On the density of parameterizations of generalized Fermat equations of signature (2,3,3) that produce locally primitive solutions

by

Sepehr Yadegarzadeh

B.Sc., University of Tehran, 2016

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty Science

SIMON FRASER UNIVERSITY
Summer 2019

Approval

Name:	**Sepehr Yadegarzadeh**
Degree:	**Master of Science (Mathematics)**
Title:	**On the density of parameterizations of generalized Fermat equations of signature (2,3,3) that produce locally primitive solutions**
Examining Committee:	**Chair:** Amarpreet Rattan Associate Professor
	Nils Bruin Senior Supervisor Professor
	Imin Chen Supervisor Associate Professor
	Stephen Choi Internal Examiner Professor
Date Defended:	**May 15, 2019**

Abstract

We consider the equations

$$Ax^2 + By^3 = Cz^3,$$

where A, B, C are square-free and pairwise co-prime integers. A solution (x, y, z) is called primitive if it consists of co-prime integers. Adapting earlier work for the equations

$$x^2 + y^3 = Cz^3,$$

we show that primitive solutions give rise to integer Klein forms of degree four, with discriminant A^3B^2C. Whether Klein forms come from primitive solutions is determined by local conditions. We show that for primes p dividing B, there are exactly four $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalence classes of Klein forms that are relevant, and that exactly half of those classes come from $\mathbb{Z}_p$-primitive solutions.

We also show that if we set $A = 1$, then further restricting B, C to square-free and co-prime integers leaves us with an asymptotically positive proportion of triples.

Keywords: Fermat equations ; Klein forms

Acknowledgements

I would like to express my heartfelt gratitude to my supervisor Nils Bruin. His unending patience and kindness helped me tremendously throughout my studies. It was a great honor to work with him. I would like to thank my dear friends Akbar and Jasem who helped me whenever I needed help. Finally, I thank my family for their support and encouragement.

Table of Contents

Chapter 1

Introduction

Coined by French mathematicians in 17th century the term *Diophantine equations* refers to equations, or systems of equations with rational coefficients, the solutions of which are sought for in integers or rational numbers. The term refers to Diophantus of Alexandria, an Alexandrian mathematician of third century AD. He was the author of a series of books called Arithmetica, in which he dealt with solving algebraic equations.

An important example of the study of Diophantine equations was Pierre de Fermat's discovery in number theory. Around 1637, Fermat wrote what is now known as *Fermat's last therorem* in the margin of his copy of Arithmetica, claiming that he has found a "truly marvelous" (demonstrationem mirabilem) proof for it. The theorem states that the equation $x^n + y^n = z^n$ has no positive integer solutions, when $n > 2$.

It took mathematics a very long time to see a proof of this statement. In 1994, Wiles and Taylor finally finished and corrected Wiles' initial proof of Fermat's last theorem, which heavily uses modern techniques.

Wiles' proof gave a fresh impetus to this area of mathematical research and *generalized Fermat equations* became the focus of serious study. This thesis belongs to this area of research. We study the forms that generate the primitive (pairwise co-prime) solutions to the equation

$$x^2 + By^3 = Cz^3,$$

where $B, C \in \mathbb{Z}$. We also insist that B, C are square-free and co-prime.

In this chapter we introduce the *generalized Fermat equations*, and give a quick survey of what is known about them.

1.1 The generalized Fermat equation

A *generalized Fermat equation* is a ternary equation of the form

$$Ax^p + By^q = Cz^r \tag{1.1}$$

where $p, q, r \in \mathbb{Z}_{\geq 2}$ and $A, B, C \in \mathbb{Z}_{\neq 0}$. We define the *signature* of (1.1) to be the triple (p, q, r). We say a solution $(x, y, z) \in \mathbb{Z}^3$ is *primitive* if it satisfies $\gcd(x, y, z) = 1$. Non-primitive solutions are often easily constructed. For example, from $a + b = c$, by multiplication by $a^{33}b^{44}c^{54}$ we get

$$(a^{17}b^{22}c^{27})^2 + (a^{11}b^{15}c^{18})^3 = (a^3b^4c^5)^{11}$$

which produces infinitely many non-primitive solutions to $x^2 + y^3 = z^{11}$. For this equation it is conjectured that no non-trivial primitive solutions exist. This example is mentioned in [5].

The main characteristics of equation (1.1) are governed by the value of

$$\chi = 1/p + 1/q + 1/r.$$

We call this constant the *Euler characteristic* of equation (1.1).

It happens that we can very aptly classify the behaviour of equation (1.1) by the value of the characteristic. Depending on the value of its characteristic, we have the following three cases.

1.1.1 Hyperbolic Case: $\chi < 1$

There is no method known for solving these equations for arbitrary (p, q, r). It seems that we are currently very far from any satisfactory result in this case. For a survey of the numerous partial results in this case look at Beukers' article [2]. The following conjecture due to Tijdeman and Zagier, belongs to this case.

Conjecture 1.1 (Tijdeman-Zagier)**.** If $x^p + y^q = z^r$, where p, q, r, x, y and z are positive integers and p, q, r are all greater than 2, then x, y, z must have a common prime factor.

Number theory enthusiast and banker Andrew Beal initially offered $5000 for a correct proof. The prize value has been increased several times, and at the time of writing is US$1,000,000. This conjecture is now known as the *Beal prize problem.*

In 1995, Darmon and Granville used Faltings' theorem to prove the following important theorem.

Theorem 1.2 (Darmon and Granville (1995))**.** *Let $A, B, C \in \mathbb{Z}_{\neq 0}$ and $p, q, r \in \mathbb{Z}_{\geq 2}$ such that $\chi < 1$. The equation $Ax^p + By^q = Cz^r$ has only finitely many co-prime integer solutions.*

1.1.2 Euclidean Case: $\chi = 1$

The only possible signatures are $(2, 3, 6), (3, 3, 3)$ and $(2, 4, 4)$. In this case, primitive solutions correspond to rational points on a finite set of genus 1 curves. The corresponding curves determine whether the equation has zero, finite or infinitely many solutions.

1.1.3 Spherical Case: $\chi > 1$

In this case the possible signatures are $(2,3,3),(2,3,4),(2,3,5)$ or $(2,2,m)$ where $m \geq 2$. Here, the equation possibly has infinitely many solutions. Frits Beukers investigated this in [1].

Theorem 1.3 (Beukers (1998)). *Assume $A,B,C \in \mathbb{Z}$ with $ABC \neq 0$, and $p,q,r \in \mathbb{Z}_{\geq 2}$. If $\chi > 1$ then the equation $Ax^p + By^q = Cz^r$ has either zero or infinitely many solutions (x,y,z) in $\mathbb{Z}$ with $\gcd(x,y,z) = 1$ and $Ax^p + By^q = Cz^r$. Furthermore, there is a finite set of triples of binary forms $(X,Y,Z) \in \mathbb{Q}[s,t]$ such that every primitive integral solution (x,y,z), can be obtained by specializing one of these triples, that is for one of these triples (X,Y,Z), there exist $s,t \in \mathbb{Q}$ such that $x = X(s,t), y = Y(s,t)$ and $z = Z(s,t)$.*

Beukers shows that we can take $Z(s,t)$ in the above theorem to be a *Klein form* of degree $4,6,12$ for $p = 2,\ q = 3$, and $r = 3,4,5$ respectively, and that the corresponding $X(s,t)$ and $Y(s,t)$ can be derived from $Z(s,t)$ (see Section 4.1).

For an elementary example of this result consider the Pythagorean equation

$$X^2 + Y^2 = Z^2.$$

This equation has infinitely many solutions and every solution is the integral specialization of one the following 4 parameterizations

$$(s^2 - t^2)^2 + (2st)^2 = \pm(s^2 + t^2)^2$$
$$(2st)^2 + (s^2 - t^2)^2 = \pm(s^2 + t^2)^2.$$

Beukers' result does not provide a practical method for actually calculating parameterizations. This was done by Edwards in [5]. Before a quick review of Edwards' results, we mention two other known instances of spherical equations.

The equation $x^2 + y^3 = z^3$ with $\gcd(x,y,z) = 1$, was solved by Mordell in his 1969 book Diophantine equations [10].

The equation $x^2 + y^3 = \pm z^4$ with $\gcd(x,y,z) = 1$, was solved by Zagier and the results are mentioned in Beukers' survery article [2].

1.2 Edwards' method

Edwards developed a unified new approach to solve the equations of the type $x^2 + y^3 = dz^r$, where d is an integer and $r \in \{3,4,5\}$. His method solved the hitherto unsolved equation $x^2 + y^3 = z^5$. Edwards' result has its roots in Mordell's method of solving the equation $x^2 + y^3 = z^3$.

Edwards ([5]) proves that a primitive solution to $x^2 + y^3 = z^r$ (with $r = 3,4,5$) can be obtained from a Klein form of given discriminant and with *integer* coefficients. We

adapt that theorem to apply to $x^2 + By^3 = Cz^3$, with B, C square-free and co-prime (see Theorem 5.3).

Furthermore, he uses Hermite reduction theory [5, Theorem 11.1.5.] to show that Klein forms with integer coefficients and bounded discriminant have a *reduced* representative with coefficients bounded by an explicit function of the discriminant. That means there are only *finitely many* $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of Klein forms of bounded discriminant.

1.3 Results in this Thesis

In this thesis we consider the generalized Fermat equation

$$x^2 + By^3 = Cz^3, \tag{1.2}$$

with $B, C \in \mathbb{Z}$. We also insist that B, C are square-free and co-prime.

Definition 1.4. A solution $(x, y, z) \in \mathbb{Z}^3$ to the equation

$$x^2 + By^3 = Cz^3,$$

is called *primitive* if $\gcd(x, y, z) = 1$.

Proposition 1.5. *If B and C are square-free and co-prime integer, then a primitive solution (x, y, z) to the equation*

$$x^2 + By^3 = Cz^3,$$

satisfies

$$\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1.$$

Proof. If $p \mid \gcd(x, y)$, then $p^2 \mid Cz$. Since C is square-free it follows that $p \mid z$, which contradicts $\gcd(x, y, z) = 1$. If $p \mid \gcd(y, z)$ or $p \mid \gcd(x, z)$ we obtain contradictions in a similar way, hence

$$\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1.$$

□

As we show in Section 7, the restriction that B, C are square-free and co-prime leaves us with a positive asymptotic proportion of all equations. We are ultimately motivated by describing how often spherical generalized Fermat equations (particularly those of signature $(2, 3, 3)$) admit primitive solutions. A concrete way of formulating this question is by considering

$$V(M) = \{(B, C) \in \mathbb{Z} : BC \neq 0 \text{ and } \max(|B|, |C|) \leq M\},$$

and

$$W(M) = \{(B, C) \in V(M) : x^2 + By^3 = Cz^3 \text{ admits a primitive solution}\}.$$

Question 1.6. Determine the values of

$$\limsup_{M\to\infty} \frac{W(M)}{V(M)} \text{ and } \liminf_{M\to\infty} \frac{W(M)}{V(M)}.$$

Ryan McMahon [9] provides numerical evidence that these values agree and take a value strictly below 1, i.e., that a positive proportion of generalized Fermat equations of signature $(2,3,3)$ does not admit primitive solutions.

In Lemma 6.3 we show that an integral Klein form produces primitive solutions if and only if it produces $\mathbb{Z}_p$-primitive solutions for all primes p. The main contribution in this thesis consists of the following two theorems. It establishes the first systematic description of (some of the) local conditions on Klein forms that produce primitive solutions locally.

A motivation for our results is the following observation. If (x,y,z) is a solution to the equation

$$x^2 + By^3 = Cz^3, \tag{1.3}$$

then (Bx, By, z) is a solution to the equation

$$x'^2 + y'^3 = B^2Cz'^3. \tag{1.4}$$

Solutions to (1.4) are obtained from Klein forms of discriminant B^2C (see [5], Theorem 6.1.1). We look at the forms that parameterize (1.4) and investigate which of them produce primitive solutions for (1.3).

Theorem 1.7. *Let $p > 3$ be a prime and suppose that $f \in \mathbb{Z}_p[s,t]$ is a Klein form of degree 4, and discriminant p^2d, with $d \in \mathbb{Z}_p^\times$. Let $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, c, p, cp\}$, where c is a non-square p-adic unit. Then f is $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalent to one of the following four forms*

f_1	$t(s^3 - p^2dt^3)$
f_2	$t(cs^3 - (p^2d/c^2)t^3)$
f_3	$t(ps^3 - dt^3)$
f_4	$t(pcs^3 - (d/c^2)t^3)$

Theorem 1.8. *Each of the f_i's above induces a parameterization for an equation*

$$x^2 + By^3 + Cz^3 = 0,$$

with $B^2C = p^2d$, with B, C co-prime and square-free and $p \mid B$, but only f_3, f_4 produce $\mathbb{Z}_p$-primitive solutions.

Chapter 2

First Definitions

Let $\mathbb{Z}$ denote the ring of rational integers and let p be a prime. We write $\mathbb{Z}_p$ for the p-adic completion of $\mathbb{Z}$, and write $\mathbb{Q}_p$ for its field of fractions. We write

$$v_p \colon \mathbb{Q}_p^* \to \mathbb{Z}$$

for the associated discrete valuation.

2.1 Definitions

Definition 2.1 ($\mathbb{Z}$-primitive and $\mathbb{Z}_p$-primitive solutions)**.** Let p be a prime. We denote the set of $\mathbb{Z}$-primitive solutions by

$$\mathcal{D}(B,C) = \{(x,y,z) \in \mathbb{Z}^3 \colon x^2 + By^3 = Cz^3 \text{ and } \gcd(x,y,z) = 1\},$$

and the set of $\mathbb{Z}_p$-primitive solutions by

$$\mathcal{D}_p(B,C) = \{(x,y,z) \in \mathbb{Z}_p^3 \colon x^2 + By^3 = Cz^3 \text{ and } \min\{v_p(x), v_p(y), v_p(z)\} = 0\}.$$

When the context allows we simply write these sets as $\mathcal{D}$ and $\mathcal{D}_p$. When $B = 1$ we write $\mathcal{D}(C)$ for $\mathcal{D}(1,C)$.

Definition 2.2. (Action of $\mathrm{GL}_2(K)$). Let K be a ring, and $g(x,y) \in K[x,y]$. The group $\mathrm{GL}_2(K)$ acts on g in the following way:

$$g(x,y) \mapsto g^M(x,y) = g\left(M \begin{pmatrix} x \\ y \end{pmatrix}\right) = g(ax+by, cx+dy)$$

where

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K).$$

We also consider the action of $\mathrm{GL}_2(K) \times \mathrm{GL}_1(K)$ on $K[x, y]$ by letting the pair (M, λ) with $M \in \mathrm{GL}_2$, and $\lambda \in \mathrm{GL}_1$ act via the mapping

$$g(x, y) \mapsto \lambda^2 g^M(x, y).$$

Definition 2.3 (Proper Equivalence)**.** Two forms $g_1, g_2 \in K[x, y]$ are called *properly equivalent* if there is a pair (M, λ) with $M \in \mathrm{GL}_2(K)$, and $\lambda \in \mathrm{GL}_1(K)$, such that $g_1 = \lambda^2 g_2^M$.

The reason for insisting that the scalar be a square will become clear later.

Chapter 3

Invariant Theory

In this chapter we introduce basic concepts from classical invariant theory. The original reference is an account of the lectures given by Hilbert in 1897 in Göttingen [7], which is still very readable. For a more modern exposition see [12].

3.1 Definitions

We restrict ourselves to a field K of characteristic zero. We start by defining a binary form f of degree k:

$$f = a_0x^k + a_1x^{k-1}y + a_2^{k-1}y^2 + \cdots + a_ky^k.$$

We define the degree of a binary form to be its degree in x, y. We usually represent f by $[a_0, \cdots, a_k]$.

Definition 3.1 (Covariant)**.** Let $f = [a_0, \cdots, a_k]$ be a binary form of degree k. A *covariant of f of order w* is a binary form $C(f) \in K[a_0, \cdots, a_k][x, y]$ which is separately homogeneous in both x, y and $a_0, \cdots, a_k$, satisfying the following identity:

$$C(f)^M = \det(M)^w C(f^M)$$

for all $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(K)$.

Definition 3.2 (Invariant)**.** Let $f = [a_0, \cdots, a_k]$ be a binary form of degree k. An *invariant of f of order w* is a homogeneous polynomial $I(f)$, in the variables $a_0, \cdots, a_k$, satisfying

$$I(f^M) = \det(M)^w I(f)$$

for all $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(K)$.

3.2 Basic Properties

Here we introduce two covariants associated with a binary form $f = [a_0, \cdots, a_k][x, y] \in K[a_0, \cdots, a_k]$ of degree k, namely the *Hessian* and *Jacobian* covariants

$$\mathbf{H}(f) := \Big(\frac{1}{k(k-1)}\Big)^2 \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix}, \quad \mathbf{t}(f) := \frac{1}{k(k-2)} \begin{vmatrix} f_x & f_y \\ \mathbf{H}_x & \mathbf{H}_y \end{vmatrix}.$$

It can be verified that $\mathbf{H}$ and $\mathbf{t}$ are covariants of weights 2 and 3 respectively.

Definition 3.3. (Differential Operators for Invariant Theory). Let x', y' be variables. We define

$$\begin{aligned} D &:= a_1 \frac{\partial}{\partial a_1} + 2a_1 \frac{\partial}{\partial a_2} + \cdots + k a_{k-1} \frac{\partial}{\partial a_k}, \\ \Delta &:= k a_1 \frac{\partial}{\partial a_0} + (k-1) a_2 \frac{\partial}{\partial a_1} + \cdots + a_k \frac{\partial}{\partial a_{k-1}}, \\ \Omega &:= \frac{\partial^2}{\partial x \partial y'} - \frac{\partial^2}{\partial x' \partial y}. \end{aligned}$$

Definition 3.4. (Isobaric Property). A polynomial $C \in K[a_0, \cdots, a_k][x, y]$ is called *isobaric of weight* w, if each term of C has the same weight w, when the coefficient a_i is given the weight i, for $i \in \{0, \cdots, k\}$.

We introduce the transvectant mechanism to construct new covariants from the existing ones.

Definition 3.5. (Transvectant). Let $C_1, C_2 \in K[a_0, \cdots, a_k][x, y]$. We define the *i-th transvectant* by

$$(C_1, C_2)_i := \left(\left(\frac{(k-i)!}{k!} \right)^2 \Omega^i C_1(x, y) C_2(x', y') \right) \Big|_{(x', y') = (x, y)}.$$

If C_1, C_2 are covariants of a base form f, where f is a binary form of degree k, then (C_1, C_2) is also a covariant of the base form f. We introduce a sequence of transvectants that are of special interest to us,

$$\tau_{2m}(f) := \frac{1}{2}(f, f)_{2m}, \quad \tau_{2m+1}(f) := \frac{k}{k-2}(f, \tau_{2m}(f))_1.$$

Lemma 3.6. *The* $\mathbf{H}$*, and* $\mathbf{t}$ *defined above are* τ_2*, and* τ_3 *respectively.*

Proof. We have

$$\begin{aligned}\tau_2(f) = \frac{1}{2}\big(f,f\big)_2 &= \frac{1}{2}\Big(\frac{(k-2)!}{k!}\Big)^2\Omega^2\Big(f(x,y),f(x',y')\Big)\Big|_{(x,y)=(x',y')}\\ &= \frac{1}{2}\Big(\frac{1}{k(k-1)}\Big)^2\Big(\frac{2\partial^4}{\partial^2 x\partial^2 y'}(f(x,y)f(x',y'))\\ &\qquad - 2\frac{\partial^4}{\partial x'\partial y\partial y'\partial x}(f(x,y)f(x',y'))\Big)\Big|_{(x,y)=(x',y')}\\ &= \Big(\frac{1}{k(k-1)}\Big)^2\Big(f_{xx}f_{yy}-f_{xy}^2\Big) = \mathbf{H}(f),\end{aligned}$$

and

$$\begin{aligned}\tau_3(f) = \Big(f,\mathbf{H}(f)\Big)_1 &= \Big(\frac{k}{k-2}\Big)\Big(\frac{(k-1)!}{k!}\Big)^2\Omega\Big(f(x,y),\mathbf{H}(f)(x',y')\Big)\Big|_{(x,y)=(x',y')}\\ &= \frac{1}{k(k-2)}\Big(\frac{\partial}{\partial x}f(x,y)\frac{\partial}{\partial y'}\mathbf{H}(f)(x',y')\\ &\qquad - \frac{\partial}{\partial y}f(x,y)\frac{\partial}{\partial x'}\mathbf{H}(f)(x',y')\Big)\Big|_{(x,y)=(x',y')}\\ &= \frac{1}{k(k-2)}\Big(f_x\mathbf{H}(f)_y - f_y\mathbf{H}(f)_x\Big) = \mathbf{t}(f).\end{aligned}$$

□

Definition 3.7. (I and J invariants for quartics). Let $f=[a_0,a_1,a_2,a_3,a_4]$ be a quartic binary form, i.e. a binary form of degree 4. We define two basic invariants for quartics:

$$I = 12a_0a_4 - 3a_1a_3 + a_2^2$$

of degree 2 and isobaric weight 4, and

$$J = 72a_0a_2a_4 + 9a_1a_2a_3 - 27a_0a_3^2 - 27a_4a_1^2 - 2a_2^2$$

of degree 3 and isobaric weight 6. The invariant J is known as the *catalecticant* of f.

We mention a result from classical invariant theory.

Proposition 3.8 ([12], page 40)**.** *The degree n invariants of a binary quartic form, form a vector space whose basis consists of the monomials I^rJ^s where $r,s\geq 0$ and $2r+3s=n$.*

In particular, I and J are algebraically independent. The discriminant of a quartic Δ has degree 6 and weight 12, and therefore it must be a linear combination of I^3 and J^2;

$$27\Delta = 4I^3 - J^2 \tag{3.1}$$

Chapter 4

Klein forms

Here we introduce Klein forms and their basic properties. In later chapters we will explain the central role they play in studying the Diophantine equations of our interest.

4.1 Definitions

In [8] Klein inscribes the tetrahedron, octahedron, and icosahedron in the sphere, and projects it into the extended complex plane. After suitable rotation of the sphere and homogenization we get the following forms whose roots are the vertices of the corresponding solids.

As in [5], to each $r \in \{3, 4, 5\}$ we associate a solid: the tetrahedron, the octahedron, and the icosahedron, respectively. We denote the order of the group of rotational symmetries of the corresponding solid by N.

Throughout this chapter K will be an arbitrary field, with $\mathrm{char}(K) \neq 2, 3, 5$.

Definition 4.1. In the following tables we fix some notations. We define three polynomials that define the vertices of the corresponding solid. Let N denote the order of the group of rotational symmetries of the corresponding solid.

r	Solid	Form	d	N
3	Tetrahedron	$F_3 = 4y(x^3 + y^3)$	-1	12
4	Octahedron	$F_4 = 36xy(x^4 + y^4)$	-3	24
5	Icosahedron	$F_5 = 1728xy(x^{10} - 11x^5y^5 - y^{10})$	1	60

r	$\mathbf{H}(F_r)$
3	$-x^4 + 8xy^3$
4	$-36x^8 + 504x^4y^4 - 36y^8$
5	$-20736x^{20} - 4727808x^{15}y^5 - 10243584x^{10}y^{10} + 4727808x^5y^{15} - 20736t^{20}$

r	$\mathbf{t}(F_r)/2$
3	$x^6 + 20x^3y^3 - 8y^6$
4	$216x^{12} + 7128x^8y^4 - 7128x^4y^8 - 216y^{12}$
5	$2985984x^{30} - 1558683648x^{25}y^5 - 29874769920x^{20}y^{10} - 29874769920x^{10}y^{20}$ $+1558683648x^5y^{25} + 2985984y^{30}$

We have the following equation, which shows the arithmetic relevance of covariants

$$\Big(\frac{1}{2}\mathbf{t}(F_r)\Big)^2 + \mathbf{H}(F_r)^3 + dF_r^r = 0, \tag{4.1}$$

where $r, F_r, \mathbf{H}(F_r), \mathbf{t}(F_r), d$ are stated in the above tables.

Proposition 4.2. *Let $f \in K[a_0, \cdots, a_k][x, y]$ be a form of total degree n in variables x, y. Assume f satisfies*

$$\Big(\frac{1}{2}\mathbf{t}(f)\Big)^2 + \mathbf{H}(f)^3 + df^r = 0 \tag{4.2}$$

for some $d \in K^*$, and $r \in \{3, 4, 5\}$. Let $g = \lambda f^M$ where $\lambda \in K^*$ and $M \in \mathrm{GL}_2(K)$. Then

$$\Big(\frac{1}{2}\mathbf{t}(g)\Big)^2 + \mathbf{H}(g)^3 + d'g^r = 0$$

where $d' = \lambda^{6-r} \det(M)^{-6} d$.

Proof. Note that $\mathbf{t}$ and $\mathbf{H}$ are covariants of weight 3 and 2. Hence $\mathbf{t}^2$ and $\mathbf{H}^3$ are covariants of weight 6, and both are invariants of order $6 - r$ in the a_i, the result follows. □

Definition 4.3. (Klein Forms). We define $\mathcal{C}(r)$ to be the set of all forms $f \in K[a_0, \cdots, a_k][x, y]$ where $f = F_r \circ M$ for $r \in \{3, 4, 5\}$, and $M \in \mathrm{GL}_2(\bar{K})$. A form in $\mathcal{C}(r)$ is called a *Klein form*. Let f be Klein form satisfying $(\frac{\mathbf{t}(f)^2}{2}) + \mathbf{H}(f)^3 + df^r = 0$, we say that d is the *Klein form discriminant* of f. We denote all such Klein forms with $\mathcal{C}_r(d)(K)$,

$$\mathcal{C}_r(d)(K) = \Big\{ f \in \mathcal{C}(r)(K) \quad | \quad \Big(\frac{1}{2}\mathbf{t}(f)\Big)^2 + \mathbf{H}(f)^3 + df^r = 0 \Big\}.$$

4.2 Classification of Klein forms

Via a classical theorem of Gordon, we can get an equivalent definition of a Klein form, which is of great help to us.

Theorem 4.4 ([6],page 204)**.** *Let K be a field and k an integer greater that 3. Suppose that one of the following is true.*

- *char(K) = 0*
- *$k = 4, 6$ or 12; and $char(K) > k - 4$.*

- $char(K) \geq k^2$.

Then the fourth transvectant $\tau_4(f)$ of a form f of order k, is identically zero if and only if $f = F_r \circ M$ where $M \in \mathrm{GL}_2(\overline{K})$.

Now we can completely classify $\mathcal{C}_r(d)$.

Theorem 4.5 ([5], Classification of quartic Klein forms)**.** *Suppose $N, d \in \bar{K}^*$. If $char(K) = 0$, then*

$$\begin{aligned}
&\mathcal{C}_3(d)(\bar{K}) = \{f \in \bar{K}[x,y]_4 \quad | \quad \tau_4(f) = 0, \quad J(f) = 2^6 3^3 d\},\\
&\mathcal{C}_4(d)(\bar{K}) = \{f \in \bar{K}[x,y]_6 \quad | \quad \tau_4(f) = 0, \quad \tau_6(f) = -72d\},\\
&\mathcal{C}_5(d)(\bar{K}) = \{f \in \bar{K}[x,y]_{12} \quad | \quad \tau_4(f) = 0, \quad 7\tau_6(f) = -360d, \quad 7\tau_{12}(f) = 3110400d^2\}.
\end{aligned}$$

This theorem basically shows that a quartic form f is a Klein form if and only if $\tau_4(f)$ vanishes. Now we take a close look at the 4-th transvectant of a form of degree 4. Writing,

$$f = [a_0, a_1, \cdots, a_4] \in K[a_0, a_1, \cdots, a_4][x, y],$$

we see that

$$12\tau_4(f) = 12a_0a_4 - 3a_1a_3 + a_2^2 = I(f).$$

Hence f is a quartic Klein form if and only if $I(f) = 0$. We recall from last chapter the following identity:

$$27\Delta = 4I^3 - J^2$$

Hence according to Theorem 4.5 for a quartic Klein form $f \in \mathcal{C}_r(d)$ we have:

$$\Delta(f) = -2^6 d^2. \tag{4.3}$$

Remark 4.6. Here we defined the Klein forms using the associated invariants I and J. Since this is likely to be confused with the invariant of the associated elliptic curve, from now on instead of the J-invariant of a Klein form f, we stick to the more convenient Klein form discriminant $d(f)$, satisfying $J(f) = 2^6 3^3 d$.

Chapter 5

Properties of Parameterizations

So far we have obtained a classification of Klein forms of fixed discriminant. Let $(x, y, z) \in \mathbb{Z}^3$ satisfy the equation

$$x^2 + y^3 = dz^3.$$

We want to find a Klein form f such that $\Big(\frac{1}{2}\mathbf{t}(f)(s,t), \mathbf{H}(f)(s,t), f(s,t)\Big) = (x, y, z)$ for some $s, t \in \mathbb{Z}$. This motivates our next definition.

Definition 5.1. (Parameterization $\eta(f)$). For $f \in C_r(d)(\mathbb{Q})$ we define

$$\eta(f) = \Big(\frac{1}{2}\mathbf{t}(f), \mathbf{H}(f), f\Big).$$

Note that from Equation (4.1) and Proposition 4.2 it follows that $\eta(f) \in \mathcal{C}_r(d)(\mathbb{Q})$.

Any $f \in \mathcal{C}_3(d)$ induces a parameterization $\eta(f)$, and we get the following map

$$\begin{aligned} \pi \colon \mathcal{C}_3(d) &\to \mathcal{D}(d) \\ f &\mapsto \Big(\frac{1}{2}\mathbf{t}(f)(1,0), \mathbf{H}(f)(1,0), f(1,0)\Big). \end{aligned}$$

We start by proving some nice properties of parameterizations.

In this chapter R is a domain and K is its field of fractions. We assume K is of zero characteristic.

Proposition 5.2 ([5], Proposition 5.2.5)**.** *Suppose $d \in K^*$. If $(x, y, z) \in K^3 \setminus (0, 0, 0)$, satisfies the equation*

$$x^2 + y^3 = dz^3,$$

then there is a $\phi \in \mathcal{C}_3(d)(K)$ with $\pi(\phi) = (x, y, z)$. It is given by

$$\phi = \begin{cases} [z, 0, \frac{6y}{z}, \frac{8x}{z^2}, \frac{-3y^2}{z^3}] & \text{if } z \neq 0 \\ [0, \frac{-x}{y}, 0, 0, \frac{-2^6 y^2 d}{x^2}] & \text{if } z = 0 \end{cases}$$

Proof. Direct calculation gives the result. □

Theorem 5.3. *Let A, B, C be square-free integers, such that*

$$\gcd(A, B) = \gcd(A, C) = \gcd(B, C) = 1.$$

If $x, y, z \in \mathbb{Z}$ satisfy

$$Ax^2 + By^3 = Cz^3,$$

and $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$, then there exists a Klein form $f \in \mathcal{C}_3(CA^3B^2)(\mathbb{Z})$ such that

$$\Big(\frac{\boldsymbol{t}(1,0)}{2A^2B}, \frac{\boldsymbol{H}(f)(1,0)}{AB}, f(1,0)\Big) = (x, y, z).$$

Proof. We observe that (A^2Bx, ABy, z) is a solution for the equation

$$x'^2 + y'^3 = CA^3B^2z'^3.$$

Proposition 5.2 gives us $f \in \mathcal{C}_3(d)(\mathbb{Q})$ with $\pi(f) = (A^2Bx, ABy, z)$. First we consider the case $z = 0$. Since $Ax^2 + By^3 = 0$, and $\gcd(x, y) = 1$, the fact that A and B are square-free implies that $x, y \in \mathbb{Z}^*$, and hence $\frac{x}{y} \in \mathbb{Z}^*$. Thus we have

$$f = [0, \frac{-x}{y}, 0, 0, \frac{-2^6y^2d}{x^2}] \in \mathcal{C}_3(CA^3B^2)(\mathbb{Z}).$$

Now we consider the case where $z \neq 0$. The existence of $f \in \mathcal{C}_3(CA^3B^2)(\mathbb{Q})$ is guaranteed by Proposition 5.2. Let $f = [a_0, a_1, \cdots, a_4]$. Since $\pi(f) = (A^2Bx, ABy, z)$ we have

$$\begin{aligned} z &= a_0, \\ ABy &= (8a_0a_2 - 3a_1^2)/48, \qquad (5.1) \\ A^2Bx &= (2^3a_0^2a_3 - 2^2a_0a_1a_2 + a_1^3)/2^6. \qquad (5.2) \end{aligned}$$

We can act on f by a matrix $M = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix}$, with $\alpha \in \mathbb{Q}$. Since $\det(M) = 1$, we have $\pi(f^M) = \pi(f) = (A^2Bx, ABy, z)$. By a suitable choice of α we can make sure that a_1 takes any value. We claim that $\gcd(ABy, z) = 1$. Assume $p \mid z$, and $p \mid ABy$. If $p \mid B$, then since $Ax^2 + By^3 = Cz^3$, we get that $p \mid Ax^2$, and hence $p \mid x$, which is a contradiction. Similarly, we can prove $p \nmid A$, thus we must have $p \mid y$, but this implies $p \mid x$, which contradicts the primitivity of (x, y, z). Similarly, we can prove that $\gcd(A^2Bx, z) = 1$. Hence ABy is invertible modulo z^3, and we can choose α such that $a_1 \in \mathbb{Z}$ and $a_1 = -4(A^2Bx)(ABy)^{-1} \pmod{z^3}$. Observe that since $\gcd(A^2Bx, z) = 1$, we get that $\gcd(a_1, z) = 1$. We replace f with f^M.

Now we prove that $f \in \mathcal{C}_3(CA^3B^2)(\mathbb{Z})$. Let S be the multiplicative set generated by z^3, and $\mathbb{Z}_S$ the localization of $\mathbb{Z}$ at S. Since a_0 and a_1 are in $\mathbb{Z}$, by (5.1) and (5.2) we get that $f \in \mathcal{C}_3(CA^3B^2)(\mathbb{Z}_S)$. If $z \in \mathbb{Z}^*$ there is nothing to prove, so we assume $z \notin \mathbb{Z}^*$.

We define the valuation v as follows

$$\begin{aligned} v\colon \mathbb{Z}_S &\to \mathbb{Z} \\ \alpha &\mapsto \max\{n \mid z^{-n}\alpha \in \mathbb{Z}\}. \end{aligned}$$

From (5.1) and (5.2) we get

$$\begin{aligned} a_0a_2 &= \frac{(48(ABy)+3a_1^2)}{8} = \frac{(48(ABy)+3(\frac{-4(A^2Bx)}{(ABy)})^2)}{8} = 6\Big((ABy)+\frac{(A^2Bx)^2}{(ABy)^2}\Big) \\ &= 6\frac{CA^3B^2z^3}{(ABy)^2} \pmod{z^3}, \\ a_0^2a_3 &= 2^6(A^2Bx) - 2^53(\frac{CA^2B^2z^3}{(ABy)^3}) + 2^6\frac{(A^2Bx)^3}{(ABy)^3} = -2^5\frac{CA^3B^2(A^2Bx)z^3}{(ABy)^3} \pmod{z^3}. \end{aligned}$$

Recalling $a_0 = z$, we immediately get

$$v(a_0) = 1, \quad v(a_1) = 0, \quad v(a_2) \geq 2, \quad v(a_3) \geq 1.$$

□

Chapter 6

The Equation $x^2 + By^3 = Cz^3$

In this chapter we return to our main objective, namely to understand the Klein forms that generate the co-prime integer solutions for the equation

$$x^2 + By^3 = Cz^3, \tag{6.1}$$

where B, C are non-zero, square-free and co-prime integers.

If we multiply the above equation with B^2, we get the following equation

$$(Bx)^2 + (By)^3 = B^2Cz^3. \tag{6.2}$$

If we look at the Klein forms of discriminant B^2C, we can ask the following question: when does a Klein form of discriminant B^2C produces $\mathbb{Z}$-primitive solutions for Equation (6.1)? In this chapter we answer this question by calculating the equivalence classes of Klein forms that parameterize Equation (6.2) under different notions of equivalence.

Throughout this chapter B, C are assumed to be square-free integers with $\gcd(B, C) = 1$, and $p \mid B$, where p is a prime not equal to $2, 3$. Whenever we talk about primitive solutions we refer to Equation (6.1), unless otherwise stated.

Definition 6.1. We say that a Klein form $f \in \mathbb{Q}[s, t]$ produces a primitive solution, or is $\mathbb{Z}$-productive for the equation

$$Ax^2 + By^3 + Cz^3,$$

if for some $s, t \in \mathbb{Q}$, the triple $\left(\frac{\mathbf{t}(f)(s,t)}{2A^2B}, \frac{\mathbf{H}(f)(s,t)}{AB}, f(s,t)\right)$ is a $\mathbb{Z}$-primitive solution. Similarly, we say f is $\mathbb{Z}_p$-productive, if for some $s, t \in \mathbb{Q}_p$, the triple $\left(\frac{\mathbf{t}(f)(s,t)}{2A^2B}, \frac{\mathbf{H}(f)(s,t)}{AB}, f(s,t)\right)$ is a $\mathbb{Z}_p$-primitive solution.

6.1 Local Analysis

In this section we will justify studying Equation (6.1) locally at a prime p. First we prove a lemma.

Lemma 6.2 ([9], Lemma 4.1.1)**.** *Let $X, Y, Z \in \mathbb{Q}[x, y]$ be forms of degree n that satisfy $AX^2 + BY^3 = CZ^3$. If there exist $s_p, t_p \in \mathbb{Q}_p$, such that $\Big(X(s_p, t_p), Y(s_p, t_p), Z(s_p, t_p)\Big)$ is a locally primitive solution at p, then there exists a positive integer k_p such that if $s, t \in \mathbb{Q}$ with $v_p(s - s_p) \geq k_p$ and $v_p(t - t_p) \geq k_p$ then*

$$\Big(X(s,t), Y(s,t), Z(s,t)\Big)$$

is also a locally primitive solution at p.

Proof. Let M be a non-negative integer. We write $X(s,t) = \sum_{i=1}^{n} a_i s^i t^{n-i}$. Suppose that

$$v_p(s - s_p),\ v_p(t - t_p) \geq M.$$

Hence we get that

$$\begin{aligned} s &= s_p + p^M e_s, \\ t &= t_p + p^M e_t, \end{aligned}$$

for some $e_s, e_t \in \mathbb{Q}_p$, with $v_p(e_s),\ v_p(e_t) \geq 0$. It follows that

$$v_p(s^i t^{n-i} - s_p^i t_p^{n-i}) \geq nM,$$

for all i. But then

$$\begin{aligned} v_p(X(s,t) - X(s_p, t_p)) &\geq \min\Big(v_p(a_i) + v_p(s^i t^{n-i} - s_p^i t_p^{n-i}\Big) \\ &\geq \min\{v_p(a_i)\}_i + nM \end{aligned} \tag{6.3}$$

Therefore, if $v_p(X(s_p, t_p)) = v$, and we set $M > v - \min\{v_p(a_i)\}_i/n$, then by (6.3) we get

$$v_p(X(s,t) - X(s_p, t_p)) > nv > v = v_p(X(s_p, t_p)).$$

But this means $v_p(X(s,t)) = v$. For Y and Z we get similar bounds for M. If we take k_p to be the maximum of these bounds, then the result follows. □

Theorem 6.3. *Let $X(s,t), Y(s,t), Z(s,t) \in \mathbb{Q}[s,t]$ be forms such that*

$$AX(s,t)^2 + BY(s,t)^3 = CZ(s,t)^3,$$

where A, B, C are square-free and pairwise co-prime integers. Assume that $X(s,t), Y(s,t), Z(s,t)$ do not have factors in common as polynomials. If for every p there are $s_p, t_p \in \mathbb{Q}_p$ such that $\min\{v_p(X(s_p, t_p)), v_p(Y(s_p, t_p)), v_p(Z(s_p, t_p))\} = 0$, then there exist a pair $s_0, t_0 \in \mathbb{Q}$ such

that

$$\gcd(X(s_0,t_0),Y(s_0,t_0),Z(s_0,t_0))=1.$$

Proof. If a common factor H would divides both X and Y, then it would divide CZ^2 as well and hence it would divide Z. Hence $X(s,t)$ and $Y(s,t)$ have no common factor. From this it follows that the resultant $R=\mathrm{Res}(X(s,t),Y(s,t))$ is a nonzero rational number, say m/n.

Let S be the set of primes that divide mn or the denominator of a coefficient of X,Y or Z. According to Lemma 6.2, for all primes $p\in S$, there exists k_p such that for $s,t\in\mathbb{Q}$, if

$$\begin{cases} v_p(s-s_p)\geq k_p \\ v_p(t-t_p)\geq k_p, \end{cases}$$

then at least one of $X(s,t),Y(s,t),Z(s,t)$ is not divisible by p. Let

$$\begin{aligned} e_p &= \min\{v_p(s_p),0\} \\ f_p &= \min\{v_p(t_p),0\}, \end{aligned}$$

for all $p\in S$. We write

$$\begin{aligned} D_s &= \prod_{p\in S} p^{-e_p} \\ D_t &= \prod_{p\in S} p^{-f_p}. \end{aligned}$$

Then we get that $D_s s_p,\ D_t t_p\in\mathbb{Z}$. Now by Chinese remainder theorem we can find $s',t'\in\mathbb{Z}$ such that

$$\begin{aligned} s' &= D_s s_p \pmod{p^{k_p-e_p}} \\ t' &= D_t t_p \pmod{p^{k_p-f_p}}, \end{aligned}$$

for all $p\in S$. Let $s_0=s'/D_s$ and $t_0=t'/D_t$. It is easy to see that

$$\begin{cases} s_0-s_p=0 \pmod{p^{k_p-e_p}} \\ t_0-t_p=0 \pmod{p^{k_p-f_p}}. \end{cases}$$

Hence we get that

$$\begin{cases} v_p(s_0-s_p)\geq k_p-e_p\geq k_p \\ v_p(t_0-t_p)\geq k_p-f_p\geq k_p. \end{cases}$$

Thus we have that

$$\min\{v_p(X(s_0,t_0)), v_p(Y(s_0,t_0)), v_p(Z(s_0,t_0))\} = 0,$$

for $p \in S$.

For any prime $q \notin S$, if $v_q(s),\ v_q(t) > 0$, then we will have that

$$X(s/q, t/q) = q^{-\deg X} X(s,t),$$

and we see that scaling s and t by $1/q$, does not affect primitivity at primes in S. Thus without loss of generality we can assume that $\min\{v_p(s), v_p(t)\} = 0$, for $p \notin S$.

It remains to show that

$$\min\{v_p(X(s,t)), v_p(Y(s,t)), v_p(Z(s,t))\} = 0,$$

for $p \notin S$. Let $q \notin S$ be a prime. Since q neither divides R, nor it divides the denominator of any of the coefficients of X, Y and Z, we have that the reductions

$$\bar{X}(s,t), \bar{Y}(s,t), \bar{Z}(s,t) \in \mathbb{F}_q[s,t],$$

also have nonzero resultant, and hence no common roots. Therefore as long as

$$\min\{v_q(s), v_q(t)\} = 0,$$

both $X(s,t)$ and $Y(s,t)$ are also not divisible by q. This means

$$\min\{v_q(X(s,t)), v_q(Y(s,t)), v_q(Z(s,t))\} = 0,$$

for a prime q not in S. □

6.2 Elliptic Curves

We are studying Klein forms $f \in \mathcal{C}_3(d)(\mathbb{Q}_p)$, with $v_p(d) = 2$. We need some machinery from the theory of elliptic curves. Here we closely follow Cassels ([4], §15). Throughout this section we assume $K = \mathbb{Q}_p$, and $R = \mathbb{Z}_p$.

Assume $d \in \mathbb{Q}_p$ such that $v_p(d) = 2$. Let $g = x^3 - d \in \mathbb{Q}_p[x]$. If there exists $\alpha \in \mathbb{Q}_p$ such that $\alpha^3 - d = 0$, then $\beta = \alpha^2/p$ satisfies $x^3 - d^2/p^3$, which is Eisenstein, hence g is irreducible over $\mathbb{Q}_p$. We associate an elliptic curve to d in the following way

$$E_d \colon y^2 = g(x) = x^3 - d. \tag{6.4}$$

We define the field $M = \mathbb{Q}_p[\theta] = \mathbb{Q}_p[x]/(g(x))$, where θ is the image of x. We have the norm map

$$N\colon \mathbb{Q}_p[\theta] \to \mathbb{Q}_p$$

defined as follows. For $\alpha \in \mathbb{Q}_p[\theta]$ we define $N(\alpha)$ to be the determinant of the map

$$\begin{aligned} \mathbb{Q}_p[\theta] &\to \mathbb{Q}_p[\theta] \\ \zeta &\mapsto \alpha\zeta, \end{aligned}$$

considered as a $\mathbb{Q}_p$-linear map between $\mathbb{Q}_p$-vector spaces. Let M' be defined as follows

$$M' = \{a \in \mathbb{Q}_p^*[\theta]\colon N(a) \in \mathbb{Q}_p^{*2}\}.$$

For an elliptic curve E over $\mathbb{Q}_p$, we write $E[2]$ for the two-torsion on E and we write $\mathrm{H}^1(\mathbb{Q}_p, E[2])$ for its first cohomology group when considered as a group scheme over $\mathbb{Q}_p$. See [13, Chapter 4] for details. The group $\mathrm{H}^1(\mathbb{Q}_p, E[2])$ admits an elementary description in the following way.

Theorem 6.4 ([14], Corollary 4.2)**.** *Let E_d, M and M' be defined as above. Then*

$$\mathrm{H}^1(\mathbb{Q}_p, E_d[2]) \simeq M^{'}/M^{*2}.$$

Definition 6.5. Let C be a genus one curve. We say that $\pi : C \to E$ is a 2-covering of E if there is an isomorphism $\phi\colon C \to E$ defined over $\bar{K}$, such that the following diagram commutes

$$\begin{array}{ccc} E & \xrightarrow{[2]} & E \\ {\scriptstyle\phi}\uparrow & \nearrow_{\pi} & \\ C & & \end{array}.$$

Two 2-coverings (C_1, π_1, ϕ_1) and (C_2, π_2, ϕ_2) are isomorphic if $\phi_1^{-1} \circ \phi_2\colon C_2 \to C_1$ is an isomorphism over K.

Let $f \in K[x, y]$ be a quartic Klein form with Klein form discriminant d. We have the following syzygy:

$$\mathbf{t}(f)^2 = -4\mathbf{H}(f)^3 - 4df^3$$

If we rewrite this syzygy for a projective curve C with affine equation $y^2 = f(x, 1)$, we get

$$16[\mathbf{t}(f)(x, 1)]^2 = [-4\mathbf{H}(f)(x, 1)]^3 - 64dy^6,$$

dividing by $64y^6$ we obtain

$$\Big(\frac{\mathbf{t}(f)(x, 1)}{2y^3}\Big)^2 = \Big(\frac{-\mathbf{H}(f)(x, 1)}{y^2}\Big)^3 - d.$$

This equation defines an elliptic curve isomorphic to $E_d\colon y^2 = x^3 - d$.

Theorem 6.6. *Let $f \in \mathcal{C}_3(d)$ be a Klein form, and let C be a projective curve defined by the affine equation $C\colon y^2 = f(x,1)$. Let $E_d\colon Y^2 = X^3 - d$ be an elliptic curve. The map $\pi\colon C \to E_d$ defined by*

$$(x,y) \mapsto \Big(\frac{-\mathbf{H}(f)(x,1)}{y^2}, \frac{\mathbf{t}(f)(x,1)}{2y^3}\Big),$$

is a 2-covering of E_d.

Proof. First we show that π has degree four. Given $(x,1)$ on $\mathcal{C}$, we see that $(x,1)$ satisfies the quartic equation $Xf(x,1)+\mathbf{H}(f)(x,1)$, where (X,Y) are the coordinates of $K(E_d)$, and y is uniquely determined, $y = \frac{-X\mathbf{t}(f)(x,1)}{2Y\mathbf{H}(f)(x,1)}$.

Let $E' = \mathrm{Jac}(C)$ and assume $\theta\colon C \to E'$ is the map from C to its Jacobian, defined by sending one root of f to infinity and the other three roots to the roots of $X^3 - d$ in some order. Define $\mu = \pi \circ \theta^{-1}\colon E' \to E_d$. Then μ has degree four. It maps $0_{E'}$ to 0_{E_d}, so it is a group homomorphism ([13], Proposition 3.1). It also maps the four 2-torsion points $E'[2]$ to 0, so $\ker(\mu) = E'[2]$. Thus we get $E_d \cong E'/E'[2] = E'$. By Corollary 4.11 in [13] we get that $\mu = [2] \circ \alpha$, for some automorphism α of E_d. It follows that $\pi = [2] \circ \theta$, where $\theta = \alpha \circ \theta_1$. □

In this way any Klein form induces a 2-covering. We have the following proposition.

Proposition 6.7 ([3], Lemma 2)**.** *Two Klein forms with Klein form discriminant d are properly equivalent if and only if they give rise to the same 2-covering of E_d.*

Proof. Let f_1 and f_2 be two properly equivalent quartics (see Definition 2.3). Hence $f_1 = \lambda^2 f_2^M$, for some $\lambda \in K^*$, and $M \in \mathrm{GL}_2(K)$. Based on Proposition 6.6 we can associate a 2-covering to each Klein form. Let $\pi_1\colon C_1 \to E_d$ be the 2-covering associated to f_1, and $\pi_2\colon C_2 \to E_d$ be the 2-covering associated to f_2, where C_i is the projective curve with affine equation $y^2 = f_i(x,1)$ for $i = 1, 2$. Since $\mathbf{H}$, and $\mathbf{t}$ are covariants of weight 2 and 3, we get that

$$\pi_1(x,y) = \Big(\frac{-\lambda^4 \det(M)^2 \mathbf{H}(f_2)(x,1)}{y^2}, \frac{\lambda^6 \det(M)^3 \mathbf{t}(f_2)(x,1)}{2y^3}\Big).$$

Since $f_1 = \lambda^2 f_2^M$, we get that $d_1 = \lambda^6 \det(M)^6 d_2$, where d_1 and d_2 are the Klein form discriminants of f_1 and f_2 respectively. But since $d_1 = d_2 = d$, we get that $\lambda \det(M) = \zeta$ is a root of unity. This implies that

$$\pi_1(x,y) = \Big(\frac{-\lambda^2\zeta^2 \mathbf{H}(f_2)(x,1)}{y^2}, \frac{\lambda^3\zeta^3 \mathbf{t}(f_2)(x,1)}{2y^3}\Big).$$

We observe that

$$\pi_2(x,y) = \Big(\frac{-\mathbf{H}(f_2)(x,1)}{y^2}, \frac{\mathbf{t}(f_2)(x,1)}{2y^3}\Big).$$

From this it follows that

$$\pi_1(x,y) = \pi_2\Big(x, \frac{y}{\zeta\lambda}\Big).$$

This shows that π_1 and π_2 are isomorphic 2-coverings.

Now we prove the converse direction. Since f_1 and f_2 are both Klein forms with the same Klein form discriminant, it follows that both curves $C\colon y^2 = f_1(s,1)$, and $C'\colon y'^2 = f_2(s',1)$ have the same Jacobian curve, namely $E_d\colon y^2 = x^3 - d$ (see [3], Lemma 2). Hence there is a birational map $C \to C'$ defined over K which maps the points with $y = 0$ to the points with $y' = 0$. Such a mapping must be linear between s and s'; thus there exists $\lambda \in K^*$, and $M \in \mathrm{GL}_2(K)$ such that

$$f_1(s,t) = \lambda f_2^M(s',t').$$

From this equality we get that $d_1 = \lambda^3 \det(M)^6 d_2$, where d_1 and d_2 are the Klein form discriminants of the f_1 and f_2 respectively. But since $d_1 = d_2 = d$, we get that $\lambda = \det(M)^2$. Let $\mu = \det(M)$, we see that

$$f_1(s,t) = \mu^2 f_2^M(s',t').$$

Hence f_1 and f_2 are properly equivalent. □

For an elliptic curve E there is a standard identification of $\mathrm{H}^1(\mathbb{Q}_p, E[2])$ with the set of 2-coverings of E up to isomorphism.

Theorem 6.8 ([13], Theorem 2.2)**.** *There is an isomorphism*

$$\mathrm{H}^1(\mathbb{Q}_p, E[2]) \simeq \{2\text{-}\textit{coverings of } E\}.$$

6.3 Classifying Klein forms

In what follows we classify Klein forms in $\mathcal{C}_3(d)(\mathbb{Q})$, where $d \in \mathbb{Q}_p^*$ and $v_p(d) = 2$. We start by classifying the forms up to *proper equivalence* (see Definition 2.3), and after that we refine our classification to $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalence. Finally, we classify and list $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalence classes with integral representatives.

6.3.1 Proper Equivalence

Theorem 6.9. *Let $d \in \mathbb{Q}_p$, such that $v_p(d) \not\equiv 0 \pmod 3$. Up to proper equivalence there is only one Klein form in $\mathcal{C}_3(d)(\mathbb{Q}_p)$, namely $f(s,t) = t(s^3 - dt^3)$.*

Proof. Let $M = \mathbb{Q}_p[\theta] = \mathbb{Q}_p[x]/(f(x))$, where $f(x) = x^3 - d$ and θ is the image of x. Also let $M' = \{a \in \mathbb{Q}_p^*[\theta]\colon N(a) \in \mathbb{Q}_p^{*2}\}$. Since M is a local field we have

$$M^*/(M^*)^2 = \{1, c, p, cp\},$$

where $c \in M^*$ is a non-square. Since c, p, cp have non-square norms we get that $M'/(M^*)^2$ is trivial. This together with Theorem 6.4 and Theorem 6.8 implies that E_d admits only the trivial 2-covering. Now Proposition 6.7 completes the proof. □

6.3.2 $\mathrm{GL}_2(\mathbb{Q}_p)$-Equivalence

We first define the notion of GL_2-equivalence.

Definition 6.10. Two forms $f_1, f_2 \in K[x, y]$ are $\mathrm{GL}_2(K)$-equivalent if there exists $M \in \mathrm{GL}_2(K)$ such that $f_1 = f_2^M$.

Assume $d \in \mathbb{Q}_p^*$, such that $v_p(d) \not\equiv 0 \pmod 3$. Let $f \in \mathcal{C}_3(d)(\mathbb{Q}_p)$. Then according to Theorem 6.9 there exists $(\lambda, M) \in \mathbb{Q}_p^* \times \mathrm{GL}_2(\mathbb{Q}_p)$, such that

$$f = \lambda^2 t(s^3 - d_0 t^3)^M.$$

We have that $d(f) = \lambda^6 \det(M)^6 d = d$, and hence $\lambda \det(M) = 1$. Now if λ is a square, say $\lambda = \mu^2$, multiplication with λ^2 can be represented by a matrix N.

$$N = \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix}$$

Then $\lambda^2 f = f^N$. Since $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq (\mathbb{Z}/2\mathbb{Z})^2$, for $p \neq 2$, we have 4 different $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalence classes. We summarize the above argument in the following proposition.

Proposition 6.11. *Let $d \in \mathbb{Q}_p^*$, such that $v_p(d) \not\equiv 0 \pmod 3$. Up to $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalence there are four forms in $\mathcal{C}_3(d)(\mathbb{Q}_p)$. Let $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, c, p, cp\}$, where c is a non-square. We list these forms in the following table.*

f_1	$t(s^3 - dt^3)$
f_2	$t(cs^3 - d/c^2 t^3)$
f_3	$t(ps^3 - (d/p^2)t^3)$
f_4	$t(pcs^3 - (d/p^2c^2)t^3)$

6.3.3 $\mathrm{GL}_2(\mathbb{Q}_p)$ classes with representatives in $\mathbb{Z}_p[x, y]$

We have shown in the previous section that there are only four $\mathrm{GL}_2(\mathbb{Q}_p)$ classes of forms in $\mathcal{C}_3(d)(\mathbb{Q}_p)$, where $v_p(d) \not\equiv 0 \pmod 3$. Here we investigate the number of integral representatives for each of four $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalence classes. First we prove a lemma.

Lemma 6.12. *For any $M \in \mathrm{GL}_p(\mathbb{Q}_p)$, there exists $S \in \mathrm{SL}_2(\mathbb{Z}_p)$ and $U \in \mathrm{GL}_2(\mathbb{Q}_p)$, such that U is upper triangular and $M = US$.*

Proof. Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_p)$. It is enough to find $S \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that MS is upper triangular. If $\gamma = 0$ we can take S to be the identity matrix. If $\gamma \neq 0$, then there are co-prime $a, b \in \mathbb{Z}_p$ such that $a\gamma + c\delta = 0$, and we also can choose $b, d \in \mathbb{Z}_p$ such that $ad - bc = 1$. Now we can take $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p)$. □

Let $g \in \mathcal{C}_3(d)(\mathbb{Q}_p)$ where $v_p(d) \not\equiv 0 \pmod 3$. By Proposition 6.11 there is a matrix $M \in \mathrm{GL}_2(\mathbb{Q}_p)$, such that $g = f^M$, where f is one of the four forms stated in the Proposition 6.11. Since all of those four forms have Klein form discriminant d, we get that $\det M = 1$. According to Lemma 6.12, we obtain $M = US$ where $U \in \mathrm{GL}_2(\mathbb{Q}_p)$ is triangular, and $S \in \mathrm{SL}_2(\mathbb{Z}_p)$. Since $\det M = 1$, it follows that $\det U = 1$. Hence $g = f^{US}$, and $g^{S^{-1}} = f^U$. Since $S^{-1} \in \mathrm{SL}_2(\mathbb{Z}_p)$, we have that $f^U \in \mathcal{C}_3(d)(\mathbb{Z}_p)$. Thus in order to find all the $\mathrm{GL}_2(\mathbb{Q}_p)$-orbits of $\mathcal{C}_3(d)(\mathbb{Q}_p)$ that have representatives in $\mathcal{C}_3(d)(\mathbb{Z}_p)$, it is enough to determine the triangular matrix $U \in \mathrm{SL}_2(\mathbb{Q}_p)$ for which f_i^U has coefficients in $\mathbb{Z}_p$, where f_i is one of the forms listed in Proposition 6.11. We do this in the following theorem.

Theorem 6.13. *Let $d \in \mathbb{Q}_p$ such that $v_p(d) = 2$. Up to $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalence there are four forms in $\mathcal{C}_3(d)(\mathbb{Z}_p)$.*

Proof. According to the above argument, any Klein form $g \in \mathcal{C}_3(d)(\mathbb{Z}_p)$ can be written as $g = f^M$, where f is one of the four forms in Proposition 6.11, $S \in \mathrm{GL}_2(\mathbb{Z}_p)$ and $M = \begin{pmatrix} 1/a & b \\ 0 & a \end{pmatrix}$, with $a, b \in \mathbb{Q}_p$. We can assume $\det(M) = 1$, because

$$d = d(g) = \det(M)^6 d(f) = d.$$

Hence $\det(M)$ is a unit, we assume it to be 1. Without loss of generality we can represent f as $f = t(ws^3 + et^3)$ with $w, e \in \mathbb{Q}_p$, where $(w, e) \in \{(1, d), (c, d/c^2), (p, d/p^2), (cp, d/c^2p^2)\}$. We observe that $v_p(e) + 2v_p(w) = 2$.

By direct calculation we get

$$f^M = \Big(\frac{bw}{a^3} + b^4 e\Big)s^4 + \Big(\frac{w}{a^2} + 4b^3 ae\Big)s^3 t + (6b^2 a^2 e)s^2 t^2 + (4ba^3 e)st^3 + (a^4 e)t^4.$$

Since we want f to have coefficients in $\mathbb{Z}_p$ we get the following constraints:

$$v_p(a^4e) \geq 0, \tag{6.5}$$
$$v_p(4ba^3e) \geq 0, \tag{6.6}$$
$$v_p(6b^2a^2e) \geq 0, \tag{6.7}$$
$$v_p\Big(\frac{w}{a^2} + 4b^3ae\Big) \geq 0, \tag{6.8}$$
$$v_p\Big(\frac{bw}{a^3} + b^4e\Big) \geq 0. \tag{6.9}$$

From Proposition 6.11 we know that $v_p(e)$ is either 0 or 1. In both cases, condition (6.5) implies that $v_p(a) \geq 0$. If $v_p(a) \neq 0$, then $v_p(\frac{w}{a^2}) < 0$. Thus condition (6.8) implies that

$$v_p\Big(\frac{w}{a^2}\Big) = v_p(w) - 2v_p(a) = v_p(4b^3ae) = 3v_p(b) + v_p(a) + v_p(e).$$

If we substitute $v_p(e) = 2 - 2v_p(w)$ in the above equality, we get that

$$2 = 3v_p(w) - 3v_p(b) - 3v_p(a),$$

which is a contradiction. Thus $v_p(a) = 0$. Since $v_p(e) \geq 0$, condition (6.7) implies that $v_p(b) \geq 0$. Hence we see that $M \in \mathrm{GL}_2(\mathbb{Z}_p)$.

This shows that we have exactly four $\mathrm{GL}(\mathbb{Q}_p)$-equivalence classes of Klein forms in $\mathcal{C}_3(d)(\mathbb{Z}_p)$. □

Theorem 6.14. *Let $d \in \mathbb{Z}_p$ with $v_p(d) = 2$. Only half of the $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalence classes of Klein forms in $\mathcal{C}_3(d)(\mathbb{Z}_p)$ produce $\mathbb{Z}_p$-primitive solutions for the equation*

$$x^2 + By^3 = Cz^3, \tag{6.10}$$

where B, C are square-free integers, such that $\gcd(B, C) = 1$, $v_p(B) = 1$, and $d = B^2C$.

Proof. According to Theorem 5.3 all the solutions to (6.10) are produced by Klein forms in $\mathcal{C}_3(d)(\mathbb{Q}_p)$. Since acting via $\mathrm{GL}_2(\mathbb{Z}_p)$ does not affect productivity, and we showed that any Klein form in $\mathcal{C}_3(d)(\mathbb{Z}_p)$ is $\mathrm{GL}_2(\mathbb{Q}_p)$-equivalent to one of the forms listed in Proposition 6.11, without loss of generality we can prove the result for these four forms. Let $f = t(ws^3 + et^3)$, be one of the following forms

f_1	$t(s^3 - dt^3)$
f_2	$t(cs^3 - d/c^2t^3)$
f_3	$t(ps^3 - (d/p^2)t^3)$
f_4	$t(pcs^3 - (d/p^2c^2)t^3)$

We observe that $v_p(w) = 0, 1$, and we have the identity $v_p(e) + 2v_p(w) = 2$. We recall

$$\begin{aligned}\mathbf{H}(f) &= 3w^2s^4 - 24west^3,\\ \mathbf{t}(f) &= w^3s^6 + 20(w^2e)s^3t^3 - (8we^2)t^6.\end{aligned}$$

From Chapter 3, we recall that

$$(\mathbf{t}(f)/2)^2 + \mathbf{H}(f)^3 = df^3.$$

Hence the triple $(\mathbf{t}(f)/2B, \mathbf{H}(f)/B, f)$ produces a primitive solution for the equation

$$x^2 + By^3 = Cz^3,$$

exactly when there exist $s_0, t_0 \in \mathbb{Z}_p$ for which we have

$$\min\{v_p(\mathbf{t}(f)(s_0, t_0)/B), v_p(\mathbf{H}(f)(s_0, t_0)/B), v_p(f(s_0, t_0))\} = 0.$$

In particular, $v_p(\mathbf{H}(f)(s_0, t_0)/p) \geq 0$. But that means we have

$$(3w^2s_0^4)/p - (24wes_0t_0^3)/p \in \mathbb{Z}_p.$$

If $v_p(w) = 1$, then obviously $(3w^2s_0^4)/p - (24wes_0t_0^3)/p \in \mathbb{Z}_p$, and if we evaluate the triple $(\mathbf{t}(f)/2B, \mathbf{H}(f)/B, f)$ at $(1, 0)$ we get $(w^3/2B, 3w^2/B, 0)$ which is obviously a primitive solution. It remains to check the case where $v_p(w) = 0$, which implies $v_p(e) = 2$. For the sake of contradiction we assume $v_p(e) = 2$. First consider the case where $v_p(s_0) = 0$. We should have

$$2v_p(w) + 4v_p(s_0) - 1 = v_p(w) + v_p(e) - 1 + v_p(s_0) + 3v_p(t_0),$$

If we plug $2 = 2v_p(w) + v_p(e)$, we get

$$3v_p(w) - 2 = v_p(t_0) - 3v_p(s_0).$$

Since $v_p(w) = 0$, we get that $v_p(t_0) - 3v_p(s_0) = -2$, which immediately rules out the case $v_p(s_0) = 0$. It remains to rule out the case where $v_p(s_0) > 0$. In this is case it is easily seen that

$$\min\{v_p(\mathbf{t}(f)(s_0, t_0)/p), v_p(\mathbf{H}(f)(s_0, t_0)/p), v_p(f(s_0, t_0))\} > 0.$$

We have proved that for the equation

$$x^2 + By^3 = Cz^3,$$

the forms f_3, f_4 are productive, and the forms f_1, f_2 are not productive. $\square$

Chapter 7

Density Heuristics

In previous chapters we studied the Diophantine equation

$$x^2 + By^3 = Cz^3,$$

where $\gcd(B, C) = 1$, and B, C are square-free integers. In this chapter we first prove that these equations form a positive proportion of the set of equations with no constraints on B and C. After that we discuss possible applications of our result. We introduce some terminology first.

Definition 7.1. Let B be a positive integer. We define the following sets,

$$E(B) = \{(b, c) \colon |b| \leq B, |c| \leq B\},$$
$$E'(B) = \{(b, c) \colon |b| \leq B, |c| \leq B, \gcd(b, c) = 1,\ b \text{ and } c \text{ are square free}\}.$$

Theorem 7.2 ([11], Theorem 1)**.** *We have*

$$\#E'(B) = 4\frac{B^2}{\zeta(2)^2} \prod_p \Big(1 - \frac{1}{(p+1)^2}\Big) + O(B^{3/2}).$$

Theorem (7.2) implies that the relative density $D := \frac{\#E'(B)}{\#E(B)}$ is

$$D = \frac{1}{\zeta(2)^2} \prod_p \Big(1 - \frac{1}{(p+1)^2}\Big) \approx 0.28674742843447873411$$

In proving Theorem (7.2) we use the following facts from analytical number theory

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise,} \end{cases} \tag{7.1}$$

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} (1 - \frac{1}{p}). \tag{7.2}$$

All of these are standard facts from analytical number theory. A good reference containing proofs is Tenenbaum [15]. Before stating the proof we prove two lemmas.

Lemma 7.3 ([11], Lemma 1)**.** *Let $d \geq 1$ be an integer. Let*

$$S_d(x) = \sum_{\substack{n \leq x \\ (d,n)=1}} \mu(n)^2.$$

We have

$$S_d(x) = \frac{x}{\zeta(2)\prod_{p|d}(1+\frac{1}{p})} + O(2^{\omega(d)}\sqrt{x}),$$

where $\omega(d)$ denotes the number of distinct prime divisors of d.

Proof. Let $T_d(x)$ denote the number of natural numbers $n \leq x$ coprime to d. According to (7.1), and (7.2) we get

$$T_d(x) = \sum_{\substack{n \leq x \\ (n,d)=1}} 1 = \sum_{n \leq x} \sum_{\substack{\alpha | n \\ \alpha | d}} \mu(\alpha) = \sum_{\alpha | d} \mu(\alpha)[\frac{x}{\alpha}] = \frac{\phi(d)}{d}x + O(2^{\omega(d)}), \tag{7.3}$$

where $[x]$ is the integral part of x. By the inclusion and exclusion principle we obtain

$$S_d(x) = \sum_{\substack{m \leq \sqrt{x} \\ (d,m)=1}} \mu(m) T_d(\frac{x}{m^2}).$$

Now by (7.3), we deduce

$$S_d(x) = x\frac{\phi(d)}{d} \sum_{\substack{m \leq \sqrt{x} \\ (d,m)=1}} \frac{\mu(m)}{m^2} + O(2^{\omega(d)}\sqrt{x}).$$

By completing the sum,

$$S_d(x) = x\frac{\phi(d)}{d} \sum_{\substack{m=1 \\ (d,m)=1}}^{\infty} \frac{\mu(m)}{m^2} + O(2^{\omega(d)}\sqrt{x})$$

Recall the well-known identity

$$\sum_{\substack{m=1 \\ (d,m)=1}} \frac{\mu(m)}{m^2} = \prod_{p \nmid d}(1-\frac{1}{p^2}) = \frac{1}{\zeta(2)\prod_{p|d}(1-1/p^2)}.$$

Using this identity and (7.2) the lemma is proved. □

Lemma 7.4 ([11], Lemma 2)**.** *We have*

$$\sum_{d\le x}\frac{2^{\omega(d)}}{d^{3/2}}=O(1),\quad \sum_{d\le x}\frac{2^{\omega(d)}}{\sqrt{d}}=O(\sqrt{x}\log x),\quad \sum_{d\le x}\frac{4^{\omega(d)}}{d}=O(\log^3 x).$$

7.1 Proof of Theorem 7.2

Note that

$$\#E'(B)=4\sum_{m\le B}\sum_{n\le B}\mu(m)^2\mu(n)^2\sum_{d|m,\ d|n}\mu(d).$$

By swapping the order of summation, we get

$$\#E'(B)=4\sum_{d\le B}\mu(d)\sum_{\substack{m\le B\\ d|m}}\mu(m)^2\sum_{\substack{n\le B\\ d|n}}\mu(n)^2. \tag{7.4}$$

Note that

$$\sum_{\substack{m\le B\\ d|m}}\mu(m)^2=\mu(d)^2\sum_{\substack{k\le B/d\\ (d,k)=1}}\mu(k)^2=\mu(d)^2S_d\Big(\frac{B}{d}\Big), \tag{7.5}$$

where the rightmost equality is from Lemma (7.3). By (7.5) and the fact that $\mu(d)=\mu(d)^5$ we get

$$\#E'(B)=4\sum_{d\le B}\mu(d)S_d\Big(\frac{B}{d}\Big)^2. \tag{7.6}$$

According to Lemma (7.3), we get

$$\#E'(B)=4\frac{B^2}{\zeta(2)^2}\sum_{d\le B}\frac{\mu(d)}{d^2\prod_{p|d}(1+1/p)^2}+O(x^{3/2}\sum_{d\le B}\frac{2^{\omega(d)}}{d^{3/2}})+O(x\sum_{d\le B}\frac{4^{\omega(d)}}{d}).$$

By completing the first sum and noting that

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2\prod_{p|d}(1+1/p)^2)}=\prod_p\Big(1-\frac{1}{(p+1)^2}\Big),$$

we get

$$\#E'(B)=4\frac{B^2}{\zeta(2)^2}\prod_p\Big(1-\frac{1}{(p+1)^2}\Big)+O(B^{3/2}\sum_{d\le B}\frac{2^{\omega(d)}}{d^{3/2}})+O(B\sum_{d\le B}\frac{4^{\omega(d)}}{d}).$$

Now the theorem follows from Lemma (7.4).

7.2 Density Heuristics

In this section we sketch how we envision the results from Chapter 6 might help in determining the average number of productive Klein forms for equations of the form

$$x^2 + By^3 + Cz^3 = 0. \tag{7.7}$$

As we have seen in Theorem 5.3, primitive solutions to (7.7) give rise to quartic Klein forms in $\mathbb{Z}[s,t]$ with Klein form discriminant equal to $d = B^2C$, and we say two primitive solutions are equivalent if their Klein forms are $\mathrm{GL}_2(\mathbb{Z})$-equivalent. The motivation is that a Klein form gives rise to a parametric solution, and equivalent solutions can be obtained as specializations of the same parametrization.

As Edwards explains in [5, Chapter 11], each $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of Klein forms admits a Hermite reduced representative. Such representatives have their coefficients bounded by an explicit function of d. It follows that there are only finitely many equivalence classes of Klein forms of bounded discriminant, and hence we get an estimate of the average number of Klein forms per discriminant (as a function of d).

As we have seen in Theorem 6.3, whether a Klein form is productive for a given equation is determined by local conditions. These translate into congruence conditions on the coefficients of the Klein form, and thus give us local densities for the locally productive Klein forms in the space of Klein forms with coefficients in $\mathbb{Z}_p$.

Our heuristic assumption is that the integral Klein forms distribute approximately uniformly over the $\mathbb{Z}_p$-equivalence classes. As a consequence, for each Klein form discriminant d, we expect the proportion of productive Klein forms to be measured by the product of the relevant local densities. As our results suggest, these local densities would be about $\frac{1}{2}$ for each prime dividing B.

It should be possible to make this heuristic rigorous by establishing that the space of equivalence classes of Klein forms is rational. A further quantitative analysis should make it possible to make quantitative estimates of the densities and number of equivalence classes involved. We are hopeful to execute this programme in future work.

Bibliography

[1] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91(1):61–88, 1998.

[2] Frits Beukers. *The diophantine equation* $Ax^p + BY^q = Cz^r$, 2004. `http://www.staff.science.uu.nl/~beuke106/Fermatlectures.pdf`.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[4] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[5] Johnny Edwards. *Platonic Solids and solutions to* $X^2 + Y^3 = Z^r$. PhD thesis, Utrecht, 2005.

[6] Paul Gordon. *Vorlessung über invariantentheorie*. Teubner, Leipzig, 1887.

[7] David Hilbert. *Theory of algebraic invariants*. Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher, Edited and with an introduction by Bernd Sturmfels.

[8] Felix Klein. *Lectures on the ikosahedron and the solution of equations of the fifth degree (translation of the original 1884 edition*. Dover publications, New York, 1956.

[9] Patrick Ryan McMahon. *Solvability of ternary equations of signature (3,3,2)*. Simon Fraser University, Master's thesis, 2014.

[10] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London-New York, 1969.

[11] Pieter Moree. *Counting carefree couples*, 2005. `http://https://arxiv.org/abs/math/0510003`.

[12] Peter J. Olver. *Classical Invariant Theory*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[13] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag New York, 2009.

[14] Fisher T. Some improvements to 4-descent on an elliptic curve. *van der Poorten A.J., Stein A. (eds) Algorithmic Number Theory. ANTS Lecture Notes in Computer Science*, 5011, 2008.

[15] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.