A Complete Solution of $X^2 + Y^3 + Z^5 = 0$

Johnny Edwards

29 November 2001

Abstract

An algorithm is described which produces a finite list of $\mathbb{Z}_S[x_1, x_2]$ solutions to a diophantine equations of the form

$$AX^2 + BY^3 + CZ^r = 0$$

where $r \in \{3, 4, 5\}$, S is a finite set of primes, $A, B \in \mathbb{Z}_S^*, C \in Z_S$. This list has the property that all integer solutions with $\gcd(X, Y, Z) \in \mathbb{Z}_S^*$ occur by specializing the parameters (x_1, x_2) in one of the parameterized solutions to integers.

The algorithm is used to construct a finite list of $\mathbb{Z}[x_1, x_2]$ solutions of :

$$X^2 + Y^3 + Z^5 = 0$$

such that all integer solutions with $\gcd(X, Y, Z) = 1$ occur by specializing the parameters (x_1, x_2) in one of the parameterized solutions to integers.

Contents

1 Introduction

In this paper I prove the following theorem:

Theorem 1.1 *Fix $r \in \{3,4,5\}$. Fix a finite set of primes S. Fix $A, B \in Z_S^*$ and non zero $C \in Z_S$. There is is a finite set of solutions in $\mathbb{Z}_S[x_1, x_2]$ to :*

$$Ax^2 + By^3 + Cz^r = 0 \tag{1}$$

such that

- *their integer specializations include all integer solutions with* $\gcd(X,Y,Z) \in \mathbb{Z}_S^*$
- *their $\mathbb{Z}_S$ specializations include all $\mathbb{Z}_S$ solutions with* $\gcd(X,Y,Z) \in \mathbb{Z}_S^*$.

Furthermore there is an explicit algorithm to create these parameterizations.

This is a generalizes a result of Beukers [FB98], as:

- The parameterizations are now in $\mathbb{Z}_S[x_1, x_2]$ rather than just $\mathbb{Q}[x_1, x_2]$.
- The algorithm is explicit

I illustrate the latter point by producing sets of $\mathbb{Z}[x_1, x_2]$ solutions of the equations:

$$X^2 + Y^3 \pm Z^r, \quad r \in \{3,4,5\}$$

whose integer specializations include all integer solutions with $\gcd(X,Y,Z) = 1$. Before this paper, (complete) sets were only known for $r = 3$ (Mordell 1969) and $r = 4$ (Zagier 1998 in [FB98]).

The method given here is a generalization of an algorithm for the $2,3,3$ case, presented by Mordell in his book *Diophantine Equations* [Mo69][ch. 25].

1.2 Layout of Paper

The lion's share of the paper in devoted to producing $\mathbb{Z}[x_1, x_2]$ parameterizations to:

$$X^2 + Y^3 + dZ^r = 0 \tag{2}$$

(d is a non-zero integer) whose integer specializations include all relatively prime integer solutions. I.e. we prove the main theorem for the special cases when $S = \emptyset$, $A = B = 1$. This is done in the following sections:

- Section 2, describes the invariant theory and other properties of Klein forms needed in the paper.
- Section 3 show how integer solutions to (2) can be lifted to parameterized solutions
- Section 4 proves various properties of real Klein forms, needed to apply Hermite reduction in the algorithm.
- Section 5 describes Hermite reduction theory
- Section 6 merges the theory of the previous sections into an algorithm for producing complete sets of parameterized solutions to (2).

Section 7 shows how to generalize to the case $AX^2 + BY^3 + CZ^r = 0, \#S < \infty$, thus proving the main Theorem 1.1.

Appendix A gives complete parameterizations to the equations $X^2 + Y^3 \pm Z^r = 0, S = \emptyset$.

1.3 Acknowledgements

I'd like to thank Frits Beukers for introducing me to the problem, as well as his continued help and encouragement while I was writing this paper. It was his idea to try to generalize Mordell's method for the $2,3,3$ equation.

This led me to Tonny Springer, who is thanked for helping me to my crucial Invariant Theory reference: [PG87, p 204]. Finally, thanks to Michael Stoll and Don Zagier for comments that have made their way into this article.

2 The Invariant Theory of Klein Forms

2.1 Definition of Covariants

This section fixes the notation and gives the basics of the invariant theory to be used in this paper. Take a generic form of order k given by:-

$$f = \sum_{i=0}^{k} \left(\begin{array}{c} k \\ i \end{array} \right) a_i \, x_1^{k-i} x_2^i$$

Let $g = \left(\begin{array}{cc} g_{11} & g_{12} \\ g_{21} & g_{22} \end{array} \right) \in \mathrm{GL}(2,\mathbb{C})$ act on $\mathbb{C}^2$ by:

$$(x_1, x_2) \mapsto (g_{11}x_1 + g_{12}x_2, g_{21}x_1 + g_{22}x_2)$$

define a' by $f(a', x_1, x_2) := f(a, g(x_1, x_2))$.

Definition 2.2 *A form $H \in \mathbb{C}[a_0, \ldots a_k, x_1, x_2] = \mathbb{C}[a, x_1, x_2]$ is a covariant iff there is a $p \in \mathbb{Z}_{\geq 0}$ such that:*

$$H(a', x_1, x_2) = \det(g)^p H(a, g(x_1, x_2))$$

for all $g \in GL(2,\mathbb{C})$. The number p is called the weight of the covariant.

We write $H = H(f)$ to emphasis the dependence on the coefficients of f.

Lemma 2.3 *H is a covariant of weight p iff for all $g \in GL(2,\mathbb{C})$:*

$$H(f) \circ g = \det(g)^{-p} H(\bar{f})$$

where $\bar{f} = f \circ g$.

2.4 Examples of covariants

Consider:

$$H(f) = \left(\frac{1}{k(k-1)} \right)^2 \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix}$$

$$t(f) = \frac{1}{k(k-2)} \begin{vmatrix} f_x & f_y \\ H_x & H_y \end{vmatrix}$$

These can be shown (e.g. [DG95, Lecture XXVI, p88]) to be covariants of weight $2,3$ respectively. Written explicitly:

$$\begin{aligned} f &= a_0 x_1^k + \ldots \\ H(f) &= (a_0 a_2 - a_1^2) x_1^{2k-4} + \ldots \\ t(f) &= (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) x_1^{3k-6} + \ldots \end{aligned}$$

2.5 The Klein Forms

In [FK84], Felix Klein embeds the tetrahedron, octahedron, icosahedron on the 2 sphere which he then projects onto the extended complex plane $\mathbb{P}^\infty$. After a suitable rotation of the sphere, forms whose roots correspond to the vertices of the solid are:

Definition 2.6

r	*Solid*	*The vertices*	k	N	β_r
3	*Tetrahedron*	$\tilde{f}_3 = x_2^4 - 2\sqrt{3}x_1^2x_2^2 - x_1^4$	4	12	$3\sqrt{3}$
4	*Octahedron*	$\tilde{f}_4 = x_1x_2(x_1^4 - x_2^4)$	6	24	432
		$\tilde{f}_4^* = x_1x_2(x_1^4 + x_2^4)$			
5	*Icosahedron*	$\tilde{f}_5 = x_1x_2(x_2^{10} - 11x_1^5x_2^5 - x_1^{10})$	12	60	1728

In the definition k denotes the number of vertices of the solid, N the order of the group of rotational symmetries of the solid.

Covariants of the $\tilde{f}_r$ correspond to unions of orbits on the sphere. Klein's relations become:

$$(\frac{1}{2}t(\tilde{f}_r))^2 + H(\tilde{f}_r)^3 + \frac{1}{\beta_r}\tilde{f}_r^r = 0 \tag{3}$$

The $\tilde{f}_4^*$ also represents the octahedron. It satisfies:

$$(\frac{1}{2}t(\tilde{f}_4^*))^2 + H(\tilde{f}_4^*)^3 - \frac{1}{\beta_4}\tilde{f}_4^{*4} = 0 \tag{4}$$

Definition 2.7 *For $r \in \{3,4,5\}$ and for $d \in \mathbb{C}^*$ define:*

$$\begin{aligned} \mathcal{C}(r) &:= \{\tilde{f}_r \circ g \mid g \in GL(2,\mathbb{C})\} \\ \mathcal{C}(r,d) &:= \{f \in \mathcal{C}(r) \mid (\frac{1}{2}t(f))^2 + H(f)^3 + df^r = 0\} \end{aligned}$$

Lemma 2.8 *For $g \in GL(2,\mathbb{C})$ and $\lambda \in \mathbb{C}^*$ we have:*

$$\begin{array}{ccc} & \tilde{f}_r \in \mathcal{C}(r,\beta_r^{-1}) & \\ f \in \mathcal{C}(r,d) & \Longleftrightarrow & f \circ g \in \mathcal{C}(r,\det(g)^6 d) \\ f \in \mathcal{C}(r,d) & \Longleftrightarrow & \lambda f \in \mathcal{C}(r,\lambda^{6-r}d) \end{array}$$

Proof. The first claim comes from the definition of β_r. The second claim follows by Lemma 2.3 since $t(f)^2, H(f)^3$ are covariants of weight 6 but f^r is a covariant of weight 0. The third follows since $t(f)^2, H(f)^3$ homogeneous of degree 6 in the a_i, and f^r is of degree r.

q.e.d

Proposition 2.9 *We have:*

$$\mathcal{C}(r,d) = \{f = \tilde{f}_r \circ g \mid \det(g)^6 = \beta_r d\}$$

and

$$\mathcal{C}(r) = \bigsqcup_{d \in \mathbb{C}^*} \mathcal{C}(r,d)$$

(disjoint union of non empty sets).

Proof. This follows by Lemma 2.8.

q.e.d

Notation 2.10 (Klein forms) *We call $\mathcal{C}(3) \cup \mathcal{C}(4) \cup \mathcal{C}(5)$ the Klein forms. $\mathcal{C}(3)$ are the tetrahedral Klein forms, $\mathcal{C}(4)$ the octahedral Klein forms, and $\mathcal{C}(5)$ the icosahedral Klein forms. A Klein form is called a* real Klein form *if all its coefficients are real.*

2.11 Characterizing the $\mathcal{C}(r, d)$

For general k define the 4th and 6th covariants of f by:-

$$\tau_4(f) = \frac{1}{2}\left(\frac{(k-4)!}{k!}\right)^2 \Omega^4 f(x,y)f(x',y')\Big|_{\substack{x,x'=x_1\\ y,y'=x_2}}$$

$$\tau_6(f) = \frac{1}{2}\left(\frac{(k-6)!}{k!}\right)^2 \Omega^6 f(x,y)f(x',y')\Big|_{\substack{x,x'=x_1\\ y,y'=x_2}}$$

where

$$\Omega = \left(\frac{\delta^2}{\delta x \delta y'} - \frac{\delta^2}{\delta y \delta x'}\right)$$

Then

$$\begin{aligned}\tau_4(f) &= (a_0a_4 - 4a_1a_3 + 3a_2^2)x_1^{2k-8} + \dots\\ \tau_6(f) &= (a_0a_6 - 6a_1a_5 + 15a_2a_4 - 10a_3^2)x_1^{2k-12} + \dots\end{aligned}$$

These are up to a constant factor the 4th and 6th transvections of base form with itself (see [DH97, XXVI, p88]). They have weight 4 and 6 respectively.

For base forms of order $k = 4$ define the catalecticant invariant j by:

$$\begin{aligned}j(f) &= \begin{vmatrix} a_0 & a_1 & a_2\\ a_1 & a_2 & a_3\\ a_2 & a_3 & a_4\end{vmatrix}\\ &= a_0a_2a_4 + 2a_1a_2a_3 - a_2^3 - a_0a_3^2 - a_1^2a_4\end{aligned}$$

(see [Mo69, ch25, p233]). This also has weight 6.

In answer to a question posed by Clebsch, Gordan proved:

Theorem 2.12 (Gordan 1887) *Let f be a form of order k. Then $\tau_4(f) \equiv 0$ iff f is $GL(2,\mathbb{C})$ equivalent to x_1^k, $x_1^{k-1}x_2$ or one of the Klein forms: $\tilde{f}_3$,$\tilde{f}_4$ or $\tilde{f}_5$.*

See [PG87, p 204].

The fact that the covariant of x_1^k , $x_1^{k-1}x_2$ disappear can be explained by the following :

Lemma 2.13 *Let G be a covariant of weight p, homogeneous of degree n in the a_i. If $p > n$ then $G(x_1^k) \equiv 0$, $G(x_1^{k-1}x_2) \equiv 0$.*

Proof.Let $G = \sum_{j=0}^{m} G_j x_1^{m-j}x_2^j$. The theory of covariants (e.g. [DH97, XIII, p43]) shows that each coefficient G_j is isobaric of weight $\geq p$ in the a_i. For $f = x_1^k, x_1^{k-1}x_2$ the only non zero a_i have $i = 0$ or 1 and so $G(f) \equiv 0$.

q.e.d

Theorem 2.14 (Classification of Klein Forms) *Fix $d \in \mathbb{C}^*$.*

$$\begin{aligned}
\mathcal{C}(3,d) &= \{f \in \mathbb{C}[x_1, x_2]_4 \mid \tau_4(f) = 0, j(f) = 4d\} \\
\mathcal{C}(4,d) &= \{f \in \mathbb{C}[x_1, x_2]_6 \mid \tau_4(f) \equiv 0, \tau_6(f) = 72d\} \\
\mathcal{C}(5,d) &= \{f \in \mathbb{C}[x_1, x_2]_{12} \mid \tau_4(f) \equiv 0, \tau_6(f) \equiv \frac{360}{7} df\}
\end{aligned}$$

Proof. Fix $r \in \{3,4,5\}$. Call the right hand sides of the above equalities: $V(3,d)$, $V(4,d)$, $V(5,d)$.

j and τ_6 both have weight 6 and are homogeneous of degree 3 and 2 in the a_i. So by Lemma 2.13 $x_1^k, x_1^{k-1}x_2 \notin V(r,d)$. By Theorem 2.12 we can restrict attention to f which are $\mathrm{GL}(2,\mathbb{C})$ equivalent to a Klein form. Using Lemma 2.3 and the fact that τ_6, j have weight 6 we get that

$$f \in V(r,d) \iff f \circ g \in V(r, \det(g)^6 d)$$

So by Proposition 2.8 we only have to show that $\tilde{f}_r \in V(r, \beta_r^{-1})$. This is verified by direct calculation.

q.e.d

2.15 Defining Integral Forms

Here we define what we mean for f to be integral. As for quadratic forms there are two common ways to consider these higher order forms to be integral: one of them is that $f \in \mathbb{Z}[x_1, x_2]$ and the other is that $a_i \in \mathbb{Z}$. However, it turns out prudent for us to use the following intermediate definition:

Definition 2.16 (Integrality of Forms) *Given $r \in \{3,4,5\}$ we consider base forms of order $k = 4, 6, 12$ respectively. We define:*

$$\begin{aligned}
\Omega_3 &:= \{a_0, \ldots a_4\} \\
\Omega_4 &:= \{a_0, a_1, \ldots a_6\} \\
\Omega_5 &:= \{a_0, \ldots a_5, 7a_6, a_7 \ldots a_{12}\}
\end{aligned}$$

and consider a form to be integral if it is in $\mathbb{X}_r$ where:

$$\mathbb{X}_r[x_1, x_2] := \{f = \sum_{i=0}^{k} \binom{k}{i} a_i x_1^{k-i} x_2^i \mid \Omega_r \text{ consists of integers } \}$$

Proposition 2.17 *The classes $\mathbb{X}_3, \mathbb{X}_4, \mathbb{X}_5$ are closed under the action of $GL(2,\mathbb{Z})$.*

Proof. $\mathrm{GL}(2,\mathbb{Z})$ is generated by:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$\mathbb{X}_r$ are clearly closed under S, U. We only have to show it is closed under T. Let

$$f = \sum_{i=1}^{k} \begin{pmatrix} k \\ i \end{pmatrix} a_i x_1^{k-i} x_1^i$$

and let $f' := f(x_1 + x_2, x_2)$ have coefficients a' Then:-

$$a'_t = a_t + \sum_{i=0}^{t-1} \left(\begin{array}{c} t \\ i \end{array} \right) a_i$$

The result follows trivially in the cases $r = 3, 4$ and from the fact that 7 divides $\binom{t}{6}$ for $6 < t \leq 12$ in the case $r = 5$.

q.e.d

Proposition 2.18 *Fix $r \in \{3, 4, 5\}$ and $k \in \{4, 6, 12\}$ respectively for the order of the base forms. Let $C = \sum_{i=0}^{m} C_i x_1^{m-i} x_2^i$ be a covariant. Suppose $C_0 \in \mathbb{Z}[a_0 ... a_k]$ and if $r = 5$ that the covariant has weight ≤ 5. Then $C(f) \in \mathbb{Z}[\Omega_r; x_1, x_2]$. In particular:*

$$f \in \mathbb{X}_r[x_1, x_2] \implies C(f) \in \mathbb{Z}[x_1, x_2]$$

Proof. By [DH97, I.12, p103], $C(f)$ can be gotten by replacing the a_i in C_0 by

$$\begin{aligned} f_i &:= \frac{(k-i)!}{k!} f^{(i)} \\ &= \sum_r \left(\begin{array}{c} k-i \\ r \end{array} \right) a_r x_1^{k-r-i} x_2^r \end{aligned}$$

where $f^{(i)}$ denotes the i-th derivative of f wrt x_1. This implies the result for $r = 3, 4$. For $r = 5$ the extra assumption means that C_0 is isobaric of weight ≤ 5 in the a_i. But $f_0, f_1 \ldots f_5 \in \mathbb{Z}[\Omega_5; x_1, x_2]$ and the result for $r = 5$ follows too.

q.e.d

3 Lifting Integer Solutions to Parameterizations

We now show how integer solutions to our diophantine equations can be used to construct integral parameterizations to the same equation.

3.1 Existence of Lifts

This section will be devoted to proving the following theorem:

Theorem 3.2 (Lifting Theorem) *Fix d a non zero integer and $r \in \{3, 4, 5\}$. Suppose that X, Y, Z satisfy $X^2 + Y^3 + dZ^r = 0$ with $X, Y, Z \in \mathbb{Z}$, $\gcd(X, Y, Z) = 1$. Then there exists a binary form $f \in \mathbb{X}_r \cap \mathcal{C}(r, d)$ and $s_0, t_0 \in \mathbb{Z}$ such that:*

$$X = \frac{1}{2} t(f)(s_0, t_0), \quad Y = H(f)(s_0, t_0), \quad Z = f(s_0, t_0)$$

where H, t are the covariants defined in 2.4.

3.2.1 Common Part of Proof

We start with an arbitrary $f \in \mathcal{C}(r, d)$. $\frac{1}{2} t(f), H(f), f \in \mathbb{C}[s, t]$ define a map from $\mathbb{A}^2$ into the surface $V \subset \mathbb{A}^3$ defined by:-

$$V \quad : \quad X^2 + Y^3 + dZ^r = 0$$

Lemma 3.3 *the map is onto.*

Proof.Consider, first, $\tilde{f} = \tilde{f}_3, \tilde{f}_4^*, \tilde{f}_5$ along with $\tilde{m} = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$ respectively. In all cases $\det(\tilde{m}) = -1$, $\tilde{f} \circ \tilde{m} = \tilde{f}$. Since f equals $\tilde{f} \circ h$ for some $h \in \mathrm{GL}(2, \mathbb{C})$, $m = h^{-1}\tilde{m}h$ is a matrix of determinant -1 fixing f.

Now take $X, Y, Z \in V(\mathbb{C})$. Use elimination theory to find (s_0, t_0) with $H(f)(s_0, t_0), f(s_0, t_0) = Y, Z$. We must have $\frac{1}{2}t(f)(s_0, t_0) = \pm X$. If it is $+X$ we are through. Otherwise replace $(s_0, t_0)^T$ by $m(s_0, t_0)^T$, where m is as above. Since f, H, t have weight $0, 2, 3$, Lemma 2.3 shows that s_0, t_0 now maps to X, Y, Z.

q.e.d Lemma

By applying a $\mathrm{SL}(2, \mathbb{C})$ transformation to the f we can suppose that the triple is the image of the point $(1, 0)$.

$$\begin{aligned} f(1,0) &= a_0 = Z, \\ H(1,0) &= (a_0 a_2 - a_1^2) = Y, \\ t(1,0) &= (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) = 2X \end{aligned}$$

We now replace $f(x_1, x_2)$ by $f(x_1 + \lambda x_2, x_2)$ for an appropriate $\lambda \in \mathbb{C}$. The map $(x, y) \mapsto (x + \lambda y, y)$ has determinant 1 and preserves the value of the forms at $(1, 0)$. We specify λ as follows:

(Case I: $Z = 0$) If $Z = 0$, we have $a_1 \neq 0$ since the Klein forms do no have multiple roots. We choose λ so that $a_2 = 0$.

Since $\gcd(X, Y) = 1$ we have $X, Y, Z = \pm 1, -1, 0$. This means we can assume $a_0, a_1, a_2 = 0, \pm 1, 0$.

(Case II: $Z \neq 0$) If $Z \neq 0$ we can choose λ so that a_1 takes on an arbitrary value.

In all cases, we use that fact that $\gcd(Y, Z) = \gcd(X, Y, Z) = 1$ to choose $a_1 \equiv -\frac{X}{Y}$ modulo Z^r. For any prime dividing Z let $\nu(x) = \nu_p(x)$ and $\nu^*(x) = \nu(x)/\nu(Z)$. From the formula $H(1, 0) = Y$:

$$a_0 a_2 \equiv Y + (\frac{X}{Y})^2 = -\frac{dZ^r}{Y^2}$$

From the formula $t(1, 0) = 2X$:

$$a_0^2 a_3 \equiv -X\frac{X^2 + Y^3}{Y^3} = \frac{-dXZ^r}{Y^3}$$

This shows that $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ and that for primes dividing Z:

$$\nu^*(a_0) = 1, \quad \nu^*(a_1) = 0, \quad \nu^*(a_2) \geq r - 1, \quad \nu^*(a_3) \geq r - 2$$

3.3.1 Tetrahedron

The relations We have the $\tau_4(f) = 0$ and $j(f) = 4d$:

$$\begin{aligned} 0 &= a_0 a_4 - 4a_1 a_3 + 3a_2^2 \\ 4d &= a_0 a_2 a_4 + 2a_1 a_2 a_3 - a_2^3 - a_0 a_3^2 - a_1^2 a_4 \end{aligned}$$

(Case I: $Z = 0$) Since $a_0, a_1, a_2 = 0, \pm 1, 0$, the relations in section 3.3.1 imply that:

$$[a_0, a_1, \ldots a_4] = [0, \pm 1, 0, 0, -4d]$$

(Case II: $Z \neq 0$) We already have that $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ and for primes dividing Z that:

$$\nu^*(a_0) = 1, \quad \nu^*(a_1) = 0, \quad \nu^*(a_2) \geq 2, \quad \nu^*(a_3) \geq 1$$

so $\tau_4(f) = 0$ implies that $a_4 \in \mathbb{Z}$ also.

3.3.2 Octahedron

The relations Let $\tau_4(f) = \sum_{i=0}^{4} D_i x_1^{4-i} x_2^i$. Using PARI we get the following relations from the first four coefficients:-

$$\begin{aligned} D_0/1:0 &= a_4 a_0 - 4a_3 a_1 + 3a_2^2 \\ D_1/2:0 &= a_5 a_0 - 3a_4 a_1 + 2a_3 a_2 \\ D_2/1:0 &= a_6 a_0 - 9a_4 a_2 + 8a_3^2 \\ D_3/2:0 &= a_6 a_1 - 3a_5 a_2 + 2a_4 a_3 \end{aligned}$$

The relationship $\tau_6(f) = 72d$ means:

$$72d = a_6 a_0 - 6a_5 a_1 + 15a_4 a_2 - 10a_3^2$$

(Case I: $Z = 0$) Since $a_0, a_1, a_2 = 0, \pm 1, 0$, the relations in section 3.3.2 imply that:

$$[a_0, a_1, \ldots a_6] = [0, \pm 1, 0, 0, 0, \mp 12d, 0]$$

(Case II: $Z \neq 0$) We already have that $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ and for primes dividing Z that:

$$\nu^*(a_0) = 1, \quad \nu^*(a_1) = 0, \quad \nu^*(a_2) \geq 3, \quad \nu^*(a_3) \geq 2$$

Going through the coefficients of D gives:

$$\begin{aligned} D_0 = 0 &\implies \nu^*(a_4) \geq 1 \\ D_1 = 0 &\implies \nu^*(a_5) \geq 0 \\ D_2 = 0 &\implies \nu^*(a_6) \geq 3 \end{aligned}$$

(due to the disappearance of an $a_1 a_5$ term in D_2)

Since the relations also show that only primes p dividing Z will occur in the denominators of the a_i we have that $a_i \in \mathbb{Z}$.

3.3.3 Icosahedron

The relations Let $\tau_4(f) = \sum_{i=0}^{16} D_i x_{16-i} x_2^i$. Using PARI we get the following relation from the first 10 coefficients:

$$\begin{aligned}
D_0/1: \ 0 &= a_0a_4 - 4a_1a_3 + 3a_2^2 \\
D_1/8: \ 0 &= a_0a_5 - 3a_1a_4 + 2a_2a_3 \\
D_2/4: \ 0 &= a_0(7a_6) - 12a_1a_5 - 15a_2a_4 + 20a_3^2 \\
D_3/56: \ 0 &= a_0a_7 - 6a_2a_5 + 5a_3a_4 \\
D_4/14: \ 0 &= 5a_0a_8 + 12a_1a_7 - 6a_2(7a_6) - 20a_3a_5 + 45a_4^2 \\
D_5/56: \ 0 &= a_0a_9 + 6a_1a_8 - 6a_2a_7 - 4a_3(7a_6) + 27a_4a_5 \\
D_6/28: \ 0 &= a_0a_{10} + 12a_1a_9 + 12a_2a_8 - 76a_3a_7 - 3a_4(7a_6) + 72a_5^2 \\
D_7/8: \ 0 &= a_0a_{11} + 24a_1a_{10} + 90a_2a_9 - 130a_3a_8 - 405a_4a_7 + 60a_5(7a_6) \\
D_8/1: \ 0 &= a_0a_{12} + 60a_1a_{11} + 534a_2a_{10} + 380a_3a_9 - 3195a_4a_8 - 720a_5a_7 + 60(7a_6)^2 \\
D_9/8: \ 0 &= a_1a_{12} + 24a_2a_{11} + 90a_3a_{10} - 130a_4a_9 - 405a_5a_8 + 60(7a_6)a_7
\end{aligned}$$

Furthermore using that $D_4 = D_3 = D_2 = 0$ we can express a_8 in terms of $a_0 \dots a_5$. We call this expression D_4^*:

$$D_4^*: \ a_0^3a_8 = 12a_4a_3a_1a_0 + 18a_4a_2^2a_0 - 24a_3^2a_2a_0 + 4a_5a_3a_0^2 - 9a_4^2$$

We also have $7\tau_6(f) - 360df = 0$. Using PARI, the x_1^{12} and $x_1^{11}x_2$ terms give the following relations:

$$\begin{aligned}
R_0/1: \ 360da_0 &= a_0(7a_6) - 42a_5a_1 + 105a_4a_2 - 70a_3^2 \\
R_1/6: \ 720da_1 &= 7a_7a_0 - 5a_1(7a_6) + 63a_5a_2 - 35a_4a_3
\end{aligned}$$

(Case I: $Z = 0$) Since $a_0, a_1, a_2 = 0, \pm 1, 0$, the relations in section 3.3.3 imply that:

$$[a_0, a_1, \dots a_{12}] = [0, \pm 1, 0, 0, 0, 0, -\frac{144d}{7}, 0, 0, 0, 0, \mp(144d)^2, 0]$$

(Case II: $Z \neq 0$) We already have that $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ and for primes dividing Z that:

$$\nu^*(a_0) = 1, \quad \nu^*(a_1) = 0, \quad \nu^*(a_2) \geq 4, \quad \nu^*(a_3) \geq 3$$

Going through the relations (using the fact that the a_6 only occur in the form $7a_6$) gives:

$$\begin{aligned}
D_0 = 0 &\implies \nu^*(a_4) \geq 2 \\
D_1 = 0 &\implies \nu^*(a_5) \geq 1 \\
D_2 = 0 &\implies \nu^*(7a_6) \geq 0 \\
D_3 = 0 &\implies \nu^*(a_7) \geq 4 \\
D_4^* = 0 &\implies \nu^*(a_8) \geq 3 \\
D_5 = 0 &\implies \nu^*(a_9) \geq 2 \\
D_6 = 0 &\implies \nu^*(a_{10}) \geq 1 \\
D_7 = 0 &\implies \nu^*(a_{11}) \geq 0 \\
D_9 = 0 &\implies \nu^*(a_{12}) \geq 3
\end{aligned}$$

Since the relations also show that only primes p dividing Z will occur in the denominators of the a_i (resp. $7a_6$) we have that Ω_5 consists of integers.

q.e.d Proof of Theorem 3.2

3.4 Uniqueness of Lifts

Fix $r \in \{3,4,5\}$ and d a non zero integer. For a given $f \in \mathbb{X}_r \cap \mathcal{C}(r,d)$ define $\Upsilon(f) \subset \mathbb{Z}^3$ to be the set of relatively prime integers X, Y, Z which occur by specializing the parameterization $t(f)/2, H(f), f$ to integers.

Theorem 3.5 *Suppose $f_1, f_2 \in \mathbb{X}_r \cap \mathcal{C}(r,d)$. Suppose $(X,Y,Z) \in \Upsilon(f_1)$. Then:*

$$\begin{aligned} (X,Y,Z) \in \Upsilon(f_2) &\implies f_1 \text{ is } SL(2,Z) \text{ equivalent to } f_2 \\ (-X,Y,Z) \in \Upsilon(f_2) &\implies f_1 \text{ is } SL(2,Z) \text{ equivalent to } f_2(x_1,-x_2) \end{aligned}$$

In particular the $\Upsilon(f_i)$ are either equal or disjoint.

Proof. Suppose $(X,Y,Z) \in \Upsilon(f_1)$. We will show that f_1 is $\mathrm{SL}(2,\mathbb{Z})$ equivalent an f whose coefficients are determined totally by (X,Y,Z). This means that f_2 will also be equivalent to f if $(X,Y,Z) \in \Upsilon(f_2)$ and the first claim will follow.

Since $f_1 \in \mathbb{X}_r[x_1,x_2]$ we have $f_1, H(f_1) \in \mathbb{Z}[x_1,x_2]$ so the integer parameters s_1, s_2 witnessing the specialization:

$$f_1(s_1,s_2) = Z, \quad H(f_1)(s_1,s_2) = Y, \quad t(f_1)(s_1,s_2) = 2X$$

are relatively prime. Therefore there is an $A \in \mathrm{SL}(2,\mathbb{Z})$ such that $A(1,0)^T = (s_1,s_2)^T$. Replacing f_1 by $f_1 \circ A$ we can assume that the specialization is at $(1,0)$. We now show that f is uniquely determined up to $(x_1,x_2) \mapsto (x_1 + nx_2, x_2), n \in \mathbb{Z}$.

(Case I : $Z = 0$) We must have $(X,Y,Z) = (\pm 1, -1, 0)$ and so $a_0 = 0, a_1 = \mp 1$. By replacing $f_1(x_1,x_2)$ by $f_1(x_1 + nx_2, x_2)$ for a suitable integer n we can also assume that $a_2 = 0$ or 1. Since the leading term of $\tau_4(f)$ is $a_0a_4 - 4a_1a_3 + 3a_2^2$ and $a_0, \ldots a_4 \in \mathbb{Z}$ we must have $a_2 = 0$. The remaining a_i are now completely determined by the various relations given in section 3.1.

(Case II : $Z \neq 0$) We have $a_0 = Z$. Since the leading term of $\tau_4(f)$ is $a_0a_4 - 4a_1a_3 + 3a_2^2$, we have that a_2 is even if a_0 is even. This plus $H(f)(1,0) = Y$ and $t(f)(1,0) = 2X$ imply that $a_1 \equiv -\frac{X}{Y}$ modulo Z. By replacing $f(x_1,x_2)$ by $f(x_1 + nx_2, x_2)$ for a suitable integer n we can assume $0 \leq a_1 < |Z|$. This determines a_1. a_2 is now determined from $H(f)(1,0) = Y$, after which a_3 by $t(f)(1,0) = 2X$. The remaining a_i are now completely determined by the various relations given in section 3.1.

The first of the 2 claims is now proven.

For the second claim, take any $A \in \mathrm{GL}(2,\mathbb{Z})$ with determinant -1. Let $f' = f \circ A$. Since the f, H, t have weights $0, 2, 3$ respectively we get that:

$$(\frac{1}{2}t(f'), H(f'), f') = (-\frac{1}{2}t(f) \circ A, H(f) \circ A, f \circ A)$$

and the second claim follows from the first.

q.e.d

4 Properties of Real Klein Forms

In this section we examine Klein forms $f \in \mathcal{C}(r) \cap \mathbb{R}[x_1, x_2]$. By the characterization of $\mathcal{C}(r,d)$ this implies that $f \in \mathcal{C}(r,d)$ for some $d \in \mathbb{R}^*$.

Theorem 4.1 *All real Klein forms in the same $\mathcal{C}(r,d)$ have the same signature. In fact:*

Case	*Signature of real forms*
$r = 3$	$(2, 1)$
$r = 4, d > 0$	$(2, 2)$
$r = 4, d < 0$	$(4, 1)$
$r = 5$	$(4, 4)$

Furthermore if f, f' are real Klein forms with the same signature then f is $GL(2, \mathbb{R})$ equivalent to $\pm f'$.

This theorem will be proved in this section.

4.2 Preamble

Stereographic projection produces a 1-1 correspondence between the Riemann Sphere $S_2(\mathbb{R})$ and the extended complex plane $\mathbb{P}^\infty$. It take circles to circles if we agree that straight line are also circles passing through ∞ on $\mathbb{P}^\infty$. Furthermore we can join points on the sphere by edges and see what happens under this projection. We get a similar graph of points and edges, albeit slightly deformed, so the concepts of adjacency, paths, path length, being inside/outside a closed loop e.t.c. are preserved.

Any $\mathrm{GL}(2, \mathbb{C})$ matrix induces a bijective action on $\mathbb{P}^\infty$ which takes circles to circles. $\mathrm{GL}(2, \mathbb{C})$ is path connected, in the sense that any matrix can be gradually deformed until it becomes the identity. The induced action can therefore be gradually deformed until it is the identity. This means that the graph theoretic properties mentioned above are invariant under $\mathrm{GL}(2, \mathbb{C})$ actions.

4.3 Some lemmas about circles

Lemma 4.4 *Take $2n$ distinct points, symmetric about the real axis, none of which is on the real axis and not all on a single vertical line. Then there is a finite circle:*

- *with its center on the real axis*
- *with all $2n$ points on or inside the circle.*
- *with at least 4 of the points on the circumference*

Proof. Wlog each vertical line contains at most 2 points and the right most points $\beta, \bar{\beta}$ lie on the imaginary axis. Consider the circle thru $(0, t), \beta, \bar{\beta}$ for $t \in \mathbb{R}^{>0}$. For small t it contains all $2n$ points. For large t only 2. Somewhere in between it witnesses the claim of the lemma. (note this is not necessarily a circle of smallest radius containing all points).

q.e.d

Lemma 4.5 . *Take 6 distinct points, symmetric about the real axis. If there is a circle through exactly 5 points then one of these points is on the real line and the circle passes thru it.*

Let μ be the number of points on the real line. Since its even, the circle will go though one of them provided $\mu \neq 0$. We now suppose $\mu = 0$. If the circle does not go thru β, remove β and its reflection in the real axis $\bar{\beta}$. The circle must go thru the remaining 2 pairs on distinct conjugate points. It is therefore a vertical line or a circle with center on the real line. It therefore passes thru an even number of the original 6 points. Contradiction.

q.e.d

4.6 Number of Real Roots

Proposition 4.7 *Any real tetrahedral form has exactly* 2 *real roots*

Proof. There are no circles on the tetrahedron containing 4 vertices, so there can be no circles on the extended complex plane containing all 4 roots of a tetrahedron form. The roots cannot then all lie on the extended real line since this is considered a circle. Neither can they by Lemma 4.4 occur as 2 pairs of complex conjugate roots. Therefore a real tetrahedral form has exactly 2 real roots.

q.e.d

Proposition 4.8 *Any real octahedral form has exactly* 2 *or* 4 *real roots*

Proof. The circles on the octahedron contain at most 4 vertices. Furthermore the circles with 4 have 1 additional vertex inside and one outside. An octahedral form cannot have 6 real roots (too many roots on the extended real line). If it had 3 pairs of complex conjugate roots then by Lemma 4.4 we could draw a circle thru 4 of these roots with the remaining 2 points inside. Contradiction. A real octahedral form has therefore exactly 2 or 4 real roots.

q.e.d

Proposition 4.9 *Any real icosahedral form has exactly* 4 *real roots*

Proof. The circles on the icosahedron contain at most 5 vertices. Therefore a real icosahedral form has $\mu = 0, 2$ or 4 real roots.

Suppose $\mu = 0$ then it has 6 pairs of complex conjugate roots. Then by Lemma 4.4 there is a circle through 4 roots with 8 on the inside. Circles thru 4 vertices on the icosahedron always have 4 vertices on each side. Contradiction.

Suppose $\mu = 2$ so there are 5 pairs of complex conjugate roots and 2 real roots. Then by Lemma 4.4 there is a large circle C through 4 of the complex roots the remaining 6 complex roots inside the circle. If we are not going to get the same problem as with $\mu = 0$, the circle must pass thru 5 roots - i.e. one of the real roots also lies on it. Circles on the icosahedron thru 5 vertices 5-circles occur in non intersecting pairs. These split $\mathrm{S}_2(\mathbb{R})$ into 3 distinct regions with exactly 2 regions being non adjacent. There is one additional vertex in each of the non adjacent regions. In particular a 5-circle has 1 vertex on one side and 6 on the other. The remaining real root of f must therefore lie outside the circle C and another 5 circle C' must pass thru exactly 5 of the complex conjugate roots inside C. This is a contradiction by Lemma 4.5.

A real icosahedral form therefore has exactly 4 real roots.

q.e.d

4.10 $\mathrm{GL}(2, \mathbb{R})$ equivalence

Proposition 4.11 *If f, f' are two real tetrahedral Klein forms then f is $GL(2, \mathbb{R})$ equivalent to $\pm f'$.*

Proof. Wlog $f = \tilde{f}_3$. Let $f' = f \circ g$ some $g \in \mathrm{GL}(2, \mathbb{C})$. Replacing g by a multiple of $R \circ g$ where R corresponds to a rotation of the tetrahedron, we can suppose that g maps the 2 real roots of f to the 2 real roots of f'.

Take f and map the 2 real roots via $\mathrm{GL}(2, \mathbb{R})$ to $0, \infty$. Do the same to f'. The two forms now differ by an action which fixes 0 and ∞. The only such actions are rotation and expansion. Since the complex roots are conjugate, the rotation must be thru 0 or π. The whole action is then $\mathrm{GL}(2, \mathbb{R})$ and the result follows.

q.e.d

Proposition 4.12 *If f, f' are two real octahedral Klein forms with the same number of real roots then f is $GL(2,\mathbb{R})$ equivalent to $\pm f'$.*

Proof. If there are 4 real roots they all lie on the real line so we can choose 2 corresponding to opposite vertices on the octahedron. If there are 2 real roots, there is a circle passing through the 4 complex roots, so the real roots are 'opposite vertices'. Take f and map 2 opposite real roots via $\mathrm{GL}(2,\mathbb{R})$ to $0, \infty$. Rotating the octahedron through $\pi/2$ around the axis through the opposite vertices permutes permutes the remaining vertices cyclically. There must be a similar action on the $\mathbb{P}^\infty$ fixing $0, \infty$. This must be rotation about the origin thru $\pi/2$. The remaining roots must line on a circle center the origin which we can assume has radius 1. Since the form is still real the roots must be $\pm 1, \pm i$ if there are 4 real roots, or $\frac{1}{\sqrt{2}}(\pm 1 \pm i)$ if there are 2 real roots.

Do the same to f'. Both real forms have been $\mathrm{GL}(2,\mathbb{R})$ reduced to a form with the same roots. The result follows.

q.e.d

Corollary 4.13 *Let $f \in \mathcal{C}(4,d)$ have real roots. If $d > 0$ then f has 4 real roots. If $d < 0$ it has 2 real roots.*

By Proposition 4.8, f has either 2 or 4 real roots. By Proposition 4.12, $\pm f$ must be $\mathrm{GL}(2,\mathbb{R})$ equivalent to $\tilde{f}_4$ if it has 4 real roots, or $\tilde{f}_4^*$ if it has only 2. The result now follows from equations (3,4) and Lemma 2.8.

q.e.d

Proposition 4.14 *If f, f' are two real icosahedral Klein forms then f is $GL(2,\mathbb{R})$ equivalent to $\pm f'$.*

Proof. Wlog $f = \tilde{f}_5$. Let $f' = f \circ g$ some $g \in \mathrm{GL}(2,\mathbb{C})$. Replacing g by a multiple of $R \circ g$ where R corresponds to a rotation of the icosahedron, we can suppose that g maps the 4 real roots of f to the 4 real roots of f'.

Let $\alpha_0 = g^{-1}0$, $\alpha_\infty = g^{-1}\infty$. Take f' and map these 2 real roots via $\mathrm{GL}(2,\mathbb{R})$ to $0, \infty$. The two forms now differ by an action which fixes 0 and ∞.

The only such actions are rotation and expansion. Since the there is a circle center the origin containing exactly 5 roots of $\tilde{f}_5$ spaced equally, the rotation can only be thru 0 or π. The whole action on the roots is then $\mathrm{GL}(2,\mathbb{R})$ and the result follows.

q.e.d

5 Hermite Reduction Theory

Hermite reduction theory is a generalization of the reduction theory of positive definite real binary forms. In the latter theory, we say that a form is reduced if the unique root z_0 in $\mathbb{H}$ is in the usual fundamental domain for $\mathrm{SL}(2,\mathbb{Z})$. Every form is $\mathrm{SL}(2,\mathbb{Z})$ equivalent to some reduced form, and there is a bound for the coefficients of reduced forms in terms of the discriminant.

Hermite reduction theory applies to higher order forms. The Hermite determinant takes the place of the discriminant. There is an associated representative point $z_0 \in \mathbb{H}$ - usually unique. A form is reduced if z_0 in $\mathbb{H}$ is in the usual fundamental domain for $\mathrm{SL}(2,\mathbb{Z})$. Every form is $\mathrm{SL}(2,\mathbb{Z})$ equivalent to some reduced form, and there is a bound for the coefficients of reduced forms in terms of the Hermite determinant.

5.1 Definition of the Hermite Determinant

Take a form $f \in \mathbb{R}[x_1, x_2]$ of degree k with roots $(\mu_i; \nu_i) \in \mathbb{P}_1(\mathbb{C})$. Then:

$$f = A \prod_i (\nu_i x_1 - \mu_i x_2)$$

for some $A \in \mathbb{C}^*$. For $t_i \in \mathbb{R}^*$ define $\varphi = \varphi(\overrightarrow{t})$ by:

$$\varphi = \sum_{i=1}^{k} t_i^2 (\nu_i x_1 - \mu_i x_2)(\bar{\nu}_i x_1 - \bar{\mu}_i x_2)$$

This is a real quadratic form, and real values of x_1, x_2 with $(x_1, x_2) \neq (0, 0)$ give positive values of φ. So φ is a positive definite quadratic form for all t_i. Let δ be its determinant. I.e. if $\varphi = Px_1^2 - 2Qx_1x_2 + Rx_2^2$ then $\delta = PR - Q^2$.

For a fixed set of representatives μ_i, ν_i for the roots of f define:

$$\Psi(\overrightarrow{t}) := \frac{|A|^2 \delta^{k/2}}{(\prod t_i)^2}$$

Definition 5.2 (Hermite Covariant) *For our form $f \in \mathbb{R}[x_1, x_2]$ and any $z \in \mathbb{C}$ define:*

$$\Theta(f, z) := \begin{cases} \min \Psi(\overrightarrow{t}) & \text{over all } \overrightarrow{t} \text{ s.t. } \varphi(z) = 0 \\ \infty & \text{if } \varphi(z) = 0 \text{ for all } \overrightarrow{t} \end{cases}$$

The use of the minimum ensures that $\Theta(f, z)$ is independent of the representatives for the roots and so is a well defined function of f and z. Since the quadratic form φ is always real and positive definite it is often convenient to assume $z \in \mathbb{H}$.

Definition 5.3 (Hermite Determinant) *For any form $f \in \mathbb{R}[x_1, x_2]$:*

$$\Theta(f) := \min_{z \in \mathbb{H}} \Theta(f, z)$$

Definition 5.4 (Representative Point) *For any form $f \in \mathbb{R}[x_1, x_2]$ a Representative Point is any $z \in \mathbb{H}$ such that $\Theta(f, z) = \Theta(f)$.*

5.5 Covariant Properties

Theorem 5.6 *Let $f \in \mathbb{R}[x_1, x_2]$ be homogeneous of order k. Let $M \in GL(2, \mathbb{R})$ have determinant Δ. Then:*

$$\Theta(f \circ M, z) = |\Delta|^k \Theta(f, Mz)$$

Write f, φ, ν, μ be as above. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R})$ with determinant Δ. Define:

$$\begin{aligned} f' &:= f \circ M \\ \varphi' &:= \varphi \circ M \\ \nu', \mu' &:= a\nu_i - c\mu_i, -b\nu_i + d\mu_i \end{aligned}$$

We have:

$$\begin{aligned} f' &= A \prod_i (\nu_i' x_1 - \mu_i' x_2) \\ \varphi' &= \sum_{i=1}^{k} t_i^2 (\nu_i' x_1 - \mu_i' x_2)(\bar{\nu}_i' x_1 - \bar{\mu}_i' x_2) \end{aligned}$$

and the discriminant δ' of φ' satisfies:

$$\delta' = |\Delta|^2 \delta$$

If we choose ν_i', μ_i' to represent the roots of f'. This gives:

$$\begin{aligned} \varphi'(z) &= \varphi(Mz) \\ \Psi(f', \overrightarrow{t}) &= |\Delta|^k \Psi(f, \overrightarrow{t}) \end{aligned}$$

The result follows.

q.e.d

Corollary 5.7 *If $f' = f \circ M$ for some $M \in GL(2, \mathbb{R})$ of determinant Δ. Then:*

$$\Theta(f') = |\Delta|^k \Theta(f)$$

5.8 Calculating the Hermite Determinant I

In Julia's work [Ju17], he gives formulae for the representative point and Hermite determinant of all real biquadratic forms with distinct roots all of which are finite. We quote his results for finding the representative point.

If the signature of a real form is (r, s) then it will have real roots $\alpha_1, \ldots \alpha_s$ and pairs of complex conjugate roots $\beta_1, \bar{\beta}_1, \ldots \beta_s, \bar{\beta}_s$. Using the AM/GM inequality you can show that the weight factors (t_i^2) at complex conjugate roots causing the Hermite determinant to be attained can be assumed to be equal. We therefore use the naming convention that the weights assigned to the real roots are $t_1^2, \ldots t_r^2$, and those assigned to the complex roots are $u_1^2, u_1^2, \ldots u_s^2, u_s^2$.

Proposition 5.9 (4 Real Roots) *Suppose f has 4 distinct real roots α_i all finite. Then weights t_i, which cause the Hermite determinant to be attained are given by:*

$$t_i^2 = \frac{1}{|f'(\alpha_i, 1)|}$$

where f' denotes the derivative of f with respect to x_1.

Proof. See [Ju17, p 59].

Proposition 5.10 (2 Real Roots) *Suppose f has 2 distinct real roots α_1, α_2, both finite, and a complex root $\beta \in \mathbb{H}$. Then weights t_1, t_2, u_1 which cause the Hermite determinant to be attained are given by:*

$$\begin{aligned} t_1^2 &= |\beta - \bar{\beta}||\alpha_2 - \beta|^2 \\ t_2^2 &= |\beta - \bar{\beta}||\alpha_1 - \beta|^2 \\ u_1^2 &= |\alpha_1 - \alpha_2||\alpha_1 - \beta||\alpha_2 - \beta| \end{aligned}$$

Proof. See [Ju17, p 57].

Proposition 5.11 (0 Real Roots) *Suppose f has 2 distinct complex roots $\beta_1, \beta_2 \in \mathbb{H}$. Then weights u_1, u_2 which cause the representative point to be attained are given by:*

$$\begin{aligned} u_1^2 &= |\beta_2 - \bar{\beta}_2| \\ u_2^2 &= |\beta_1 - \bar{\beta}_1| \end{aligned}$$

Proof. See [Ju17, p 48].

5.12 Calculating the Hermite Determinant II

In this section we reference some results in a paper by Stoll/Cremona [SC00] which give us additional tools for finding the representative point and calculating the Hermite determinant.

Proposition 5.13 *Suppose f is a real form of order $k \geq 3$ with distinct roots then its representative point in $\mathbb{H}$ is unique.*

Proof. Clearly we can assume the roots are finite. This is now [SC00, Prop 3.4].

Proposition 5.14 *Suppose $f = A\prod_i(\nu_i x_1 - \mu_i x_2)$ is a real form of order $k \geq 3$ with k distinct roots. Let $(t,u) \in \mathbb{R} \times \mathbb{R}_+$. Then $t+ui \in \mathbb{H}$ is the representative point iff:*

$$\begin{aligned} \sum_{j=1}^{k} \frac{|\nu_j u|^2}{|\nu_j t - \mu_j|^2 + |\nu_j u|^2} &= \frac{k}{2} \\ \sum_{j=1}^{k} \frac{|\nu_j|^2 t - \Re(\overline{\nu_j}\mu_j)}{|\nu_j t - \mu_j|^2 + |\nu_j u|^2} &= 0 \end{aligned}$$

The associated t_j are given up to a multiplicative constant by:

$$t_j^2 = \frac{|\nu_j u|^2}{|\nu_j t - \mu_j|^2 + |\nu_j u|^2}$$

Proof. When all the roots are finite this is [SC00, Prop 3.4]. When there is a root at ∞ use a limiting process.

q.e.d

Proposition 5.15 *Let f be as in Proposition 5.14. Define:-*

$$\widetilde{F}(t,u) = |A|^2 \prod_{j=1}^{k} \left(|\nu_j t - \mu_j|^2 + |\nu_j u|^2\right)$$

This is well defined. Then $t+ui \in \mathbb{H}$ is a representative point iff (t,u) is a minimizing point (in $\mathbb{R} \times \mathbb{R}_+$) of the function:

$$(t,u) \mapsto \frac{\widetilde{F}(t,u)}{u^k}$$

Moreover, the Hermite determinant $\Theta(f)$ is then:

$$\Theta(f) = \left(\frac{k}{2}\right)^k \min_{(t,u)} \frac{\widetilde{F}(t,u)}{u^k}$$

Proof. If the roots are all finite this is [SC00, Prop 3.5]. (Note: the definition of the Hermite determinant in [SC00] is 2^k bigger than ours - hence the extra factor $(\frac{1}{2})^k$ here). When there is a root at ∞ use a limiting process.

q.e.d

5.16 Application to Klein Forms

Theorem 5.17 *The real Klein forms $\tilde{f}_3, \tilde{f}_4, \tilde{f}_4^*, \tilde{f}_5$ all have representative point i. They have Hermite determinant $575, 2^4 3^6, 2^4 3^6, 6^{12} 5^5$. Furthermore i is also:*

- *the location of the unique complex root of $\tilde{f}_4$ in $\mathbb{H}$.*
- *the representative point of 'the' form defined by the 4 complex roots of $\tilde{f}_4^*$*
- *the representative point of 'the' form defined by the 4 real roots of $\tilde{f}_5$*

This theorem will be proved in the following sections. Assuming the truth of the theorem we get the following corollaries.

Corollary 5.18 *All real $f \in \mathcal{C}(r,d)$ have the same Hermite determinant. Its value is given by:*

Class	$\Theta(f)$
$\mathcal{C}(3,d)$	$2^6 3^3 \lvert d\rvert^{2/3}$
$\mathcal{C}(4,d)$	$2^8 3^9 \lvert d\rvert$
$\mathcal{C}(5,d)$	$2^{24} 3^{18} 5^5 \lvert d\rvert^2$

Proof. Proof. If $f \in \mathcal{C}(r,d) \cap \mathbb{R}[x_1, x_2]$ then by the results of section 4.10, $\pm f = \tilde{f} \circ M$ where $M \in \mathrm{GL}(2,\mathbb{R})$ and $\tilde{f} = \tilde{f}_3, \tilde{f}_4, \tilde{f}_4^*, \tilde{f}_5$ depending on which of the cases we are in. By Corollary 5.7 and the results of section 2.5

$$\begin{aligned} \Theta(f) &= |\det(M)|^k \Theta(\tilde{f}) \\ \det(M)^6 &= \beta_r |d| \end{aligned}$$

The result follows.

q.e.d

Corollary 5.19 *The representative point of any $f \in \mathcal{C}(r,d)$ can be found as follows:*

Case	*Method*
$r = 3$	*Apply Julia's formula (Prop 5.10)*
$r = 4, d > 0$	*Its the unique complex root in $\mathbb{H}$*
$r = 4, d < 0$	*Construct a form from its 4 complex roots then get its representative point using Prop 5.11*
$r = 5$	*Construct a form from its 4 real roots then get its representative point using Prop 5.9*

Proof. If $f \in \mathcal{C}(r,d) \cap \mathbb{R}[x_1, x_2]$ then $\pm f = \tilde{f} \circ M$ where $M \in \mathrm{GL}(2,\mathbb{R})$ and $\tilde{f} = \tilde{f}_3, \tilde{f}_4, \tilde{f}_4^*, \tilde{f}_5$ depending on which of the 4 cases we are in. The covariant properties of the representative point under $\mathrm{GL}(2,\mathbb{R})$ transformations means that the claims are inherited from the extra properties of $\tilde{f}$ quoted in Theorem 5.17

q.e.d

5.20 Proof of Theorem 5.17

The Tetrahedron Applying Proposition 5.10, we find that $\tilde{f}_3$ has representative point i. Applying now Proposition 5.15 gives that its Hermite determinant is 576.

The Icosahedron We now use the Poincaré Disc model of the hyperbolic plane. (intuitively we go to $+i\infty$ and look at the riemann sphere side on). Rotating the disc thru π corresponds to an $\mathrm{SL}(2,\mathbb{R})$ action on $\mathbb{H}$.

This permutes the roots of $\tilde{f}_5$ in their totality, as well as the 4 real roots lying on the boundary of the disc.

By Proposition 5.13 the representative point of a form with distinct roots of order ≥ 3 is unique, so it must be a fixed point of this action. Therefore the center of the disc is the representative point of both $\tilde{f}_5$ and the form constructed from its 4 real roots.

The center of the disc corresponds on $\mathbb{H}$ to i. The roots of $\tilde{f}_5$ are $0, \infty$ and $r_i\epsilon^j$ where ϵ is a primitive 5th root of unity and:

$$r_1 = \frac{-1+\sqrt{5}}{2}, \quad r_2 = \frac{1+\sqrt{5}}{2}$$

We can now apply prop 5.15 to give:

$$\Theta(\tilde{f}_5) = \left(\frac{12}{2}\right)^{12} (r_1^2+1)^5(r_2^2+1)^5 = 6^{12}5^5$$

The Octahedron We again use the Poincaré Disc model of the hyperbolic plane. For both $\tilde{f}_4$ and $\tilde{f}_4^*$ rotating the disc thru π corresponds to an $\mathrm{SL}(2,\mathbb{R})$ action on $\mathbb{H}$.

This permutes the roots of $\tilde{f}$ in their totality, as well as the real roots lying on the boundary of the disc.

By Proposition 5.13 the representative point of a form with distinct roots of order ≥ 3 is unique, so it must be a fixed point of the action. Therefore the center of the disc is the representative point of both $\tilde{f}_4$ and $\tilde{f}_4^*$, as well as the form defined by the 4 complex roots of $\tilde{f}_4^*$. It is also the location of the unique complex root of $\tilde{f}$ in the upper half plane.

The center of the disc corresponds on $\mathbb{H}$ to i. Both $\tilde{f}_4, \tilde{f}_4^*$ have roots at $0, \infty$ and 4 roots on the circle $\{|z| = 1\}$. We now apply prop 5.15 to get:

$$\Theta(\tilde{f}_4) = \Theta(\tilde{f}_4^*) = \left(\frac{6}{2}\right)^6 2^4 = 3^6 2^4$$

5.21 Bounding the Coefficients

Both Julia [Ju17] and Stoll/Cremona [SC00] give bounds on the coefficients of reduced forms in terms of the Hermite determinant.

In this section I produce my own bound on the products $|a_i a_j|$. For my application, it is stronger than anything in the 2 referenced papers. This section is devoted to proving the following:

Theorem 5.22 *Suppose*

$$f = \sum_{i=1}^{k} \binom{k}{i} a_i x_1^{k-i} x_2^i$$

is a real form of order k. Let $z \in \mathbb{H}$ and write $z = x + iy$. Then:

$$|a_r|^2 \leq \frac{|z|^{2r}}{(ky)^k}\Theta(f,z) \qquad \textit{for all } r$$

This will be proved in the next section. Assuming it is true we get the following corollaries:

Theorem 5.23 *We say that a form is Hermite reduced if its representative point is in the usual fundamental domain for $SL(2,\mathbb{Z})$. Suppose f as in Theorem 5.22 is Hermite reduced, then:*

$$|a_r a_s| \leq \left(\frac{4}{3k^2}\right)^{\frac{k}{2}} \Theta(f) \qquad \textit{whenever } r+s \leq k$$

Proof. This follows from the fact that $y \geq \frac{\sqrt{3}|z|}{2}$ in the fundamental domain.

q.e.d

5.23.1 Proof of Theorem 5.22

Set $\Theta = \Theta(f,z)$. Choose (μ_i, ν_i) to represent the roots in such a way that $f = \prod(\nu_i x_1 - \mu_i x_2)$. By the definition of Θ there is $\delta > 0$ and $t_i > 0$ s.t.:

$$f = \frac{\sqrt{\Theta}}{\delta^{\frac{k}{4}}} \prod (t_i \nu_i x_1 - t_i \mu_i x_2) \tag{5}$$

with :

$$\varphi = Px_1^2 - 2Qx_1x_2 + Rx_2^2$$

where

$$P = \sum t_i^2 |\mu_i|^2, \quad Q = \sum t_i^2 (\mu_i \bar{\nu}_i + \bar{\mu}_i \nu_i), \quad R = \sum t_i^2 |\nu_i|^2$$

a positive definite quadratic form of determinant $\delta = PR - Q^2$ which has z as a root. Writing $z = x + iy$ this means:-

$$Q = xP, \quad R = P|z|^2, \quad \delta = P^2 y^2$$

Define $b_i, c_i \in \mathbb{C}$ by:

$$\sqrt{P} b_i = \mu_i t_i, \quad \sqrt{R} c_i = -\nu_i t_i$$

Then

$$\sum |b_i|^2 = \sum |c_i|^2 = 1$$

We have :

$$a_r = \sqrt{\Theta} \Upsilon_r \Xi_r$$

where

$$\Upsilon_r = \frac{\sqrt{P}^{k-r} \sqrt{R}^r}{\delta^{\frac{k}{4}}} = \frac{|z|^r}{y^{k/2}}$$

$$\Xi_r = \binom{k}{r}^{-1} \left(\sum_{\#S=k} b_S c_{S'} \right)$$

Where S is a variable denoting a set of distinct integers in $[1,k]$, S' denote the complement of S in $[1,k]$, and

$$b_S = \prod_{i \in S} b_i$$

The theorem now follows from Lemma 5.24

q.e.d

5.23.2 A nice Inequality

Lemma 5.24 *Suppose $b_i, c_i \in \mathbb{C}$ with $\sum_1^k |b_i|^2 = \sum_1^k |c_i|^2 = 1$ then:*

$$|\sum_{\#S=r} b_S c_{S'}| \leq \left(\begin{array}{c} k \\ r \end{array} \right) \left(\frac{1}{k}\right)^{\frac{k}{2}}$$

Proof. Wlog b_i, c_i are real and non negative. By the Cauchy Schwartz inequality ([BB90][p9]) :

$$\left(\sum_S b_S c_{S'}\right)^2 \leq \left(\sum_S b_S^2\right)\left(\sum_S c_{S'}^2\right)$$

By the generalized AM/GM Inequality ([BB90][p15, exercise 22]):

$$\begin{aligned} \sum_S b_S^2 &\leq \left(\begin{array}{c} k \\ r \end{array} \right) \left(\frac{\sum_i b_i^2}{k}\right)^r \\ \sum_{S'} c_{S'}^2 &\leq \left(\begin{array}{c} k \\ r \end{array} \right) \left(\frac{\sum_i c_i^2}{k}\right)^{k-r} \end{aligned}$$

Combining these inequalities gives the result.

q.e.d

6 The Algorithm for $X^2 + Y^3 + dZ^r = 0$

This section presents the explicit algorithm. Let $r \in \{3, 4, 5\}$ and d a non-zero integer. Consider the diophantine equation:

$$X^2 + Y^3 + dZ^r = 0$$

An algorithm to produce a finite set of $\mathbb{Z}[x_1, x_2]$ solutions such that all relatively prime integer solutions occur by specializing the parameters (x_1, x_2) in one of these parameterizations to integers is:

ALGORITHM $(X^2 + Y^3 + dZ^r = 0)$
INPUT (r,d)
Produce a complete list of Hermite reduced $f \in \mathcal{C}(r, d) \cap \mathbb{X}_r$ (section 6.1)
Reduce the list down to a set of $\mathrm{GL}(2, \mathbb{Z})$ inequivalent forms (section 6.4)
Remove forms not specializing to rel.prime integers (section 6.8)
OUTPUT$(f_1, f_2, \ldots f_n)$
STOP

We arrive at a finite set of forms: $f_1, f_2 \ldots f_n$. A finite set of solutions in $\mathbb{Z}[x_1, x_2]$ with the claimed properties is given by:

$$X_i = \pm t(f_i)/2, \quad Y_i = H(f_i), \quad Z_i = f_i$$

By Theorem 3.5, this list is optimum: No f_i can be removed, and any other list includes a form $\mathrm{GL}(2, \mathbb{Z})$ equivalent to f_i.

If you do not like the $\pm$ you should add $f_i(x_1, x_2)^* := f_i(x_1, -x_2)$ to the list for every f_i whose $\mathrm{GL}(2,\mathbb{Z})$ equivalence class splits into 2 $\mathrm{SL}(2,\mathbb{Z})$ classes. Section 6.6 shows how to identify such forms. The larger list $f_1, f_2 \ldots f_m$ gives a finite set of solutions:

$$X_i = t(f_i)/2, \quad Y_i = H(f_i), \quad Z_i = f_i$$

By Theorem 3.5, this list is optimum: No f_i can be removed, and any other list includes a form $\mathrm{SL}(2,\mathbb{Z})$ equivalent to f_i.

6.1 Listing Hermite Reduced forms

For a given $r \in \{3,4,5\}$ and non zero integer d we show how to find all Hermite reduced forms in $\mathcal{C}(r,d) \cap \mathbb{X}_r$.

Theorem 6.2 *If we restrict to Hermite reduced forms inside $\mathcal{C}(r,d) \cap \mathbb{R}[x_1, x_2]$ we can suppose that $|a_r a_s|$ satisfy :*

$$\max\{|a_r a_s| \mid r + s \le k\} \le B^2$$

where the bound B is given by:

Class	B
$\mathcal{C}(3,d)$	$2\sqrt{3}\lvert d\rvert^{1/3}$
$\mathcal{C}(4,d)$	$16\sqrt{\lvert d\rvert}$
$\mathcal{C}(5,d)$	$1600\sqrt{5}\lvert d\rvert \sim 3578\lvert d\rvert$

In particular $|a_i| \le B$ for all $i \le \frac{1}{2}k$.

Proof. The bounds are gotten applying Theorem 5.23 to the Hermite determinant calculations listed in Corollary 5.18.

q.e.d

If $a_0 \neq 0$ then the coefficients are totally determined by the relations given in section 3.1 once a_1, a_2, a_3 are given. a_3 can have at most 2 possible values once a_0, a_1, a_2 are given. The values a_3 are gotten by finding the possible values of X, Y, Z when the parameterization would be specialized at $(1,0)$.

The following algorithm outputs all $f \in \mathcal{C}(r,d) \cap \mathbb{X}_r[x_1, x_2]$ whose coefficients satisfy the bounds of the theorem with $a_0 \neq 0$:

```
ALGORITHM( Bounded Solutions, a_0 ≠ 0)
    INPUT (r,d)
    Calculate B from table above
    FOR a_0, a_1, a_2 ∈ Z with |a_i| ≤ B, a_0 ≠ 0 DO
        Z := a_0, Y := a_0 a_2 − a_1^2
        FOR the at most 2 integers X := ±√(−Y^3 − dZ^r) DO
            Determine a_3 from a_0^2 a_3 − 3a_0 a_1 a_2 + 2a_1^3 = 2X
            The remaining a_4, ... a_k are determined from
                the relations in section 3.1

            IF all of Ω_r are integers
            AND the a_i satisfy the bounds of Theorem 6.2
                OUTPUT the associated parameterization
            END-IF
        END-FOR
    END-FOR
    STOP
```

If $a_0 = 0$ then $a_1 \neq 0$ and the coefficients are totally determined by the relations given in section 3.1 once a_1, a_2 are given.

ALGORITHM(Bounded Solutions, $a_0 = 0$)
INPUT (r,d)
Calculate B from table above
FOR $a_0, a_1, a_2 \in \mathbb{Z}$ with $|a_i| \leq B, a_0 = 0$ DO
The remaining $a_3, \ldots a_k$ are determined from
the relations in section 3.1
IF all of Ω_r are integers
AND the a_i satisfy the bounds of Theorem 6.2
OUTPUT the associated parameterization
END-IF
END-FOR
STOP

Running these 2 algorithms produces exactly the set of $f \in \mathcal{C}(r,d) \cap \mathbb{X}_r[x_1, x_2]$ whose coefficients satisfy the bounds in the table above. By the theorem this includes all Hermite reduced $f \in \mathcal{C}(r,d) \cap \mathbb{X}_r[x_1, x_2]$. Using corollary 5.19, we now calculate the representative point of each form. We discard forms for which the point is not in the fundamental domain.

Remark 6.3 (Implementation)

- *For practical reasons (size of list) it is wise to also discard forms if* $\gcd(\Omega_r) \neq 1$. *By Proposition 2.18, we have* $f, H(f) \in \mathbb{Z}[\Omega_r][x_1, x_2]$. *These parameterizations can never specialize to relatively prime* X, Y, Z.
- *We can speed up everything by a factor* 2 *by only taking* $a_1 \geq 0$ *in the algorithms, and changing the output statement to "OUTPUT* $f(x_1, x_2)$ *and* $f(x_1, -x_2)$*". The representative point of these forms differ by a reflection in the y-axis so they are both or neither reduced. The even coefficients are the same, their odd coefficients differ in sign.*
- *This is the computationally expensive part of the algorithm. My C program running in a* 350 *Mhz Pentium II took* 6 *hours to produce the list associated with the icosahedral equation* $X^2 + Y^3 + Z^5 = 0$.

6.4 Identifying $\mathbf{GL}(2, \mathbb{Z})$ equivalent forms

We show how to take a list of Hermite reduced forms, and reduce the list to a set of $\mathrm{GL}(2, \mathbb{Z})$ inequivalent forms.

$\mathrm{GL}(2, \mathbb{Z})$ acts on $\mathbb{C} - \mathbb{R}$. Note that conjugation acts freely on $\mathbb{C} - \mathbb{R}$ and commutes with the $\mathrm{GL}(2, \mathbb{Z})$ action. Since $\mathbb{H} = (\mathbb{C} - \mathbb{R})/ <$ conjugation $>$ it follows that $\mathrm{GL}(2, \mathbb{Z})$ acts on $\mathbb{H}$ The $\mathrm{GL}(2, \mathbb{Z})$ map $z \mapsto -z$ becomes $x + iy \mapsto -x + iy$ on $\mathbb{H}$.

A fundamental domain for $\mathrm{GL}(2, \mathbb{Z})$ is given by

$$\mathcal{D}^- := \{z = x + iy \mid |z| \geq 1, -\frac{1}{2} \leq x \leq 0\}$$

Every $z \in \mathbb{H}$ is $\mathrm{GL}(2, \mathbb{Z})$ equivalent to a unique $z \in \mathcal{D}^-$. We say that a form F is $\mathrm{GL}(2, \mathbb{Z})$ reduced if $z(F) \in \mathcal{D}^-$. We throw away all but the $\mathrm{GL}(2, \mathbb{Z})$ reduced forms.

Furthermore 2 reduced forms F_1, F_2 are $\mathrm{GL}(2, \mathbb{Z})$ equivalent iff $z(F_1) = z(F_2) =: z$ and $F_1 = F_2 \circ g$ for some $g \in \mathrm{Stab}(z) := \mathrm{Stab}(z, \mathrm{GL}(2, \mathbb{Z}))/\pm I$. The following lemma gives us a definite test of which forms are equivalent.

Lemma 6.5 *Let $i = \sqrt{-1}, \omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Suppose $z = x + iy \in \mathcal{D}^-$. Stab(z) is trivial on the interior of $\mathcal{D}^-$. On the boundary of $\mathcal{D}^-$ it is the finite group given in the table below:*

z	$Stab(z)$	$\#Stab(z)$	$z \neq i, w$	$Stab(z)$	$\#Stab(z)$
w	$< ST, US >$	6	$x = 0$	$< U >$	2
i	$< S, U >$	4	$\|z\| = 1$	$< US >$	2
			$x = -\frac{1}{2}$	$< U >$	2

where:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

6.6 When f is $\mathrm{SL}(2,\mathbb{Z})$ equivalent to $f(x_1, -x_2)$

Only listing $\mathrm{GL}(2,\mathbb{Z})$ representatives keeps our lists as short as possible. However by Theorem 3.5, every f gives us potentially two parameterizations $\pm\frac{1}{2}t(f), H(f), f$. These correspond to one or two distinct parameterization depending on whether the $\mathrm{GL}(2,\mathbb{Z})$ class of f splits into one or two $\mathrm{SL}(2,\mathbb{Z})$ classes. This can also be recognized using the representative point.

Proposition 6.7 *Let a $GL(2,\mathbb{Z})$ class be represented by f with representative point in $\mathcal{D}^-$. Let $z = x+iy$ be that point. f remains a single $SL(2,\mathbb{Z})$ class iff z is on the boundary of $\mathcal{D}^-$ and:*

$(z = \omega)$ $f(s+t, -t) = f(s,t), f(-t, s+t)$ *or* $f(s+t, -s)$

$(z = i)$ $f(x,y) = f(y,x)$ *or the odd coefficients of f are zero.*

$(z \neq i, \omega)$

- $x = 0$ *and the odd coefficients of f are zero.*
- *or* $|z| = 1$ *and* $f(x,y) = f(y,x)$
- *or* $x = -\frac{1}{2}$ *and* $f(s+t, -t) = f(s,t)$

Proof. If it is also an $\mathrm{SL}(2,\mathbb{Z})$ class, there must be an $M \in \mathrm{SL}(2,\mathbb{Z})$ so that $f \circ M = f(x_1, -x_2)$. This must map $z = x + iy \mapsto -x + iy$. The proposition enumerates the possibilities.

q.e.d

6.8 Checking we can specialize to rel.prime integers

Now we check that a given parameterization specializes somewhere to relatively prime integers. If not we can throw it away. We define Res to be the resultant of 2 forms as in [La95, IX].

Proposition 6.9 *Let $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ be two forms of orders k_1, k_2 and $M \in GL(2,\mathbb{C})$ a matrix of determinant δ. Then:*

$$Res(f_1 \circ M, f_2 \circ M) \quad = \quad \delta^{k_1 k_2} Res(f_1, f_2)$$

See [La95, IX, Cor 3.14].

Corollary 6.10 *$Res(f, H(f))$ is an invariant of the class $\mathcal{C}(r,d)$. For integer d, $Res(f, H(f)) \in \mathbb{Z}$ and for primes p:*

$$p | Res(f, H(f)) \iff p | Nd$$

where for $r = 3, 4, 5$, $N = 12, 24, 60$ as usual.

Proof. This follows by calculating $\mathrm{Res}(f, H(f))$ when $f = \tilde{f}_3, \tilde{f}_4, \tilde{f}_5$, then applying Proposition 2.9 and Proposition 6.9.

q.e.d

Proposition 6.11 *Let $f_1, f_2 \in \mathbb{Z}[x_1, x_2]$ be two forms of orders k_1, k_2. Let $R := Res(f_1, f_2) \in \mathbb{Z}$ be their resultant. Let $k = \max(k_1, k_2)$. Then there are $g_{i,j} \in \mathbb{Z}[x_1, x_2]$ such that:*

$$\begin{aligned} x_1^k R &= g_{1,1} f_1 + g_{1,2} f_2 \\ x_2^k R &= g_{2,1} f_1 + g_{2,2} f_2 \end{aligned}$$

Proof. By Proposition 6.9:

$$\mathrm{Res}(f_1(x_1, x_2), f_2(x_1, x_2)) = \pm \mathrm{Res}(f_1(x_2, x_1), f_2(x_2, x_1))$$

The result now follows from [La95, IX, Theorem 3.8].

q.e.d

We can now check whether a parameterization specializes anywhere to relatively prime integers using. The following shows that we only have to test via a finite set of parameters (s, t):-

Corollary 6.12 *Fix $r \in \{3, 4, 5\}$ and $d \in \mathbb{Z}_{\neq 0}$. Take $f \in \mathbb{X}_r \cap \mathcal{C}(r, d)$ and $s, t \in \mathbb{Z} \times \mathbb{Z}$.*

$$Z = f(s, t), \quad Y = H(f)(s, t)$$

Let $s_0 \equiv s(\mod dN)$ and $t_0 \equiv t(\mod dN)$

$$Z_0 = f(s_0, t_0), \quad Y_0 = H(f)(s_0, t_0)$$

then

$$\gcd(X, Y) = 1 \iff \gcd(s, t) = \gcd(X_0, Y_0) = 1$$

Proof. If $\gcd(s, t) = 1$, then by Proposition 6.11 the gcd of X, Y divides $\mathrm{Res}(f, H(f))$. By cor 6.10 this only contains primes dividing Nd, so it is 1 iff $\gcd(X_0, Y_0) = 1$. Conversely if $p | \gcd(s, t)$, some prime, then $p | \gcd(X, Y)$. This is because $f, H(f) \in \mathbb{Z}[x_1, x_2]$ by prop 2.18.

q.e.d

7 Generalizing to $Ax^2 + By^3 + Cz^r = 0$

Proposition 7.1 *We fix $r \in \{3, 4, 5\}$ and a non zero integer d and a finite set of primes S. There is a finite set of solutions in $\mathbb{Z}_S[x_1, x_2]$ to :*

$$x^2 + y^3 + dz^r = 0 \tag{6}$$

such that

- *their integer specializations include all integer solutions with $\gcd(X, Y, Z) \in \mathbb{Z}_S^*$*
- *their $\mathbb{Z}_S$ specializations include all $\mathbb{Z}_S$ solutions with $\gcd(X, Y, Z) \in \mathbb{Z}_S^*$.*

Proof. Fix $r \in \{3,4,5\}$ and let $N = 12, 24, 60$ as usual. Fix a parameterization $\chi = (\frac{1}{2}t(f), H(f), f)$. For any $\lambda \in \mathbb{C}$:

$$\chi(s,t) = (X,Y,Z) \iff \chi(\lambda s, \lambda t) = (\lambda^{N/2}X, \lambda^{N/3}Y, \lambda^{N/r}) \tag{7}$$

The claim about $\mathbb{Z}_S$ solutions now follows from the claim about $\mathbb{Z}$ solutions. We now assume X, Y, Z are $\mathbb{Z}$-integers. By (7) we we can also assume that the valuation of $\gcd(X^2, Y^3, Z^r)$ at any prime p is less than N.

Take a prime $p|\gcd(X,Y)$. If $p^5|dZ^r$ then :

$$X = p^3X', \quad Y = p^2Y', \quad dZ = d'(p^sZ')$$

for some $s \geq 0$ and some X', Y', Z', d' integers satisfying:

$$X'^2 + Y'^3 + d'Z'^r = 0 \tag{8}$$

In this way we can reduce to a finite set of equations in which we can assume that:

$$p|\gcd(X,Y) \implies \nu_p(Z^r) < 5$$

For $r = 5$ this is equivalent to assuming $\gcd(X,Y,Z) = 1$. For $r = 3, 4$ it is $p|\gcd(X,Y) \implies \nu_p(Z) \leq 1$.

The proofs go through producing $f \in \mathbb{Z}_S[x_1, x_2]$ with coefficients of both bounded absolute value and bounded denominator. (if $r = 5$, $f \in \mathbb{Z}[x_1, x_2]$). Hermite reduction can therefore still be used to produce the parameterizations.

q.e.d

Theorem 7.2 *Fix $r \in \{3,4,5\}$. Fix a finite set of primes S. Fix $A, B \in Z_S^*$ and non zero $C \in Z_S$. Then: There is a finite set of solutions in $\mathbb{Z}_S[x_1, x_2]$ to :*

$$Ax^2 + By^3 + Cz^r = 0 \tag{9}$$

such that

- *their integer specializations include all integer solutions with $\gcd(X,Y,Z) \in \mathbb{Z}_S^*$*
- *their $\mathbb{Z}_S$ specializations include all $\mathbb{Z}_S$ solutions with $\gcd(X,Y,Z) \in \mathbb{Z}_S^*$.*

Proof. Wlog $A, B, C \in \mathbb{Z}$. Multiply the diophantine equation by A^3B^2 to give:

$$(A^2Bx)^2 + (ABy)^3 + (A^3B^2C)z^r = 0$$

Since $A^2B, AB \in \mathbb{Z}_S^*$ the theorem follows from Proposition 7.1.

q.e.d

A Parameterizing $X^2 + Y^3 \pm Z^r$

This section gives complete parameterizations to $X^2 + Y^3 \pm Z^r$ To keep the lists as short as possible, we identify the parameterizations identifying $\pm X$. If the corresponding $\mathrm{GL}(2,\mathbb{Z})$ class of f breaks into two $\mathrm{SL}(2,\mathbb{Z})$ classes these are really 2 distinct parameterizations.

The case $r = 3$ was already done by Mordell in [Mo69][ch 25] using a syzygy from invariant theory. The cases $r = 4$ were done by Zagier and quoted in [FB98][appendix A]. The $r = 5$ case is new.

A.1 Complete Parameterization of $X^2 + Y^3 + Z^3 = 0$

Using the algorithm, we get a complete list of parameterizations:

	f	$RepresentativePoint$
$A1$	$[0,1,0,0,-4]$	$\sqrt{2}i$
$A2$	$[-1,0,0,2,0]$	$\sqrt{2}i$
$B1$	$[-2,-1,0,-1,-2]$	$-0.268+0.963i$
$B2$	$[-1,1,1,1,-1]$	$-0.268+0.963i$
$C1$	$[-1,0,-1,0,3]$	$\sqrt[4]{3}i$
$C2$	$[1,0,-1,0,-3]$	$\sqrt[4]{3}i$

In Mordell's book [Mo69] he further shortens the list by assuming that Y is odd. This means that $A1, B1$ can be omitted. However, Mordell gives 5 parameterizations: $A2, B2, C1, C2$ and $f = [-1,-2,-4,-6,0]$ According to my theory the 5th should be superfluous. It is. I calculate its representative point to be $-2+\sqrt{2}i$. This means that $f(x_1 - 2x_2, x_2)$ must be $A1$ or $A2$. It is $A2$!

Beukers [FB98][p 78] omits parameterizations gotten by interchanging Y and Z. For $f \in \mathcal{C}(3,1)$ we have $H^2(f) = f$, so that interchanging $Y \leftrightarrow Z$ is the same as swapping between $f \leftrightarrow H(f)$. The naming has been chosen so that $A2 = H(A1)$ e.t.c. Therefore a full set of parameterizations in this sense is given by $A1, B1, C1$ - the same number as given in that paper.

A.2 Complete Parameterization of $X^2 + Y^3 \pm Z^4 = 0$

These two equations were solved by Zagier, see Beukers. To keep the lists short we identify $\pm X$ and $\pm Z$. This means every parameterization in the list is shorthand for $\pm f(x_1, \pm x_2)$. The first $\pm$ is the $\pm Z$.

A.2.1 $X^2 + Y^3 + Z^4 = 0$

Now applying the algorithm gives 4 parameterizations:

	f	Representative Point
f_1	$[0,1,0,0,0,-12,0]$	$1.86i$
f_2	$[0,3,0,0,0,-4,0]$	$1.07i$
f_3	$[-1,0,1,0,3,0,-27]$	$1.73i$
f_4	$[-3,-4,-1,0,1,4,3]$	$-0.268+0.964i$

In Beukers, we also have 4 parameterizations: f_1, f_2, f_3 and a 4th one involving denominators

A.2.2 $X^2 + Y^3 - Z^4 = 0$

Now applying the algorithm gives 7 parameterizations:

	f	Representative Point
f_1	$[0,1,0,0,0,12,0]$	$1.86i$
f_2	$[0,3,0,0,0,4,0]$	$1.07i$
f_3	$[-1,0,0,2,0,0,32]$	$1.78i$
f_4	$[-1,0,-1,0,3,0,27]$	$1.73i$
f_5	$[-1,1,1,1,-1,5,17]$	$-0.158+1.50i$
f_6	$[-5,-1,1,3,3,3,9]$	$-0.436+1.01i$
f_7	$[-7,-1,2,4,4,4,8]$	ω

Beukers gives 6 parameterizations: $f_1, \ldots f_6$. This means that the list there is incomplete, since the minimality property proven in section 6 shows that f_7 cannot be dropped!

A.3 Complete Parameterization of $X^2 + Y^3 + Z^5$

The $2, 3, 5$ case is new. Beukers was able to produce parameterizations, though his method was unable to produce a complete set. If we identify $\pm X$, the algorithm produces the following complete set:

$$
\begin{aligned}
f_1 &= [0,1,0,0,0,0,-144/7,0,0,0,0,-20736,0] \\
f_2 &= [-1,0,0,-2,0,0,80/7,0,0,640,0,0,-102400] \\
f_3 &= [-1,0,-1,0,3,0,45/7,0,135,0,-2025,0,-91125] \\
f_4 &= [1,0,-1,0,-3,0,45/7,0,-135,0,-2025,0,91125] \\
f_5 &= [-1,1,1,1,-1,5,-25/7,-35,-65,-215,1025,-7975,-57025] \\
f_6 &= [3,1,-2,0,-4,-4,24/7,16,-80,-48,-928,-2176,27072] \\
f_7 &= [-10,1,4,7,2,5,80/7,-5,-50,-215,-100,-625,-10150] \\
f_8 &= [-19,-5,-8,-2,8,8,80/7,16,64,64,-256,-640,-5632] \\
f_9 &= [-7,-22,-13,-6,-3,-6,-207/7,-54,-63,-54,27,1242,4293] \\
f_{10} &= [-25,0,0,-10,0,0,80/7,0,0,128,0,0,-4096] \\
f_{11} &= [6,-31,-32,-24,-16,-8,-144/7,-64,-128,-192,-256,256,3072] \\
f_{12} &= [-64,-32,-32,-32,-16,8,248/7,64,124,262,374,122,-2353] \\
f_{13} &= [-64,-64,-32,-16,-16,-32,-424/7,-76,-68,-28,134,859,2207] \\
f_{14} &= [-25,-50,-25,-10,-5,-10,-235/7,-50,-49,-34,31,614,1763] \\
f_{15} &= [55,29,-7,-3,-9,-15,-81/7,9,-9,-27,-135,-459,567] \\
f_{16} &= [-81,-27,-27,-27,-9,9,171/7,33,63,141,149,-67,-1657] \\
f_{17} &= [-125,0,-25,0,15,0,45/7,0,27,0,-81,0,-729] \\
f_{18} &= [125,0,-25,0,-15,0,45/7,0,-27,0,-81,0,729] \\
f_{19} &= [-162,-27,0,27,18,9,108/7,15,6,-51,-88,-93,-710] \\
f_{20} &= [0,81,0,0,0,0,-144/7,0,0,0,0,-256,0] \\
f_{21} &= [-185,-12,31,44,27,20,157/7,12,-17,-76,-105,-148,-701] \\
f_{22} &= [100,125,50,15,0,-15,-270/7,-45,-36,-27,-54,-297,-648] \\
f_{23} &= [192,32,-32,0,-16,-8,24/7,8,-20,-6,-58,-68,423] \\
f_{24} &= [-395,-153,-92,-26,24,40,304/7,48,64,64,0,-128,-512] \\
f_{25} &= [-537,-205,-133,-123,-89,-41,45/7,41,71,123,187,205,-57] \\
f_{26} &= [359,141,-1,-21,-33,-39,-207/7,-9,-9,-27,-81,-189,-81] \\
f_{27} &= [295,-17,-55,-25,-25,-5,31/7,-5,-25,-25,-55,-17,295]
\end{aligned}
$$

Just in case anyone was wondering, the associated Representative points $z(f) = x + iy$ are:-

	$\lvert z(f)\rvert$	x	$x+iy$
f_1	2.701	0	$2.701i$
f_2	2.615	0	$2.615i$
f_3	2.590	0	$2.590i$
f_4	2.590	0	$2.590i$
f_5	2.464	-0.06962	$-0.06962+2.463i$
f_6	2.142	-0.03610	$-0.03610+2.141i$
f_7	1.765	-0.2189	$-0.2189+1.752i$
f_8	1.603	-0.2272	$-0.2272+1.586i$
f_9	1.530	-0.3756	$-0.3756+1.483i$
f_{10}	1.529	0	$1.529i$
f_{11}	1.413	-0.4664	$-0.4664+1.334i$
f_{12}	1.388	-0.5000	$-0.5000+1.295i$
f_{13}	1.316	-0.4652	$-0.4652+1.231i$
f_{14}	1.313	-0.3451	$-0.3451+1.266i$
f_{15}	1.298	-0.1409	$-0.1409+1.291i$
f_{16}	1.295	-0.3560	$-0.3560+1.245i$
f_{17}	1.158	0	$1.158i$
f_{18}	1.158	0	$1.158i$
f_{19}	1.135	-0.1915	$-0.1915+1.119i$
f_{20}	1.121	0	$1.121i$
f_{21}	1.111	-0.2856	$-0.2856+1.073i$
f_{22}	1.106	-0.3119	$-0.3119+1.061i$
f_{23}	1.071	-0.01805	$-0.01805+1.070i$
f_{24}	1.022	-0.3479	$-0.3479+0.9612i$
f_{25}	1.000	-0.4131	$-0.4131+0.9106i$
f_{26}	1.000	-0.2619	$-0.2619+0.9650i$
f_{27}	1.000	-0.1459	$-0.1459+0.9893i$

Using the techniques of section 6.6, we get that the $\mathrm{GL}(2,\mathbb{Z})$ classes of $f_3, f_4, f_{17}, f_{18}, f_{27}$ are also $\mathrm{SL}(2,\mathbb{Z})$ classes, otherwise they become 2 $\mathrm{SL}(2,\mathbb{Z})$ classes. This means that the above list becomes 49 parameterizations if we do not identify $\pm X$.

References

[Be98] Frits Beukers, *The Diophantine Equation $Ax^p + By^q = Cz^r$*, Duke Maths Journal, Vol **91** (1998), 61–88.

[Bo90] Bela Bollobas, *Linear Analysis*, Cambridge University Press, 1990.

[DG95] H.Darmon and A.Granville, *On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$.*, Bull London Math. Soc. **27** (1995), 513–543.

[Go87] Paul Gordan, *Paul Gordan's Vorlesungen über Invariantentheorie*, Leipzig: Teubner, 1887.

[GY03] J.H.Grace and A.Young (1903), *The Algebra of Invariants*, New York: Chelsea, 1965.

[Hi97] David Hilbert (1897), *Theory of Algebraic Invariants*, Cambridge University Press, 1993.

[Ju17] Gaston Julia, *Étude sur les formes binaires non quadratiqes*, Mem. Acad. Sci. l'Inst. France **55** (1917), 1–293.

[Kl84] Felix Klein (1884), *Lectures on the icosahedron and the solution of equations of the fifth degree* , New York: Dover publications, 1956.

[La95] Serge Lang, *Algebra*, Third Edition, Addison-Wesley, Reading MA, 1995.

[Mo69] L.E.Mordell, *Diophantine Equations*, Academic Press, London, 1969.

[SC00] Michael Stoll and John Cremona, *On the Reduction Theory of Binary Forms*, Preprint (2000), available via http://www.math.uni-duesseldorf.de/ stoll .

[Th96] Steve Thiboutot, *Courbes Elliptiques, représentations galoisiennes et l'équation* $x^2 + y^3 = z^5$, Master's Thesis, McGill Univ., Montreal, 1996.