Parametric Solutions to the Generalized Fermat Equation

27 April 2016

Advisor: Dr. Tom Fisher

Contents

1 Introduction

1.1 The Generalized Fermat Equation

The 1990's were a great time for Diophantine equations, with the obvious high point being the proof of Fermat's Last Theorem. Less well known are a few other results, which study the generalized Fermat equation.

Let $p, q, r \in \mathbb{Z}^{\geq 2}$, and let A, B, C be nonzero integers. Consider the following equation for $x, y, z \in \mathbb{Z}$:

$$Ax^p + By^q + Cz^r = 0, \qquad \gcd(x, y, z) = 1, \qquad xyz \neq 0. \tag{1.1}$$

First off, why do we care about $\gcd(x, y, z) = 1$? One reason is we can multiply a valid solution through, say by $m^{lcm(p,q,r)}$ for any m to create new solutions. Another less obvious occurrence is illustrated by an example ([7] page 2): starting with $a + b = c$, multiply through by $a^{33}b^{44}c^{54}$ to obtain:

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

In this essay we will be using the restriction that $\gcd(x, y, z)$ only contains primes from S, which is chosen to be a finite set of primes.

Returning to our equation now, it turns out that a defining feature is the quantity $\frac{1}{p} + \frac{1}{q} + \frac{1}{r}$. In 1995, Darmon and Granville proved that in the *hyperbolic case*, when $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, there are only *finitely* many solutions to equation 1.1 [3]. In the *Euclidean* case, when $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$, the equation 1.1 becomes an elliptic curve. Thus the question boils down to finding rational points on this elliptic curve; a hot topic in mathematics today, but not the focus of this essay.

The final case is the *spherical* case, when $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$. A quick analysis of this equation yields that the multiset $\{p, q, r\}$ is one of $\{2, 2, k\}$ $(k \geq 2)$, $\{2, 3, 3\}$, $\{2, 3, 4\}$, and $\{2, 3, 5\}$. The 1998 paper by Frits Beukers [1] studying this case will be the first main focus of this essay. In this paper, Beukers proves:

Theorem 1.1. *Let $p, q, r \in \mathbb{Z}^{\geq 2}$ be such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$, and A, B, C be nonzero integers. Then:*
i) There exists a finite set of polynomial triples $(X_i(s,t), Y_i(s,t), Z_i(s,t)) \in (\mathbb{Q}[s,t])^3$ $(1 \leq i \leq n)$ which satisfy $AX_i{}^p + BY_i{}^q + CZ_i{}^r = 0$, such that for any integral solution (x, y, z) to equation 1.1 there exists integers i, s, t such that $(x, y, z) = (X_i(s,t), Y_i(s,t), Z_i(s,t))$. In other words, all integral solutions are parametrized by a finite set of polynomials.
ii) If equation 1.1 has at least one solution, then it has infinitely many.

Unfortunately, Beukers's paper doesn't provide an efficient means of computing the polynomials in question. Alternate methods existed in certain cases, but $\{2, 3, 5\}$ was still unsolved. This gap was completed by Beukers's PhD student Johnny Edwards in 2004 (see [6]), and it also is the focus of his thesis [7].

1.2 Outline of the Essay

We will start off by studying invariants obtained by looking at rotation groups; much of this material was developed in the late 1800s, especially by Klein. This provides the motivation for having polynomial solutions to equation 1.1. Much of the material derives from Klein's *Lectures on the icosahedron and the solution of equations of the fifth degree*, [8]. For a more complete account of the invariant theory used, see Hilbert's tranlsated lecture notes *Theory of algebraic invariants*, [5].

We now delve into the proof of the main result due to Beukers in [1]. His approach is quite theoretical and geometric in motivation; he also proves more general results than what he needs. We will specialize his

results just to study equation 1.1, which is what we are interested in. In most cases this makes the proofs shorter, easier, and clearer.

The downside to Beukers approach is it does not lend itself to an algorithm to compute the finite list of parametrized solutions. As noted on page 214 of [6], alternate methods to do this were found by Mordell in 1969 for the case $(p, q, r) = (2, 3, 3)$, and by Zagier in 1998 for $(p, q, r) = (2, 3, 4)$; the $(2, 3, 5)$ case was however unknown. Beukers had the idea to generalize Mordell's method, and as mentioned previously, this problem became the subject of his student Johnny Edwards's thesis [7]. Edwards's approach was much more algebraic and hands on; it is often necessary to consult a list of equations and verify things explicitly.

Edwards's approach is approximately as follows: a general homogeneous binary form of a specific degree satisfies equation 1.1 if and only if a certain set of polynomials in its coefficients is satisfied. In a similar fashion to binary quadratic forms, one can introduce the notion of a *reduced* form, and obtain a bound on its coefficients. Running through our defining equations subject to the bounds allows us to have a finite set of forms to check, and checking which ones work gives us our list.

Since Edwards's approach also yields an algorithm to compute explicit solutions, it would make sense to ignore Beukers's paper altogether, and instead prove all of the results of Edwards. However the arguments in Beukers's paper are (as mentioned before) nicer and more theoretical in nature; they give a better understanding to the reader of what is going on. Furthermore, his original paper is a fair bit more general than we require, so his propositions and proofs can be a bit confusing at times when he doesn't give a specific example to reference to. As such, I feel that it is nice to have a "cleaner" presentation, which is what I intend this to be.

After presenting the algorithm we give the results of running it on some test cases. From this data we derive a few propositions and conjectures. I have used the software MAGMA at the University of Cambridge; many thanks to my essay advisor Dr. Tom Fisher for giving me access and getting me started with MAGMA.

2 Invariant Theory and Klein Forms

2.1 Finite Rotation Groups

Consider the complex plane, and add a vertical axis through the origin. Draw a sphere of radius 1 centred at the origin, and consider the stereographic projection from the top of the sphere, i.e. $(0, 0, 1)$ onto the complex plane. This is a homeomorphism between the unit sphere and the complex plane with a point at infinity ($\mathbb{CP}^1$); this is referred to as the Riemann Sphere.

For a point (x_1, y_1, z_1) on the unit sphere, it is mapped to

$$\left(\frac{x_1}{1-z_1}, \frac{y_1}{1-z_1}\right) = \frac{x_1}{1-z_1} + \frac{y_1}{1-z_1}i = (x_1 + y_1 i : 1 - z_1), \tag{2.1}$$

where the first two equations give the point at infinity when $z_1 = 1$. This formula will be useful later when calculating invariants.

The general setup involves taking G to be a the group of rotations of an n-gon (in 3−space and not the plane, i.e. $G \cong D_{2n}$), tetrahedron, octahedron, and icosahedron. In each case G can be realized as a finite subgroup of both $PGL(2, \mathbb{C})$ and $GL(2, \mathbb{C})$. Indeed, G is a subgroup of rotations of the unit sphere, so upon stereographic projection this corresponds to a subgroup of $PGL(2, \mathbb{C})$, the Möbius transformations of $\mathbb{CP}^1$. We pull G back to $GL(2, \mathbb{C})$ by taking its inverse image in the natural map $SL(2, \mathbb{C}) \to PGL(2, \mathbb{C})$.

We can think of G as acting on $\mathbb{CP}^1$: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in PGL(2,\mathbb{C})$ corresponds to the Möbius map $f(z) = \frac{az+b}{cz+d}$. It also acts on $\mathbb{C}^2$ via left multiplication on a column vector, i.e. $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} z_1 \\ z_2 \end{smallmatrix}\right)$.

If F_k is the set of homogeneous binary forms on $\mathbb{C}^2$ of degree k, then G acts on F_k via:

$$f(z_1, z_2) \to g \cdot f := f(g^{-1}(z_1, z_2)) \text{ for } g \in G.$$

Note that we use g^{-1}; this is necessary to make it a group action.

2.2 Invariant Polynomials

We will now introduce the notion of an invariant polynomial, and study how different invariant polynomials relate to each other. We will follow the general method due to Felix Klein in Chapter 2, Section 9 of his book *Lectures on the Icosahedron*, cited as [8]. As the title hints at, the theory is developed with the intent to apply it to the group of rotations of a platonic solid.

Definition 2.1. For $\mathbf{u} \in \mathbb{C}^2$, $Q \in \mathbb{CP}^1$, P on the unit sphere, call $\mathbf{u}, Q, P$ *regular* if its stabilizer is trivial under the action of G. Thus it has $|G|$ distinct images under the action of G.

Definition 2.2. Given a finite subgroup G of $GL(2,\mathbb{C})$ and a homogeneous binary form $f(z_1, z_2)$ on $\mathbb{C}^2$, call the form *invariant* under G if $f = g \cdot f$ for all $g \in G$. If $|G| = n$, call the form a *ground form* if f has degree n.

Let $P \in \mathbb{C}^2$ be non-zero, let G be one of the groups of rotations, and let $P_1, P_2, \ldots, P_n$ be the $n = |G|$ images of P under the action of G (written with multiplicity). Writing $P_i = \left(\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right)$ for $1 \leq i \leq n$, define

$$f_P(z_1, z_2) = (a_1 z_2 - b_1 z_1)(a_2 z_2 - b_2 z_1) \cdots (a_n z_2 - b_n z_1).$$

Proposition 2.3. *For any $P \in \mathbb{C}^2 \backslash \{(0,0)\}$, f_P is invariant under G.*

Proof. If $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then $g^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ (g has determinant 1), and so

$$g \cdot (a_i z_2 - b_i z_1) = (a_i(-cz_1 + az_2) - b_i(dz_1 - bz_2)) = ((aa_i + bb_i)z_2 - (ca_i + db_i)z_1).$$

Note that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right) = \left(\begin{smallmatrix} aa_i + bb_i \\ ca_i + db_i \end{smallmatrix}\right)$, so we see that the term which has root P_i is sent to the term which has root $g \cdot P_i$. Thus $g \cdot f_P = f_P$.

□

Remark. If $P \in \mathbb{C}^2 \backslash \{(0,0)\}$ has $v = |\mathrm{Stab}_G(P)| > 1$, then each root of f_P is repeated v times, whence $f_P = (f'_P)^v$ for some homogeneous binary form f'_P. By following the above proposition, we see that the form f'_P is also invariant under G!

Proposition 2.4. *Let f_1,f_2,f_3 be three ground forms under G. Then they are linearly dependent over $\mathbb{C}$.*

Proof. I first claim that we can replace f_3 with f_P where P is regular. Indeed, if we have this result then apply it to $\{f_1, f_2, f_P\}$, $\{f_1, f_3, f_P\}$, and $\{f_2, f_3, f_P\}$. If any of the linear relations has 0 as the coefficient of f_P we are done, so we can assume it is 1:

$$\lambda_1 f_1 + \lambda_2 f_2 + f_P = 0$$
$$\lambda_3 f_1 + \lambda_4 f_3 + f_P = 0$$
$$\lambda_5 f_2 + \lambda_6 f_3 + f_P = 0$$

By subtracting each of the 3 possible pairs, we will get a nonzero relation, as otherwise we must have $\lambda_i = 0$ for all i implying $f_P = 0$, contradiction.

Now, take $\lambda_1, \lambda_2 \in \mathbb{C}$ not both 0 such that $(\lambda_1 f_1 + \lambda_2 f_2)(P) = 0$. Since $\lambda_1 f_1 + \lambda_2 f_2$ is invariant and 0 at P, it must have all the images of P under G as roots, hence as P is regular it must be divisible by f_P. But $\lambda_1 f_1 + \lambda_2 f_2$ has degree $|G|$ (or equals 0), whence it is a scalar multiple of f_P, so we get a non-trivial linear relation. □

Remark. We had to be slightly careful when proving the above theorem by introducing f_P with P regular. Indeed we determine a binary form by its degree and its roots, where we can't determine the multiplicity of a root. For example, we have no way of distinguishing $f_P^a f_Q^b$ from $f_P^c f_Q^d$ as long as these polynomials have the same degree. By choosing P so that $\deg(f_P) = n$ we avoid this problem.

The above proposition is a first glimpse at the motivation in solving equations like $x^p + y^q + z^r = 0$. If we can find non-regular P_1, P_2, P_3 with $\mathrm{Stab}_G(P_i) = v_i > 1$ for $i = 1, 2, 3$, then $f_{P_1}, f_{P_2}, f_{P_3}$ are ground forms and we get a relation of the form $\lambda_1 {f'_{P_1}}^{v_1} + \lambda_2 {f'_{P_2}}^{v_2} + \lambda_3 {f'_{P_3}}^{v_3} = 0$. As long as P_1, P_2, P_3 are distinct upon projection to $\mathbb{CP}^1$, this relation will be non-trivial!

We are now ready to apply this to specific examples! An important part of the above is the results aren't just good in theory, but they are all easily computable. Indeed, thinking of G as acting on the corresponding n-gon or polyhedron inscribed into a sphere, it is clear that the sets of vertices, midpoints of edges, and centres of faces all have non-trivial stabilizer. We project each point onto $\mathbb{CP}^1$, take a $P \in \mathbb{C}^2$ which descends to this point, and find the corresponding f'_P. It's worth noting that if $P = \lambda Q$ in $\mathbb{C}^2$ for $\lambda \in \mathbb{C}$, then $f_P = \lambda^n f_Q$. Thus the possible forms we get from a point in $\mathbb{CP}^1$ are the same up to a constant, so the choice of representative $P \in \mathbb{C}^2$ is irrelevant.

2.3 Regular Plane Polygons

Inscribe the regular polygon X with n vertices into the unit sphere such that it is in the complex plane with a vertex on the positive real axis. The group of rotations is $G = D_{2n}$, the dihedral group of order $2n$ (if we were working in the plane then the rotation group is the cyclic group of order n, however since we are in 3 dimensions the "reflection" is actually a rotation).

Our first choice of P is a vertex of X, so that $\mathrm{Orb}_G(P)$ is the set of vertices of X, which is of size n. Thus $v_1 = 2$, and $\mathrm{Orb}_G(P) = \{e^{\frac{2\pi i}{n} j} | 1 \leq j \leq n\}$. This corresponds to $z_1^n - 1$, so after homogenizing we get $f_1(z_1, z_2) = z_1^n - z_2^n$.

Our next choice of P comes from the midpoint of an edge of X, and projecting outward to the sphere from the origin. This time $v_2 = 2$, $\mathrm{Orb}_G(P) = \{e^{\frac{\pi i}{n} + \frac{2\pi i}{n} j} | 1 \leq j \leq n\}$; we get $z_1^n + 1$, and so $f_2(z_1, z_2) = z_1^n + z_2^n$.

The final choice of P is taking the bottom of the sphere, i.e. 0. Now $v_3 = n$ and $\mathrm{Orb}_G(P) = \{(0:1), (1:0)\}$. In this case our we obtain $f_3(z_1, z_2) = z_1 z_2$.

These equations combine to give the familiar $f_2^2 = f_1^2 + 4 f_3^n$, a parametrization of the case $\{2, 2, n\}$.

2.4 Octahedron

The group of rotations of the octahedron X has size 24 (it is in fact S_4). Take the vertices of the octahedron to be (using $(x+yi,z)$ to mean (x,y,z)):

$$\left\{\left(0,1\right),\left(1,0\right),\left(i,0\right),\left(-1,0\right),\left(-i,0\right),\left(0,-1\right)\right\}.$$

We first take P to be a vertex, so $v_1 = 4$. The vertices correspond to:

$$\{\infty, 1, i, -1, -i, 0\}$$

which give us equation:

$$f_1(z_1,z_2) = z_1z_2(z_1^4 - z_2^4).$$

Next, we take P to be the midpoint of an edge, so $v_2 = 2$. The midpoints have coordinates:

$$\left\{\left(\frac{1}{2},\frac{1}{2}\right),\left(\frac{i}{2},\frac{1}{2}\right),\left(-\frac{1}{2},\frac{1}{2}\right),\left(-\frac{i}{2},\frac{1}{2}\right),\left(\frac{1+i}{2},0\right),\left(\frac{-1+i}{2},0\right),\right.$$
$$\left.\left(\frac{-1-i}{2},0\right),\left(\frac{1-i}{2},0\right),\left(\frac{1}{2},-\frac{1}{2}\right),\left(\frac{i}{2},-\frac{1}{2}\right),\left(-\frac{1}{2},-\frac{1}{2}\right),\left(-\frac{i}{2},-\frac{1}{2}\right)\right\}.$$

Rescaling to the sphere, we get:

$$\left\{\left(\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{2}\right),\left(\frac{\sqrt{2}i}{2},\frac{\sqrt{2}}{2}\right),\left(-\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{2}\right),\left(-\frac{\sqrt{2}i}{2},\frac{\sqrt{2}}{2}\right),\left(\frac{(1+i)\sqrt{2}}{2},0\right),\left(\frac{(-1+i)\sqrt{2}}{2},0\right),\right.$$
$$\left.\left(\frac{(-1-i)\sqrt{2}}{2},0\right),\left(\frac{(1-i)\sqrt{2}}{2},0\right),\left(\frac{\sqrt{2}}{2},-\frac{\sqrt{2}}{2}\right),\left(\frac{\sqrt{2}i}{2},-\frac{\sqrt{2}}{2}\right),\left(-\frac{\sqrt{2}}{2},-\frac{\sqrt{2}}{2}\right),\left(-\frac{\sqrt{2}i}{2},-\frac{\sqrt{2}}{2}\right)\right\}.$$

Projecting downwards to the plane gives us:

$$\left\{\sqrt{2}+1,(\sqrt{2}+1)i,-(\sqrt{2}+1),-(\sqrt{2}+1)i,\frac{(1+i)\sqrt{2}}{2},\frac{(-1+i)\sqrt{2}}{2},\right.$$
$$\left.\frac{(-1-i)\sqrt{2}}{2},\frac{(1-i)\sqrt{2}}{2},\sqrt{2}-1,(\sqrt{2}-1)i,-(\sqrt{2}-1),-(\sqrt{2}-1)i\right\},$$

from which we get:

$$f_2(z_1,z_2) = z_1^{12} - 33z_1^8z_2^4 - 33z_1^4z_2^8 + z_2^{12}.$$

Finally, we take P to be the centre of a face, where $v_3 = 3$. We get coordinates of the centres being:

$$\left\{\left(\frac{1+i}{3},\frac{1}{3}\right),\left(\frac{-1+i}{3},\frac{1}{3}\right),\left(\frac{-1-i}{3},\frac{1}{3}\right),\left(\frac{1-i}{3},\frac{1}{3}\right),\right.$$
$$\left.\left(\frac{1+i}{3},-\frac{1}{3}\right),\left(\frac{-1+i}{3},-\frac{1}{3}\right),\left(\frac{-1-i}{3},-\frac{1}{3}\right),\left(\frac{1-i}{3},-\frac{1}{3}\right)\right\}.$$

Projecting to the sphere yields:

$$\left\{\left(\frac{(1+i)\sqrt{3}}{3},\frac{\sqrt{3}}{3}\right),\left(\frac{(-1+i)\sqrt{3}}{3},\frac{\sqrt{3}}{3}\right),\left(\frac{(-1-i)\sqrt{3}}{3},\frac{\sqrt{3}}{3}\right),\left(\frac{(1-i)\sqrt{3}}{3},\frac{\sqrt{3}}{3}\right),\right.$$
$$\left.\left(\frac{(1+i)\sqrt{3}}{3},-\frac{\sqrt{3}}{3}\right),\left(\frac{(-1+i)\sqrt{3}}{3},-\frac{\sqrt{3}}{3}\right),\left(\frac{(-1-i)\sqrt{3}}{3},-\frac{\sqrt{3}}{3}\right),\left(\frac{(1-i)\sqrt{3}}{3},-\frac{\sqrt{3}}{3}\right)\right\}.$$

Projecting downwards gives us:

$$\left\{\frac{(1+i)(\sqrt{3}+1)}{2},\frac{(-1+i)(\sqrt{3}+1)}{2},\frac{(-1-i)(\sqrt{3}+1)}{2},\frac{(1-i)(\sqrt{3}+1)}{2},\right.$$
$$\left.\frac{(1+i)(\sqrt{3}-1)}{2},\frac{(-1+i)(\sqrt{3}-1)}{2},\frac{(-1-i)(\sqrt{3}-1)}{2},\frac{(1-i)(\sqrt{3}-1)}{2}\right\},$$

from which we derive:

$$f_3(z_1, z_2) = z_1^8 + 14z_1^4 z_2^4 + z_2^8.$$

Checking the coefficients of $x^{24}, x^{20}y^4$ in the expansion of f_1^4, f_2^2, f_3^3 yields the equation:

$$108f_1^4 + f_2^2 = f_3^3,$$

which can be verified by multiplying out the terms.

2.5 Tetrahedron and Icosahedron

We could choose the octahedron to have friendly coordinates, which made the calculations not too bad, something which is less true in the tetrahedral and icosahedral cases. The process is the same as the octahedron: for the points P, we choose a vertex, a midpoint of an edge, and the centre of a face. From this we get exponent triples of $2, 3, 3$ for the tetrahedron, and $2, 3, 5$ for the icosahedron; these round out all possible sets of exponents to make the generalized Fermat equation spherical. Instead of running through the calculations, we will just present the final invariants that Beukers uses in his paper (the tetrahedral case is scaled so that the coefficients are integers).

Tetrahedron:

$$\begin{aligned} f_1 =& z_1^6 + 20z_1^3 z_2^3 - 8z_2^6 \\ f_2 =& z_1(z_1^3 - 8z_2^3) \\ f_3 =& z_2(z_1^3 + z_2^3) \end{aligned}$$

with the relation $f_1^2 - f_2^3 - 64f_3^3 = 0$.

Icosahedron:

$$\begin{aligned} f_1 =& z_1^{30} - 522z_1^{25}z_2^5 - 10005z_1^{20}z_2^{10} - 10005z_1^{10}z_2^{20} + 522z_1^5 z_2^{25} + z_2^{30} \\ f_2 =& z_1^{20} + 228z_1^{15}z_2^5 + 494z_1^{10}z_2^{10} - 228z_1^5 z_2^{15} + z_2^{20} \\ f_3 =& z_1 z_2(z_1^{10} - 11z_1^5 z_2^5 - z_2^{10}) \end{aligned}$$

with the relation $f_1^2 - f_2^3 + 1728f_3^5 = 0$.

Remark. Our results can be applied to the cube and dodecahedron, however we do not get any new information as these cases correspond to the results for the octahedron and icosahedron respectively.

Remark. In each case we found three orbits of G on the unit sphere where G does not act freely. If we found another then we would get more relations of the form $\lambda_1 {f'_{P_1}}^{v_1} + \lambda_2 {f'_{P_2}}^{v_2} + \lambda_3 {f'_{P_3}}^{v_3} = 0$. However, by looking at the stabilizer of each element of G, we see that the only possible orbits which G does not act transitively on correspond to vertices, midpoints of edges, and centres of faces of our polyhedron.

2.6 Klein Forms

We derived polynomial relations geometrically, and there is a more algebraic interpretation of them which comes from the study of *covariants*.

Definition 2.5. A generic *form* of order k is

$$f = \sum_{i=0}^{k} \binom{k}{i} a_i z_1^{k-i} z_2^i.$$

Note the convention that the coefficients are not a_i but $\binom{k}{i} a_i$; this matches the notation historically used in the study of covariants. As it turns out, it will also simplify the defining equation of the platonic solids (see Proposition 4.5 and Appendix A).

From now on, $g \in GL(2,\mathbb{C})$ acts on forms of order k by $g \cdot f = f \circ g$. This is no longer a group action as $(gh) \cdot f = h \cdot g \cdot f$, but this is of no concern to us. Let $\mathbf{a} = (a_0, a_1, \ldots, a_k)$, and let $g \cdot f$ correspond to $\mathbf{a}' = (a_0', a_1', \ldots, a_k')$.

Definition 2.6. A form $C \in \mathbb{C}[a_0, a_1, \ldots, a_k, z_1, z_2]$ is called a *covariant* if there exists a nonnegative integer p such that

$$C(\mathbf{a}', \mathbf{z}) = \det(g)^p C(\mathbf{a}, g\mathbf{z})$$

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

A common example of a covariant is the discriminant of a binary quadratic form; this has no z_i terms and is of weight 2 (hence invariant over $SL(2,\mathbb{C})$). We will be stating and using without proof various results on covariants now and in Section 4. The theory of covariants is fully developed in Hilbert's lecture notes on algebraic invariants, [5], and most proofs can be found there.

For now, we only consider the following covariants:

$$\mathbf{H}(f) = \left(\frac{1}{k(k-1)}\right)^2 \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix} = (a_0 a_2 - a_1^2) z_1^{2k-4} + \cdots$$

$$\mathbf{t}(f) = \frac{1}{k(k-2)} \begin{vmatrix} f_x & f_y \\ \mathbf{H}_x & \mathbf{H}_y \end{vmatrix} = (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) z_1^{3k-6} + \cdots$$

One can check that these are covariants of weights $2, 3$ respectively. A motivation for their definition is they appear naturally when applying the transvectant process, which creates covariants from a pair of forms.

When Klein embedded the regular solids into the unit sphere and projected their vertices onto $\mathbb{CP}^1$, he obtained $f(z_1, z_2)$, and relations involving f, $\mathbb{H}(f)$, and $\mathbf{t}(f)$.

r	Solid	Form	β_r
3	Tetrahedron	$\tilde{f}_3 = z_2^4 - 2\sqrt{3} z_1^2 z_2^2 - z_1^4$	$3\sqrt{3}$
4	Octahedron	$\tilde{f}_4 = z_1 z_2 (z_1^4 - z_2^4)$	432
5	Icosahedron	$\tilde{f}_5 = z_1 z_2 (z_2^{10} - 11 z_1^5 z_2^5 - z_1^{10})$	1738

The relations he derived are:

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

for $r = 3, 4, 5$.

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

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

For $f \in \mathscr{C}(r,d)$ define

$$\begin{aligned}\chi(f) : \mathbb{C}^2 &\to \mathbb{C}^3\\ (z_1, z_2) &\to (\frac{1}{2}\mathbf{t}(f), \mathbf{H}(f), f).\end{aligned}$$

Note that $\tilde{f}_r \in \mathscr{C}(r, \frac{1}{\beta_r})$.

Lemma 2.8. *Suppose $f \in \mathscr{C}(r,d)$. Then:*

- *If $g \in GL(2,\mathbb{C})$, then $f \circ g \in \mathscr{C}(r, \det(g)^6 d)$.*
- *If $\mu \in \mathbb{C}^*$, then $\mu f \in \mathscr{C}(r, \mu^{6-r} d)$.*

Proof. Clear, using that $\mathbf{H}$ and $\mathbf{t}$ are covariants of weights $2, 3$. □

Definition 2.9. Call $\mathscr{C}(3) \cup \mathscr{C}(4) \cup \mathscr{C}(5)$ the *Klein forms*.

The algebraic approach given here will be the main tool in Section 4, where we compute explicit solutions. For the intervening sections we will however mostly ignore this, and focus on the geometric approach originally described.

3 Parametrized Solutions

3.1 Some Preliminaries

We will start by recapping the results of the previous section in a table. Note that we have permuted and rescaled some the polynomials f_i of the previous section to make nicer relations.

Figure	(p,q,r)	f_1	f_2	f_3	Relation
$n-$gon	$(2,2,n)$	$z_1^n - z_2^n$	$z_1^n + z_2^n$	$z_1 z_2$	$f_1^2 - f_2^2 + 4f_3^n = 0$
Tetrahedron	$(2,3,3)$	$z_1^6 + 20z_1^3 z_2^3 - 8z_2^6$	$z_1(z_1^3 - 8z_2^3)$	$z_2(z_1^3 + z_2^3)$	$f_1^2 - f_2^3 - 64f_3^3 = 0$
Octahedron	$(2,3,4)$	$z_1^{12} - 33z_1^8 z_2^4 - 33z_1^4 z_2^8 + z_2^{12}$	$z_1^8 + 14z_1^4 z_2^4 + z_2^8$	$z_1 z_2 (z_1^4 - z_2^4)$	$f_1^2 - f_2^3 + 108f_3^4 = 0$
Icosahedron	$(2,3,5)$	*	*	*	$f_1^2 - f_2^3 + 1728f_3^5 = 0$

For the icosahedron we have:

$$\begin{aligned}f_1 =& z_1^{30} - 522z_1^{25}z_2^5 - 10005z_1^{20}z_2^{10} - 10005z_1^{10}z_2^{20} + 522z_1^5 z_2^{25} + z_2^{30}\\ f_2 =& z_1^{20} + 228z_1^{15}z_2^5 + 494z_1^{10}z_2^{10} - 228z_1^5 z_2^{15} + z_2^{20}\\ f_3 =& z_1 z_2 (z_1^{10} - 11z_1^5 z_2^5 - z_2^{10})\end{aligned}$$

Let S be a finite set of primes and A, B, C be nonzero integers. Let (p,q,r) be one of the above triples, and consider the equation

$$Ax^p + By^q + Cz^r = 0 \text{ with } (x,y,z) \in \mathbb{Z}^3, \tag{3.1}$$

with the restriction that

$$xyz \neq 0 \text{ and } p \nmid \gcd(x,y,z) \text{ for all } p \notin S. \tag{3.2}$$

Let G be the group of rotations corresponding to the triple (p,q,r). By rescaling f_1, f_2, f_3, we have polynomials $h_1(s,t), h_2(s,t), h_3(s,t) \in \mathbb{C}[s,t]$ such that $Ah_1^p + Bh_2^q + Ch_3^r = 0$. Let V be the zero set of $F(x,y,z) = Ax^p + By^q + Cz^r$ in $\mathbb{C}^3$.

The main result of this essay is the following theorem, which is proved in the next section.

Theorem 3.1. *There exist a finite set of polynomial triples $F_i = (f_i, g_i, h_i) \in \mathbb{Q}[z_1, z_2]^3$, $1 \leq i \leq r$ such that if (x,y,z) is a solution to equations 3.1 and 3.2, then there exist integers z_1, z_2 and i with $1 \leq i \leq r$ such that $(x,y,z) = F_i(z_1, z_2)$. In more informal terms, there is a finite list of two variable polynomials over $\mathbb{Q}$ such that all solutions to to equations 3.1 and 3.2 can be obtained by specializing the inputs to be integers.*

The rest of this subsection is spent on setting up the proof of the above theorem. Define:

$$\begin{aligned} \phi : \mathbb{C}^2 &\to V \\ (x,y) &\to (h_1(x,y), h_2(x,y), h_3(x,y)) \end{aligned}$$

Proposition 3.2. *The map $\phi : \mathbb{C}^2 \to V$ is surjective.*

Proof. Let $X, Y, Z \in V$, and consider $h_2(x,y) = Y, h_3(x,y) = Z$. Let $d_i = \deg(h_i)$, and then this is equivalent to $h_2(x/y, 1) = \frac{Y}{y^{d_2}}$ and $h_3(x/y, 1) = \frac{Z}{y^{d_3}}$, so $Z^{d_2} h_2(x/y,1)^{d_3} = Y^{d_3} h_3(x/y,1)^{d_2}$. This is a polynomial in the variable x/y, so it has a root r say, and then we can choose an appropriate y so that $h_2(r,1) = \frac{Y}{y^{d_2}}$ and $h_3(r,1) = \frac{Z}{y^{d_3}}$. Taking $x = yr$, we have a solution to $h_2(x,y) = Y, h_3(x,y) = Z$. Considering the defining equation for V, this gives $X^2 = h_1(x,y)^2$, so $h_1(x,y) = \pm X$. If it is X then we are done, so assume otherwise.

We will be done if we find a matrix m such that $h_1 \circ m = -h_1$ and $h_i \circ m = h_i$ for $i = 2, 3$. Considering our expressions for f_i above, we see that we can take m to be (ζ_8 is a primitive 8^{th} root of unity):

$$\begin{pmatrix} 0 & 1 \\ 1 & 0, \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i, \end{pmatrix}, \begin{pmatrix} 0 & \zeta_8 \\ \zeta_8^{-1} & 0, \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i, \end{pmatrix}$$

for the $n-$gon, tetrahedral, octahedral, and icosahedral cases respectively. □

Remark. For clarity we did the above over $\mathbb{C}$, but it clearly remains true when working over an algebraically closed field of characteristic 0. We will be using it for $\overline{\mathbb{Q}}$.

We will run into a slight problem when ϕ is not defined over $\mathbb{Q}$, as there can be different conjugates of ϕ, namely $\phi^\sigma = \sigma\phi\sigma^{-1}$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. As it turns out, there exists a linear polynomial homeomorphism p (i.e. $p \in GL(2, \overline{\mathbb{Q}})$) such that $\phi^\sigma = \phi \circ p$. The proof is a result of the more general Theorem 1.3 of [1]. Alternatively, one can check this explicitly from our equations for f_1, f_2, f_3. For example, in the n-gon case, we have

$$\begin{aligned} h_1 = af_1, h_2 = bf_2, h_3 = cf_3 \\ a = \sqrt{\frac{1}{A}}, b = \sqrt{\frac{1}{-B}}, c = \sqrt[n]{\frac{4}{C}} \end{aligned}$$

As A, B, C are integers, $\phi^\sigma = \phi \cdot (\pm 1, \pm 1, \zeta)$ with multiplication taken pointwise, some choice of signs $\pm$ (depending on if $A, -B$ are rational squares) and ζ being an n^{th} root of unity. Letting η be a n^{th} root of -1, then we can then choose p to be

Case	p	Case	p
$(1,1,\zeta)$	$\left(\begin{smallmatrix}1&0\\0&\zeta\end{smallmatrix}\right)$	$(1,-1,\zeta)$	$\left(\begin{smallmatrix}0&\eta\zeta\\\eta^{-1}&0\end{smallmatrix}\right)$
$(-1,1,\zeta)$	$\left(\begin{smallmatrix}0&\zeta\\1&0\end{smallmatrix}\right)$	$(-1,-1,\zeta)$	$\left(\begin{smallmatrix}\eta\zeta&0\\0&\eta^{-1}\end{smallmatrix}\right)$

The other cases can be checked similarly. Define:

$$\mathcal{G} = \{g \in GL(2,\overline{\mathbb{Q}}) | \exists \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) : \phi^\sigma = \phi \circ g\}.$$

Note that $\mathcal{G}$ contains G but is not necessarily a group. The use of $\mathcal{G}$ is found in the following proposition.

Lemma 3.3. *Suppose $\phi^\sigma(\mathbf{v}) = \phi(\mathbf{u})$ for some $\mathbf{u}, \mathbf{v} \in \mathbb{C}^2$, where $\mathbf{u}$ is regular. Then there exists a unique $g \in \mathcal{G}$ such that $g(\mathbf{v}) = \mathbf{u}$.*

Proof. Let $p \in GL(2,\overline{\mathbb{Q}})$ be such that $\phi^\sigma = \phi \circ p$. Thus we have $\phi(p(\mathbf{v})) = \phi(\mathbf{u})$. Let $\mathbf{w} = p(\mathbf{v})$; then $h_i(\mathbf{w}) = h_i(\mathbf{u})$ for $i = 1,2,3$. As any three ground forms are linearly dependent, and $h_1^{e_1}$,$h_2^{e_2}$ are two linearly independent ground forms which take the same value at $\mathbf{u}, \mathbf{w}$, we see that all ground forms agree at $\mathbf{u}, \mathbf{w}$. In particular, $0 = f_{\mathbf{w}}(\mathbf{w}) = f_{\mathbf{w}}(\mathbf{u})$, so $\mathbf{u}$ is a root of $f_{\mathbf{w}}$, and thus $\mathbf{u} = \lambda g_1 \mathbf{w}$ for some $g_1 \in G$, $\lambda \in \mathbb{C}^*$. As $h_i(\mathbf{w}) = h_i(\mathbf{u})$ for each i, we see $\lambda = \pm 1$, and if it is -1 then it can be absorbed into g_1. Thus $\mathbf{u} = g_1 \circ p(\mathbf{v})$, so let $g = g_1 \circ p$. We have $\phi^\sigma = \phi \circ p = \phi \circ g_1 \circ p = \phi \circ g$, so $g \in \mathcal{G}$, and thus we have existence. Note that we did not need $\mathbf{u}$ to be regular for existence.

To show uniqueness, assume we have $g = g_1 \circ p$ and $g' = g_2 \circ p'$ which work. Thus $\phi^\sigma = \phi \circ p = \phi \circ p'$, so as above we have a $g_3 \in G$ such that $p = g_3 \circ p'$. Thus $g' = (g_2 g_3) \circ p$. However, $\mathbf{u}$ being regular implies that given p, the choice of g_1 we made was unique, thus $g_1 = g_2 g_3$ and $g = g'$. □

Definition 3.4. A matrix $m \in GL(2,\overline{\mathbb{Q}})$ such that $\phi \circ m$ is defined over $\mathbb{Q}$ is called a $\mathbb{Q}-$matrix.

Note that Proposition 3.2 implies that all parametrized solutions of degree $|G|$ arise from $\mathbb{Q}-$matrices.

Definition 3.5. If m is a $\mathbb{Q}-$matrix, then for any $g \in G$ and $r \in GL(2,\mathbb{Q})$ we have $g \circ m \circ r$ is also a $\mathbb{Q}-$matrix. Call these matrices equivalent; this is an equivalence relation on $\mathbb{Q}-$matrices.

The path ahead is now fairly clear. Twisting ϕ by two equivalent $\mathbb{Q}-$matrices will produce two polynomials with rational coefficients, which output the same set of values when the inputs are taken to be rational. Thus the goal is to show that there are finitely many equivalence classes of $\mathbb{Q}-$matrices from which all solutions with the restriction in equation 3.2 can be derived.

3.2 Proof of the Main Result

Note that enlarging the set S by a adding in a finite number of primes does not change the generality of Theorem 3.1. We will enlarge S so that the following conditions are met ($\mathcal{O}_S$ is the ring of $S-$integral algebraic integers):
1) S contains the primes ramifying in the fields of definition of G and ϕ (and thus $\mathcal{G}$);
2) $\mathcal{G} \subset GL(2,\mathcal{O}_S)$;
3) $h_1, h_2, h_3 \in \mathcal{O}_S[z_1, z_2]$
4) If $\mathfrak{p}$ is a prime not above a prime in S, then the natural reduction map $\mathcal{G} \to GL(2) \pmod{\mathfrak{p}}$ is injective.

We continue with a lemma and a proposition, before moving on to the actual proof of Theorem 3.1.

Lemma 3.6. *Let m be a $\mathbb{Q}-$matrix. Then for every $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, let $g_\sigma = m\sigma(m)^{-1}$. Then we have $g_\sigma \in \mathcal{G}$.*

Proof. First, take $h \in \mathcal{G}$ such that $\phi^\sigma = \phi \circ h$. Thus we get:

$$\phi \circ m = \sigma(\phi \circ m) = \phi^\sigma(\sigma(m)) = \phi \circ h \circ \sigma(m),$$

so thus there must exist $g \in G$ such that $m = gh \circ \sigma(m)$, so $g_\sigma = gh \in \mathcal{G}$. □

Proposition 3.7. *Let $\mathbf{t} = (x, y, z)$ be a solution of equations 3.1 and 3.2. Then there exists a $\mathbb{Q}-$matrix m and $\mathbf{s} \in \mathbb{Q}^2$ such that $\mathbf{t} = (\phi \circ m)(\mathbf{s})$. Furthermore, the equivalence class of m is uniquely determined by $\mathbf{t}$, and the field generated by the elements of m is unramified outside of S.*

Proof. Take $\mathbf{u} \in \overline{\mathbb{Q}}^2$ such that $\mathbf{t} = \phi(\mathbf{u})$. Since $xyz \neq 0$, we see that $\mathbf{u}$ is a regular vector. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so $\phi^\sigma(\sigma(\mathbf{u})) = \sigma(\mathbf{t}) = \mathbf{t} = \phi(\mathbf{u})$; as $\mathbf{u}$ is regular we have by Lemma 3.3 there exists a unique $g_\sigma \in \mathcal{G}$ such that $g_\sigma\sigma(\mathbf{u}) = \mathbf{u}$.

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, note that since

$$\phi^\sigma(g_\sigma^{-1}\mathbf{u}) = \phi^\sigma \circ \sigma(\mathbf{u}) = \mathbf{t} = \phi(\mathbf{u}) = \phi \circ g_\sigma(g_\sigma^{-1}\mathbf{u})$$

we get that this must be true in general, i.e. $\phi^\sigma = \phi \circ g_\sigma$ (it is true for a unique $g \in \mathcal{G}$, and true with $g = g_\sigma$ for $g_\sigma^{-1}\mathbf{u}$, a regular vector). Therefore for $\phi, \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

$$\phi \circ (g_\sigma\sigma(g_\tau)(\mathbf{r})) = \phi^\sigma(\sigma(g_\tau)(\mathbf{r})) = \sigma(\phi(g_\tau(\sigma^{-1}(\mathbf{r})))) = \sigma(\phi^\tau(\sigma^{-1}(\mathbf{r}))) = \phi^{\sigma\tau}(\mathbf{r})$$

whence we have the cocycle property, $g_{\sigma\tau} = g_\sigma\sigma(g_\tau)$. Hilbert's 90 for $GL(n)$ states that $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), GL(n, \overline{\mathbb{Q}})) = 0$, so we conclude that there exists a $m \in GL(2, \overline{\mathbb{Q}})$ such that $g_\sigma = m\sigma(m)^{-1}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We have:

$$\sigma(\phi \circ m) = \phi^\sigma \circ \sigma(m) = \phi^\sigma \circ g_\sigma^{-1} \circ m = \phi \circ m,$$

for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, whence m is a $\mathbb{Q}-$matrix. Also, $\phi \circ m(m^{-1}(\mathbf{u})) = \mathbf{t}$, and for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have

$$\sigma(m^{-1}(\mathbf{u})) = m^{-1}g_\sigma(\sigma(\mathbf{u})) = m^{-1}(\mathbf{u}).$$

So $\mathbf{s} = m^{-1}(\mathbf{u}) \in \mathbb{Q}^2$ and $(\phi \circ m)(\mathbf{s}) = \mathbf{t}$.

Next, we need to show the uniqueness of the equivalence class of m. Assume that we also have a $\mathbb{Q}-$matrix m' and $\mathbf{s}' \in \mathbb{Q}$ so that

$$\mathbf{t} = (\phi \circ m')(\mathbf{s}') = (\phi \circ m)(\mathbf{s}) = \phi(\mathbf{u}).$$

As $\mathbf{u}$ is regular, there exists a unique $g \in G$ with $m(\mathbf{s}) = gm'(\mathbf{s}')$. Since we consider the equivalence class of m, we can assume WLOG that $g = \mathrm{id}$ and $\mathbf{u} = m(\mathbf{s}) = m'(\mathbf{s}')$. From Lemma 3.6, we have for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ a $g_\sigma, g'_\sigma \in \mathcal{G}$ such that

$$\begin{aligned} g_\sigma &= m\sigma(m)^{-1} \\ g'_\sigma &= m'\sigma(m')^{-1}. \end{aligned}$$

Therefore we get

$$\sigma(\mathbf{u}) = \sigma(m(\mathbf{s})) = g_\sigma^{-1}(m(\mathbf{s})) = g_\sigma^{-1}\mathbf{u} \tag{3.3}$$

$$\sigma(\mathbf{u}) = \sigma(m'(\mathbf{s}')) = (g'_\sigma)^{-1}(m'(\mathbf{s}')) = (g'_\sigma)^{-1}\mathbf{u} \tag{3.4}$$

whence $g_\sigma = g'_\sigma$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Rearranging $m\sigma(m)^{-1} = g_\sigma = g'_\sigma = m'\sigma(m')^{-1}$ implies $m^{-1}m' = \sigma(m^{-1}m')$, whence $m^{-1}m' \in GL(2, \mathbb{Q})$, i.e. m and m' are equivalent.

For the last part, let K be the normal closure of the field generated by the elements of m, let $p \notin S$ be prime, and let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$ above p. Taking $I_\mathfrak{p}$ to be the inertia group of $\mathfrak{p}$, to show $\mathfrak{p}$ is unramified we need to show that this group is trivial. Assumptions 2, 3 imply that the map ϕ descends to a map $\phi \pmod{\mathfrak{p}}$ which is a quotient map for $G \pmod{\mathfrak{p}}$. As $\mathbf{t} = \phi(\mathbf{u})$ does not descend to 0, $\mathbf{u} \pmod{\mathfrak{p}}$ is a regular vector for $G \pmod{\mathfrak{p}}$. For $\sigma \in I_\mathfrak{p}$, $\sigma(\mathbf{u}) \equiv \mathbf{u} \pmod{\mathfrak{p}}$, and so using equation 3.3 and $\mathbf{u}$ being regular, we get $g_\sigma \equiv id \pmod{\mathfrak{p}}$. Since $\mathcal{G}$ injects into $GL(2) \pmod{\mathfrak{p}}$, we get that $g_\sigma = id$, so $\sigma(m) = m$ for all $\sigma \in I_\mathfrak{p}$. By definition of K we get $\sigma = id$, so $I_\mathfrak{p}$ is trivial, and $\mathfrak{p}$ is unramified in K. □

Remark. One can in fact avoid using Hilbert's 90 and explicitly construct m: there exist invariants I_1, I_2 such that the matrix of partial derivatives

$$J = \begin{pmatrix} \frac{\partial I_1}{\partial z_1} & \frac{\partial I_1}{\partial z_2} \\ \frac{\partial I_2}{\partial z_1} & \frac{\partial I_2}{\partial z_2}, \end{pmatrix}$$

evaluated at $\mathbf{u}$ has nonzero determinant. One can check that $m = J(\mathbf{u})^{-1}$ satisfies the desired equation $g_\sigma = m\sigma(m)^{-1}$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proposition 3.8. *There is a finite set M of $\mathbf{Q}-$matrices such that for every solution $\mathbf{t}$ of equations 3.1 and 3.2, there exists $m \in M$ and $\mathbf{s} \in \mathbb{Q}^2$ such that $\mathbf{t} = (\phi \circ m)(\mathbf{s})$.*

Proof. Using Proposition 3.7, we can choose M to be a set of non-equivalent $\mathbb{Q}-$matrices satisfying the proposition; it remains to show that M is finite.

Let K be a number field over which $\mathcal{G}$ is defined. Pick $m \in M$, and let L be the field over K generated by the elements of m. If d is the degree of the field of definition of ϕ, then we know the size of $\mathcal{G}$ is at most $d|G|$. But we also know that for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma(m) = g_\sigma^{-1} m$ whence L is normal over K and $[L : K] \leq d|G|$. Proposition 3.7 also tells us that L is unramified outside of the *finite* set S, so by Hermite's theorem there are finitely many choices for L.

The final step is given an L, there are finitely many $m \in M$ which give rise to L. Indeed, the map

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\to \mathcal{G} \\ \sigma &\to g_\sigma \end{aligned}$$

factors over $\mathrm{Gal}(L/\mathbb{Q})$, and there are finitely many maps $\mathrm{Gal}(L/\mathbb{Q}) \to \mathcal{G}$. As checked in Proposition 3.7, two $\mathbb{Q}-$matrices giving rise to the same map are equivalent, completing the proposition. □

The above proposition is almost the result we claimed: we wish to take the inputs of parametrized solutions to be integers, and currently we have them as rational numbers. We will now fix this to prove Theorem 3.1.

Lemma 3.9. *Let $g_1, g_2 \in \mathbb{Q}[z_1, z_2]$ be coprime homogeneous polynomials of positive degree. Let Λ be the $\mathbb{Z}-$module spanned by all $\mathbf{s} \in \mathbb{Q}^2$ such that $g_i(\mathbf{s}) \in \mathbb{Z}$ for $i = 1, 2$. Then Λ is a lattice of rank 2.*

Proof. By clearing the denominators of the g_i, we can assume WLOG that $g_i \in \mathbb{Z}[z_1, z_2]$ for $i = 1, 2$. It is sufficient to show that there exists an integer N such that $N\Lambda \subset \mathbb{Z}^2$. Assume this statement is false; then there are arbitrarily large integers N such that there exist $a, b \in \mathbb{Z}$ with at least one of a, b coprime to N such that $g_1(\frac{a}{N}, \frac{b}{N}), g_2(\frac{a}{N}, \frac{b}{N}) \in \mathbb{Z}$. Multiplying through by N, we get $N^{k_1} \mid g_1(a, b)$ and $N^{k_2} \mid g_2(a, b)$ with k_i being the degree of g_i. As g_1, g_2 are coprime, we can run Euclid's algorithm on $g_1(1, \frac{z_2}{z_1}), g_2(1, \frac{z_2}{z_1})$ and $g_1(\frac{z_1}{z_2}, 1), g_2(\frac{z_1}{z_2}, 1)$ and multiply thorough by a certain power of z_1, z_2 to get polynomials $A_1, A_2, B_1, B_2 \in \mathbb{Z}[z_1, z_2]$ such that

$$\begin{aligned} A_1 g_1 + A_2 g_2 &= A z_1^{e_1} \\ B_1 g_1 + B_2 g_2 &= B z_2^{e_2} \end{aligned}$$

for some integer constants A, B, and positive integers e_1, e_2. Plugging in $(z_1, z_2) = (a, b)$, we see that as $k_i \geq 1$, we have $N \mid Aa^{e_1}, Bb^{e_2}$. But N is coprime to one of a, b whence $N \mid A$ or $N \mid B$. In any case, $|N| \leq |AB|$ whence such arbitrarily large N cannot exist. □

Proof of Theorem 3.1. Let m be a $\mathbb{Q}-$matrix. Let $\Lambda(m)$ be the set of $\mathbf{s} \in \mathbb{Q}^2$ such that $\phi \circ m(\mathbf{s}) \in \mathbb{Z}^2$. By the above lemma, this is a $\mathbb{Z}-$lattice of rank two, so let it be generated by $\mathbf{s}_1, \mathbf{s}_2$. Therefore replacing $\phi \circ m(\mathbf{z})$ by $g(z_1, z_2) = \phi \circ m(\mathbf{s_1} z_1 + \mathbf{s_2} z_2)$ means that all integral values that $\phi \circ m$ takes are in $g(\mathbb{Z}^2)$. Repeat this for the finite set of non-equivalent $\mathbb{Q}-$matrices to deduce the theorem. □

4 Constructing Explicit Solutions

4.1 Restricting to Klein Forms

We will now be studying Klein forms, which only seem to parametrize solutions to $Ax^2 + By^3 + Cz^r = 0$ when $A = B = 1$. However, multiply by A^3B^2 to get:

$$(A^2Bx)^2 + (ABy)^3 + A^3B^2Cz^r = 0.$$

Thus by restricting to the case $A = B = 1$ we lose no generality; when we give our final algorithm we will comment on the changes which must be made.

4.2 Classification of Klein Forms

To determine the parametrizations of the generalized Fermat equation, it suffices to determine the Klein Forms. It turns out there is a quite simple algebraic characterization of them, which will form the basis of an algorithm to calculate integer parametrizations explicitly. We inherit the notation and conventions of Section 2.6; in particular recall that a general form of order k is written as

$$f = \sum_{i=0}^{k} \binom{k}{i} a_i z_1^{k-i} z_2^i.$$

For any k, define the 4^{th} and 6^{th} covariants of a form f of order k by:

$$\tau_4(f) = \frac{1}{2}\left(\frac{(k-4)!}{k!}\right)^2 \Omega^4 f(x,y) f(x',y')\Big|_{\substack{x,x'=z_1 \\ y,y'=z_2}}$$
$$\tau_6(f) = \frac{1}{2}\left(\frac{(k-6)!}{k!}\right)^2 \Omega^6 f(x,y) f(x',y')\Big|_{\substack{x,x'=z_1 \\ y,y'=z_2}}$$

with

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

The first term is given by

$$\tau_4(f) = (a_0a_4 - 4a_1a_3 + 3a_2^2) z_1^{2k-8} + \cdots,$$
$$\tau_6(f) = (a_0a_6 - 6a_1a_5 + 15a_2a_4 - 10a_3^2) z_1^{2k-12};$$

these are (up to a constant) the 4^{th} and 6^{th} transvectants of f with itself, and have weight $4, 6$ respectively. The next three results are proved (or a reference is given) in Edwards's paper [6]. The main ideas essentially come from the algebraic relations that being a covariant implies; see Hilbert's lecture notes [5] for more detail.

For forms of order 4, define the catalecticant invariant j by

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

which is covariant of weight 6.

Theorem 4.1 (Gordan 1887)**.** *Let f be a form of order k. Then $\tau_4(f) = 0$ if and only if f is $GL(2,\mathbb{C})$ equivalent to $z_1^k, z_1^{k-1}z_2$, or one of the Klein forms $\tilde{f}_3$, $\tilde{f}_4$, or $\tilde{f}_5$.*

Lemma 4.2. *Let C be a covariant of weight p, homogeneous of degree n in the a_i. If $p > n$, then $C(z_1^k) = C(z_1^{k-1}z_2) = 0$.*

Theorem 4.3 (Classification of Klein Forms)**.** *Fix $d \in \mathbb{C}^*$. Then:*

$$\begin{aligned} \mathscr{C}(3,d) =& \{f \in \mathbb{C}[z_1,z_2]_4 | \tau_4(f) = 0, j(f) = 4d\}, \\ \mathscr{C}(4,d) =& \{f \in \mathbb{C}[z_1,z_2]_6 | \tau_4(f) = 0, \tau_6(f) = 72d\}, \\ \mathscr{C}(5,d) =& \left\{ f \in \mathbb{C}[z_1,z_2]_{12} \middle| \tau_4(f) = 0, \tau_6(f) = \frac{360}{7}df \right\}, \end{aligned}$$

The proof of the classification is a consequence of the previous theorem and lemma, along with a calculation done for the forms $\tilde{f}_r$ that Klein found (Section 2.6). The classification generates a list of polynomials equations in the a_i, which are necessary and sufficient for f to be a Klein form. This is the first key ingredient in generating explicit solutions.

The two defining equations for the tetrahedron are:

$$0 = a_0a_4 - 4a_1a_3 + 3a_2^2 \tag{4.1}$$

$$4d = a_0a_2a_4 + 2a_1a_2a_3 - a_2^3 - a_0a_3^2 - a_1^2a_4. \tag{4.2}$$

We list the equations for the Octahedron and Icosahedron in Appendix A; these calculations were done by Edwards in Appendix A of [7].

4.3 Lifting Integer Solutions

This subsection is the parallel to finding a $\mathbb{Q}-$matrix associated to an integral solution. The upshot of the method presented here is we get a lot more information on the coefficients of the form f.

To define what it means for a form to be *integral*, we use a slightly funny definition.

Definition 4.4. For $r \in \{3,4,5\}$ define:

$$\begin{aligned} \mathscr{U}_3 =& \{a_0, \ldots, a_4\}, \mathscr{U}_4 = \{a_0, \ldots, a_6\} \\ \mathscr{U}_5 =& \{a_0, \ldots, a_5, 7a_6, a_7, \ldots, a_{12}\} \end{aligned}$$

For f a form of order k ($k = 4, 6, 12$ respective to $r = 3, 4, 5$), denote $\mathscr{U}_r(f)$ to be the specialization of $\mathscr{U}_r$ to the coefficients of f. For a ring $R \subset \mathbb{C}$, define

$$\mathscr{C}(r,d)(R) = \{f \in \mathscr{C}(r,d) | \mathscr{U}_r(f) \subset R\};$$

we call such forms $R-$integral.

Remark. Since $GL(2,\mathbb{Z})$ is generated by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, it is easy to check that $\mathscr{C}(r,d)(\mathbb{Z})$ is closed under the action of $GL(2,\mathbb{Z})$.

Proposition 4.5. *Let d be a nonzero integer and $r \in \{3,4,5\}$. If (X,Y,Z) satisfy $X^2+Y^3+dZ^r=0$ where X,Y,Z are coprime integers, then there exists a form $f \in \mathscr{C}(r,d)(\mathbb{Z})$ and $\mathbf{s}=(s_1,s_2) \in \mathbb{Z}^2$ such that $\chi(f)(s_1,s_2)=(X,Y,Z)$ (χ is defined in Definition 2.7).*

Proof. Pick any $f \in \mathscr{C}(r,d)$. Proposition 3.2 implies that there exist $(s_1,s_2) \in \mathbb{C}^2$ such that $\chi(f)(s_1,s_2)=(X,Y,Z)$ (all parametrizations are $GL(2,\mathbb{C})$ twists of each other). By applying a transformation in $SL(2,\mathbb{C})$ we can assume that $(s_1,s_2)=(1,0)$, and so we have the equations:

$$\begin{aligned} 2X =& \mathbf{t}(1,0) = a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3 \\ Y =& \mathbf{H}(1,0) = a_0a_2 - a_1^2 \\ Z =& f(1,0) = a_0. \end{aligned} \tag{4.3}$$

Note for $\lambda \in \mathbb{C}$, replacing $f(z_1,z_2)$ by $f(z_1+\lambda z_2, z_2)$ corresponds to $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$, so our form remains in $\mathscr{C}(r,d)$ and the above equations for X,Y,Z remain unchanged. We will now show how to choose λ so that the resulting form is in $\mathscr{C}(r,d)(\mathbb{Z})$, which will complete the proof. We will use the above three equations to play with a_0,a_1,a_2,a_3, and use the defining equations of the Klein forms to deduce the result for the rest of the coefficients.

Case 1: $Z=0$

We have $a_0=0$, and since Klein forms are separable (just check $\tilde{f}_3,\tilde{f}_4,\tilde{f}_5$) we must have $a_1 \neq 0$. Therefore we can choose λ making $a_2=0$. Plugging this into equations 4.3 and using the coprimality of $X,Y,Z=0$, we see that $a_1=\pm 1$ and $(X,Y,Z)=(\pm 1,-1,0)$.
For the tetrahedron case, the defining equations 4.1 imply that

$$(a_0,a_1,\ldots,a_4)=(0,\pm 1,0,0,-4d),$$

so indeed, $\mathscr{U}_3(f) \subset \mathbb{Z}$, as required. The octahedral and icosahedral cases can be completed in similar fashion.

Case 2: $Z \neq 0$

This case requires a bit more work; as $a_0=Z\neq 0$, varying λ implies that we can take a_1 to be any value we like. Note that Y,Z must be coprime, so we can take a_1 to be an integer satisfying:

$$a_1 \equiv -\frac{X}{Y} \pmod{Z^r}$$

This equivalence can be reverse engineered from the resulting expressions for a_2,a_3 (from equations 4.3):

$$\begin{aligned} a_0a_2 =& Y + a_1^2 \equiv Y + \left(\frac{X}{Y}\right)^2 = \frac{-dZ^r}{Y^2} \equiv 0 \pmod{Z^r} \\ a_0^2a_3 =& 2X + 3a_0a_1a_2 - 2a_1^3 \equiv 2X - 2\left(-\frac{X}{Y}\right)^3 \equiv 2X\frac{-dZ^r}{Y^3} \equiv 0 \pmod{Z^r}, \end{aligned}$$

(noting that the first equation implies $Z^{r-1} \mid a_0$ whence $Z^r \mid 3a_0a_1a_2$.
In particular, this imples that $a_0,a_1,a_2,a_3 \in \mathbb{Z}$ and for any prime p dividing Z they satisfy:

$$p^1||a_0, \quad p^0||a_1, \quad p^{r-1}|a_2, \quad p^{r-2}|a_3.$$

For the tetrahedron, our equation for a_4 is:

$$a_0a_4 = 4a_1a_3 - 3a_2^2$$

from which it follows that $a_4 \in \mathbb{Z}$ and $f \in \mathscr{C}(3,d)(\mathbb{Z})$. The octahedral and icosahedral cases can be completed in similar fashion. □

Remark. The occurrence of $7a_6$ in $\mathscr{U}_5$ may still seem strange. An arbitrary form f of degree 12 has coefficients $\binom{12}{i}a_i$, and the only value of i for which $7 \mid \binom{12}{i}$ is $i = 6$. When the defining equations for the tetrahedral case are calcualted, this 7 remains always attached to the a_6 term. In particular we have the equation:

$$0 = a_0(7a_6) - 12a_1a_5 - 15a_2a_4 + 20a_3^2$$

whereas for all the other a_i, $i > 0$ there is an equation with term a_0a_i and integer coefficients (we need to work a little bit in the icosahedral case when $i = 8$). Thus we account for this by only requiring $7a_6$ to be an integer.

Remark. When proving Theorem 3.1, we were working with a finite set of primes S where $p \nmid \gcd(X, Y, Z)$ for all $p \notin S$. In the above result, we are essentially working with S being the empty set, so how does the result change when S is non-empty? Working through the proof of Proposition 4.5 it is clear that we can replace $f \in \mathscr{C}(r, d)(\mathbb{Z})$ by $f \in \mathscr{C}(r, d)(\mathbb{Z}_S)$, with $\mathbb{Z}_S$ being the localization of $\mathbb{Z}$ with respect to the primes in S. We consider the changes this makes to our algorithm in Section 5.4.

4.4 Hermite Reduction Theory

This subsection is very reminiscent of the theory of binary quadratic forms; indeed, it is a direct generalization of it. Let $\mathbb{H}$ be the upper half plane, and $\mathscr{D}$ be the fundamental domain for $SL(2, \mathbb{Z})$, i.e.

$$\mathscr{D} = \left\{ z = x + iy \middle| |z| \geq 1, -\frac{1}{2} \leq x \leq \frac{1}{2} \right\}.$$

The goal is given a form f, to be able to associate a representative point $z(f) \in \mathbb{H}$ which respects the action of $SL(2, \mathbb{Z})$ on the form. Explicitly, we want

$$z(g \cdot f) = g^{-1}z(f)$$

for all $g \in SL(2, \mathbb{Z})$.

Every form will then be equivalent to one with representative point in $\mathscr{D}$, and we want this to imply that the coefficients of the form are bounded by some given number. Then if we are studying integral forms, there is a finite number of possibilities for the coefficients, so we can check them all and generate a finite list of integral forms with one from each equivalence class.

In this section will be useful to restrict to *real forms*, i.e. homogeneous $f \in \mathbb{R}[z_1, z_2]$. Such an f has *signature* (r, s) where f has r real roots and s pairs of complex roots, with $r + 2s = \deg(f) = k$ (note this r is different to our previous usage of r).

As noted on page 2 of [9], there can be more than one way to define $z(f)$ when $k \geq 5$ or $k = 3, 4$ and $(r, s) = (1, 1), (2, 1)$ respectively. Note that when $s = 1$, there is a unique root of f in $\mathbb{H}$ so we can take that to be $z(f)$. However, this choice does not obviously extend to other possible values of (r, s).

Another viewpoint that is taken by Stoll and Cremona in [9] is to associate a positive definite real binary quadratic form $Q(f)$ to f; this is essentially the same as associating a $z(f)$ since each point in the upper half plane corresponds to a unique real positive definite binary quadratic form (up to multiplication by a positive constant), and vice versa.

Let $f \in \mathbb{R}[z_1, z_2]$ be a form of order k. Factorize it as

$$f = a \prod_{i=1}^{k} (v_i z_1 - u_i z_2)$$

with $a \in \mathbb{C}^*$. For $t_i \in \mathbb{R}^*$, $1 \le i \le k$, define $\phi(\mathbf{t})$ by

$$\phi(\mathbf{t}) = \sum_{i=1}^{k} t_i^2 (v_i z_1 - u_i z_2)(\overline{v_i} z_1 - \overline{u_i} z_2) = \sum_{i=1}^{k} t_i^2 |v_i z_1 - u_i z_2|^2.$$

Note that ϕ is then a positive definite real quadratic form! Let δ be its determinant, i.e. if $\phi = Az_1^2 + 2Bz_1z_2 + Cz_2^2$ then $\delta = AC - B^2 > 0$.

As it turns out, the key is to look at an expression introduced by Hermite in [4]

$$\Phi(\mathbf{t}) = \frac{|a|^2 \delta^{k/2}}{(\prod t_i)^2}$$

Definition 4.6. For a form $f \in \mathbb{R}[z_1, z_2]$ and any $z \in \mathbb{C}$, define the *Hermite Covariant* as

$$\Theta(f, z) = \begin{cases} \min \Phi(\mathbf{t}) & \text{over all } \mathbf{t} \text{ such that } \phi(z, 1) = 0, \\ \infty & \text{if } \phi(z, 1) = 0 \text{ for all } \mathbf{t}. \end{cases}$$

We now check that the definition of Θ is independent of the choice of a, u_i, v_i. Indeed, if

$$f = a' \prod_{i=1}^{k} (v_i' z_1 - u_i' z_2)$$

corresponds to ϕ', Φ', then we have some $c, c_1, c_2, \ldots, c_k \in \mathbb{C}$ such that

$$a' = ca, u_i' = c_i u_i, v_i' = c_i v_i, cc_1c_2 \cdots c_k = 1$$

Let $\mathbf{t}' = (\frac{t_1}{|c_1|}, \ldots, \frac{t_k}{|c_k|})$, and we have

$$\phi'(\mathbf{t}') = \sum_{i=0}^{k} \left(\frac{t_i}{|c_i|} \right)^2 |v_i' z_1 - u_i' z_2|^2 = \sum_{i=0}^{k} t_i^2 |v_i z_1 - u_i z_2|^2 = \phi(\mathbf{t}).$$

Therefore $\phi(z, 1) = \phi'(z, 1)$, and if $\phi(z, 1) = 0$ then we have

$$\Phi'(\mathbf{t}') = \frac{|a'|^2 \delta^{k/2}}{(\prod t_i')^2} = \frac{|a|^2 |c|^2 \delta^{k/2}}{(\prod t_i / |c_i|)^2} = \Phi(\mathbf{t}),$$

since $|cc_1c_2 \cdots c_k|^2 = 1$. For Θ, we take the minimum of $\Phi(\mathbf{t})$ over all $\mathbf{t}$, whence the different expressions for f produce the same Θ, so it is well defined.

Definition 4.7. For a form $f \in \mathbb{R}[z_1, z_2]$ define the *Hermite determinant* as

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

Definition 4.8. For any form $f \in \mathbb{R}[z_1, z_2]$, a *representative point* is any $z \in \mathbb{H}$ such that $\Theta(f, z) = \Theta(f)$.

Definition 4.9. A form $f \in \mathbb{R}[z_1, z_2]$ is called *Hermite reduced* if it has a representative point in $\mathscr{D}$.

For an example, consider f to be a positive definite real binary quadratic form, say with leading coefficient 1. Then as the roots are complex conjugates, we get $\phi = (t_1^2 + t_2^2) f$, and so $\Theta(f, z)$ is undefined for all z apart from the two roots of $f(z, 1)$, where it is ∞. So the Hermite determinant is ∞, and the representative point agrees with the notion of a representative point for a binary quadratic form. Thus f is Hermite reduced if

and only if f is reduced as a positive definite binary quadratic form.

Lemma 4.2 of [9] implies that if our form f has order at least 3 and has distinct roots, then the representative point in *unique*. As Klein forms have distinct roots and order at least 3, we will assume this from now on and denote the unique representative point by $z(f)$.

We now have a series of results which allow us to bound coefficients of a Hermite reduced form. It essentially follows the sequence of results in Section 4 of [6].

Proposition 4.10. *Let $f \in \mathbb{R}[z_1, z_2]$ be a form of order k. Then for $g \in GL(2, \mathbb{R})$ we have*

$$\Theta(f \circ g, z) = |\det(g)|^k \Theta(f, gz).$$

Therefore $\Theta(f \circ g) = |\det(g)|^k \Theta(f)$.

Proof. This is clear from carefully plugging $f \circ g$ into the definition of Θ. □

Corollary 4.11. *Let $f \in \mathbb{R}[z_1, z_2]$ be a form of order k, and $g \in GL(2\mathbb{R})$. Then*

$$z(g \cdot f) = g^{-1} z(f)$$

Proof. This immediately follows from Proposition 4.10. □

Thus we have justified that our choice of representative point is a reasonable way to define a reduction theory.

4.5 Bounds on Hermite Reduced Forms

We start off with a few results which produce bounds on the coefficients of f in terms of Θ (see Theorem 4.2.5 and Appendix A of [6]).
Denote $\{1, \ldots, n\}$ by $[n]$, and if $S \subset [n]$ let $S' = [n] \backslash S$. If $b \in \mathbb{C}^k$, let $b_S = \prod_{i \in S} b_i$.

Lemma 4.12. *Let $b_i, c_i \in \mathbb{C}$ with $\sum_{i=1}^k |b_i|^2 = \sum_{i=1}^k |c_i|^2 = 1$. Then*

$$\left| \sum_{S \subset [k], |S|=r} b_{S'} c_S \right| \leq \binom{k}{r} \left(\frac{1}{k}\right)^{k/2}$$

Proof. By the triangle inequality and Cauchy-Schwartz, we have

$$\left| \sum_{S \subset [k], |S|=r} b_{S'} c_S \right|^2 \leq \left(\sum_{|S|=r} |b_{S'} c_S| \right)^2 \leq \left(\sum_{|S|=r} |b_{S'}|^2 \right) \left(\sum_{|S|=r} |c_S|^2 \right).$$

Generalized AM-GM ([2], page 15, exercise 22) gives

$$\left(\sum_{|S|=r} |b_{S'}|^2 \right) \leq \binom{k}{k-r} \left(\frac{\sum_{i=1}^k |b_i|^2}{k} \right)^{k-r}, \left(\sum_{|S|=r} |c_S|^2 \right) \leq \binom{k}{r} \left(\frac{\sum_{i=1}^k |c_i|^2}{k} \right)^{r}.$$

Combining inequalities and using $\sum_{i=1}^k |b_i|^2 = \sum_{i=1}^k |c_i|^2 = 1$, $\binom{k}{k-r} = \binom{k}{r}$ gives the result. □

Theorem 4.13. *Let $f = \sum_{i=0}^k \binom{k}{i} a_i z_1^{k-i} z_2^i$ be a real form of order k, and let $z = x + iy \in \mathbb{H}$. Then for all $0 \leq r \leq k$,*

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

Proof. For simplicity, denote $\Theta = \Theta(f, z)$. Write $f = \prod_{i=1}^{k}(v_i z_1 - u_i z_2)$; by the definition of Θ, there exists $t_i > 0$ so that

$$\Theta = \frac{\delta^{k/2}}{(\prod t_i)^2}$$

where δ is the determinant of the positive definite quadratic form $\phi(z_1, z_2) = Pz_1^2 - 2Qz_1z_2 + Rz_2^2$, where $\phi(z, 1) = 0$ and

$$P = \sum t_i^2 |v_i|^2, 2Q = \sum t_i^2 (u_i \overline{v_i} + \overline{u_i} v_i), R = \sum t_i^2 |u_i|^2.$$

Using $z = x + iy$, we have

$$x = \frac{Q}{P}, |z|^2 = \frac{R}{P}$$

and thus

$$\delta = PR - Q^2 = P^2|x + iy|^2 - P^2x^2 = P^2y^2$$

Rearranging our expression for Θ gives $1 = \frac{\sqrt{\Theta}}{\delta^{k/4}} \prod t_i$, so

$$f = \frac{\sqrt{\Theta}}{\delta^{k/4}}(\prod t_i) f = \frac{\sqrt{\Theta}}{(Py)^{k/2}} \prod_{i=1}^{k} (t_i v_i z_1 - t_i u_i z_2).$$

Let $b_i = \frac{v_i t_i}{\sqrt{P}}$ and $c_i = \frac{-u_i t_i}{\sqrt{R}}$; then $\sum |b_i|^2 = \sum |c_i|^2 = 1$. We have

$$\begin{aligned}
\binom{k}{r} a_r =& \frac{\sqrt{\Theta}}{y^{k/2}} \sum_{S \subset [k], |S| = r} \Big(\prod_{i \in S'} \frac{t_i v_i}{\sqrt{P}} \Big) \Big(\prod_{i \in S} \frac{-t_i u_i}{\sqrt{P}} \Big) \\
=& \frac{\sqrt{\Theta}}{y^{k/2}} \left(\frac{\sqrt{R}}{\sqrt{P}} \right)^r \sum_{S \subset [k], |S| = r} (\prod_{i \in S'} b_i)(\prod_{i \in S} c_i) \\
=& \frac{\sqrt{\Theta}|z|^r}{y^{k/2}} \sum_{S \subset [k], |S| = r} b_{S'} c_S
\end{aligned}$$

Apply Lemma 4.12 to deduce the result. □

Theorem 4.14. *Let*

$$f(z_1, z_2) = \sum_{i=0}^{k} \binom{k}{i} a_i z_1^{k-i} z_2^i$$

be a real form of order k. If f is Hermite reduced, then

$$|a_i a_j| \leq \left(\frac{4}{3k^2} \right)^{\frac{k}{2}} \Theta(f)$$

whenever $i + j \leq k$.

Proof. Let $z = x+iy$ be the representative point of f. As it is in the fundamental domain, $y \geq \frac{\sqrt{3}}{2} \max\{1, |z|\}$. Use this in Theorem 4.13 to cancel the $|z|$ and y terms, from which we deduce the result. □

We now need to be able to calculate $\Theta(f)$.

Proposition 4.15. *Let $f = a \prod_i (v_i z_1 - u_i z_2)$ be a real form of order $k \geq 3$ with distinct roots. If $z = x+iy \in \mathbb{H}$ is the representative point, then*

$$\Theta(f) = \left(\frac{k}{2y} \right)^k |a|^2 \prod_{j=1}^{k} (|v_j x - u_j|^2 + |v_j y|^2).$$

Proof. This follows from Proposition 5.1 of [9] when all the roots of f are finite (the definition of Θ used in [9] differs from ours by the constant factor $(\frac{2}{k})^k$). When f has an infinite root, an application of Propositon 4.10 does the trick. □

Thus given a form and its representative point, we have a way to compute its Hermite determinant. We will need some more information on the representative point; how to calculate it for forms of order 4 and what it is for $\tilde{f}_r$ will suffice.

Looking at the definition of ϕ, one can see that weights t_i^2 which give the Hermite determinant must be equal for the pairs of complex conjugate roots. Thus we will assign weights $t_1^2, \ldots, t_r^2$ to the real roots and $u_1^2, u_1^2, \ldots, u_s^2, u_s^2$ to the complex roots.

Proposition 4.16. *Let f be a real form of order 4 with all roots finite. Then the weights t_i which cause the Hermite determinant to be obtained are given in the following table:*

Signature	*Roots*	*Weights*
$(4,0)$	$\alpha_1, \alpha_2, \alpha_3, \alpha_4$	$t_i^2 = \frac{1}{\lvert\frac{\partial f}{\partial z_1}(\alpha_i, 1)\rvert}$
$(2,1)$	α_1, α_2	$t_1^2 = \lvert\beta - \overline{\beta}\rvert\lvert\alpha_2 - \beta\rvert^2$, $t_2^2 = \lvert\beta - \overline{\beta}\rvert\lvert\alpha_1 - \beta\rvert^2$
	$\beta, \overline{\beta}$	$u_1^2 = \lvert\alpha_1 - \alpha_2\rvert\lvert\alpha_1 - \beta\rvert\lvert\alpha_2 - \beta\rvert$
$(0,2)$	$\beta_1, \overline{\beta_1}$	$u_1^2 = \lvert\beta_2 - \overline{\beta_2}\rvert$
	$\beta_2, \overline{\beta_2}$	$u_2^2 = \lvert\beta_1 - \overline{\beta_1}\rvert$

Proof. See Proposition 4.2.4 of [6]. □

Lemma 4.17. *The representative point of $\tilde{f}_3, \tilde{f}_4, \tilde{f}_5$ is i.*

Proof. See Proposition 4.24, Lemma 4.26 in [6]. The key point for $\tilde{f}_4, \tilde{f}_5$ is $f(z_2, -z_1) = \pm f(z_1, z_2)$. □

Proposition 4.18. *Let $f \in \mathscr{C}(r,d)(\mathbb{R})$. Then f has a real root.*

Proof. We can assume that f has no infinite root by applying a suitable transformation. Recalling Section 2, we can inscribe the platonic solid corresponding to d into the unit sphere, so that the roots of f correspond to the projection of the vertices onto the plane. Note that for each the tetrahedron, octahedron, and icosahedron, if a circle goes through an even number of points, then it goes through at most 4. Furthermore, if it goes through 4, then the two regions of the sphere formed also contain vertices of the solid. Under projection, circles go to circles and these properties are transferred to the plane.

If f has no real root, then all of its roots come in complex conjugate pairs. Taking a large circle containing all of its roots, we can shrink it down until it contains at least 4 roots on it (two pairs of complex conjugate roots, the first ones hit) and all of the rest inside. But then the centre of the circle must lie on the real axis, so it will have an even number of roots on the circle, which contradicts the properties above. □

Proposition 4.19. *Let $f \in \mathscr{C}(r,d)(\mathbb{R})$ and $f' \in \mathscr{C}(r,d)(\mathbb{R})$.*
a) If $dd' > 0$, then f, f' are $GL(2,\mathbb{R})^+$ equivalent.
b) If $dd' < 0$, and r is odd, then f is $GL(2,\mathbb{R})^+$ equivalent to $-f'$.

Proof. Lemma 2.8 implies that $-f \in \mathscr{C}(r,(-1)^r d)$ whence b) follows from a). For a), we can apply Lemma 2.8 again to get a $GL(2,\mathbb{R})^+$ transformation so that $d = d' = \pm 1$. By Proposition 4.18, f, f' have real roots. Thus there is a $SL(2,\mathbb{R})$ translation taking the root to ∞ and so that $(a_0, a_1, a_2) = (0, 1, 0)$ (recall the proof of Proposition 4.5). The defining equations of $\mathscr{C}(r,d)$ found in Appendix A imply that all coefficients are determined, so our forms are equal. □

Theorem 4.20. *Suppose $f \in \mathscr{C}(r,d)(\mathbb{R})$, and write $f = f_1 f_2$ where f_i are real forms with all the roots of f_1 being real, and all of the roots of f_2 being complex. Then the following table gives the Hermite determinant of f, as well as a description of the representative point:*

Class	*Signature*	$\Theta(f)$	*Representative Point*
$\mathscr{C}(3,d)$	$(2,1)$	$2^6 3^3 \lvert d\rvert^{2/3}$	-
$\mathscr{C}(4,d), d>0$	$(4,1)$	$2^8 3^9 \lvert d\rvert$	*Unique root of f_2 in $\mathbb{H}$*
$\mathscr{C}(4,d), d<0$	$(2,2)$	$2^8 3^9 \lvert d\rvert$	*Representative point of f_2*
$\mathscr{C}(5,d)$	$(4,4)$	$2^{24} 3^{18} 5^5 \lvert d\rvert^2$	*Representative point of f_1*

Thus we can either use Proposition 4.16 or find the roots of a quadratic equation to find the representative point of a Klein form.

Proof. Lemma 4.17 tells us that i is a representative point of $\tilde{f_r}$, and using Proposition 4.15 we calculate the Hermite determinants to be as indicated in the above table. Proposition 4.19, the properties in 2.8, and the covariance of Θ imply that the same is true for all $f \in \mathscr{C}(r,d)(\mathbb{R})$. □

Theorem 4.21. *Let $f \in \mathscr{C}(r,d)(\mathbb{R})$ be Hermite reduced. Then we have*

$$\max\{|a_i a_j| \big| i+j \le k\} \le B^2$$

where B is given by

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

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

Proof. Apply Theorem 4.14 to the bounds obtained in Theorem 4.20. □

5 Algorithm to Produce Parametrized Solutions

We will now describe the algorithm used to produce solutions to $x^2+y^3+dz^r = 0$ for $r = 3,4,5$ (as mentioned in 4.1, this can be easily generalized to $Ax^2 + By^3 + Cz^r = 0$ if one desires). The short form is:

- Produce a list of Hermite reduced $f \in \mathscr{C}(r,d)(\mathbb{Z})$
- Remove forms which do not have have co-prime specializations
- Reduce to a list of $GL(2,\mathbb{Z})$ equivalent forms

5.1 Listing Hermite Reduced Forms

Note that all forms we are working with are of order $k \ge 4$. Therefore Theorem 4.21 implies that $|a_0|, |a_1|, |a_2| \le B$. Furthermore, taking $(z_1, z_2) = (1,0)$ we get that:

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

satisfy $X^2+Y^3+dZ^r=0$. Therefore for each selection of integers a_0, a_1, a_2 in the range $[-B, B]$, we calculate Y, Z and $X = \pm\sqrt{-Y^3 - dZ^r}$. If X is not an integer then we get no solution. Otherwise, we have at most 2 choices for X, and we *must* have the start of a parametrization which specializes to $(\pm X, Y, Z)$. In the case $a_0 \neq 0$, the equation for X determines a_3, and the equations found in Appendix A show that the rest of the a_i are uniquely determined. If $a_0 = 0$ then the defining equations determine the rest of the coefficients uniquely.

Calculate the representative point using Theorem 4.20 and Proposition 4.16; if it lies in $\mathscr{D}$ then we must have a Hermite reduced form in $\mathscr{C}(r,d)(\mathbb{Z})$. Note that if our form has a root at infinity, then before applying Proposition 4.16 we apply a suitable Möbius map, and then translate the representative point back.

When programming the algorithm, one must be aware of the limitations of floating point arithmetic. When checking if a point is in the fundamental domain, one should increase the bounds of the domain slightly; for example, if the representative point z has $|z| = 1$, the program may calculate $|z|$ as 0.9999999 and then $|z| \geq 1$ would be false. In increasing our tolerance we may also let in a few non-reduced forms, which we will remove later.

5.2 Coprime Specializations

For $r = 3, 4, 5$, let $N = 12, 24, 60$ respectively (the size of the rotation group r corresponds to). Then we have the following proposition

Proposition 5.1. *Let $f \in \mathscr{C}(r,d)(\mathbb{Z})$ where $d \neq 0$, and let $\phi = (\frac{1}{2}\mathbf{t}(f), \mathbf{H}(f), f)$. Then if ϕ has coprime integer specializations, then there exist $(z_1, z_2) \in \mathbb{Z}^2$ such that $|z_i| \leq N'$ such that $\phi(z_1, z_2)$ is coprime, where N' is product of all odd primes dividing Nd.*

Proof. If $f, \mathbf{H}(f)$ have resultant R, then thinking of them as integer polynomials, we have $A, B \in \mathbb{Z}[z_1, z_2]$ such that $Af + B\mathbf{H}(f) = R$. Thus we are done if we show that the primes dividing the resultant of $f, \mathbf{H}(f)$ are the primes dividing Nd.

The resultant can also be thought of as follows: let $a(x) = A\prod_{i=1}^{m}(x - a_i)$ and $b(x) = B\prod_{i=1}^{n}(x - b_i)$. Then $Res(A, B) = A^n B^m \prod_{1\leq i\leq m, 1\leq j\leq n}(a_i - b_j)$.

Now, we have the form $f = [0, 1, 0, 0, -4d] \in \mathscr{C}(3, d)$, and we can check the proposition directly for f. We can do the same with $r = 4, 5$ by starting with $(a_0, a_1, a_2) = (0, 1, 0)$ and following the defining equations to get a form $f \in \mathscr{C}(r, d)$. A general $g \in \mathscr{C}(r, d)$ is $SL(2, \mathbb{C})$ equivalent to f, and $SL(2, \mathbb{C})$ is generated by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ for $\lambda \in \mathbb{C}$. Using the covariance of $\mathbf{H}(f)$ and the above definition of resultant, we see that applying $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ does not change the value of the resultant, and applying $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ will also not change the value of the resultant, whence the claim. □

5.3 Removing equivalent forms

A list with no $GL(2, \mathbb{Z})$ equivalent forms is a minimal list, as all integer solutions occur as integer specializations of an entry on our list, and any two entries give different integer specializations. When working over $GL(2, \mathbb{Z})$, we add in the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to the mix which changes the fundamental domain to

$$\mathscr{D}^- = \left\{ z = x + iy \,\middle|\, |z| \geq 1, -\frac{1}{2} \leq x \leq 0 \right\}.$$

Furthermore, two distinct forms can only be equivalent when their representative point is on the boundary of the fundamental domain! Thus we can calculate the stabilizer of each such point and test if our forms are related by these maps. Edwards does this in [6], and the stabilizer is of size 2 outside of i and ω, the primitive

cube root of unity (where the size is now $6, 4$ respectively).

This provides a good algorithm, however we will take a slightly different approach. MAGMA has the built in function "IsGL2Equivalent", which takes two forms of a specified degree and tests if they are equivalent over $GL(2, K)$, with K being the base field of the forms. The benefit of this is (as mentioned previously), we account for rounding errors by potentially including forms which have representative point not quite in the fundamental domain. Using this function allows us to also rid those forms. This change should increase computation time, however is is minimal as the list of forms we consider is small (the computationally expensive part is generating the initial list of Hermite reduced forms).

When using "IsGL2Equivalent" we do have to be slightly careful, as it works over $\mathbb{Q}$ and not $\mathbb{Z}$. Thus for each transition matrix we get, we must check that it has determinant ± 1 and integer entries.

5.4 Modifying the algorithm for general S

We wish to have something slightly better than the remark following Proposition 4.5, where we said that we can take $f \in \mathscr{C}(r, d)(\mathbb{Z}_S)$. Indeed, assume we are given X, Y, Z with $X^2 + Y^3 + dZ^r = 0$, and let p be any prime dividing $\gcd(X, Y)$. If $p^5 \mid dZ^r$, then working modulo powers of p we get that $p^3 \mid X$, $p^2 \mid Y$, and $p^6 \mid dZ$. So we can divide through by p^6 to get an equation of the form $X_1^2 + Y_1^3 + d_1 Z_1^r = 0$ with $\frac{d}{d_1}$ being a power of p. Repeat and we see that we can assume $p^5 \nmid d' Z^r$ where d' is some divisor of d with $\frac{d}{d'}$ being a power of p (there are finitely many such possibilities).

If $r = 5$ then $p \nmid Z$, and for $r = 3, 4$ we have $p^2 \nmid Z$. Thus following Proposition 4.5, when we lift out integer solution we take $a_0 = Z$, and following through the equations we see that $\mathscr{U}(f) \subset \mathbb{Z}$ if $r = 5$ and $\mathscr{U}(f) \subset \frac{1}{p}\mathbb{Z}$ for $r = 3, 4$. This implies we can continue taking $\mathscr{U}(f) \subset \mathbb{Z}$ if $r = 5$ (though we need to repeat for all $d' \mid d$ where $\frac{d}{d'}$ only has prime divisors from the set S). As our set S is finite, let P be the product of the primes in S, and for $r = 3, 4$ we can take $\mathscr{U}(f) \subset \frac{1}{P}\mathbb{Z}$. Thus we still have a finite algorithm (coefficients are bounded with bounded denominators!

Checking that our solutions have specializations where the only primes dividing $\gcd(X, Y, Z)$ are in S is completely analogous to Proposition 5.1, as we only need to consider the resultant of $f, \mathbf{H}(f)$.

6 Explicit Calculations and Varying d

We shall give some results of our program, and compare them to the results presented by Edwards in [6]. We will only consider the Tetrahedral and Octahedral cases, as the Icosahedral case is very computationally demanding. Note that a form $f \in \mathscr{C}(d, r)$ will be presented as $[a_0, a_1, \ldots, a_k]$.

6.1 Tetrahedron

We may as well take $d > 0$ for the tetrahedron, since -1 being an integral cube implies the cases of d and $-d$ are analogous. Comparing the case of $d = 1$ with Edwards's results on page 233 of [6] we get

$d = 1$

Our Results	Representative Point	Edwards's Results
$[-2,-1,0,-1,-2]$	$-0.268 + 0.963i$	$[-2,-1,0,-1,-2]$
$[-1,1,1,1,-1]$	$-0.268 + 0.963i$	$[-1,1,1,1,-1]$
$[-1,0,-1,0,3]$	$\sqrt[4]{3}i$	$[-1,0,-1,0,3]$
$[1,0,-1,0,-3]$	$\sqrt[4]{3}i$	$[1,0,-1,0,-3]$
$[-1,0,0,-2,0]$	$\sqrt{2}i$	$[-1,0,0,2,0]$
$[0,1,0,0,-4]$	$\sqrt{2}i$	$[0,1,0,0,-4]$

We have rearranged them so that they come in pairs with the same representative point. As noted in [6], $X^2+Y^3+Z^3=0$ is symmetric in Y, Z, and the consecutive pairs correspond to switching (Y,Z) with (Z,Y).

We next calculate the reduced forms, find the number N of non-equivalent reduced forms for $d = 1, 2, \ldots, 60$, and present this data in a table.

d	**N**	**d**	**N**	**d**	**N**	**d**	**N**	**d**	**N**	**d**	**N**
1	6	11	8	21	4	31	4	41	4	51	4
2	3	12	5	22	3	32	2	42	2	52	6
3	4	13	4	23	4	33	4	43	8	53	12
4	5	14	2	24	8	34	2	44	11	54	6
5	4	15	8	25	8	35	8	45	8	55	12
6	2	16	4	26	9	36	12	46	6	56	6
7	4	17	12	27	6	37	12	47	8	57	8
8	9	18	6	28	11	38	3	48	8	58	4
9	8	19	8	29	4	39	8	49	8	59	4
10	5	20	5	30	3	40	6	50	6	60	6

There are relatively few occurrences of N being odd, and they only occur when d is even. This leads to the conjecture that if d is odd, then N is even.
We also see that $N > 0$ for all d, i.e. $\mathscr{C}(3,d)(\mathbb{Z})$ is never empty. Inspired by an observation in the Octahedral case (see Theorem 6.2), we prove the following theorem.

Theorem 6.1. *Let d be a non-zero integer, and write $|4d| = (p_1^{e_1}\cdots p_s^{e_s})^2 q_1^{f_1}\cdots q_t^{f_t}$ where p_i, q_j are distinct primes and f_j is odd for all j. Let S be the set of integers which are a product of a subset of $\{p_1^{e_1}, \ldots, p_s^{e_s}\}$ (the product of the empty set is 1; note that S has size 2^s). Let $N = |S \cap [1, \sqrt{2}\sqrt[3]{d}]|$, i.e. the number of elements of S which are positive and at most $\sqrt{2}\sqrt[3]{d}$. Then there are exactly N non-equivalent forms $f = [a_0, a_1, \ldots, a_4] \in \mathscr{C}(3,d)(\mathbb{Z})$ such that $a_0 = a_2 = 0$. In particular, $\mathscr{C}(3,d)(\mathbb{Z})$ is non-empty.*

Proof. Following the defining equations we get

$$f = [0, a, 0, 0, \frac{-4d}{a^2}]$$

Thus we get a form for all integers a with $a^2 \mid -4d$. If $b = \frac{-4d}{a^2}$, then we calculate the covariants $\frac{1}{2}\mathbf{t}, \mathbf{H}$ to be

$$\begin{aligned}\frac{1}{2}\mathbf{t}(f)(z_1,z_2) =& a^3 z_1^6 + 5a^2 b z_1^3 z_2^3 - \frac{ab^2}{2} z_2^6 \\ \mathbf{H}(f)(z_1,z_2) =& -a^2 z_1^4 + 2ab z_1 z_2^3 \\ f(z_1,z_2) =& 4a z_1^3 z_2 + b z_2^4\end{aligned}$$

As our form needs coprime specializations, we cannot have a prime divide both a and b, else said prime will divide all of $\frac{1}{2}\mathbf{t}, \mathbf{H}, f$. From $\left(\frac{1}{2}\mathbf{t}\right)^2 + (\mathbf{H})^3 + df^3 = 0$, coprimality among all three is equivalent to $f, \mathbf{H}$ being coprime.

I claim that if a, b are coprime, then the form has coprime specializations. Indeed, consider taking $(z_1, z_2) = (1, 1)$. Then $-\mathbf{H}(1,1) = a^2 - 2ab = a(a-2b)$, and $f(1,1) = 4a + b$. As a, b are coprime, $\gcd(a, 4a+b) = 1$ so

$$\gcd(-\mathbf{H}, f) = \gcd(a-2b, 4a+b) = \gcd(2(4a+b)+a-2b, 4a+b) = \gcd(9a, 4a+b) = \gcd(9, 4a+b).$$

Thus we are done if $3 \nmid 4a+b$. If $3 \mid 4a+b$, then take $(z_1, z_2) = (1, -1)$ to get $-\mathbf{H}(1,-1) = a^2 + 2ab = a(a+2b)$ and $f(1,-1) = b - 4a$. As above, $\gcd(\mathbf{H}, f) = \gcd(9, b-4a)$. Thus if this is also not 1, $3 \mid b - 4a$ whence $3 \mid (4a+b) + (b-4a) = 2b$ so $3 \mid b$, and so $3 \mid a$, contradicting a, b being coprime.

Next we calculate the representative point of f. WLOG we can take $a > 0$ and $d > 0$. We first do the transformation $(z_1, z_2) \to (-z_2, z_1)$ to shift away the root at infinity. We are thus left to consider the roots of $z^4 - \frac{4a}{b} z = z^4 + \frac{a^3}{d} z$. Letting $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ be a primitive cube root of unity, we have real roots $\alpha_1 = 0, \alpha_2 = \frac{-a}{\sqrt[3]{d}}$ and complex roots $\beta, \overline{\beta}$ with $\beta = \frac{-a}{\sqrt[3]{d}}\omega$.

We have weights

$$\begin{aligned}t_1^2 =& |\beta - \overline{\beta}||\alpha_2 - \beta|^2 = \frac{a\sqrt{3}}{\sqrt[3]{d}}\left(\frac{a\sqrt{3}}{\sqrt[3]{d}}\right)^2 = \frac{3\sqrt{3}a^3}{d} \\ t_2^2 =& |\beta - \overline{\beta}||\alpha_1 - \beta|^2 = \cdots = \frac{\sqrt{3}a^3}{d} \\ u_1^2 =& |\alpha_1 - \alpha_2||\alpha_1 - \beta||\alpha_2 - \beta| = \frac{\sqrt{3}a^3}{d}.\end{aligned}$$

So our quadratic form is

$$g(x) = \frac{\sqrt{3}a^3}{d}\left(3x^2 + \left(x + \frac{a}{\sqrt[3]{d}}\right)^2 + 2(x-\beta)(x-\overline{\beta})\right) = \frac{6\sqrt{3}a^3}{d}\left(x^2 + \frac{a^2}{2\sqrt[3]{d^2}}\right),$$

which has root in the upper half plane of $\frac{a}{\sqrt{2}\sqrt[3]{d}} i$. Translating back to the equation for f means that f has representative point

$$\frac{\sqrt{2}\sqrt[3]{d}}{a} i.$$

Thus our form is reduced if and only if $a \leq \sqrt{2}\sqrt[3]{d}$. Since $a, \frac{-4d}{a^2} = b$ must be coprime, any prime that divides $4d$ to an odd power must not divide a. Each prime dividing $4d$ to an even power can either not divide a, or fully divide a. The theorem thus follows. □

Unfortunately we cannot give a simpler statement of N in the above theorem, as the $\sqrt{2}\sqrt[3]{d}$ bound creates some problems (this will be in contrast to Theorem 6.2, the analogous result for the octahedron, where a simpler statement does exist). One will need to look at the exact factorization of any given d to determine the exact behaviour. However we do have a bound on N; clearly $N \leq 2^s$ where s is as in the problem statement. This bound is also exact in many cases, for example when d is a prime (or a product of odd powers of primes).

6.2 Octahedron

We first test our program with $d = \pm 1$ and compare with Edwards's results found on page 234 of [6]. For $d = 1$ we get:

$d = 1$

Our Results	Representative Point	Edwards's Results
$[0, 1, 0, 0, 0, -12, 0]$	$1.861i$	$[0, 1, 0, 0, 0, -12, 0]$
$[0, 3, 0, 0, 0, -4, 0]$	$1.075i$	$[0, 3, 0, 0, 0, -4, 0]$
$[1, 0, -1, 0, -3, 0, 27]$	$\sqrt{3}i$	$[1, 0, -1, 0, -3, 0, 27]$
$[3, 4, 1, 0, -1, -4, -3]$	$-0.268 + 0.963i$	$[-3, -4, -1, 0, 1, 4, 3]$

We matched up our results to Edwards's results using the representative point. Note that the forms on the same row are indeed equal or $GL(2, \mathbb{Z})$ equivalent (the last row only). Also of note is the representative point calculated by Edwards for $[-3, -4, -1, 0, 1, 4, 3]$ is $-0.268 + 0.964i$; the difference is due to rounding in his calculation.

For $d = -1$ we get:

$d = -1$

Our Results	Representative Point	Edwards's Results
$[0, 1, 0, 0, 0, 12, 0]$	$1.861i$	$[0, 1, 0, 0, 0, 12, 0]$
$[0, 3, 0, 0, 0, 4, 0]$	$1.074i$	$[0, 3, 0, 0, 0, 4, 0]$
$[1, -1, -1, -1, 1, -5, -17]$	$-0.158 + 1.509i$	$[-1, 1, 1, 1, -1, 5, 17]$
$[1, 0, 0, -2, 0, 0, -32]$	$1.782i$	$[-1, 0, 0, 2, 0, 0, 32]$
$[1, 0, 1, 0, -3, 0, -27]$	$\sqrt{3}i$	$[-1, 0, -1, 0, 3, 0, 27]$
$[5, 1, -1, -3, -3, -3, -9]$	$-0.436 + 1.011i$	$[-5, -1, 1, 3, 3, 3, 9]$
$[8, 4, 4, 4, 2, -1, -7]$	$-1/2 + \sqrt{3}/2i$	$[-7, -1, 2, 4, 4, 4, 8]$

We set out program to calculate the number reduced forms for d between -30 and 30. It took around 26.5 minutes to compute, and we also outputted the list of forms for each such d (the lists for a few values of d appears in Appendix B). Letting N be the number of non-equivalent reduced forms we get, then our calculations give:

d	**N**	**d**	**N**	**d**	**N**	**d**	**N**	**d**	**N**	**d**	**N**
-30	7	-20	6	-10	7	1	4	11	10	21	7
-29	8	-19	8	-9	14	2	4	12	3	22	4
-28	10	-18	5	-8	13	3	3	13	7	23	12
-27	8	-17	19	-7	9	4	6	14	4	24	5
-26	7	-16	7	-6	7	5	6	15	8	25	10
-25	18	-15	8	-5	8	6	2	16	4	26	12
-24	12	-14	7	-4	4	7	8	17	6	27	5
-23	9	-13	6	-3	6	8	7	18	6	28	10
-22	11	-12	8	-2	5	9	3	19	10	29	10
-21	4	-11	8	-1	7	10	4	20	6	30	4

There was not much to note in the list of forms, however when $d = 6, 14, 22, 30$ the list of forms all had the first and last coefficient being 0. We tested this for $d \equiv 6 \pmod 8$ between 6 and 86; the same held true for $d = 6, 14, 22, 30, 46, 62, 70, 78, 86$, but failed for $d = 38, 54$. Furthermore, for d in the first list, the size of list is in $\{2, 4, 8\}$ which are powers of two. In all cases, the solutions with $a_0 = 0$ all have exactly two nonzero coefficients, being the second and second last. For example, $d = 70$ corresponds to the list

$$[0, 1, 0, 0, 0, -840, 0] \quad [0, 3, 0, 0, 0, -280, 0] \quad [0, 5, 0, 0, 0, -168, 0]$$
$$[0, 7, 0, 0, 0, -120, 0] \quad [0, 8, 0, 0, 0, -105, 0] \quad [0, 15, 0, 0, 0, -56, 0]$$
$$[0, 21, 0, 0, 0, -40, 0] \quad [0, 24, 0, 0, 0, -35, 0]$$

Examining our list for when $d < 0$ is 6 (mod 8), we notice no similarities. This should not come as a huge surprise considering the cases $d > 0$ and $d < 0$ are somewhat different when $r = 4$.

This leads to the hypothesis that all reduced forms take this form for some "large" subset of $d \equiv 6 \pmod 8, d > 0$. Before addressing this further, we will prove a statement about the number of such reduced forms for a general d.

Theorem 6.2. *Let d be a non-zero integer, and let there be s distinct prime divisors of $-12d$. Then there are exactly 2^{s-1} non-equivalent forms $f = [a_0, a_1, \ldots, a_6] \in \mathscr{C}(4, d)(\mathbb{Z})$ such that $a_0 = a_2 = 0$. In particular, $\mathscr{C}(4, d)(\mathbb{Z})$ is non-empty.*

Proof. Following the defining equations we get

$$f = [0, a, 0, 0, 0, \frac{-12d}{a}, 0]$$

Thus we get a form for all integers a dividing $-12d$. If $b = \frac{-12d}{a}$, then we calculate the covariants $\frac{1}{2}\mathbf{t}, \mathbf{H}$ to get

$$\begin{aligned}\frac{1}{2}\mathbf{t}(f)(z_1, z_2) =& a^3 z_1^{12} - 396adz_1^8 z_2^4 + 396bdz_1^4 z_2^8 - b^3 z_2^{12} \\ \mathbf{H}(f)(z_1, z_2) =& -a^2 z_1^8 - 168dz_1^4 z_2^4 - b^2 z_2^8 \\ f(z_1, z_2) =& 6az_1^5 z_2 + 6bz_1 z_2^5\end{aligned}$$

As our form needs coprime specializations, we cannot have a prime divide both a and b, else said prime will divide all of $\frac{1}{2}\mathbf{t}, \mathbf{H}, f$. From $\left(\frac{1}{2}\mathbf{t}\right)^2 + (\mathbf{H})^3 + df^4 = 0$, coprimality among all three is equivalent to $f, \mathbf{H}$ being coprime.

I claim if a, b are coprime then the form obtained does indeed have coprime specializations. Indeed, consider $(z_1, z_2) = (1, 1)$. Then $-\mathbf{H} = a^2 - 14ab + b^2$, and $f = 6a + 6b$. As $ab = -12d$, and a, b are coprime, exactly one of a, b is even, and exactly one is a multiple of 3. Thus $2, 3 \nmid a^2 - 14ab + b^2$ and so

$$\gcd(\mathbf{H}(1,1), f(1,1)) = \gcd(a^2 - 14ab + b^2, a + b) = \gcd(a^2 - 14ab + b^2 - (a+b)^2, a + b) = \gcd(-16ab, a + b).$$

Again, $2 \nmid a+b$, and any prime factor of a, b cannot divide $a+b$. Therefore this equals 1 and the claim is proven.

We now calculate the representative points. We have $f = 6z_1 z_2(az_1^4 - \frac{12d}{a} z_2^4)$, so we have cases based on the sign of d (as we should expect by Theorem 4.20).

Case 1: $d > 0$ We note that f has 4 real roots, so we just need the appropriate root of $z^4 - \frac{12d}{a^2}$, namely $\sqrt[4]{\frac{12d}{a^2}}i$. As $a, b = \frac{-12d}{a}$ are coprime, we see that $a^2 \neq 12d$. Thus this is in the fundamental domain if and only if $a^2 < 12d$, and then it is not on the boundary. The transformation $(z_1, z_2) \to (-z_1, z_2)$ shows we can assume $a > 0$, and then all of these forms are not equivalent since their representative points are not on the boundary.

Writing $12d = p_1^{e_1} \cdots p_s^{e_s}$, each prime p_i either fully divides a or doesn't divide a. Thus there are 2^s possible choices of $a > 0$ making $a, \frac{-12d}{a}$ coprime. Such a do not satisfy $a^2 = 12d$, so they come in pairs with precicely one of the two satisfying $a^2 < 12d$, i.e. where we are in the fundamental domain. Therefore we get exactly 2^{s-1} forms.

Case 2: $d < 0$ Now we consider $g(z) = z^4 - \frac{12d}{a^2}$, which has no real roots. Following Proposition 4.16 we have roots

$$\beta_1 = \sqrt[4]{\frac{-12d}{a^2}}\left(\frac{1+i}{\sqrt{2}}\right), \quad \beta_2 = \sqrt[4]{\frac{-12d}{a^2}}\left(\frac{-1-i}{\sqrt{2}}\right),$$

and thus weights

$$\begin{aligned} u_1^2 =& |\beta_2 - \overline{\beta_2}| = \sqrt{2}\sqrt[4]{\frac{-12d}{a^2}} \\ u_2^2 =& |\beta_1 - \overline{\beta_1}| = \sqrt{2}\sqrt[4]{\frac{-12d}{a^2}} = u_1^2. \end{aligned}$$

This gives

$$g(z) = 4u_1^2\left(z^2 + \sqrt{\frac{-12d}{a^2}}\right),$$

so the representative point is $\sqrt[4]{\frac{-12d}{a^2}}i$. This case is finished exactly as in Case 1. □

Definition 6.3. If $f \in \mathscr{C}(4,d)(\mathbb{Z})$ is a form with $a_0 = a_2 = 0$, call f a *zero-form*.

Note if $f = [0, a, 0, 0, 0, \frac{-12d}{a}, 0]$ is not reduced, then the transformation $z_1 \to z_2, z_2 \to -z_1$ takes f to $f[0, \frac{12d}{a}, 0, 0, 0, -a, 0]$, which is reduced. Therefore given d, to show that a complete list of reduced forms contains only zero-forms, it suffices to show that every form is equivalent to a zero-form. The following lemma and proposition gives an alternate characterization of such forms.

Lemma 6.4. *Assume $d \in \mathbb{Z}$ is such that $3d$ is not a perfect square. If $f \in \mathscr{C}(4,d)(\mathbb{Z})$ satisfies $a_0 = a_6 = 0$, then f is a zero-form.*

Proof. As in the proof of Theorem 6.2, if $a_2 = 0$ then we are done (also $a_1 = 0$ implies $f = 0$, so $a_1 \neq 0$). Thus assume $a_1, a_2 \neq 0$, and following the equations in Appendix A we derive:

$$\begin{aligned} a_3 =& \frac{3a_2^2}{4a_1} \\ a_4 =& \frac{2a_2a_3}{3a_1} = \frac{a_2^3}{2a_1^2} \\ a_5 =& \frac{2a_3a_4}{3a_2} = \frac{a_2^4}{4a_1^3} \end{aligned}$$

Plugging this into the equation for $72d$ gives

$$72d = \frac{-3}{2}\frac{a_2^4}{a_1^2} + \frac{15}{2}\frac{a_2^4}{a_1^2} - \frac{45}{8}\frac{a_2^4}{a_1^2} = \frac{3}{8}\frac{a_2^4}{a_1^2},$$

whence

$$\left(\frac{a_2^2}{a_1}\right)^2 = 192d = 2^6 3d.$$

Thus $3d$ is a perfect square, contradiction. □

Note that the above proof still works in many (but not all) cases in which $3d$ is a perfect square, as then most resulting forms do not have coprime specializations (for example, if $a_1 \mid a_2$ then the form is always divisible by a_1).

Proposition 6.5. *Assume $d \in \mathbb{Z}$ is such that $3d$ is not a perfect square. Then $f \in \mathscr{C}(4,d)(\mathbb{Z})$ is equivalent to a zero-form if and only if it has at least two roots r_1, r_2 satisfying either 1) or 2):*
1) $r_1 = \infty$ and one of $r_2, \frac{1}{r_2}$ is an integer (and vice versa)
2) $r_1 = \frac{p_1}{q_1}$ and $r_2 = \frac{p_2}{q_2}$ with $(p_1, q_1) = (p_2, q_2) = 1$, and $|p_1 q_2 - p_2 q_1| = 1$.

Proof. Zero forms have the roots $0, \infty$, and the forms they are equivalent to are all $GL(2,\mathbb{Z})$ transformations of themselves. By considering whether $0, \infty$ go to finite or infinite places, we get that 1) or 2) always holds.

For the only if, we consider doing the if in reverse to transform our form so that it has roots at $0, \infty$. Thus $a_0 = a_6 = 0$, so by Lemma 6.4 we have a zero-form. □

Conjecture 6.6. For a "large" subset of $d > 0, d \equiv 6 \pmod 8$, every form $f \in \mathscr{C}(4,d)(\mathbb{Z})$ has two roots satisfying conditions 1) or 2).

Note that if $d \equiv 6 \pmod 8$, then $3d \equiv 2 \pmod 4$ so it cannot be a perfect square. Thus by our work in this section, a proof of the conjecture would prove that such d have only zero-forms as reduced forms, and also that there are exactly 2^{s-1} equivalence classes of forms, where s is the number of prime divisors of $12d$.

7 Further Research

In the tetrahedral case, the phenomenon of the number N of non-equivalent reduced forms being mostly even (and always even when d is odd) is potentially worth investigating. A possible approach would be: for every form $f \in \mathscr{C}(3,d)(\mathbb{Z})$, assign it a "dual form" such that equivalent forms have equivalent dual forms. If a form is never self-dual, then this would imply that N is even. The fact that any two forms are related by an element of $SL(2,\mathbb{R})^+$ could potentially lead to a way to assign the dual forms.

For the octahedron, the case of $d \equiv 6 \pmod 8$ and $d > 0$ is quite interesting: why are all reduced forms normally zero-forms, and why are there exceptions? An attempt at proving Conjecture 6.6 seems to be the the most approachable method of doing this. A plausible method would be showing the form has two rational roots, shifting one to ∞, and then showing that either the numerator or denominator of the remaining root must be 1.

A Appendix A

The defining equations of the tetrahedron, octahedron, and icosahedron can be obtained by finding algebraic expressions for τ_r, τ_6, j as seen in Theorem 4.3. One can repeat the calculations using a computer math package, or by hand if they are feeling rather ambitious. We present the final calculations as given in Edward's thesis, [6]. Note that his definition of d differs to ours by a minus sign.

For the format, we have

$$\begin{aligned} f =& \sum_{i=0}^{k} \binom{k}{i} a_i z_1^{k-i} z_2^i \\ \tau_4(f) =& A_0 z_1^{2k-8} + \cdots \\ \tau_6(f) =& B_0 z_1^{2k-12} + \cdots \end{aligned}$$

The equations we will present are useful when writing a program to do calculations, in which we also have:

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

A.1 Tetrahedron

These were presented at just after Theorem 4.3:

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

A.2 Octahedron

The defining equations $\tau_4(f) = 0$, $\tau_6(f) = 72d$ give:

$$\begin{aligned} A_0/1 : 0 =& a_0 a_4 - 4a_1 a_3 + 3a_2^2 \\ A_1/2 : 0 =& a_0 a_5 - 3a_1 a_4 + 2a_2 a_3 \\ A_2/1 : 0 =& a_0 a_6 - 9a_2 a_4 + 8a_3^2 \\ A_3/2 : 0 =& a_1 a_6 - 3a_2 a_5 + 2a_3 a_4 \\ A_4/1 : 0 =& a_2 a_6 - 4a_3 a_5 + 3a_4^2 \\ B_0 : 72d =& a_0 a_6 - 6a_1 a_5 + 15a_2 a_4 - 10a_3^2 \end{aligned}$$

A.3 Icosahedron

The defining equations are $\tau_4(F) = 0$ and $\tau_6(f) = \frac{360}{7}df$. We present A_0 through A_9, B_0, B_1, as this is all that is required for calculations.

$$
\begin{aligned}
A_0/1 : 0 =& a_0a_4 - 4a_1a_3 + 3a_2^2 \\
A_1/8 : 0 =& a_0a_5 - 3a_1a_4 + 2a_2a_3 \\
A_2/4 : 0 =& a_0(7a_6) - 12a_1a_5 - 15a_2a_4 + 20a_3^2 \\
A_3/56 : 0 =& a_0a_7 - 6a_2a_5 + 5a_3a_4 \\
A_4/14 : 0 =& 5a_0a_8 + 12a_1a_7 - 6a_2(7a_6) - 20a_3a_5 + 45a_4^2 \\
A_5/56 : 0 =& a_0a_9 + 6a_1a_8 - 6a_2a_7 - 4a_3(7a_6) + 27a_4a_5 \\
A_6/28 : 0 =& a_0a_{10} + 12a_1a_9 + 12a_2a_8 - 76a_3a_7 - 3a_4(7a_6) + 72a_5^2 \\
A_7/8 : 0 =& a_0a_{11} + 24a_1a_{10} + 90a_2a_9 - 130a_3a_8 - 405a_4a_7 + 60a_5(7a_6) \\
A_8/1 : 0 =& a_0a_{12} + 60a_1a_{11} + 534a_2a_{10} + 380a_3a_9 - 3195a_4a_8 - 720a_5a_7 + 60(7a_6)^2 \\
A_9/8 : 0 =& a_1a_{12} + 24a_2a_{11} + 90a_3a_{10} - 130a_4a_9 - 405a_5a_8 + 60(7a_6)a_7 \\
B_0/1 : 0 =& -360a_0d + a_0(7a_6) - 42a_1a_5 + 105a_2a_4 - 70a_3^2 \\
B_1/6 : 0 =& -720a_1d + 7a_0a_7 - 5a_1(7a_6) + 63a_2a_5 - 35a_3a_4
\end{aligned}
$$

B Appendix B

B.1 Tetrahedral forms list

We present the list of tetrahedral forms obtained for $d = 21, \ldots, 26$.

$d = 21$	$d = 22$	$d = 23$
$[-3,-3,0,-2,-8]$	$[-4,2,2,3,-3]$	$[0,1,0,0,-92]$
$[-2,-1,0,-6,-12]$	$[-1,1,2,6,-12]$	$[0,2,0,0,-23]$
$[0,1,0,0,-84]$	$[0,1,0,0,-88]$	$[1,1,-2,-4,-28]$
$[0,2,0,0,-21]$		$[4,2,-2,-2,-7]$

$d = 24$	$d = 25$	$d = 26$
$[-5,-1,-3,-3,3]$	$[-6,-3,-4,-2,4]$	$[-5,-2,-1,4,7]$
$[-4,0,-2,-4,3]$	$[-4,0,0,5,0]$	$[-4,-2,-2,3,9]$
$[-1,0,-2,-8,12]$	$[-3,-1,0,6,8]$	$[-3,0,1,6,1]$
$[-1,0,1,10,3]$	$[-1,0,0,10,0]$	$[-1,0,-1,-10,3]$
$[-1,3,1,1,-9]$	$[0,1,0,0,-100]$	$[0,-3,-2,-1,-12]$
$[0,1,0,0,-96]$	$[0,2,0,0,-25]$	$[0,1,0,0,-104]$
$[0,4,4,3,-4]$	$[1,2,-1,-2,-19]$	$[1,0,-3,-2,-27]$
$[3,0,-3,-2,-9]$	$[2,3,0,-2,-12]$	$[4,-1,-4,-4,-8]$
		$[4,2,-2,-3,-9]$

B.2 Octahedral forms list

We present the list of octahedral forms obtained for $d = -15, -14, -13, 13, 14, 15$.

$d = -15$	$d = -14$	$d = -13$
$[0, 1, 0, 0, 0, 180, 0]$	$[0, 1, 0, 0, 0, 168, 0]$	$[0, 1, 0, 0, 0, 156, 0]$
$[0, 4, 0, 0, 0, 45, 0]$	$[0, 3, 0, 0, 0, 56, 0]$	$[0, 3, 0, 0, 0, 52, 0]$
$[0, 5, 0, 0, 0, 36, 0]$	$[0, 7, 0, 0, 0, 24, 0]$	$[0, 4, 0, 0, 0, 39, 0]$
$[0, 8, 8, 6, 4, 25, 69]$	$[0, 8, 0, 0, 0, 21, 0]$	$[0, 12, 0, 0, 0, 13, 0]$
$[0, 9, 0, 0, 0, 20, 0]$	$[2, 1, 0, 7, 14, 21, -196]$	$[5, 1, 2, 8, 4, -4, -88]$
$[1, -10, -9, -6, -3, -18, -45]$	$[7, 3, 2, -6, -12, -12, -72]$	$[11, 1, -2, -8, -4, -4, -40]$
$[1, 0, -1, -8, -3, -16, -485]$	$[9, 3, 6, 6, -4, -12, -56]$	
$[21, 4, 7, 0, -7, -4, -21]$		

$d = 13$	$d = 14$	$d = 15$
$[0, 1, 0, 0, 0, -156, 0]$	$[0, 1, 0, 0, 0, -168, 0]$	$[0, 1, 0, 0, 0, -180, 0]$
$[0, 3, 0, 0, 0, -52, 0]$	$[0, 3, 0, 0, 0, -56, 0]$	$[0, 4, 0, 0, 0, -45, 0]$
$[0, 4, 0, 0, 0, -39, 0]$	$[0, 7, 0, 0, 0, -24, 0]$	$[0, 5, 0, 0, 0, -36, 0]$
$[0, 8, 8, 6, 4, -17, -57]$	$[0, 8, 0, 0, 0, -21, 0]$	$[0, 9, 0, 0, 0, -20, 0]$
$[0, 12, 0, 0, 0, -13, 0]$		$[1, -1, -3, -3, -15, 27, 333]$
$[1, 4, -1, 0, -3, -36, 27]$		$[5, -2, -6, -6, -12, 0, 72]$
$[15, 16, 5, 0, -5, -16, -15]$		$[9, 0, -6, -6, -12, -8, 40]$
		$[9, 18, 12, 6, 0, -16, -32]$

References

[1] F. Beukers, The Diophantine equation $Ax^p + By^q = Cz^r$, *Duke Math. J.* **91** (1998), no. 1, $61 - 88$.

[2] B. Bollobas, *Linear Analysis*, Cambridge University Press, 1990.

[3] 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), no. 6, $513 - 543$.

[4] C. Hermite, Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indéterminées, *J. reine agnew. Math.* **36** (1848)

[5] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, 1993 (translation of lecture notes from 1897).

[6] J. Edwards, A complete solution to $X^2 + Y^3 + Z^5 = 0$, *J. reine angew. Math.* **571** (2004), $213 - 236$.

[7] J. Edwards (2005). *Platonic Solids and Solutions to* $X^2 + Y^3 = dZ^r$ (Doctoral dissertation). Retrieved from `http://dspace.library.uu.nl/bitstream/handle/1874/7696/?sequence=24`

[8] Felix Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, Kegan Paul, Trench, Trübner & Co. Ltd., London, 1913 (translation of original 1884 edition)

[9] M. Stoll and J.E. Cremona, On the reduction theory of binary forms, *J. reine angew. Math.* **565** (2003), $79 - 99$.