Chapter 11

Parameterizations in $\mathbb{Z}$

This chapter describes an algorithm to construct a finite set of parameterizations of $D(r,d)(\mathbb{Z})$ for any non-zero integer $d$, with the property that their $\mathbb{Z}$-specializations include all co-prime $(X,Y,Z) \in D(r,d)(\mathbb{Z})$.

By Theorem 6.1.1 we can assume that the parameterizations are of the form $\chi(f)$ with $f \in C(r,d)(\mathbb{Z})$. By Theorem 6.2.4 constructing a complete set of parameterizations is now equivalent to giving a representative $f_\alpha$ for every $\text{SL}_2(\mathbb{Z})$-orbit of $C(r,d)(\mathbb{Z})$ that contains a binary form $f$ whose parameterization $\chi(f)$ has a co-prime $\mathbb{Z}$-specialization.

A main ingredient to this algorithm is the fact that $C(r,d)(\mathbb{R})$ is a homogeneous $\text{SL}_2(\mathbb{R})$ space. This means that we can calculate the Hermite Determinant and list all of the Hermite-reduced $f \in C(r,d)(\mathbb{Z})$ via a finite computer search.

The algorithm then takes this list and reduces it further so that to all $f$ in the list are $\text{SL}_2(\mathbb{Z})$-distinct and have a co-prime specialization. This is the output of the algorithm.

A variant on the algorithm reduces the list further to a list of $\text{GL}_2(\mathbb{Z})$ distinct forms. By Theorem 6.2.4, reducing to a set of representatives of the $\text{GL}_2(\mathbb{Z})$-orbits is equivalent to identifying $(\pm X,Y,Z) \in D(r,d)(\mathbb{Z})$.

A final section 11.7 shows how the algorithm can be generalized to produce complete sets of parameterizations to diophantine equations of the type

$$AX^2 + BY^3 = CZ^r, \quad \gcd(X,Y,Z) = 1,$$

where $A, B, C \in \mathbb{Z}$ and the unknowns $X, Y, Z$ are required to be in $\mathbb{Z}$.

11.1 Hermite Reduction Attributes

This section shows that $C(r,d)(\mathbb{R})$ is a homogeneous $\text{SL}_2(\mathbb{R})$-space. We can, therefore, associate a Hermite Determinant $\Theta$ to $C(r,d)(\mathbb{Z})$. Its value is
calculated along with the associated bounds on the coefficients of Hermite-reduced \( f \in C(r,d)(\mathbb{R}) \). A method of calculating the Representative Point of \( f \in C(r,d)(\mathbb{R}) \) is presented.

**Lemma 11.1.1.** If \( f \in C(r,d)(\mathbb{R}) \), then \( f \) has a real root.

**Proof.** The Klein forms \( \bar{f}_r \) were produced by taking the roots to be the image of the vertices of the platonic solids under the 1-1 correspondence between the Riemann Sphere \( S_2(\mathbb{R}) \) and the extended complex plane \( \mathbb{P}(\mathbb{C}) \), given by stereographic projection.

As such the roots of \( \bar{f}_r \) inherit the following properties from the platonic solid:

<table>
<thead>
<tr>
<th>(Special Properties)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No circles on ( \mathbb{P}(\mathbb{C}) ) going through an even number of roots of ( \bar{f}_r ) can go through more than 4 roots.</td>
<td></td>
</tr>
<tr>
<td>If a circle goes through 4 roots, the circle will split ( \mathbb{P}(\mathbb{C}) ) into 2 distinct regions. There will be roots in the interior of both regions.</td>
<td></td>
</tr>
</tbody>
</table>

Since the action of \( \text{GL}_2(\mathbb{C}) \) is continuous on \( \mathbb{P}(\mathbb{C}) \) and \( \text{GL}_2(\mathbb{C}) \) is connected, topological properties are \( \text{GL}_2(\mathbb{C}) \) invariant. The action also sends circles to circles.\(^1\) This means that these special properties of \( \bar{f}_r \) will be true of all \( \text{GL}_2(\mathbb{C}) \) twists as well.

Suppose that \( f \in C(r,d)(\mathbb{R}) \) has only complex roots. By shrinking a large circle enclosing all its roots we can produce a circle witnessing the fact that \( f \) cannot possibly have these special properties.

Therefore \( f \) has a real root. \( \square \)

**Theorem 11.1.2.** Let \( f \in C(r,d)(\mathbb{R}) \) and \( f' \in C(r,d')(\mathbb{R}) \) be real Klein forms.

- If \( dd' > 0 \) then \( f, f' \) are \( \text{GL}_2(\mathbb{R})^+ \)-equivalent
- If \( dd' < 0 \) and \( r \) is odd, then \( f \) is \( \text{GL}_2(\mathbb{R})^+ \)-equivalent to \( -f' \).

(Here \( \text{GL}_2(\mathbb{R})^+ \) is the set of \( \text{GL}_2(\mathbb{R}) \) matrices of positive determinant).

**Proof.** By Proposition 4.1.2, \( -f \in C(r, (-1)^rd) \), so the second claim follows from the first. We therefore assume that \( dd' > 0 \). Another call to Proposition 4.1.2 shows that we can apply a \( \text{GL}_2(\mathbb{R})^+ \) transformation and assume \( d = d' = \pm 1 \).

By Lemma 11.1.1, \( f \) has a real root. Therefore we can apply an \( \text{SL}_2(\mathbb{R}) \) transformation and assume that the root is \( \infty \) and the initial coefficients \([a_0, a_1, a_2, \ldots] \) of \( f \) are \([0, 1, 0, \ldots] \). The defining equations for \( C(r,d) \) determine \( f \) completely.

We can do the same to \( f' \). This means that \( f, f' \) are \( \text{GL}_2(\mathbb{R})^+ \)-equivalent. \( \square \)

\(^1\)where as usual we count straight lines through \( \infty \) as circles in \( \mathbb{P}(\mathbb{C}) \)
Corollary 11.1.3. If \( d \in \mathbb{R}^* \), then \( \mathcal{C}(r, d)(\mathbb{R}) \) is a homogeneous \( SL_2(\mathbb{R}) \)-space.

Theorem 11.1.4. Suppose \( f \in \mathcal{C}(r, d)(\mathbb{R}) \). Write \( f = f_1 f_2 \), where \( f_1, f_2 \) are real forms, and all roots of \( f_1 \) are real and all roots of \( f_2 \) are complex. Then:

<table>
<thead>
<tr>
<th>Class</th>
<th>Signature</th>
<th>( \Theta(f) )</th>
<th>A fast way to find the Representative Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{C}(3, d) )</td>
<td>(2, 1)</td>
<td>( 2^{8/3}</td>
<td>d</td>
</tr>
<tr>
<td>( \mathcal{C}(4, d), d &gt; 0 )</td>
<td>(4, 1)</td>
<td>( 2^{8/3}</td>
<td>d</td>
</tr>
<tr>
<td>( \mathcal{C}(4, d), d &lt; 0 )</td>
<td>(2, 2)</td>
<td>( 2^{8/3}</td>
<td>d</td>
</tr>
<tr>
<td>( \mathcal{C}(5, d) )</td>
<td>(4, 4)</td>
<td>( 2^{24/5}</td>
<td>d</td>
</tr>
</tbody>
</table>

In particular, the representative point of \( f \) can be found using at most an application of Proposition 10.2.4 to find the representative point of a biquadratic form.

Proof. We start by verifying the table for the special representatives of the 4 rows: \( \bar{f} = \bar{f}_3, \bar{f}_4, \bar{f}_4^*, \bar{f}_5 \). Certainly the signature is correct.

Using Proposition 10.2.4, we find that \( i \) is the representative point of \( \bar{f}_3 \). By Lemma 10.2.6, \( i \) is also the representative point of the other \( f \) and the suggested method in the last column is a way of finding the representative point of these \( \bar{f} \). Knowing that \( i \) is the representative point, we can use Proposition 10.2.3 and verify that the table produces the correct value for \( \Theta(\bar{f}) \). So the table is correct for \( \bar{f} \).

By Theorem 11.1.2, a general \( f \in \mathcal{C}(r, d) \) satisfies \( \pm f = \bar{f} \circ g \) for some \( g \in GL_2(\mathbb{R})^+ \). Furthermore, by Proposition 4.1.2 and Theorem 10.2.1

\[
\det(g)^6 = d, \quad \Theta(f) = |\det(g)|^6 \Theta(\bar{f}).
\]

This and the covariance of the representative point under \( GL_2(\mathbb{R})^+ \) transformations show that the table is correct for all \( f \in \mathcal{C}(r, d) \).

Theorem 11.1.5. Suppose \( f \in \mathcal{C}(r, d)(\mathbb{R}) \) is Hermite-reduced. Then the \( |a_i a_j| \) satisfy

\[
\max \{|a_i a_j| : i + j \leq k \} \leq B^2,
\]

where the bound \( B \) is given by

<table>
<thead>
<tr>
<th>Class</th>
<th>( B )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{C}(3, d) )</td>
<td>( 2\sqrt[3]{</td>
</tr>
<tr>
<td>( \mathcal{C}(4, d) )</td>
<td>( 16\sqrt[3]{</td>
</tr>
<tr>
<td>( \mathcal{C}(5, d) )</td>
<td>( 1600\sqrt[5]{</td>
</tr>
</tbody>
</table>

In particular \( |a_i| \leq B \) for all \( i \leq \frac{1}{2}k \).

Proof. The bounds are obtained applying Theorem 10.2.5 to the Hermite determinant as listed in the table in Theorem 11.1.4.
11.2 Listing Hermite-reduced $f \in C(r, d)(\mathbb{Z})$

By Theorem 11.1.5, Hermite-reduced $f \in C(r, d)(\mathbb{Z})$ have coefficients that are bounded in terms of $r$ and $d$. Furthermore, examining the defining equations of $C(r, d)$ shows that the form is known once $a_0, a_1, a_2, a_3$ is given.

The following pseudo-code shows how to produce a list of $f \in C(r, d)(\mathbb{Z})$ including all forms which are Hermite-reduced and have $a_0 \neq 0$.

```
ALGORITHM( Hermite-reduced Forms; $a_0 \neq 0$)
    INPUT (r,d)
    Calculate $B$ from the table in Theorem 11.1.5
    FOR $a_0, a_1, a_2 \in \mathbb{Z}$ with $|a_i| \leq B, a_0 \neq 0$ DO
        $Z := a_0, Y := a_0a_2 - a_1^2$
        FOR the at most 2 integers $X := \pm \sqrt{-Y^3 - dZ^r}$ DO
            Determine $a_3$ from $a_3^2 - 3a_0a_1a_2 + 2a_1^3 = 2X$
            The remaining $a_4, \ldots, a_k$ are determined from
            the equations defining $C(r, d)$
            IF all of $\Omega_r$ are integers
                AND the $a_i$ satisfy the bounds of Theorem 11.1.5
                OUTPUT the form $f = [a_0, a_1 \ldots a_k]$
            END-IF
        END-FOR
    END-FOR
END-FOR
STOP
```

A slight variant on this pseudo-code allows us to list the Hermite-reduced forms with $a_0 = 0$. We use Theorem 11.1.4 to find the representative points of the forms. We reduce our list to a set of Hermite-reduced $f \in C(r, d)(\mathbb{Z})$ by discarding any forms for which the representative point is not in the fundamental domain.

**Remark 11.2.1.** This is the computationally expensive part of the algorithm. My $C$ program running in a 350 Mhz Pentium II took 6 hours to produce the list associated with the icosahedral equation $X^2 + Y^3 = -Z^5$.

11.3 Listing $GL_2(\mathbb{Z})$-orbits of $C(r, d)(\mathbb{Z})$

In this section, we show how to take the list of Hermite-reduced forms, and reduce the list to a set of $GL_2(\mathbb{Z})$ inequivalent forms.

The group $GL_2(\mathbb{Z})$ acts on $\mathbb{C} - \mathbb{R}$. Conjugation acts freely on $\mathbb{C} - \mathbb{R}$ and commutes with the $GL_2(\mathbb{Z})$ action. Since $\mathbb{H} = (\mathbb{C} - \mathbb{R})/ <\text{conjugation}>$ it follows that $GL_2(\mathbb{Z})$ acts on $\mathbb{H}$. The $GL_2(\mathbb{Z})$ map $z \mapsto -z$ becomes $x + iy \mapsto -x + iy$ on $\mathbb{H}$. 
A fundamental domain for $GL_2(\mathbb{Z})$ is given by

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

Every $z \in \mathbb{H}$ is $GL_2(\mathbb{Z})$-equivalent to a unique $z \in D^-$. We say that a form $f$ is $GL_2(\mathbb{Z})$ reduced if $z(f) \in D^-$. We throw away all but the $GL_2(\mathbb{Z})$ reduced forms.

Furthermore 2 reduced forms $f_1, f_2$ are $GL_2(\mathbb{Z})$-equivalent if and only if $z(f_1) = z(f_2) =: z$ and $f_1 = f_2 \circ g$ for some $g \in Stab(z) := Stab(z, GL_2(\mathbb{Z}))/\pm I$. The following lemma gives us a definite test of which forms are equivalent.

**Lemma 11.3.1.** Let $i = \sqrt{-1}$ and $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Define $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Suppose $z = x + iy \in D^-$. The group $Stab(z)$ is trivial on the interior of $D^-$. On the boundary of $D^-$ it is the finite group given in the following table.

<table>
<thead>
<tr>
<th>$z$</th>
<th>$Stab(z)$</th>
<th>$#Stab(z)$</th>
<th>$z \neq i, \omega$</th>
<th>$Stab(z)$</th>
<th>$#Stab(z)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$w$</td>
<td>$&lt; ST, US &gt;$</td>
<td>6</td>
<td>$x = 0$</td>
<td>$&lt; U &gt;$</td>
<td>2</td>
</tr>
<tr>
<td>$i$</td>
<td>$&lt; S, U &gt;$</td>
<td>4</td>
<td>$</td>
<td>z</td>
<td>= 1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$x = -\frac{1}{2}$</td>
<td>$&lt; U &gt;$</td>
<td>2</td>
</tr>
</tbody>
</table>

### 11.4 Listing $SL_2(\mathbb{Z})$-orbits of $C(r, d)(\mathbb{Z})$

Only listing representatives of $GL_2(\mathbb{Z})$-orbits keeps our lists as short as possible. However by Theorem 6.2.2, every $f$ gives us potentially two parameterizations $(\pm \frac{1}{2} t(f), H(f), f)$. These correspond to one or two distinct parameterizations depending on whether the $GL_2(\mathbb{Z})$-orbit of $f$ splits into one or two $SL_2(\mathbb{Z})$-orbits. This section shows how to recognize when a $GL_2(\mathbb{Z})$-orbit splits using the representative point.

**Proposition 11.4.1.** Let a $GL_2(\mathbb{Z})$-orbit be represented by $f$ with representative point in $D^-$. Let $z = x + iy$ be that point. The binary form $f \in \mathbb{R}[s, t]$ remains the representative of a single $SL_2(\mathbb{Z})$-orbit if and only if $z$ is on the boundary of $D^-$ and:

- $(z = \omega)$ $f(s + t, -t) = f(s, t), f(-t, s + t)$ or $f(s + t, -s)$.
- $(z = i)$ $f(s, t) = f(t, s)$ or the odd index coefficients of $f$ are zero.
- $(z \neq i, \omega)$
  - $x = 0$ and the odd index coefficients of $f$ are zero.
CHAPTER 11. PARAMETERIZATIONS IN $\mathbb{Z}$

- Or $|z| = 1$ and $f(s, t) = f(t, s)$.
- Or $x = -\frac{1}{2}$ and $f(s + t, -t) = f(s, t)$.

Proof. If it is also an $\text{SL}_2(\mathbb{Z})$ class, there is a $g \in \text{SL}_2(\mathbb{Z})$ so that $f \circ g = f(s, -t)$. This must map $z = x + iy \mapsto -x + iy$. The proposition enumerates the possibilities.

11.5 Ensuring Co-prime Specializations

This section shows how we can establish whether an $f \in \mathcal{C}(r, d)(\mathbb{Z})$ has any co-prime $\mathbb{Z}$-specializations.

Proposition 11.5.1. Fix $f \in \mathcal{C}(r, d)(\mathbb{Z})$ with $d \in \mathbb{Z} \neq 0$. Either

- $\chi(f)$ has no co-prime integer specializations; or
- there are $(s_1, s_2) \in \mathbb{Z}^2$ with $|s_i| \leq N_0$ such that $\chi(f)(s_1, s_2)$ are co-prime;

where $N_0$ is the product of all odd primes dividing $Nd$.

Proof. (sketch) This is a standard application of resultant theory (e.g. [16], Chapter IX) to the forms $f, H(f)$. These forms have integer coefficients, and the primes that divide their resultant can be shown to be exactly the primes dividing $Nd$.

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

This section presents the explicit algorithm to construct a complete set of parameterizations of $\mathcal{D}(r, d)(\mathbb{Z})$ whose $\mathbb{Z}$-specializations include all co-prime $(X, Y, Z) \in \mathcal{D}(r, d)(\mathbb{Z})$.

ALGORITHM ($X^2 + Y^3 = dZ^r$)

INPUT ($r, d$)

- Produce a complete list of Hermite-reduced $f \in \mathcal{C}(r, d)(\mathbb{Z})$ (section 11.2)
- Reduce the list down to a set of $\text{GL}_2(\mathbb{Z})$ inequivalent forms (section 11.3)
- Remove forms not specializing to co-prime integers (section 11.5)

OUTPUT($f_1, f_2, \ldots, f_n$)

STOP

For every co-prime integer solution $(X, Y, Z)$, at least one of $(\pm X, Y, Z)$ is an integer specialization of one of the parameterizations $\chi(f_1), \ldots, \chi(f_n)$. By Theorem 6.2.2, this list is minimal.

If you do not like the $\pm$ you should add $f_i(x_1, s_2)^*: = f_i(x_1, -x_2)$ to the list for every $f_i$ whose $\text{GL}_2(\mathbb{Z})$-equivalence class splits into two $\text{SL}_2(\mathbb{Z})$ classes. Section 11.4 shows how to identify such forms. The integer specializations of this larger list $\chi(f_1), \ldots, \chi(f_m)$ includes all co-prime integer solutions. By Theorem 6.2.2, this list is also minimal.
11.7 Generalizing to $AX^2 + BY^3 = CZ^r$

In this section we show how the algorithm can be generalized to some other diophantine problems associated to the indices $\{2, 3, r\}$.

**Proposition 11.7.1.** Fix a non zero integer $d$ and a finite set of primes $S$. There is a finite set of solutions in $\mathbb{Z}_S[x_1, x_2]$ to

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

such that

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

**Proof.** Suppose $f \in \mathcal{C}(r, d)(\mathbb{C})$, $\lambda \in \mathbb{C}^*$ and $s_1, s_2 \in \mathbb{C}$. If $\chi(f)(s_1, s_2) = (X, Y, Z)$ then

$$\chi(f)(\lambda s_1, \lambda s_2) = (\lambda^{N/2}X, \lambda^{N/3}Y, \lambda^{N/r}).$$

(11.1)

The claim about $\mathbb{Z}_S$ solutions follows from the claim about $\mathbb{Z}$ solutions. We assume $X, Y, Z$ are $\mathbb{Z}$-integers. By (11.1) we can assume that the valuation of $\gcd(X^2, Y^3, Z^r)$ at any prime $p$ is less than $N$.

Take a prime $p$ that divides $\gcd(X, Y)$. If $p^3|dZ^r$ then:

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

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

$$X'^2 + Y'^3 = d'Z'^r.$$

In this way we can reduce to a finite set of equations in which we can assume that if $p$ divides $\gcd(X, Y)$ then $\nu_p(Z^r)$ is less than 5. For $r = 5$ this is equivalent to assuming $\gcd(X, Y, Z) = 1$. For $r = 3, 4$ it is that $p|\gcd(X, Y)$ implies that $\nu_p(Z) = 0$ or 1.

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

**Theorem 11.7.2.** Fix $r \in \{3, 4, 5\}$. Fix a finite set of primes $S$. Fix $A, B \in \mathbb{Z}_S^*$ and non zero $C \in \mathbb{Z}_S$. Then there is a finite set of solutions in $\mathbb{Z}_S[x_1, x_2]$ to

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

such that
CHAPTER 11. PARAMETERIZATIONS IN $\mathbb{Z}$

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

Proof. Without loss of generality $A, B, C \in \mathbb{Z}$. Multiply the diophantine equation by $A^3B^2$ to give:

$$(A^2BX)^2 + (ABY)^3 = (A^3B^2C)Z^r.$$

Since $A^2B, AB \in \mathbb{Z}_S$ the theorem follows from Proposition 11.7.1. \qed