Topological uniqueness results for Lefschetz fibrations over the disc

Aknazar Kazhymurat
+7 (747) 200–11–48
fourier845@gmail.com

under the direction of

Mr. Barış Kartal
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
July 31, 2018

Abstract

We prove that a Lefschetz fibration over the disc that, after compactification, has the same singular fibers as an extremal rational elliptic surface can be obtained by deleting a singular fiber and a section from the rational extremal elliptic surface, i.e. such a Lefschetz fibration is determined up to topological equivalence by its set of singular of fibers. In general, a Lefschetz fibration is not determined by its set of singular fibers.

The main theorem is the first known topological uniqueness result for Lefschetz fibrations of genus 1 over the disc (as opposed to the sphere). We get a complete clasification of Lefschetz fibrations with 2 I_1 fibers as a byproduct of our results.

The proof is inspired by homological mirror symmetry and Karpov–Nogin's theorem on constructivity of helices on del Pezzo surfaces.

It would be interesting to extend our results to the case of Lefschetz fibrations that have the same singular fibers as an extremal K3 surface.

Summary

We study Lefschetz fibrations over the disc. A Lefschetz fibration can be vizualized as a continuous assignment of a torus (i.e. the surface of a doughnut) to every point on the 2-dimensional disc. For some points, the assigned torus degenerates to a sphere. We prove that under additional hypotheses a Lefschetz fibration is uniquely determined by the number of points where torus degenerates to a sphere.

1 Introduction

Morse theory describes the topology of a smooth manifold in terms of the critical points of a generic smooth real-valued function on it. Given a Morse function on a smooth manifold one can construct a handle decomposition of this manifold (see e.g. [1]).

Picard–Lefschetz theory is a complex analogue of Morse theory where the role of Morse functions is played by Lefschetz fibrations, i.e. holomorphic maps to the Riemann sphere with non-degenerate critical points.

Lefschetz fibrations were later extended to the setting of symplectic manifolds. Donaldson has shown that every compact symplectic manifold, possibly after removing a real codimension 2 submanifold, is a total space of some Lefschetz fibration. Because the class of compact symplectic manifold is topologically diverse (for example, every finitely presented group arises as a fundamental group of some compact symplectic 4-manifold [2]), this shows that Lefschetz fibrations are a powerful instrument to understand the topology of 4-manifolds.

There is no general classification result known for Lefschetz fibrations. The rich topological behaviour displayed by Lefschetz fibrations makes such a classification inaccessible with the present tools; for example, Lefschetz fibrations of genus at least 2 over the disk were used by Ozbagci [3] to find contact 3-manifolds admitting infinitely many pairwise non-diffeomorphic Stein fillings. Prior to Auroux [4], however, it was generally believed that the classification of Lefschetz fibrations of genus 1 over the disk is comparatively simple.

Auroux [4] constructed examples of 2 inequivalent Lefschetz fibrations of genus 1 over the disk with 2 singular fibers. His construction relied on the connection between Lefschetz fibrations and factorizations in the mapping class group. His results imply that there exist contact 3-manifolds admitting 2 inequivalent Stein fillings with diffeomorphic total spaces. This demonstrates the interesting topology of Lefschetz fibrations with 2 singular fibers over the disc.

The main result of the paper for each of the 14 extremal rational types there exists only one Lefschetz fibration up to topological equivalence. This implies, in particular, that every Lefschetz fibration of extremal rational type is algebraic. Furthermore, we obtain a complete classification of Lefschetz fibrations with 2 singular fibers of type I_1.

In Section 2 we define Lefschetz fibrations and describe their relationship to monodromy factorizations in the mapping class group. In Section 3 we prove Proposition 3.2 connecting monodromy factorizations and algebraic intersection numbers of vanishing cycles. In Section 4 we use Proposition 3.2 to prove that the algebraic intersection numbers of vanishing cycles satisfy Markov type equations. The transitivity of the braid group action on the set of positive integral solutions of Markov type equations, first established by Karpov–Nogin [5], then implies the topological uniqueness of the Lefschetz fibration over the disc with extemal rational type.

2 Preliminaries

Mapping class group

Let Σ be a compact oriented surface with boundary $\partial\Sigma$. *The mapping class group* of Σ is the group $\mathrm{MCG}(\Sigma)$ of isotopy classes of orientation-preserving homeomorphisms of Σ that fix ∂M pointwise.

Let $\Sigma_{1,1}$ be the torus with one boundary component. It is known that $\mathrm{MCG}(\Sigma_{1,1}) \approx B_3$ [6].

The first singular homology group of $\Sigma_{1,1}$ has rank 2 as a $\mathbb{Z}$-lattice. The intersection form $\langle \cdot, \cdot \rangle$ defines a symplectic form on $H_1(\Sigma_{1,1}, \mathbb{Z})$.

The group $\mathrm{MCG}(\Sigma_{1,1})$ has a natural representation on $H_1(\Sigma_{1,1}, \mathbb{Z})$ called the *symplectic representation*. This representation is a surjective homomorphism $\mathrm{MCG}(\Sigma_{1,1}) \to SL(2, \mathbb{Z})$ whose kernel coincides with the center of $\mathrm{MCG}(\Sigma_{1,1})$ (see for example [6]). A Dehn twist

around a simple closed curve C acts on a homology class $\gamma \in H_1(\Sigma_{1,1}, \mathbb{Z})$ as follows

$$\tau_C \gamma = \gamma + \langle [C], \gamma \rangle [C]. \tag{1}$$

The group $\mathrm{MCG}(\Sigma_{1,1})$ is generated by the Dehn twists τ_a, τ_b around any two simple closed curves intersecting transversely at one point. The Dehn twist around a curve parallel to the boundary component is $\delta = (\tau_a \tau_b)^6$. It generates the kernel of the symplectic representation $\mathrm{MCG}(\Sigma_{1,1}) \to SL(2, \mathbb{Z})$.

The abelianization of $\mathrm{MCG}(\Sigma_{1,1})$ is $\mathbb{Z}$. Under the abelianization map Dehn twists around non-separating simple closed curves map to 1, while δ maps to 12 [6].

Remark 2.0.1. For $\Sigma_{1,1}$, every primitive homology class contains exactly one isotopy class of simple closed curves [7], [6]. This means that to specify the Dehn twist τ_C around a curve C it is enough to give the homology class $[C] \in H_1(\Sigma_{1,1}, \mathbb{Z})$.

Lefschetz fibrations

A *Lefschetz fibration* over the disc is a smooth surjective map $f : M \to D^2$ from a compact oriented smooth 4-dimensional manifold M with boundary ∂M to the closed 2-disc D^2 having the following properties:

- it is a submersion away from the critical points;
- it has finitely many critical points and each critical point is non-degenerate and lies in the interior of D^2;
- each critical point has an orientation-preserving complex chart in which $f(z_1, z_2) = z_1^2 + z_2^2$.

Note that some authors require f to be injective on the set of critical points.

Let $f : M \to D^2$ be a Lefschetz fibration with critical points $p_1, \ldots, p_r$. A *smooth fiber* of the Lefschetz fibration $f : M \to D^2$ is the preimage under f of a point in $D^2 \backslash \{f(p_1), \ldots, f(p_r)\}$.

Ehresmann's lemma shows that smooth fibers corresponding to two different points in $D^2/\{f(p_1),\ldots,f(p_r)\}$ are diffeomorphic.

Analogously, a *singular fiber* of the Lefschetz fibration $f : M \to D^2$ is the preimage under f of $f(p_i) \in D^2$ for some i, $1 \leq i \leq r$. The Lefschetz fibrations we consider have singular fibers of the following type:

- type I_1, i.e. an immersed sphere of homological self-intersection 0 with one positive double point;
- type I_n, $n \geq 2$, i.e. a chain of n spheres with homological self-intersection -2.

Let $f : M \to D^2$ be a Lefschetz fibration with critical values $p_1,\ldots,p_r$. Ehresmann's lemma implies that the restriction of f to a map $M\backslash\{f^{-1}(p_1),\ldots,f^{-1}(p_r)\} \to D^2\backslash\{p_1,\ldots,p_r\}$ is a fiber bundle E. Fix a reference point $p_* \in D^2\backslash\{p_1,\ldots,p_r\}$ whose fiber $f^{-1}(p_*)$ we denote as F. Choose a set of paths $l_i : [0,1] \to M\backslash\{f^{-1}(p_1),\ldots,f^{-1}(p_r)\}$ for $1 \leq i \leq r$ such that $l_i(0) = l(i) = p_*$ and such that l_i encloses p_i and no other critical values. The paths l_i are called *vanishing paths*. We can consider the pullback of the fiber bundle E to $[0,1]$. Since every fiber bundle over $[0,1]$ is trivial, there exists a trivialization $T : [0,1] \times F \to l_i^* E$. The induced diffeomorphism $T|_{\{1\}\times F} \cdot T^{-1}|_{\{0\}\times F}$, which is a well-defined element of the mapping class group of F, is called *the monodromy* around p_i. It can be shown that the monodromy around a critical value p_i corresponding to a fiber of type I_n is equal to the n-th power of a Dehn twist around some simple closed curve $C \subset F$; this curve is called *the vanishing cycle* of the fiber $f^{-1}(p_i)$ [8].

The ordered set of monodromies around points p_i is called *the monodromy factorization* of f. Lefschetz fibration can be reconstructed (up to topological equivalence) from its monodromy factorization. There are two group actions on the set of monodromy factorizations that preserve the corresponding Lefschetz fibration:

- The braid group

$$B_r = \langle \sigma_1, \ldots, \sigma_{r-1} | \sigma_i\sigma_j = \sigma_j\sigma_i \text{if} |i-j| \geq 2, \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{for} 1 \leq i \leq n-2 \rangle \quad (2)$$

acts by *Hurwitz moves* (or *mutations*)

$$\sigma_i : (\tau_1, \ldots, \tau_i, \tau_{i+1}, \ldots, \tau_r) \to (\tau_1, \ldots, \tau_i\tau_{i+1}\tau_i^{-1}, \tau_i, \ldots, \tau_r) \qquad \text{for } 1 \leq i \leq r.$$

- The mapping class group of the smooth fiber F acts by *global conjugation*

$$\phi : (\tau_1, \ldots, \tau_r) \to (\phi\tau_1\phi^{-1}, \ldots, \phi\tau_r\phi^{-1}).$$

The problem of classifying Lefschetz fibrations over the disc is equivalent to the problem of classifying the equivalence classes of monodromy factorizations up to Hurwitz moves and global conjugation (see for example [9]).

Lefschetz fibrations of genus 1

We restrict to the case of Leschetz fibrations with smooth fiber diffeomorphic to a torus with one boundary component $\Sigma_{1,1}$.

Definition 2.0.1. *A Lefschetz fibration of extremal rational type* is a Lefschetz fibration having 3 singular fibers of type I_{l_0}, I_{m_0}, I_{n_0} for l_0, m_0, n_0 assuming values indicated in Table 1 such that, for some choice of vanishing paths, the vanishing cycles C_1, C_2, C_3 satisfy

$$\tau_{C_1}^{l_0}\tau_{C_2}^{m_0}\tau_{C_3}^{n_0} = \delta\tau_C^{m_0+l_0+n_0-12}. \quad (3)$$

for some non-separating simple closed curve $C \subset \Sigma_{1,1}$.

Remark 2.0.2. Each of the 14 extremal rational types is realized by a Lefschetz fibration constructed by deleting a singular fiber and a section from an extremal rational elliptic surface. Note that extremal rational elliptic surfaces have been completely classified by Miranda–Ulf [10].

Table 1: The possible values of l_0, m_0, n_0, and the configuration of vanishing cycles with the least possible intersection numbers realizing the given extremal rational type. Here $[u]$, $[v]$ denote some symplectic basis of $H_1(\Sigma_{1,1}, \mathbb{Z})$.

Number	l_0	m_0	n_0	$[C_{1,min}]$	$[C_{2,min}]$	$[C_{3,min}]$	$[C_{min}]$
(1)	1	1	1	$[v]-3[u]$	$[v]$	$[v]+3[u]$	$[u]$
(2)	1	1	2	$[v]-4[u]$	$[v]$	$[v]+2[u]$	$[u]$
(3)	1	2	3	$[v]-3[u]$	$[v]$	$[v]+[u]$	$[u]$
(4)	1	1	5	$[v]+3[u]$	$2[v]+[u]$	$[v]$	$[u]$
(5)	2	2	4	$[v]-2[u]$	$[v]$	$[v]+[u]$	$[u]$
(6)	3	3	3	$[v]-3[u]$	$[v]$	$[v]+3[u]$	$[u]$
(7)	1	2	6	$2[v]-3[u]$	$[v]$	$[v]+[u]$	$[u]$
(8)	1	1	8	$2[v]-3[u]$	$2[v]-[u]$	$[v]$	$[u]$
(9)	2	4	4	$2[v]-[u]$	$[v]$	$[v]$	$[u]$
(10)	1	3	6	$3[v]-2[u]$	$[v]$	$[v]+[u]$	$[u]$
(11)	1	1	9	$3[v]-2[u]$	$3[v]-[u]$	$[v]$	$[u]$
(12)	2	2	8	$4[v]-3[u]$	$2[v]-[u]$	$[v]$	$[u]$
(13)	2	3	6	$3[v]-2[u]$	$2[v]-[u]$	$[v]$	$[u]$
(14)	1	5	5	$5[v]-3[u]$	$2[v]-[u]$	$[v]$	$[u]$

3 Computations in the mapping class group

Binary quadratic forms f and g are called *equivalent* if there exist a, b, c, $d \in \mathbb{Z}$ such that

$$f(ax+by, cx+dy) = g(x,y), \qquad ad-bc=1.$$

It is well-known that the discriminants of equivalent quadratic forms are equal.

Let us fix a symplectic basis $[u]$, $[v]$ of $H_1(\Sigma_{1,1}, \mathbb{Z})$. For any $\phi \in \mathrm{MCG}(\Sigma_{1,1})$, the expression

$$\langle \phi\gamma, \gamma \rangle$$

for $\gamma = p[v]+q[u]$ defines a binary quadratic form in p, q. We denote its discriminant as $d(\phi)$. Note that $d(\phi)$ does not depend on the choice of symplectic basis of $H_1(\Sigma_{1,1}, \mathbb{Z})$ because any two symplectic bases are related by an element of $SL(2,\mathbb{Z})$ (so the resulting quadratic forms are equivalent).

Lemma 3.1. *Let C_1, $C_2 \subset \Sigma_{1,1}$ be simple closed curves with intersection $[C_1] \cdot [C_2] = a$.*

Then for positive integers m, n we have

$$d(\tau_{C_1}^m \tau_{C_2}^n) = m^2 n^2 a^4 - 4mna^2.$$

Proof. Choose a symplectic basis $[u]$, $[v]$ of $H_1(\Sigma_{1,1}, \mathbb{Z})$ such that

$$[C_1] = [u], \qquad [C_2] = a[v] + b[u]$$

for some $b \in \mathbb{Z}$.

Compute the value of the quadratic form $\langle \tau_{C_1}^m \tau_{C_2}^n \gamma, \gamma \rangle$ for a homology class $\gamma = p[v] + q[u]$

$$\tau_{C_2}^n \gamma - \gamma = n\langle [C_2], \gamma \rangle [C_2],$$

$$\tau_{C_1}^m \tau_{C_2}^n \gamma - \gamma = m\langle [C_1], \gamma \rangle [C_1] + n\langle [C_2], \gamma \rangle [C_2] + mn\langle [C_2], \gamma \rangle \langle [C_1], [C_2] \rangle [C_1],$$

$$\langle \tau_{C_1}^m \tau_{C_2}^n \gamma, \gamma \rangle = m\langle [C_1], \gamma \rangle^2 + n\langle [C_2], \gamma \rangle^2 + mn\langle [C_1], \gamma \rangle \langle [C_2], \gamma \rangle \langle [C_1], [C_2] \rangle =$$

$mp^2 + n(bp - aq)^2 + mnp(bp - aq)a = (m + nb^2 + mnab)p^2 - a(2nb + mna)pq + na^2q^2$.

Therefore,

$$d(\tau_{C_1}^m \tau_{C_2}^n) = a^2(2nb + mna)^2 - 4(m + nb^2 + mnab)na^2 = m^2n^2a^4 - 4mna^2.$$

□

Proposition 3.2. *Let C_1, C_2, C_3, $C_4 \subset \Sigma_{1,1}$ be non-separating simple closed curves such that*

$$\tau_{C_1}^m \tau_{C_2}^n = \delta \tau_{C_3}^{-k} \tau_{C_4}^{-l} \tag{4}$$

for some $m, n, k, l \in \mathbb{N}$. Then

$$mn\langle [C_1], [C_2] \rangle^2 = lk\langle [C_3], [C_4] \rangle^2.$$

Proof. Note that under the abelianization map $\mathrm{MCG}(\Sigma_{1,1}) \to \mathbb{Z}$ the element δ maps to 12 while Dehn twists around non-separating curves map to 1. Therefore, Equation (4) implies that $m + n + k + l = 12$.

Let us consider the action of both sides of Equation (4) on a homology class $\gamma \in H_1(\Sigma_{1,1}, \mathbb{Z})$

$$\gamma + n\langle [C_2], \gamma \rangle [C_2] + m\langle [C_1], \gamma \rangle [C_1] + mn\langle [C_2], \gamma \rangle \langle [C_1], [C_2] \rangle [C_1] =$$
$$\gamma - l\langle [C_4], \gamma \rangle [C_4] - k\langle [C_3], \gamma \rangle [C_3] + kl\langle [C_4], \gamma \rangle \langle [C_3], [C_4] \rangle [C_3]. \tag{5}$$

Let us first deal with the case $\langle [C_1], [C_2] \rangle = 0$. Because $[C_1]$ and $[C_2]$ are primitive homology classes by assumption, this implies $[C_1] = \pm [C_2]$. We claim that then necessarily $\langle [C_3], [C_4] \rangle = 0$. To see this, consider (5) for $\gamma = [C_1]$

$$l\langle [C_4], [C_1] \rangle [C_4] = k(l\langle [C_4], [C_1] \rangle \langle [C_3], [C_4] \rangle - \langle [C_3], [C_1] \rangle)[C_3]. \tag{6}$$

If $\langle [C_4], [C_1] \rangle \neq 0$, then Equation 6 implies that $[C_4] = \lambda [C_3]$ for some $\lambda \in \mathbb{Q}$ so $\langle [C_3], [C_4] \rangle = 0$.

If $\langle [C_4], [C_1] \rangle = 0$, then Equation (6) implies that $\langle [C_3], [C_1] \rangle = 0$. Because $[C_1]$, $[C_3]$, and $[C_4]$ are primitive homology classes, we have $[C_3]$, $[C_4] = \pm [C_1]$ so $\langle [C_3], [C_4] = 0$.

Now we assume that $\langle [C_1], [C_2] \rangle \neq 0$. Lemma 3.1 shows that

$$m^2 n^2 \langle [C_1], [C_2] \rangle^4 - 4mn \langle [C_1], [C_2] \rangle^2 = k^2 l^2 \langle [C_3], [C_4] \rangle^4 - 4kl \langle [C_3], [C_4] \rangle^2.$$

By rearranging the terms we get

$$(mn\langle [C_1], [C_2] \rangle^2 - kl\langle [C_3], [C_4] \rangle^2)(mn\langle [C_1], [C_2] \rangle^2 + kl\langle [C_3], [C_4] \rangle^2) =$$
$$4(mn\langle [C_1], [C_2] \rangle^2 - kl\langle [C_3], [C_4] \rangle^2).$$

If $mn\langle [C_1], [C_2] \rangle^2 - kl\langle [C_3], [C_4] \rangle^2 \neq 0$, we can simplify to get

$$mn\langle [C_1], [C_2] \rangle^2 + kl\langle [C_3], [C_4] \rangle^2 = 4. \tag{7}$$

Note that $\langle [C_1], [C_2] \rangle^2 \geq 1$ and $\langle [C_3], [C_4] \rangle^2 \geq 1$. Because $m + n + k + l = 12$, at least one of the summands on the left-hand side of Equation (7) is larger than or equal to 5. Therefore, Equation (7) cannot hold. □

4 Topological uniqueness for Lefschetz fibration of extremal rational type

In this section we prove the topological uniqueness of Lefschetz fibrations of extremal rational type. To do this, we prove that the intersection numbers of C_1, C_2, C_3 with C are related by a Markov-type equation (11). We then verify that the transitive action of the braid group on the set of positive integral solutions of Equation 11 is realized at the level of

vanishing cycles by Hurwitz moves (Lemma 4.6). This implies that by a sequence of Hurwitz moves, we can reduce the intersection numbers of C_1, C_2, C_3 with C to 1. After this, the problem is solved by an application of the change of coordinates principle in the sense of Margalit–Farb [6] (Lemma 4.8).

Let C_1, C_2, C_3 be non-separating simple closed curves in $\Sigma_{1,1}$ such that

$$\tau_{C_1}^l \tau_{C_2}^m \tau_{C_3}^n = \delta \tau_C^{-9} \tag{8}$$

for some non-separating simple closed curve C. The integers l, m, n are some permutation of l_0, m_0, n_0 of Table 1.

Denote the algebraic intersections numbers as follows

$$x = \langle [C], [C_1] \rangle, \qquad y = \langle [C], [C_2] \rangle, \qquad z = \langle [C], [C_3] \rangle. \tag{9}$$

Lemma 4.1. *The following equations hold (possibly after a change of orientation of C_1 and C_3)*

$$\langle C_1, C_2 \rangle = -\sqrt{\frac{(12-l-m-n)n}{lm}} z, \qquad \langle C_2, C_3 \rangle = -\sqrt{\frac{(12-l-m-n)l}{mn}} x. \tag{10}$$

Proof. Let us apply Proposition 3.2 to the factorizations

$$\tau_{C_1}^l \tau_{C_2}^m = \delta \tau_C^{l+m+n-12} \tau_{C_3}^{-n}$$

and

$$\tau_{C_2}^m \tau_{C_3}^n = \delta \tau_{C_1}^{-l} \tau_C^{l+m+n-12}.$$

Then

$$lm\langle C_1, C_2 \rangle^2 = (12-l-m-n)nxz^2, \qquad mn\langle C_2, C_3 \rangle^2 = (12-l-m-n)lx^2.$$

Because the Dehn twist around a curve does not depend on the orientation of the curve, we may orient C_1 and C_3 in such a way that (10) holds. □

Proposition 4.2. *The following equation holds*

$$lx^2 + my^2 + nz^2 = \sqrt{lmn(12-l-m-n)}xyz. \tag{11}$$

Proof. Consider the factorization

$$\tau_{C_2}^m \tau_{C_3}^n = \delta \tau_{C_1}^{-l} \tau_C^{l+m+n-12}. \tag{12}$$

The right-hand side of Equation (12) applied to $[C] \in H_1(\Sigma_{1,1}, \mathbb{Z})$ gives

$$\delta\tau_{C_1}^{-l}\tau_C^{l+m+n-12}[C] = [C] - l\langle [C_1], [C]\rangle [C_1], \tag{13}$$

while the left-hand side of Equation (12) gives

$$\tau_{C_2}^m\tau_{C_3}^n[C] = [C] + m\langle [C_3], [C]\rangle [C_3] + n\langle [C_2], [C]\rangle [C_2] + mn\langle [C_3], [C]\rangle\langle [C_2], [C_3]\rangle [C_2]. \tag{14}$$

Considering the intersection number of (13) and (14) with $[C]$ we get the following

$$-lx^2 = mz^2 + ny^2 + mnz\langle [C_2], [C_3]\rangle y. \tag{15}$$

Equations (10) and (15) imply the statement of the proposition. □

Proposition 4.3. *$x, y, z \neq 0$.*

Proof. Assume without loss of generality that $x = 0$. Then Equation (11) implies that y and z are zero as well, i.e. $[C_1]$, $[C_2]$, $[C_3]$ all have zero algebraic intersection with $[C]$. Because $[C_1]$, $[C_2]$, $[C_3]$ are primitive homology classes, this means that all of them are equal to $\pm[C]$. Therefore, we have the following identity

$$\tau_C^{12} = \delta. \tag{16}$$

The right-hand side of Equation (16) acts on $H_1(\Sigma_{1,1}, \mathbb{Z})$ trivially while the left-hand side acts non-trivially because C is assumed to be non-separating. This is a contradiction. □

The following lemma is necessary for the proof of Lemma 4.6 as it controls the effect of Hurwitz moves on x, y, z.

Lemma 4.4. *The following equality holds*

$$\langle [C_1], [C_3]\rangle + m\langle [C_1], [C_2]\rangle\langle [C_2], [C_3]\rangle = \sqrt{\frac{(12-l-m-n)m}{ln}}y. \tag{17}$$

Proof. Consider the action of both sides of Equation (8) on $[C] \in H_1(\Sigma_{1,1}, \mathbb{Z})$

$$\begin{aligned}
&[C] + n\langle [C_3], [C]\rangle [C_3] + \\
&m\langle [C_2], [C]\rangle [C_2] + mn\langle [C_3], [C]\rangle\langle [C_2], [C_3]\rangle [C_2] + \\
&l\langle [C_1], [C]\rangle [C_1] + ln\langle [C_3], [C]\rangle\langle [C_1], [C_3]\rangle [C_1] + \\
&lm\langle [C_2], [C]\langle [C_1], [C_2]\rangle [C_1] + lmn\langle [C_3], [C]\rangle\langle [C_2], [C_3]\rangle\langle [C_1], [C_2]\rangle [C_1] = [C].
\end{aligned} \tag{18}$$

Consider the intersection number of both sides of Equation (18) with $[C]$

$$nz^2 + my^2 + mn(-z)\langle [C_2], [C_3]\rangle(-y) + lx^2 +$$

$$ln(-z)\langle [C_1], [C_3]\rangle(-x) + lm(-y)\langle [C_1], [C_2]\rangle(-x) + lmn(-z)\langle [C_2], [C_3]\rangle\langle [C_1], [C_2]\rangle(-x) = 0.$$

Substitute Equation (10)

$$nz^2 + my^2 - \sqrt{(12-l-m-n)lmn}xyz + lx^2 + lnxz\langle [C_1], [C_3]\rangle -$$

$$\sqrt{(12-l-m-n)lmn}xyz + lmn(-z)\langle [C_2], [C_3]\rangle\langle [C_1], [C_2]\rangle(-x) = 0.$$

Simplifying using Equation (11) gives Equation (17). □

Since Dehn twists do not depend on the orientation on the vanishing cycles, there is some ambiguity in the choice of orientation on C_1, C_2, C_3. Let us fix it by adding additional restrictions.

Definition 4.4.1. A choice of orientation on C_1, C_2, C_3 is called *admissible* if $x, y, z > 0$ and Equation (10) is satisfied.

Lemma 4.5. *There exists a unique admissible choice of orientation on C_1, C_2, C_3.*

Proof. The uniqueness follows from the requirement $x, y, z > 0$. Let us prove existence of an admissible choce of orientation. We have already proved that it is possible to orient C_1, C_2, C_3 in such a way that Equation (10) and thus Equation (11) hold. Because the left-hand side of Equation (11) is strictly positive (Proposition 4.3), we see that either none of x, y, z is negative (in which case we are done) or exactly two are negative —- in this case we change the orientation of the two corresponding curves. Such a change of orientation preserves Equation (10); to see this, assume without loss of generality that we change orientation on C_1, C_2. Then $\langle [C_1], [C_2]\rangle$ and $\langle [C], [C_3]\rangle$ are not changed while $\langle [C_2], [C_3]\rangle$ and $\langle [C], [C_1]\rangle$ both change sign. Therefore, Equation (10) is preserved. □

Definition 4.5.1. *Mutations* are the following 3 transformations of vanishing cycles

1. $(C_1, C_2, C_3) \to (C_1, -\tau_{C_2}^m C_3, C_2)$,

2. $(C_1, C_2, C_3) \to (-\tau_{C_1}^{l} C_2, C_1, C_3)$,

3. $(C_1, C_2, C_3) \to (C_2, -\tau_{C_2}^{-m} C_1, C_3)$.

Lemma 4.6. *Mutations of vanishing cycles preserve the admissible orientation and Equations* (8) *and* (10) *if we change l, m, n as follows*

1. $(l', m', n') = (l, n, m)$ *for mutation 1;*

2. $(l', m', n') = (m, l, n)$ *for mutation 2;*

3. $(l', m', n') = (m, l, n)$ *for mutation 3.*

Proof. We only write the proof for mutation 1. The proof for other mutations is analogous.

Equation (8) is preserved because $\tau_{C_1}^{l} \tau_{-\tau_{C_2}^{m} C_3}^{n} \tau_{C_2}^{m} = \tau_{C_1}^{l} \tau_{C_2}^{m} \tau_{C_3}^{n} \tau_{C_2}^{-m} \tau_{C_2}^{m} = \tau_{C_1}^{l} \tau_{C_2}^{m} \tau_{C_3}^{n} = \delta \tau_C^{-9}$. Equation (10) is preserved because

$$\langle [C_1'], [C_2'] \rangle = -\langle [C_1], [C_3] \rangle - m \langle [C_2], [C_3] \rangle \langle [C_1] = -\sqrt{\frac{(12 - l - m - n)m}{ln}} y, [C_2] \rangle =$$

$$\langle [C_2'], [C_3'] \rangle = \langle [C_2], [C_3] \rangle = -\sqrt{\frac{(12 - l - m - n)l}{mn}} x.$$

To verify that the admissible orientation is preserved we only need to verify that $y' = -z + m\langle [C_2], [C_3] \rangle y > 0$:

$$z - m\langle [C_2], [C_3] \rangle y = \sqrt{\frac{(12 - l - m - n)lm}{n}} xy - z = \frac{lx^2 + my^2 + nz^2}{\sqrt{n} z} - z > 0.$$

□

The following Lemma is proved in [5].

Lemma 4.7. *Any 3 vanishing cycles satisfying* (8) *can be transformed by mutations to vanishing cycles C_1', C_2', C_3' such that*

$$\langle [C], [C_1'] \rangle = \langle [C], [C_{1,min}] \rangle, \qquad \langle [C], [C_2'] \rangle = \langle [C], [C_{2,min}] \rangle,$$
$$\langle [C], [C_3'] \rangle = \langle [C], [C_{3,min}] \rangle = 1. \tag{19}$$

Lemma 4.8. *Let C_1', C_2', C_3' be simple closed curves in $\Sigma_{1,1}$ that satisfy the conclusion of Lemma 4.7. Then the factorizations $\tau_{C_1'}^{l} \tau_{C_2'}^{m} \tau_{C_3'}^{n}$ and $\tau_{C_{1,min}}^{l} \tau_{C_{2,min}}^{m} \tau_{C_{3,min}}^{n}$ are globally conjugate.*

Proof. Denote the homology class of C as $[u] \in H_1(\Sigma_{1,1}, \mathbb{Z})$. Since C is a non-separating simple closed curve, there exists a $[v] \in H_1(\Sigma_{1,1}, \mathbb{Z})$ such that $[u]$ and $[v]$ form a symplectic basis of $H_1(\Sigma_{1,1}, \mathbb{Z})$. By the assumptions, we have the following

$$[C_1'] = p_1[v] + q_1[u], \qquad [C_2'] = p_2[v] + q_2[u], \qquad [C_3'] = [v] + q_3[u],$$
$$[C_{1,min}] = p_1[v] + q_{1,min}[u], \qquad [C_{2,min}] = p_2[v] + q_{2,min}[u], \qquad [C_{3,min}] = [v] + q_{3,min}[u]$$

for some integers p_1, p_2, q_1, q_2, q_3, $q_{1,min}$, $q_{2,min}$, $q_{3,min}$. Equations (10) and (17) imply

$$p_1q_2 - p_2q_1 = p_1q_{1,min} - p_2q_{2,min}, \qquad p_2q_3 - q_2 = p_2q_{3,min} - q_{2,min}, \qquad p_1q_3 - q_1 = p_1q_{3,min} - q_{1,min},$$

or, equivalently,

$$p_1(q_{3,min} - q_3) = q_{1,min} - q_1, \qquad p_2(q_{3,min} - q_3) = q_{2,min} - q_2.$$

This together with the identity $\tau_{1,0}\tau_{q,p}\tau_{1,0}^{-1} = \tau_{q+p,p}$ implies that the global conjugation of $\tau_{C_1'}^l \tau_{C_2'}^m \tau_{C_3'}^n$ by $\tau_C^{q_{3,min}-q_3}$ is equal to $\tau_{C_{1,min}}^l \tau_{C_{2,min}}^m \tau_{C_{3,min}}^n$. □

Theorem 4.9. *For each of the 14 extremal rational types, there exists a unique Lefschetz fibration over the disc (up to topological equivalence).*

Proof. Lemma 4.7 shows that any factorization $\tau_{C_1}\tau_{C_2}\tau_{C_3}$ satisfying (8) can be related by mutations to a factorization $\tau_{C_1'}\tau_{C_2'}\tau_{C_3'}$ with intersection numbers of vanishing cycles given by Equation (19). Lemma 4.8 then shows that $\tau_{C_1'}\tau_{C_2'}\tau_{C_3'}$ can be globally conjugated to $\tau_{C_{1,min}}^l \tau_{C_{2,min}}^m \tau_{C_{3,min}}^n$. Because mutations and global conjugation are invertible, this implies that any two factorizations satisfying (8) can be related by a sequence of mutations and a global conjugation. □

5 Lefschetz fibrations with 2 type I_1 fibers

The following definition was implicitly introduced in [4].

Definition 5.0.1. Let $[C_1]$, $[C_2]$ be two primitive homology classes in $H_1(\Sigma_{1,1}, \mathbb{Z})$ with $\langle [C_1], [C_2] \rangle = n > 0$. Let $[u]$, $[v]$ be some symplectic basis of $H_1(\Sigma_{1,1}, \mathbb{Z})$ such that

$$[C_1] = [u], \qquad [C_2] = n[v] + k[u] \tag{20}$$

for some $k \in \mathbb{Z}$. The residue class $k \pmod n$ is called the *Auroux invariant* of the pair of homology classes $[C_1]$, $[C_2]$.

Remark 5.0.1. Because we require $[C_2]$ to be a primitive homology class in Definition 5.0.1, the Auroux invariant is relatively prime to n.

Lemma 5.1. *The value of Auroux invariant does not depend on the choice of symplectic basis in Definition 5.0.1.*

Proof. Let $[C_1]$, $[C_2]$ be primitive homology classes with intersection number $n > 0$ and let $[u]$, $[v]$ be a symplectic basis of $H_1(\Sigma_{1,1}, \mathbb{Z})$ such that Equation (20) holds. The basis vector $[u]$ is uniquely determined by $[C_1]$. Therefore, under a change of basis the second basis vector can only change as $[v] \to [v] + m[u]$ for some integer m. Under such change of basis the value of k in Equation (20) changes as $k \to k - mn$. Therefore, $k \pmod n$ is independent of the choice of basis. □

Let n be a positive integer. Let H_n be the set of ordered pairs $([C_1], [C_2])$ of primitive homology classes $[C_1]$, $[C_2] \in H_1(\Sigma_{1,1,}, \mathbb{Z})$ such that $[C_1] \cdot [C_2] = n > 0$. The mapping class group $\mathrm{MCG}(\Sigma_{1,1})$ acts on H_n

$$([C_1], [C_2]) \to (\phi[C_1], \phi[C_2]). \tag{21}$$

There is an action of B_2 on H_n; the action of the generator $\sigma = \sigma_1$ (see Equation (2)) is given by

$$([C_1], [C_2]) \to (-\tau_{C_1}[C_2], [C_1]), \tag{22}$$

where C_1 is a simple closed curve representing $[C_1]$

Let F_n be the set of monodromy factorizations $\tau_{C_1}\tau_{C_2}$ of length 2 in $\mathrm{MCG}(\Sigma_{1,1})$ such that $\langle [C_1], [C_2] \rangle = \pm n$.

There is a bijective map $f : H_n \to F_n$ which maps a pair of primitive homology classes $([C_1], [C_2])$ to the monodromy factorization $\tau_{C_1}\tau_{C_2}$, where C_1, C_2 are simple closed curves representing $[C_1]$, $[C_2]$ respectively. Because the bijection $f : H_n \to F_n$ is equivariant with

respect to $\mathrm{MCG}(\Sigma_{1,1})$ and B_2 (see Appendix), we can define the Auroux invariant of an element of F_n as the Auroux invariant of its inverse image in H_n.

Lemma 5.2. *The Auroux invariant of an element of H_n changes as $k \to -k^{-1}$ under action of $\sigma \in B_2$.*

Proof. Let $([C_1], [C_2])$ be an element of H_n with Auroux invariant equal to k. Choose a symplectic basis $[u]$, $[v] \in H_1(\Sigma_{1,1}, \mathbb{Z})$ such that

$$[C_1] = [u], \qquad [C_2] = n[v] + k[u].$$

By Equation (1) we have

$$-\tau_{C_1}[C_2] = -(n[v] + (k+n)[u]).$$

Choose a symplectic basis $[u']$, $[v']$ of $H_1(\Sigma_{1,1}, \mathbb{Z})$ such that

$$-\tau_{C_1}[C_2] = [u'], \qquad [C_1] = n[v'] + k'[u']. \tag{23}$$

Equation (23) implies

$$1 \equiv -k'k \,(\mathrm{mod}\, n).$$

Therefore, the Auroux invariant of $\sigma([C_1], [C_2])$ is $-k^{-1}$. □

Lemma 5.3. *The monodromy factorizations $\tau_{C_1}\tau_{C_2}$ and $\tau_{C_3}\tau_{C_4}$ are equivalent under Hurwitz moves and global conjugation if and only if their Auroux invariants k_1, k_2 satify either $k_1 = k_2$ or $k_1 = -k_2^{-1}$.*

Proof. Assume that the Auroux invariants of $\tau_{C_1}\tau_{C_2}$ and $\tau_{C_3}\tau_{C_4}$ satisfy $k_1 = -k_2^{-1}$. After a Hurwitz move applied to $\tau_{C_1}\tau_{C_2}$ Auroux invariants become equal $k_1 = k_2 = k$, i.e. we have

$$[C_1] = [u], \qquad [C_2] = n[u] + k[u],$$
$$[C_3] = [u'], \qquad [C_4] = n[v'] + k[u']$$

for some symplectic bases $[u]$, $[v]$ and $[u']$, $[v']$ of $H_1(\Sigma_{1,1}, \mathbb{Z})$. Because the symplectic representation of $\mathrm{MCG}(\Sigma_{1,1})$ is surjective, there exists an element $\phi \in \mathrm{MCG}(\Sigma_{1,1})$ such that $\phi[u] = [u']$ and $\phi[v] = [v']$. Then ϕ conjugates $\tau_{C_1}\tau_{C_2}$ to $\tau_{C_3}\tau_{C_4}$.

To see the converse statement, note that global conjugation does not change the Auroux invariant of a factorization. Therefore Lemma 5.2 implies that if $\tau_{C_1}\tau_{C_2}$ and $\tau_{C_3}\tau_{C_4}$ are equivalent under Hurwitz moves and global conjugation, then either $k_1 = k_2$ or $k_1 = -k_2^{-1}$. □

Let $(\mathbb{Z}/m\mathbb{Z})^*$ be the set of invertible elements of the monoid $\mathbb{Z}/m\mathbb{Z}$.

Lemma 5.4. *The set of equivalence classes of the elements of F_n under Hurwitz moves and global conjugation is in bijection with the quotient of $(\mathbb{Z}/m\mathbb{Z})^*$ by the involution $k \to -k^{-1}$.*

Proof. The invariance of the Auroux invariant under global conjugation and Lemma 5.2 imply that the Auroux invariant map $k : H_n \to (\mathbb{Z}/m\mathbb{Z})^*$ induces a map from the set of equivalence classes of the elements of F_n under Hurwitz moves and global conjugation to the quotient $(\mathbb{Z}/m\mathbb{Z})^*$ by involution $k \to -k^{-1}$.

The induced map is surjective since k is surjective.

Lemma 5.3 implies that the induced map is injective. □

Define the function $\psi : \mathbb{Z} \to \{0, 1\}$ as follows

$$\psi(n) = \begin{cases} 1 \text{ if } n = 2^i k \text{ with } k \text{ odd and } 0 \leq i \leq 1 \\ 0 \text{ otherwise} \end{cases}$$

Theorem 5.5. *The number of distinct equivalence classes of elements of F_n under Hurwitz moves and global conjugation is*

$$\frac{\phi(n) + \psi(n) \prod \left(1 + (-1)^{\frac{p_i - 1}{2}}\right)}{2},$$

where ϕ is the Euler totient function and the product ranges over odd prime number dividing n.

Proof. Lemma 5.4 implies that we only have to find the cardinality of the quotient of $(\mathbb{Z}/n\mathbb{Z})^*$ by the involution $k \to -k^{-1}$. This is done in the appendix. □

6 Conclusion

We have established the topological uniqueness of Lefschetz fibrations of extremal rational type.

Our results do not concern fibrations of non-extremal rational type. A transition from topological uniqueness (exhibited by fibrations of extremal type) to a complete failure of topological uniqueness (exhibited by Auroux's examples) must occur in this regime. An interesting question is whether all Lefschetz fibrations of rational elliptic singularity type are algebraic.

Another problem that we did not consider is the problem of topological uniqueness for Lefschetz fibrations of extremal elliptic K3 singularity type. Our techniques yield less information about the intersections of vanishing cycles in this case because there are more singular fibers.

7 Acknowledgments

I would first like to thank my mentor Barış Kartal. I also would like to thank Prof. Paul Seidel for suggesting the problem of topological uniqueness. Dr. Tanya Khovanova and Dr. John Rickert have given me several useful suggestions regarding mathematical writing. I would like to thank MIT, CEE, and RSI for giving me the opportunity to come to the Research Science Institute. Lastly, I would like to acknowledge the financial support of JSC NIS.

References

[1] J. Milnor. *Morse theory*. Princeton University Press, 1963.

[2] R. E. Gompf. A new construction of symplectic manifolds. *Annals of Mathematics*, 142(3):527–595, 1995.

[3] B. Ozbagci and A. Stipsicz. Contact 3-manifolds with infinitely many inequivalent Stein fillings. *Proc. Amer. Math. Soc.*, (132):1549–1558, 2004.

[4] D. Auroux. Factorizations in $SL(2,\mathbb{Z})$ and simple examples of inequivalent Stein fillings. *Journal of Symplectic Geometry*, 13(2):261–277.

[5] B. V. Karpov and D. Y. Nogin. Three-block exceptional collections over Del Pezzo surfaces. *Izv. Math.*, 62(3):429–463, 1998.

[6] B. Farb and D. Margalit. *A primer on mapping class groups*. Princeton University Press, 2011.

[7] G. McShane and I. Rivin. Simple curves on hyperbolic tori. *C. R. Acad. Sci. Paris Sér. I Math.*, 320(12):1523–1528, 1995.

[8] R. Gompf and A. Stipsicz. *4-manifolds and Kirby calculus*. A.M.S., 1999.

[9] D. Auroux. Mapping class group factorizations and symplectic 4-manifolds: some open problems. In *Problems on Mapping Class Groups and Related Topics*, volume 74 of *Proc. Symp. Pure Math.*, pages 123–132. Amer. Math. Soc., 2006.

[10] P. U. Miranda, Rick. On extremal rational elliptic surfaces. *Mathematische Zeitschrift*, 193:537–558, 1986.

A Equivariance lemmas

We prove that the map f defined in Section 5 is equivariant with respect to the action of $\mathrm{MCG}(\Sigma_{1,1})$ and B_2.

Lemma A.1. *Let B_2 act on H_n according to Equation (22) and act on F_n by Hurwitz moves. Then the map f is equivariant with respect to B_2.*

Proof. Let $([C_1], [C_2])$ be an element of H_n. Then

$$f(\sigma([C_1], [C_2])) = f((-\tau_{C_1}[C_2], [C_1])) = \tau_{\tau_{C_1}C_2}\tau_{C_2} = \sigma f(([C_1], [C_2])).$$

□

Lemma A.2. *Let $\mathrm{MCG}(\Sigma_{1,1})$ act on H_n according to Equation (21) and act on F_n by global conjugation. Then the map f is equivariant with respect to $\mathrm{MCG}(\Sigma_{1,1})$.*

Proof. Let $([C_1], [C_2])$ be an element of H_n. Then

$$f(\phi([C_1], [C_2])) = f((\phi[C_1], \phi[C_2])) = \tau_{\phi C_1}\tau_{\phi C_2} = \phi\tau_{C_1}\phi^{-1} \cdot \phi\tau_{C_2}\phi^{-1} = \phi f([C_1], [C_2]).$$

□

B Number–theoretic lemmas

Let n be a positive integer and $\mathbb{Z}/n\mathbb{Z}$ the monoid of residue classes mod n. Let $(\mathbb{Z}/n\mathbb{Z})^*$ be the set of invertible elements of $\mathbb{Z}/n\mathbb{Z}$. By the definition of Euler's totient function ϕ, we have $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$. Here we compute the cardinality of the quotient of $(\mathbb{Z}/n\mathbb{Z})^*$ by the involution $k \to -k^{-1}$.

The fixed points of the involution $k \to -k^{-1}$ are residue classes k satisfying $k^2 = -1 \pmod n$. Denote the number of such residue classes by $r(n)$.

Lemma B.1. *Let n be a positive integer having the following decomposition into prime*

powers

$$n = \prod_{i=1}^{m} p_i^{a_i}.$$

Then $r(n) = \prod_{i=1}^{m} r(p_i^{a_i})$.

Proof. Let us construct a bijection between the set $R(n)$ of residue classes in $\mathbb{Z}/n\mathbb{Z}$ satisfying $k^2 \equiv -1 \pmod{n}$ and the direct product $\prod_{i=1}^{m} R(p_i^{a_i})$ of the sets of residue classes satisfying $k^2 \equiv -1 \pmod{p_i^{a_i}}$ for $1 \leq i \leq m$.

If we have an integer k such that $k^2 + 1 \equiv 0 \pmod{n}$, then obviously $k^2 + 1 \equiv 0 \pmod{p_i^{a_i}}$ for $1 \leq i \leq m$. This defines a map $R(n) \to \prod_{i=1}^{m} R(p_i^{a_i})$.

Now suppose we are given a collection of integer $k_1, \ldots, k_m$ such that $k_i^2 + 1 \equiv 0 \pmod{p_i^{a_i}}$ for $1 \leq i \leq m$. By the Chinese remainder theorem, there exists an integer k such that $k \equiv k_i \pmod{p_i^{a_i}}$ for $1 \leq i \leq m$. Moreover, the integer k is unique mod n. Therefore, $k^2 + 1 \equiv k_i^2 + 1 \equiv 0 \pmod{n}$ for $1 \leq i \leq m$. This implies that $k^2 + 1 \equiv 0 \pmod{n}$ so we have constructed a map $\prod_{i=1}^{m} R(p_i^{a_i}) \to R(n)$. Because the integer k is unique mod n, this map is inverse to the previously constructed map $R(n) \to \prod_{i=1}^{m} R(p_i^{a_i})$. □

Lemma B.2. *Let p be an odd prime number and a be a positive integer. Then* $r(p^a) = 1 + (-1)^{\frac{p-1}{2}}$.

Proof. If $p \equiv 3 \pmod{4}$ then obviously $r(p^a) = 0$. Therefore, we may assume that $p \equiv 1 \pmod{4}$.

Let us prove that $r(p^a) \leq 2$ for any positive integer a. Assume that $r(p^{a_0}) \geq 3$ for some positive integer a_0. Then there exist 2 integers x, y such that $x^2 \equiv y^2 \equiv -1 \pmod{p^{a_0}}$, $x \not\equiv y \pmod{p^{a_0}}$ and $x + y \not\equiv 0 \pmod{p^{a_0}}$. Then we have

$$x^2 - y^2 \equiv (x - y)(x + y) \equiv 0 \pmod{p^{a_0}}.$$

Because $x + y \not\equiv 0 \pmod{p^{a_0}}$ and $x - y \not\equiv 0 \pmod{p^{a_0}}$, there exists an integer s such that $0 < s < a_0$ and

$$x - y = tp^s,$$

where t is an integer relatively prime to p. Therefore,

$$(y + tp^s) \equiv y^2 + t^2p^{2s} + 2tp^s y \equiv -1 \,(\mathrm{mod}\, p^{a_0}).$$

If we substract $y^2 \equiv -1 \,(\mathrm{mod}\, p^{a_0})$ from both sides, we have

$$t^2p^{2s} + 2tp^s y \equiv 0 \,(\mathrm{mod}\, p^{a_0}).$$

This implies

$$2tp^s y \equiv 0 \,(\mathrm{mod}\, p^{\min(2s,a_0)}.$$

Because t is relatively prime to p, this implies that $y \equiv 0 \,(\mathrm{mod}\, p)$. This is a contradiction because by assumption $y * (-y) \equiv 1 \,(\mathrm{mod}\, p)$, i.e. y is invertible mod p.

Now we prove that $r(p^a) \geq 2$ for any positive integer a. Let us first consider the case $a = 1$. We know from Euler's criterion that $r(p) > 0$, i.e. there exists an integer k such that $k^2 \equiv -1 \,(\mathrm{mod}\, p)$. Note that $k' = -k$ satisfies $k'^2 \equiv -1 \,(\mathrm{mod}\, p)$ and that $k' \not\equiv k \,(\mathrm{mod}\, p)$ because p is odd. Therefore, $r(p) \geq 2$.

Assume that we know that $r(p^a) \geq 2$ for some positive integer a. We claim that $r(p^{a+1}) \geq 2$. Let k be an integer such that $k^2 \equiv -1 \,(\mathrm{mod}\, p^a)$. Let us find an integer q such that $(p^a q + k)^2 \equiv -1 \,(\mathrm{mod}\, p^{a+1})$. We have

$$(p^a q + k)^2 \equiv p^{2a}q^2 + k^2 + 2p^a qk \equiv k^2 + 2p^a qk \equiv -1 \,(\mathrm{mod}\, p^{a+1}),$$

or equivalently

$$p^a q \equiv -2^{-1}(k + k^{-1}) \,(\mathrm{mod}\, p^{a+1}), \tag{24}$$

where the inverses are taken in the monoid $\mathbb{Z}/p^{a+1}\mathbb{Z}$. Because $k + k^{-1} \equiv 0 \,(\mathrm{mod}\, p^a)$, we can divide both sides of Equation (24) by p^a to get q. Because $-(p^a q + k)^2 \equiv -1 \,(\mathrm{mod}\, p^{a+1})$ and $-(p^a q + k) \not\equiv p^a q + k \,(\mathrm{mod}\, p^{a+1})$, we have $d(p^a) \geq 2$. □

Considering quadratic residues mod 4, we see that $d(2^a)$ is 1 for $0 \leq a \leq 1$ and 0 for $a \geq 2$.

Proposition B.3. *Let n be a positive integer having the following decomposition into prime*

powers

$$n = 2^{a_1} \prod_{i=2}^{m} p_i^{a_i}.$$

The cardinality of the quotient of $(\mathbb{Z}/n\mathbb{Z})^*$ *by the involution* $k \to -k^{-1}$ *is*

$$\frac{\phi(n) + \psi(n) \prod_{i=2}^{m} \left(1 + (-1)^{\frac{p_i - 1}{2}}\right)}{2},$$

where

$$\psi(n) = \begin{cases} 1 \text{ if } n = 2^i k \text{ with } k \text{ odd and } 0 \leq i \leq 1 \\ 0 \text{ otherwise} \end{cases}$$

Proof. We have proved that the number of fixed points of the involution equals $r(n) = \psi(n) \prod_{i=2}^{m} \left(1 + (-1)^{\frac{p_i - 1}{2}}\right)$. Therefore, the cardinality of the quotient is

$$\frac{\phi(n) - r(n)}{2} + r(n) = \frac{\phi(n) + \psi(n) \prod_{i=2}^{m} \left(1 + (-1)^{\frac{p_i - 1}{2}}\right)}{2}.$$

□