{2k-1} are the Riemann zeta function, the Bernoulli numbers and the divisor sum function respectively.

Another important example of holomorphic modular forms is the modular discriminant, which is the cusp form of weight 12 defined as

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1-q^n)^{24}, \ q = \exp(2\pi i \tau).$$

This cusp form is related to the Eisenstein series E_4, E_6 by $1728\Delta = E_4^3 - E_6^2$.

Let R be a sub-ring of $\mathbb{C}$, we define for any integer k the R-module

$$M_k(R) = \left\{ F \in M_k(\mathbb{C}) \mid F(\tau) = \sum_{n=0}^{\infty} a_n q^n \text{ with } a_n \in R \right\}$$

and the R-algebra

$$M(R) = \bigoplus_{k\geq 0} M_k(R).$$

It is natural to consider the case $R = \mathbb{Z}$. We know by Deligne [9, Proposition 6.1] that the algebra $M(\mathbb{Z})$ is generated by E_4, E_6 and cusp form Δ. Here E_4, E_6 are defined over $\mathbb{Z}$, since in (4.5) we see that $4k/B_{2k} \in \mathbb{Z}$ for $k = 2, 3$. The modular forms E_4, E_6 and Δ are thus defined over any field K. Moreover, if $\mathrm{char}(K) \neq 2$ or 3, then 1728 is invertible over K so that we can express Δ in terms of E_4 and E_6. In other words

$$M(K) = K[E_4, E_6]. \tag{4.6}$$

Then one can naturally define modular forms over $\mathbb{F}_p$ for a prime number p by taking reduction modulo p each coefficient in the q-expansion of a modular form with integer coefficients.

It is natural to relate invariants to modular forms when looking over the complex numbers. For a smooth genus one curve C given by a Weierstrass form ϕ with

$C(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for some $\tau \in \mathbb{H}$, then ϕ is of the form $y^2 - 4x^3 + g_2x + g_3$. One can write the two coefficients g_2, g_3 of ϕ as $g_2 = 60G_4, g_3 = 140G_6$ with G_4, G_6 defined in (4.4). By some elementary computations, the normalized invariants of the model ϕ are related to the normalized Eisenstein series as follows:

$$c_4(\phi) = (4\pi)^4 E_4(\tau),\ c_6(\phi) = (4\pi)^6 E_6(\tau). \tag{4.7}$$

Hence, Proposition 4.2.2 and the formulae (4.6), (4.7) provide a correspondence between weakly holomorphic modular forms and invariants of smooth Weierstrass equations in characteristic not 2 or 3. It can also be seen from (4.7) that the discriminant Δ_ϕ of ϕ is related to the modular discriminant by

$$\Delta_\phi = (4\pi)^{12}\Delta(\tau).$$

The situation is more complicated in characteristic 2 and 3. In this case, a modular form of weight 1 or 2 over $\mathbb{F}_p$ $(p = 2, 3)$ can not be lifted to a modular form over $\mathbb{Z}$ since there are no non-zero modular forms of weight 1 and 2 over $\mathbb{Z}$. Thus, we do not have the correspondence with the invariants a_1, b_2 of weight 1,2 respectively in Proposition 4.2.2. To see the connection with invariants in this case, we extend the notion of modular forms in the next section.

Geometric modular forms

The formal definition of geometric modular forms can be found in Paper III (see Definition 4.1). Generally speaking, a geometric modular form $\mathcal{F}$ of weight $k \in \mathbb{Z}$ over a ring R is a rule, which assigns to every pair $(C/R, \omega)$ of an elliptic curve C over R and a regular 1-form ω on C an element $\mathcal{F}(C, \omega) \in R$. It should satisfy the following transformation for any $\lambda \in R^*$:

$$\mathcal{F}(C, \lambda\omega) = \lambda^{-k}\mathcal{F}(C, \omega). \tag{4.8}$$

One can extend this definition by replacing an elliptic curve by a smooth curve of genus one. To get an intuition about geometric modular forms, one can see the correspondence to weakly holomorphic modular forms over $\mathbb{C}$ by looking at the discussion in Katz [21, p. 91] as follows. Let $\mathcal{F}$ be a geometric modular form over $\mathbb{C}$ of weight k and $C_\tau := \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ for any $\tau \in \mathbb{H}$. We define the corresponding weakly holomorphic modular form F of weight k defined by $F(\tau) = \mathcal{F}(C_\tau, 2\pi i\ dz)$. Here dz is the canonical differential on $\mathbb{C}$. Katz [21, pp. 91-93] also proved the meromorphicity of F at ∞.

By this construction, we are able to define modular forms of small weights. More concretely, let p be any prime, there is a geometric modular form $\mathcal{A}_p$ over $\mathbb{F}_p$ called the Hasse invariants defined for instance in [21] (p. 29). This is a geometric modular form over $\mathbb{F}_p$ of weight $p-1$.

The crucial point is that, a geometric modular form $\mathcal{F}$ of weight k over a field K determine an invariant of the same weight $I_{\mathcal{F}}$ of X_n^0 for any $n \leq 4$ and also for $n = 5$ if $\mathrm{char}(K) \neq 2$. Here X_n^0 is the subset of smooth genus one models of degree n in X_n. The invariant $I_{\mathcal{F}}$ is defined by

$$I_{\mathcal{F}}(\phi) = \mathcal{F}(C_\phi, \omega_\phi), \tag{4.9}$$

where (C_ϕ, ω_ϕ) is the pair of a smooth curve of genus one C_ϕ and a natural regular 1-form defined by $\phi \in X_n^0$. The detail about this regular 1-form is described in [13, Section 5.4]. For instance, the natural regular 1-form of the Weierstrass model ϕ corresponding to (2.1) is $\omega_\phi = dx/(2y + a_1x + a_3)$.

This correspondence works in any characteristic. It makes an important role in Paper III to study invariants, where we construct formulae relating invariants of smooth models of genus one of degree $n \leq 4$ and their Jacobians. To be precise, in that paper we define an explicit map $\varphi_n : X_n \to W$ from the affine space X_n of genus one models of degree n to the affine space W of Weierstrass forms based on the classical explicit map f_n in [1]. The map $f_n : C_\phi \to E_\phi$ $(n = 2, 3, 4)$ from a smooth curve defined by $\phi \in X_n^0$ to its corresponding Jacobian E_ϕ is defined by a divisor D of degree n on C_ϕ as $f_n(P) = nP - D$. Here the Jacobian E_ϕ is given by a Weierstrass equation and the divisor D is chosen to be the intersection of C_ϕ with the hyperplane at infinity (see [1, p. 305]).

There exists $\alpha_n = \alpha_n(\phi) \in K^*$ such that $\varphi_n^*(\omega_{\varphi_n(\phi)}) = \alpha_n\omega_\phi$ for any $\phi \in X_n^0(K)$. The transformation property (4.8) gives us the following identity for a geometric modular form $\mathcal{F}$ of weight k

$$I_{\mathcal{F}}(\phi) = \alpha_n^k I_{\mathcal{F}}(\varphi_n(\phi)). \tag{4.10}$$

The formula (4.10) provides us then the invariants of smooth genus one models through the corresponding ones of a Weierstrass form. This is the crucial idea in Paper III since Weierstrass forms are more well-understood.

4.4 Determinantal representation and discriminant

This section discusses the second approach to study invariants of genus one models over the complex numbers focusing on discriminants of ternary cubics. To be precise, we use determinantal representations to relate the coefficients of a ternary cubic to theta functions. Theta functions are fundamental examples of which can be used to construct modular forms.

Discriminants and theta functions

As a motivating example, we consider the discriminant of a plane cubic curve which is a polynomial of degree 12 in the coefficients of the cubic with 2040 monomials. This is inconvenient to work with. But in the case of complex number, we have shorter expressions for the discriminants in terms of theta constants. Consider the smooth genus one curve C defined by the Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$. Using the Weierstrass parametrization, there exists a lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with some complex numbers ω_1, ω_2 such that $\mathrm{Im}(\omega_2/\omega_1) > 0$ and $C(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Let $\tau := \omega_2/\omega_1$ and define the theta constants $a = \theta_2(0,\tau) = e^{\frac{\pi i\tau}{4}}\theta(\frac{1}{2}\tau,\tau)$, $b = \theta_3(0,\tau) = \theta(0,\tau)$, $c = \theta_4(0,\tau) = \theta(\frac{1}{2},\tau)$ with the Jacobi theta function

$$\theta(z,\tau) := \sum_{n=-\infty}^{\infty} \exp(\pi i n^2\tau + 2\pi i n z).$$

The discriminant formula $\Delta = 2^{12}(g_2^3 - 27g_3^2)$ yields

$$\Delta = 2^{16}\left(\frac{\pi}{\omega_1}\right)^{12}(abc)^8. \tag{4.11}$$

This discriminant formula comes from [2, p. 367-368] with the normalized invariants $c_4 = 2^6 3 g_2$, $c_6 = 2^9 3^3 g_3$.

This algebraic-analytic connection between discriminants and theta functions is remarkable. One can ask if we also have similar phenomena in more general cases? We will try to answer this question with a new approach using determinantal representations.

Determinantal representations

Let ϕ be a homogeneous polynomial of degree d, we construct a $d \times d$ matrix U whose elements are linear forms such that $\phi = \lambda \det(U)$ for some constant $\lambda \neq 0$. The study of ϕ has thus been moved to the study of the matrix U. Let us start with a simple

example in which we consider the binary quadratic form $\phi = ax^2 + bxy + cy^2$. Then $\phi = \det(U)$ with

$$U = \begin{pmatrix} ax + cy & (a + c - b)x \\ y & x + y \end{pmatrix}.$$

To construct a less trivial example we move to the case of ternary cubic. For instance, consider the cubic form $\phi = y^2z - 4x^3 - xz^2 + 4z^3$, then $\phi = \det(U)$ with U is equal to

$$\begin{pmatrix} 2x + z & y + z & 4z \\ 0 & x - z & y - z \\ z & 0 & -2x - z \end{pmatrix}.$$

Dickson [10] proved that in general, only plane curves, quadratic and cubic surfaces, quadratic three-folds admit a determinantal representation. The reader can have a look at [5] for a general overview to this topic. We continue with a smooth curve C_ϕ given in Weierstrass form

$$\phi(x, y, z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3, \tag{4.12}$$

where g_2 and g_3 are elements in a field K. Determinantal representations of Weierstrass forms has been established by Vinnikov [32, Section 2], where he provided the representations for another type of Weierstrass equations of the form $y^2z = x(x+\vartheta_1 z)(x+\vartheta_2 z)$ for some constants $\vartheta_1, \vartheta_2 \in K$. Following Vinnikov's method, we obtain for ϕ the determinantal representations

$$\begin{pmatrix} 2x + tz & y + dz & (3t^2 - g_2)z \\ 0 & x - tz & y - dz \\ z & 0 & -2x - tz \end{pmatrix}, \tag{4.13}$$

with $t, d \in \overline{K}$ be such that $d^2 = 4t^3 - g_2t - g_3$. One can check that the determinant of the matrix (4.13) is equal to ϕ.

When $K = \mathbb{C}$, as mentioned in Chapter 1, $C_\phi(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for the lattice Λ coming from the Weierstrass parametrization. One can write $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ for some $\omega_1, \omega_2 \in \mathbb{C}$ with $\tau = \omega_2/\omega_1 \in \mathbb{H}$. The two coefficients g_2 and g_3 of the curve given by (4.12) is determined by (see [34, p. 509])

$$g_2 = \frac{2}{3}\left(\frac{\pi}{\omega_1}\right)^4 (a^8 + b^8 + c^8),$$

$$g_3 = \frac{4}{27}\left(\frac{\pi}{\omega_1}\right)^6 (a^4+b^4)(b^4+c^4)(c^4-a^4),$$

where a, b, c are even theta constants defined in the previous section. Since (t, d) is a point on the affine curve associated to C_ϕ defined by $\{z \neq 0\}$, it is determined by theta constants and so are all the elements of the matrix (4.13). To be precise, we consider the Weierstrass $\mathcal{P}$-function associated to the lattice Λ. The point (t, d) on the curve can be parametrized as $t = \mathcal{P}(s)$ and $d = \mathcal{P}'(s)$ for some $s \notin \Lambda$. In addition, the choice of the 2-torsion point, $s = \omega_2/2$ say, will give us the following representation of ϕ

$$\begin{pmatrix} 2x - \frac{\pi^2}{3\omega_1^2}(a^4+b^4)z & y & -(\frac{\pi}{\omega_1})^4 c^8 z \\ 0 & x + \frac{\pi^2}{3\omega_1^2}(a^4+b^4)z & y \\ z & 0 & -2x + \frac{\pi^2}{3\omega_1^2}(a^4+b^4)z \end{pmatrix}. \tag{4.14}$$

Since the discriminant of a polynomial can be computed by the resultant of its partial derivatives (see [16, p. 434]), the discriminant Δ_ϕ of the curve C_ϕ is equal to

$$\Delta_\phi = 2^{16}\left(\frac{\pi}{\omega_1}\right)^{12}(abc)^8.$$

The classical formula (4.11) has thus been recovered. We want to study this phenomena in more general cases, i.e., to see if one can representation a certain polynomial as the determinant of some matrix whose elements are written in theta constants as in (4.14). In this direction, Ball and Vinnikov [4, Theorem 5.1] provide an important result, which is the key point in Paper III to expand this study to general cubic forms.

Plane quartics and Klein's formula

Although this thesis focus on curves of genus one, but it is also interesting to mention a beautiful formula of Klein on plane quartics, which are non-hyperelliptic curves of genus three. More concretely, let C_ϕ be a smooth plane curve over $\mathbb{C}$ given by a quartic ϕ, let $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3$ be a symplectic basis of $H_1(C_\phi, \mathbb{Z})$ and let η_1, η_2, η_3 be the classical basis of holomorphic 1-forms of $\Omega^1_{\mathbb{C}}(C_\phi)$ defined in [23, p. 329]. We construct from these the period matrix $[\Omega_1\ \Omega_2]$ whose entries are

$$(\Omega_1)_{ij} = \int_{\alpha_i} \eta_j \text{ and } (\Omega_2)_{ij} = \int_{\beta_i} \eta_j, \text{ for } i, j = 1, 2, 3.$$

De note by $\tau = \Omega_2^{-1}\Omega_1$, the discriminant Δ_ϕ of ϕ satisfies the following formula (see [22, p. 72]):

$$\Delta_\phi^2 = \prod_{\delta \text{ even}} \theta_\delta(0, \tau). \tag{4.15}$$

Here θ_δ is the Riemann theta function with characteristic $\delta = (\delta_1, \delta_2)$, where $\delta_1, \delta_2 \in \{0, 1\}^3$, defined for any $z \in \mathbb{C}^3$ as:

$$\theta_\delta(z, \tau) = \sum_{n \in \mathbb{Z}^3} \exp 2\pi i \left(\frac{1}{2}(n + \delta_1)^t \tau (n + \delta_1) + (n + \delta_1)^t (z + \delta_2) \right).$$

The product in (4.15) runs over all 36 even theta characteristics of genus three. The characteristic δ is called even if the corresponding theta function θ_δ is an even function in z. This formula should be compared with (4.11) in Weierstrass case. One can ask if it is possible to use determinantal representations to establish the formula (4.15) or not? For this, the authors in [18] and [25] have obtained determinantal representations for plane quartics described by theta constants. Thus it might be possible to explore this problem in this case.

Chapter 5

Summary of papers

5.1 Paper I

In this paper, we work on the uniform bounds for the number

$$N(C,B) = \sharp\{P \in C(\mathbb{Q}) : \ H(P) \leq B\}$$

of $\mathbb{Q}$-points of height at most B on a non-singular plane curve C, which is defined by a cubic form F. We follow the approach of [20] closely except that the p-adic determinant method is replaced by the global determinant method of Salberger [24]. This gives the following improvements of Theorem 1.2 and Corollary 1.3 in [20].

Theorem 5.1.1. *Let C be a smooth plane cubic curve and r be the rank of Jac(C). Then for any positive integer m and any $B \geq 3$, we have*

$$N(C,B) \ll m^r \left(B^{\frac{2}{3m^2}} + m^2\right) \log B$$

and

$$N(C,B) \ll (\log B)^{2+r/2}.$$

The bounds are uniform in the sense that the implicit constants only depend on the rank r of the corresponding Jacobian.

In the appendix, we also include an even better estimate (see [29, Theorem 9]), which is obtained by a re-examination of the argument in [20]. This is based on a deep result of David [8] about successive minima for the quadratic form corresponding to the canonical height on Jac(C). The estimates in Theorem 5.1.1 and [29, Theorem 9] should be compared with the classical result of Néron:

$$N(C,B) \sim c_F (\log B)^{r/2},$$

where c_F is a constant depending on F. But the proof of that result gives very little information about the error terms and no uniform bounds for $N(C, B)$.

5.2 Paper II

In this paper (see [30]), we study the rational points counting problem on non-singular quartic curves C over $\mathbb{Q}$ given by complete intersections of two quadrics in $\mathbb{P}^3$. As C is of genus one, the Jacobian $\mathrm{Jac}(C)$ is again an elliptic curve given by a Weierstrass equation and one can apply descent theory.

We first use descent and the global determinant method to prove the following bound for the number $N(C, B)$ of rational points of height at most B on C.

Theorem 5.2.1. *Let C be a smooth complete intersection of two quadric surfaces and r be the rank of Jac(C). Then for any positive integer m and any $B \geq 3$, we have*

$$N(C, B) \ll m^r \left(B^{\frac{1}{2m^2}} + m^2 \right) \log B.$$

Taking $m = 1 + [\sqrt{\log B}]$ we obtain $N(C, B) \ll (\log B)^{2+r/2}$.

This result should be compared with Theorem 5.1.1 for cubic curves. The second goal of this paper is to moreover improve the uniformity by establishing the estimate which does not depend on the rank r of $\mathrm{Jac}(C)$. The following result is established:

Theorem 5.2.2. *Let C be a non-singular complete intersection of two simultaneously diagonal quadrics in $\mathbb{P}^3$. Then*

$$N(C, B) \ll_\varepsilon B^{1/2-3/392+\varepsilon}. \tag{5.1}$$

The proof bases on the same basic dichotomy as in two articles [12] of Ellenberg and Venkatesh and [20] of Heath-Brown and Testa:

- For curves of small height we use descent and the determinant method for unramified covers of C. To sum over the descent classes, we will also need upper estimates for the rank of $\mathrm{Jac}(C)$ in terms of its discriminant.
- For curves of large height, we use a refinement of the determinant method where we find extra factors in the determinant which come from the coefficients of the quadratic forms defining C.

One difficulty is that we first need to define a height function on a parameter variety of such quartic curves. This is much easier for cubic curves, where the height function

can be defined by the maximum modulus of coefficients of the polynomial F defining the curve. Unfortunately, the author has not been able to prove the main estimate (5.1) for general non-singular complete intersections of two quadrics in $\mathbb{P}^3$. So we will only consider the case where C is given by a complete intersection of two simultaneously diagonal quadratic forms.

Suppose that C is given by a complete intersection of two simultaneously diagonal quadratic forms $q = a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ and $r = b_0x_0^2 + b_1x_1^2 + b_2x_2^2 + b_3x_3^2$ with integral coefficients. One can check that C is smooth if and only if all six minors $d_{ij} = a_ib_j - a_jb_i \neq 0$, $0 \leq i < j \leq 3$. These six minors will satisfy a quadratic Plücker relation. So C is parametrized by a rational point P on a quadric in $\mathbb{P}^5$ with coordinates given by those six minors. The height $H(C)$ of C is then defined to be the height of P in $\mathbb{P}^5$. We have thus

$$H(C) = \max_{0\leq i<j\leq 3}(|d_{ij}|)/\gcd_{0\leq i<j\leq 3}(d_{ij}).$$

Then we use a refinement of Heath-Brown's p-adic determinant method to prove that

$$N(C,B) \ll_\varepsilon B^{1/2+\varepsilon}/H(C)^{1/8} + B^\varepsilon. \tag{5.2}$$

This bound is an analog of the bound

$$N(C,B) \ll_\varepsilon B^{2/3+\varepsilon}/H(C)^{1/9} + B^\varepsilon$$

in [12] for plane cubic curves.

Next step is to use a standard 2-descent argument as in Brumer and Kramer [3] to bound the rank r of $\mathrm{Jac}(C)$ in terms of its discriminant Δ. This discriminant measures the singularity of the curve $\mathrm{Jac}(C)$. One can prove that for any $c > 1/(2\log 2)$ we have

$$r < c\,\log|\Delta| + \mathrm{O}_\varepsilon(1).$$

This is discussed by Ellenberg and Venkatesh [12, p. 2177]. In Theorem 5.2.1, if we take $m = 2$ then

$$N(C,B) \ll 2^r B^{1/8}\log B \ll_\varepsilon |\Delta|^{1/2+\varepsilon}B^{1/8}\log B. \tag{5.3}$$

The discriminant Δ of $\mathrm{Jac}(C)$ can be computed by means of the formulas in [1, Sections 3.1 and 3.3]. This gives

$$\Delta = 2^{-8}\prod_{0\leq i\neq j\leq 3}(a_ib_j - a_jb_i).$$

One can reduce to the case where (q, r) is a pair with $\gcd_{0\leq i<j\leq 3}(a_i b_j - a_j b_i) = 1$, in which case we prove that

$$|\Delta| \leq H(C)^{12}. \tag{5.4}$$

From (5.3) and (5.4) we obtain that

$$N(C, B) \ll_\varepsilon H(C)^{6+\varepsilon} B^{1/8} \log B. \tag{5.5}$$

Comparing (5.2) with (5.5) we see that the worst case is when $H(C) = B^{3/49}$. Theorem 5.2.2 is then obtained.

5.3 Paper III

In the previous two papers, there is an object called the discriminant which naturally appears in the rational points counting problem. This object characterizes the bad reduction of polynomials and thus has an important role in the determinant method. The discriminant is a classical example of an invariant. It provides an inspiration to this paper, where we study invariants of models of genus one. Here a model of genus one is a set of polynomials, which generically defines a genus one curve (see Section 2.3). An invariant of a genus one model is a polynomial in the coefficients of the model that is unchanged under certain linear transformations.

The aim of this paper is to give a different way to express the normalized invariants, which are the ones defined over the integers, of a genus one model of degree $n = 2, 3, 4$ over a field K. To do this, we construct an explicit map φ_n from the affine space X_n of genus one models of degree n to the space of Weierstrass equations. This gives a formula relating invariants of a smooth genus one model to the corresponding ones of a Weierstrass form of the model. The map φ_n is constructed at the end of Section 4.3. As a first step, we compute the discriminant directly using the singularities of the models. The first result of the paper is the following:

Theorem 5.3.1. *Let C_ϕ be a curve defined by a genus one model ϕ of degree n ($n = 2, 3, 4$) over a field K and $\Delta_\phi, \Delta_{\varphi_n(\phi)}$ be the discriminants of ϕ and its corresponding Weierstrass form $\varphi_n(\phi)$. We have (up so sign)*

$$\Delta_\phi = \alpha_n^{12} \Delta_{\varphi_n(\phi)},$$

where $\alpha_2 = 1, \alpha_3 = 1/2, \alpha_4 = 2$.

One can obtain a generalization of Theorem 5.3.1 by replacing the discriminant by

any invariant coming from a (geometric) modular form, which was defined in Section 4.3. To be precise, in this paper we naturally associate to a geometric modular form $\mathcal{F}$ an invariant $I_{\mathcal{F}}$ of X_n^0 of the same weight (see (4.9)). Here X_n^0 is the subset of X_n consisting of all smooth genus one models of degree n.

As an example, let $\mathcal{E}_4, \mathcal{E}_6$ be the corresponding (geometric) modular forms of the normalized Eisenstein series E_4, E_6 respectively and let $\mathcal{D}$ be the cusp form of weight 12 satisfying $1728\mathcal{D} = \mathcal{E}_4^3 - \mathcal{E}_6^2$. Let c_4, c_6 be the normalized invariants of weights 4,6 respectively of X_n and $\Delta = (c_4^3 - c_6^2)/1728$ be the discriminant. We prove in the paper that $I_{\mathcal{E}_4} = c_4, I_{\mathcal{E}_6} = -c_6$ and $I_{\mathcal{D}} = \Delta$ on X_n^0. Here we use the notation $\mathcal{D}$ for the cusp form in order to avoid the confusion with the discriminant Δ. The next result in the paper is the following:

Theorem 5.3.2. *Let C_ϕ be a smooth curve of genus one defined by a model ϕ of degree n ($n = 2, 3, 4$) over a field K with the corresponding Jacobian E_ϕ defined by $\varphi_n(\phi)$. Let k be an integer and $I_{\mathcal{F}}$ be the invariant of weight k associated to a geometric modular form $\mathcal{F}$ of weight k. We then have*

$$I_{\mathcal{F}}(\phi) = \alpha_n^k I_{\mathcal{F}}(\varphi_n(\phi)),$$

where $\alpha_2 = 1, \alpha_3 = 1/2, \alpha_4 = 2$.

The second part of the paper uses determinantal representations to study invariants over the complex numbers focusing mainly on discriminants of ternary cubics. A first result represents Weierstrass cubics as determinants (see [31, Proposition 1.5]). This is then extended to general complex plane curves as below by following closely the method in [4]:

Theorem 5.3.3. *Let $C_\phi \subset \mathbb{P}^2$ be a non-rational irreducible complex plane curve defined by $\phi = 0$, where $\phi(x, y, z)$ is an irreducible homogeneous polynomial of degree d. Suppose the d intersection points of C_ϕ with the line $\{y = \alpha x + \gamma z\}$ are distinct non-singular points $P_1, ..., P_d$ with coordinates $P_i = (1, \alpha + \gamma\beta_i, \beta_i)$, $\beta_i \neq 0$. Then up to multiplication by some constant:*

$$\phi(x, y, z) = \det((M - \alpha N)x + Ny + (I - \gamma N)z),$$

where $M = \mathrm{diag}(-\beta_1, ..., -\beta_d)$ and $N = (n_{ij})_{i,j}$ with

$$n_{ii} = -\frac{\beta_i \frac{\partial \phi}{\partial y}(P_i)}{(\frac{\partial \phi}{\partial x} + \alpha \frac{\partial \phi}{\partial y})(P_i)}$$

and for $i \neq j$

$$n_{ij} = \frac{\theta[\delta](\varphi(P_j) - \varphi(P_i))}{\theta[\delta](0)E(P_j, P_i)} \frac{\beta_i - \beta_j}{\sqrt{\beta_i(\alpha dx - dy)(P_i)}\sqrt{\beta_j(\alpha dx - dy)(P_j)}}.$$

Here δ *is an even theta characteristic such that* $\theta[\delta](0) \neq 0$, $\varphi : X \to J(X)$ *is the Abel-Jacobi map from the desingularizing Riemann surface* X *of* C_ϕ *to its Jacobian and* $E(.,.)$ *is the prime form on* $X \times X$.

Using this theorem, we find in particular a formula for the discriminant of plane cubics in terms of theta functions. More precisely, a smooth plane cubic C_ϕ can be linearly transformed to a Weierstrass form E_ϕ by a fixed flex point on the curve C_ϕ (see [7, Section 4.4]). Denote by M the linear transformation, the resulting Weierstrass form E_ϕ is isomorphic to $\mathbb{C}/\Lambda$ for the lattice Λ coming from the Weierstrass parametrization. One can write $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ for the complex numbers ω_1, ω_2 with $\mathrm{Im}(\omega_2/\omega_1) > 0$ and denote by $\tau = \omega_2/\omega_1$. We obtain the following result:

Theorem 5.3.4. *Let* C_ϕ *be a smooth plane curve over* $\mathbb{C}$ *defined by a cubic form* ϕ *and* Δ_ϕ *be the discriminant of* ϕ, *we have*

$$\Delta_\phi = \frac{2^{16}}{\det(M)^{12}} \left(\frac{\pi}{\omega_1}\right)^{12} (\theta_2(0,\tau)\theta_3(0,\tau)\theta_4(0,\tau))^8.$$

This algebraic-analytic relation between discriminants and theta functions is known but the above approach is new. This approach might be possible to apply to general plane curves.

Similar formulae for other genus one models are obtained by Theorem 5.3.1. To be precise, let C_ϕ be a smooth curve of genus one over $\mathbb{C}$ defined by a model ϕ of degree n ($n = 2, 3, 4$) with the corresponding Weierstrass form E_ϕ defined by $\varphi_n(\phi)$. The Weierstrass parametrization provides a lattice Λ such that $E_\phi(\mathbb{C}) \cong \mathbb{C}/\Lambda$. We write $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with some complex numbers ω_1, ω_2 satisfying $\mathrm{Im}(\omega_2/\omega_1) > 0$. The following is a consequence of Theorem 5.3.1:

Corollary 5.3.5. *Let* C_ϕ *be a smooth curve of genus one over* $\mathbb{C}$ *defined by a model* ϕ *of degree* n ($n = 2, 3, 4$) *and let* Δ_ϕ *be the discriminant of* C_ϕ. *We have*

$$\Delta_\phi = 2^{16}\alpha_n^{12} \left(\frac{\pi}{\omega_1}\right)^{12} (\theta_2(0,\tau)\theta_3(0,\tau)\theta_4(0,\tau))^8,$$

where $\alpha_2 = 1, \alpha_3 = 1/2$ *and* $\alpha_4 = 2$.

In the case $n = 3$, this result is slightly different from Theorem 5.3.4 since we are

using the explicit map φ_3 to send a cubic to a Weierstrass form instead of the linear transformation M.

Bibliography

[1] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum and A. R. Perlis, *Jacobians of genus one curves*, J. Number Theory **90**, 2001, no. 2, 304-315.

[2] M. Artin, F. Rodriguez-Villegas, J. Tate, *On the Jacobians of plane cubics*, Adv. Math. **198**, 2005, 366-382.

[3] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44**, 1977, no.4, 715-743.

[4] J. A. Ball, V. Vinnikov, *Zero-pole interpolation for matrix meromorphic functions on a compact Riemann surface and a matrix Fay trisecant identity*, Amer. J. Math. **121**, 1999, 841-888.

[5] A. Beauville, *Determinantal hypersurfaces*, Michigan Math. Journal **48**, 2000, 39-64.

[6] J. Cremona, T. Fisher, M. Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory **4**, No. 6, 2010, 763-820.

[7] J. Cremona, *G1CRPC: Rational points on curves*, Section 4.4, 29-31, `https://www.cise.ufl.edu/research/SpaceTimeUncertainty/Spatial3D/crem03.pdf`.

[8] S. David, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory **64**, no. 1, 1997, 104-129.

[9] P. Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, 53-73.

[10] L. E. Dickson, *Determination of all homogeneous polynomials expressible as determinants with linear elements*, Trans. Amer. Math. Soc., **22**, 1921, 167-179.

[11] J. Dixmier, *On the projective invariants of quartic plane curves*, Advances in Mathematics **64**, 1987, 279-304.

[12] J. Ellenberg and A. Venkatesh, *On uniform bounds for rational points on nonrational curves*, Int. Math. Res. Not. **35**, 2005, 2163-2181.

[13] T. Fisher, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. **97**, no. 3, 2008, 753-782.

[14] T. Fisher, *A formula for the Jacobian of a genus one curve of arbitrary degree*, Algebra Number Theory **12**, no. 9, 2018, 2123-2150.

[15] T. Fisher, *Genus one curves defined by Pfaffians*, `https://www.dpmms.cam.ac.uk/~taf1000/`, Preprint.

[16] I. M. Gelfand, M. M. Kapranov, A. V. Zelevinsky *Discriminants, resultants, and multidimensional determinants*, Mathematics: Theory and Applications. Birkhauser Boston Inc., 1994.

[17] P. Gordan, *Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coeffizienten einer endlichen Anzahl solcher Formen ist*, J. Reine. Angew. Math. **69**, 1868, 323-354.

[18] J. Guàrdia, *On the Torelli problem and jacobian nullwerte in genus three*, Michigan Math. Journal **60**, no. 1, 2011, 51-65.

[19] D. R. Heath-Brown, *The density of rational points on curves and surfaces*, Ann. of Math. (2) **155**, 2002, 553-595.

[20] D. R. Heath-Brown, D. Testa, *Counting rational points on cubic curves*, Sci. China Math., **53**, 2010, No. 9, 2259-2268.

[21] N. M. Katz, *p-adic properties of modular schemes and modular forms*, Lecture Notes in Mathematics, **350**, Springer, Berlin, 1973.

[22] F. Klein, *Zur theorie der abelschen funktionen*, Math. Annalen **36**, 1889-90, 1-83.

[23] G. Lachaud, C. Ritzenthaler, A. Zykin, *Jacobians among abelian threefolds: a formula of Klein and a question of Serre*, Math. Res. Lett. **17** (2), 2010, 323-333.

[24] P. Salberger, *Counting rational points on projective varieties*, preprint.

[25] F. D. Piazza, A. Fiorentino, R. Salvati Manni, *Plane quartics: the universal matrix of bitangents*, Israel J. Math. **217**, 2017, 111-138.

[26] G. Salmon, *A treatise on the higher plane curves*, Hodges, Foster and Figgis, Dublin, 1979.

[27] J. P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[28] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[29] M. H. Tran, *Counting rational points on smooth cubic curves*, Journal of Number Theory, **189**, 2018, 138-146.

[30] M. H. Tran, *Uniform bounds for rational points on comple intersections of two quadric surfaces*, Acta Arithmetica, **186**, 2018, 301-318.

[31] M. H. Tran, *Invariants of models of genus one curves via modular forms and determinantal representations*, preprint, arXiv:1911.01350.

[32] V. Vinnikov, *Complete description of determinantal representations of smooth irreducible curves*, Linear Algebra Appl., **125**, 1989, 103-140.

[33] M. N. Walsh, *Bounded rational points on curves*, Int. Math. Re. Notices **14**, 2015, 5644-5658.

[34] Z. X. Wang, D. R. Guo, *Special Functions*, World Scientific Publishing, Teaneck, NJ, 1989.

[35] A. Weil, *Remarques sur un mémoire d'Hermite*, Arch. Math. **5**, 1954, 197-202.